UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS VII – GOVERNADOR ANTÔNIO MARIZ
CENTRO DE CIÊNCIAS EXATAS E SOCIAIS APLICADAS – CCEA
CURSO DE LICENCIATURA EM COMPUTAÇÃO

THEOPHALES DANTAS DE SOUSA

ANÁLISE DE VULNERABILIDADES COM O OPENVAS E O LANGUARD E PROPOSTA DE SEGURANÇA PARA REDES DE COMPUTADORES DE PEQUENO E MÉDIO PORTE

PATOS – PB
2016

THEOPHALES DANTAS DE SOUSA

ANÁLISE DE VULNERABILIDADES COM O OPENVAS E O LANGUARD E PROPOSTA DE SEGURANÇA PARA REDES DE COMPUTADORES DE PEQUENO E MÉDIO PORTE

Trabalho de Conclusão de Curso apresentada ao Curso de Licenciatura Plena em Computação da Universidade Estadual da Paraíba, em cumprimento à exigência para obtenção do título de Licenciado em Computação.

Orientador: Prof. Pablo Roberto Fernandes de Oliveira

PATOS – PB

2016

S725a Sousa, Theophales Dantas de
Análise de vulnerabilidades com o OpenVAS e o LanGuard e proposta de segurança para redes de computadores de pequeno e médio porte [manuscrito] / Theophales Dantas de Sousa. - 2016.
27 p. : il. color.

Digitado.
Trabalho de Conclusão de Curso (Graduação em Computação) - Universidade Estadual da Paraíba, Centro de Ciências Exatas e Sociais Aplicadas, 2016.
"Orientação: Prof. Esp. Pablo Roberto Fernandes de Oliveira, CCEA".

1. Redes de Computadores. 2. Segurança de rede de computadores. 3. OpenVAS. 4. LanGuard. 5. BrazilFW. I. Título.
21. ed. CDD 004.6

Theophales Dantas de Sousa

ANÁLISE DE VULNERABILIDADES COM O OPENVAS E O LANGUARD E PROPOSTA DE SEGURANÇA PARA REDES DE COMPUTADORES DE PEQUENO E MÉDIO PORTE

Trabalho de Conclusão de Curso apresentado ao Curso de Licenciatura em Computação da Universidade Estadual da Paraíba, em cumprimento à exigência para obtenção do grau de Licenciado em Computação

Aprovado em 18 de outubro de 2016

BANCA EXAMINADORA

Pablo Roberto Fernandes de Oliveira
Pablo Roberto Fernandes de Oliveira
(Orientador)

Nadia Farias dos Santos
Nádia Farias dos Santos
(Examinadora)

Wellington C. Araujo
Wellington Candeia de Araujo
(Examinador)

ANÁLISE DE VULNERABILIDADES COM O OPENVAS E O LANGUARD E PROPOSTA DE SEGURANÇA PARA REDES DE COMPUTADORES DE PEQUENO E MÉDIO PORTE

Theophales Dantas de Sousa[1]

RESUMO

Este artigo apresenta uma abordagem sobre a Segurança da Informação nas redes de computadores dando ênfase as vulnerabilidades, propondo a utilização de um *Firewall* para gerenciar redes de pequeno e médio porte. Para tanto realizou-se um estudo de caso para verificar a segurança de uma rede de computadores de uma empresa utilizando ferramentas de escaneamento de vulnerabilidades de sistemas, são apresentadas duas ferramentas muito utilizadas atualmente por administradores de redes, uma proprietária que é o LanGuard e outra software livre que é o OpenVAS. Devido a vasta gama de vulnerabilidades em aplicações e sistemas que colocam em risco a segurança da informação, a utilização destas ferramentas é de grande importância para um monitoramento preventivo do ambiente. Concluiu-se que a utilização dessas ferramentas atingiram o objetivo proposto pois o retorno obtido pelos softwares expôs informações que poderiam deixar os sistemas vulneráveis. Por fim apresentamos uma proposta de utilização de um servidor *Firewall* eficaz e de baixo custo para gerenciamento de redes de pequeno e médio porte o BrazilFW.

Palavras-chave: Redes de Computadores. Segurança. OpenVAS. LanGuard. BrazilFW.

1 INTRODUÇÃO

Em decorrência dos benefícios que as redes de computadores oferecem, o seu crescimento é cada vez maior, uma vez que seus recursos e aplicações tornam-se ainda mais indispensáveis. Com esta expansão, a possibilidade de ocorrerem problemas de segurança também aumenta, podendo levar as redes a um estado de inoperância ou a níveis inadequados de desempenho

Nos dias atuais é difícil imaginar algum computador que não esteja conectado em uma rede, segundo Zotto (2012) até mesmo os dispositivos móveis como celulares, ipads, não conseguem ficar isolados de qualquer rede que seja. Neste âmbito, temos a maior parte destas redes e destes computadores interligados em uma grande rede, formando uma conectividade global através da Internet.

Segundo Brasil Escola (2016) A internet é a rede mundial de computadores, ou seja, um grande conjunto de redes de computadores interligadas pelo mundo inteiro que permite o acesso e troca de informações em qualquer lugar do planeta, e com essa grandiosidade cresce a preocupação com a segurança da informação e as vulnerabilidades existentes. Porém,

[1] Aluno de Graduação em Licenciatura da Computação na Universidade Estadual da Paraíba – Campus VII
E-mail: theophales@gmail.com

mesmo com tantos riscos é difícil controlar as pessoas e organizações sobre o modo de uso da internet e da rede, e que usem estratégias eficazes para assegurar seus dados e informações corporativas.

O presente trabalho, tem por objetivo apresentar alguns tópicos relacionados à segurança de rede, mais especificamente a segurança de redes de pequeno e médio porte, com a aplicação de um estudo de caso.

A partir dos conceitos sobre segurança, buscando conhecer as principais técnicas de segurança, analisar s*oftwares* que possibilitem a técnica de varredura de vulnerabilidades, buscando em seus resultados uma possibilidade para que as vulnerabilidades sejam controladas e suspensas, a fim de prevenir ações de caráter prejudicial ao sistema.

Foi apresentado uma proposta de implantação do BrazilFW que é uma ferramenta de baixo custo e de fácil configuração e administração para prevenção de falhas de segurança na rede, e um maior controle das informações que trafegam na rede.

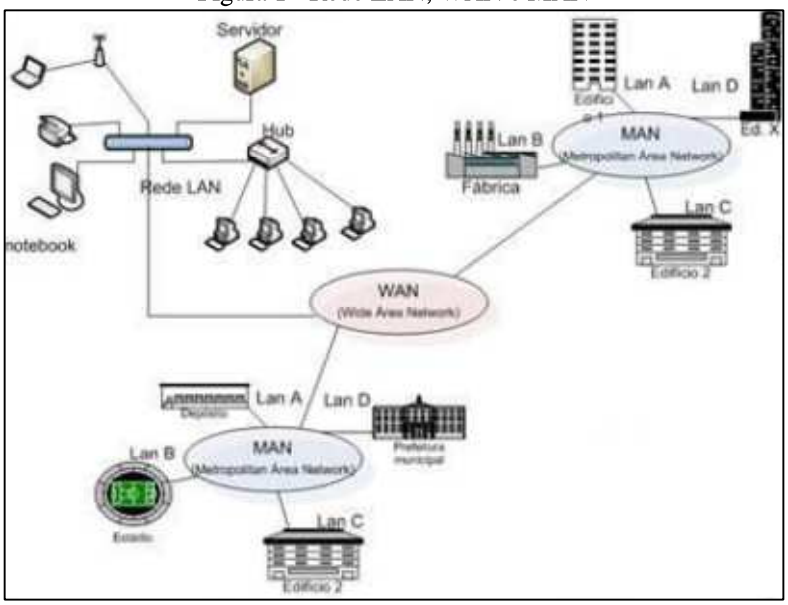
2 REDES DE COMPUTADORES

Segundo Miranda (2008) Uma rede de computadores é uma conexão de dois ou mais computadores para permitir o compartilhamento de recursos e a troca de informações entre as máquinas, é importante ressaltar que uma rede não precisa ser constituída unicamente por computadores, sendo comum a presença de impressoras, scanners e outros dispositivos de rede.

Um dos objetivos da criação das redes foi compartilhar recursos com os usuários, como aplicações, equipamentos e dados, independentemente da localização física deste recurso ou do próprio usuário, um exemplo de rede mundialmente difundida é a *Internet,* que possui milhares de computadores interconectados trocando as mais diversas informações, tais como *e-mail*, arquivos, páginas pessoais e corporativas.

Segundo Tanenbaum (2003, p. 27). "As redes possuem diversos tamanhos, entretanto as classificações mais comuns são: *Local Area Network* (LAN), *Wide Area Network* (WAN) e *Metropolitan Area Network* (MAN)", conforme a Figura 1.

Figura 1 - Rede LAN, WAN e MAN



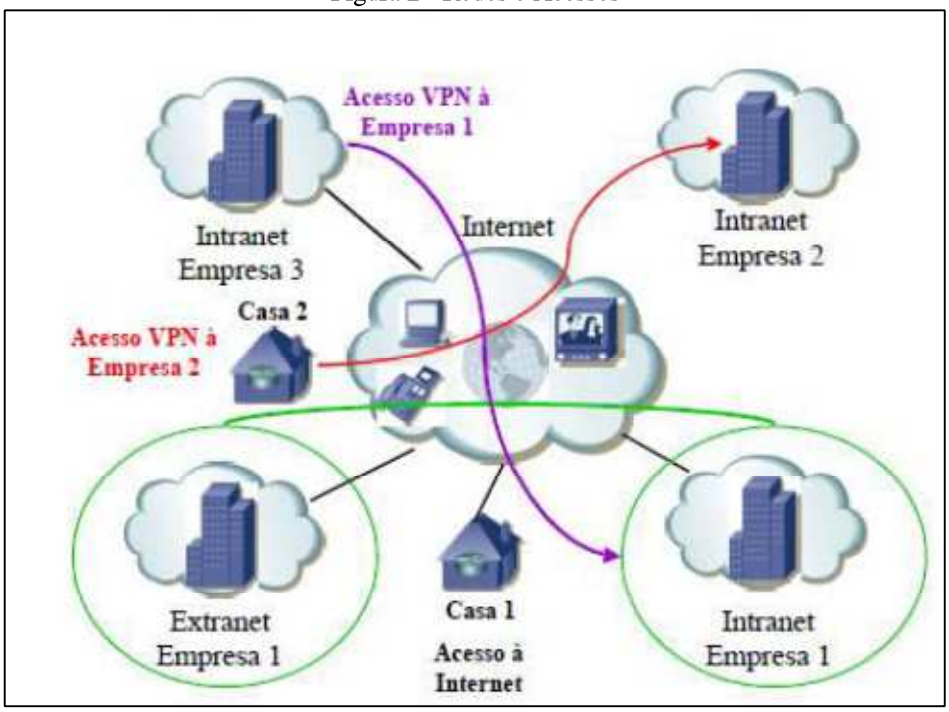
Fonte: Disponível em: <http://www.metropoledigital.ufrn.br/aulas/disciplinas/sist_conect/aula_03.html> Acesso em jun. 2014

Os tipos de redes são conceituadas como segue (TANENBAUM, 2003):

- LAN (*Local Area Network* – Redes Locais): São redes em que os computadores localizam-se em uma faixa que varia de poucos metros até alguns quilômetros, abrangendo instalações em escritórios, residências, prédios comerciais e industriais.
- MAN (*Metropolitan Area Network* – Redes Metropolitanas): São redes de computadores onde a localização entre as máquinas começa a atingir distâncias metropolitanas. Abrange uma região com dimensões bem maiores do que a das redes LAN, normalmente um campus de uma universidade, a instalação de uma fábrica e seus escritórios, ou até uma cidade inteira.
- WAN (*Wide Area Network* – Redes Geograficamente Distribuídas): Esse tipo de rede apareceu devido à necessidade de compartilhamento de recursos entre usuários geograficamente dispersos, este tipo de rede tem dimensões geográficas imensuráveis. Isto quer dizer que ela pode interligar todos os continentes, países e regiões extensas utilizando enlaces mais extensos, como satélites ou cabos (submarinos ou terrestres), etc.

Alguns dos conceitos importantes de redes é a *Internet, Intranet, Extranet* e VPN. Abaixo segue uma descrição de cada um desses conceitos como mostra a Figura 2.

Figura 2 - Redes e Acessos



Fonte: WEBER, 2012? p. 12.

- *Internet*: É o conjunto de redes de computadores interligadas pelo mundo inteiro. Utiliza a arquitetura TCP/IP, disponibiliza o acesso a serviços, permite a comunicação e troca de informação aos usuários do planeta.
- *Intranet*: É a rede de computadores de uma determinada organização, baseada na arquitetura TCP/IP. Fornece serviços aos empregados, e permite a comunicação entre os mesmos, de forma controlada, ao ambiente externo (a *Internet*). Também conhecida como Rede Corporativa.
- *Extranet*: É um conceito que permite o acesso, de funcionários e fornecedores de uma organização, aos recursos disponibilizados pela *Intranet*. Podemos dizer que é uma extensão da *Intranet*. Desta maneira, podemos disponibilizar um padrão unificado entre as diversas empresas, filiais, do grupo.
- VPN (Rede Privada Virtual): É uma rede virtual estabelecida entre dois ou mais pontos, que oferece um serviço que permite o acesso remoto, de funcionários ou fornecedores a uma determinada rede, a fim de executarem suas tarefas. Muito utilizada por funcionários, para terem acesso aos *e-mails* corporativos via *Intranet*, ou para as equipes de suporte técnico solucionarem problemas em seus sistemas de maneira remota.

Segundo Pinheiro (2006) À medida que essas redes foram crescendo e tornando-se integradas às organizações. As redes passaram então a fazer parte do cotidiano das pessoas

como uma ferramenta que oferece recursos e serviços que permitem uma maior interação entre os usuários e um consequente aumento de produtividade.

Além dos serviços de compartilhamento de recursos, novos serviços, tais como correio eletrônico, transferência de arquivos, *Internet*, aplicações multimídia, dentre outras, foram acrescentadas, aumentando ainda mais a complexidade das redes. (Pinheiro, 2006)

Para Melchiors (1999 apud SANTOS, 2010, p. 2) o crescimento do número e da heterogeneidade dos equipamentos envolvidos nas redes, o número de problemas potenciais e a complexidade envolvida nestes problemas tornam-se críticos, e exigem que os gerentes de rede possuam uma vasta quantidade de informação sobre as redes manuseadas e os problemas destas.

Definitivamente uma rede sem gerenciamento está muito mais suscetível a falhas de segurança, ficando mais vulnerável a ataques, ameaças, intrusões e violações.

3 SEGURANÇA DE REDES

Segundo Tanenbaum (2003), a segurança de redes em sua forma mais simples se preocupa em garantir que pessoas mal-intencionadas não leiam ou, pior ainda, modifiquem secretamente mensagens enviadas a outros destinatários e não tenham acesso a serviços remotos sem autorização.

Segurança em tecnologia da informação é definida como: "a capacidade de assegurar a prevenção ao acesso e à manipulação ilegítima da informação, ou ainda, de evitar a interferência indevida na sua operação normal" (ISO, 2005). Segundo os padrões internacionais a segurança é fundamentada em três propriedades básicas:

- **Confidencialidade:** Propriedade que limita o acesso à informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação, essa propriedade protege a informação para que não seja acessada por pessoas não autorizadas.
- **Integridade:** Propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (nascimento, manutenção e destruição), é a garantia que sua informação permanece íntegra, que não sofreu nenhuma alteração feita por terceiros.
- **Disponibilidade:** Propriedade que garante a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação.

A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. Isto pode ser feito em conjunto com outros processos de gestão do negócio. (ABNT NBR ISO/IEC 17799, 2005, p. 09).

3.1 Vulnerabilidades

Uma vulnerabilidade é um ponto onde o sistema é susceptível a um ataque. Segundo Cert.br (2014a) "Uma vulnerabilidade é definida como uma condição que, quando explorada por um atacante, pode resultar em uma violação de segurança", ou seja, qualquer característica que um sistema possa apresentar que permita a usuários não autorizados assumir o controle sobre ele, ou o impeça de operar corretamente.

Vulnerabilidades são resultados de falhas nas implementações de sistemas operacionais, serviços, aplicativos e protocolos, que podem ser exploradas por atacantes para executar ações maliciosas, como invadir um sistema, acessar informações confidenciais, disparar ataques contra outros computadores ou tornar um serviço inacessível (NAKAMURA; GEUS, 2007 apud BUZZATTE, 2014).

A análise de rede é um dos passos iniciais na busca por vulnerabilidades, normalmente, precede outros tipos de ataque mais específicos, sendo considerado como fase de reconhecimento de alvo. A análise de rede de computadores tem como objetivo a identificação de 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 (CERT.BR, 2014).

Muitas vulnerabilidades são exploradas ou criadas a partir de softwares desenvolvidos para este fim conhecidos como malwares, que são programas que produzem efeitos danosos e indesejados.

Rodrigues (2010 apud BUZZATTE, 2014) destaca algumas falhas que podem ocorrer deixando vulnerável um sistema de informação, que são:

- Bugs: Erro no funcionamento de um software, normalmente devido a falhas de programação durante a fase de desenvolvimento, que podem ocasionar falhas na segurança da rede;

- Não cumprimento das regras básicas de segurança: Utilizadores do sistema, pelas suas ações, podem causar diversas vulnerabilidades, tais como acesso a serviços duvidosos ou inseguros, senhas com fácil decifração, entre outros;
- Desinteresse dos Administradores pela Segurança: Falta de políticas de segurança.

Ao contrário daquilo que muita gente pensa, os tipos de vulnerabilidades existentes para os computadores são muitos e não se cingem apenas aos vírus informáticos. Por exemplo, um programa desatualizado é uma vulnerabilidade, pois tendo em conta o rápido desenvolvimento na informática, sempre que é lançada uma nova versão de um programa, significa que na maior parte das vezes, este foi aprimorado não só graficamente, mas também no que diz respeito à segurança.

3.2 Mecanismos de segurança

3.2.1 Criptografia

Com a vulnerabilidade dos mecanismos de comunicação sempre existe a possibilidade de interceptação dos dados trafegados. Como muitas vezes é impossível garantir a confiabilidade do meio de transmissão, passou-se a utilizar para uma técnica para esconder a mensagem caso esta fosse interceptada durante o trajeto, chamada de criptografia.

Tanto Stallings (2008, p.18) quanto Tanenbaum (2003, p.545), afirmam que a criptografia é uma ferramenta fundamental para prover segurança, pois por meio dela, é possível atender a todos os requisitos clássicos. A maioria dos ataques a redes poderia ser solucionada pela utilização de um mecanismo criptográfico seguro. A criptografia é separada em dois ramos: simétrica e assimétrica.

- **Simétrica**: também chamada de algoritmo simétrico ou criptografia de chave simples é uma criptografia tão forte que seus algoritmos são de acesso ao público. A chave simétrica utiliza a mesma chave para codificação e decodificação.
- **Assimétrica:** (ou criptografia de chave pública) são utilizadas duas chaves diferentes. Uma para cifrar e outra para decifrar, a chave pública e privada. A chave pública deve ser distribuída aos membros da rede, enquanto que a privada deve ser mantida em segredo pelo nó.

Para Gomes (2004, p.81), A criptografia computacional protege o sistema quanto à ameaça de perda de confiabilidade, integridade ou não repúdio, é utilizada para garantir:

- **Sigilo:** somente os usuários autorizados têm acesso à informação.
- **Integridade:** garantia oferecida ao usuário de que a informação correta, original, não foi alterada, nem intencionalmente, nem acidentalmente.

- **Autenticação de usuário:** é o processo que permite a um usuário certificar-se que a mensagem recebida foi de fato enviada pelo remetente.
- **Autenticação de destinatário:** consiste em provar que a mensagem é atual, não se tratando de mensagens antigas reenviadas.

3.2.2 Firewall

Segundo Miranda (2008) Os Firewalls são mecanismos muito utilizados para aumentar a segurança de redes conectadas à Internet. São uma espécie de barreira de proteção constituídas de um conjunto de hardware, software ou ambos que garantem uma política de controle de acesso entre duas redes (normalmente a Internet e uma rede LAN).

De acordo com Kurose e Ross (2010, p. 535).

> Um firewall é uma combinação de hardware e software que isola a rede de uma organização da internet em geral, permitindo que alguns pacotes passem e bloqueando outros. Um firewall permite que um administrador de rede controle o acesso entre o mundo externo e os recursos da rede que administra gerenciando o fluxo de tráfego de e para esses recursos.

Basicamente os Firewalls são divididos em três categorias e utiliza um ou mais dos seguintes métodos para controlar o tráfego que circula na rede. Miranda (2008, p. 290) define essas categorias como:

- Filtragem de pacotes: os pacotes de dados são analisados e confrontados com um conjunto de filtros predefinidos pela configuração do firewall, por parte do utilizador. Os pacotes de dados que estiverem de acordo com os padrões pré-estabelecidos pela configuração passam pelo firewall, caso contrário serão pura e simplesmente recusados.
- Firewalls de aplicação: a informação da *Internet* é recolhida pelo firewall e seguidamente enviada para o sistema requisitante e vice-versa.
- Firewalls baseados no estado: ao contrário da filtragem de pacotes, este método inspeciona cada ligação que atravessa todas as interfaces do firewall assegurando-se que é fidedigna.

3.4 Políticas de segurança

Uma política de segurança é um instrumento importante para proteger a sua organização contra ameaças à segurança da informação que a ela pertence ou que está sob sua

responsabilidade. Uma ameaça é compreendida neste contexto como a quebra de uma ou mais de suas três propriedades fundamentais (confidencialidade, integridade e disponibilidade).

As políticas de segurança são compostas por um conjunto de regras e padrões sobre o que deve assegurar que as informações e serviços importantes para uma determinada empresa recebam a proteção conveniente, de modo garantir a confidencialidade, integridade e disponibilidade (FERREIRA & ARAÚJO, 2008, p. 36).

A política de segurança não define procedimentos específicos de manipulação e proteção da informação, mas atribuem direitos e responsabilidades às pessoas (usuários, administradores de redes e sistemas, funcionários, gerentes, etc.) que lidam com essa informação.

4 TRABALHOS RELACIONADOS

Este estudo apresenta uma análise à segurança em redes de computadores, com ênfase no uso de *software* de descoberta de vulnerabilidades. Foram encontrados alguns estudos com escopo semelhantes que serviram para nortear os rumos da pesquisa.

Buzzate (2014) apresenta scanners detectores de vulnerabilidades capazes de realizar a varredura das redes domésticas e corporativas e apresentar relatórios indicando os pontos mais propensos às vulnerabilidades, bem como portas abertas, serviços ativos e patches ausentes, equiparando instalação, usabilidade, eficiência e resultados dos scanners de vulnerabilidades LanGuard, Nessus e OpenVAS. Conclui em seu estudo os principais pontos positivos e negativos de cada *software.*

Proposta semelhante é feita por Martinelo e Bellezi (2014) que em estudo recente abordam os principais tipos de vulnerabilidades e ataques conhecidos. Defendem o uso de *software* no auxílio de descobertas possíveis ameaças, com uma comparação de resultados do escaneamento entre Nessus e OpenVAS. Concluindo como positivo o uso de ambos principalmente porque também servem de auxílio na prevenção e seus relatórios sugerem possíveis soluções aos riscos detectados.

Moreira et al. (2008) defendem a análise de riscos como processo essencial de qualquer programa de gerência de segurança da informação. Para o estudo foram utilizados os *scanners* Nessus e LanGuard, Tendo por objetivo encontrar medidas cabíveis e de fácil aplicação, para as diferentes situações de riscos detectadas.

O trabalho proposto e os demais citados acima está a visão de que no cenário atual onde as ameaças aumentam em ritmo avanço justifica a importância de toda ferramenta que venha de alguma forma contribuir na manutenção da segurança.

5 METODOLOGIA

A metodologia adotada por este trabalho foi um estudo de caso (GIL, 2009) que se constituiu na identificação de vulnerabilidades em redes de computadores, em que se verifica e analisa as vulnerabilidades que existem em um determinado sistema. Foram utilizados scanners detectores de vulnerabilidades OpenVAS e LanGuard e feito uma proposta de segurança para a realização do projeto de segurança em rede para redes de pequeno e médio porte, primeiro foi mostrado o conceito de Rede (capítulo 2), e o conceito de Segurança de redes de computadores (capítulo 3), para facilitar a compreensão do trabalho abordado.

Realizou-se um breve estudo sobre as ferramentas de análises de vulnerabilidades utilizadas (capítulo 6). Foi selecionada a rede do Instituto Estrela de fomento ao microcrédito para a realização de testes práticos, com intuito de analisar o desempenho e os modelos de relatórios apresentados por cada programa. Os resultados relativos às vulnerabilidades da rede escaneada foram então visualizados de maneira diferente em cada software.

Depois de feito o estudo sobre análise de vulnerabilidade, foi feita uma proposta com soluções para os problemas encontrados na maioria das redes de pequeno e médio porte, e configuração de uma ferramenta de auxílio para segurança de redes de computadores, que vai estar em apêndice (Apêndice A). A partir deste ponto serão elencados quais serviços são explicitamente necessários e quais devem ser proibidos, com base nas principais redes utilizadas atualmente.

6 ANÁLISE DAS VULNERABILIDADES COM O OPENVAS E LANGUARD

O Profissional de segurança possui em mãos ferramentas de apoio que vão facilitar o seu trabalho, alguns *softwares* existentes que atendem ao requisito no processo de escaneamento de redes são: Retina, *Microsoft Baseline Security Analyzer* (MBSA), *Core Impact*, GFI *LanGuard, QualysGuard, Nexpose*, *Open Vulnerability Assessment System* (OpenVAS) e Nessus. Para este trabalho serão usadas as seguintes ferramentas: *LanGuard* e OpenVAS.

LanGuard por ser umas das principais ou a principal ferramenta paga e OpenVAS por ser a principal ferramenta *opensource*.

6.1 LanGuard

Segundo Buzzate (2014) esta ferramenta foi criada em 2000 pela empresa GFI Software, o seu objetivo é assegurar o bom funcionamento de uma rede local, é um scanner de

segurança que oferece solução de gerenciamento de patches (atualização de segurança) e auditoria de rede e sua versão é disponível apenas para Microsoft Windows.

Uma das principais ferramentas de pesquisa da vulnerabilidade, o LanGuard pode ser encontrado no sítio (languard.gfi.com). Ela se encontra na categoria dos scanners 'híbridos'. O mesmo possui características de detecção de portas e vulnerabilidades. Segundo Queiroz (2007, p. 36) o LanGuard é classificado como uma boa ferramenta para ser usada no dia-a-dia, pelos administradores de redes. O LanGuard apresenta como principais características:

- O gerenciamento de *patches*
- A avaliação da vulnerabilidade
- Auditoria de gestão de rede
- Observância
- Relatórios BYOD[2]
- A descoberta de rede
- Atualização de software terceiros
- A exploração das portas

A Seguir, a Figura 3 representa a tela inicial da ferramenta LanGuard.

Figura 3 - A tela inicial do LanGuard.

Fonte: Autor

[2] B.Y.O.D. é a sigla para "Bring Your Own Device", significa na prática que a empresa permite que você utilize seus próprios dispositivos para acessar informações corporativas.

6.2 OpenVAS

O OpenVAS é um sistema de avaliação de vulnerabilidades de código aberto, é uma estrutura de vários serviços e ferramentas que oferecem uma solução abrangente e poderosa varredura de vulnerabilidades e gerenciamento de vulnerabilidades. Distribuído sob a licença GPL *General Public license* (GNU), e é um fork[3] livre do buscador de vulnerabilidade Nessus. O propósito inicial do projeto era permitir o livre desenvolvimento do agora proprietário Nessus *Security Scanner*. Possui versões disponíveis para as distribuições do Linux: Debian, Fedora, OpenSuse, RedHat, além de versão para Windows.

Segundo Schwarzer (2011) citador por Buzzatte (2014) OpenVAS oferece um ambiente completo de avaliação de segurança, com uma série de serviços e componentes que podem ser organizados em diversas formas para construir um ambiente de avaliação adequado a rede. OpenVAS assim como o Nessus segue o modelo cliente/servidor, o servidor é o componente central que contém as funcionalidades utilizadas para execução de um grande número de testes, é responsável pelo agendamento e pela execução de buscas. O cliente é constituído de uma interface gráfica onde é possível configurar as atividades, como buscas e acessar os resultados.

O OpenVAS possui algumas ferramentas de segurança integradas, as quais incluem-se o nmap (scanner de portas), nikito (teste de servidor web), ike-scan (varreduras em servidores IPsec), entre outros. Após completar a varredura da rede OpenVAS oferece um relatório listando os detalhes com base nas portas, serviços encontrados em sua rede, ele destaca as vulnerabilidades com prioridades alta, moderada e baixa, sendo possível exportá-lo em vários formatos, incluindo HTML, XML e PDF (BUZZATTE, 2014).

6.3 Descrição de ambiente de teste

Após descrição dos programas, foram realizados os testes práticos, com intuito de analisar a execução e os modelos de relatórios apresentados por cada um. Os resultados relativos às vulnerabilidades da rede serão visualizados de maneiras diferentes em cada software. Para a realização dos testes foi escaneada a rede do Instituto Estrela de fomento ao microcrédito. O LanGuard foi aplicado primeiro, enquanto o OpenVAS teve seus recursos testados logo em seguida.

Esta etapa tem como objetivo apresentar as ferramentas na prática, seus resultados e suas vantagens na utilização. Foi utilizado um notebook com sistema operacional Windows

[3] Fork é uma derivação com base em um *software* ou S.O. Acontece quando um desenvolvedor inicia um projeto independente com base no código-fonte de um projeto já existente.

10 Pro e uma máquina virtual Oracle VM VirtualBox 5.0.16 com o sistema operacional Ubuntu *14.04*, a fim de satisfazer as configurações necessárias para a instalação de cada *software.*

6.3.1 Teste com LanGuard.

A ferramenta LanGuard foi instalada em um notebook com sistema operacional Windows 10 Pro. Foi utilizada a versão do GFI LanGuard 2015, disponível para realização de teste por trinta dias. O ambiente é apresentado ao usuário através de um aplicativo disponível para *download* no endereço: http://www.gfi.com/downloads.

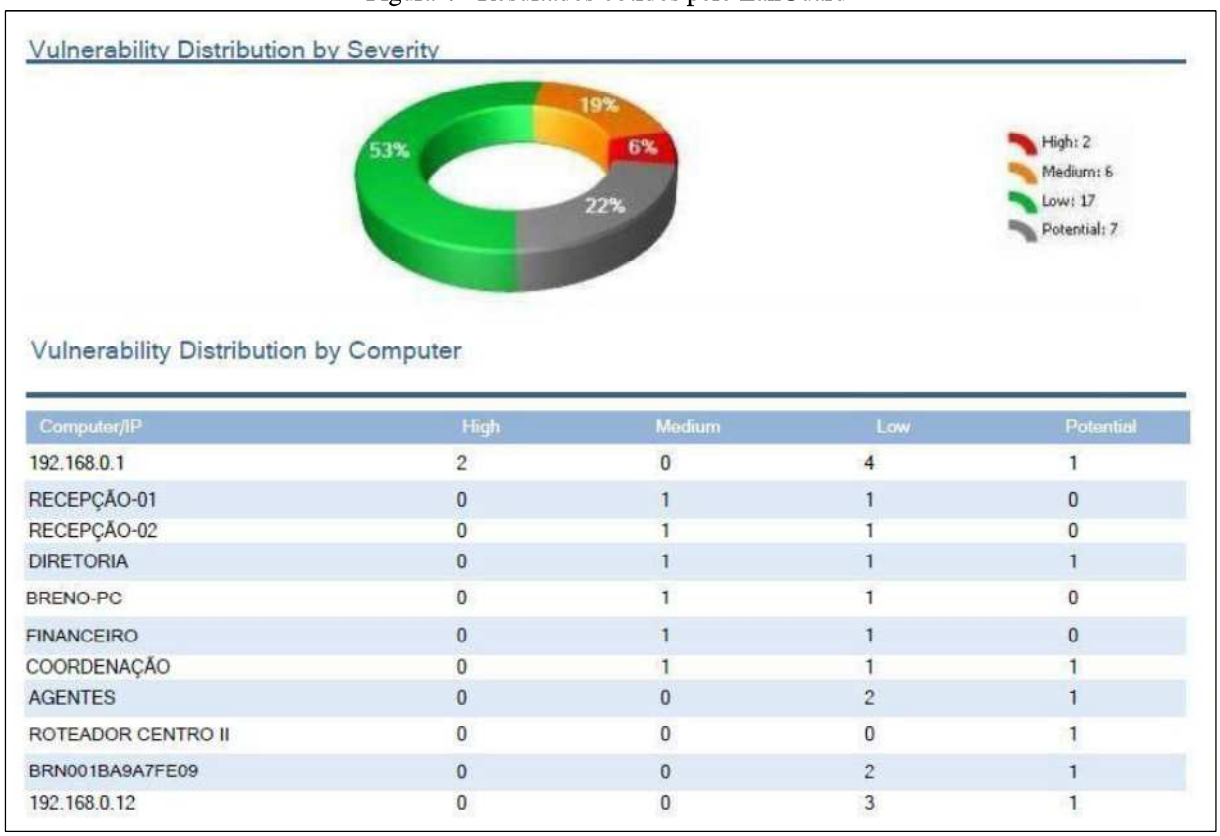
O *software* não necessita de nenhum servidor *web* para seu funcionamento. Após sua inicialização e atualização automática dos *plug-ins*, foi definido um intervalo de IP's (*Internet Protocol*) para que o *scanner* pudesse identificar as máquinas na rede. Na Figura 3 tem-se a tela inicial do *LanGuard,* onde foi realizado o escaneamento da rede.

Para dar início a varredura, digitou-se em *ScanTarget*[4], a faixa de IP da rede, e em seguida clicou-se em *Scan*. Depois de feito e escaneamento gerou-se o relatório.

O relatório do LanGuard apresentou não somente o modo texto, mas também o recurso gráfico através de percentuais e total dentro de cada percentual das vulnerabilidades identificadas. A Figura 4 mostra os dispositivos encontrados e os resultados obtidos através do escaneamento da rede com seus respectivos nomes, vulnerabilidades detectadas e grau de risco das vulnerabilidades encontradas.

[4] *ScanTarget* é uma opção no Software LanGuard onde se define uma faixa de IP válido para se fazer uma varredura na rede.

Figura 4 - Resultados obtidos pelo LanGuard



Vulnerability Distribution by Computer

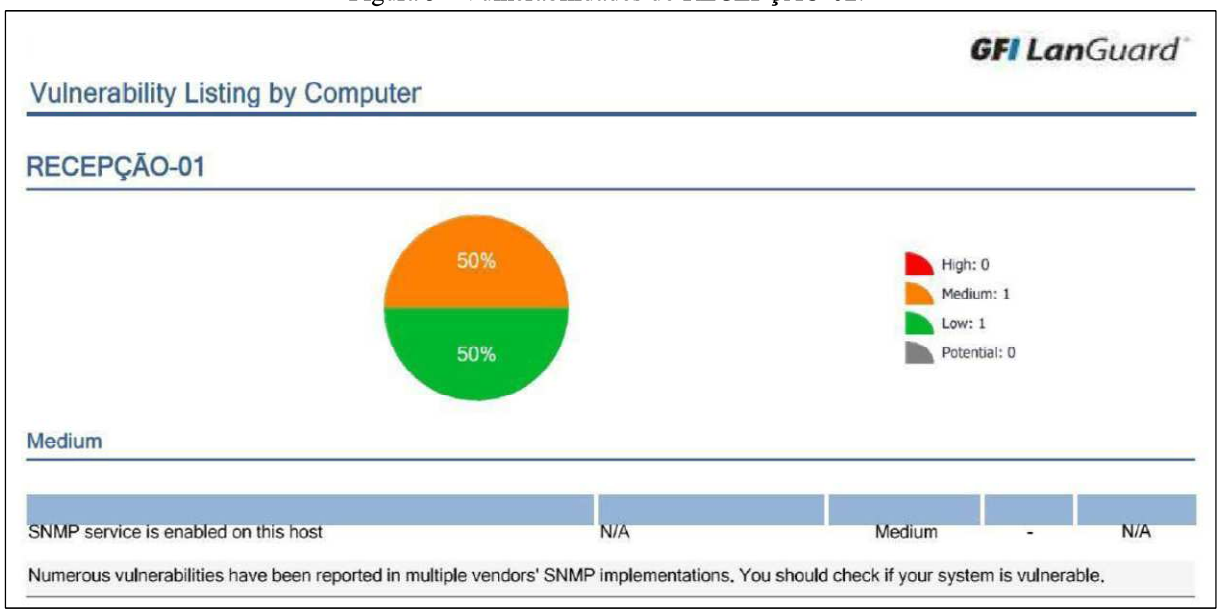
Computer/IP	High	Medium	Low	Potential
192.168.0.1	2	0	4	1
RECEPÇÃO-01	0	1	1	0
RECEPÇÃO-02	0	1	1	0
DIRETORIA	0	1	1	1
BRENO-PC	0	1	1	0
FINANCEIRO	0	1	1	0
COORDENAÇÃO	0	1	1	1
AGENTES	0	0	2	1
ROTEADOR CENTRO II	0	0	0	1
BRN001BA9A7FE09	0	0	2	1
192.168.0.12	0	0	3	1

Fonte: LanGuard2015

Foi destacado para a análise da vulnerabilidade um dispositivo de médio risco, um dispositivo com risco em potencial e baixo. Não foi avaliado o de alto risco porque é o notebook onde o *software* de varredura estava sendo executado, sendo detectadas vulnerabilidades de alto risco para a segurança do computador.

No dispositivo identificado como RECEPÇÃO-01, foi detectada uma vulnerabilidade de risco médio e uma vulnerabilidade de baixo risco, totalizando duas vulnerabilidades encontradas neste dispositivo. O relatório nos traz a informação que o serviço *Simple Network Management Protocol* (SNMP) está habilitado e ainda esclarece que várias vulnerabilidades foram relatadas em implantações SNMP de vários fornecedores. A Figura 5 ilustra o gráfico gerado pelo relatório do LanGuard.

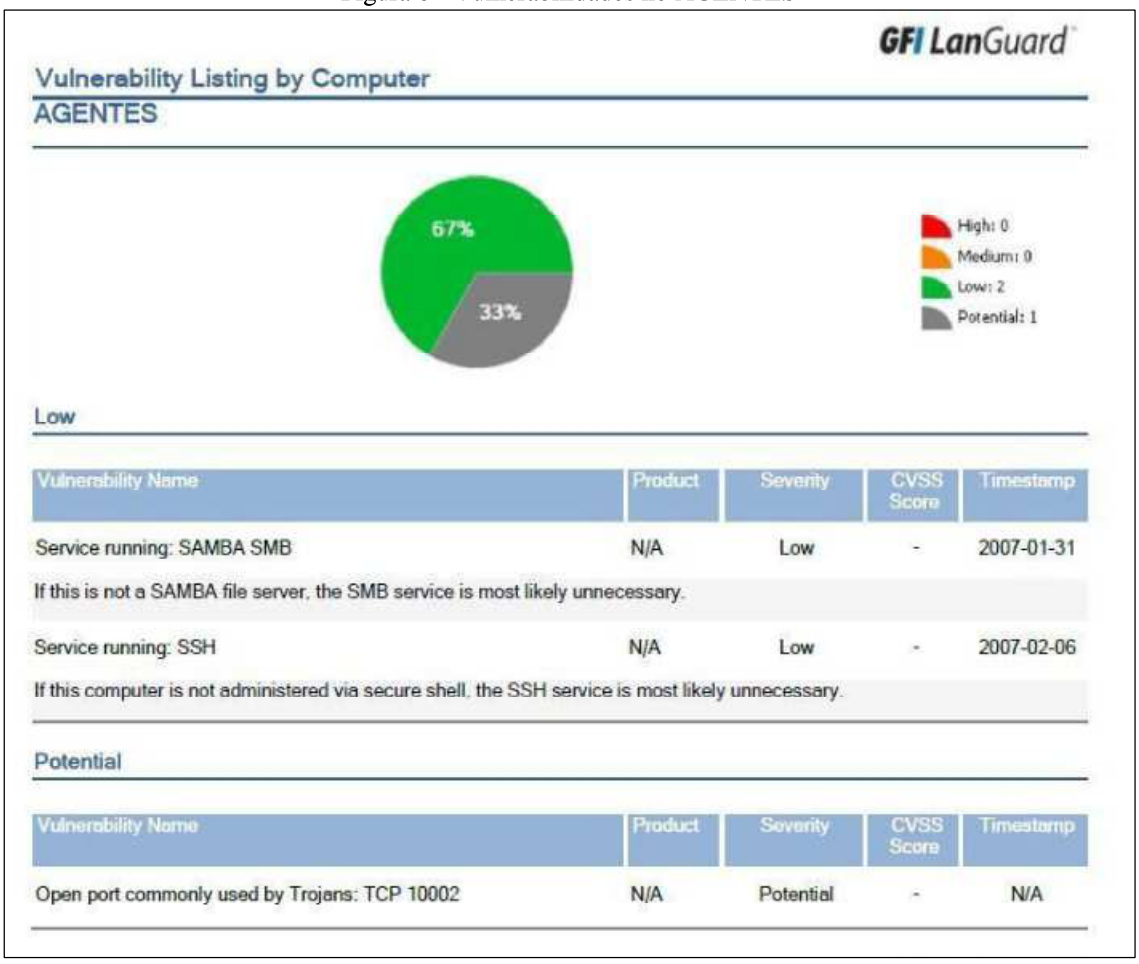
Figura 5 - Vulnerabilidades do RECEPÇÃO-02.



Fonte: LanGuard2015

No dispositivo identificado como AGENTES, foi possível observar que 67% possuem vulnerabilidades de baixo risco (*Low*) e 33% de vulnerabilidades potenciais (*Potential*). A Figura 6 apresenta o gráfico com as vulnerabilidades encontradas nesse dispositivo.

Figura 6 - Vulnerabilidades no AGENTES



Fonte: LanGuard2015

As vulnerabilidades de baixo risco estão associadas a serviços que estão rodando no dispositivo, os quais são: Serviço em execução SAMBA e SSH. Para os dois serviços detectados, o *software* informou que se o dispositivo não for servidor de arquivos SAMBA e não for administrado via shell seguro, não se faz necessário os serviços listados estarem ativos. Com o objetivo de evitar que esse dispositivo fique exposto a possíveis ataques.

6.3.2 Testes com OpenVAS

Para realização dos testes de varredura de vulnerabilidades, foi utilizado o *software* OpenVAS 5, instalado em uma máquina virtual Oracle VM VirtualBox 5.0.16 com sistema operacional Ubuntu 14.04. O programa foi instalado através de pacotes binários, ou seja, o usuário instala o sistema direto do repositório do fabricante. Após instalado, o OpenVAS é acessado através de uma interface *web*, disponível em http://localhost:9392.

Com essa ferramenta realizou-se o escaneamento da rede. O relatório gerado pelo OpenVAS informa a data de início e fim da varredura, descreve os resultados encontrados para cada *host* identificado e oferece recomendações a fim de corrigir os problemas detectados. Para obter maior desempenho da ferramenta na detecção de vulnerabilidades, sugere-se atualizar os *plugins* através do comando *openvas-nvt-sync*, inserido no terminal, que atualmente conta com mais de 35.000 NVTs. Através da varredura da rede foram detectados 12 *hosts*, como mostra a Figura 7.

Figura 7 - Resultados do OpenVAS.

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.0.1	2	12	1	41	0
192.168.0.2 RECEPCAO-01	0	6	1	25	0
192.168.0.3 RECEPCAO-02	0	2	1	11	0
192.168.0.4 DIRETORIA	0	2	1	10	0
192.168.0.5 CONT-01	0	2	1	11	0
192.168.0.6 CONT-02	0	2	1	10	0
192.168.0.7 COORDENACAO	0	2	1	11	0
192.168.0.8 AGENTES	0	2	1	10	0
192.168.0.9	0	2	1	10	0
192.168.0.10	0	2	1	11	0
192.168.0.11	0	2	1	11	0
192.168.0.12	0	4	1	22	0
Total: 12	2	40	12	183	0

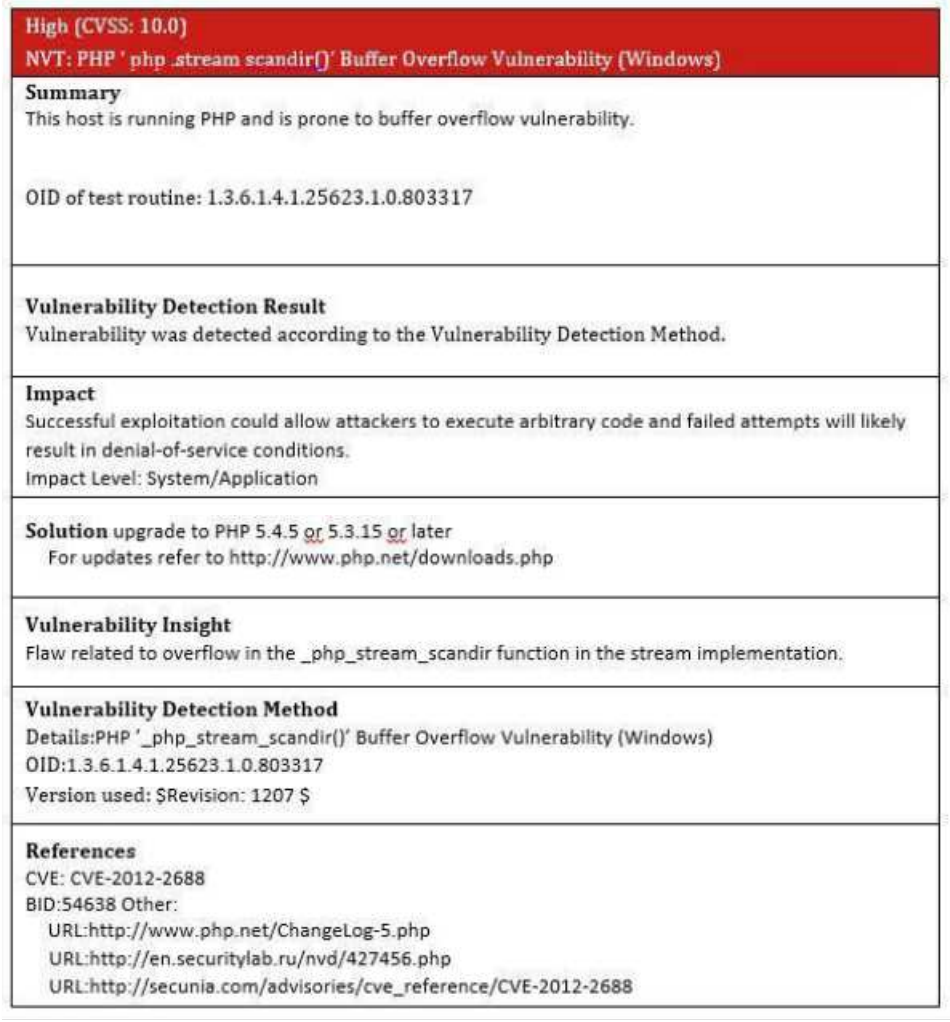
Fonte: OpenVAS 5

O relatório do OpenVAS é destacado em três níveis Alto (High), médio (Medium) e baixo (Low). Outro campo em destaque é processo de registro (*Log)*, que contém a informação que é retornada pelo *plugin*, que apresenta informações mais detalhadas sobre os eventos encontrados durante o escaneamento. Será apresentado um exemplo de cada nível de risco para demonstrar os resultados encontrados com a utilização dessa varredura.

Entre os *hosts* detectados foi escolhido o que possui IP 192.168.0.1 que apresentou o maior número de vulnerabilidade de risco *High*. As vulnerabilidades encontradas pelo OpenVAS neste *host*, foram na versão PHP, que sofre vulnerabilidade de estouro de inteiros e erros de estouro de *buffer* e no serviço Firebird.

A Figura 8 apresenta o detalhamento de uma vulnerabilidade de alto risco encontrada neste host.

Figura 8 - Alto risco



High (CVSS: 10.0)
NVT: PHP ' php_stream scandir()' Buffer Overflow Vulnerability (Windows)

Summary
This host is running PHP and is prone to buffer overflow vulnerability.

OID of test routine: 1.3.6.1.4.1.25623.1.0.803317

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation could allow attackers to execute arbitrary code and failed attempts will likely result in denial-of-service conditions.
Impact Level: System/Application

Solution upgrade to PHP 5.4.5 or 5.3.15 or later
For updates refer to http://www.php.net/downloads.php

Vulnerability Insight
Flaw related to overflow in the _php_stream_scandir function in the stream implementation.

Vulnerability Detection Method
Details:PHP '_php_stream_scandir()' Buffer Overflow Vulnerability (Windows)
OID:1.3.6.1.4.1.25623.1.0.803317
Version used: $Revision: 1207 $

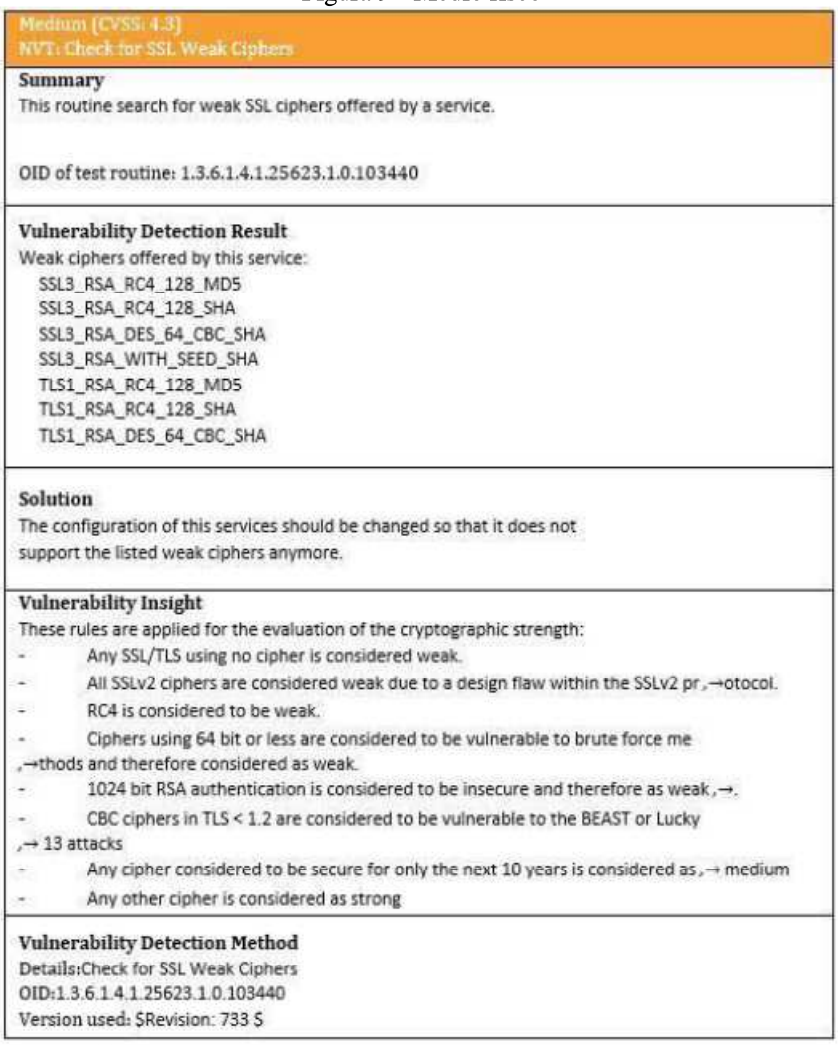
References
CVE: CVE-2012-2688
BID:54638 Other:
URL:http://www.php.net/ChangeLog-5.php
URL:http://en.securitylab.ru/nvd/427456.php
URL:http://secunia.com/advisories/cve_reference/CVE-2012-2688

Fonte: OpenVAS 5

Este servidor que está executando o PHP foi o que apresentou maior propensão a exploração de vulnerabilidades de alto risco, através dos testes o OpenVAS detectou que este *host* está propenso a vulnerabilidade de um possível um estouro de Buffer.

A vulnerabilidade apresentada na Figura 9 retrata a situação de uma falha de risco *Medium* no *host* com IP 192.168.0.2.

Figura 9 - Médio risco



Medium (CVSS: 4.3)
NVT: Check for SSL Weak Ciphers

Summary
This routine search for weak SSL ciphers offered by a service.

OID of test routine: 1.3.6.1.4.1.25623.1.0.103440

Vulnerability Detection Result
Weak ciphers offered by this service:
SSL3_RSA_RC4_128_MD5
SSL3_RSA_RC4_128_SHA
SSL3_RSA_DES_64_CBC_SHA
SSL3_RSA_WITH_SEED_SHA
TLS1_RSA_RC4_128_MD5
TLS1_RSA_RC4_128_SHA
TLS1_RSA_DES_64_CBC_SHA

Solution
The configuration of this services should be changed so that it does not support the listed weak ciphers anymore.

Vulnerability Insight
These rules are applied for the evaluation of the cryptographic strength:
- Any SSL/TLS using no cipher is considered weak.
- All SSLv2 ciphers are considered weak due to a design flaw within the SSLv2 pr,→otocol.
- RC4 is considered to be weak.
- Ciphers using 64 bit or less are considered to be vulnerable to brute force me ,→thods and therefore considered as weak.
- 1024 bit RSA authentication is considered to be insecure and therefore as weak,→.
- CBC ciphers in TLS < 1.2 are considered to be vulnerable to the BEAST or Lucky ,→ 13 attacks
- Any cipher considered to be secure for only the next 10 years is considered as,→ medium
- Any other cipher is considered as strong

Vulnerability Detection Method
Details:Check for SSL Weak Ciphers
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: $Revision: 733 $

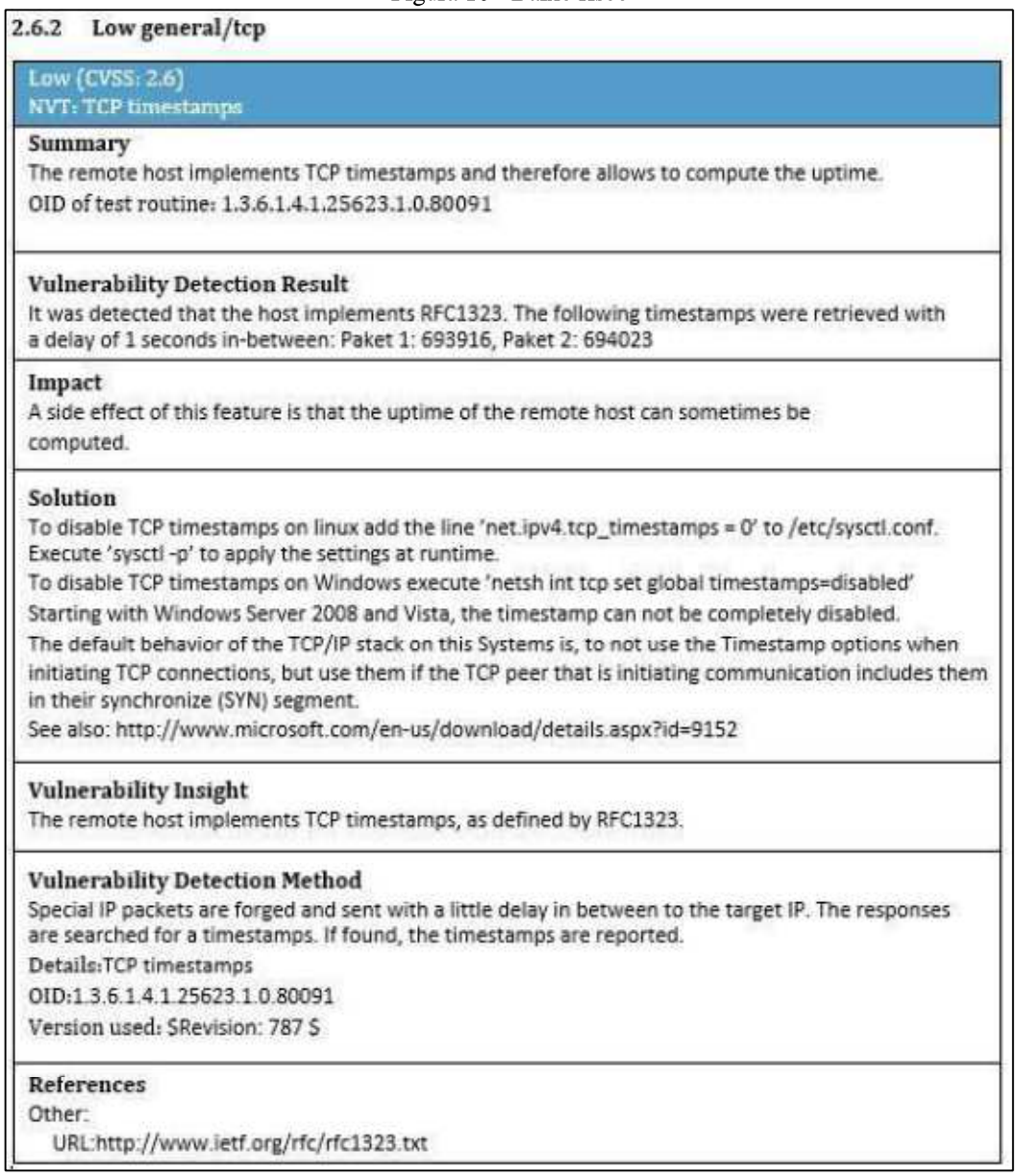
Fonte: OpenVAS 5

No relatório mostra uma vulnerabilidade de risco através dos testes de vulnerabilidade de rede (NVTs). As regras aplicadas pelos NVTs apresentaram uma série de informações sobre aplicação de codificação fracas na utilização do SSL.

Como solução para as vulnerabilidades citadas pelo OpenVAS, alterar a configuração desses serviços, a fim de garantir que não utilize as cifras fracas listadas, seria uma forma de proteger a rede de possíveis ataques. O OpenVAS ainda fornece as cifras utilizadas por esses serviços e classificadas como fracas que são descritas na Figura 9 na seção de detecção de vulnerabilidades.

Para vulnerabilidades de baixo risco o *host* com IP 192.168.0.2 está com TCP timestamps e, portanto, permite calcular o tempo de atividade, como pode ser visto na Figura 10.

Figura 10 - Baixo risco



2.6.2 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.
OID of test routine: 1.3.6.1.4.1.25623.1.0.80091

Vulnerability Detection Result
It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 693916, Paket 2: 694023

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.
To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'
Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.
The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details:TCP timestamps
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: $Revision: 787 $

References
Other:
URL:http://www.ietf.org/rfc/rfc1323.txt

Fonte: OpenVAS 5

O OpenVAS informa que neste host está ativado o TCP timestamps, e um impacto que pode causar o timestamps ativado é que o tempo de atividade do host remoto pode ser calculado.

Esta vulnerabilidade em certas implementações TCP pode ser explorada para causar uma negação de serviço, forçando ambos terminais envolvidos em uma conexão TCP para soltar os segmentos TCP. Que acabará por repor a conexão. O problema surge devido à forma como algumas pilhas TCP implementam a opção TCP timestamp.

6.3.3 Comparativo entre LanGuard e OpenVAS

Tabela 1 - Comparação entre os Softwares

Risco/Software	LanGuard	OpenVAS
Alto (High)	2	2
Médio (Medium)	6	40
Baixo (Low)	17	12

Fonte: Autor

Nota-se uma diferença acentuada entre o total de riscos classificados como baixo e alto entre o LanGuard e o OpenVAS, O contrário acontece para os riscos categorizados como médio, onde o OpenVAS encontra um número superior de vulnerabilidades.

6.3.4 Conclusão

Os relatórios apresentados pelas ferramentas de escaneamento evidenciaram diversas vulnerabilidades, em diversos níveis de risco. Dessa forma é possível analisar as possíveis soluções sugeridas pelos *softwares* e aplicá-las para correção das falhas de modo que seja possível sanar todas as vulnerabilidades encontradas ou evitar futuros problemas. Entretanto, alguns itens apontados como falhas ou vulnerabilidades são na verdade configurações necessárias para que serviços funcionem de maneira correta.

6.3.5 Uma proposta de melhoria de segurança para redes de computadores.

Segundo Zotto (2012) a primeira coisa para ter em mente é o conceito de que qualquer investimento em segurança é melhor do que nenhum investimento. Pois, de nada adianta investir em ferramentas, por mais simples e de baixo custo que sejam, se as mesmas não forem eficazes, e acima de tudo se não forem gerenciadas.

Para a proposta de segurança optou-se pelo software BrazilFW – Firewall and Router (BFW). Pois preenche os principais requisitos necessários para uma boa rede de pequeno e médio porte: requisitos como: DHCP, DNS, QOS, VPN, filtro de pacote, filtro de conteúdo, roteamento, entre outros.

O BFW está disponibilizado gratuitamente, possui interface amigável que facilita sua implementação, podendo ser instalados em computadores com poucos recursos de hardware, e integrado por diversas ferramentas para administração e monitoramento de redes, tornando-se assim uma ferramenta muito poderosa. Todos os conceitos e como funciona a fundo a ferramenta estão no Apêndice A.

Para entender a escolha desta ferramenta como servidor Firewall/ Proxy e Roteador de rede será apresentado uma análise dos pontos fortes e fracos do BFW. Segundo Zotto (2012) os principais pontos são demonstrados na Tabela 2.

Tabela 2 - Pontos Principais

PONTOS FORTES	PONTOS FRACOS
• Fácil Instalação e Configuração básica; • Contempla as funções de Firewall, Proxy e Roteador na mesma ferramenta; • Baixo custo de Hardware; • Software Livre (Open source); • Software Estável; • Atualizações constantes e comunidade participativa; • Fácil gerenciamento; • Muitos Addons que permitem embutir diversas funcionalidades; • Possui um limite imenso de usuários;	• Alguns Updates podem matar alguns addons; • Para uma maior eficácia e personalização requer um pouco de conhecimento em Linux; • Não possui Suporte, visto que se trata de um projeto livre; • Não trabalha com integração em Cluster; • À medida que novas funcionalidades são acrescentadas, exige maior capacidade de Hardware; • Regras mais complexas exigem um conhecimento mais profundo;

Fonte: Zotto (2012)

7 CONSIDERAÇÕES FINAIS

Tendo-se em vista o exposto neste artigo, pode-se concluir que a segurança da informação é de fundamental importância para a sobrevivência das organizações nos dias atuais. Considerando que as tecnologias de segurança em redes de computação estão em constante crescimento, já existem milhares de ferramentas que podem ser utilizadas para combater problemas de segurança, porém muitas empresas de pequeno e médio porte possuem pouca ou nenhuma tecnologia de proteção à rede.

Um segundo fator que prejudica as redes de computadores de pequeno e médio porte no quesito segurança da informação, é a falta de políticas de segurança da informação eficazes e tangíveis, ou a falta de quem elabore e gerencie estas políticas de segurança.

É possível observar que é possível identificar vulnerabilidades em um sistema e pode ser solucionado as ameaças e descobertas porém ao mesmo tempo que se soluciona outras vulnerabilidades são exploradas e novas técnicas de ataques são criadas, por isso não se pode afirmar que uma rede é totalmente segura. Existem várias ferramentas para prevenir e auxiliar na tarefa de identificar problemas de segurança nas redes.

Diante desse cenário a análise de vulnerabilidades, torna-se uma necessidade quando se trata de segurança de redes. Através da frequente análise e avaliação da segurança da rede, um profissional de segurança é capaz de avaliar o nível de segurança da sua rede e adotar medidas de segurança adequadas em tempo hábil. Os scanners detectores de vulnerabilidades são uma das ferramentas utilizadas que podem ser incorporadas na rotina dos administradores de redes.

Os *softwares*, como o LanGuard e o OpenVAS, utilizados nesse trabalho, auxiliam na descoberta de vulnerabilidades nas redes, bem como sistemas operacionais em execução, portas abertas, serviços ativos e a necessidade de atualização de *patches*. Através dos testes realizados com estas ferramentas foi possível listar as vulnerabilidades, é possível entender a importância da utilização de ferramentas que realizam a varredura de rede auxiliando dessa forma o administrador na manutenção da segurança.

Foi proposta também a implantação do BrazilFW, uma ferramenta que contempla paralelamente um servidor Firewall, um Proxy e um roteador de fácil instalação, configuração e de fácil gerenciamento. Esta ferramenta foi selecionada dentre outras opções no mercado, pelo bom nível de proteção que oferece, pela baixa complexidade de gerenciamento e pelo baixo custo de implantação. Foram apresentadas suas principais características.

VULNERABILITY ANALYSIS WITH OPENVAS AND LANGUARD AND MOTION FOR SECURITY FOR SMALL COMPUTER NETWORKS AND MID-SIZED

ABSTRACT

This paper presents an approach to information security in computer networks emphasizing the Vulnerability, proposing the use of a firewall to manage small and medium-sized networks. Therefore we carried out a case study to verify the security of a computer network of a company using system vulnerability scanning tools are presented two tools very currently used by network administrators, a landlady who is LanGuard and other free which is the OpenVAS. Because of the wide range of vulnerabilities in applications and systems that jeopardize the security of information, the use of these tools is very important for a preventive monitoring of the environment. It was concluded that the use of these tools have reached the proposed objective for the return obtained by the software exposed information that could leave systems vulnerable. Finally we present a proposal to use an effective firewall server and low cost to management of small and medium networks the BrazilFW

Keywords: Computer Networks. Safety. OpenVAS. LanGuard. BrazilFW.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 17799. **Tecnologia da informação, técnicas de segurança, código de prática para a gestão da segurança da informação**. Rio de Janeiro: ABNT, 2005.

BRASIL ESCOLA, **Internet.** Disponível em: <http://brasilescola.uol.com.br/informatica/internet.htm> Acesso em 02 Set 2016.

BUZZATE, P. M. **Análise de vulnerabilidades através de *Scanners* detectores**. 2014. Disponível em <http://www.redes.ufsm.br/docs/tccs/TCC_2014_I/TCC_Patricia_Buzzatte.pdf> Acesso em 17 Dez 2015

CERT.BR. Disponível em: <http://www.cert.br/stats/>. Acesso em: 17 Nov. 2015.

FERREIRA, Fernando N. F. ARAÚJO, Márcio T. **Políticas de segurança da informação - Guia prático para elaboração e implementação**. Rio de Janeiro: Ciência Moderna, 2008.
GFI NETWORK SECURITY. Disponível em: < http://www.gfi.com/languard/>. Acesso em: 15 Dez. 2015.

GIL, A. C**. Como elaborar projetos de pesquisa.** 5. ed. São Paulo: Atlas, 2009.

GOMES, Tito L. O. **Política de segurança computacional**. 2004. Disponível em: <http://www.projetoderedes.com.br>. Acesso em: 5 jul. 2014.

KUROSE, James; ROSS, Keith. **Rede de computadores e a internet. Uma abordagem top-down**. 5ª ed. São Paulo: Pearson 2010.

MCCLURE, S.; SCAMBRAY, J.; KURTZ, G. **Hackers Expostos: Segredo e Solução para a Segurança de Redes**. 7 ed. Porto Alegre: Bookman Companhia Editora Ltda, 2012.

MARTINELO, C. G.; BELLEZI, M. A. **Análise de Vulnerabilidades com OpenVAS e Nessus**, Revista T.I.S vol. 3, São Carlos, 2014.

MIRANDA. Anibal D. A. **Introdução às redes de computadores.** 2008 Disponível em: <https://fasul.edu.br/portal/files/biblioteca_virtual/7/introduceoaredesdecomputadores.pdf.> Acesso em: 7 set. 2016

MOREIRA et al. **Scanners de Vulnerabilidades Aplicados a Ambientes Organizacionais**. Revista Eletrônica da Faculdade Metodista Granbery: Jul/Dez, 2008.

NAKAMURA, E. T.; GEUS, P. L de. **Segurança de redes em ambientes cooperativos**. São Paulo: Novatec Editora, 2007.

OPENVAS - **OpenVAS** ***Open Vulnerability Assessment System***. Disponível em: <http://www.openvas.org/>. Acesso em: 17 Dez. 2015.

PINHEIRO, José M. S. **Gerenciamento de Redes de Computadores: Uma breve introdução**. Disponível em:

<http://www.projetoderedes.com.br/artigos/artigo_gerenciamento_de_redes_de_computadores.php>. Acesso em: 7 ago. 2015.

RODRIGUES, P.E.B. **Segurança Informática de Redes e Sistemas (Abordagem Open-Source)**. Dissertação para obtenção de grau de Mestre – Universidade de Trásos- Monte e Alto Douro, 2010.

SANTOS, M. C. D.; SILVA, J. R. **Avaliação de Diferentes Ferramentas para Realização de Testes de Segurança em Computadores e em Redes Locais (Lan's)**. Mestrado em Ciência da Computação- Universidade do Porto (FEUP), 2012.

SCHWARZER, S. **OpenVAS 4 Análise detalhada. Linux Magazine**, São Paulo, Out. 2011.

STALLINGS, W. **Criptografia e segurança de redes. Princípios e práticas**. 4ª ed. São Paulo: Pearson 2008.

TANENBAUM, Andrew S. **Redes de Computadores**. Rio de Janeiro: Campus, 2003.

WEBER, Carlos E. **Apostila de Redes de Computadores**. Disponível em: <http://pt.scribd.com/doc/100231744/Apostila-de-Redes>. Acesso em: 23 jun. 2014.

ZOTTO, Fernando D. **Segurança da informação: uma proposta para segurança de redes em pequenas e médias empresas**. 2012. Disponível em: <http://www.projetoderedes.com.br>. Acesso em: 5 jul. 2014.

APÊNDICE A

1 PROPOSTA DE SEGURANÇA PARA REDES DE COMPUTADORES

A tecnologia da informação faz-se presente e necessárias em todos os ambientes, tanto em uma escola ou universidade quanto em uma empresa pequena ou de grande porte. Muitos se adequaram e investem pesado para usá-la de forma correta, outras impulsionadas pela necessidade não se precaveram para os perigos oferecidos por ela. A partir destes pontos foi realizada uma pesquisa a procura de software de gerenciamento de segurança de rede, com o objetivo de fazer escolha mais consciente de que ferramenta utilizar para implantar e gerenciar o ambiente de rede com qualidade e maior eficiência.

Segundo Zotto (2012) a primeira coisa para ter em mente é o conceito de que qualquer investimento em segurança é melhor do que nenhum investimento. Pois, de nada adianta investir em ferramentas, por mais simples e de baixo custo que sejam, se as mesmas não forem eficazes, e acima de tudo se não forem gerenciadas.

Dentre os softwares livre, foi executada uma pesquisa por um que preenchesse todos os requisitos necessários para uma boa rede de pequeno e médio porte: requisitos como: DHCP, DNS, QOS, VPN, filtro de pacote, filtro de conteúdo, roteamento, entre outros, optando pelo software BrazilFW – Firewall and Router (BFW).

O BFW está disponibilizado gratuitamente, possui interface amigável que facilita sua implementação, podendo ser instalados em computadores com poucos recursos de hardware, e integrado por diversas ferramentas para administração e monitoramento de redes, tornando-se assim uma ferramenta muito poderosa.

1.1 Brazil firewall e router (BFW)

Segundo BRAZILFW (2014) o BFW é uma mini distribuição Linux, composta pelas funções de Roteador e Firewall, bem como em sua última versão também a função de Proxy integrado. Tem como objetivo transformar máquinas com pouco recurso de hardware em um servidor de alta performance.

O BFW é o sucessor do Coyote Linux[5], que foi projetado por Joshua Jackson o qual foi descontinuada em 2005, onde os brasileiros Claudio e Marcelo - Brasil, deram continuidade no projeto mudando seu nome para o atual BrazilFW.

Atualmente, o BFW está na versão 3.x, que foi inteiramente codificada e recomeçada do zero por Washington Rodrigues.

O BFW torna possível instalar serviços de rede rapidamente como compartilhamento de internet, firewalls, ou pontos de acesso sem fio. Agrega muitas funções extras, mas tenta manter a simplicidade na administração e nos requisitos de hardware.

Para entender a escolha desta ferramenta como servidor Firewall/ Proxy e Roteador de rede será apresentado uma análise dos pontos fortes e fracos do BFW. Segundo Zotto (2012) os principais pontos são demonstrados na Tabela .

Tabela 1 - Pontos Principais

PONTOS FORTES	PONTOS FRACOS
• Fácil Instalação e Configuração básica; • Contempla as funções de Firewall, Proxy e Roteador na mesma ferramenta; • Baixo custo de Hardware; • Software Livre (Open source); • Software Estável; • Atualizações constantes e comunidade participativa; • Fácil gerenciamento; • Muitos Addons que permitem embutir diversas funcionalidades; • Possui um limite imenso de usuários;	• Alguns Updates podem matar alguns addons; • Para uma maior eficácia e personalização requer um pouco de conhecimento em Linux; • Não possui Suporte, visto que se trata de um projeto livre; • Não trabalha com integração em Cluster; • À medida que novas funcionalidades são acrescentadas, exige maior capacidade de Hardware; • Regras mais complexas exigem um conhecimento mais profundo;

Autor: Zotto (2012)

O seu código fonte está disponível sob a licença GNU GPL para que qualquer pessoa possa utilizar, estudar, modificar e distribuir livremente de acordo com os termos da licença. O BFW possui suporte através de fórum do projeto acessado pelo endereço

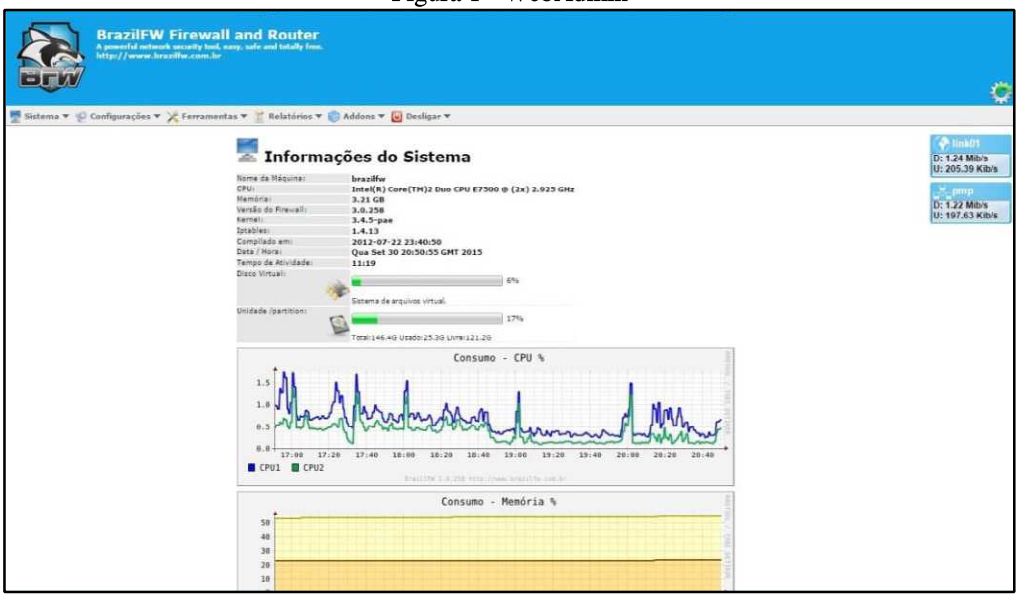
[5] Coyote Linux é uma pequena distribuição Linux desenvolvido pela Vortech Consulting contendo apenas os serviços necessários para transformar um computador em um roteador ou firewall.

http://www.brazilfw.com.br. Para adquirir o sistema, basta acessar o site do BFW para fazer o download de suas versões.

Além do mais de modo simplificado a configuração do BFW pode ser feita via browser com interface amigável que facilita a implementação e a configuração do sistema, ou se preferir pode ser feita via terminal.

Seu acesso é dado através do navegador com a interface do painel WebAdmin[6] com endereço padrão https://192.168.0.1.8181, possui login e senha pré-definidas como: login root e senha root, sua autenticação é feita por meio de chave SSL, que garante a autenticação segura de acordo com as normas de segurança.

Figura 1 - WebAdmin



Fonte: Autor

1.1.1 Segurança

É possível com o BFW criar regras de acordo com a política de segurança da instituição. Pode-se bloquear a execução de programas não permitidos nas estações, que possam interferir na produtividade da mesma, como: redes sociais, jogos, e outros aplicativos em desacordo com a política de segurança da instituição.

Umas das formas encontradas para restringir o acesso a uma determinada rede é mediante o cadastramento dos dispositivos da rede. Como o endereço MAC (Media Access Control) identifica de forma única cada interface de rede, apenas os dispositivos cadastrados

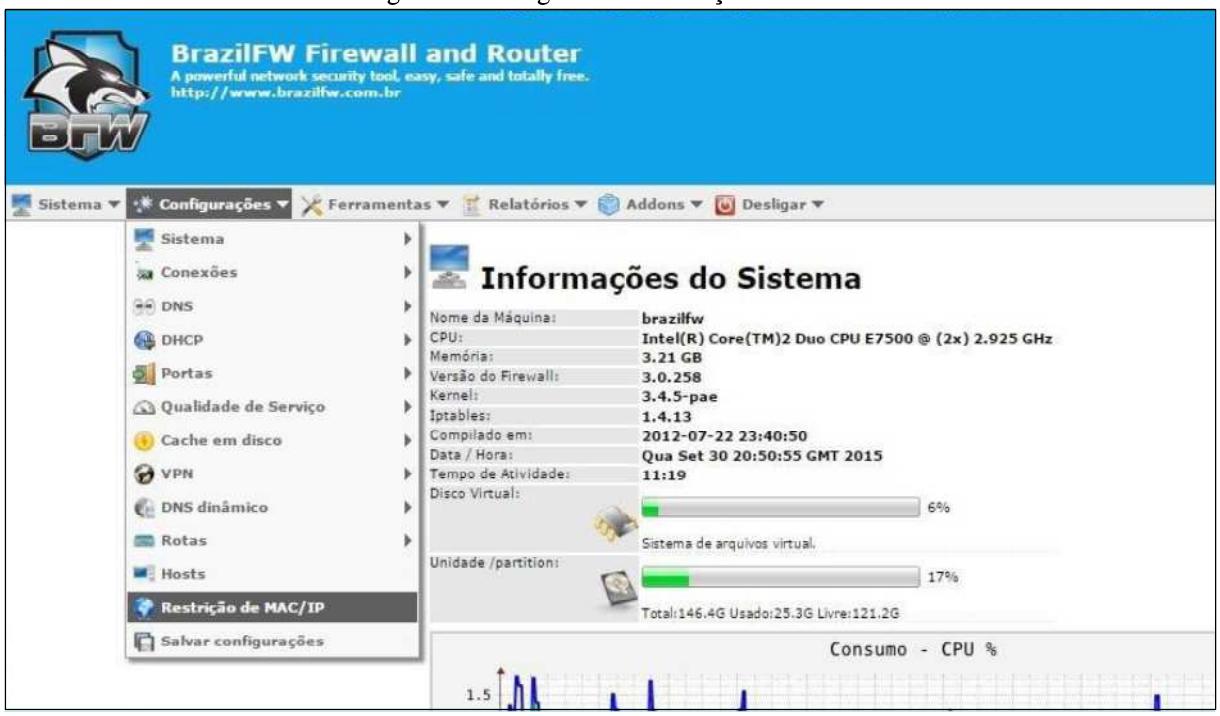
[6] O WebAdmin é uma ferramenta de gerenciamento com interface gráfica para servidores Linux.

previamente terão acesso permitido. É uma boa solução para redes e ambientes com poucas mudanças, esse tipo de autenticação permite a identificação do equipamento na rede.

O BFW usa a restrição de MAC/IP, que além de fazer a reservar de IP, também proíbe a intrusão de host[7] que não estão cadastrados na rede.

No BFW a restrição é o de Lista Branca, ou seja, só navega quem estiver na lista. Se a Restrição MAC/IP estiver ativa e o MAC não estiver cadastrado o host não conseguirá navegar. Na Figura 2 mostra a tela onde são adicionadas as restrições MAC/IP

Figura 2 - Configurando a Restrição MAC/IP



Fonte: Autor

1.1.2 Firewall

No BFW o firewall é uma das suas funções principais, aplicando as políticas de segurança de acordo com a necessidade da instituição.

Um firewall evita que perigos vindos da internet se espalhem na rede interna, colocando entre a rede interna e a rede externa o firewall, controla todo o trafego que passa por ela tendo a certeza que é aceitável de acordo a política de segurança da instituição oferecendo uma excelente proteção contra ameaças vindas da rede externa.

As políticas de segurança podem ser aplicadas de diversas maneiras utilizando um firewall, exemplos: bloqueando sites indevidos filtrando pacotes vindos da internet,

[7] host ou *hospedeiro*, é qualquer máquina ou computador conectado a uma rede.

determinando quem deve e quem não deve utilizar a internet. O BFW tem como ferramenta principal para Firewall o dansguardian, que será mais detalhado nos tópicos a seguir.

Alguns dos benefícios que o Firewall do BFW oferece:

- ✓ Evitar os ataques de outros servidores à rede privada;
- ✓ Permite ao administrador da rede definir um funil, mantendo a margem os usuários não-autorizados;
- ✓ Permite monitorar a segurança, quando aparece alguma atividade suspeita, este gerará um aviso;
- ✓ Concentra segurança, centraliza os acessos;
- ✓ Gera alarmes de segurança, traduz direção NAT;
- ✓ Monitora e registra uso de serviços de WWW e FPT;
- ✓ Controla o uso da internet. Permite bloquear o material não adequado.

1.1.3 Router (roteador)

Segundo Forouzan (2008, p. 74) "roteador é um dispositivo de três camadas; ele opera nas camadas físicas, de enlace de dados e de redes." Na camada física ele regenera o sinal recebido. Como enlace de dados verifica os endereços de destino e origem dos pacotes e como dispositivos da camada de rede, o roteador verifica os endereços da camada de redes, ou seja, número do IP. "Um roteador é um dispositivo de interligação em rede: ele interliga redes independentes para formar uma rede de redes." (FOROUZAN, 2008, p.74).

O roteador do BFW faz com que duas ou mais redes se comuniquem de forma indireta, não transparente. O roteador só encaminha informação nos protocolos que ele conhece, No ADSL, o roteador fica com o endereço de IP "real" e realiza NAT (network address translation), permitindo que os computadores dentro da rede local tenham endereços de IP privados (não validos na internet). Ou seja, permite que, com somente um endereço de IP válido, vários computadores, numa rede local, possam ter acesso à internet.

Algumas das vantagens que o roteador do BFW oferece:

- ✓ Compartilha a conexão com uma rede de computadores.
- ✓ Se necessário ele pode distribuir, dinamicamente, endereços IP (DHCP) para os computadores, não sendo necessário, na maioria dos casos, configurar nada nos computadores da rede, pois, por padrão, eles se conectam automaticamente à internet.
- ✓ Maior segurança, pois conta com firewall interno e os computadores conectados recebem um endereço de IP local, não ficando diretamente expostos na internet.

- ✓ Não é necessária a instalação ou configuração de discadores, o BFW faz a autenticação automaticamente.
- ✓ Possibilidades de diferentes configurações e controle de tráfego, conforme o desejado.

A principal característica é selecionar a rota mais apropriada para repassar os pacotes recebidos. Ou seja, encaminhar os pacotes para o melhor caminho disponível para um determinado destino, são particionados em duas categorias: roteamento *estático* e *dinâmico*.

No roteamento estático as rotas são definidas manualmente e não mudam. Já nos roteamentos dinâmicos as rotas são feitas aleatoriamente pelo BFW onde são atualizadas dinamicamente reconhecendo sempre o melhor caminho ou caminho disponível a serem trafegados os dados.

1.1.3.1 Funcionamento

Os roteadores iniciam e fazem a manutenção de tabelas de rotas executando processos e protocolos de atualização de rotas, especificando os endereços e domínios de roteamento, atribuindo e controlando métricas de roteamento. O administrador pode fazer a configuração estática das rotas para a propagação dos pacotes ou através de processos dinâmicos executando nas redes.

Os roteadores passam adiante os pacotes baseando-se nas informações contidas na tabela de roteamento. O problema da configuração das rotas estáticas é que, toda vez que houver alteração na rede que possa vir a afetar essa rota, o administrador deve refazer a configuração manualmente. Já os conhecimentos de rotas dinâmicas são diferentes. Depois que o administrador fizer a configuração através de comandos para iniciar o roteamento dinâmico, o conhecimento das rotas será automaticamente atualizado sempre que novas informações forem recebidas através da rede. Essa atualização é feita através da troca de conhecimento entre os roteadores da rede.

As redundâncias são de extrema importância quando o assunto é alta disponibilidade, no BFW pode-se trabalhar com redundâncias de Links de Internet, a fim de garantir alta disponibilidade de conexão com a internet.

O BFW usa o smart route (Rota inteligente) quando se tem mais de um link de internet no mesmo servidor, onde é possível realizar o load balance (balanceamento de carga). Outra grande vantagem do balanceamento de carga do BFW é a alta disponibilidade conseguida através do reajuste de rota, caso algum dos links de conexão caia. O mesmo fará automaticamente o redirecionamento de todo o trafego da rede pelo link que estiver com status UP, e desconsiderará temporariamente o Link que estiver com status Down.

O link é verificado a cada 10 segundos, havendo alteração o squid e as rotas são recarregados. Quando um link cai (down), o smart route redireciona as conexões para um novo link, tanto o download como o upload individualmente (BRAZILFW 2014).

Para visualizar as rotas é na opção webamin => Confiragurações => Rotas => Visualizar. Como mostra a Figura 3 e Figura 4

Figura 3 - Visualizar rotas

Fonte: Autor

Figura 4 - visualização das rotas que foram definidas

Fonte: Autor

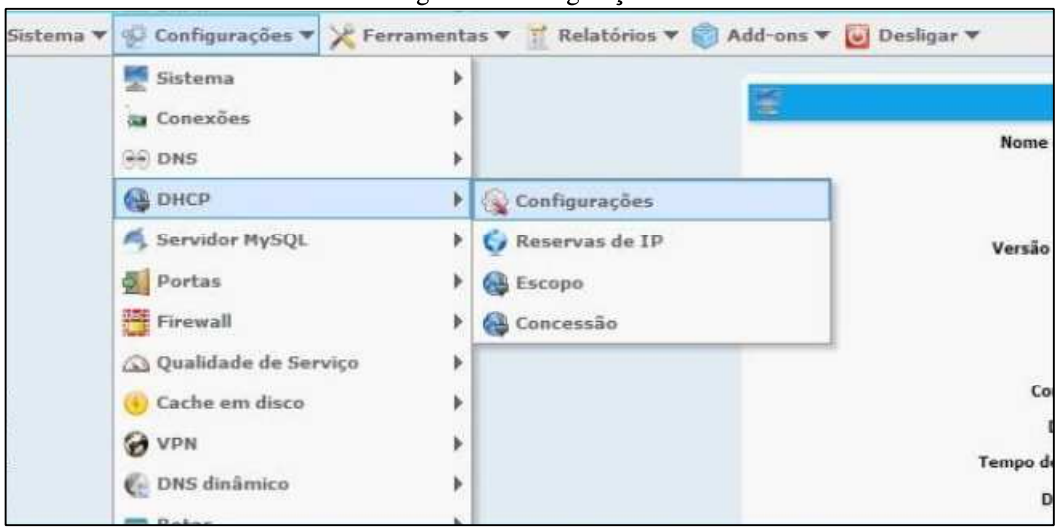
1.1.4 DHCP

O DHCP é um protocolo de serviço TCP/IP que oferece configuração dinâmica de terminais, com concessão de endereços IP de host e outros parâmetros de configuração para clientes de rede. Estes protocolos e o sucessor do BOOTP que, embora mais simples, tornou-se limitados para as exigências atuais.

Segundo BRAZILFW (2015) o DHCP opera da seguinte forma: Um cliente envia um pacote UDP em broadcast (destinados a todas as maquinas) com um pedido DHCP, os servidores DHCP que capturam esse pacote irão responder (se o cliente se enquadra em uma seria de critérios) com um pacote com configurações onde constara pelo menos um endereço IP, uma máscara de rede e outros dados opcionais, como gateway, servidores DNS e etc.

O DHCP usa um modelo cliente-servidor, no qual o servidor DHCP mantém o gerenciamento centralizado dos endereços IP usados na rede. No BFW para configurar o DHCP é na opção WebAdmin => Configurações => DHCP => Configurações. Por padrão ele vem Habilitado. Conforme ilustra as Figura 5 e Figura 6.

Figura 5 - Configurações.



Fonte: Autor

Figura 6 - Configurando o servidor DHCP

Fonte: Autor

1.1.5 Servidor proxy

O proxy é uma ferramenta que suporta os protocolos HTTP, FTP e outros. Ele reduz a utilização da conexão e melhora os tempos de respostas fazendo cache das páginas requisitadas frequentemente de uma rede de computadores, Segundo Ricci e Mendonça (2006, p. 1) "proxy refere-se a um software que atua como gateway de aplicação entre cliente e o serviço a ser acessado, interpretando as requisições e repassando-as ao servidor de destino". No BFW o proxy nativo é o squid.

O squid foi originalmente desenvolvido para rodar em sistemas operacionais tipo Unix mais ele também funciona em sistemas Windows desde sua versão 2.6. No cache são armazenados os objetos da internet (páginas web). Os navegadores então usam o squid local como um servidor proxy HTTP, reduzindo o tempo de acesso aos objetos que já estão armazenados no cache do servidor reduzindo a conexão. Para melhorar a velocidade da navegação da rede.

Para solucionar o controle de acesso à internet é imprescindível o uso do proxy. No BFW usa-se o squid que fica encarregado de filtrar os tráfegos http e ftp da rede, sendo personalizado bloqueios e acessos a sites autorizados.

O squid está continuamente melhorando sua performance, além de adicionar novos recursos e ter uma excelente estabilidade em condições extremas. Sua compatibilidade com

várias plataformas a imensa gama de software para analisar logs, gerar relatórios melhorar o desempenho e adicionar segurança provido pela comunidade open source.

Além da capacidade de intermediar o acesso à internet, como já mencionado, o squid tem outros recursos que o torna uma excelente alternativa para aproveitamento mais racional da comunicação. Dentre esses recursos podemos destacar: Cache – através desse recurso o squid armazena em cache o conteúdo acessado, de forma que se algum host fizer novamente, ele recebe diretamente do cache, sem a necessidade de efetuar uma nova busca dos dados na internet.

1.1.5.1 Cache em disco

A configuração do *proxy* no BFW é feita pela configuração de *cache em disco*, e o serviço disponibilizado é o Squid que até o momento o único modo disponível é o transparente[8].

Para habilitar e configurar o Squid no BFW é disponibilizado pelas alternativas: Configurações, Regras personalizadas, Domínios não cacheados, Informações e Registro de eventos.

Em *Configurações* estão contidos os diretórios do cache, dos logs, dos relatórios, tamanhos dos caches na memória e no disco, tamanhos máximos do objeto na memória e no disco, detalhes do cache, filtro de conteúdo, repasse transparente, ocultar proxy e relatório.

As regras podem ser feitas também de forma personalizadas, ou seja, criar um arquivo com as ACLs e regras como no arquivo original do Squid o squid.conf.

Uma ótima ferramenta que também vem nativo no BFW é o Dansguardian. "O Dansguardian é um filtro de conteúdo que se integra ao Squid para a filtragem de "material impróprio", segundo configuração padrão existente" (BRAZILFW, 2014). Seus recursos são diversos como comparação de palavras, expressões regulares e substituição de palavras.

O Dansguardian associado ao Squid faz com que o controle se torne de alto nível. Para habilitá-lo deve-se marcar *filtro de pacotes* contidos em *cache em disco => configurações*.

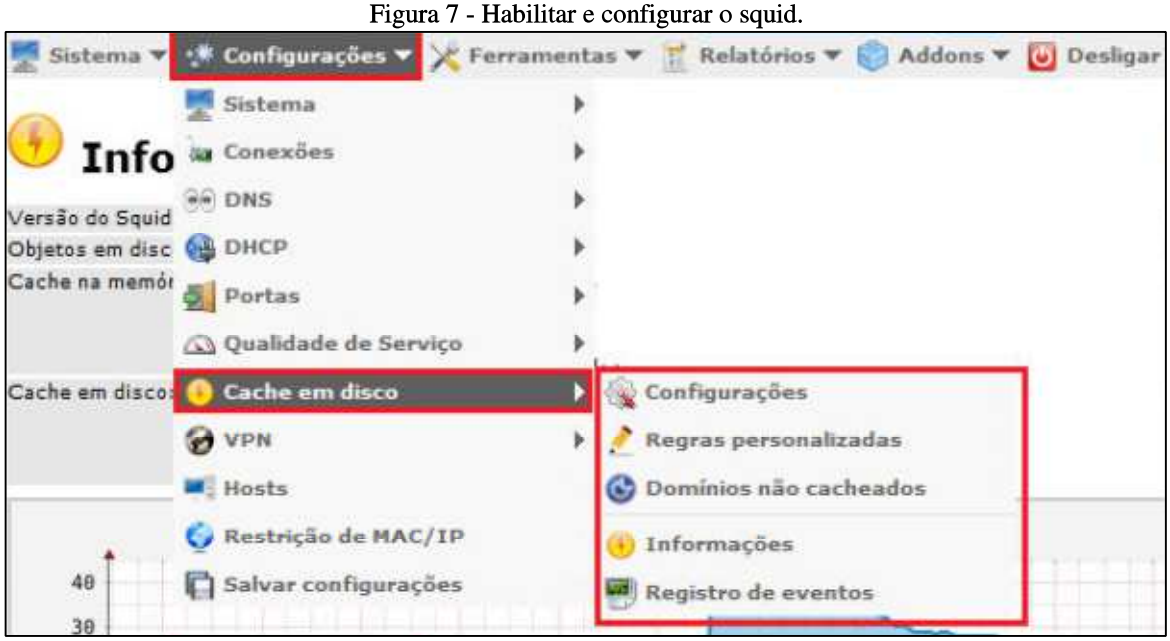
Os acessos de todo o tráfego da internet podem ser facilmente visualizados através de relatórios. O relatório é uma forma de controle e de certa forma serve como análise de acessos. Sua visualização é dada na ativação de relatório, contidos nas configurações de cache, tendo disponíveis dois módulos já instalados no sistema o FREE-AS e o Webalizer.

---

[8] Modo transparente – recebe o nome de transparente por não necessitar ser configurado o proxy no browser do cliente.

Para habilitar e configurar o Squid no *BFW 3.x* é em *webadmin => Configurações => Cache em Disco.* Nesta opção teremos: *Configurações*, *Regras personalizadas*, *Domínios não cacheados*, *Informações* e *Registro de eventos*. Como segue a Figura 7.

Figura 7 - Habilitar e configurar o squid.



Fonte: Autor

1.1.5.2 Dansguardian

Segundo BRAZILFW (2014) o dansguardian é um filtro de conteúdo que se integra ao Squid para a filtragem de "material impróprio", segundo configuração padrão existente. O mesmo é muito útil em redes onde se necessita de um controle bem rigoroso de páginas visitadas. Embora rigoroso, ele é extremamente flexível.

No dansguardian seu filtro é dinâmico que é o grande diferencial. Todo o site é analisado, e para cada tipo de palavra ou característica encontrada uma pontuação é acrescentada. Por exemplo, se achar uma palavra “sexo” ele soma 30, se achar “anal” soma mais 40, e Aa final se a página atingir um valor pré-definido o site é bloqueado.

Pode usar grupos de usuários com limites diferentes. Quanto maior o limite, mais liberal é o acesso. Há possibilidade de criar listas para controle, por exemplo, brancas, negras para site, urls, domínios, ips, usuários, extensões de arquivos e muitas outras.

REFERÊNCIAS

BRAZILFW. Disponível em: <http://www.brazilfw.com.br/forum/portal.php>. Acesso em: 20 Nov 2015.

FOROUZAN, B. A. **Comunicação de dados e redes de computadores**. 4. ed. São Paulo: McGraw-Hill, 2008.

ZOTTO, Fernando D. **Segurança da informação: uma proposta para segurança de redes em pequenas e médias empresas**. 2012. Disponível em: <http://www.projetoderedes.com.br>. Acesso em: 5 jul. 2014.