CENTRO PAULA SOUZA

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

MAURI CONSENTINO JUNIOR

ESTUDO COMPARATIVO SOBRE AS VULNERABILIDADES DOS EQUIPAMENTOS DE CONECTIVIDADE

Americana, SP

2014

CENTRO PAULA SOUZA

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

MAURI CONSENTINO JUNIOR

ESTUDO COMPARATIVO SOBRE AS VULNERABILIDADES DOS EQUIPAMENTOS DE CONECTIVIDADE

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação da Fatec Americana, sob orientação do Prof. Dr. José Luís Zem Área de concentração: Segurança de redes.

Americana, SP

2014

Consentino Junior, Mauri

C767e Estudo comparativo sobre as vulnerabilidades dos equipamentos de conectividade. / Mauri Consentino Junior. – Americana: 2014.

51f.

Monografia (Graduação de Tecnologia em Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.

Orientador: Prof. Dr. José Luiz Zem

1. Redes de computadores 2. Cabeamento de redes I. Zem, José Luiz II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU: 681.519

621.315

MAURI CONSENTINO JUNIOR

ESTUDO COMPARATIVO SOBRE AS VULNERABILIDADES DOS EQUIPAMENTOS DE CONECTIVIDADE

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana. Área de concentração: Segurança de redes.

Americana, _____ de _____ de 2014.

Banca Examinadora:

_____
José Luís Zem (Presidente)
Doutor
FATEC Americana

_____
Luciene Maria Garbuio Castello Branco
Mestre
FATEC Americana

_____
Rogério Nunes de Freitas
Especialista
FATEC Americana

AGRADECIMENTOS

Agradeço a Deus por ter me dado força e saúde para enfrentar todas as dificuldades encontradas durante o curso. Aos meus familiares, em especial meu pai e minha mãe que sempre me deram todo o apoio para que eu pudesse desenvolver esta monografia.

Ao meu orientador José Luíz Zem que me deu suporte suficiente para eu desenvolver o trabalho, tirando as minhas dúvidas, agradecer também pelas suas correções. À professora Ana Lucia Spigolon que me auxiliou nos conselhos e correções. À minha namorada que me deu força para o desenvolvimento deste trabalho. A minha irmã Vanessa que me auxiliou. E a todos que de uma forma ou de outra fizeram parte da minha formação, e meu muito obrigado.

DEDICATÓRIA

Dedico esta monografia a meu pai, minha mãe e minhas duas irmãs que me deram todo o apoio e força possível para que eu pudesse desenvolver esta monografia e nunca desistir. Aos professores que ao longo do curso compartilharam seus conhecimentos.

RESUMO

Com o desenvolvimento repentino de tantas tecnologias interligadas, todos passaram a utiliza-la. Através deste cenário surgiram pessoas maliciosas com a intenção de causar dano à tecnologia com o objetivo de roubar informações valiosas, indisponibilizar recursos digitais, etc. Devido a isso foi desenvolvida a seguinte monografia com o objetivo de localizar possíveis vulnerabilidades nos equipamentos de conectividade, definir maneiras para corrigir os erros e assim manter a segurança dos equipamentos, evitando perda de informação ou indisponibilidade de recursos aos usuários finais. Para alcançar este objetivo, foram analisados os recursos de segurança de três tipos de equipamentos de marcas distintas. E através de tabelas comparativas, confrontaram-se as ameaças de cada um. Foi utilizada pesquisa qualitativa e cientifica, para aprofundarmos no tema de segurança dos equipamentos de conectividade. Utilizou-se livros, artigos científicos, *websites* e documentação de equipamentos para o levantamento de dados.

Palavras-chave: Redes de Computadores. Vulnerabilidades. Ameaças; Segurança da Informação.

ABSTRACT

With the sudden development of many interconnected technologies, everybody started to use it. Therefore, it has appeared malicious people with intent to cause damage to technology with the goal to stolen the important information and to unavailable digital resources, etc. Because of this, it was the interest in development this monograph with the goal to locate vulnerabilities in the connectivity equipment, to identify ways to correct errors and, thus, to maintain the security, avoiding the data loss or unavailability of resources. For achieve this, it was analyzed features of three kinds of equipment of different brands. And through comparative tables, were confronted threats of each. Qualitative and scientific research was used to deepen the theme of safety equipment connectivity. It was used books, journal articles, websites and documentation of equipment for data collection.

Keywords*: Computer Networks. Vulnerabilities. Threats; Information Security.*

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

3DES: Triple Data Encryption Standard

AES: Advanced Encryption Standard

ARP: Address Resolution Protocol

CLI: Command Line Interface

DAI: Dynamic ARP Inspection

DDos: Distributed Denal of Service

DES: Data Encryption Standard

DHCP: Dynamic Host Configuration Protocol

DMZ: Demilitarized Zone

DoS: Denial of Service

DSCP: Domain to Service Processor Communication Protocol

GRE: Generic Routing Encapsulation

GUI: Graphical User Interface

HTTP: Hyper Text Transfer Protocol

HTTPS: Hyper Text Transfer Protocol Secure

ICMP: Internet Control Message Protocol

IGMP: Internet Group Management Protocol

IOS: Internetwork Operating System

IP: Internet Protocol

IPS: Sistema de prevenção de intrusão

LL2P: Layer 2 Tunneling Protocol

MAC: Media Access Control

MD5: Message-Digest algorithm 5

MPPE: Microsoft Point-to-Point Encryption

NFS: Network File System

OSI: Open System Interconection

PPTP: Point-to-Point Tunneling Protocol

PSK: Pre-Shared Key

RADIUS: Remote Authentication Dial In User Service

SHA: Secure Hash Algorithm

SSID: Service Set IDentifier

SSL: Secure Sockets Layer

SNMP: Simple Network Management Protocol

SSH: Secure Shell

TCP/IP: Transmission Control Protocol/Internet Protocol

TCP: Transmission Control Protocol

TFTP: Trivial File Transfer Protocol

TLS: Transport Layer Security

UDP: User Datagram Protocol

URL: Uniform Resource Locator

VLAN: Virtual Local Area Network

VoIP: Voice over Internet Protocol

VPN: Virtual Private Network

WEP: Wired Equivalent Privacy

Wi-Fi: Wireless Fidelity

WLAN: Wireless Local Area Network

WPA: Wi-Fi Protected Access

SUMÁRIO

1 INTRODUÇÃO

O tema desta pesquisa foi focado na segurança de equipamentos de conectividade, pois com o desenvolvimento da informática e toda a facilidade de acesso aos computadores torna-se praticamente obrigatório ter um computador nas residências, não só por praticidade, mas também por necessidade. Antigamente, aqueles que tinham computadores em suas casas usavam-nos de maneira isolada do mundo, não tinham nenhuma ligação com outros computadores.

Porém, atualmente, com a utilização destes computadores conectados em rede obtém-se uma série de benefícios, tais como compartilhar arquivos, recursos como *scanner* e impressora, consultar banco de dados, jogos em rede, compartilhamento de *Internet*, entre outras e desta maneira, é difícil imaginar uma casa sem computador não estar ligado a uma rede.

> "Devido ao crescimento das redes wi-fi, somos obrigados a pensar em protegê-las, aplicando alguma segurança. No entanto, elas possuem uma série de peculiaridades nas suas configurações, que um usuário comum ou até mesmo algum técnico desconheça". (PINZON, 2009).

Entretanto, todos esses benefícios trazem consigo um problema: o computador estará ligado através de equipamentos de conectividade, tais como *Switches*, roteadores, repetidores, pontes, *access points* e, também, através de meios guiados (*wired*) e não guiado (*wireless*) o que os tornam vulneráveis a ataques provenientes dos demais computadores. Assim, uma preocupação que não existia anteriormente surge no horizonte dos usuários, a questão da segurança, das informações contidas no computador, e também a segurança do próprio computador e dos equipamentos de conectividade.

Nos dias atuais, vem crescendo a utilização de equipamentos de conectividade para o uso pessoal em razão do aumento de celulares, *smartphones, notebooks* e computadores pessoais.

O **problema** é que muitas pessoas não tomam ou se preocupam com medidas de segurança em sua rede doméstica, ou por serem leigos no assunto, ou por falta de tempo ou ainda pela fácil instalação dos equipamentos (tecnologia *plug and play*). Com isso acabam expondo, de maneira vulnerável, o acesso às informações e aos computadores.

Já existem vários protocolos previamente existentes para garantir a segurança dos equipamentos de conectividade, mas a questão é se ao utilizar tais protocolos e padrões os equipamentos e a informação estarão realmente seguros.

A **justificativa** para o desenvolvimento desta monografia reside na intenção de que os usuários saibam como proteger seus equipamentos de conectividade diminuindo os riscos de ataques aos mesmos, deixando os usuários mais confortáveis e seguros.

Alguns procedimentos de segurança já são aplicados atualmente e, na maioria dos casos são:

- Alteração da senha de acesso;
- Alteração dos métodos de criptografia;
- Desabilitação o *broadcast* do SSID (*Service Set IDentifier*);
- Filtragem dos usuários pelo endereço de MAC;
- Atribuição de endereços IP exclusivamente para usuários registrados;
- Desabilitação o do DHCP (*Dynamic Host Configuration Protocol*).

O **objetivo principal** desta pesquisa foi identificar as vulnerabilidades nos equipamentos de conectividade, levantando dados e comparando os mesmos, por meio de tabelas, com a intenção de sempre alcançar maiores cuidados com os aspectos de segurança, mantendo os equipamentos de conectividade protegidos.

O **objetivo específico** desta pesquisa foi o de identificar o motivo das vulnerabilidades na segurança dos equipamentos de conectividade, tentando mostrar formas de manter os equipamentos de conectividade seguro com o objetivo de que não haja perda e nem danos às informações dos usuários finais.

O projeto inseriu uma **proposta metodológica** qualitativa e pesquisa científica, de aprofundamento no tema de segurança dos equipamentos de conectividade.

Sendo que a pesquisa qualitativa buscou informações qualificadas para a estruturação desta monografia e a pesquisa cientifica foi feita através de *websites*, livros e artigos científicos.

Usando como **sujeito** da pesquisa os equipamentos de conectividade, tais como: *Access Point*, *Switch*, *Hub* e Modem.

A **coleta de dados** foi feita através de artigos, livros e *websites;* sobre Equipamentos de Conectividade, Segurança da Informação, Rede de Computadores, ameaças e vulnerabilidades.

2 REFERENCIAL TEÓRICO

Esta seção aborda as principais áreas envolvidas no desenvolvimento desta pesquisa sobre equipamentos de conectividade. Abordam questões relativas à segurança de redes, Segurança da Informação e os Equipamentos de Conectividade, Técnicas de Segurança para os Equipamentos de Conectividade, Tipos de Invasões e Ameaças, Procedimentos Metodológicos, Discussão dos Resultados e Conclusão.

2.1 SEGURANÇA DE REDES

A segurança de redes são procedimentos físicos e virtuais implantados de maneira adequada em situações específicas nos equipamentos de conectividade e que garantem a comunicação entre eles de maneira segura, sem nenhuma interceptação, modificação ou remoção nos dados que trafegam pela rede.

Para que tais procedimentos garantam o máximo de segurança possível devem ser implantados respeitando-se os três pilares da segurança da informação que segundo (SENAC, 2014) são, Confidencialidade, Integridade e Disponibilidade.

Uma das maneiras mais eficientes para de se obter a segurança de rede é a criptografia, garantindo a privacidade das informações, outra maneira é a utilização de *hashing*, a autenticação de usuários para a garantia de que o acesso ao dispositivo ou sistema seja feito apenas pelo usuário autorizado. O gerenciamento de chaves, *firewall* (equipamentos ou aplicações que têm a função de filtro do que entra e sai da rede permitindo somente o fluxo de pacotes autorizados), VPN-*Virtual Private Network* que implementa a comunicação de dois ou mais locais, distantes geograficamente por meio de um túnel criado na *Internet*.

2.2 A SEGURANÇA DA INFORMAÇÃO E OS EQUIPAMENTOS DE CONECTIVIDADE

Conforme o Dicionário Aurélio[1] Segurança é “Ação ou efeito de segurar. / Situação do que está seguro; afastamento de todo perigo”.

Conforme o Dicionário Aurélio[2] Informação é a “Ação de informar ou informar-se. / Notícia recebida ou comunicada; informe. / Quantidade de informação, medida quantitativa da incerteza de uma mensagem em função do grau de probabilidade de cada sinal que compõe essa mensagem”.

A informação sempre foi um bem muito importante. Antigamente a informação era armazenada basicamente em uma folha de papel. Desta maneira a disseminação da informação era algo mais complexo, sendo que a sua segurança se tornava mais simples de se implementar; era só armazenar em uma gaveta trancada e limitar o acesso físico àquele local. Hoje, com a utilização de computadores de grande porte e a informatização das empresas, mudou-se o local de armazenamento das informações, que passou a ser guardada não mais em papéis dentro de armários ou gavetas, mas sim em computadores e servidores de maneira digital, porém ainda centralizados. Com a chegada das redes de computadores para interligar os dispositivos ao mundo, por intermédio dos equipamentos de conectividade, a informação se disseminou mais rapidamente para todo o mundo e com isso ela ficou mais exposta e vulnerável.

> “A informação é um bem tal como vários outros, portanto deve ser vista como um “Ativo” da instituição. Ela deve ser mantida pelo tempo necessário conforme seu grau de importância. As interligações das empresas através das redes de computadores, pessoas e eventos naturais, podem mostrar as vulnerabilidades que põem em risco as informações. Por isso, é necessária a implantação de processos de segurança que resguardem a informação contra essas ameaças.” (RAMIRO, 2008).

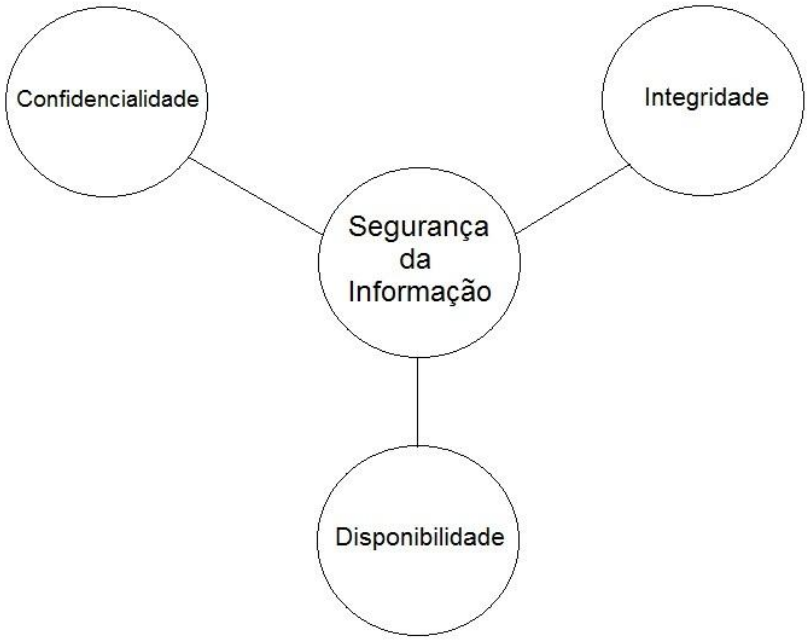
Segurança da Informação é uma maneira de proteção de informações buscando assegurar a originalidade de um conjunto de dados.

[1] Disponível em <http://www.dicionariodoaurelio.com/Seguranca.html>. Acesso em: 13 abr. 2014.
[2] Disponível em <http://www.dicionariodoaurelio.com/Informacao.html>. Acesso em 13 abr. 2014.

> “Segurança da informação não pode mais se preocupar apenas com a perda de dados relacionada a um acidente com os meios de arquivamento. Há agora a ameaça de ataques via rede, vandalismos ou técnicas de negação de serviço – DoS – do inglês *Deny of Service*. Além disso, existe ainda o perigo do ataque.”(RAMIRO, 2008)

Assim, necessita-se da implantação da segurança para que a informação não deixe de atender a nenhum item dos três pilares da segurança da informação apresentados a seguir.

Figura 1 - Os três Pilares da Segurança da Informação.



Fonte: Elaborada pelo autor.

Observando-se a Figura 1, pode-se afirmar que há três pilares importantes que sustentam a Segurança da Informação, para que de fato a segurança seja efetiva necessita-se de confidencialidade, integridade e disponibilidade. Neste caso a segurança da informação aplica-se à sistemas computacionais, equipamentos de conectividade e informações eletrônicas.

A **Confidencialidade**, segundo (SENAC, 2014) como o próprio nome diz, é a garantia de que todos os dados trafegados através dos equipamentos de conectividade sejam acessíveis apenas pelos usuários que tenham a autorização de acesso independente de onde esta informação esteja ou do meio de acesso para se chegar à ela.

A **Integridade** segundo (SENAC, 2014) é a garantia de que a informação seja mantida em seu estado inicial a partir do momento de sua criação pelo proprietário; buscando a proteção da informação contra alterações acidentais (usuário a altera sem a intenção, algum problema em sua transmissão, problemas no armazenamento ou desastres naturais), indevidas ou intencionais (informação alterada propositalmente por algum motivo, *hackers*).

E a **Disponibilidade** segundo (SENAC, 2014) é a manutenção para que a informação fique sempre disponível para que os usuários legítimos, ou seja, aqueles que estejam autorizados a ter acesso à informação específica.

De acordo com o Dicionário Michaelis Equipamento é o “Conjunto de instrumentos e instalações necessários para um trabalho ou profissão”.

Conectividade de acordo com Dicionário Michaelis é a “Capacidade de um dispositivo de se conectar com outros dispositivos e transferir informação”.

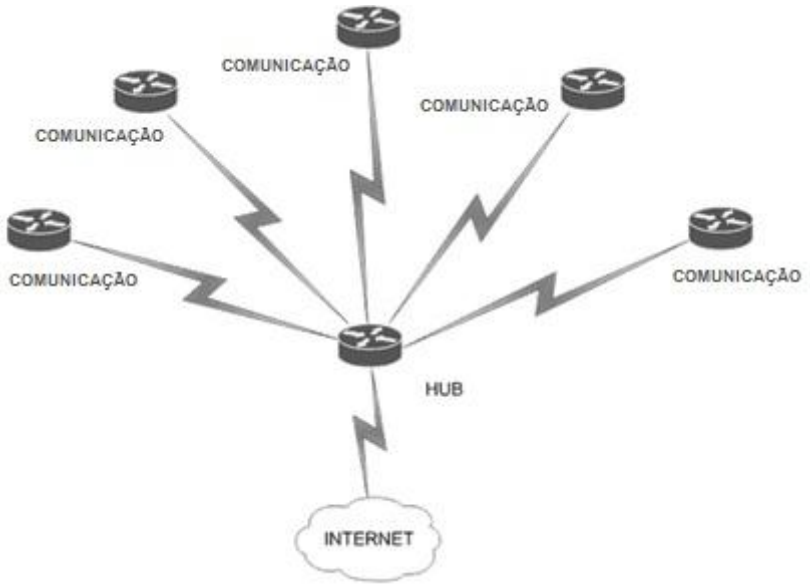
Assim, os equipamentos de conectividade são aqueles que viabilizam a comunicação de dois ou mais dispositivos, como exemplos de equipamentos de conectividade tem-se o *Hub*, o *Switch*, o Roteador, o Modem, o *Access Point,* entre outros.

O ***Hub*** conforme Figura 2, segundo (BRITO, 2014) é um equipamento de conectividade relativamente antigo e que trabalha na camada física do modelo OSI (Para mais informações sobre o Modelo OSI, leia o livro TANENBAUM, Andrew S. **Rede de Computadores**.). Ele é um concentrador que conecta vários computadores de uma rede e permite a transmissão de pacote entre os mesmos, porém possui um ponto fraco em sua operação: ao pegar pacotes do computador de origem para enviar ao de destino, o *Hub* envia os pacotes para todos os computadores nele conectados a ele (*Broadcast*). Este procedimento gera dois grandes problemas, um

deles é o grande tráfego de dados na rede, ocasionando congestionamento e lentidão na entrega de pacotes, assim prejudicando o desempenho da rede. Outro problema é que ele acaba expondo dados à qualquer computador conectado e se houver uma pessoa mal intencionada nessa rede, pode ocorrer um problema ainda maior de segurança.

Em razão destes pontos fracos o *Hub* tornou-se pouco utilizado e com a criação do *Switch* ele foi sendo substituído gradativamente.

Figura 2 – *Hub.*



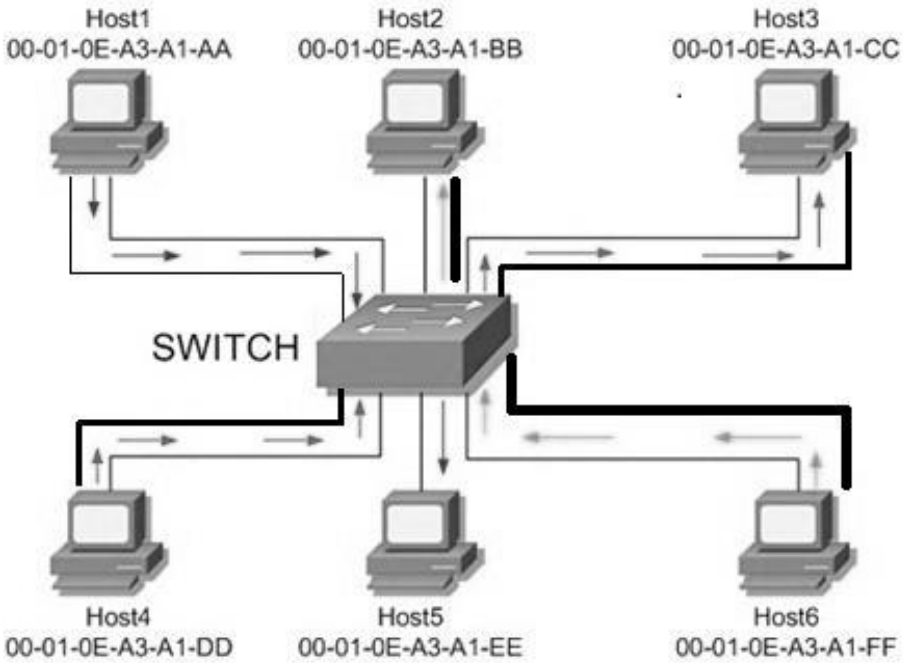
Fonte: (REDES PRÁTICAS, 2014).

O ***Switch*** conforme Figura 3, segundo (BRITO, 2014), é um equipamento de conectividade, que trabalha na camada enlace do modelo OSI. Um dos motivos de sua criação foi para solucionar os problemas apresentados pelo *Hub* relatado anteriormente.

Ele é um concentrador de tal como o *Hub*, mas tem como diferença a capacidade de, quando um computador enviar um pacote para outro computador este pacote será repassado apenas ao destinatário, fazendo com que os pacotes não fiquem expostos à outros computadores.

Este processo decodifica o cabeçalho do pacote e encontra informações sobre o receptor dos dados. O *switch* armazena os endereços dos destinatários em uma tabela criada em sua memória. Com essas informações o *switch* consegue entregar o pacote somente para o destinatário correto, e assim diminui o tráfego de dados na rede, possibilitando um maior desempenho para a mesma.

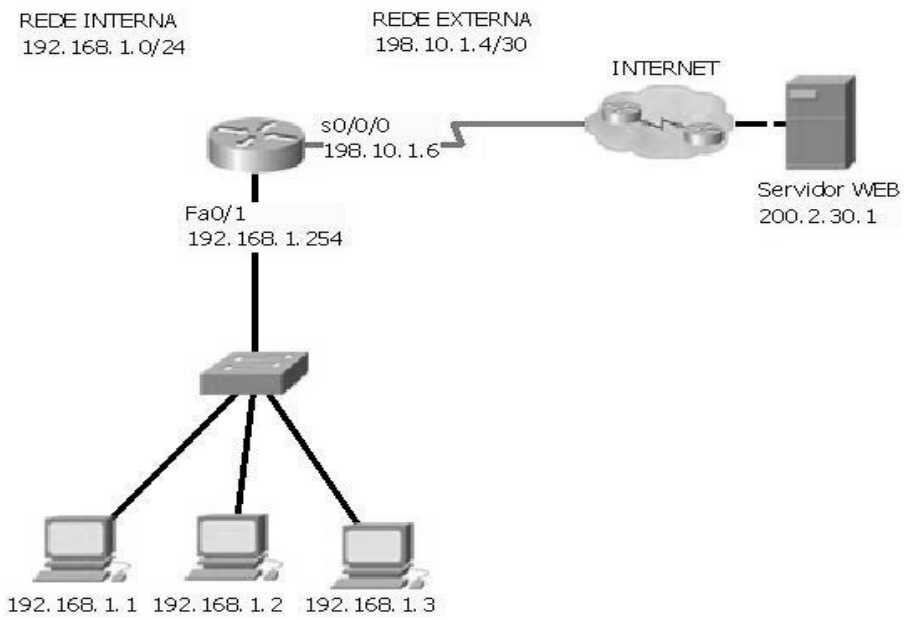
Figura 3 – *Switch.*



Fonte: (ORTEGA, 2010).

O **Roteador** conforme Figura 4, segundo (BRITO, 2014), é um equipamento que trabalha na camada de rede do modelo OSI, e faz o papel de intermediador na rede, possibilitando trocas de pacotes entre redes diferentes.

Figura 4 – Roteador.

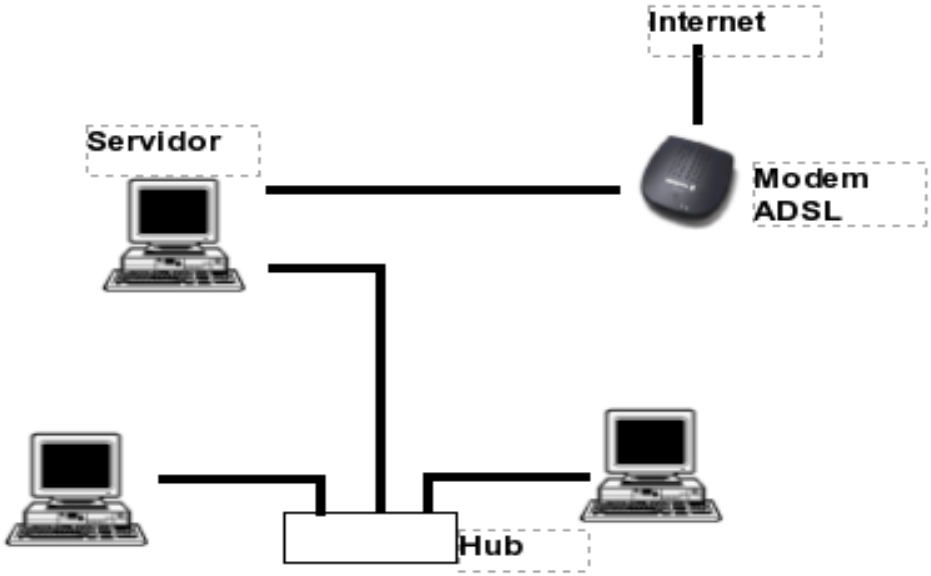


Fonte: (TI - REDES, 2011).

A utilização deste equipamento é necessária quando é preciso interligar redes separadas e ao mesmo tempo mantê-las isoladas. Na utilização de um computador em uma rede que contém um roteador, ele não vai conseguir enxergar a outra rede. Podem ser encontrados roteadores em formato de equipamentos dedicados ou em computadores com dois ou mais placas de rede.

O **Modem** conforme Figura 5, segundo (BRITO, 2014) é um equipamento que trabalha na camada física do modelo OSI, e sua função é modular o sinal digital em onda analógica para haver transmissão por linha telefônica, e demodular sinal analógico e converte-lo novamente para digital. Desta maneira ele cria uma comunicação entre os dois pontos. Por este motivo o equipamento tem este nome, com a junção das duas palavras (MO)dulador e (DEM)odulador.

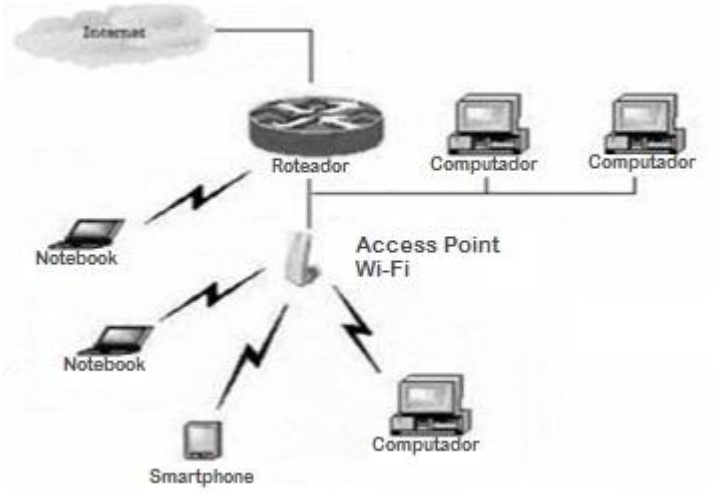
Figura 5 – Modem.



Fonte: (MORIMOTO, 2010).

O ***Access Point*** conforme Figura 6, segundo (BRADLEY, 2014), trabalha na camada física do modelo OSI, e são equipamentos configurados para redes *wireless*. O *Access Point* transmite e recebe sinais de radiofrequência sem fio e são bastante utilizados para dar suporte a uma rede domestica e também à redes corporativas, buscando ampliar o sinal *wireless,* e consequentemente, aumentar a área de cobertura.

Figura 6 – *Access Point.*



Fonte: (MIURA, 2014).

2.3. TÉCNICAS DE SEGURANÇA PARA OS EQUIPAMENTOS DE CONECTIVIDADE

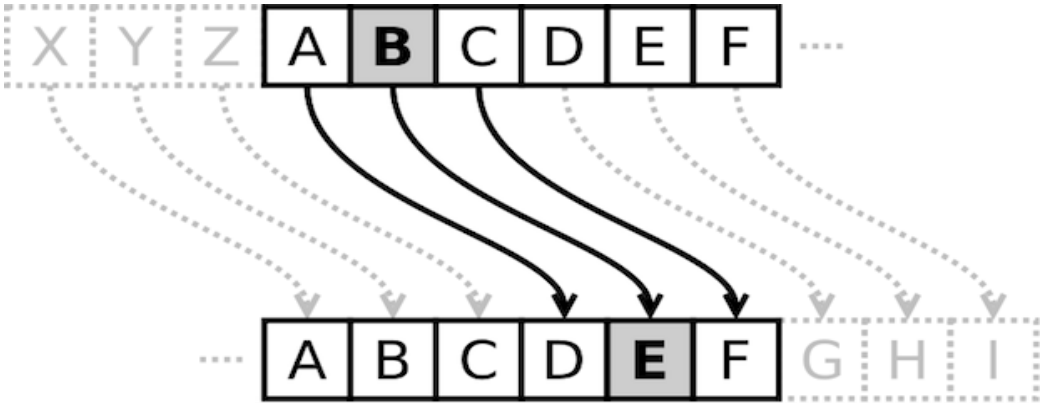
Com o crescimento da utilização de todos os equipamentos citados anteriormente, muitos dados importantes e valiosos passaram a trafegar por equipamentos de conectividade, e devido a este fato, criou-se o interesse de pessoas ou organizações interessadas em obter, alterar ou excluir tais informações pessoais ou corporativas. Para combater estas ações, houve-se a necessidade de criar diversos métodos de segurança para dispositivos de rede.

Nesta seção são abordadas técnicas de segurança para equipamentos de conectividade, destacando-se a Criptografia, Autenticação, Controle de Acesso, Controle de Roteamento, Integridade dos dados e *Firewall*.

Criptografia, segundo (PISA, 2012), é uma técnica muito importante na segurança de rede principalmente, se houver a necessidade de se obter privacidade no tráfego dos dados. Ela é um conjunto de técnicas usadas para mascarar dados de acessos não autorizados. A criptografia transforma qualquer tipo de informação como textos, arquivos, senhas ou e-mails, por exemplo, em um conjunto de caracteres, embaralhados, procurando fazer com que um usuário não autorizado não consiga entender o seu conteúdo. Há um conceito de chave na criptografia e ele consiste em que apenas quem possuir a chave de decriptação conseguirá visualizar a informação de maneira legível.

Segundo os historiadores, o Código de César conforme Figura 7, é um dos métodos criptográficos mais antigos. Ele é relativamente simples, desloca as letras do alfabeto de acordo com a chave, se a chave era três, transformava-se o valor inicial no valor final dela, como o A transformava-se em D, B transformava-se em E, e o C transformava-se em F e assim sucessivamente. Porém este tipo de código era muito inseguro, possuindo somente vinte e seis variações diferentes.

Figura 7 - Código de César.



Fonte: (PISA, 2012).

Acompanhando os avanços tecnológicos a criptografia também evoluiu, e hoje tem-se técnicas eficientes e seguras como o 3DES (*Triple Data Encryption Standard)* e o AES (*Advanced Encryption Standard*) ambos são algoritmos base dos protocolos SSL (*Secure Sockets Layer)* e TLS (*Transport Layer Security*) muito utilizados atualmente para a segurança dos dados na Internet (PISA, 2012).

A **Autenticação**, segundo (AMOROSO, 2009), é uma técnica de segurança implantada em equipamentos de conectividade, sistemas operacionais e etc, para confirmar se um usuário é ou não autorizado a acessar aquele equipamento ou sistema.

Na rede de computadores uma maneira comum de autenticação é a utilização de senhas para o acesso. Neste caso o conhecimento da senha correta já é o suficiente para fazer a autenticação do usuário. A utilização de uma autenticação em qualquer equipamento de conectividade é de suma importância, pois impede que o usuário faça qualquer conexão com o dispositivo e para que impossibilite que qualquer usuário não autorizado faça o acesso ao equipamento.

O **Controle de Acesso**, segundo a MICROSOFT é um processo de autorização de usuários, grupos e computadores para ter o acesso à rede usando direitos de usuários ou permissões. Pode ser utilizado em alguns equipamentos de conectividade tais como roteador e *Access Point* para permitir ou bloquear acesso a recursos de configuração dos dispositivos e acesso a sites.

O **Controle de Roteamento** segundo Soares (1995 apud CARNEIRO e Júnior, 1999) é um método que consiste na garantia de que a informação seja transmitida de maneira segura por rotas físicas fazendo, com que os canais de comunicação disponibilizem níveis de segurança suficiente pare que os dados trafeguem de maneira segura. Por meio deste controle as rotas para a transferência de dados devem ser especificadas corretamente pelo administrador da rede.

A **Integridade dos dados** segundo Soares (1995 apud AMBROSI, 2004) é uma técnica utilizada para fazer o controle da integridade de dados isolados, e trabalha em dois níveis: controle de integridade de uma conexão e controle de integridade de conexão.

No primeiro nível, há maneiras de realizar a verificação de modificações que são ligadas a detecção de erros de *bits*, erros na sequência ou pacotes, isto é, usado para garantir que os dados trafegados estejam íntegros e que cheguem ao usuário final em perfeito estado. Para que os dados se mantenham íntegros há a necessidade de que eles estejam confidenciais.

Agora para que consiga controlar corretamente as modificações na sequencia dos pacotes transmitidos em uma conexão, precisa-se de técnicas que consiga mantê-los íntegros, garantindo a transmissão dos pacotes sem erros (Soares, 1995 apud AMBROSI, 2004).

O ***Firewall,*** segundo Kanishima, et al (2000 apud JASCONE, 2003), é uma técnica útil para a complementação de uma segurança de rede, principalmente em redes que estão conectadas à *Internet*. Como é possível verificar com a tradução de *firewall* (parede de fogo), sua função é gerar uma barreira de proteção criada por *hardware* e/ou *software*. Pode ser visto como dois tipos de mecanismo: bloqueio de tráfego ou permissão do tráfego de dados na rede, e para que ele seja extremamente eficaz dependerá do administrador de rede configurá-lo de maneira correta, estabelecendo políticas e regras de segurança suficientes para a proteção.

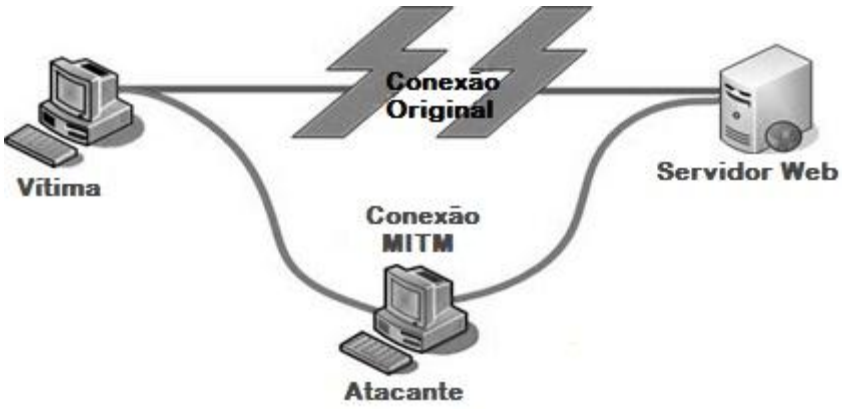
2.4 TIPOS DE AMEAÇAS E DE INVASÕES POSSÍVEIS

As seções seguintes explicarão detalhadamente tipos de ameaças e de invasões possíveis, tais como: *Spoofing, Sniffing, Mapping, Hijacking, Trojan e* Engenharia Social.

2.4.1 *SPOOFING*

Segundo (MENEZES, 1998) é uma técnica de falsificação de IP, essa técnica consiste em alterar o endereço de origem de um pacote para o endereço de outra máquina, sendo assim o computador do usuário poderá se passar por qualquer outra máquina, desta maneira é possível que o atacante assuma a identidade de qualquer máquina na *Internet.* Este ataque é mais perigoso ainda quando direcionado aos serviços baseados no protocolo UDP (*User Datagram Protocol*) grande parte dos serviços que rodam neste protocolo limitam-se a acesso à algumas máquinas. O NFS (*Network File System*) é um serviço de compartilhamento de arquivos e diretórios na rede é um bom exemplo, o atacante envia um pacote UDP ao servidor onde está hospedado o serviço NFS, se passando por uma máquina cliente que esteja apta a editar e gravar algo em algum diretório, após o envio do pacote ao servidor, o servidor vai entender que esta máquina que está enviando é algum cliente dele devido ao fato do IP de origem ter sido falsificado, sendo assim todas as solicitações feitas pelo atacante serão atendidas pelo servidor. Para bloquear o *Spoofing* conforme Figura 8, há a necessidade de um *firewall* na rede, realizando o bloqueio a partir do momento em que o provedor configura quais interfaces de rede ele receberá pacotes. Assim, o atacante envia pacotes tentando se passar por uma máquina da rede interna para o *firewall*, e imediatamente ele descarta o pacote, pois ele verifica que este pacote não pertence a uma rede válida.

Figura 8 – *Spoofing*.

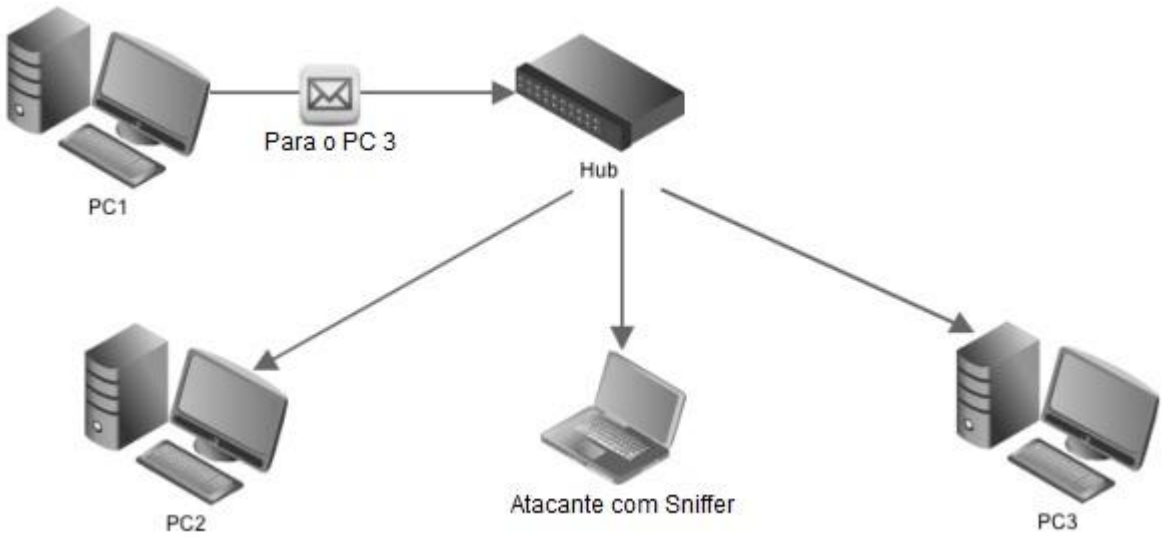


Fonte: (Ethical Hacking, 2011).

2.4.2 *SNIFFING*

Segundo (SOUZA, 2014) *Sniffing* conforme Figura 9, é um procedimento feito por um software chamado *sniffer* que intercepta e faz o registro do tráfego de dados em uma rede. O *sniffer* faz a captura de pacotes, e em certos momentos ele decodifica e analisa o conteúdo do mesmo. Devido a esta funcionalidade ele começou a ser utilizado de maneira maliciosa por *crackers* para capturar o tráfego da rede para benefícios próprios, tais como: captura de senhas de usuários, arquivos com informações importantes durante a transmissão ou até mesmo visualizar conversações no momento em que elas estão acontecendo. Um dos *softwares* para realizar o *sniffing* é o *Wireshark*.

Figura 9 – *Sniffing*.

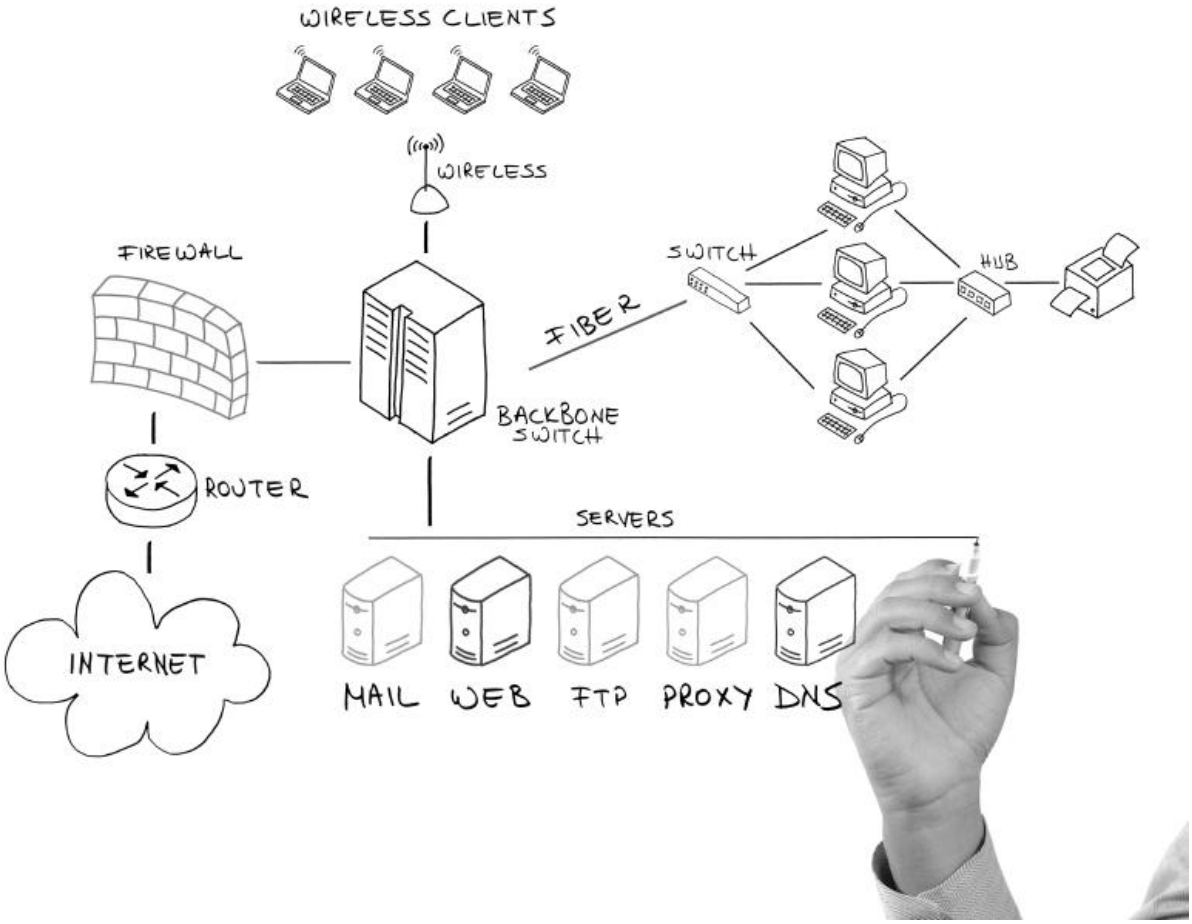


Fonte: (JOHN V., 2012).

2.4.3 *MAPPING*

Em quase todas as vezes que o atacante pretende invadir uma rede, este é o primeiro procedimento realizado para fazer o mapeamento da rede. *Mapping* conforme Figura 10, consiste em capturar o máximo de informações sobre a rede que o atacante deseja invadir, sendo assim ele passa a conhecer detalhes que o possibilitam a ele realizar ataques em pontos específicos com um menor risco de ser descoberto. O êxito maior ou menor do atacante dependerá do grau de segurança que existe na rede. Um dos *softwares* para realizar o *mapping* é o Nmap.

Figura 10 – *Mapping*.



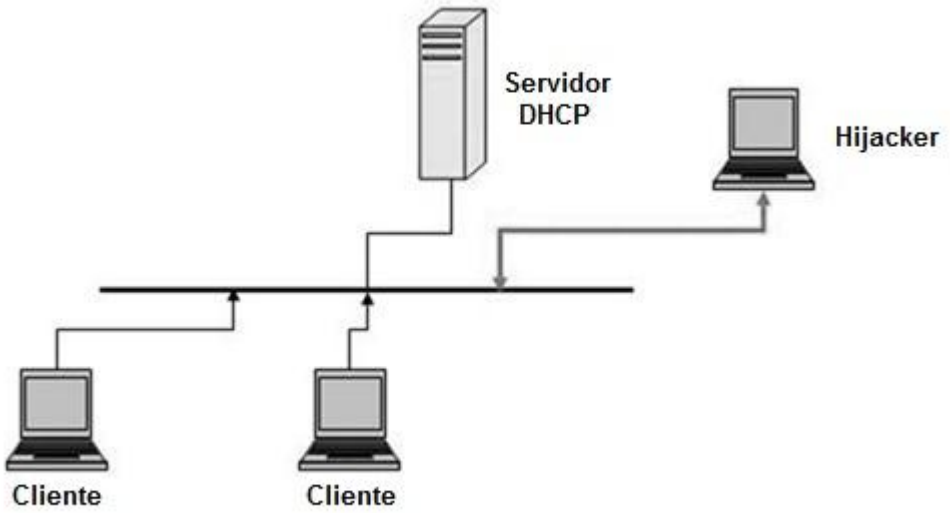
Fonte: (PROFESSIONAL COMPUTER SERVICES, 2012).

2.4.4 *HIJACKING*

Segundo (ROUSE, 2007) a tradução para português de *Hijacking* conforme Figura 11 é: sequestro e nele o atacante obtém o controle da comunicação. Este ataque consiste em assumir uma conexão que já está estabelecida e em andamento. Os *crackers* utilizam softwares que acessam o computador sem que o usuário perceba, utilizando brechas na segurança e tendo como, um dos objetivos é o acesso às mensagens, mesmo antes delas serem transmitidas.

Os atacantes utilizam este ataque pelo navegador, eles modificam a página inicial do navegador no computador, começam abrir muitas páginas sem a solicitação do usuário.

Figura 11 – *Hijacking*.



Fonte: (REESE, 2011).

2.4.5 *TROJAN*

Segundo (PEREIRA, 2008) *Trojan* conforme Figura 12, é um *software* malicioso, introduzindo no computador disfarçado como programas que simulam ser úteis e funcionais aos usuários, mas na verdade é um *software* que pode trazer prejuízos ao computador. A função dele é abrir portas do computador para que, futuramente, o atacante consiga o acesso ao computador no qual o *Trojan* foi instalado. São dois os tipos de *Trojans,* os *Backdoors* que são utilizados para a abertura de portas do

computador e *Keylogger,* que são utilizados para a captura de senhas. Um dos *softwares* para se atacar com *Trojan* é o *turkojan.*

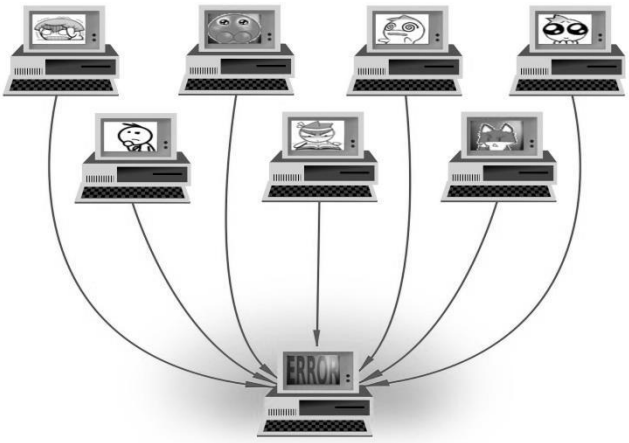
Figura 12 – *Trojan*.

Fonte: (HYPHENET, 2013).

2.4.6 *DENIAL-OF-SERVICE E DISTRIBUTED DENIAL-OF-SERVICE*

DoS e DDoS conforme Figura 13, são tipos de ataque que consistem em muitas tentativas de acesso a um servidor, fazendo com que ele não consiga realizar serviços para os quais ele foi configurado. O atacante solicita muitas requisições à máquina até que ela chegue a um ponto em que não possa atendê-las; o equipamento fica tão sobrecarregado e acaba negando serviço. Um dos *softwares* para realizar o DoS é o *Slowloris.*

Figura 13 – *Dos*.



Fonte: (DELGADO, 2011).

2.4.7 ENGENHARIA SOCIAL

Segundo (SKYPE, 2014) São técnicas de abordagem criadas para que os atacantes possam obter informações importantes e particulares fazendo com que as pessoas as revelem. Para conseguir acesso à dados e informações armazenadas em computadores, os atacantes utilizam a engenharia tanto *online* quanto pessoalmente. Por meio *online,* grande parte dos atacantes utilizam *e-mails* para aplicar esta técnica; os *e-mails*, muitas vezes, vêm com textos ou imagens chamativas contendo algum *link* para que o usuário clique e redirecione para algum site que a pessoa informe dados e até senhas sobre algo relacionado a ela. Pessoalmente ou por telefone o atacante costuma dizer que é de uma empresa e solicita informações pessoais ou corporativa de maneira persuasiva, a pessoa acabe cedendo as informações a ele.

3 LEVANTAMENTO DE INFORMAÇÕES E DISCUSSÃO DOS RESULTADOS

Este capítulo trata da discussão dos resultados obtidos, contendo tabelas comparativas entre Roteadores, *Switches*, e *Access Points* com três tipos distintos de equipamentos em cada uma delas. Foram analisados manuais de equipamentos de conectividade através de *websites* para obter todas as especificações de segurança de cada um deles, com isso foram criado as tabelas comparativas. Foram escolhidos as marcas como D-link, Cisco e TP-Link, pois são as mais conhecidas e utilizadas.

Para cada tipo de equipamento tem-se duas tabela, uma para comparar os tipos de seguranças que cada um possui e outra para comparar quais dispositivos são ou não vulneráveis aos tipos de ameaças citadas em anteriormente.

3.1 ANÁLISE DE ROTEADORES

A Análise de Roteadores trata-se da identificação de cada roteador levantando todas as especificações de segurança e analisando se eles são ou não vulneráveis a cada tipo de ameaça.

Os Roteadores utilizados no levantamento das informações foram: Roteador *Wireless* N de Serviços Unificados - DSR-500N para D-Link; Roteador *SafeStream Gigabit Dual*-WAN VPN - TL-ER6120 para TP-Link e Roteador C1905 2GE HWIC-1T *IPBase* BR para Cisco.

Tabela 1: Roteador - Tipos de ameaças

	D-Link	**TP-Link**	**Cisco**
Spoofing	NV por causa do (IPS)	NV, por causa da inseção ARP	NV por causa do (IPS)
Sniffing	NV por causa do (IPS), VPN e cript	NV por causa do VPN e cript	NV por causa do (IPS), VPN e cript

Mapping	NV por causa do (IPS), VPN, cont. de ameaça e cript.	NV por causa da VPN, cont. de ameaça e cript.	NV por causa do (IPS), VPN, cont. de ameaça e cript.
Browser hijacking	NA	NA	NA
Trojan	NA	NA	NA
DoS e DDoS	V	NV	NV
Engenharia Social	NA	NA	NA

NA - Não Aplicável - **V –** Vulnerável - **NV -** Não Vulnerável (Fonte: Próprio autor)

Todos os roteadores analisados não são vulneráveis às ameaças de ***Spoofing***, ***Sniffing*** *e* ***Mapping****.*

Em relação à ameaça de ***Spoofing****,* os itens de segurança que os deixam protegidos são, o IPS no roteador da D-Link e Cisco, e a inspeção ARP no da TP-Link.

Itens de segurança que protegem os roteadores da D-Link e Cisco contra a ameaça de ***Sniffing*** são IPS, VPN e criptografia, e os itens VPN e criptografia protegem o roteador da TP-Link.

Em relação ao ***Mapping*** nos roteadores da D-Link e Cisco os itens que os protegem são IPS, VPN, controle de ameaça e criptografia, agora no roteador da TP-Link são os itens VPN, controle de ameaça e criptografia.

Em relação à ameaça **Dos** e **DDos** somente o roteador da D-link é vulnerável.

As ameaças de ***Browser Hijacking****,* ***Trojan*** *e* **Engenharia Social** não são aplicáveis à roteadores.

Tabela 2: Roteador - Tipos de seguranças

	D-Link	TP-Link	Cisco
Controle da Aplicação IM, P2P	NCD	Sim	NCD
Inspeção ARP	NCD	Inspeção ARP com Envio de pacotes	NCD

		GARP, varredura de ARP por WAN / LAN e Vinculação de IP-MAC	
Filtro de MAC	NCD	Sim	NCD
Filtro de URL	Sim, Filtragem de conteúdos web (URL estática, palavras chave)	Sim, Palavra-Chave, filtro de conteúdo web, (Java, *ActiveX*, *cookies*)	Sim , URL e palavra-chave
IPS	Sim, pacote de assinaturas incluído no *firmware*	NCD	Sim, Cisco IOS
Configuração do Equipamento	Web HTTP, HTTPS	Web, CLI e Telnet	Via Browser, Gerenciamento de identidade com autenticação, autorização e contabilidade (AAA), e infraestrutura de chave pública, *CiscoWorks* LMS, Cisco *Works* NCM , *Security Manager*, *License Manager* e Cisco Configuration *Engine*, Cisco *License Manager*
Controle de Acesso/Ameaça	Sim, *Firewall* : Pacote assinatura incluída em *Firmware*, protocolo GRE	Sim, Proteção auto. p/ detectar e bloquear ataques DoS e DDoS , tais como TCP, UDP e ICMP *Flooding*, TCP *Scanning*, Ping da Morte e outras ameaças, hardware DMZ para configuração de servidores públicos para não expor a rede interna	Sim, Cisco IOS *Firewall*, Cisco IOS *Firewall Zone-Based*, Cisco IOS Filtro de Conteúdo, prevenção de intruso e serviços de segurança avançadas

NCD - Não consta na documentação (Fonte: Próprio autor)

Em relação aos itens de segurança, o item **controle da aplicação IM, P2P** está presente no roteador da TP-Link, no roteador da D-Link, porém no da Cisco não consta na documentação.

A **inspeção ARP** só consta na documentação do roteador da TP-Link com a seguinte descrição: Inspeção ARP com Envio de pacotes GARP, varredura de ARP por WAN/LAN e Vinculação de IP-MAC, também somente no TP-Link consta na documentação que contêm filtro de MAC.

Todos os roteadores vêm com o item de segurança de **filtro de URL** com a seguinte descrição: roteador da D-Link: Filtragem de conteúdos *web* (URL estática, palavras

chave); roteador da TP-Link: Palavra-Chave, filtro de conteúdo *web*, (Java, *ActiveX*, *cookies*); roteador da Cisco: filtro de URL e palavra-chave**.**

O item **IPS** está presente no roteador da D-Link e da Cisco com a seguinte descrição roteador da D-Link: pacote de assinaturas incluído no *firmware*; roteador da Cisco: IPS no Cisco IOS, agora no roteador da TP-Link não consta na documentação.

A **configuração do roteador** D-Link é feita por *Web* HTTP e HTTPS, a do TP-Link é feita por *Web*, CLI e *Telnet* e no roteador da Cisco é feita Via *Browser*, Gerenciamento de identidade com autenticação, autorização e contabilidade (AAA), e infraestrutura de chave pública, *CiscoWorks* LMS, Cisco *Works* NCM , *Security Manager*, *License Manager* e **Cisco** *Configuration Engine* e Cisco *License Manager*.

Todos os roteadores possuem **controle de acesso/ameaça**, características de cada roteador: roteador D-Link: *Firewall*: Pacote assinatura incluída em *Firmware*, protocolo GRE; roteador TP-Link: Proteção automática para detectar e bloquear ataques DoS e DDoS , tais como TCP, UDP e ICMP *Flooding*, TCP *Scanning*, Ping da Morte e outras ameaças, *hardware* DMZ para configuração de servidores públicos para não expor a rede interna; roteador Cisco: Cisco IOS *Firewall*, Cisco IOS *Firewall Zone-Based*, Cisco IOS Filtro de Conteúdo, prevenção de intruso e serviços de segurança avançadas.

Tabela 3: Roteador - Tipos de seguranças (VPN)

	D-Link	**TP-Link**	**Cisco**
Criptografia da VPN IPSec	DES, 3DES, AES, *Twofish*, *Blowfish*, CAST-128, NULL	DES, 3DES, AES128, AES192, AES256	Acelerado por *hardware* incorporado(IPsec + SSL)
VPN SSL	Sim	NCD	Sim
Criptografia da VPN	SSL: DES, 3DES, AES RC4-128, Integridade de mensagens SSL: MD5, SHA; e Assinatura avançada de IDP/IPS	NCD	Acelerado por *hardware* incorporado (IPsec + SSL)
VPN IPSec	Sim, com *Dead Peer Detection*	Sim, com *Dead Peer Detection*	Sim
Algoritmo de Autenticação da VPN	NCD	SHA1, MD5	NCD

Virtual *Private Network* PPTP (VPN)	Sim	Sim, com criptografia MPPE	Sim
Virtual *Private Network* LL2P (VPN)	Sim	Sim	Sim
Virtual *Private Network* GRE (VPN)	Sim	NCD	Sim

NCD - Não consta na documentação (Fonte: Próprio autor)

Todos os roteadores tem **criptografia da VPN IPSec**, descrição da criptografia de cada, roteador da D-Link: DES, 3DES, AES, *Twofish*, *Blowfish*, CAST-128, NULL; roteador da TP-Link: DES, 3DES, AES128, AES192, AES256; roteador da Cisco: não consta na documentação qual é a criptografia mas consta que é Acelerado por *hardware* incorporado(IPsec + SSL)**.**

VPN IPSec todos os roteadores tem, sendo que no roteador da D-Link e da TP-Link tem VPN IPSec com *Dead Peer Detection*.

Somente no roteador da TP-Link consta que o **algoritmo de autenticação da VPN** é SHA1, MD5.

Somente o roteador da TP-Link não consta na documentação que contém **VPN SSL**.

O roteador da D-Link e TP-Link consta na documentação a **criptografia da VPN**, no roteador da D-Link a descrição é a seguinte: SSL: DES, 3DES, AES RC4-128, Integridade de mensagens SSL: MD5, SHA; e Assinatura avançada de IDP/IPS, no roteador da TP-Link não consta na documentação e no na Cisco só fala que a criptografia é Acelerada por *hardware* incorporado (IPsec + SSL).

VPN PPTP e VPN LL2P os três roteadores possuem, sendo que no roteador da TP-Link está especificado que a VPN PPTP contém a criptografia MPPE, e **VPN GRE** só não consta na documentação do roteador da TP-Link.

3.2 ANÁLISE DE *ACCESS POINTS*

A Análise de *Access Points* trata-se da identificação de cada *Access Point* levantando todas as especificações de segurança e analisando se eles são ou não vulneráveis a cada tipo de ameaça.

Os *Access Points* utilizados no levantamento das informações foram: *Access Point AirPremier N DAP-2310* para D-Link; *Access Point Wireless N 300Mbps TL-WA901ND* para TP-Link e *Access Point Wireless-N* Cisco 300 MBPS com POE - WAP121-A-K9-NA para Cisco.

Tabela 4: Access Point - Tipos de ameaças

	D-Link	TP-Link	Cisco
Spoofing	V	V	V
Sniffing	NV, possui isolamento do cliente, autent. e cript.	V	NV, possui isolamento do cliente e cript.
Mapping	NV, possui isolamento do cliente, autent. e cript.	NV, possui autent. e cript.	NV, possui isolamento do cliente e cript.
Browser hijacking	NA	NA	NA
Trojan	NA	NA	NA
DoS e DDoS	V	V	V
Engenharia Social	NA	NA	NA

NA - Não Aplicável - **V –** Vulnerável - **NV -** Não Vulnerável (Fonte: Próprio autor)

Os três *Access Points* são vulneráveis a ***Spoofing***, **Dos** e **DDos**.

As ameaças de ***Browser Hijacking, Trojan*** e **Engenharia Social** não são Aplicáveis a *Access Points.*

Somente o A*ccess Point* da TP-Link é vulnerável a ***Sniffing****,* o A*ccess Points* da D-Link não é vulnerável por que possui isolamento do cliente, autenticação e criptografia, e o da Cisco não é por que possui isolamento do cliente e criptografia.

Os três A*ccess Points* não são vulneráveis a ***Mapping***, pois o A*ccess Points* da D-Link possui, isolamento de cliente, autenticação e criptografia, o da TP-Link possui autenticação e criptografia, e o da Cisco possui isolamento de cliente e criptografia.

Tabela 5: Access Point - Tipos de seguranças

	D-Link	TP-Link	Cisco
Segurança *wireless*	WEP 64/128/152-bit, WPA - *Personal*, WPA2 - *Enterprise*, WPA2 - *Personal*, Autenticação 802.1X RADIUS	WEP 64/128/152-bit / WPA / WPA2 (ambas *Personal* e *Enterprise*), WPA-PSK / WPA2-PSK, autenticação 802.1X RADIUS	WPA/WPA2/WEP (*Personal* e *Enterprise*), autenticação 802.1X RADIUS
QSS	NCD	Sim (Na forma de *hardware*, por botão)	Sim (Porém não há botão, configuração é feita via *software*)
Filtro de MAC	Sim	Sim	Sim
SSID *Broadcast Disable*	Sim	Sim	Sim
Segmentação de WLAN	Sim (até 8 SSID)	Sim (até 4 SSID)	Sim (até 4 SSID)
Gerenciamento do Equipamento	Via HTTP e HTTPS, SSH e *Telnet*	Via SNMP	Via HTTP e HTTPS
Detecção de pontos de acesso não autorizado	Sim	NCD	Sim
Mecanismo de isolamento do cliente sem fio	Sim	NCD	Sim
Lista de controle de acesso de gerenciamento (ACL)	NCD	NCD	Sim

NCD - Não consta na documentação (Fonte: Próprio autor)

A **segurança *wireless*** do *Access Point* da D-Link é a seguinte: WEP 64/128/152-bit, WPA - *Personal*, WPA2 - *Enterprise*, WPA2 - *Personal*, Autenticação 802.1X *RADIUS*, do TP-Link: WEP 64/128/152-bit / WPA / WPA2 (ambas *Personal* e *Enterprise*), WPA-PSK / PA2-PSK, autenticação 802.1X *RADIUS*, e do Cisco: WPA/WPA2/WEP (*Personal* e *Enterprise*), autenticação 802.1X *RADIUS*.

Somente o *Access Point* da D-Link não consta na documentação **QSS**, sendo que no *access point* da TP-Link possui na forma de *hardware* por botão, já no da Cisco não tem o botão, a configuração é feita via *software*.

Todos os *Access Points* possuem **Filtro de MAC** e **SSID *Broadcast Disable***, e segmentação de WLAN sendo que no da D-Link pode ter até 8 SSID e no da TP-Link e Cisco somente 4 SSID.

O **Gerenciamento** no *Access Point* da D-Link é feito via HTTP, HTTPS, SSH e Telnet, do *Access Point* da TP-Link é feito via SNMP e do A*ccess Point* da Cisco é via HTTP e HTTPS.

Somente o *Access Point* da D-Link e Cisco constam na documentação que possui **detecção de pontos de acesso não autorizado** e **mecanismo de isolamento do cliente sem fio**.

Somente o roteador Cisco conta que possui **Lista de controle de acesso de gerenciamento.**

3.3 ANÁLISE DE *SWITCHES*

A Análise de *Switches* trata-se da identificação de cada *Switch* levantando todos as especificações de segurança e analisando se eles são ou não vulneráveis a cada tipo de ameaça.

Os *Switches* utilizados no levantamento das informações foram: *Switch Web Smart* para D-Link; *Switch Gigabit* de Gerenciamento Básico L2 de 24 portas com 4 slots SFP *JetStream* - TL-SG5428 para TP-Link e *Switch* SLM224G 24 portas 10/100 + 2 portas *Gigabit* - *Switch* Inteligente: SFP para Cisco.

Tabela 6: *Switch* - Tipos de ameaças

	D-Link	TP-Link	Cisco
Spoofing	NV, devido a Proteção a ARP	NV, devido a Proteção a ARP	V
Sniffing	NV,possui cipt, *switch* não é vuln., Seg. em porta, Proteção a ARP	NV,possui cipt, *switch* não é vuln., Seg. em porta, Proteção a ARP	NV,possui cipt, *switch* não é vuln. Seg. em porta
Mapping	NV,possui cipt, Seg. em porta, Proteção a ARP	NV,possui cipt, Seg. em porta, Proteção a ARP	NV,possui cipt, Seg. em porta
Browser hijacking	NA	NA	NA
Trojan	NA	NA	NA
DoS e DDoS	V	NV	V
Engenharia Social	NA	NA	NA

NA - Não Aplicável - **V –** Vulnerável - **NV -** Não Vulnerável (Fonte: Próprio autor)

Somente o *Switch* da Cisco é vulnerável a ***Spoofing***, o *Switch* da D-Link e da TP-Link não é vulnerável pois possui proteção a ARP.

Nenhum dos *Switches* são vulneráveis a ***Sniffing***, pois o S*witch* da D-Link e da TP-Link possui criptografia, segurança em porta e proteção a ARP, agora o da Cisco possui criptografia e Segurança em porta.

Os três não são vulneráveis a ***Mapping*** por que o *switch* da D-Link e TP-Link possui criptografia, Segurança em porta e Proteção a ARP e o da Cisco por que possui criptografia e Segurança em porta.

As ameaças de ***Browser Hijacking*****,** ***Trojan*** e **Engenharia Social** não são aplicáveis a *switches*.

Somente o *Switch* da TP-Link não é vulnerável a **Dos** e **DDoS**.

Tabela 7: *Switch* - Tipos de seguranças

	D-Link	TP-Link	Cisco
Autenticação 802.1X	Sim, baseada em portas, rede autenticada através de servidores RADIUS externos e 400 entradas de vinculação de IP-MAC-Porta-VID	Sim, com servidores RADIUS, Criptografia: MD5/SHA1	Sim, Autenticação de portas RADIUS, Criptografia MD5
Segurança de Porta	Sim, Suporta até 64 endereços MAC por porta	Sim	Sim
Storm Control	Sim	Sim	Sim, *Broadcast and Multicast*
Rastreamento DHCP	Sim	Sim	NCD
Proteção a ARP	Sim, impede a rede de ser cortado ou escutado por *hackers* usando ARPs falsos	Sim, DAI (*Dynamic* ARP *Inspection*)	NCD
Proteção a DoS	NCD	Sim	NCD
***Access Control List* (ACL)**	Sim, ACL com base em Endereço MAC(Suporta 256 entradas MAC estáticos), Endereço IPv4 (ICMP / IGMP / TCP / UDP), VLAN ID, Prioridade 802.1p, DSCP. Suporta SSL v1/v2/v3, possui D-Link *Safeguard Engine*	Sim, restringem o acesso a recursos de rede sensíveis ao negar pacotes com base na fonte e destino do MAC, do endereço IP, das portas TCP / UDP e até mesmo da ID VLAN	NCD, consta somente que possui gerenciamento de controle de acesso e Filtragem baseada em MAC
VLAN	Sim, VLAN individual, esses recursos garantem a qualidade e segurança do tráfego VoIP	Sim, separada para convidados, aumentando o nível de segurança	Sim, também fornecer uma camada adicional de segurança, mantendo dados sensíveis separadas de outros grupos de trabalho na rede.
Configuração do Dispositivo	Gerenciamento por CLI (Interface via Linha de Comando), através de Telnet e Gerenciamento GUI baseada na *Web* HTTP	Sim, via Interface GUI (Interface *Web* Gráfica) e CLI (Interface via Linha de Comando), com criptografia SSL e SSH v1/v2, SSL v2/v3/TLSv1	Sim, Interface de usuário web embutido para configuração baseada em navegador fácil (HTTP) e configuração de *upload* e *backup* via HTTP ou TFTP

NCD - Não consta na documentação (Fonte: Próprio autor)

Todos os *Switches* possuem Autenticação 802.1X, sendo que as características da autenticação no *Switch* D-Link são: baseada em portas, rede autenticada através de servidores *RADIUS* externos e 400 entradas de vinculação de IP-MAC-Porta-VID, no *Switch* TP-Link são: com servidores *RADIUS*, Criptografia: MD5/SHA1 e no *Switch* da Cisco são: Autenticação de portas *RADIUS*, Criptografia MD5.

Todos possuem **segurança de porta** sendo que no D-Link suporta até 64 endereços MAC por porta.

Todos possuem ***Storm Control.*** Somente o *Switch* da D-Link e TP-Link consta na documentação que possui **rastreamento DHCP.**

O item de segurança **proteção a ARP** contêm no *switch* da D-Link com a seguinte descrição: impede a rede de ser cortado ou escutado por *hackers* usando ARPs falsos, possui também no *Switch* da TP-Link com a seguinte descrição: DAI, e no S*witch* da Cisco não consta na documentação.

A **proteção contra DoS** só consta na documentação do *switch* TP-Link.

O S*witch* da D-Link possui **ACL** com base em Endereço MAC(Suporta 256 entradas MAC estáticos), Endereço IPv4 (ICMP / IGMP / TCP / UDP), VLAN ID, Prioridade 802.1p, DSCP. Suporta SSL v1/v2/v3, possui D-Link *Safeguard Engine*, o *switch* da TP-Link também possui ACL que restringem o acesso a recursos de rede sensíveis ao negar pacotes com base na fonte e destino do MAC, do endereço IP, das portas TCP / UDP e até mesmo da ID VLAN, agora o *switch* da Cisco conta na documentação que somente que possui gerenciamento de controle de acesso e Filtragem baseada em MAC**.**

O *switch* da D-Link possui **VLAN individual**, esses recursos garantem a qualidade e segurança do tráfego VoIP, *switch* da TP-Link também possuem VLAN separada para convidados, aumentando o nível de segurança, e o *switch* da Cisco possui VLAN que também fornece uma camada adicional de segurança, mantendo dados sensíveis separadas de outros grupos de trabalho na rede.

Agora a **Configuração** do *switch* da D-Link é pela interface CLI, através de Telnet e GUI baseada na Web HTTP, do *switch* da TP-Link é feita via Interface GUI e CLI, com criptografia SSL e SSH v1/v2, SSL v2/v3/TLSv1, e a do *switch* Cisco é feita por Interface de usuário *web* embutido para configuração baseada em navegador fácil (HTTP) e configuração de *upload* e *backup* via HTTP ou TFTP.

4. CONCLUSÃO

Esta monografia trouxe conhecimentos sobre a segurança de redes, segurança da informação com as seguintes técnicas: Criptografia, Autenticação, Controle de Acesso, Controle de roteamento, Integridade de dados, e *Firewall*, equipamentos de conectividade tais como *Hub*, *Switch*, Roteador, Modem e *Access Point* e foram citadas as seguintes ameaças: *Spoofing, Sniffing, Mapping, Hijacking, Trojan, Denial-of-Service, Distributed Denial-of-Service* e Engenharia Social.

Foram feitas comparações de equipamentos de conectividade, contendo três produtos de marcas distintas. Para cada equipamento, primeiramente levantando todas as características de segurança de cada um deles, após isso foram confrontados em uma tabela os três produtos para cada equipamento, utilizando como critério as ameaças pesquisadas nesta monografia, para verificar qual equipamento é vulnerável e qual equipamento não é vulnerável a tais ameaças.

Para os **Roteadores**, foram escolhidos modelos corporativos com alto nível de segurança e com vários recursos disponíveis, devido a este motivo os modelos não são vulneráveis a grande parte das ameaças. Pois bem, o roteador da TP-Link e Cisco ficaram empatados como os mais seguros e o roteador da D-Link ficou na última colocação.

Dentre os ***Switches*** escolhidos para serem analisados, o que possui maior segurança contra as ameaças é o da TP-Link que não é vulnerável a nenhuma das ameaças analisadas, sendo que o da Cisco ficou em ultimo e o da D-Link ficou na segunda posição.

Foram escolhidos ***Access Points*** de uso intermediário, ideal para ambiente domestico e para pequenas empresas. Na análise dos três *access points* houve empate, o da D-Link e Cisco são os que são menos vulneráveis às ameaças, o da TP-Link ficou na ultima colocação.

A partir de todas as informações contidas nesta monografia, abre-se um leque de opções para dar continuidade nos estudos apresentados aqui; uma delas é aplicar

de maneira prática as ameaças apresentadas nos equipamentos de conectividade, estudar e confrontar os resultados de análise teóricas a implementação prática.

REFERÊNCIAS BIBLIOGRÁFICAS

AMBROSI, Airison. **Protótipo de software para atualização automática de versão de arquivos** Disponível em <http://campeche.inf.furb.br/tccs/2004-II/2004-2airisonambrosivf.pdf>. Acessado em 08 jun. 2014.

AMOROSO, Danilo, **O que é autenticação?.** Disponível em <http://www.tecmundo.com.br/seguranca/1971-o-que-e-autenticacao-.htm>. Acessado em 27 fev. 2014.

CARNEIRO, Leonardo Ferreira e JÚNIOR , Nilton Alves. **Roteadores e Segurança em Redes**. Disponível em <http://www.rederio.br/downloads/pdf/roteador.pdf>. Acessado em 09 jun. 2014.

BRADLEY, Mitchell, **Access point, wireless**. Disponível em <http://compnetworking.about.com/cs/wireless/g/bldef_ap.htm>. Acessado em 25 fev. 2014.

BRITO, Edivaldo, **Entenda a diferença entre *Hub*, s*witch*, roteador e modem.** Disponível em <http://www.techtudo.com.br/artigos/noticia/2013/05/entenda-diferenca-entre-*Hub*-switch-roteador-e-modem.html>. Acessado em 20 fev. 2014.

DELGADO, Pablo. **El punto flaco de internet, los ataques DoS.** Disponível em <http://todobytes.es/2011/08/el-punto-flaco-de-internet-los-ataques-dos/>. Acessado em 08 jun 2014.

ETHICAL HACKING, **DNS Spoofing** - Ettercap Backtrack5 Tutorial. Disponível em <http://www.ehacking.net/2011/08/dns-spoofing-ettercap-backtrack5.html>. Acessado em 08 jun. 2014.

HYPHENET. **Experian Spam Used to Spread Data-Stealing Trojan**. Disponível em <http://www.hyphenet.com/blog/experian-spam-trojan/>. Acessado em 08 jun. 2014.

JASCONE, Fábio Luis Tavares. **Protótipo de software para ocultar texto criptografado em imagens digitais.** Disponível em <http://www.bc.furb.br/docs/MO/2003/278719_1_1.pdf>. Acessado em 10 mar. 2014.

JOHN V. **Managed File Transfer and Network Solutions**. Disponível em <http://www.jscape.com/blog/bid/91906/Countering-Packet-Sniffers-Using-Encrypted-FTP>. Acessado em 08 jun. 2014.

MENEZES, Fernando Melo. **Segurança via internet na transmissão de arquivos comerciais.** Disponível em <http://www.computacao.unitri.edu.br/downloads /monografia/63411129383910.pdf>. Acessado em 12 mar. 2014.

MICROSOFT. **Controle de acesso** Disponível em <http://technet.microsoft.com/pt-br/library/cc732699(v=ws.10).aspx>. Acessado em 28 fev. 2014.

MIURA, Alex. **PARA QUE SERVE UM ACCESS POINT?** Disponível em <http://aprendiz-info.blogspot.com.br/2012/07/pra-que-serve-um-access-point.html>. Acessado em 08 jun. 2014.

MORIMOTO, Carlos E. **Como compartilhar a conexão usando uma única placa de rede.** Disponível em <http://www.hardware.com.br/artigos/compartilhar-placa/>. Acessado em 08 jun. 2014.

ORTEGA , André. ***Hub* x *Switch*:** Como funcionam. Disponível em <http://www.brainwork.com.br/2010/08/19/*Hub*-x-switch-como-funcionam/>. Acessado em 08 jun. 2014.

PEREIRA, Ana Paula. **O que é Trojan?** Disponível em <http://www.tecmundo.com.br/seguranca/196-o-que-e-um-trojan-.htm >. Acessado em 18 mar. 2014.

PINZO, Alexandre. **Vulnerabilidade da segurança em rede sem fio.** Trabalho monográfico de graduação. Centro universitário ritter dos reis, 2009.Disponível em <http://www.uniritter.edu.br/graduacao/informatica/sistemas/downloads/tcc2k9/TCCII_2009_1_Alexandre.pdf> Acessado em 25 set. 2013.

PISA, Pedro, **O que é criptografia ?.** Disponível em <http://www.techtudo.com.br/artigos/noticia/2012/06/o-que-e-criptografia.html>. Acessado em 27 fev. 2014.

PROFESSIONAL COMPUTER SERVICES. **Network Management**. Disponível em <http://www.fjpcs.com.au/network-management>. Acessado em 08 jun. 2014.

RAMIRO, Marcelo Lepsch. **Gestão da segurança da informação:** certificação digital. Dissertação de Mestrado**.** Escola brasileira de administração de empresas, 2008**.** Disponível em <http://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/4069/ACF286.pdf?sequence=1>. Acessado em 22 fev. 2014.

REDES PRÁTICAS, **O.D.R**. - On Demand Routing. Disponível em <http://www.redespracticas.com/enrutamiento/odr/cdp/cisco/comandos/ios/?pag=txtEnrutamientoODRcsco.php&Njs=t#top>. Acessado em 08 jun. 2014.

REESE, Arthur. **REVERSING RORPIAN** – DHCP Hijacking Malware. Disponível em <http://resources.infosecinstitute.com/reversing-rorpian/>. Acessado em 08 jun. 2014.

ROUSE, Margaret. ***Hijacking.*** Disponível em <http://searchsecurity.techtarget.com/definition/hijacking>. Acessado em 17 mar. 2014.

SENAC . **PSI** – Política de Segurança da Informação - Documento de Diretrizes e Normas Administrativas. Disponível em <http://www.sp.senac.br/normasadministrativas/psi_normas_administrativas.pdf>. Acessado em 19 fev. 2014.

SKYPE. **O que é engenharia social?** Disponível em <https://support.skype.com/pt/faq/FA10921/o-que-e-engenharia-social>. Acessado em 19 mar. 2014.

SOUZA, Ricardo José Cabeça. **Segurança de Redes de Computadores.** Disponível em < http://ricardojcsouza.com.br/download/Seguranca_Redes_2.pdf >. Acessado em 12 mar. 2014.

TANENBAUM, Andrew S. **Rede de computadores**. 4.ed. Rio de Janeiro, Elsevier, 2003.

TI – REDES, **NAT** - Configurando NAT por portas em roteadores Cisco (PAT). Disponível em <http://www.ti-redes.com/roteamento/nat/nat-configurando-nat-por-portas-em-roteadores-cisco/>. Acessado 08 jun. 2014.