UNIVERSIDADE ESTADUAL DO MARANHÃO

CENTRO DE CIÊNCIAS TECNOLÓGICAS

CURSO DE ENGENHARIA DE COMPUTAÇÃO

CARLOS ADRIANO SANTANA SILVA

ANÁLISE DE VULNERABILIDADES EM REDES WIRELESS: PROPOSTA DE SOLUÇÕES PARA ATAQUES DO TIPO MITM (*MAN-IN-THE-MIDDLE*)

SÃO LUIS

2019

CARLOS ADRIANO SANTANA SILVA

ANÁLISE DE VULNERABILIDADES EM REDES WIRELESS: PROPOSTA DE SOLUÇÕES PARA ATAQUES DO TIPO MITM (*MAN-IN-THE-MIDDLE*)

Trabalho de conclusão de curso apresentado ao curso de Engenharia de Computação, da Universidade Estadual do Maranhão, como registro para obtenção do grau de Bacharel em Engenharia de Computação.

Orientador: Prof. Dr. Reinaldo de Jesus da Silva

SÃO LUIS

2019

CARLOS ADRIANO SANTANA SILVA

ANÁLISE DE VULNERABILIDADES EM REDES WIRELESS: PROPOSTA DE SOLUÇÕES PARA ATAQUES DO TIPO MITM (*MAN-IN-THE-MIDDLE*)

Aprovada em: / /

BANCA EXAMINADORA

_____

Prof. Dr. Reinaldo de Jesus da Silva

Orientador

_____

Prof. MSc. Diógenes Carvalho Aquino

Primeiro membro

_____

Prof. Esp. Rafael Martins da Cruz

Segundo Membro

DEDICATÓRIA

À Deus e a minha família.

AGRADECIMENTOS

Primeiramente, quero agradecer ao Deus Todo-Poderoso.

A minha mãe, Ana Cristina, meu pai, Jorge Carlos, minha avó, Raimunda, e a todos os meus familiares por toda educação, incentivo e apoio emocional.

Ao meu orientador Prof. Dr. Reinaldo de Jesus pelos seus ensinamentos e orientações.

A Cinara Siqueira, por seu constante incentivo e apoio emocional.

A Daniel Gusmão, que, sem medir esforços, várias vezes me ajudou.

A Júlio Cesar, Danilo Dias, Douglas Costa, Cledilson, Kleyton, Hidalgo, Viegas e a todos os meus amigos que direta e indiretamente me ajudaram no desenvolvimento deste trabalho.

A todos os professores e colegas de curso da Universidade Estadual do Maranhão, que contribuíram e foram importantes na minha formação acadêmica.

E, por fim, a todos aqueles que, de alguma forma, contribuíram para a elaboração deste trabalho.

Não sabendo que era impossível, ele foi lá e fez.
(Jean Cocteau)

RESUMO

O uso das redes de computadores sem fio (wireless) vem crescendo com o passar dos anos e garante maior mobilidade e facilidade de acesso a milhares de usuários ao redor do mundo. Porém, as formas de ataques às falhas e vulnerabilidades encontradas nas redes wireless vêm aumentando significativamente. A técnica de ataque do tipo Man-in-the-middle (Homem no meio) é uma das técnicas mais poderosas e eficientes, no que tange o roubo de informações confidenciais trafegadas em redes sem fio. Este trabalho lista e analisa as principais técnicas de ataques do tipo Man-in-the-middle voltadas a redes de computadores sem fio. Por fim, como resultado desta pesquisa, são relacionadas propostas de soluções para garantir a segurança de redes contra os ataques do tipo Man-in-the-middle.

Palavras-chave: Redes sem fio, Man-in-the-middle, Segurança de redes

ABSTRACT

The use of wireless computer networks has been growing with greater mobility and ease of access to thousands of users around the world. However, the forms of attacks against the flaws and vulnerabilities found in the wireless networks have been increasing significantly. The Man-in-the-middle attack technique is one of the most powerful and efficient techniques in the theft of confidential information over wireless networks. This paper lists and discusses the main techniques of Man-in-the-middle attacks targeting wireless computer networks. Finally, as a result of this research, proposals for solutions to guarantee network security against Man-in-the-middle attacks are related.

Keywords: Wireless networks, Man-in-the-middle, Network security

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ARP	Address Resolution Protocol
ARPA	Advanced Research Projects Agency
DNS	Domain Name Service
DNSSEC	Domain Name System Security Extensions
DoS	Denial of Service
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
ID	Identificador
IEEE	Instituto de Engenheiros Eletricistas e Eletrônicos
IP	Internet Protocol
LAN	Local Area Network
MAC	Media Access Control
MAN	Metropolitan Area Network
NFS	Network File System
RARP	Reverse Address Resolution Protocol
SMTP	Simple Network Management Protocol
SMTPS	Simple Mail Transfer Protocol Secure
SSL	Secure Socket Layers
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
USB	Universal Serial Bus
VPN	Virtual Private Network

WAN	Wide Area Network
WEP	Wired Equivalency Privacy
WPA	Wi-Fi Protected Access

Sumário

1. INTRODUÇÃO

É perceptível o crescente avanço dos dispositivos relacionados a tecnologia da informação, assim como também das redes responsáveis pela interconexão destes dispositivos. Devido ao grande número de pessoas que passaram a utilizar a rede mundial de computadores, e também por conta da crescente popularidade dos dispositivos móveis, percebeu-se a necessidade do surgimento de uma rede de computadores capaz de garantir facilidade de acesso e mobilidade aos usuários da rede. Por conta disto, surgiram as redes sem fio (wireless). A rede sem fio tornou-se a tecnologia de rede mais utilizada no mundo e está presente em praticamente todos os ambientes, sejam públicos ou privados.

Exponencialmente ao crescente avanço das redes de computadores, cresce a quantidade de formas de ataques a estas redes, cujo o objetivo é, entre outros, acessar indevidamente informações alheias, inviabilizar a comunicação de dados ou até mesmo interceptar e alterar informações trafegadas na rede. Apesar disto, em contrapartida está a segurança de rede. De acordo com Vasconcellos (2013), os problemas referentes a segurança em redes de computadores dar-se-á principalmente pelo despreparo dos administradores e usuários das próprias redes. Um exemplo é que grande parte dos ataques logram êxito por conta de simples problemas de configuração em dispositivos de redes, como acontece nos roteadores, onde a maioria dos usuários mantém as senhas padrões pré-configuradas pelos fabricantes.

Existem diversas formas de ataques às falhas e vulnerabilidades de redes wireless, como os ataques de engenharia social, ataques de força bruta, ataques DoS e ataques *Man-in-the-middle* (Homem no meio). Segundo Moreno (2015), os ataques *Man-in-the-middle* são um dos tipos de ataques mais poderosos da atualidade e tem como objetivo interceptar todo o tráfego de dados em uma comunicação entre dispositivos em redes wireless.

Assim, por conta desta problemática referente às falhas e vulnerabilidades em redes wireless, pretende-se neste trabalho analisar as principais técnicas relacionadas a ataques *Man-in-the-middle* e, além disso, propor soluções para garantir proteção contra cada um destes ataques.

1.1 Objetivos

O objetivo geral e os objetivos específicos serão descritos a seguir.

1.1.1 Objetivo Geral

Analisar as principais falhas e vulnerabilidades e propor soluções contra os ataques do tipo MITM (*Man-in-the-middle*) em redes wireless.

1.1.2 Objetivos Específicos

- Realizar uma revisão bibliográfica acerca dos assuntos relacionados ao trabalho;
- Verificar e analisar as principais técnicas de invasão do tipo *Man-in-the-middle* em redes wireless;
- Propor soluções contra os ataques de invasão do tipo *Man-in-the-middle* em redes wireless.

1.1.3 Apresentação do Trabalho

Este trabalho está dividido em 6 capítulos dispostos da seguinte maneira:

- O capítulo 2 apresenta o referencial teórico acerca dos temas relacionados a esta pesquisa;
- No capítulo 3 são apresentados os trabalhos relacionados ao tema desta pesquisa;
- O capítulo 4 apresenta de forma detalhada cada uma das principais técnicas do tipo Man-in-the-middle;
- O capítulo 5 mostra as propostas de soluções contra os ataques do tipo Man-in-the-middle;
- Por fim, no capítulo 6, serão apresentadas as conclusões e trabalhos futuros desta pesquisa.

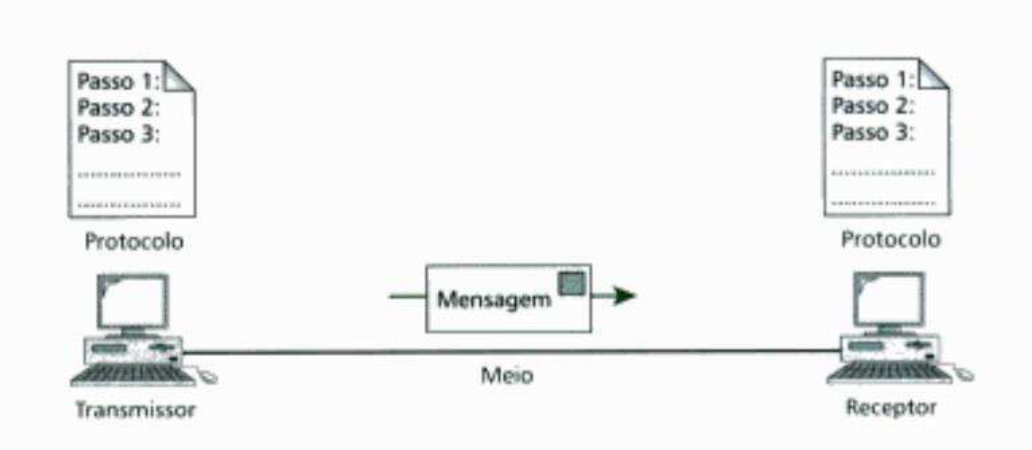
2 REFERENCIAL TEÓRICO

2.1 Comunicação de Dados

De acordo com Forouzan (2006), a comunicação de dados acontece basicamente quando dois ou mais dispositivos trocam informações através de um meio de comunicação. Um sistema de comunicação de dados deve possuir os seguintes elementos:

- Mensagem: são os dados a serem transmitidos.
- Transmissor: é todo dispositivo que transmite a mensagem.
- Receptor: é todo dispositivo que recebe a mensagem.
- Meio de transmissão: é o caminho por onde a mensagem percorre.
- Protocolo: são as regras que regem a comunicação de dados.

Figura 1: Elementos da comunicação de dados



Fonte: Forouzan (2006)

2.2 Redes de Computadores

Uma rede de computadores é um conjunto de dispositivos interconectados através de um meio de comunicação. Dois ou mais dispositivos estão interconectados quando podem realizar uma comunicação de dados (TANENBAUM, 2003).

De acordo com Forouzan (2006), as redes de computadores podem ser basicamente divididas em três:

- Redes locais (LAN): são redes cujo tamanho pode ser delimitado em poucos quilômetros. As redes locais são formadas basicamente por dispositivos interconectados dentro de uma casa, edifícios, escritórios etc.
- Redes Metropolitanas (MAN): são redes cujo tamanho se estendem por toda uma cidade. As redes de TV a cabo ou as redes de telefonia pública são grandes exemplos de redes metropolitanas.
- Redes Geograficamente Distribuídas (WAN): são redes cujo tamanho podem se estender a grandes distâncias geográficas compreendendo um ou mais países ou até mesmo o mundo inteiro.

2.3 Internet

A Internet é basicamente um conjunto de redes de computadores interligando milhares de dispositivos no mundo inteiro. A Internet é formada por milhares de LANs e WANs interconectadas. A internet teve origem na década de 60 quando o *Advanced Research Projects Agency* (ARPA) criou a ARPANET, uma rede de computadores capaz de compartilhar pesquisas e informações através de dispositivos localizados em diferentes regiões (FOROUZAN, 2006).

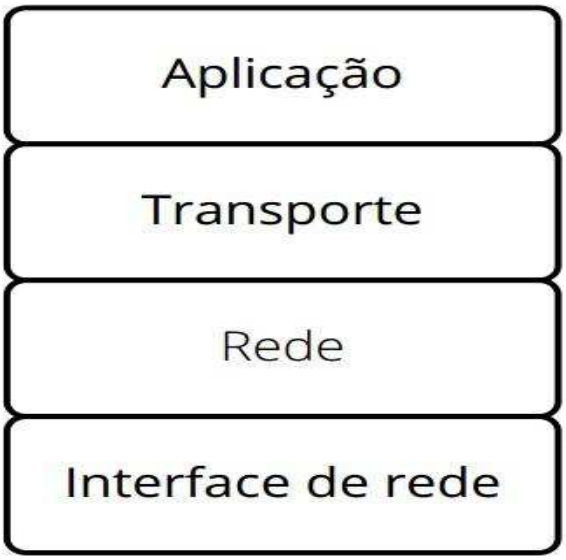
Segundo Tanenbaum (2003), os protocolos da ARPANET não eram capazes de garantir a comunicação entre diversas redes. Por conta disto, fora idealizado e desenvolvido o modelo e protocolo TCP/IP. Por conta da sua popularização e ampliação, muitas novas redes estavam sendo conectadas à ARPANET e o protocolo TCP/IP garantia a comunicação entre redes de computadores em suas mais diversas variações no que tange seu tamanho, computadores, topologias etc. O número de redes, computadores e usuários cresceu exponencialmente com o passar dos anos. Por volta dos anos 80, os usuários passaram a chamar este grande aglomerado de redes de computadores de inter-rede e, por fim, passaram a chamar de Internet.

2.4 Protocolo TCP/IP

Segundo Forouzan (2006), o protocolo que rege os processos de comunicação de dados na Internet é o TCP/IP. Os idealizadores e desenvolvedores do protocolo TCP/IP identificaram quais as funções de redes possuíam correlação e as agrupou em camadas.

De acordo com Elias e Lobato (2013), o protocolo TCP/IP é constituído por quatro camadas: Aplicação, Transporte, Rede e Interface de Rede.

Figura 2: Camadas do protocolo TCP/IP



Fonte: Elias e Lobato (2013)

2.4.1 Camada de aplicação

As aplicações são o cerne das redes de computadores. As redes de computadores existem para que aplicações em diferentes dispositivos consigam se comunicar. Desde a década de 70, centenas de aplicações foram desenvolvidas, desde aplicações clássicas de texto, como também aplicações de transferência de arquivos, bate-papo, compartilhamento de arquivos, aplicações de áudio e vídeo e até mesmo a mundialmente conhecida *Word Wide Web* (Kurose, 2010).

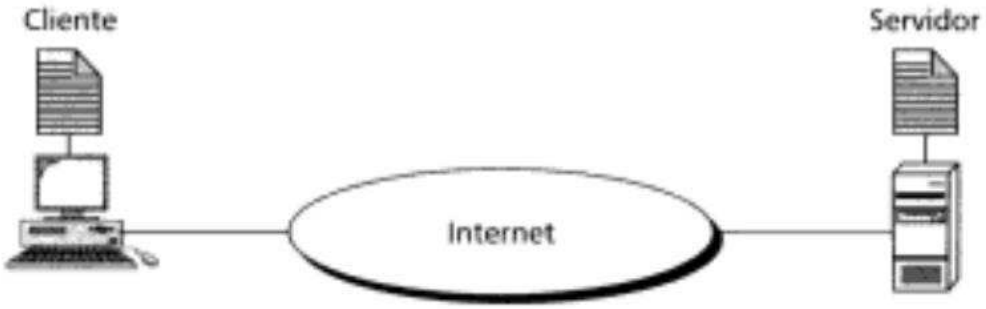
De acordo com Filippetti (2008), os protocolos imprescindíveis para que a comunicação entre as aplicações de rede seja efetivamente realizada são definidos pela camada de aplicação. A camada de aplicação é responsável por disponibilizar interfaces ao usuário final. Alguns dos protocolos comumente utilizados na camada de aplicação são:

- DNS (Domain Name Service)
- SMTP (Simple Network Management Protocol)
- FTP (File Transfer Protocol)
- Telnet
- NFS (Network File System)

- HTTP (Hypertext Transfer Protocol)

A finalidade de uma rede de computadores é oferecer serviços para os usuários através das aplicações. As aplicações de rede baseiam-se na arquitetura cliente-servidor. Um clássico exemplo é quando um usuário utilizando um computador deseja fazer o *download* de um arquivo em outro computador. Para que isso aconteça, o computador (*cliente)* deve possuir uma aplicação para solicitar o serviço desejado e o outro computador (*servidor)* deve possuir uma aplicação para entregar o serviço solicitado. Ambas as aplicações devem ser capazes de comunicarem entre si. Todo dispositivo conectado à rede de computadores, seja ele *cliente* ou *servidor*, possui um endereço. O endereço de um dispositivo conectado em uma rede de computadores é chamado de IP (Internet Protocol). Um computador *cliente* deve possuir o endereço IP do computador *servidor* ao solicitar um serviço (FOROUZAN, 2006).

Figura 3: Arquitetura Cliente-Servidor



Fonte: Forouzan (2006)

2.4.1.1 Protocolo DNS

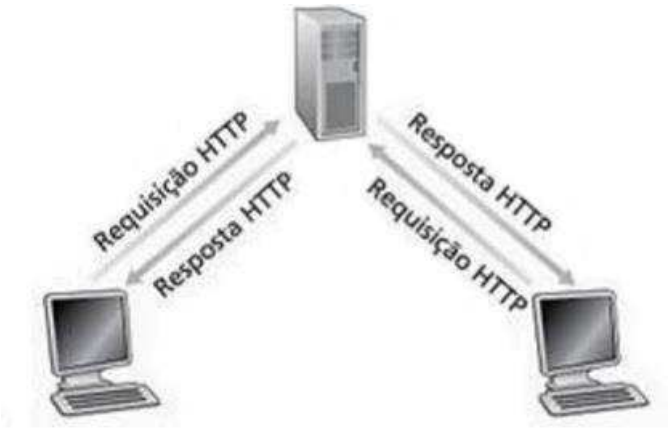
Sabe-se que a comunicação de dados entre diferentes aplicações na rede de computadores ocorre apenas se os dispositivos conectados à rede possuem endereçamento IP. Existem incontáveis aplicações conectadas nas redes de computadores ao redor do mundo tornando bem difícil memorizar os endereços IPs dos dispositivos onde se encontra cada uma delas. Por conta disso fora introduzido a possibilidade de uma aplicação se conectar a outra através do uso de nomes como, por exemplo, carlos@adriano.com. Nota-se que é bem mais fácil memorizar

endereços nominais do que endereços IPs como, por exemplo, 121.134.192.4. Entretanto, uma rede de computadores reconhece apenas endereços IPs. Por conta disso é imprescindível a existência de um protocolo capaz de traduzir os endereços nominais em endereços IPs. O protocolo utilizado para este fim é o protocolo DNS (TANENBAUM, 2003).

2.4.1.2 Protocolo HTTP

A mundialmente conhecida Word Wide Web, e talvez a mais importante aplicação já desenvolvida, surgiu na década de 90. A web, diferentemente do rádio e da televisão, funciona por demanda. Ou seja, usuários tem a sua disposição aquilo que desejam acessar, assistir, ouvir, ler etc. O HTTP é o protocolo da camada de aplicação que rege a comunicação de dados na Web. Dois dispositivos, *cliente* e *servidor*, comunicam-se através de mensagens HTTP. O protocolo HTTP determina como é realizada a requisição de um *cliente* a um *servidor* e como o *servidor* responde a está requisição (Kurose, 2010).

Figura 4: Protocolo HTTP



Fonte: Kurose (2010)

2.4.2 Camada de Transporte

Uma das principais problemáticas encontradas durante a comunicação de dados entre dispositivos conectados à rede de computadores é a de garantir confiabilidade na entrega dos dados em meios de comunicação não confiáveis (Kurose, 2010).

Segundo Tanenbaum (2003), os protocolos da camada de transporte têm como principal objetivo garantir confiabilidade, eficiência e economia na troca de dados durante a comunicação em redes de computadores, independente dos meios de comunicação utilizados, sejam eles confiáveis ou não.

A camada de transporte tem a função de mascarar a complexidade da rede para a camada de aplicação e seus usuários finais. Existem dois protocolos na camada de transporte: os protocolos TCP (Transmission Control Protocol) e UDP (User Datagram Protocol).

2.4.2.1 Protocolo TCP

O protocolo TCP funciona basicamente da seguinte forma: Antes da comunicação de dados entre aplicações em um dispositivo transmissor e um dispositivo receptor iniciar, o protocolo TCP do transmissor comunica-se com o protocolo TCP do receptor afim de estabelecer uma conexão virtual. Esse tipo de comunicação é comumente chamado de orientada à conexão. O protocolo TCP do transmissor recebe da aplicação a mensagem a ser transmitida e a divide em segmentos que por sua vez são numerados e sequenciados. Dessa forma o protocolo TCP do receptor é capaz de remontar a mensagem através dos segmentos recebidos. Após a transmissão dos segmentos, o transmissor espera pela confirmação do dispositivo receptor, e retransmite os segmentos que não foram recebidos. Por conta disto o protocolo TCP garante que toda a mensagem será transmitida, garantindo confiabilidade na entrega da mensagem mesmo que os meios de comunicações não sejam totalmente confiáveis (FILIPPETTI, 2008).

2.4.2.2 Protocolo UDP

Da mesma forma que acontece no protocolo TCP, o protocolo UDP recebe da aplicação a mensagem a ser transmitida e a divide em segmentos. Em seguida, diferentemente do protocolo TCP, o UDP apenas enumera os segmentos e os encaminha ao receptor que por sua vez recebe os segmentos e remonta a mensagem, porém não envia nenhum tipo de confirmação ao transmissor. Por conta disto, o protocolo UDP, diferentemente do protocolo TCP, é considerado não-orientado a conexão e um protocolo não-confiável. Por não criar uma conexão virtual e não requerer confirmação de recebimento pelo receptor, a comunicação de dados utilizando o protocolo UDP consome menos largura de banda e transmite a

mensagem com mais rapidez, sendo assim o protocolo mais econômico da camada de transporte (FILIPPETTI, 2008).

2.4.3 Camada de Rede

Geralmente, dispositivos comunicando-se entre si na Internet encontram-se separados por uma infinidade de redes de computadores. A camada de rede tem como principal função realizar o *internetworking* que, por sua vez, é a interconexão lógica dessas redes. O *internetworking* garante para as camadas de transporte e aplicação que a interconexão lógica das mais diversas redes conectadas na Internet hajam como uma única rede. Outra importante função da camada de rede é o roteamento que, por sua vez, tem a função de definir a melhor rota por onde os pacotes de dados devem percorrer durante a comunicação entre dispositivos na Internet. Basicamente a camada de redes possui quatro protocolos: IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol) e RARP (Reverse Address Resolution Protocol) (FOROUZAN, 2006).

2.4.3.1 Protocolo IP

Sabe-se que todo dispositivo conectado na Internet possui endereçamento IP. O responsável por endereçar cada um desses dispositivos é o protocolo IP. Além disso o protocolo IP também é responsável pelo roteamento. Durante a troca de informações entre dispositivos na Internet, o protocolo IP analisa os IPs dos dispositivos envolvidos e seleciona a melhor rota por onde as informações serão transmitidas (FILIPPETTI, 2008).

2.4.3.2 Protocolo ARP

Todo computador, esteja ele conectado à Internet ou não, possui um endereço MAC. O endereço MAC é basicamente o endereço físico de dispositivos que podem se conectar em redes de computadores. O protocolo de resolução de endereços, conhecido como protocolo ARP, é responsável por identificar o endereço MAC de um determinado dispositivo através de seu respectivo endereço IP. Basicamente, o protocolo ARP realiza o mapeamento do endereço lógico (IP) dos dispositivos para o seu endereço físico (MAC) (FILIPPETTI, 2008).

2.4.4 Camada de Interface de Rede

A camada de interface de rede é responsável por definir os protocolos de acesso ao meio como, por exemplo, Ethernet, Token Ring etc. É também responsável por definir as topologias de rede e os padrões de sinalização elétrica como, por exemplo, o padrão IEEE 802.3 em casos de rede cabeada ou o padrão IEEE 802.11 em casos de rede sem fio (Wireless) (FILIPPETTI, 2008).

2.4.4.1 Padrão IEEE 802.11

É perceptível que, atualmente, as redes wireless tornaram-se uma das mais importantes tecnologias de acesso à rede mundial de computadores: a Internet. No início da década de 90 surgiram dezenas de tecnologias e padrões de redes wireless. Porém, apenas um dos padrões se destacou e tornou-se o padrão mundialmente utilizado em redes wireless nos dias atuais: o padrão IEEE 802.11, comumente conhecida como Wi-Fi (Kurose, 2010).

2.5 Segurança de rede

Digamos que dois usuários A e B desejam se comunicar em uma rede de computadores. É fato que o usuário A deseja que apenas o usuário B receba e entenda a mensagem a ser transmitida, mesmo que ambos estejam em uma rede não confiável, onde existem usuários que podem interceptar qualquer mensagem. Ambos os usuários também querem que a mensagem chegue ao destino sem alterações. Neste caso, de acordo com Moreno (2015), a comunicação segura dar-se-á através de algumas propriedades:

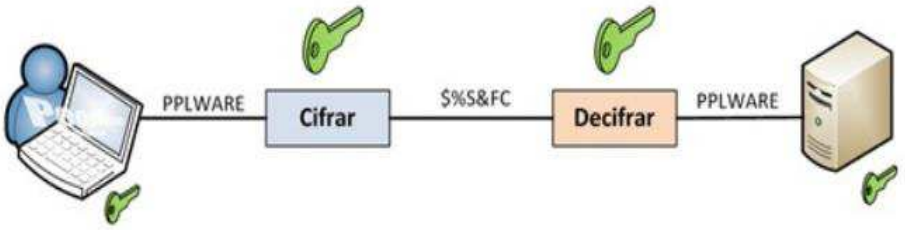
- Confidencialidade: Apenas os usuários participantes da comunicação devem entender o conteúdo da mensagem transmitida.
- Integridade: A mensagem deve ser transmitida sem sofrer alterações.
- Disponibilidade: Os usuários devem ser capazes de manter a comunicação a todo instante.
- Autenticidade: Garante que a mensagem está sendo transmitida por uma fonte segura e legítima, e não foi alterada por usuários intrusos.

2.5.1 Criptografia

A criptografia é o cerne da segurança em redes de computadores. O principal objetivo da criptografia é tornar a mensagem transmitida em redes de computadores incompreensível a possíveis intrusos. O processo de criptografia funciona da seguinte forma: A mensagem original tem seus dados substituídos por outros dados tornando a mensagem totalmente incompreensível (cifragem). Para realizar o processo inverso da criptografia (decifragem) e tornar a mensagem compreensível é necessário a utilização de uma chave de acesso. De acordo com Munhoz (2011 apud CRUZ, 2014), existem dois tipos de métodos criptográficos básicos:

- Criptografia simétrica: utiliza a mesma chave para realizar a cifragem e decifragem dos dados. Ou seja, tanto o transmissor quanto o receptor possuem a mesma chave criptográfica.

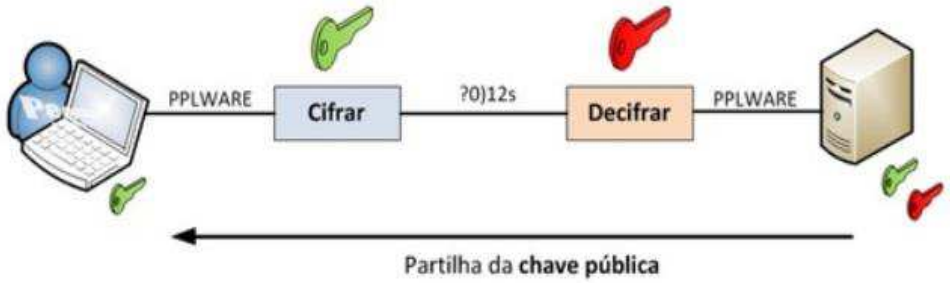
Figura 5: Criptografia Simétrica



Fonte: Pinto (2010)

- Criptografia assimétrica (criptografia de chave pública): Utiliza um par de chaves distintas: chave privada e chave pública. A chave pública é utilizada para realizar a cifragem dos dados, enquanto a chave privada é utilizada para realizar a decifragem dos dados.

Figura 6: Criptografia Assimétrica



Fonte: Pinto (2010)

No que tange a segurança de redes wireless, destacam-se dois protocolos voltados a criptografia: os protocolos WEP (Wired Equivalency Privacy) e WPA (Wi-Fi Protected Access).

2.5.1.1 Protocolo WEP

O WEP é um protocolo de criptografia oferecido pelo padrão IEEE 802.11 para solucionar problemas de segurança em redes wireless. O objetivo central do protocolo WEP era garantir às redes wireless o mesmo grau de segurança existente em redes cabeadas. Todavia, o protocolo WEP não conseguiu lograr êxito neste objetivo. Pois, o protocolo WEP utiliza o método criptográfico de chave simétrica. Ou seja, usuários realizando comunicação de dados em redes de computadores possuem a mesma chave criptográfica para cifrar e decifrar os dados transmitidos. Por conta disto, por mais segura que seja a distribuição destas chaves, muitos usuários, principalmente em redes bem extensas, terão acesso às chaves. Caso a segurança de apenas um desses componentes da rede seja violada, e um possível intruso tenha acesso a chave criptográfica, toda a rede será comprometida (RUFINO, 2005 apud FERREIRA, 2013).

2.5.1.3 Protocolo WPA

O protocolo WPA foi desenvolvido para suprir os problemas encontrados no protocolo WEP. Uma das principais melhorias encontradas no WPA é em relação a autenticação dos usuários. Diferentemente do WEP, o WPA distribui diferentes chaves para cada usuário da rede e ainda torna possível a implementação de uma infraestrutura de chaves públicas. A comunicação de dados, utilizando o WPA, funciona através de sessões. Ou seja, após os usuários autenticarem-se na rede,

uma chave mestra de criptografia é gerada e uma sessão de comunicação é iniciada. A transmissão de dados ocorre utilizando esta mesma chave até que a sessão seja encerrada (OLIVEIRA, 2010).

2.5.2 Pentest

O Pentest (testes de penetração ou testes de intrusão) é basicamente uma série de testes comumente utilizados por auditores de segurança em infraestruturas de redes de computadores, ou até mesmo em sistemas operacionais, aplicativos, banco de dados etc. O objetivo do Pentest é encontrar falhas e vulnerabilidades. A partir das falhas e vulnerabilidades encontradas torna-se possível criar métodos de segurança adequados. Todavia, usuários intrusos também podem utilizar os testes de intrusão com o intuito de acessar, através das falhas e vulnerabilidades da rede, dados e informações confidenciais. Por conta disto, é imprescindível que toda instituição que possui infraestruturas de redes de computadores priorize a segurança afim de evitar possíveis intrusos e consequentemente o comprometimento de toda a confidencialidade e integridade da rede (MORENO, 2015).

2.5.3 Técnicas de ataques em redes wireless

2.5.3.1 Engenharia Social

Segundo Moreno (2015), a engenharia social consiste basicamente no ato de obter informações confidenciais das pessoas através da persuasão, manipulação etc. Através da engenharia social, é possível subtrair do alvo informações importantes, como por exemplo: senhas de acesso a dispositivos computacionais como computadores pessoais, roteadores, servidores etc. Os ataques efetuados através da engenharia social podem ser tanto voltados aos usuários como também voltados aos dispositivos computacionais. No que tange os ataques voltados a dispositivos computacionais, temos como exemplo o uso de e-mails falsos ou até mesmo dispositivos USB infectados com programas maliciosos. Com relação aos ataques voltados aos usuários, temos como característica o uso da persuasão através do contato direto com o usuário alvo. O processo de ataque através da engenharia social dar-se-á da seguinte forma: coleta de informações, confiança, vetor de ataque e execução:

- Coleta de informações: São coletadas as informações iniciais referentes ao alvo;
- Confiança: O atacante necessita criar um vínculo de confiança com o alvo. Para isto, é necessário que sejam coletadas informações bem especificas acerca do alvo;
- Vetor de Ataque: O atacante deve decidir e planejar o tipo de ataque a ser realizado: voltado ao usuário ou voltado a dispositivos computacionais;
- Execução: Etapa de execução do ataque.

2.5.3.2 Negação de Serviço (DoS)

De acordo com Laufer et al. (2015), o ataque de negação de serviço ou *Denial of Service* (DoS) é uma das técnicas de ataques mais conhecidas e mais utilizadas na Internet. Diferente do que acontece em grande parte dos ataques em redes wireless, um ataque DoS não busca invadir sistemas de redes afim de subtrair informações confidenciais, como senhas de acesso. O objetivo deste tipo de ataque é tornar inacessível ao usuário alvo o acesso à rede. Por fim, com o usuário desconectado da rede, o atacante pode utilizar outros métodos de ataques, como criar redes falsas e assim capturar senhas e informações confidenciais.

2.5.3.3 Força bruta

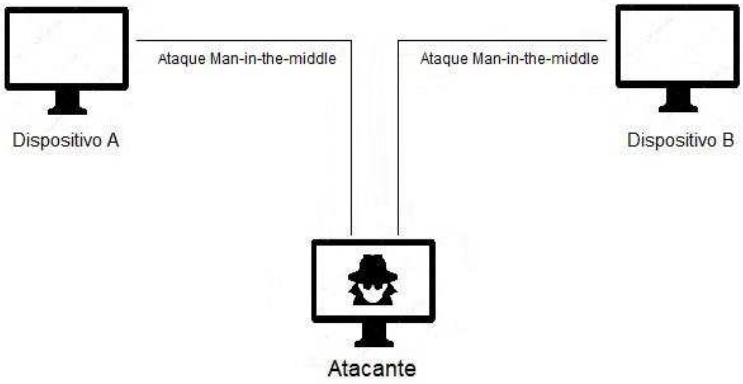
A técnica de ataque de força bruta consiste basicamente em obter ilegalmente senhas de acesso confidenciais como, por exemplo, senhas de redes wireless. Os atacantes utilizam *Wordlists* que, por sua vez, são listas com uma série de combinação de caracteres que podem ser possíveis senhas de acesso. Basicamente, os softwares de ataques de força bruta testam todas as combinações existentes nas *Wordlists* utilizadas até que a senha de acesso seja encontrada. Por conta disto, nos dias atuais está técnica é uma das menos eficientes no que diz respeito ao tempo levado para efetivar o ataque. Pois grande parte das redes já utilizam métodos criptográficos com chaves de acesso bem mais difíceis de serem quebradas, como por exemplo o WPA.

2.5.3.4 Man-in-the-middle

Segundo Moreno (2015), as técnicas de ataque do tipo *Man-in-the-middle* são uma das técnicas mais poderosas e eficientes contra redes wireless. Os ataques

Man-in-the-middle funcionam da seguinte forma: o atacante fica no meio de uma comunicação entre dispositivos monitorando todo o tráfego de dados sem que estes dispositivos tenham conhecimento que a confidencialidade e integridade da comunicação está comprometida. Com isto, o atacante pode ter acesso a informações confidenciais, assim como também capturar e alterar estas informações, ou até mesmo redirecionar estas informações a outros dispositivos.

Figura 7: Man-in-the-middle



Fonte: Autor

3 TRABALHOS RELACIONADOS

Este capítulo aborda diferentes trabalhos científicos que se relacionam com o tema desta pesquisa. Deste modo, os principais trabalhos relacionados a vulnerabilidades em redes wireless com foco em ataques *Man-in-the-middle* são descritos a seguir.

Em seu trabalho de conclusão de curso, Cruz (2014) faz um apanhado geral sobre alguns tipos específicos de ataques a dados que trafegam em redes wireless de computadores, a saber, ataques *Man-in-the-middle*. O autor demonstra diversas maneiras de como um intruso pode interceptar e manipular dados que trafegam em redes wireless. Além do mais, o autor traz alguns dos principais softwares existentes no mercado e utilizados para realizar estes ataques. Como resultado de seu trabalho, o autor traz alguns métodos utilizados para identificar e evitar que intrusos se conectem a redes wireless e acessem informações confidenciais. Entretanto, o

autor não propõe soluções específicas contra cada uma das técnicas de ataques do tipo *Man-in-the-middle* apresentadas em sua pesquisa.

Em “Ataque de Homem do Meio em Aplicações de Realidade Virtual”, projeto de Graduação apresentado à Escola de Informática Aplicada da Universidade Federal do Estado do Rio de Janeiro pelos estudantes Daniel Quintana de Andrade e Gabriel Castrillon Silva dos Santos, são apresentadas possíveis vulnerabilidades relacionadas à segurança da informação em aplicações de realidade virtual. O autor, através de experimentos, foca nas vulnerabilidades voltadas aos ataques do tipo *Man-in-the-middle*, mostrando algumas das falhas dos protocolos que regem a realidade virtual e as redes wireless, e como explorar estas falhas, tornando possível a um usuário intruso interceptar e alterar as imagens que são mostradas aos usuários das aplicações de realidade virtual. No entanto, o foco dos autores está apenas nos métodos de ataques do tipo *Man-in-the-middle* em sistemas de realidade virtual e não se aprofunda nas propostas de soluções para esses ataques (ANDRADE e CASTRILLON, 2018).

O artigo dos autores Botti e Martins (2015) apresenta uma análise comparativa entre duas ferramentas de ataque *Man-in-the-middle*: o Kali Linux e o Cain&Abel. Os autores criaram um ambiente computacional de testes e simularam ataques *Man-in-the-middle* utilizando as duas ferramentas. Após as simulações, fora realizada a comparação entre ambas as ferramentas utilizando três atributos como critérios: tempo, usabilidade e funcionalidade. Por fim, os autores constataram que a ferramenta Cain&Abel é a mais indicada para realizar ataques *Man-in-the-Middle*, pois sua interface gráfica possui fácil usabilidade e, além disso, requer um tempo ínfimo de instalação. Porém, os autores não propõem soluções para os tipos de ataques apresentados na pesquisa e deixa a proposta de soluções para trabalhos futuros.

No estudo de caso “Vulnerabilidades em Rede Wireless”, os autores Barbosa et al. (2017) abordaram sobre falhas e vulnerabilidades em redes wireless, analisando algumas técnicas de ataques como: engenharia social, *Man-in-the-middle*, pontos de acessos falsos, ataques de força bruta, negação de serviços entre outros. Além disso, os autores apresentam uma série de indicações e medidas de segurança que devem ser tomadas por quem utiliza as redes wireless afim de evitar intrusos indesejados. No entanto, o autor não foca especificamente nas técnicas de

ataques mais poderosas e eficientes existentes, a saber, os ataques do tipo *Man-in-the-middle* e não propões soluções para estes tipos específicos de ataques.

Tabela 1 – Sumário dos trabalhos relacionados

Aspectos Relevantes	Cruz (2014)	Andrade e Castrillon (2018)	Botti e Martins (2015)	Barbosa et al. (2017)	Referente Pesquisa
Vulnerabilidades em Redes Wireless	**x**	**x**	**x**	**x**	**x**
Análise das principais técnicas de ataque do tipo Man-in-the-middle	**x**	**x**	**x**		**x**
Propostas de soluções contra os ataques Man-in-the-middle	**x**				**x**
Propostas de soluções específicas para cada uma das principais técnicas de ataque do tipo Man-in-the-middle					**x**

Fonte: Autor

Deste modo, com base nos pressupostos evidenciados na tabela referente ao sumário dos trabalhos relacionados, considera-se relevante propor soluções específicas para cara uma das principais técnicas de ataques do tipo *Man-in-the-middle* existentes atualmente. No próximo capítulo serão analisadas as principais técnicas de ataques do tipo Man-in-the-middle e por fim apresentadas as propostas de soluções contra esses tipos de ataques.

4 METODOLOGIA DA PESQUISA

A etapa que inaugura esta pesquisa, deu-se através do levantamento bibliográfico aprofundado acerca dos tópicos relacionados ao tema proposto, a saber, as redes de computadores, protocolos de rede, segurança da informação, assim como também as falhas e vulnerabilidades em redes wireless.

4.1 Análise das técnicas de ataques *Man-in-the-middle*

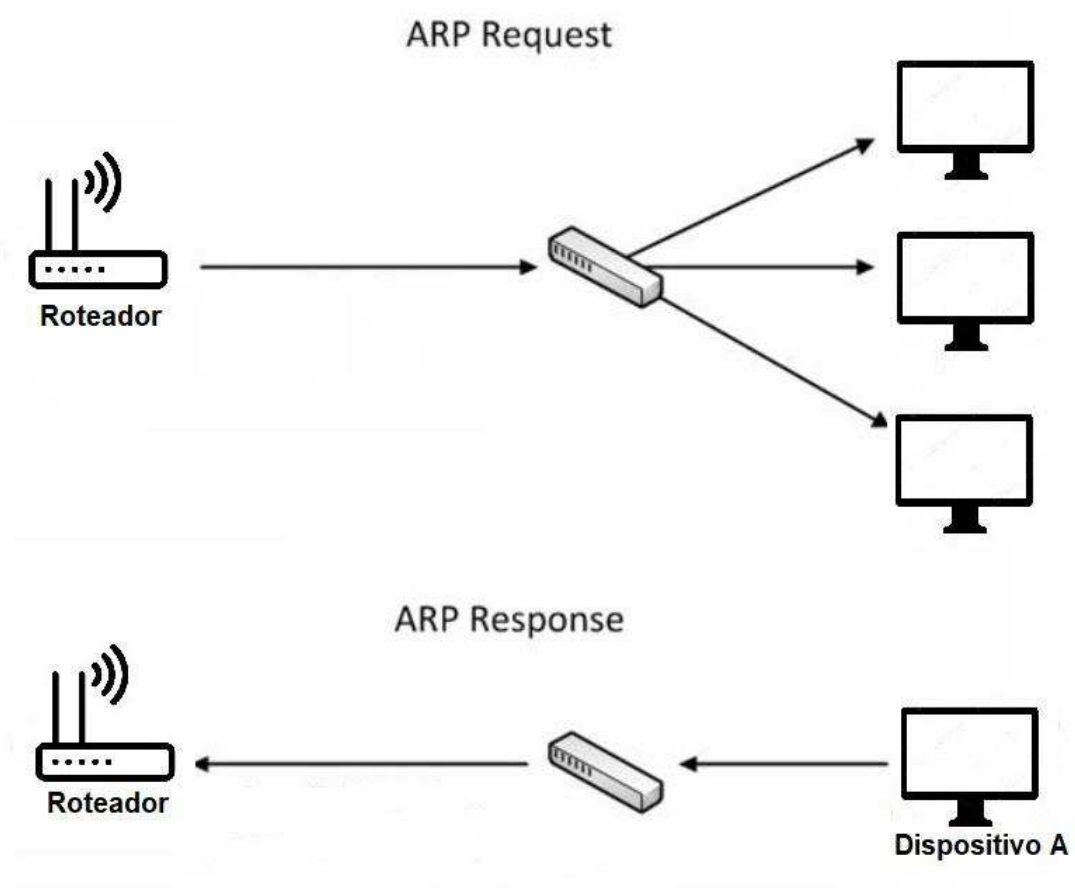
Nesta etapa, é realizada a análise das principais técnicas de ataques do tipo *Man-in-the-middle* voltadas a redes wireless. Pois, com o conhecimento aprofundado acerca de cada uma dessas técnicas torna-se possível propor soluções adequadas e eficientes a fim de evitar que usuários tenham seus dados confidenciais roubados ao conectarem-se em redes wireless.

4.1.1 ARP Cache Poisoning

O *ARP cache poisoning* (envenenamento de cache ARP) é uma das técnicas *Man-in-the-middle* mais simples de executar e, além disso, é considerada uma das mais poderosas e eficientes (SANDERS, 2010).

Sabe-se que o protocolo ARP é responsável por mapear endereços IPs em endereços MAC. O propósito do protocolo ARP é descobrir o endereço MAC de um dispositivo através do seu endereço IP. Digamos que, por exemplo, um roteador deseja enviar uma mensagem para um determinado dispositivo (dispositivo **A**) cujo o endereço IP é 192.168.0.1, porem ele desconhece e deseja descobrir o endereço MAC deste dispositivo. Para isto, segundo Sanders (2010), o protocolo ARP envia uma mensagem (*ARP Request*) a todos os dispositivos conectados na rede, buscando descobrir qual dispositivo possui o referido endereço IP. O dispositivo **A,** possuidor deste endereço IP envia uma mensagem de resposta (*ARP Response*) ao roteador, mencionando o seu respectivo endereço MAC. Por fim, o roteador adiciona em uma tabela cache (*ARP Cache Table*) o endereço IP do dispositivo **A** e seu respectivo endereço MAC e assim, o roteador e o dispositivo **A** podem se comunicar. Caso o roteador precise enviar outra mensagem ao dispositivo **A**, ele apenas consultará a sua *ARP Cache Table*.

Figura 8: Protocolo ARP



Fonte: Autor

Sabe-se que um dispositivo envia a *ARP response* a outro dispositivo quando lhe solicitam o seu endereço MAC através do *ARP request*. Porém, dispositivos que utilizam o protocolo ARP também aceitam atualizações em sua *ARP Cache Table* a qualquer instante, mesmo que não tenham sido enviadas *ARP requests*. A efetividade do *ARP Cache Poisoning* dar-se-á por conta desta vulnerabilidade onde qualquer usuário mal-intencionado pode enviar falsos *ARP responses* e assim tomar a identidade de outros usuários da rede (SANDERS, 2010). O *ARP Cache Poisoning* funciona basicamente da seguinte forma: digamos que existam 3 dispositivos conectados em uma rede:

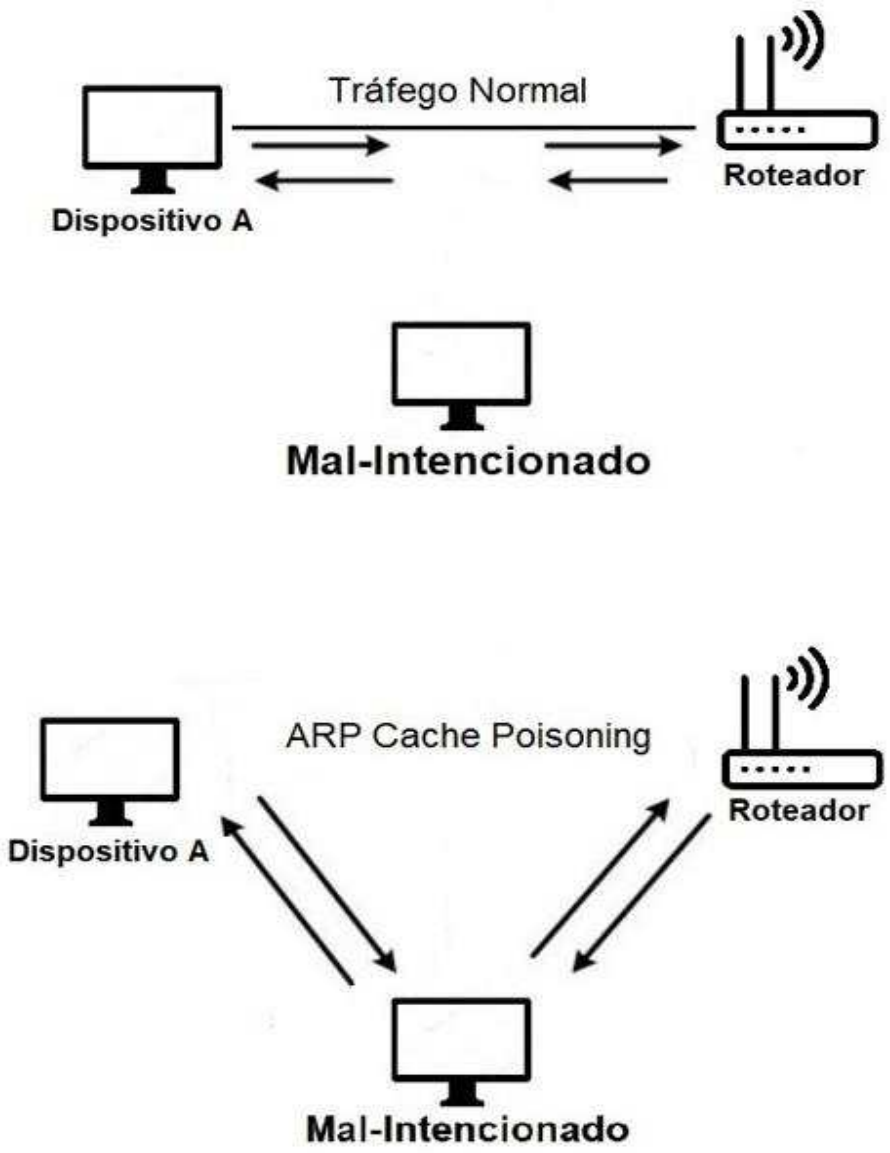
Tabela 2 – ARP Cache Table dos dispositivos da rede

	Endereço IP	**Endereço MAC**
Roteador	**192.168.0.1**	**AA:AA:AA:AA:AA:AA**
Dispositivo A	**192.168.0.2**	**BB:BB:BB:BB:BB:BB**
Dispositivo Mal-intencionado	**192.168.0.3**	**CC:CC:CC:CC:CC:CC**

Fonte: Autor

Suponhamos que nesta situação hipotética o roteador já possui em sua *ARP Cache Table* o endereço IP e MAC do dispositivo **A** e vice e versa. Afim de realizar o ataque de envenenamento, o dispositivo mal-intencionado envia uma ARP response ao roteador passando-se pelo dispositivo **A**. Assim como também envia ao dispositivo **A** outra ARP response passando-se pelo Roteador. Dessa forma todo o fluxo de dados trafegados entre o dispositivo **A** e o Roteador perpassam pelo dispositivo mal-intencionado sem que nenhum deles perceba que estão sendo monitorados.

Figura 9: ARP Cache Poisoning



Fonte: Autor

4.1.2 DNS Spoofing

O DNS Spoofing ou ataque de falsificação de DNS é utilizado para falsificar informações referentes ao protocolo DNS que são fornecidas a dispositivos conectados em redes de computadores (SACRAMENTO et al., 2017).

Quando um usuário tenta conectar-se a um determinado site na Internet, por exemplo, o site *carlos@adriano.com*, é realizada uma requisição a um servidor DNS,

solicitando o endereço IP deste site, que, por sua vez, encaminha ao usuário o endereço IP solicitado. Um servidor DNS é basicamente um dispositivo computacional que possui um banco de dados com uma série de endereços IPs e os seus respectivos endereços nominais.

Figura 10: Servidor DNS

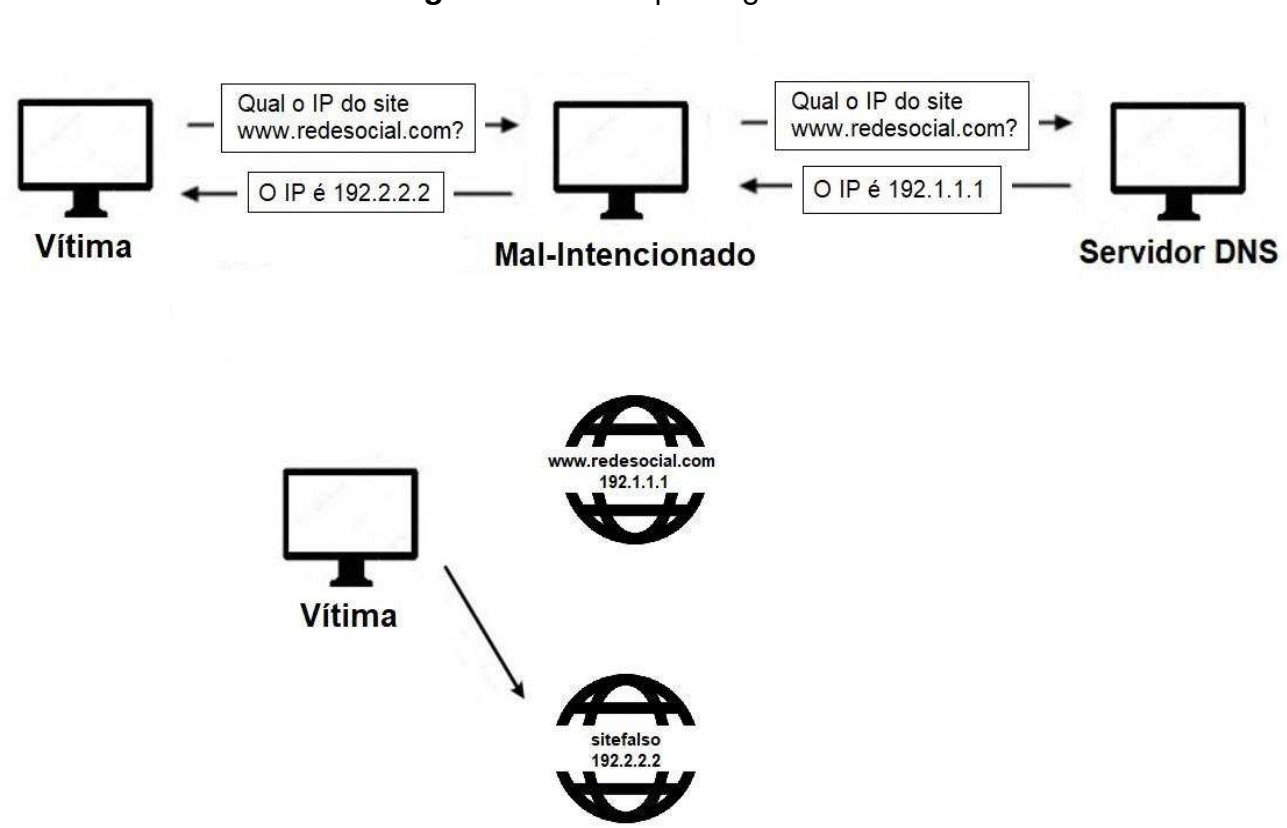
Fonte: Autor

O protocolo DNS possui um sistema de autenticidade que funciona da seguinte forma: toda requisição feita de um usuário a um servidor DNS possui um identificador numérico, e a mensagem de resposta ao usuário deve, obrigatoriamente, possuir o mesmo identificador numérico. Ou seja, caso um usuário mal-intencionado consiga interceptar a mensagem de requisição, ele pode simplesmente falsificar a mensagem de resposta, utilizando o mesmo identificador numérico e então, enviar ao usuário. Com isso, um usuário mal-intencionado pode fazer com que outros usuários da rede, ao tentarem conectar-se a um determinado site, sejam redirecionados a um site totalmente malicioso, e assim, terem seus dados confidenciais roubados (SACRAMENTO et al., 2017).

O atacante ao utilizar o DNS Spoofing deve, primeiramente, utilizar a técnica ARP Cache Poisoning para interceptar todo o tráfego de dados entre a vítima e o servidor DNS. Dessa forma, quando a vítima fizer uma requisição ao servidor DNS solicitando, por exemplo, o endereço IP do site *www.redesocial.com* (192.1.1.1), o

atacante falsifica a resposta, enviando o endereço IP de um site falso (192.2.2.2), criado unicamente para roubar as informações confidenciais da vítima. Ou seja, quando a vítima tentar acessar o site *www.redesocial.com*, ao invés de ser redirecionado para o endereço IP 192.1.1.1 ele será redirecionado para o endereço IP do site falso, e consequentemente, terá suas credenciais roubadas.

Figura 11: DNS Spoofing



Fonte: Autor

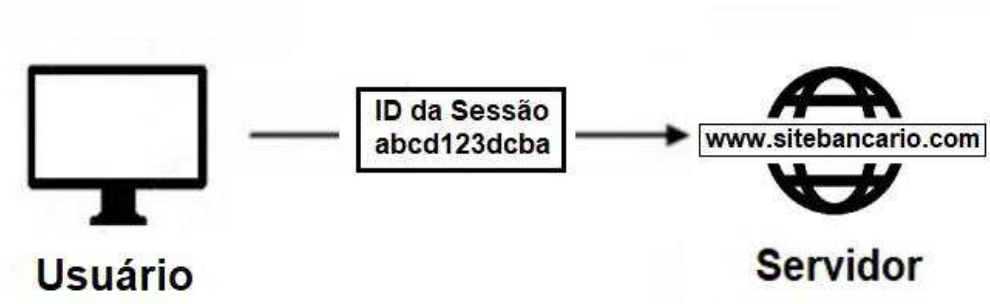
4.1.3 Sequestro de Sessão (Session Hijacking)

Quando um usuário se conecta em um site, por exemplo, uma rede social, e entra com suas credencias de Login e Senha, uma sessão de comunicação entre o usuário e o servidor web onde o site está armazenado é iniciada. Enquanto o usuário estiver conectado ao site, a sessão continuará estabelecida. A sessão é desfeita quando o usuário se desconectar do site (BAITHA, 2018). Geralmente, uma sessão é iniciada durante a comunicação entre dispositivos conectados em redes, onde existe a necessidade da autenticação de usuários, como é o caso de roteadores, servidores que armazenam sites de redes sociais, aplicativos de bancos entre outros. Basicamente, uma sessão é um período de tempo onde, por exemplo, dois computadores podem se comunicar de forma confiável, pois houve prévia autenticação entre cada um deles.

O objetivo do usuário mal-intencionado ao utilizar o ataque Session Hijacking é roubar a sessão da vítima para si (BAITHA, 2018). Com isso, o usuário mal-intencionado tomará a identidade da vítima e poderá, por exemplo, roubar seus dados confidenciais, enviar mensagens a terceiros passando-se pela vítima, realizar transações bancárias etc.

De acordo com Baitha (2018), toda sessão possui um identificador próprio (ID de sessão). Quando um usuário entra com suas credenciais em um site na web, por exemplo, o site de uma agência bancária, um ID de sessão é criado. Com isso, inicia-se uma sessão entre o usuário e o servidor web onde o site está hospedado. Dessa forma, quando o usuário solicita outras páginas do referido site ao servidor, ele não precisa entrar novamente com suas credencias. Pois, o servidor reconhece através do ID de sessão que aquele usuário é quem diz ser.

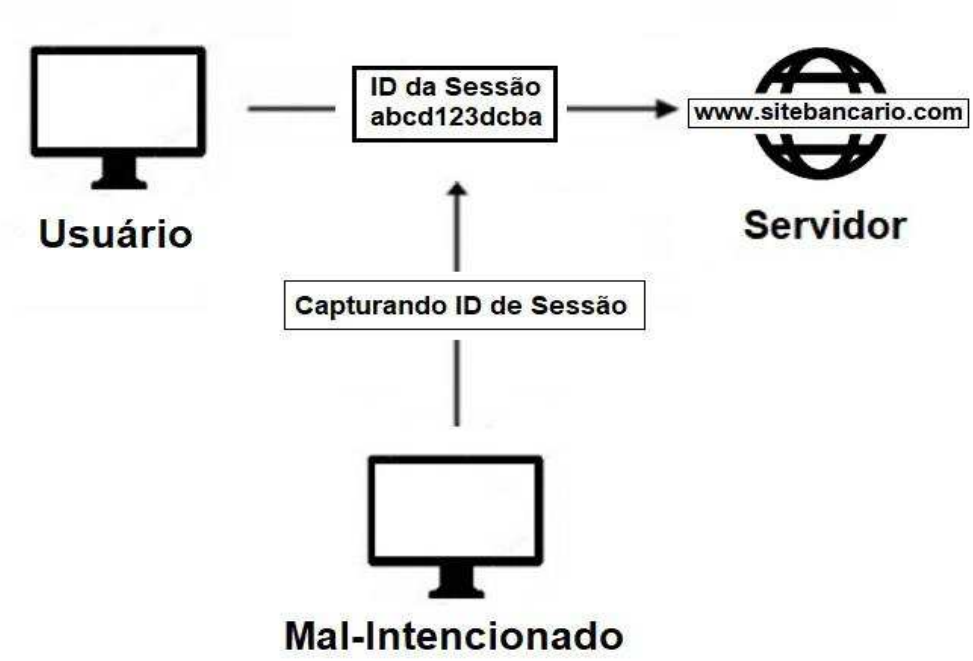
Figura 12: ID de Sessão



Fonte: Autor

A efetividade do sequestro de sessão dar-se-á da seguinte maneira: digamos que um usuário mal-intencionado deseja roubar a sessão de um usuário conectado a um site em um servidor web. Primeiramente, o usuário mal-intencionado precisa monitorar a comunicação entre a vítima e o servidor e capturar o ID de sessão desta comunicação.

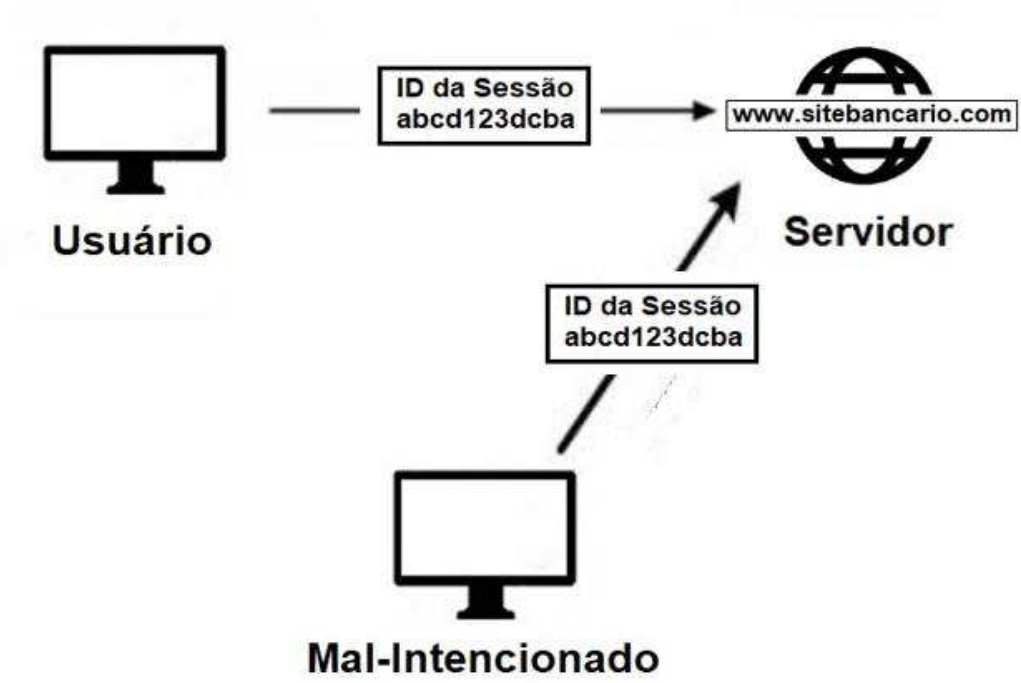
Figura 13: Capturando ID de Sessão



Fonte: Autor

Com o ID de sessão em mãos, o usuário mal-intencionado pode iniciar uma comunicação com o servidor utilizando este ID de sessão, e assim, se passar pela vítima, concluindo com êxito o ataque.

Figura 14: Sequestro de Sessão



Fonte: Autor

4.1.4 SSL Hijacking

O protocolo SSL (Secure Socket Layers ou Camada de Soquetes Segura) foi desenvolvido para prover uma camada de segurança, através da criptografia, na comunicação de dados nas redes de computadores. O protocolo SSL é utilizado em conjunto com outros protocolos, como por exemplo, o SMTP e o HTTP, que, por sua vez, tornam-se protocolos mais seguros: SMTPS e HTTPS. Ou seja, estes protocolos garantem maior segurança ao prover seus serviços em redes de computadores (SANDERS, 2010).

O Protocolo HTTPS é utilizado na comunicação de dados envolvendo servidores web que possuem informações sensíveis como informações bancárias, dados pessoais, sites de compras e vendas etc.

O ataque SSL Hijacking é comumente utilizado para interceptar dados em comunicação HTTPS, como é o caso da comunicação realizada entre usuários e

servidores web de sites bancários, sites de redes sociais ou sites de e-mails, que, por sua vez, utilizam-se da criptografia do protocolo SSL.

Basicamente, a comunicação HTTPS entre um usuário e um servidor web dar-se-á da seguinte forma: digamos que, por exemplo, um usuário deseja acessar o site *http://www.redesocial.com* usando o protocolo HTTP. Por ser um site que utiliza o protocolo de segurança SSL, o servidor web redireciona ao usuário a versão HTTPS deste site: *https://www.redesocial.com*. Em seguida, o usuário conecta-se ao site e o servidor provê um certificado digital para garantir a autenticidade do site, e assim a comunicação de dados segura e criptografada entre o usuário e o servidor web é iniciada.

Figura 15: Protocolo HTTPS

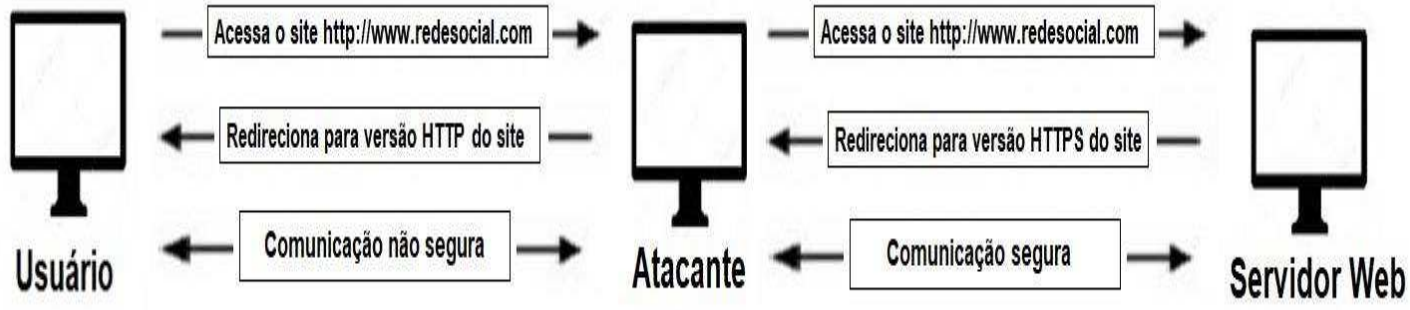
Fonte: Autor

Nota-se que a comunicação de dados entre o usuário e o servidor web inicia-se por uma solicitação de acesso do usuário ao referido site no servidor web, através do protocolo HTTP, e então, o servidor web redireciona o usuário para a versão segura do site que utiliza o protocolo SSL. O objetivo da técnica SSL Hijacking é atacar justamente o momento da transição entre a comunicação insegura HTTP e a comunicação segura HTTPS (SANDERS, 2010).

A efetividade do ataque SSL Hijacking dar-se-á da seguinte maneira: primeiramente, o atacante precisa interceptar o trafego de dados entre o usuário e o servidor web utilizando a técnica ARP Cache Poisoning. Logo após, quando o usuário solicitar acesso ao site no servidor web via protocolo HTTP, a solicitação irá chegar ao atacante que, por sua vez, irá repassar ao servidor. Então, o servidor irá

responder a solicitação do atacante com o redirecionamento ao site HTTPS, e também enviará o certificado digital de autenticidade, dando início à comunicação. Dessa forma o servidor web pensará estar comunicando-se de forma segura e criptografada com o usuário, e vice e versa. O atacante recebe todas as mensagens sem criptografia via HTTP que o usuário envia ao servidor web, e, depois de salva-las, as envia criptografadas via HTTPS ao servidor web. O servidor web responde as mensagens via HTTPS enviando ao atacante que lê a mensagem através do certificado digital e, depois de salva-las, as envia sem criptografia ao usuário.

Figura 16: SSL Hijacking



Fonte: Autor

5 RESULTADOS

5.1 Proposta de soluções contra os ataques Man-in-the-middle

Na metodologia desta pesquisa realizou-se um estudo teórico aprofundado acerca das principais técnicas de ataques do tipo Man-in-the-middle: ARP Cache Poisoning, DNS Spoofing, Sequestro de Sessão e SSL Hijacking. Foram analisadas cada uma das falhas e vulnerabilidades que tornam as redes de computadores sem fio suscetíveis a esses ataques e, assim, tornou-se possível propor soluções e contramedidas para cada uma das técnicas apresentadas.

5.1.1 Soluções contra os ataques ARP Cache Poisoning

Existem diversas medidas que podem ser tomadas em uma rede de computadores para prevenir-se de ataques do tipo ARP Cache Poisoning. Uma dessas medidas é a utilização de Redes Virtuais Privadas (VPNs). As VPNs criam um túnel criptografado entre o transmissor e receptor de uma comunicação e mesmo que um usuário atacante consiga interceptar a mensagem trafegada, ele não conseguirá visualizar o conteúdo da mensagem, pois ela estará cifrada (MORENO, 2015). A velocidade de comunicação na rede será reduzida, por conta da constante cifragem e decifragem dos dados, porém, a comunicação será mais segura e confiável. Este método é recomendável para usuários que, frequentemente, utilizam redes wireless públicas. Em LANs que possuem uma quantidade significativa de dispositivos, este método não seria uma opção viável, pois seria necessário a utilização de VPNs conectando cada um destes dispositivos, gerando um alto custo de implementação e manutenção da rede.

A utilização de tabelas cache estáticas é uma das contramedidas que podem ser utilizadas para evitar o ARP Cache Poisoning (SANDERS, 2010). Ela é recomendada para redes que possuem poucos dispositivos conectados. Nesta contramedida, o administrador da rede preenche a tabela cache com todos os endereços IPs e MACs de todos os dispositivos conectados na rede. Por conta disto, está medida se torna inviável em redes que possuem muitos dispositivos, pois sobrecarregaria o administrador da rede.

Outro método que pode ser utilizado para evitar ataques ARP Cache Poisoning é a utilização de programas de computadores desenvolvidos

especificamente para detectar este tipo de ataque, como é o caso do XArp. O XArp é um programa de segurança de redes desenvolvido especificamente para detectar ataques baseados em falhas e vulnerabilidades do protocolo ARP, como é o caso do ARP Cache Poisoning (MAYER, 2019). Programas de Antivírus e Malwares também podem ser utilizados para evitar esses tipos de ataques, e em conjunto com o XArp, a probabilidade dos ataques ARP Cache Poisoning obterem êxito diminuem consideravelmente.

Por fim, técnicas de Pentest podem ser utilizadas pelos administradores da rede para detectar possíveis falhas e vulnerabilidades relacionadas ao protocolo ARP e verificar se as contramedidas utilizadas estão sendo suficientes para garantir a confidencialidade e integridade da rede.

5.1.2 Soluções contra os ataques DNS Spoofing

Para que o ataque DNS Spoofing seja concretizado, é necessário que, inicialmente, seja realizado o monitoramento da rede através da técnica ARP Cache Poisoning para descobrir o ID das respostas dadas pelos servidores DNS. Ou seja, se os administradores das redes utilizarem as contramedidas indicadas para se proteger dos ataques ARP Cache Poisoning, as chances do ataque DNS Spoofing surtir efeito diminuem consideravelmente.

O DNSSEC é um protocolo utilizado para garantir, através da criptografia assimétrica, uma camada extra de segurança em comunicações envolvendo requisições DNS (SANDERS, 2010). O DNSSEC reduz consideravelmente a efetividade dos ataques DNS Spoofing, pois garante a autenticidade dos dispositivos que estão comunicando-se com servidores DNS, uma vez que apenas dispositivos autenticados podem realizar requisições DNS.

Programas de Antivírus, Malwares e técnicas de Pentest também podem ser utilizadas pelos administradores da rede para prover segurança em demasia aos dispositivos computacionais que se comunicam com os servidores DNS.

5.1.3 Soluções contra os ataques Sequestro de Sessão

Sabe-se que para a efetivação do ataque de Sequestro de Sessão, primeiramente, é necessário o monitoramento do tráfego de dados entre a vítima e o servidor WEB através da técnica ARP Cache Poisoning para capturar o ID de

sessão da comunicação. Ou seja, as técnicas de contramedidas utilizadas para combater o ARP Cache Poisoning, como por exemplo o uso de VPNs, são extremamente recomendadas para diminuir a chances de sucesso do ataque de Sequestro de Sessão.

Outra contramedida usada para evitar ataques de Sequestro de Sessão é evitar utilizar redes sem fio públicas. Ao conectar-se em redes sem fio públicas, o usuário deve tomar algumas precauções, como por exemplo, não se conectar em sites confidenciais, como sites de banco, redes sociais e etc. Caso haja a necessidade de se conectar em tais sites, o usuário deve dá preferência a sites que utilizam o protocolo de segurança SSL, como o HTTPS.

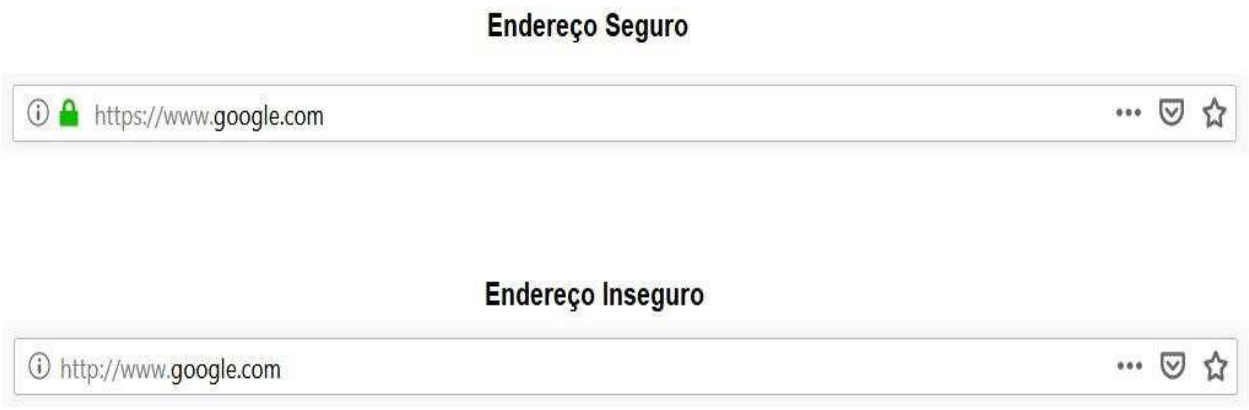
Por fim, afim de detectar as falhas e vulnerabilidade da rede no que tange os ataques de Sequestro de Sessão, técnicas de Pentest devem ser feitas constantemente pelos administradores da rede.

5.1.4 Soluções contra os ataques SSL Hijacking

Sabe-se que, assim como nas técnicas DNS Spoofing e Sequestro de Sessão, a técnica de ataque ARP Cache Poisoning é primordial para que o ataque SSL Hijacking obtenha êxito. Dessa forma, a aplicação das contramedidas usadas para evitar o ARP Cache Poisoning é crucial e essencial para combater e diminuir as chances de sucesso do ataque SSL Hijacking.

Durante o ataque SSL Hijacking, a vítima, ao invés de acessar a versão HTTPS e segura do site, acessa a sua versão insegura, ou seja, sem o protocolo SSL. Usuários devem sempre atentar-se para o endereço web no navegador e verificar se o mesmo está em sua versão HTTPS, principalmente ao conectar-se em sites que possuem dados confidenciais.

Figura 17: Endereço Web



Fonte: Autor

Além do mais, programas de Antivírus, Malwares e técnicas de Pentest também podem ser utilizadas pelos usuários ou administradores de rede para prover maior segurança de rede.

6 CONCLUSÃO

Este trabalho teve como objetivo listar e analisar as principais técnicas de ataques do tipo Man-in-the-middle em redes wireless, e, além disso, propor soluções e contramedidas para evitar estes tipos de ataques.

Foram analisadas as seguintes técnicas de ataques Man-in-the-middle: ARP Cache Poisoning, DNS Spoofing, Sequestro de Sessão e SSL Hijacking. Através das análises, notou-se a grande fragilidade e a imensa quantidade de vulnerabilidades que alguns protocolos de rede possuem. Verificou-se também que as redes de computadores, principalmente as redes sem fio públicas, são bastante suscetíveis a ataques, uma vez que, usuários mal-intencionados podem, facilmente, utilizar-se das técnicas disponíveis, e assim, monitorar e roubar os dados trafegados nas redes em que estiverem conectados.

Por fim, tivemos como resultado desta pesquisa, algumas propostas de soluções contra os ataques do tipo Man-in-the-middle que foram descritos e analisados na metodologia. Usuários e, principalmente, administradores de redes devem aplicar, de preferência, todas as contramedidas citadas nesta pesquisa, afim de garantir a confiabilidade, integridade e autenticidade de toda a comunicação de dados decorrente de redes wireless. É fato, que mesmo aplicando todas as propostas de soluções listadas nesta pesquisa, ainda existe a possibilidade de as redes sofrerem ataques do tipo Man-in-the-middle. Porém, as chances destes ataques obterem sucesso irão diminuir consideravelmente.

6.1 Trabalhos Futuros

As seguintes propostas são sugeridas para trabalhos futuros:

- Analisar e propor soluções para outras técnicas de ataques do tipo Man-in-the-middle;
- Realizar simulações das técnicas de ataques e suas contramedidas em ambientes de teste e realizar um comparativo entre as soluções

REFERÊNCIAS

ANDRADE, D. Q.; CASTRILLON, G. S. S. Ataque de Homem do Meio em Aplicações de Realidade Virtual. Projeto de Graduação (Escola de Informática Aplicada) - Universidade Federal do Estado do Rio de Janeiro. Rio de Janeiro. 2018

BAITHA, A. K.; VINOD, S. Session Hijacking and Prevention Technique. International Journal of Engineering & Technology. 2018

BARBOSA, G. A.; MEDEIROS, H. A.; XAVIER, I.; SOUZA, L. D. C.; AMARAL, E. C.; SABINO, E.; ABE, N.; OLIVEIRA, S. Estudo de Caso: Vulnerabilidades em Rede Wireless. Revista Gestão em Foco. Ed. 9. 2017

BOTTI, C. F.; MARTINS, D. M. S. M. Análise Comparativa entre Ferramentas de Ataque Man in the middle. Artigo (Sistema de Informação) – Centro de Ensino Superior de Juiz de Fora. Minas Gerais. 2015

CRUZ, D. L. Uma abordagem para detecção e proteção de ataques *Man-in-the-middle* (MITM). Monografia (Pós-graduação em Redes de Computadores e Segurança em Redes) – Universidade Tuiuti do Paraná. Paraná. 2014

ELIAS, Glêdson; LOBATO, L. C. Arquitetura e Protocolo de Rede TCP-IP. 2. ed. Rio de Janeiro: RNP/ESR: 2003

FERREIRA, J. L. M. Segurança em Redes sem Fio. Monografia (Especialização em configuração e gerenciamento de servidores e equipamentos de rede) – Universidade Federal do Paraná. Paraná. 2013

FILIPPETTI, M. A. Cisco CCNA 4.1 – Guia Completo de Estudo. Florianópolis: Visual Books, 2008

FOROUZAN, Behrouz A. Comunicação de Dados e Redes de Computadores. 3. ed. Porto Alegre: Bookman. 2006

KUROSE, James F. Redes de Computadores e a Internet: uma abordagem top-down. 5. ed. São Paulo: Addison Wesley, 2010

LAUFER, R. P.; MORAES, I. M.; VELLOSO, P. B.; BICUDO, M. D. D.; CAMPISTA, M. E. M.; CUNHA, D. O.; COSTA, L. H. M. K.; DUARTE, O. C. M. B. Negação de Serviços: Ataques e Contramedidas. Em Minicursos do Simpósio Brasileiro de

Segurança da Informação e de Sistemas Computacionais - SBSeg'2005. ISBN: 8576690470, Sociedade Brasileira de Computação. 2005

MAYER, Christoph. XARP, 2019. Página inicial. Disponível em: <http://www.xarp.net> Acesso em: 24 de jul. de 2019

MORENO, Daniel. Introdução ao Pentest. São Paulo. Novatec: 2015

OLIVEIRA, A. T. Análise das Vulnerabilidades das Redes sem Fio na Cidade de Vitória da Conquista – BA. Monografia (Curso bacharelado em Ciência da Computação) – Universidade Estadual do Sudoeste da Bahia. Bahia. 2010

SACRAMENTO, V.; MOREIRA, A.; GUIDO, L.; BATISTA, T. Especificação Formal e Implementação de Mecanismos de Segurança para Resolução de Nomes no DNS. Simpósio Brasileiro de Redes de Computadores, 2002, Búzios, RJ. Anais do XX SBRC. Rio de Janeiro: NCE/UFRJ, 2002

SANDERS, Chris. Understanding Man-In-The-Middle Attacks. Disponível em: < https://chrissanders.org/2010/06/understanding-man-in-the-middle-attacks/> Acesso em: 24 de jul. de 2019

TANENBAUM, Andrew S. Redes de Computadores. 4. ed. [S.l.]: Editora Campus, 2003

VASCONCELLOS, Ronaldo. Segurança em Redes sem Fio. Rio de Janeiro: RNP/ESR: 2003