UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE COMPUTAÇÃO
CURSO DE CIÊNCIA DA COMPUTAÇÃO

FELIPE HISTER FRANZ

MÉTODOS DE DEFESA EM SWITCHES GERENCIÁVEIS

TRABALHO DE CONCLUSÃO DE CURSO

MEDIANEIRA

2019

FELIPE HISTER FRANZ

MÉTODOS DE DEFESA EM SWITCHES GERENCIÁVEIS

Trabalho de Conclusão de Curso apresentado ao Departamento Acadêmico de Computação da Universidade Tecnológica Federal do Paraná como requisito parcial para obtenção do título de "Bacharel em Computação".

Orientador: Prof. Dr. Neylor Michel

MEDIANEIRA

2019

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Diretoria de Graduação e Educação Profissional
Coordenação do Curso de Ciência da Computação

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

TERMO DE APROVAÇÃO

MÉTODOS DE DEFESA EM SWITCHES GERENCIÁVEIS

Por

FELIPE HISTER FRANZ

Este Trabalho de Conclusão de Curso foi apresentado às 08:20h do dia 28 de junho de 2019 como requisito parcial para a obtenção do título de Bacharel no Curso de Ciência da Computação, da Universidade Tecnológica Federal do Paraná, Câmpus Medianeira. O candidato foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

Prof. Neylor Michel
UTFPR - Câmpus Medianeira

Prof. Nelson Miguel Betzek
UTFPR - Câmpus Medianeira

Prof. Ricardo Sobjack
UTFPR - Câmpus Medianeira

A folha de aprovação assinada encontra-se na Coordenação do Curso.

RESUMO

FRANZ, Felipe Hister. MÉTODOS DE DEFESA EM SWITCHES GERENCIÁVEIS. 48 f. Trabalho de Conclusão de Curso – Curso de Ciência da Computação, Universidade Tecnológica Federal do Paraná. Medianeira, 2019.

O aumento na utilização das redes de computadores, trazem diversas ameaças a segurança, que podem causar grandes prejuízos as pessoas e organizações. A proposta deste trabalho consiste na identificação dos principais ataques internos nas redes de computadores e também mecanismos de segurança para evitar estes ataques. Com base no levantamento inicial, os ataques são realizados em uma pequena rede com o objetivo de testar os mecanismos de segurança. Os testes demonstraram que mecanismos de segurança utilizados conseguem mitigar os ataques e melhorar a segurança interna da rede sem custos adicionais.

Palavras-chave: Ataques, Mecanismos de Segurança, Segurança interna

ABSTRACT

FRANZ, Felipe Hister. SECURITY AT THE DATA LINK LAYER. 48 f. Trabalho de Conclusão de Curso – Curso de Ciência da Computação, Universidade Tecnológica Federal do Paraná. Medianeira, 2019.

The increase in the use of computer networks, bring various security threats, which can cause great harm to people and organizations. The purpose of this work is to identify the main internal attacks on computer networks and also security mechanisms to avoid these attacks. Based on the initial survey, the attacks are conducted on a small network with the goal of testing the security mechanisms. The tests demonstrated that security mechanisms used to mitigate attacks and improve internal network security without additional costs.

Keywords: Attacks, Security Mechanisms, Internal security

AGRADECIMENTOS

A minha família agradeço pelo apoio e incentivo nos estudos. Aos professores que contribuíram para a minha formação. E aos meus amigos que estiveram comigo durante esta jornada.

LISTA DE FIGURAS

LISTA DE SIGLAS

ARP	Address Resolution Protocol
ASCII	American National Standard Code for Information Interchange
BPDUs	Bridge Protocol Data Units
CAM	Content Addressable Memory
CDP	Cisco Discovery Protocol
DHCP	Dynamic Host Configuration Protocol
DTP	Protocolo de Entroncamento Dinâmico
HSRP	Protocolo Hot Standby Router
IP	Internet Protocol
ISL	Inter-Switch Link Protocol
ISO	International Standards Organization
LLC	Controle de link lógico
MAC	Controle de acesso ao meio
OSI	Open Systems Interconnection
RARP	Reverse Address Resolution Protocol
STP	Spanning Tree Protocol
TTL	Tempo de vida
UDP	User Datagram Protocol
VLAN	Rede de Área Local Virtual
VTP	Protocolo VLAN Trunking Protocol

SUMÁRIO

1 INTRODUÇÃO

As redes de computadores tem grande impacto sobre as empresas ao trazerem diversos benefícios, como aumento de produtividade e rápida troca de informações. Mas essas redes também trazem ameaças para a segurança que, se amenizadas, permitem que os benefícios superem todos os riscos. Para evitar os possíveis ataques, vários mecanismos de segurança são desenvolvidos. Stallings (2014) define mecanismo de segurança como um processo que é projetado para detectar, impedir ou recuperar-se de um ataque à segurança.

Muitas empresas implementam mecanismos de segurança nas camadas mais altas do modelo de referência Open Systems Interconnection (OSI), a fim de evitar os ataques externos, mas acabam não dando a devida atenção para a camada de enlace de dados, o que abre uma vasta margem para possíveis ataques internos. Beukema et al. (2017) citam que grande parte dos ataques é executado de dentro da própria rede. Segundo um relatório da IBM X-Force (IBM, 2016), 60% dos ataques que ocorreram em 2015 eram ataques internos. Isto demonstra que a segurança das redes deve considerar medidas para impedir os ataques internos e não apenas para impedir os ataques externos.

Os ataques internos se aproveitam da baixa segurança dos dispositivos de acesso, explorando tanto características de equipamentos como dos protocolos, a fim de prejudicar a rede ou obter dados.

Quando se fala de ataques internos, não é necessário que o atacante esteja conectado fisicamente na rede da empresa. Ele pode estar conectado remotamente a alguma máquina que tenha sido infectada e a partir dela realizar os ataques.

A segurança de uma rede é tão forte quanto o seu ponto mais fraco, normalmente a maioria dos ataques ocorrem na camada de enlace de dados, o que a torna o ponto mais fraco em uma rede de computadores. Portanto, há vulnerabilidades na camada de enlace que podem ser exploradas, entretanto há mecanismos de segurança que podem ser aplicados na mitigação dos ataques envolvidos nesta camada.

1.1 JUSTIFICATIVA

O motivo para abordar a segurança na camada de enlace de dados é pelo fato dela receberem pouca atenção da maioria dos administradores de redes, na maioria das vezes só consideram medidas para segurança externa da rede, acredita-se que a rede interna é segura e confiável. De acordo com um relatório da IBM (2016), inúmeros ataques são iniciados a partir da rede interna da empresa ou remotamente a partir de algum dispositivo que foi infectado, com objetivos de danificar a rede e obter acesso aos dados.

Dentro desta situação, justifica-se o estudo de medidas de segurança para algumas das principais ameaças da camada de enlace de dados,a fim de identificar problemas de segurança interna das redes de computadores e propor possíveis soluções.

1.2 OBJETIVO GERAL

O objetivo geral deste trabalho é realizar estudos de vulnerabilidades na camada de enlace das redes de computadores, e propor possíveis soluções de segurança.

1.3 OBJETIVOS ESPECÍFICOS

Os objetivos específicos são:

1. Identificar algumas das principais vulnerabilidades da camada de enlace;
2. Definir medidas de segurança a fim de evitar os ataques;
3. Implementar as medidas de segurança para as vulnerabilidades encontradas;
4. Verificar se as medidas de segurança aplicadas evitam os ataques identificados.

1.4 ESTRUTURA DO TRABALHO

No capítulo 2 é apresentado inicialmente o modelo OSI, em seguida é apresentado alguns protocolos e o switch um equipamento da camada de enlace, por último é apresentado alguns ataques que podem ocorrer na camada de enlace.

No capítulo 3 são descritos os materiais e métodos utilizados para o desenvolvimento dos testes.

No capítulo 4 são implementados técnicas de ataque e defesa para algumas das ameaças, por fim é analisado o resultado dessas implementações.

No capítulo 5 é apresentado a conclusão final e sugestões para trabalhos futuros.

2 REVISÃO BIBLIOGRÁFICA

Neste capítulo é apresentado o referencial teórico sobre rede de computadores, o modelo de referência OSI e os protocolos e equipamento da camada de enlace. Por fim, são descritos alguns dos principais ataques realizados na camada de enlace.

2.1 REDES DE COMPUTADORES

Uma rede de computadores é formada por um grupo de computadores que estão conectados entre si por algum meio de comunicação, esta conexão pode ser feita por meio de fios de cobre, fibra óptica, micro-ondas ou infravermelho (TANENBAUM; WETHERALL, 2011). As redes de computadores são capazes de compartilhar recursos e trocar informações com qualquer usuário independente de sua localização. A Figura 1 demonstra um exemplo de rede onde está sendo compartilhada uma impressora (recurso), e os computadores podem eventualmente realizar trocas de informações.

Figura 1 – Troca de dados e compartilhamento de recursos.
Fonte: (TORRES, 2014).

Segundo Torres (2014) as redes de computadores surgem da necessidade da troca de informações. No começo as redes de computadores eram pequenas com poucos computadores, mas com o tempo cresceram e passaram a abranger todo os ramos de atividade, com isso

acabaram se tornando um recurso vital para as empresas e pessoas.

Independente do seu uso e tamanho, as redes devem garantir um compartilhamento de recursos e informações de maneira segura e confiável. Para isso as redes de computadores possuem protocolos para garantir uma comunicação segura. Para Kurose e Ross (2014) um protocolo define o formato e a ordem das mensagens trocadas entre duas ou mais entidades comunicantes, bem como as ações realizadas na transmissão e/ou no recebimento de uma mensagem ou outro evento.

2.2 MODELO DE REFERÊNCIA OSI

No inicio das redes de computadores as soluções que existiam para elas eram proprietárias, ou seja, as tecnologias existentes só eram suportadas por seus fabricantes. Não era possível mesclar tecnologias de diferentes fabricantes, pois não havia compatibilidade (TORRES, 2014; MENDES, 2015).

Se fez necessário o desenvolvimento de um modelo, para que as fabricantes dos componentes de redes pudessem usar como referência para o desenvolvimento de suas tecnologias, tornando compatível as tecnologias desenvolvidas por diferentes empresas.

Com o objetivo de facilitar a interconexão dos computadores e acabar com a incompatibilidade entre os fabricantes, a International Standards Organization (ISO) desenvolveu o modelo OSI, para que as fabricantes pudessem desenvolverem suas tecnologias a partir deste modelo (TORRES, 2014; MENDES, 2015).

O modelo OSI é um primeiro passo para se obter uma padronização. Foi desenvolvido e organizado em sete camadas conforme mostrado na Figura 2, para tratar da padronização das redes, onde cada camada possui funções bem definidas (TANENBAUM; WETHERALL, 2011)(BORA et al., 2014). Para o desenvolvimento das camadas foram aplicados os seguintes princípios:

1. Uma camada deve ser criada onde houver necessidade de outro grau de abstração;
2. Cada camada deve executar uma função bem definida;
3. A função de cada camada deve ser escolhida tendo em vista a definição de protocolos padronizados internacionalmente;
4. Os limites de camadas devem ser escolhidos para minimizar o fluxo de informações pelas interfaces;

5. O número de camadas deve ser grande o bastante para que funções distintas não precisem ser desnecessariamente colocadas na mesma camada e pequeno o suficiente para que a arquitetura não se torne difícil de controlar.

Figura 2 – Camadas do modelo OSI.
Adaptado de: (TORRES, 2014).

A seguir são descritas as sete camadas do modelo OSI.

Camada de Aplicação: É responsável por fornecer uma interface entre os protocolos de comunicação e as aplicações dos usuários, possibilitando que os aplicativos possam pedir e receber informações da rede. Quando utiliza-se um aplicativo de e-mail para acessar um e-mail, o aplicativo entrara em contato com a camada de aplicação onde efetuara o pedido para receber as informações sobre os e-mail (TORRES, 2014; MENDES, 2015; LI et al., 2011);

As principais funções desta camada são:

1. Determinar se a comunicação será full duplex onde a aplicação pode enviar e receber dados ao mesmo tempo ou half duplex onde a aplicação pode enviar ou receber dados mas não ao mesmo tempo;
2. Identificar endereços e nomes;
3. Fazer o controle de acesso;
4. Garantir a integridade dos dados.

Um dos principais protocolos desta camada é o protocolo DHCP (Dynamic Host Configuration Protocol), que é responsável por fornecer endereços IPs aos dispositivos da rede. Utiliza o protocolo UDP(User Datagram Protocol) para enviar as mensagens (RAJPUT et al., 2016), para fazer a distribuição de IPs realiza as seguintes etapas:

1. Descoberta: quando o dispositivo se conecta na rede, envia uma mensagem DHCP-DISCOVERY em modo broadcast, para descobrir os servidores DHCP e solicitar um IP;
2. Oferta: o servidor DHCP recebe o pedido do dispositivo, reserva um endereço IP

disponível e envia uma mensagem DHCP-OFFER oferecendo um endereço IP ao dispositivo;
3. Pedido: em resposta a oferta do servidor DHCP, o dispositivo envia uma mensagem DHCP-REQUEST requisitando o endereço IP oferecido;
4. Confirmação: ao receber a mensagem do dispositivo o servidor DHCP, envia uma mensagem DHCP-AKC confirmando que o IP foi atribuído.

Após o termino destas etapas o dispositivo está pronto para utilizar a rede.

Camada de Apresentação: É responsável por converter as informações vindas da camada de aplicação em um formato que possa ser usado posteriormente na transmissão dos dados, por fazer esta função, também é conhecida por camada de tradução. Quando comunica-se com um dispositivo transmissor que utiliza um padrão diferente do American National Standard Code for Information Interchange (ASCII), a camada de apresentação deve traduzir a informação para que o receptor compreenda a mensagem. Esta camada também faz a compreensão e a criptografia dos dados (TORRES, 2014; MENDES, 2015);

Camada de Sessão: Esta camada permite que usuários utilizando computadores diferentes estabeleçam uma sessão de comunicação (TANENBAUM; WETHERALL, 2011; MENDES, 2015). Ao se estabelecer a comunicação os aplicativos definem como ocorrera a transmissão dos dados e também adicionam marcações nos dados, a fim de criar pontos de sincronização, se eventualmente a comunicação for interrompida, a partir dos pontos de sincronização poderá reestabelecer a comunicação (MENDES, 2015);

Camada de Transporte: A camada de transporte recebe os dados vindos da camada de sessão, segmenta os dados em pacotes de dados menores, e os repassa para camada de rede garantindo que todas as partes cheguem corretamente ao receptor (TANENBAUM; WETHERALL, 2011); Suas principais responsabilidades são:

1. Informar qual protocolo está sendo usado na camada de cima, para qual o pacote deve ser entregue, assim permite que vários protocolos possam ser usados acima desta camada;
2. Controle de fluxo, que trata de colocar em ordem os pacotes recebidos, caso tenham chegado desordenados;
3. Verificação de erros, verifica se os pacotes chegaram corretamente ao seu destino;
4. Verificar se todos os pacotes esperados foram recebidos;
5. Verificar se houve a duplicação de pacotes.

Camada de Rede: A camada de rede é responsável por fazer o encaminhamento dos pacotes de dados, fazendo o endereçamento lógico destes pacotes e a tradução dos endereços lógicos em endereços físicos. Também é responsável por determinar o melhor caminho que

os pacotes de dados possam utilizar para chegar no seu destino (TORRES, 2014; MENDES, 2015);

Camada de Enlace de Dados: Também conhecida como link de dados ou apenas como camada de enlace, sua tarefa é criar uma interface segura entre o meio de comunicação e os dados que vão ser enviados, fazendo o controle de fluxo, detectando erros e verificando se o meio por onde os dados serão enviados esta disponível para ser usado (TANENBAUM; WETHERALL, 2011; TORRES, 2014). A camada de enlace é subdividida em duas subcamadas, a subcamada Controle de link lógico (LLC) e a subcamada Controle de acesso ao meio (MAC).

A subcamada LLC adiciona informações sobre qual protocolo de alto nível gerou o pacote de dados que vai ser enviado na rede. Com esta informação o dispositivo que vai receber este pacote de dados, sabe para qual protocolo deve entregar os dados recebidos (TORRES, 2014).

A subcamada MAC: recebe os dados vindos da subcamada LLC, então prepara os quadros de dados que serão enviados pela camada física, adicionando um cabeçalho que contem os endereços físicos MAC do dispositivo de origem e de destino. Também verifica se o meio que os dados vão ser transmitidos está disponível para uso (TORRES, 2014);

Camada Física: Esta camada é responsável pela transmissão de bits através de algum meio de comunicação. Recebe os dados vindo da camada de enlace e os converte em um sinal que pode ser elétrico, luminoso ou rádio frequência, dependendo do meio que vai ser transmitido, e também recebe os sinais vindos do meio de comunicação e os converte em bits para serem usados na camada de enlace (TORRES, 2014; MENDES, 2015).

2.3 PROTOCOLOS E EQUIPAMENTO DA CAMADA DE ENLACE

Nesta sessão são abordados alguns dos protocolos que atuam na camada de enlace de dados onde o switch que é dos principais equipamentos utilizados.

2.3.1 Endereço MAC (controle de acesso ao meio)

O endereço MAC é o endereço físico de um dispositivo de rede, este endereço é atribuído ao dispositivo no momento de sua fabricação, fazendo que cada dispositivo tenha um endereço MAC único. Equipamentos como switch que operam na camada de enlace de dados, utilizam o endereço MAC para enviar os dados para o destino correto (JORDAO, 2014).

O endereço MAC é um conjunto de 48 bits, representados em hexadecimal. Os 24 bits iniciais representam a fabricante do dispositivo e os 24 bits finais é um valor dado pela fabricante para representar o dispositivo. Exemplo de um endereço MAC 2E-C9-D3-42-62-16 (JORDAO, 2014).

2.3.2 Protocolo ARP (Address Resolution Protocol) e Protocolo RARP (Reverse Address Resolution Protocol)

O protocolo ARP é utilizado para vincular um endereço lógico IP a um endereço físico MAC. Quando um dispositivo quer saber o endereço MAC de um outro dispositivo que possui um determinado IP, é feito um pedido ARP contendo o IP do dispositivo que precisa-se descobrir o endereço MAC, então o dispositivo que possui o endereço IP solicitado, responde o pedido com o seu endereço MAC. A resposta é armazenada em uma tabela ARP onde relaciona o endereço MAC com o endereço IP, fica armazenada por um tempo determinado para usos futuros, após o tempo esgotar a resposta é eliminada da tabela, sendo necessário um novo pedido ARP (HUSSAIN et al., 2017).

A Figura 3 é um exemplo de tabela ARP, onde se esta associando um endereço MAC com um endereço IP e o campo TTL (Tempo de vida) mostra o horário que esta associação será eliminada da tabela.

Endereço IP	Endereço MAC	TTL
222.222.222.221	88-B2-2F-54-1A-0F	13:45:00
222.222.222.223	5C-66-AB-90-75-B1	13:52:00

Figura 3 – Tabela ARP.
Fonte: (KUROSE; ROSS, 2014).

O protocolo RARP tem o seu funcionamento parecido com o do ARP, mas faz o inverso, ou seja, utiliza o endereço MAC do dispositivo para descobri o seu endereço IP (TORRES, 2014).

2.3.3 Protocolo STP (Spanning Tree Protocol)

Em uma rede grande que utiliza diversos switches, podem existir diversos caminhos para chegar a um determinado dispositivo da rede, ou seja, a rede possui caminhos redundantes. Estes caminhos redundantes geram loops na rede, que trazem o problema de tempestade de broadcast, onde quadros enviados de forma broadcast ficam sendo propagados na rede de forma infinita, o que pode resultar em um mau funcionamento da rede (MAIA, 2013).

O protocolo STP resolve o problema de loop na rede, pois ele decide quais caminhos serão utilizados. Todos os caminhos da rede são identificados, então são determinados os caminhos que permanecerão ativos e quais ficarão desativados. Os caminhos mais rápidos são escolhidos para serem utilizados, os que não são utilizados são fechados (MAIA, 2013; TORRES, 2014). O protocolo STP realiza os seguintes passos para definir os caminhos que ficarão ativos:

1. Define um switch raiz. Os switchs da rede realizam uma troca de mensagem para definir quem será a raiz;
2. Os switchs definem qual será sua porta raiz, essa porta é a que possui o caminho mais rápido até o switch raiz;
3. Definir a porta designada que possui o caminho mais rápido até um determinado switch, caso exista mais de um caminho para chegar até ele;
4. As portas que levam a outro switch que não foram definidas como porta raiz ou designada são fechadas.

Se houver mudanças na rede, o protocolo STP será executado novamente de forma automática. Este protocolo permite o uso de caminhos redundantes, sem que haja qualquer problema de mau funcionamento nas redes.

2.3.4 Protocolo CDP (Cisco Discovery Protocol)

O CDP é um protocolo desenvolvido pela Cisco Systems para fazer o gerenciamento de seus dispositivos, este protocolo mantêm as informações dos equipamentos. É utilizado para compartilhar informações dos equipamentos com seus vizinhos, como o endereço IP e a versão do sistema operacional, estas informações são utilizadas para fazer o mapeamento da rede (RODRIGUEZ, 2009).

Periodicamente o CDP envia mensagens multicast com o status do dispositivo e suas configurações. O dispositivo escuta as mensagens enviadas por outros dispositivos, com isto, determina o status das interfaces de outros dispositivos da rede (RODRIGUEZ, 2009).

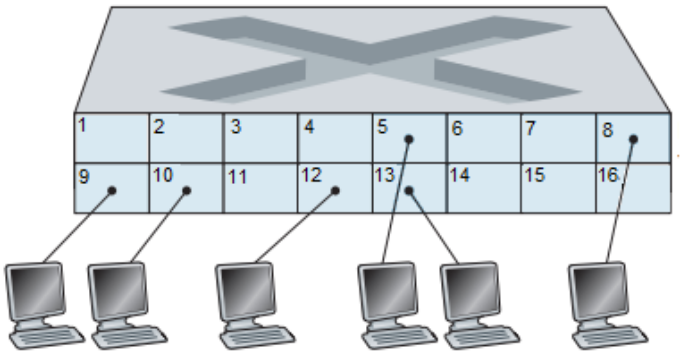
2.3.5 Switch

O switch é um equipamento que permite conectar várias redes locais ou diversos dispositivos de rede em suas portas. Sua principal função é encaminhar os quadros somente para o destino que foi endereçada, ou seja, se o computador 1 enviar dados para o computador 2, o switch encaminhara os dados apenas para o computador 2 (WHITE, 2012).

Para conseguir enviar as mensagens apenas para seu destino, os switches são capazes de aprender sobre os dispositivos que estão conectados em suas portas. Quando um dispositivo envia um quadro, o switch verifica o endereço MAC de origem da mensagem, e o armazena em sua tabela CAM (Content Addressable Memory) o endereço MAC e a porta do switch pela qual mensagem chegou (TORRES, 2014).

Toda vez que houver o envio de quadros, o switch verifica o endereço de destino do quadro e consulta sua tabela CAM, se o endereço MAC de destino estiver na tabela, enviará a mensagem pela porta que está associada ao endereço MAC. Caso o endereço MAC de destino não esteja na tabela, o switch enviará uma mensagem broadcast na rede para localizar o dispositivo que possui o endereço MAC de destino, após o dispositivo de destino responder o switch adicionará em sua tabela CAM o endereço MAC e a porta, então enviará os quadros ao seu destino (TORRES, 2014). A Figura 4 mostra um switch que aprendeu, os dispositivos que estão conectados em suas portas.

Caso o switch fique sem receber dados de algum endereço MAC por um período de tempo, este endereço MAC será eliminado da tabela, ao se fazer isto, permite que a estrutura



MAC	PORTA
2E-C9-D3-42-62-16	5
2E-C9-D3-42-62-17	8
2E-C9-D3-42-62-18	9
2E-C9-D3-42-62-19	10
2E-C9-D3-42-62-20	12
2E-C9-D3-42-62-21	13

Figura 4 – Switch e sua tabela CAM.
Adaptado de: (KUROSE; ROSS, 2014).

física da rede seja alterada e que o switch continue com sua capacidade de aprender, pois o tamanho de sua tabela interna é limitada (TORRES, 2014).

Os switches podem ser classificados quanto ao método de encaminhamento dos pacotes utilizado: *cut through* e *store-and-forward*. O switch do tipo *cut through* ao receber o quadro apenas verifica os endereços de origem e de destino, então reencaminha o quadro para o seu destino, este modo de operação garante uma rápida transmissão dos quadros. Os do tipo *store-and-forwar* esperam o quadro todo chegar, verificam se o quadro possui algum erro, caso não contenha erro o reencaminha para o seu destino, este modo de operação a transmissão de dados é mais lenta, mas garante uma transmissão com menos erros (MAIA, 2013).

2.3.6 Rede de Área Local Virtual (VLAN)

A VLAN é um recurso disponível nos switches que permite criar diversas redes locais virtuais dentro de uma mesma rede local real de forma a agrupar determinados usuários e dispositivos de rede. Os dispositivos que estão na mesma VLAN pode se comunicar entre eles normalmente, mas não podem se comunicar diretamente com dispositivos que estão em outra VLAN. Com a criação de VLANs o tráfego de broadcast fica limitado dentro delas, pois aumentam o número de domínios de broadcast (MAIA, 2013; KUROSE; ROSS, 2014).

Dentro de uma empresa que possui os departamentos de financeiro e de desenvolvimento, não é necessário que os dispositivos desses departamentos troquem informações, então cria-se uma VLAN para cada departamento separando os dispositivos,

evitando que informações sigilosas sejam acessadas por dispositivos que não possuem a devida permissão.

Para que dois dispositivos que estão conectados em switches diferentes possam estar na mesma VLAN, é utilizada a abordagem de entroncamento de VLANs, que permite os switches compartilharem suas VLANs com outros switches. As portas que conectam os switches são configuradas com portas de tronco, essas portas pertencem a todas as VLANs, é por elas que os quadros de uma VLAN fluem entre os switches. Para que os switches saibam ha qual VLAN os quadros pertencem, é utilizado o campo 802.1Q, este campo contém a informação sobre qual VLAN os quadros estão destinados (KUROSE; ROSS, 2014). O entroncamento de VLANs permite criar e utilizar VLANs independentemente da arquitetura física da rede.

A Figura 5 demonstra as VLANs dos departamentos financeiro e de desenvolvimento sendo compartilhadas entre dois swiches, permitindo que dispositivos em locais físicos distantes estejam na mesma VLAN.

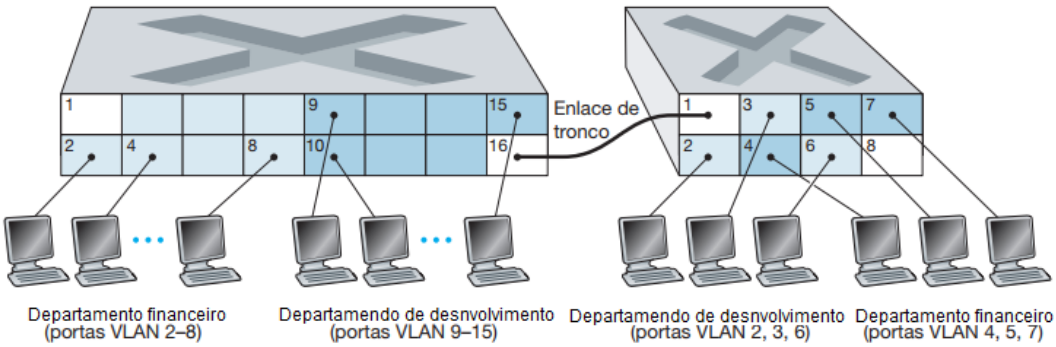


Figura 5 – Truncamento de VLANs.
Adaptado de: (KUROSE; ROSS, 2014).

2.4 ATAQUES NA CAMADA DE ENLACE

Os ataques na camada de enlace exploram o funcionamento normal dos protocolos e equipamentos, são difíceis de serem detectados quando ocorrem. Nesta sessão são apresentados os ataques mais comuns que ocorrem na camada de enlace.

2.4.1 Inundação de MAC

O atacante começa a enviar um grande número de quadros contendo diferentes endereços MAC, com o objetivo de encher a tabela interna do switch. Após a tabela interna do switch encher o mesmo passa a operar em modo broadcast, ou seja, todo quadro que chegar no switch será reenviado por todas as suas portas, então o atacante é capaz de capturar os quadros que chegam até ele e obter informações sigilosas (ANU; VIMALA, 2018). Na Figura 6 observamos o atacante utilizando a inundação de MAC para forçar o switch a operar em modo broadcast.

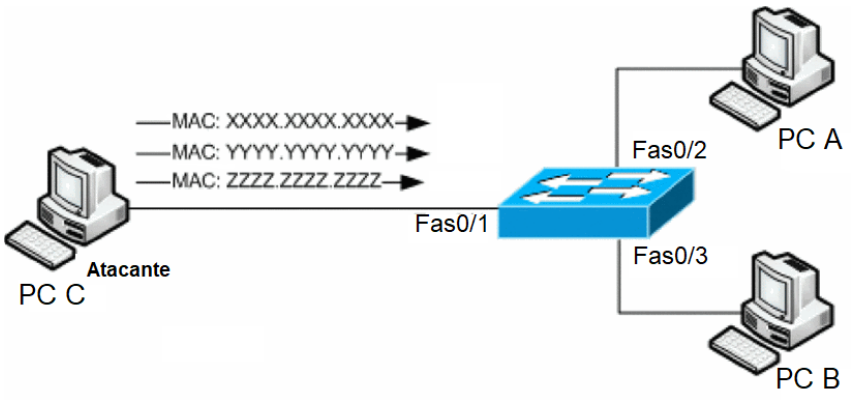


Figura 6 – Ataque por inundação de MAC.
Adaptado de: (ANU; VIMALA, 2018).

2.4.2 Falsificação de MAC

O atacante altera o seu endereço MAC e passa a utilizar o endereço MAC de outro dispositivo da rede, isto faz o switch redirecionar os quadros que estavam destinados a um dispositivo confiável para a porta que o atacante esta conectado. Isso possibilita que o atacante receba todas as informações que estavam destinas a outro dispositivo (ANU; VIMALA, 2018).

Na Figura 7 observamos o atacante falsificando o seu endereço MAC, diz para o switch que possui o endereço MAC do PC1. O switch atualiza sua tabela CAM colocando o endereço MAC do PC1 na porta Fa0/1, caso o PC2 envie uma mensagem para o PC1, o switch encaminhará a mensagem para a porta Fa0/1 onde o atacante está conectado.

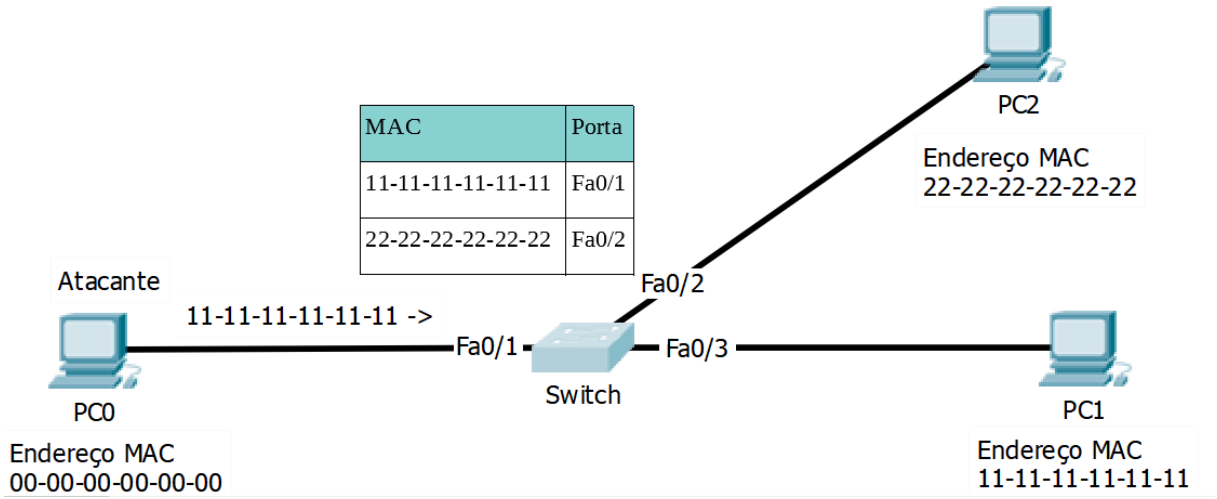


Figura 7 – Ataque de falsificação de MAC.
Fonte: Autoria própria.

2.4.3 DHCP Starvation

Este é um ataque de negação de serviço, onde o atacante envia um grande número de pacotes DHCP-DISCOVERY, com o objetivo de consumir todos os endereços IPs da rede. Como resultado o servidor DHCP fica sem endereços IPs para distribuir, então quando um novo dispositivo se conectar na rede, ele não recebera um IP, assim não poderá se comunicar com a rede (ANU; VIMALA, 2018).

2.4.4 Falsificação de DHCP

O atacante introduz um servidor de DHCP falso na rede. O servidor de DHCP real e o falso vão responder as solicitações de DHCP dos dispositivos da rede, aquele que responder primeiro fornece o endereço IP ao dispositivo. Caso o dispositivo receba um IP do servidor de DHCP falso, os dados enviados passarão primeiro pelo servidor de DHCP falso, que em seguida envia para o servidor DHCP real. Assim o atacante pode capturar todos os dados confidenciais dos dispositivos (ANU; VIMALA, 2018).

2.4.5 Falsificação de ARP

O protocolo ARP não possui métodos de autenticação, portanto pode ser facilmente falsificado. O atacante envia uma resposta ARP falsa para um dispositivo, dizendo que possui o IP de outro dispositivo, fazendo o dispositivo que recebeu a resposta ARP falsa, adicione em sua tabela ARP os dados falsos que recebeu. Quando o dispositivo atacado enviar dados para o dispositivo que realmente possui o IP que aprendeu errado, os dados passaram primeiro pelo atacante, que então os repassara para o dispositivo que realmente possui o IP. Caso queira saber os dados de retorno o atacante deve realizar o mesmo procedimento com o dispositivo de destino (ZDRNJA, 2009).

Na Figura 8 é possível observar que um pacote ARP falso foi enviado para o PC1 informando que o IP 10.0.0.4 possui o MAC CC-CC-CC-CC-CC-CC, também envia um pacote ARP falso para o PC2 dizendo que o IP 10.0.0.2 possui o MAC CC-CC-CC-CC-CC-CC. Isto faz a conversa dos PC1 e PC2 passar pelo atacante.

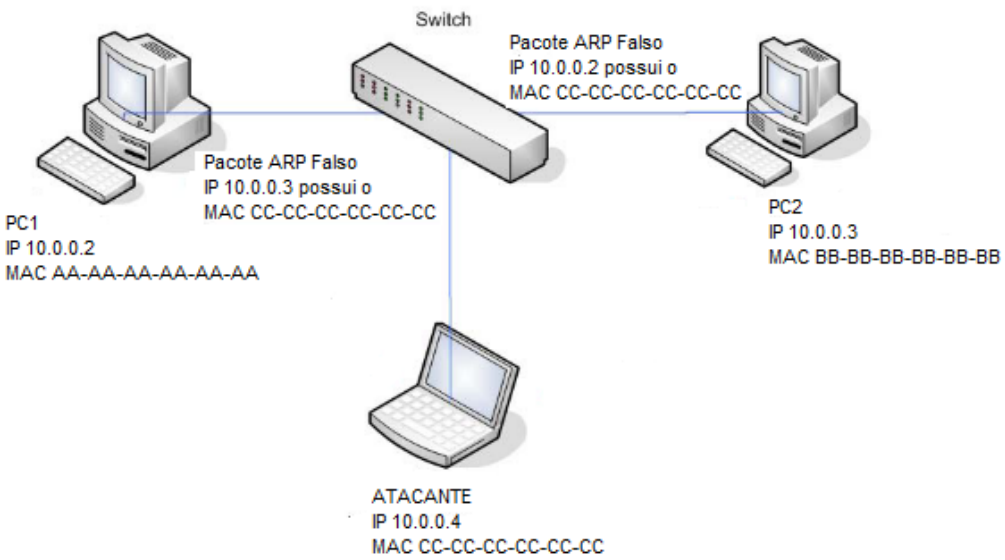


Figura 8 – Ataque por falsificação de ARP.
Adaptado de: (ANU; VIMALA, 2018).

2.4.6 Inundação do CDP

É um outro tipo de ataque de negação de serviço, onde o atacante envia diversos quadros CDP para o switch. O switch ao receber uma grande quantidade de quadros CDP, faz com que o uso do seu processador suba drasticamente, o que pode resultar no congelamento do sistema operacional (SHAHRIAR, 2017).

2.4.7 Manipulação de STP

No ataque de manipulação de STP o atacante tentará ser o novo switch raiz. Para virar o novo switch raiz o atacante envia quadros BPDUs (Bridge Protocol Data Units) falsos para os switches da rede. Isto força todos os switches a recalcular o STP. Todos os switches passam a considerar o atacante como o switch raiz, assim todo o tráfego da rede passara pelo atacante que tera acesso aos dados sigilosos (SHAHRIAR, 2017).

2.4.8 VLAN Hopping

Neste ataque o atacante que está em uma VLAN consegue se comunicar e roubar informações sigilosas de um dispositivo em outra VLAN. Este ataque pode ser feito de duas maneiras.

Uma das maneiras que o ataque pode ser feito, o atacante se aproveita de uma configuração padrão dos switches, que para criar uma ligação de entroncamento é necessário que apenas um dos lados da conexão anuncie que é uma porta tronco, o atacante faz o seu computador parecer que é uma porta tronco, para conseguir criar uma ligação de entroncamento com o switch, ao conseguir a ligação obtêm acesso a todas as VLANs da rede. Na outra maneira, o atacante insere duas tags 802.1Q no quadro, com o objetivo de enganar os switches e fazê-los reenviar o quadro para a vítima que está em outra VLAN (MASON, 2011).

3 MATERIAL E MÉTODOS

Neste capítulo são descritos os materiais que são utilizados nos testes e o método que será empregado.

3.1 MATERIAL

Para o desenvolvimento deste trabalho será necessário a utilização de alguns hardwares e softwares.

3.1.1 Hardwares

- **Switch**: um switch modelo Catalyst 2960 foi utilizado;
- **Computadores**: Três computadores são utilizados no desenvolvimento dos testes. Um computador utiliza o sistema operacional Kali linux 64 bit, os outros dois computadores utilizam o sistema operacional Windows 8;
- **Router**: Um Router cisco 2811 foi utilizado. Os routers executam funções para o direcionamento do tráfego encaminhando pacotes de dados entre redes de computadores. Também pode ser configurado para funcionar como um servidor DHCP. Neste trabalho um Router é utilizado como um servidor DHCP.

3.1.2 Softwares

- **Yersinia**[1]: É uma ferramenta de segurança, que permite realizar ataques na camada de enlace. É uma estrutura sólida para analisar e testar as redes. Os ataques podem ser realizados nos seguintes protocolos:
  1. Spanning Tree Protocol (STP);
  2. Protocolo de descoberta da Cisco (CDP);
  3. Protocolo de Entroncamento Dinâmico (DTP);
  4. Protocolo de configuração dinâmica de hosts (DHCP);
  5. Protocolo Hot Standby Router (HSRP);
  6. 802,1q;
  7. 802,1x;
  8. Inter-Switch Link Protocol (ISL);
  9. Protocolo VLAN Trunking Protocol (VTP).

  Esta ferramenta foi utilizada na versão 0.8.2;

- **Macof**[2]: Faz parte do conjunto de ferramentas Dsniff, é utilizada para inundar o switch da rede com centenas de endereços MAC falsos. Foi utilizada a versão 2.4;

- **Wireshark**[3]: O Wireshark é um software que analisa e captura o tráfego de rede, organizando por protocolos. Com ele é possível monitorar a entrada e saída de dados de um computador, onde é possível verificar a origem e o destino dos dados, junto ao protocolo que está sendo utilizado.

- **Kali Linux**[4]: É um sistema operacional desenvolvido pela Offensive Security, para realizar testes forenses e de penetração digital. Contém diversas ferramentas que podem ser utilizadas para realizar diversos testes de segurança, como testes de penetração, pesquisa de segurança, computação forense e engenharia reversa. As ferramentas Yersinia, Wireshark e Macof já vem instaladas no Kali linux. Foi utilizada a versão 2018.a de 64 Bits.

[1] https://github.com/tomac/yersinia
[2] https://www.monkey.org/~dugsong/dsniff/
[3] https://www.wireshark.org/
[4] https://www.kali.org/

3.2 MÉTODOS

Com os hardwares foi montada uma rede local experimental em laboratório conforme a Figura 9, onde o computador com o Kali Linux é o atacante, o PC-A e o PC-B são usuários da rede, o router será o servidor DHCP que fornecera IPs para a rede e o switch conecta todos os dispositivos da rede.

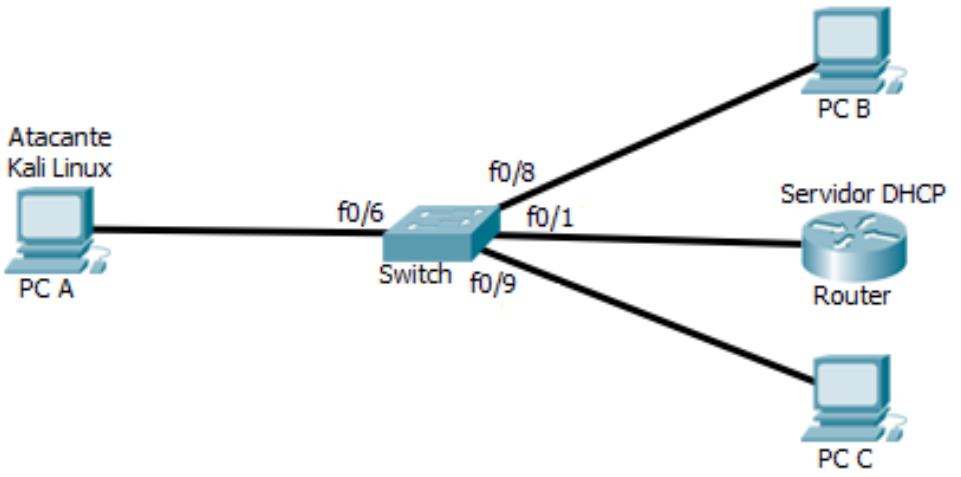


Figura 9 – Configuração da rede local utilizada no teste.
Fonte: Autoria própria.

Dos ataques descritos, os ataques de inundação de CDP, inundação de MAC, VLAN Hopping, DHCP starvation, falsificação de DHCP foram realizados a partir do computador com Kali Linux, com o objetivo de interceptar a comunicação entre os PC-A e PC-B ou de paralisar a rede. Após o término dos ataques foi mostrado o efeito que cada um teve sobre a rede. Os ataques ocorreram da seguinte maneira:

- **Inundação de MAC**: Utilizando a ferramenta Macof o ataque foi realizado com uma duração de sessenta segundos;
- **Inundação do CDP**: Utilizando a ferramenta Yersinia o ataque foi realizado com uma duração de cinco minutos;
- **VLAN Hopping**: Utilizando a ferramenta Yersinia o ataque foi realizado pelo modo onde o atacante se passa por uma porta de tronco;
- **DHCP Starvation**: Utilizando a ferramenta Yersinia foi consumido todos os endereços IPs da rede. O ataque tem uma duração de sessenta segundos;

- **Falsificação de DHCP**: Utilizando a ferramenta Yersinia foi criado um servidor DHCP falso com as seguintes configurações:
    1. ID do servidor: 192.168.1.1;
    2. IP Inicial: 192.168.1.10;
    3. IP final: 192.168.1.100;
    4. Tempo de resposta (seg): 1;
    5. Tempo para renovar o IP (seg): 50000;
    6. Sub-rede: 255.255.255.0;
    7. Rota: 192.168.1.2;
    8. DNS: 192.168.1.3;
    9. Domínio: rede.segura.

Após cada ataque realizado é verificado o seu efeito na rede. Então no switch são configurado mecanismos de segurança para cada um dos ataques. Após a configuração dos mecanismos de segurança os ataques são realizados novamente, então é verificado a eficácia desses mecanismos de segurança. A avaliação da eficácia dos mecanismos de segurança, é feita analisando se os ataques foram bem-sucedidos ou não após a configuração dos mecanismos de segurança.

4 RESULTADOS E DISCUSSÃO

Neste capítulo são relatados os ataques e configurado medidas de segurança para mitigar as ameaças, prevenindo ataques à camada de enlace, por fim, é levantado e discutido os resultados obtidos.

4.1 INUNDAÇÃO DE MAC

O ataque por inundação de MAC, se concretiza ao enviar milhares de quadros Ethernet com endereços MAC de origem aleatórios, com o objetivo de encher a tabela CAM do switch e alterar seu modo de funcionamento.

4.1.1 Realização do ataque por inundação de MAC

O ataque por inundação de MAC foi realizado na estrutura de rede demonstrada na figura 9, com o objetivo de verificar a vulnerabilidade existente no switch e a efetividade deste ataque. Antes de iniciar o ataque, foi verificado quantos endereços MAC o switch aprendeu e armazenou em sua tabela CAM. Observa-se que o switch aprendeu apenas quatro endereços MAC, e ainda pode aprender outros 7996 endereços MAC (Figura 10).

No PC A utilizando a ferramenta Macof, foi iniciado o ataque de inundação de MAC com a duração de sessenta segundos. Ao término do ataque, verificou-se que a tabela CAM ficou completamente cheia (Figura 11), portanto, impossibilitando o registro de novos endereços MAC. Nesta situação, o switch passa a operar em modo broadcast, reencaminhando os dados que chegam para todos os dispositivos conectados a ele.

```
Mac Entries for Vlan 1:
------------------------
Dynamic Address Count   : 4
Static  Address Count   : 0
Total Mac Addresses     : 4

Total Mac Address Space Available: 7996
```

Figura 10 – Tabela CAM do switch antes do ataque.
Fonte: Autoria própria.

```
Mac Entries for Vlan 1:
------------------------
Dynamic Address Count   : 8000
Static  Address Count   : 0
Total Mac Addresses     : 8000

Total Mac Address Space Available: 0
```

Figura 11 – Tabela CAM do switch após o ataque.
Fonte: Autoria própria.

Para verificar se o ataque obteve sucesso, foi criada uma comunicação entre o PC B e PC C utilizado o comando ping. No PC A utilizando a ferramenta Wireshark foi possível capturar os pacotes da comunicação que foi realizada entre os computadores, então os pacotes com origem no PC B que possui o IP 192.168.13.151 e destinados ao PC C que possui o IP 192.168.13.152 foram capturados pelo PC A (Figura 12). O switch operou em modo brodcast reenviando os pacotes que estavam destinados ao PC C para todos os dispositivos da rede, permitindo o atacante obter os dados que estão trafegando na rede.

No.	Time	Source	Destination	Protocol	Length	Info
3384…	491.597075359	192.168.13.151	192.168.13.152	ICMP	74	Echo (ping) reply
3384…	492.600333322	192.168.13.151	192.168.13.152	ICMP	74	Echo (ping) reply
3384…	493.603930770	192.168.13.151	192.168.13.152	ICMP	74	Echo (ping) reply
3384…	494.607522357	192.168.13.151	192.168.13.152	ICMP	74	Echo (ping) reply
3384…	495.611362013	192.168.13.151	192.168.13.152	ICMP	74	Echo (ping) reply

Figura 12 – Pacotes capturados da comunicação entre o PC B e o PC C.
Fonte: Autoria própria.

4.1.2 Mitigando o ataque por inundação de MAC

Para mitigar o ataque de inundação de MAC foi utilizado o recurso de segurança port-security para restringir o acesso nas portas do switch. Para ativar a segurança no switch foram utilizados os seguintes comandos:

1. “interface fastethernet range 0/1 – 24” para acessar todas as portas fastethernet do switch;
2. “switchport port-security” para ativar a segurança das portas;
3. “switchport port-security maximum 1” para limitar em um o número de endereços MAC que cada porta do switch pode aprender;
4. “switchport port-security violtion restrict” para ignorar os endereços MAC, após o limite da porta ser atingido.

Para testar a eficácia desta proteção, o ataque de inundação de MAC é realizado novamente a partir do PC A utilizando a ferramenta macof com duração de sessenta segundos. Após o termino do ataque foi verificado a tabela CAM do switch, agora o switch aprendeu poucos endereços MAC (Figura 13), o que demonstra que o ataque não obteve sucesso.

```
Mac Entries for Vlan 1:
---------------------------
Dynamic Address Count  : 4
Static  Address Count  : 0
Total Mac Addresses    : 4

Total Mac Address Space Available: 7996
```

Figura 13 – Tabela CAM do switch com segurança após o ataque.
Fonte: Autoria própria.

Utilizando o comando “show port-security interface fastethernet [número da porta]” foi acessado a porta do switch que o PC A está conectado, para verificar quantos endereços MAC foram aprendidos nesta porta e se ocorreu alguma violação. Na figura 14 é possível observar que a porta aprendeu apenas um endereço MAC e que ocorreram 10095 violações, ou seja 10095 endereços MAC foram ignorados.

```
Switch1#show port-securit interface fastEthernet 0/6
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 7c33.c41a.7b53:1
Security Violation Count   : 10095
```

Figura 14 – Informações da porta que recebeu o ataque.
Fonte: Autoria própria.

4.1.3 Análise dos resultados dos testes para o ataque de inundação de MAC

O teste realizado do ataque por inundação de MAC, demonstra que o ataque foi eficaz, permitindo que o atacante possa capturar os pacotes da rede, e com isto obter dados e informações sigilosas.

Já o teste de segurança, demonstra que limitar o número de endereços MAC em cada porta do switch pode aprender, aliado a restrição de ignorar novos endereços MAC após o limite da porta ser atingido, consegue mitigar a ameaça da inundação de MAC. Com esta proteção sendo aplicada no switch pode-se afirmar que o ataque de inundação de MAC foi mitigado com sucesso.

4.2 INUNDAÇÃO DE CDP

O ataque por inundação de CDP consiste em enviar milhares de quadros CDP falsos para o switch, com o objetivo de aumentar o uso do processador do switch, causando lentidão, podendo até paralisar temporariamente o funcionamento do switch.

4.2.1 Realização do ataque por inundação de CDP

O ataque por inundação de CDP é realizado na estrutura de rede que foi apresentada na figura 9, com o objetivo de verificar a vulnerabilidade existente no switch e a efetividade deste ataque. Antes de iniciar o ataque, no switch é utilizado o comando "show processes cpu" para verificar a utilização do processador, na figura 15 podemos observar que o switch está utilizando apenas 5% do processador.

```
CPU utilization for five seconds: 5%/0%; one minute: 7%; five minutes: 5%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           0         3          0  0.00%  0.00%  0.00%   0 Chunk Manager
   2           0       100          0  0.00%  0.00%  0.00%   0 Load Meter
   3           0        19          0  0.00%  0.00%  0.00%   0 SpanTree Helper
```

Figura 15 – Utilização do processador antes do ataque.
Fonte: Autoria própria.

Utilizando a ferramenta Yersinia no PC A, foi iniciado o ataque de inundação de CDP com duração de 5 minutos. Antes de encerrar o ataque a utilização do processador do switch aumentou para 99% de utilização (Figura 16), o que pode causar sérios prejuízos ao switch, podendo até paralisar o seu sistema operacional.

```
CPU utilization for five seconds: 99%/28%; one minute: 99%; five minutes: 97%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           0         3          0  0.00%  0.00%  0.00%   0 Chunk Manager
   2          25       672         37  0.00%  0.00%  0.00%   0 Load Meter
   3           0        23          0  0.00%  0.00%  0.00%   0 SpanTree Helper
```

Figura 16 – Utilização do processador durante o ataque.
Fonte: Autoria própria.

4.2.2 Mitigando o ataque por inundação de CDP

Para mitigar o ataque de inundação de CDP, foi desativado o protocolo CDP no switch utilizando os seguintes comandos:

1. "interface fastethernet range 0/1 – 24" para acessar todas as portas fastethernet do switch;
2. "no cdp enable" para desativar o CDP em cada uma das portas do switch.

Para testar a eficácia desta proteção, o ataque de inundação de CDP é realizado novamente a partir do PC A utilizando Yersinia. Observa-se que a utilização do processador do switch ficou em 5% de utilização (Figura 17).

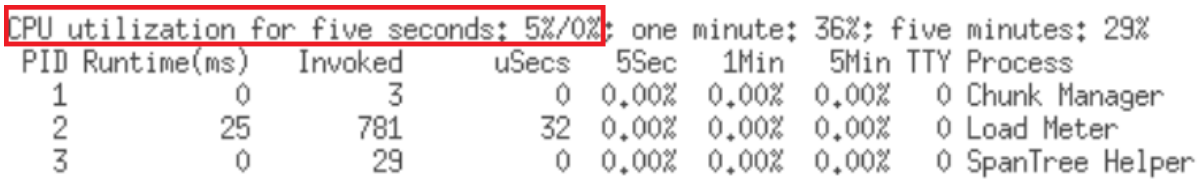


Figura 17 – Utilização do processador com segurança durante o ataque.
Fonte: Autoria própria.

4.2.3 Análise dos resultados dos testes para o ataque de inundação de CDP

O teste do ataque por inundação de CDP, demonstra que o ataque foi eficaz, fazendo o processador do switch ser utilizado ao máximo. Se este ataque for realizado em uma grande rede, pode causar lentidão, travamentos e se realizado por um longo período de tempo pode até queimar o aparelho por excesso do uso de seu processador.

O teste da segurança, demonstra que a desativação do protocolo CDP utilizando o comando “no cdp enable” consegue mitigar com sucesso o ataque de inundação de CDP. Ao se utilizar esta proteção em todas as portas que não possuem switches conectados, pode-se afirmar que o ataque de inundação de CDP foi mitigado com sucesso nas portas do switch.

4.3 VLAN HOPPING

O ataque de VLAN Hopping consiste na tentativa do atacante obter acesso as vlans que ele não possui autorização de acesso.

4.3.1 Realização do ataque de VLAN hopping

O ataque de VLAN hopping foi realizado na estrutura de rede apresentada na figura 9, com o objetivo de verificar a efetividade deste ataque, bem como a vulnerabilidade existente no switch. Antes de iniciar o ataque, foi verificado se o switch possui alguma porta de tronco utilizando o comando ”show interface trunk’, não houve retorno ao se utilizar o comando, o que significa que o switch não possui portas de tronco com nenhum outro dispositivo.

Para este teste foram criadas duas vlans no switch, a vlan 10 e a vlan 20, onde o PC A foi colocado na vlan 10 e o PC B e PC C colocados na vlan 20. O PC A que tem o endereço IP 192.168.13.150 e está na vlan 10 tenta se comunicar com o PC C que tem o endereço IP 192.168.13.152 e que está na vlan 20 através do comando de ping, na figura 18 pode-se verificar que o PC A não conseguiu se comunicar com o PC C por estarem em vlans diferentes.

```
root@DESKTOP-3448PNV:~# ping 192.168.13.152
PING 192.168.13.152 (192.168.13.152) 56(84) bytes of data.
From 192.168.13.1 icmp_seq=1 Destination Host Unreachable
From 192.168.13.1 icmp_seq=2 Destination Host Unreachable
From 192.168.13.1 icmp_seq=3 Destination Host Unreachable
```

Figura 18 – Ping do PC A com o PC C sem comunicação.
Fonte: Autoria própria.

Utilizado a ferramenta Yersinia no PC A foi iniciado o ataque de vlan hopping pelo método de truncamento, onde o atacante finge ser um switch para obter acesso a todas as vlans da rede. Conforme observado na figura 19 a ferramenta Yersinia conseguiu estabelecer uma conexão de tronco com o switch, assim o switch passa a compartilhar suas vlans com o atacante, que obtêm acesso a todas as vlans da rede.

Neighbor-ID	Status	Domain	Interface	Count
6C504DF60E06	04 ACCESS/AUTO		eth0	1
0C7CE846D595	03 ACCESS/DESIRABLE		eth0	3
6C504DF60E06	84 TRUNK/AUTO		eth0	6
0C7CE846D595	83 TRUNK/DESIRABLE		eth0	3

Figura 19 – Yersinia estabelecendo a conexão de tronco com o switch.
Fonte: Autoria própria.

Após o ataque ser iniciado, é verificado novamente se o switch possui portas de tronco,

na figura 20 observa-se que agora o switch possui uma porta de tronco, na porta fastethernet 0/6 onde o PC A esta conectado.

```
Port        Mode             Encapsulation  Status        Native vlan
Fa0/6       auto             802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/6       1-4094

Port        Vlans allowed and active in management domain
Fa0/6       1,10,20

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/6       1,10,20
```

Figura 20 – Portas de tronco do switch após o ataque por VLAN Hopping.
Fonte: Autoria própria.

Novamente o PC A que agora possui acesso a todas as vlans, tenta se comunicar com o PC C que está na vlan 20 através do comando de ping, agora a comunicação entre os computadores foi possível conforme mostrado na figura 21, onde o comando de ping disparado no PC A conseguiu se comunicar com o PC C, sendo assim o ataque foi um sucesso.

```
root@DESKTOP-3448PNV:~# ping 192.168.13.152
PING 192.168.13.152 (192.168.13.151) 56(84) bytes of data.
64 bytes from 192.168.13.152: icmp_seq=1 ttl=128 time=0.551 ms
64 bytes from 192.168.13.152: icmp_seq=2 ttl=128 time=0.347 ms
64 bytes from 192.168.13.152: icmp_seq=3 ttl=128 time=0.349 ms
```

Figura 21 – PC A se comunicando com o PC B.
Fonte: Autoria própria.

4.3.2 Mitigando o ataque de VLAN hopping

Para mitigar de VLAN Hopping foi desativado a negociação do truncamento, no switch foram utilizados os seguintes comandos:

1. “interface fastethernet range 0/1 – 24” para acessar todas as portas fastethernet do switch;
2. “switchport mode access” para indicar que se trata de uma porta de acesso onde se conectarão hosts e não outros switches;
3. “switchport nonegotiate” para desativar negociação do truncamento.

Para testar a eficácia dessa proteção, o ataque de VLAN Hopping foi realizado novamente a partir do PC A utilizando a ferramenta Yersinia, na figura 22 observa-se que a ferramenta Yersinia não conseguiu estabelecer uma conexão de tronco pois teve o acesso negado pelo switch.

0C7CE846D595	03 ACCESS/DESIRABLE		eth0	4
6C504DF60E06	84 TRUNK/AUTO		eth0	10
0C7CE846D595	83 TRUNK/DESIRABLE		eth0	7
6C504DF60E06	02 ACCESS/OFF		eth0	1

Figura 22 – Switch negando conexão de tronco com o atacante.
Fonte: Autoria própria.

Para confirmar que o ataque não obteve sucesso, foi verificado se o switch possui alguma porta de tronco utilizando o comando ”show interface trunk’, não houve retorno ao se utilizar o comando, o que significa que o switch não possui portas de tronco com nenhum outro dispositivo, ou seja, o ataque foi mitigado.

4.3.3 Análise dos resultados dos testes para o ataque de VLAN hopping

O teste do ataque realizado, demonstra que o ataque de VLAN Hopping obteve sucesso, permitindo que o atacante obtivesse acesso a todas as vlans da rede, assim o atacante pode se comunicar com qualquer dispositivo da rede mesmo que ele não possua autorização.

O teste da segurança demonstra que, indicar que se trata de uma porta de acesso onde se conectarão hosts e desativar a negociação de tronco, consegue mitigar com sucesso o ataque de VLAN Hopping. Com essa proteção sendo aplicada em todas as portas que não possuem switches conectados é possível afirmar que o ataque de VLAN Hopping foi mitigado com sucesso.

4.4 DHCP STARVATION

O ataque de DHCP starvation, consiste no atacante enviar centenas de requisições DHCP DISCOVER com endereços MAC falsos até consumir todos os endereços IP que estão disponíveis no servidor.

4.4.1 Realização do ataque de DHCP Starvation

Para verificar a vulnerabilidade existente no switch que permite o ataque bem como sua efetividade, foi realizado um teste na estrutura de rede que foi apresentada na figura 9. Antes de iniciar o ataque foi verificado as estatísticas do servidor DHCP, o servidor recebeu três mensagens DHCP-DISCOVER e enviou três mensagens DHCP-OFFER, estas mensagens são referentes as requisições de IP feitas pelos três computadores que estão conectados na rede (Figura 23).

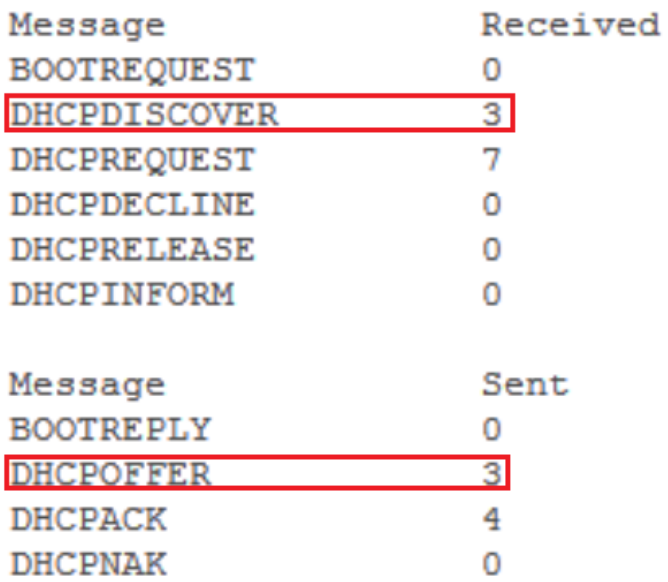
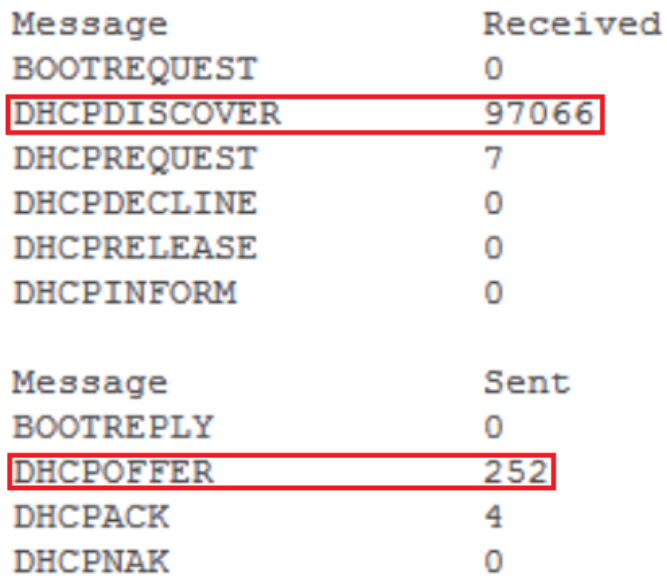


Figura 23 – Estatística do servidor DHCP antes do ataque.
Fonte: Autoria própria.

No PC A utilizando a ferramenta Yersinia foi iniciado o ataque de DHCP starvation com uma duração de sessenta segundos. Após se passar este tempo o ataque foi encerado,

então novamente foi verificado as estatísticas do servidor DHCP, observa-se que o servidor recebeu 97066 mensagens DHCP-DISCOVER e enviou 252 mensagens DHCP-OFFER, ou seja, o servidor forneceu todos os endereços IP que tinha disponível (Figura 24). Agora se um novo dispositivo se conectar na rede não receberá um endereço IP.



Message	Received
BOOTREQUEST	0
DHCPDISCOVER	97066
DHCPREQUEST	7
DHCPDECLINE	0
DHCPRELEASE	0
DHCPINFORM	0

Message	Sent
BOOTREPLY	0
DHCPOFFER	252
DHCPACK	4
DHCPNAK	0

Figura 24 – Estatística do servidor DHCP depois do ataque.
Fonte: Autoria própria.

4.4.2 Mitigando o ataque de DHCP Starvation

O método para mitigar o ataque de DHCP starvation é o mesmo utilizado no ataque de inundação de MAC, que consiste em restringir o acesso nas porta do switch. Para restringir o acesso foram utilizados dos seguintes comandos no switch:

1. “interface fastethernet range 0/1 – 24” para acessar todas as portas fastethernet do switch;
2. “switchport port-security” para ativar a segurança das portas;
3. “switchport port-security maximum 5” para limitar em cinco o número de MAC que cada porta do switch pode aprender;
4. “switchport port-security violtion restrict” para ignorar os endereços MAC, após o limite da porta ser atingido.

Para testar a eficácia desta proteção, o ataque de DHCP starvation foi realizado novamente com uma duração de sessenta segundos. Após se passar este tempo o ataque foi

encerado, então foi verificado as estatísticas do servidor DHCP, observa-se que o servidor recebeu apenas sete mensagens DHCP-DISCOVERY e enviou sete mensagens DHCP-OFFER (Figura 25), ou seja, o servidor forneceu apenas sete endereços IP.

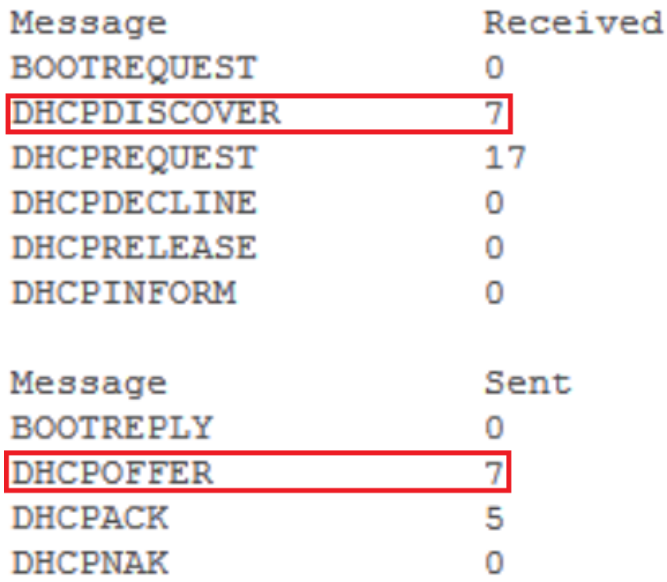


Figura 25 – Estatística do servidor DHCP após o teste da proteção.
Fonte: Autoria própria.

4.4.3 Análise dos resultados dos testes para o ataque de DHCP Starvation

O ataque realizado, demonstra que o atacante conseguiu consumir todos os endereços IP disponíveis no servidor DHCP, assim os novos dispositivos que se conectarem na rede, não vão receber um endereço IP e com isto não poderão utilizar a rede.

O teste do mecanismo de segurança, demonstra que limitar o número de endereços MAC em cada porta do switch pode aprender, aliado a restrição de ignorar novos endereços MAC após o limite da porta ser atingido, consegue mitigar a ameaça de DHCP Starvation. Com esta proteção sendo aplicada no switch, o atacante não conseguirá consumir todos os endereços IP que disponíveis no servidor DHCP, então pode-se afirmar que o ataque de DHCP Starvation foi mitigado com sucesso.

4.5 FALSIFICAÇÃO DE DHCP

A falsificação de DHCP consiste no atacante criar e inserir um servidor DHCP falso na rede.

4.5.1 Realização do ataque de falsificação de DHCP

O teste do ataque de falsificação de DHCP foi realizado na estrutura de rede apresentada na figura 9, com objetivo de verificar a efetividade deste ataque e a vulnerabilidade que permite a realização deste ataque.

No PC A utilizando a ferramenta Yersinia, foi criado um servidor DHCP utilizando os seguintes parâmetros:

- IP do servidor: 192.168.1.1;
- IP inicial: 192.168.1.10;
- IP final: 192.168.1.100;
- Tempo de resposta (seg): 1;
- Tempo para renovar o IP (seg): 50000;
- Máscara de sub-rede: 255.255.255.0;
- Gateway padrão: 192.168.1.2;
- Servidor DNS: 192.168.1.3;
- Domínio: rede.segura.

Após o servidor DHCP falso ser configurado e iniciado, o PC B foi ligado na rede sem possuir um endereço IP, após o PC B requisitar e receber um endereço IP, no prompt de comando foi utilizado o comando “ipconfig” para verificar a configuração de IP do PC B. Observa-se que o PC B possui o endereço IP 192.168.1.10 e o gateway padrão 192.168.1.2 (Figura 26), ou seja recebeu o endereço IP do servidor DHCP falso.

```
Sufixo DNS específico de conexão. . . . . : rede.segura
Endereço IPv6 de link local . . . . . : fe80::81a2:494e:4ca6:9ee0%7
Endereço IPv4. . . . . . . . . . . . : 192.168.1.10
Máscara de Sub-rede . . . . . . . . . . . : 255.255.255.0
Gateway Padrão. . . . . . . . . . . . . : 192.168.1.2
```

Figura 26 – Configuração de IP do PC B.
Fonte: Autoria própria.

4.5.2 Mitigando o ataque de DHCP Starvation

Para mitigar o ataque de falsificação de DHCP foi utilizado o recurso DHCP Snooping para configurar a porta onde o servidor DHCP verdadeiro está conectado como confiável e as portas restantes como não confiáveis. Para configurar as portas do switch com o recurso DHCP Snooping foram utilizados os seguintes comandos no switch:

1. “ip dhcp snooping” para ativar o recurso no switch, por padrão todas as portas são configuradas como não confiáveis ao se ativar o recurso;
2. “ip dhcp snooping vlan <nome vlan>” para ativar a proteção na vlan, deve ser utilizado para cada vlan existente;
3. “interface fastethernet range 0/2 – 24” para acessar as portas que não possuem o servidor DHCP;
4. “ip dhcp snooping limite rate 5” para limitar em cinco o número de requisições DHCP que as portas não confiáveis podem receber em pacotes por segundo;
5. “interface fastethernet 0/1” para acessar a porta que o servidor DHCP esta conectado;
6. “ip dhcp snooping trust” para configurar a porta como confiável.

Para testar a eficiência deste recurso, o servidor DHCP verdadeiro foi desligado da rede e o servidor DHCP falso iniciado, novamente o PC B foi ligado na rede sem possuir um endereço IP, agora o PC B não obteve um endereço IP conforme demonstrado na figura 27.

```
Sufixo DNS específico de conexão. . . . . :
Endereço IPv6 de link local . . . . . : fe80::81a2:494e:4ca6:9ee0%7
Gateway Padrão. . . . . . . . . . . . . :
```

Figura 27 – Configuração de IP do PC B após o teste de segurança.
Fonte: Autoria própria.

4.5.3 Análise dos resultados dos testes para o ataque de DHCP Starvation

O ataque de falsificação de DHCP, demonstrou que o atacante consegue criar e inserir um servidor DHCP falso na rede e fornecer endereços IP para os dispositivos que requisitarem um. Com a execução deste ataque é possível causar uma negação de serviço, pois todos os dispositivos que receberem o endereço IP do servidor DHCP falso não conseguirão utilizar serviços que necessitem um endereço IP válido.

O teste de segurança demonstra que, utilizar o recuso DHCP Snooping para indicar quais portas são confiáveis e quais não são confiáveis, o que faz descartar as mensagens DHCP-OFFER e DHCP-ACK nas portas não confiáveis. Se todas as portas do switch que possuem servidores DHCP verdadeiros ou outros switches conectados forem configuradas como confiáveis e as portas restantes como não confiáveis, pode-se afirmar que o ataque de falsificação de DHCP foi mitigado com sucesso.

5 CONCLUSÃO

Neste trabalho foram descritas algumas das principais ameaças presentes na camada de enlace de dados que trazem risco a segurança das redes de computadores. Buscando mitigar estas ameaças, propõem a identificação e implementação de mecanismos de segurança.

Na revisão bibliográfica são descritas informações importantes de como funcionam alguns dos protocolos e alguns dos ataques existentes na camada de enlace de dados, a fim de compreender o funcionamento destas ameaças, para investigar os meios necessários para mitigar estas ameaças e trazer segurança para as redes de computadores.

Foi possível verificar que os ataques são executados de maneira simples em uma rede local que não possui mecanismos de segurança, o que enfatiza a necessidade de se implementar medidas de segurança, bem como a importância deste trabalho.

As medidas encontradas conseguiram mitigar com sucesso os ataques. Com todas medidas de segurança sendo aplicadas, é possível afirmar que a rede interna ficou mais segura, pois os ataques passaram a ser mitigados.

Pode-se observar que todas as medidas utilizadas para mitigar os ataques, já estavam presentes no switch utilizado, bastando apenas ativar e configurar estas medidas, o que demostra que a fabricante deste switch já esta ciente das ameaças que ocorreram na camada de enlace de dados e consequentemente fornece as medidas necessárias para mitigar os ataques que possam vir a ocorrer, ao se observar a documentação de switches de outras fabricantes como HP, Huawei, 3Com, Dell percebe-se que elas oferecem mecanismos de segurança similares aos apresentados neste trabalho. Como as medidas de segurança ja estão presentes nos switches, não é necessário investir para melhorar a segurança da camada de enlace de dados.

5.1 TRABALHOS FUTUROS

Para trabalhos futuros propõe-se, realização e mitigação dos ataques de falsificação de MAC, falsificação de ARP e manipulação de SPT. Também recomenda-se o estudo sobre ataques externos a rede, bem como mecanismos para mitigar estes ataques.

REFERÊNCIAS

ANU, P.; VIMALA, S. A survey on sniffing attacks on computer networks. **Proceedings of 2017 International Conference on Intelligent Computing and Control, I2C2 2017**, v. 2018-January, p. 1–5, 2018.

BEUKEMA, W. J. B.; ATTEMA, T.; SCHOTANUS, H. A. Internal Network Monitoring and Anomaly Detection through Host Clustering. **Proceedings of the 3rd International Conference on Information Systems Security and Privacy**, n. Icissp, p. 694–703, 2017.

BORA, G. et al. OSI Reference Model Networking : An Overview. **International Journal of Computer Trends and Technology**, v. 7, n. 4, p. 214–218, 2014. ISSN 2231-2803.

HUSSAIN, M. A. et al. ARP enhancement to stateful protocol by registering ARP request. **Proceedings - 2016 International Conference on Network and Information Systems for Computers, ICNISC 2016**, p. 31–35, 2017.

IBM. **An integrated approach to insider threat protection**. 2016. Disponível em: <https://www.ibm.com/downloads/cas/GRQQYQBJl>. Acesso em: 06 set. 2018.

JORDAO, M. **O Endereçamento MAC e sua importância em Redes**. 2014. Disponível em: <https://www.mundotibrasil.com.br/o-enderecamento-mac-e-sua-importancia-em-redes/>. Acesso em: 20 set. 2018.

KUROSE, J. F.; ROSS, K. W. **Redes de computadores e a internet - uma abordagem top-down**. 6. ed. [S.l.]: Pearson, 2014.

LI, Y. et al. Research based on OSI model. **2011 IEEE 3rd International Conference on Communication Software and Networks, ICCSN 2011**, p. 554–557, 2011.

MAIA, L. P. **Arquitetura de redes de computadores**. 2. ed. [S.l.]: Livros Técnicos e Científicos Editora Ltda, 2013.

MASON, A. **CCNP Security Secure 642-637 Quick Reference: Cisco Layer 2 Security**. 2011. Disponível em: <http://www.ciscopress.com/articles/article.asp?p=1681033&seqNum=3>. Acesso em: 06 out. 2018.

MENDES, D. R. **Redes de computadores Teoria e Pratica**. 2. ed. [S.l.]: novatec, 2015.

RAJPUT, A. K.; TEWANI, R.; DUBEY, A. The helping protocol "DHCP". **2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)**, p. 634–637, 2016.

RODRIGUEZ, S. Topology Discovery Using Cisco Discovery Protocol. **arXiv preprint arXiv:0907.2121**, v. 30, n. 9, p. 2032–2047, 2009.

SHAHRIAR, A. **Layer 2 Infrastructure Security(Attack Vectors)(Part 2)**. 2017. Disponível em: <https://www.linkedin.com/pulse/layer-2-infrastructure-securityattack-vectors-ahnaf-shahriar?trk=portfolio_article-card_title>. Acesso em: 30 set. 2018.

STALLINGS, W. **Criptografia e segurança de redes - princípios e práticas**. 6. ed. [S.l.]: Pearson, 2014.

TANENBAUM, A. S.; WETHERALL, D. **Redes De Computadores**. 5. ed. [S.l.]: Pearson, 2011.

TORRES, G. **Redes De Computadores**. 2. ed. [S.l.]: Nova Terra, 2014.

WHITE, C. M. **Redes de computadores e comunicação de dados**. 6. ed. [S.l.]: Cengage Learning, 2012.

ZDRNJA, B. Malicious JavaScript insertion through ARP poisoning attacks. **IEEE Security and Privacy**, v. 7, n. 3, p. 72–74, 2009.