TRABALHO DE GRADUAÇÃO

Segurança em ambientes virtualizados.
Análise do comportamento de redes virtuais a ataques de rede

Gabriel Lucena Ramos

Brasília, Julho de 2019

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

UNIVERSIDADE DE BRASÍLIA
Faculdade de Tecnologia

TRABALHO DE GRADUAÇÃO

Segurança em ambientes virtualizados. Análise do comportamento de redes virtuais a ataques de rede

Gabriel Lucena Ramos

Trabalho de Graduação submetido ao Departamento de Engenharia Elétrica como requisito parcial para obtenção do grau de Engenheiro de Redes de Comunicação

Banca Examinadora

Flávio Elias de Deus, Dr., ENE/UnB _____
Orientador

Robson de Oliveira Albuquerque, Dr., ENE/UnB _____
Coorientador

Georges Daniel Amvame Nze, Dr., ENE/UnB _____
Examinador Interno

FICHA CATALOGRÁFICA

RAMOS, GABRIEL LUCENA
Segurança em ambientes virtualizados. Análise do comportamento de redes virtuais a ataques de rede [Distrito Federal] 2019.
xvi, 70 p., 210 x 297 mm (ENE/FT/UnB, Engenheiro, Engenharia Elétrica, 2019).
Trabalho de Graduação - Universidade de Brasília, Faculdade de Tecnologia.
Departamento de Engenharia Elétrica

1. Virtualização	2. Segurança
3. Ataques	4. Rede Virtual
I. ENE/FT/UnB	II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

RAMOS, G. L. (2019). *Segurança em ambientes virtualizados. Análise do comportamento de redes virtuais a ataques de rede*. Trabalho de Graduação, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 70 p.

CESSÃO DE DIREITOS

Gabriel Lucena Ramos
Depto. de Engenharia Elétrica (ENE) - FT
Universidade de Brasília (UnB)
Campus Darcy Ribeiro
CEP 70919-970 - Brasília - DF - Brasil

Agradecimentos

Agradeço aos professores pela minha formação. Agradeço aos meus orientadores pela dedicação na orientação. Agradeço a minha família e amigos pelo apoio. Agradeço a Deus por me manter firme.

Gabriel Lucena Ramos

RESUMO

Palavras-chave: *Segurança, Virtualização, Redes Virtuais, Ataques*

A virtualização se desenvolveu muito nos últimos 10 anos. A expansão do uso de uma infraestrutura virtualizada e mais recentemente o uso das tecnologias de computação em nuvem dão uma grande visibilidade as tecnologias de virtualização e com isso novos ataques voltados a virtualização tem surgido. As redes virtuais trouxeram um novo modo de trabalho e com ele uma maior segurança contra-ataques já conhecidos. Contudo a adaptação de ataques voltados a rede física para as redes virtuais também ocorre e ataques já bem conhecidos podem ser executados em redes virtuais sem nenhum problema. Apesar dos esforços para criar soluções de virtualização seguras ainda existem vulnerabilidades com formas de prevenção conhecidas que podem ser facilmente exploradas em ambientes virtuais.

Este trabalho analisará o comportamento de duas soluções de virtualização (VMware vSphere ESXi e Microsoft Hyper-V) em relação a alguns ataques de rede dentro de redes virtuais. O trabalho mostrará como os virtualizadores se comportam a alguns ataques de rede com as suas medidas protetivas ativas e até onde eles conseguem prevenir tais ataques. Dentre os ataques escolhidos no trabalho estão sniffing, spoofing e port scan. No caso de sniffing a rede virtual foi capaz de evitar os ataques com as proteções ativadas. Em relação a spoofing mesmo com as proteções ativas não conseguiu se proteger. E para port scan não havia nenhum tipo de proteção, apenas métodos que limitam o campo de atuação. As redes virtuais têm um grande potencial para a segurança, mas ainda têm vulnerabilidades a ataques simples e conhecidos.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ACRÔNIMOS

ACL	*Access Control List*
ARP	*Address Resolution Protocol*
CPU	*Central Processing Unit*
CVE	*Common Vulnerabilities and Exposures*
DHCP	*Dynamic Host Configuration Protocol*
DMZ	*Demilitarized Zone*
ETSI	*European Telecommunications Standards Institute*
HTTP	*HyperText Transfer Protocol*
HTTPS	*HyperText Transfer Protocol Secure*
IaaS	*Infrastructure as a Service*
IDC	*International Data Corporation*
IDS	*Intrusion Detection System*
IEEE	*Institute of Electrical and Electronics Engineers*
IP	*Internet Protocol*
IPS	*Intrusion Prevention System*
LDAP	*Lightweight Directory Access Protoco*
MAC	*Media Access Control*
MITM	*Man-In-The-Middle*
MPLS	*Multiprotocol Label Switching*
NAT	*Network Address Translator*
ND	*Neigbourhood Discovery*
NFV	*Network Functions Virtualization*
NIPS	*Network Intrusion Prevention System*
NMAP	*Network Mapped*
ONF	*Open Network Foundatio*
PaaS	*Plataform as a Service*
SaaS	*Software as a Service*
SDDC	*Software-Defined Data Center*
SDN	*Software-Defined Network*
TAP	*Test Access Port*
VLAN	*Virtual Local Area Network*
VM	*Virtual Machine*
VMM	*Virtual Machine Monitor*
VPN	*Virtual Private Network*
vSS	*Virtual Standard Switch*

1 INTRODUÇÃO

Apesar de ter se apresentado para o mundo como um modelo viável e se tornado o principal modelo de computação apenas nos últimos anos, o conceito de virtualização é estudado a quase cinquenta anos. Um dos grandes pesquisadores na área foi Robert P. Goldberg que definiu grande parte dos conceitos de virtualização que são adotados hoje. Com seu trabalho Architectural Principles for Virtual Computer Systems[3], Goldberg indicou o caminho para a construção do que posteriormente foi chamado Hypervisor na arquitetura x86.

Virtualização é a capacidade de desvincular os recursos de hardware do software executado a cima deles. Dessa forma é possível fazer com que vários sistemas operacionais e aplicações compartilhem um mesmo recurso sem que haja a necessidade de dedicar o uso exclusivo do recurso para apenas um sistema ou aplicação, como é no modelo tradicional. Assim a virtualização cria um modelo lógico para a utilização do hardware e não físico abstraindo a camada de hardware permitindo a criação de máquinas virtuais através de gerenciadores de recursos chamados hypervisor.

Hypervisor, também chamado de Virtual Machine Monitor (VMM), é o termo utilizado para representar a camada responsável pela abstração entre as máquinas virtuais e os recursos de hardware. Tal camada age de forma transparente para com as máquinas virtuais, gerenciando as requisições e respondendo da mesma maneira que o hardware responderia. Dessa forma o sistema operacional não consegue distinguir se está tratando com um hypervisor ou diretamente com o hardware. Outro ponto é que não existe diferença entre uma máquina física e uma máquina virtual, ambas reagem da mesma forma ao ambiente em que estão.

Com o crescimento do modelo computacional virtualizado, especialistas em segurança se dedicaram a estuda-lo com o objetivo de prover um ambiente resiliente e seguro, criando métodos de proteção para as novas soluções dentro do mundo da virtualização. Junto aos métodos de proteção também surgiram as falhas de segurança no modelo revelando formas de ataque novas e adaptando as que funcionavam no antigo modelo.

Cada dia novas medidas são tomadas a fim de criar uma arquitetura segura para uso. Grandes ameaças já foram detectadas e os sistemas prevenidos contra diversos ataques com medidas como isolamento, políticas de configuração, medidas preventivas contra hyperjacking, prevenção contra captura de dados na camada 2, entre outras diversas soluções.

Acompanhando a evolução da virtualização de servidores surgiram novos tipos de virtualização como a virtualização de rede, virtualização de armazenamento, virtualização de aplicações. Com a integração de diversos tipos de virtualização o conceito de Datacenter Definido por Software (SDDC) surgiu e com ele a computação em nuvem e a entrega de infraestrutura, plataforma e software como um serviço. Essas novas tecnologias têm apresentado novos recursos que contribuem para a segurança das redes nos dias de hoje.

1.1 MOTIVAÇÃO

Conceitos de segurança são aprimorados e reestruturados, adaptando-se ao ambiente, superando ameaças e reparando falhas no sistema. Nas duas últimas décadas grandes empresas no ramo da tecnologia da informação, como VMware e Microsoft, têm se dedicado a utilizar do conceito de virtualização para oferecer ferramentas que prometem grandes evoluções em relação ao modelo tradicional. A virtualização é um modelo amplamente difundido hoje graças a flexibilidade, escalabilidade, gerenciabilidade, portabilidade e segurança providenciados por ele. Tal modelo procura trazer melhorias na eficiência, controle de recursos e transparência. Contudo também apresenta oportunidade para novos ataques e novas brechas de segurança. Por conta disso têm sido estudados novos conceitos que buscam incorporar a solução a fim de torná-la resiliente, tolerante a falhas, segura e confiável.

A motivação desse trabalho é verificar a segurança de redes virtuais em relação a alguns ataques de rede como sniffing, spoofing e port scan de forma a observar o comportamento das redes virtuais em relação a esses ataques e como as soluções de virtualização lidam com eles.

1.2 OBJETIVO

O objetivo deste trabalho é explorar como as redes virtuais se comportam em relação a alguns ataques de forma a limitar e até impedir o acesso de objetos não autorizados em ambientes virtualizados.

1.2.1 Objetivos Específicos

- Identificar se as redes virtuais apresentam uma maior segurança para ataques de rede.
- Identificar como as tecnologias de virtualização lidam com ataques de rede.
- Contestar a segurança em ambientes virtuais e as formas que alguns ataques podem ou não ser executados nelas.

1.3 ORGANIZAÇÃO DO TRABALHO

1. Apresentação teórica dos conceitos necessários para a compreensão do modelo de virtualização e do funcionamento da segurança no modelo virtualizado. Capítulo 2
2. Apresentação do cenário para a execução de testes. Capítulo 3
3. Testes do comportamento da rede virtual. Capítulo 3
4. Apresentação dos resultados obtidos e análises. Capítulo 4

5. Discussões sobre os resultados e análises. Capítulo 4
6. Conclusões. Capítulo 5

2 FUNDAMENTAÇÃO TEÓRICA

Para uma melhor compreensão do trabalho será apresentada uma rápida contextualização e conceitos necessários para um melhor entendimento do conteúdo que seguirá.

2.1 VIRTUALIZAÇÃO

Em 1973 o cientista da computação americano Robert P. Goldberg lançou a base teórica da arquitetura x86 para sistemas computacionais virtuais em sua dissertação na universidade de Harvard, Architecture of Virtual Machines.[3] A partir deste momento uma série de outras pesquisas vinculadas a área surgiram, o próprio Goldberg lançou outros trabalhos e o conjunto de novas pesquisas pavimentaram o caminho para a criação do primeiro produto de virtualização para modelos da arquitetura x86 pela VMware em 1999 o "VMware Virtual Plataform".

De 1999 até os dias de hoje diversos produtos de virtualização foram lançados e o modelo virtualizado se espalhou não somente na vertente de servidores, mas atingiu a rede, o armazenamento, a segurança, a aplicação e os serviços sendo amplamente distribuída por diversos segmentos da computação. Por fim a evolução da virtualização possibilitou a criação de serviços em nuvem que é a tecnologia em ascensão nos dias de hoje. Tudo isso começou com dois conceitos: o de máquina virtual (Virtual Machine - VM) e o de Hypervisor (Virtual Machine Monitor - VMM), as bases da virtualização de servidores.

2.1.1 Máquina Virtual

Na década de 1960 a IBM lançou trabalhos sobre "time sharing" em seus mainframes. Esse conceito foi mais tarde utilizado por Goldberg para fundamentar seus conceitos para sistemas x86. Em seu primeiro trabalho, Goldberg explica uma máquina virtual como a simulação instrução por instrução de um sistema operacional. Algo criado para realizar teste de programas.[3]

Seu ponto era que um programa funcionaria na máquina real assim como ele funciona na máquina simulada. A máquina simulada tinha a capacidade de interagir com o hardware simulando o comportamento da máquina real e isso foi o que definiu o conceito de máquina virtual, uma máquina simulada que consegue reproduzir o exato comportamento de uma máquina real interagindo diretamente com o hardware.

Nos dias de hoje a definição mais adotada é a que uma máquina virtual é um ambiente providenciado por um Hypervisor ou Virtual Machine Monitor.

2.1.2 Virtual Machine Monitor

No mesmo trabalho de 1973, Goldberg definiu o conceito de Virtual Machine Monitor (VMM). Para ele VMM é o software capaz de gerenciar as requisições das máquinas virtual, trabalhando como a interface entre as máquinas e o hardware. O VMM, também chamado de hypervisor, faz o mapeamento dos recursos do hardware para a VM agindo como um intermediário permitindo que operações não privilegiadas (non privilege operations) sejam executadas diretamente no hardware pela VM e que operações privilegiadas (privilege operations) sejam contidas e executadas através do Hypervisor em uma operação definida por Goldberg por f-map.[4][5]

Em outro trabalho Goldberg juntamente com Gerald J. Popek resume as principais capacidades do VMM em três: O VMM providencia um ambiente para programas rodarem como se estivessem em uma máquina real; Os programas que rodam nesse ambiente não devem apresentar nenhuma diferença salvo uma pequena redução em sua velocidade; e o VMM detêm total controle sobre os recursos do sistema.[6]

2.1.2.1 Compartilhamento de Recursos

Para que possa existir virtualização é necessário que haja compartilhamento de recursos, com outras palavras as máquinas virtuais devem poder acessar os mesmos recursos de hardware. Inicialmente a virtualização surgiu com a intenção de simular programas em máquinas que conseguissem reproduzir o exato comportamento que teria uma máquina física. Contudo, o enfoque das soluções mudou quando perceberam que era possível fazer com que as máquinas fossem executadas sobre um mesmo hardware e de forma concorrente. Os hardwares de hoje em dia têm grandes capacidades de desempenho e ao se executar apenas um sistema operacional em cada hardware os recursos disponíveis geralmente sobram e ficam inutilizados sendo assim um grande desperdício de recursos. Em contrapartida em um ambiente virtual existe uma abstração dos recursos físicos de um hardware e assim é possível que eles sejam distribuídos entre diversas máquinas virtuais. Essa distribuição é o que se denomina compartilhamento de recursos em ambientes virtualizados.

2.1.2.2 Isolamento

O compartilhamento de recursos é uma característica marcante de ambientes virtualizados e com isso surge um problema: Se uma máquina compartilha recursos com outra máquina, então elas têm acesso aos mesmos recursos. Se isso não for gerenciado de forma correta uma máquina pode acabar acessando o recurso que está alocado para a outra. Isso pode gerar muitas falhas de segurança ou problemas de execução trazendo complicações ao ambiente virtual. Assim para que não existam problemas de convivência entre as máquinas é necessário que elas tenham cada uma o seu espaço sem que uma consiga acessar o que a outra está acessando e isso é denominado isolamento. O isolamento é a criação de domínios onde cada máquina possa ter um ambiente seguro e livre de intervenções para realizar suas tarefas e armazenar os seus dados. Esse isolamento geralmente e dado pela reserva dos recursos onde são atribuídos diferentes níveis de permissão para as máquinas virtuais. Assim o VMM gerencia o macro alocando os recursos para cada uma das diferentes máquinas e as máquinas têm permissão para atuar no micro gerenciando e modificando apenas os recursos atribuídos pelo VMM naquele momento a elas. Dessa forma uma máquina não terá permissão para agir sobre os recursos alocados a outra e caso isso ocorra é denominado uma falha de isolamento.[7][8]

2.1.3 Redes Virtuais

Redes virtuais é o nome dado a uma rede que existe de forma logica e não física a fim de dar conectividade entre membros de um determinado grupo. Em virtualização rede virtual é um conjunto de máquinas virtuais conectadas entre si. A forma mais comum de conexão é por meio de placas de redes virtuais das VMs a portas em um switch virtual. As redes virtuais são criadas nas memórias dos VMMs por meios de switches virtuais que são configurados em memória. Todo o tráfego de uma rede virtual é feito em memória, logo o meio físico por onde os pacotes iram transitar é a memória dos virtualizadores. [9][10][11]

Todo tráfego gerado pelas máquinas virtuais é mapeado em memória. Quando duas máquinas estão em um mesmo segmento na rede virtual a comunicação entre elas é feita diretamente da placa de rede virtual da primeira máquina para a segunda máquina. Já se estiverem em segmentos diferentes o pacote deverá ser roteado entre as redes saindo da placa de rede virtual da máquina, indo para a placa de rede física do virtualizador, seguindo para o switches até um roteador e então faz o caminho inverso entrando pela placa de rede física do virtualizador e sendo entregue a placa de rede virtual da VM em memória.[12][13]

2.2 TIPOS DE VIRTUALIZAÇÃO

A virtualização não ficou apenas sobre os servidores, o conceito de abstrair as capacidades e recursos de um hardware e gerenciar isso de forma lógica se espalhou por diversas áreas da ciência da computação como por exemplo virtualização de rede e virtualização de armazenamento.

A união de diversos tipos de virtualização compõe soluções de Computação em Nuvem, onde se torna possível abstrair completamente a infraestrutura de um datacenter e junto com processos de automação realizar a entrega de recursos na forma de serviços como IaaS, PaaS e SaaS.

Para entender um pouco mais o caminho que a virtualização tem tomado nos últimos anos serão apresentados os conceitos de virtualização de servidores, rede e armazenamento.

2.2.1 Virtualização de Servidores

Virtualizar servidores permite abstração e compartilhamento de recursos de hardware como CPU, memória, armazenamento e rede providenciado pelos servidores. Esse é o passo fundamental para qualquer outro tipo de virtualização. Esse tipo de virtualização vai permitir a criação de máquinas virtuais e a distribuição do acesso aos recursos contidos no servidor para elas.

Existem diferentes formas para se utilizar dos benefícios da virtualização de servidores entre algumas destas formas temos, Full Virtualization, Hardware-Layer Virtualization e Paravirtualization.

2.2.1.1 Full Virtualization

Nesse tipo de virtualização o VMM é instalado como uma aplicação do sistema operacional e as VMs funcionam sobre um hardware virtual gerenciado pelo VMM. Dessa forma são criados dispositivos virtuais que imitam aos dispositivos físicos assim sendo possível ao VMM redirecionar as interações entre o ambiente virtual e o hardware físico gerando o que se chama de uma virtualização completa dos dispositivos.[14] Pode-se observar um modelo representativo desse tipo de virtualização na figura 2.1.

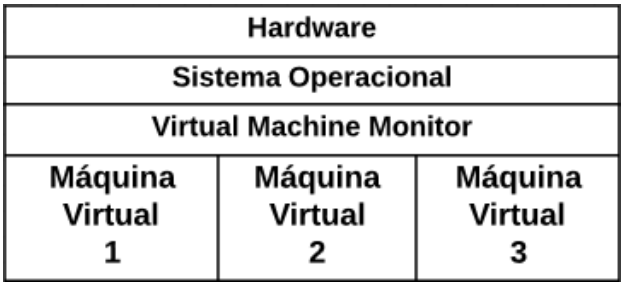

Figura 2.1: Representação da virtualização tipo: Full Virtualization.

2.2.1.2 Hardware-Layer Virtualization

Nesse tipo de virtualização o VMM é instalado diretamente no hardware e ele gerencia e sincroniza o acesso das VMs a ele. As grandes soluções corporativas usam deste tipo de virtualização, pois ela tem um melhor desempenho e maior controle, mantendo um melhor isolamento do ambiente dado que as máquinas virtuais tratam diretamente com o hardware através do VMM e não com dispositivos virtuais.[14] Um modelo representativo desse tipo de virtualização se encontra na figura 2.2. Esse tipo de virtualização será utilizado para prover a infraestrutura para a realização do ataque escolhido para o desenvolvimento deste trabalho.

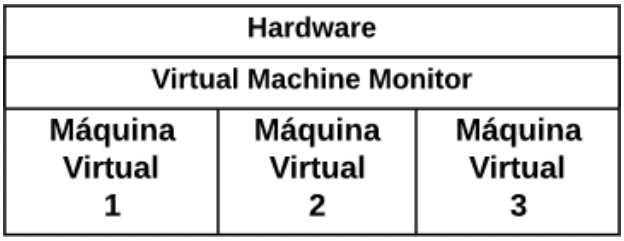

Figura 2.2: Representação da virtualização tipo: Hardware-Layer Virtualization.

2.2.1.3 Paravirtualization

Nesse tipo de virtualização o sistema operacional que será virtualizado é modificado para suportar uma interface que se comunicará com o hardware diretamente. Em contradição com os outros tipos, aqui as máquinas sabem que são virtualizadas e o VMM pode ter papeis mais simples, permitindo que o ambiente virtual atinja níveis de desempenho próximos a ambientes não virtualizados.[14] Um modelo representativo desse tipo de virtualização se encontra na figura 2.3.

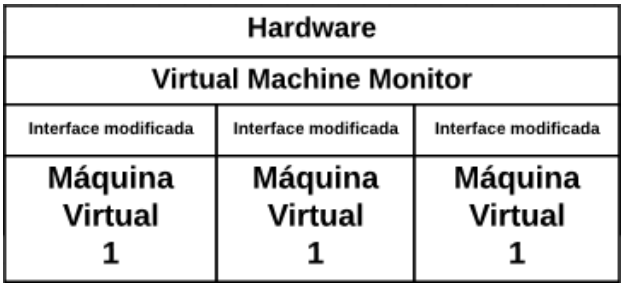

Figura 2.3: Representação da virtualização tipo: Paravirtualization.

2.2.2 Virtualização de Rede

A virtualização de rede por sua fez está principalmente dividida em dois casos: SDN e NFV. Provedores de hardware de rede, como a Cisco, e empresas de software, como a VMware, têm desenvolvidos diversos produtos utilizando desses dois tipos de virtualização. A IDC (International Data Corporation) realizou uma série de estudos de mercado para essas soluções e prevê um crescimento muito grande para os próximos 4 anos. Para NFV está previsto um valor de 5.6 bilhões de dólares em vendas até 2022.[15]

2.2.2.1 Rede Definida por Software

A rede definida por software, do inglês Software-Defined Networking (SDN), se popularizou nos últimos anos devido principalmente a iniciativa da Open Network Foundation (ONF)[16] a partir divulgação e incentivo do uso de tecnologias de código aberto como o protocolo OpenFlow, criado por um grupo de cientistas da computação de Stanford em 2008.[17]

Uma rede é caracterizada como definida por software se:[18][1]

1. Os planos de controle e de dados são separados um do outro;
2. Se a rede é programável através do plano de controle.

A ideia em uma SDN é separar a decisão sobre os dados dos dispositivos que executam a ação. Para isso foi definido um modelo de referência contendo três camadas: Camada de Aplicação, Camada de Controle e Camada de Infraestrutura, figura 2.4

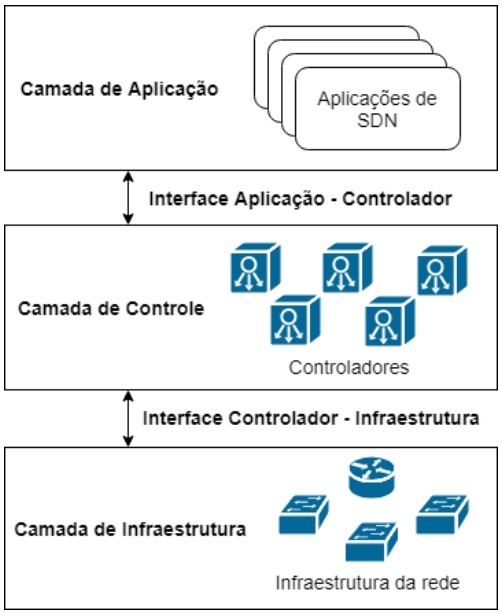

Figura 2.4: Modelo de referência para redes SDN.[1]

A camada de aplicação é aquela que define os serviços que serão disponibilizados na rede, firewall, balanceamento de carga, roteamento, switching entre outras aplicações. A camada de controle estabelece e como as regras passadas pela aplicação serão implementadas na infraestrutura. E a camada de infraestrutura recebe as instruções da camada de controle e realiza as operações sobre os dados nos dispositivos.

2.2.2.2 Virtualização das Funções da Rede

A virtualização das funções da rede, do inglês Network Function Virtualization (NFV), é o modelo que busca desvincular o hardware de rede dos serviços que eles oferecem.[2] A proposta foi feita por um grupo de empresas do ramo da tecnologia da informação e a European Telecommunications Standards Institute (ETSI) foi escolhida para determinar os padrões que definem o que é NFV.[19] Hoje a NFV se encontra na sua terceira edição, NFV Release 3 e os padrões podem ser encontrados na página do ETSI.[20]

A arquitetura para NFV é composta por 4 componentes: orquestrador, gerenciador VNF, camada de virtualização e infraestrutura virtualizada o relacionamento entre as partes pode ser visualizado na figura 2.5.[2][19]

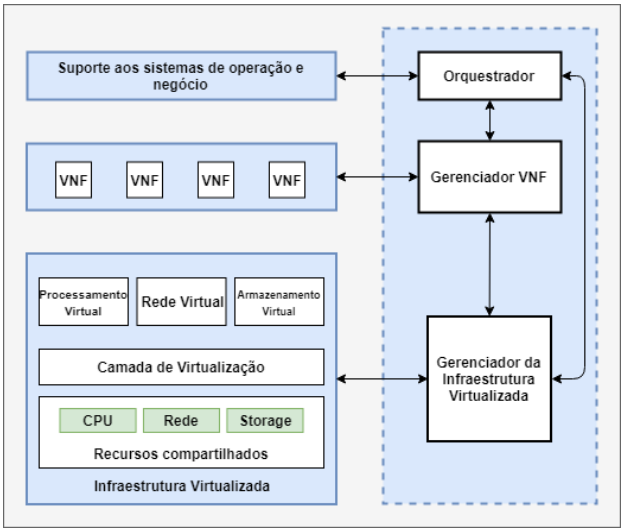

Figura 2.5: Framework da arquitetura NFV.[2]

A proposta de virtualizar as funções da rede trás três diferenças principais em relação as práticas tradicionais:

- Separação do software do hardware, permitindo que cada um evolua independentemente do outro.
- Implementação flexível das funções de rede. Com a ajuda da virtualização dos recursos é possível que os serviços de rede sejam implementados de forma rápida sobre a mesma plataforma física uma vez que os serviços podem ser instanciados em um servidor virtualizado e as conexões de rede podem ser feitas de forma flexível.

- Escalonamento dinâmico. As funções de rede podem ser implementadas ou expandidas com o surgimento da necessidade da rede sem depender da arquitetura física da rede para isso.

2.2.3 Virtualização de Armazenamento

A virtualização de armazenamento tem o objetivo de apresentar todos os meios de armazenamento (discos rígidos, storages, fitas, discos óticos, entre outros) como uma única unidade lógica de armazenamento. Isso pode ser feito de duas formas virtualização a nível de bloco, block-level, ou a nível de arquivos, file-level. Na primeira, blocos de dados são mapeados de um ou mais subsistemas de armazenamento de forma a aparecerem como um único volume. Na segunda múltiplos sistemas de arquivo aparecem como um único sistema de arquivo.[21]

2.3 SEGURANÇA EM AMBIENTES VIRTUALIZADOS

Um ambiente virtual é construído sobre uma topologia física em primeiro nível, logo ao se pensar na segurança de um ambiente virtual é necessário pensar também na segurança dos componentes físicos. Algumas das estratégias mais usadas na segurança de redes em datacenters são firewalls, IDS/IPS, VLANs, VPNs, controle de acesso, protocolos de segurança, autenticação e criptografia.[22][23][24][25][26] Tais medidas visam limitar o acesso apenas a entidades credenciadas, detectar e prevenir invasores, limitar a área de ação de invasores, filtrar ações de invasores, impedir que informações sejam vazadas ou modificadas, entre outras diversas ações de segurança. Ambientes virtuais também terão as mesmas preocupações de segurança que os ambientes físicos, contudo com o avançar da virtualização nas diversas áreas (servidores, rede, armazenamento, etc) os modos de se realizar a segurança variam. Para considerar um ambiente virtualizado seguro, deve se atentar tanto a segurança da componente física, quanto a segurança na componente virtual.

2.3.1 Segurança da rede física

Uma topologia comum de redes é a divisão da rede em rede externa, rede interna e DMZ, figura 2.6. A rede externa é considerada não confiável por ser um ambiente não controlável, não observável e compartilhado entre seus muitos usuários, geralmente a internet. A rede interna é a rede privada e confiável onde são armazenados todos os dados da empresa e a infraestrutura computacional física. A DMZ é uma rede não confiável onde estarão todos os serviços destinados a atender os usuários externos (serviços WEB, serviços de arquivos, serviços de e-mail). Ela busca minimizar os danos causados em caso de ataques aos serviços disponibilizados para os usuários externos, não afetando a rede interna.

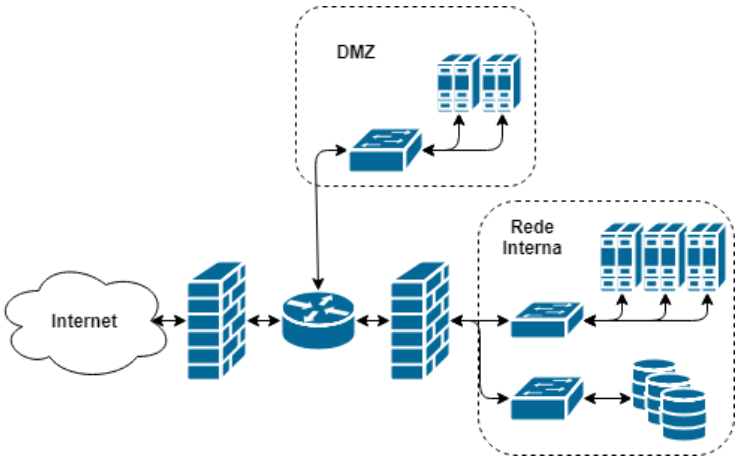

Figura 2.6: Topologia comum de redes.

A divisão das redes é realizada de diversas formas, uma boa forma de realizar a proteção básica da rede é:

- Utilizar firewalls para filtrar os dados que vem da rede externa e os dados que têm destino na rede interna. Também aquilo que tem destino de saída como forma de prevenção de vazamento de dados.
- Utilizar VLANs para segregar o tráfego entre redes e diminuir os domínios de colisão.
- Utilizar IPS para analisar o tráfego que está em suas redes, principalmente o tráfego que chega da rede externa em direção a rede interna.
- Utilizar serviços de diretório de acesso (LDAP) para impedir que usuários sem permissão consigam acessar dispositivos não permitidos.
- Utilizar protocolos de comunicação seguros.
- Utilizar VPNs para acesso externo a rede interna.
- Utilizar endpoints para suas máquinas com acesso a internet, de modo a proteger o usuário e os dados de invasores.
- Manter dispositivos de rede, servidores, storages, desktops entre outros dispositivos com suas versões de software atualizadas.

2.3.2 Segurança da rede virtual

A rede virtual é construída de forma lógica após a virtualização dos servidores. Em primeiro nível são construídos switches virtuais e grupos de portas que vão ser a infraestrutura de rede para as máquinas virtuais, figura 2.7.

Em uma rede virtual, grupo de portas é um domínio de colisão dentro do switch e terá a mesma função que VLANs têm na rede física, segregar o tráfego entre as redes. Ao separar as máquinas virtuais por grupo de portas é possível criar diferentes VLANs para diferentes grupos de portas, dessa forma uma VM em um grupo de portas não tem acesso a VM de outro grupo de portas. Os virtual switches separam os diferentes segmentos de redes. Máquinas em diferentes switches virtuais não se comunicam, segregando também o tráfego. Máquinas no mesmo servidor se comunicam sem precisar passar pela rede física, o hypervisor lida com a comunicação em memória. Em caso das máquinas se encontrarem em servidores diferentes o hypervisor envia as requisições pela rede física.

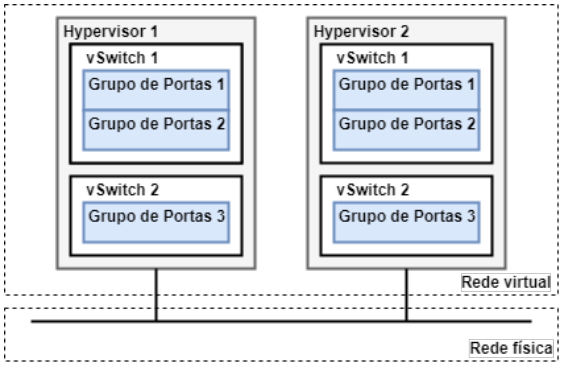

Figura 2.7: Topologia comum de redes virtuais.

Essa topologia composta por switches virtuais e grupos de portas pode se apresentar de duas formas:

- Ou cada servidor de virtualização possui uma infraestrutura virtual composta por switches e grupo de portas, figura 2.7;
- Ou os servidores de virtualização utilizam uma infraestrutura lógica compartilhada e distribuída para todos os hypervisors, figura 2.8.

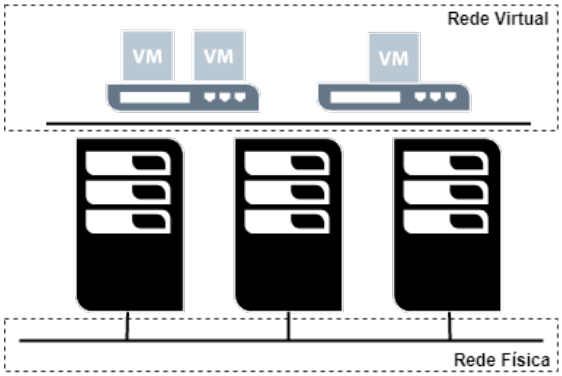

Figura 2.8: Topologia distribuída em redes virtuais.

Em um nível posterior, com a utilização de SDN e NFV, pode ser virtualizada qualquer função de rede por meio de criação de VMs e serviços providos pelo gerenciador do ambiente. Com a construção deste nível é possível criar firewalls, IPS, roteadores, hubs, balanceadores de carga entre outras funções de rede dentro da infraestrutura virtualizada. Neste nível o consumo recurso para a criação da rede virtual é muito maior sendo aconselhado até mesmo que sejam reservados recursos de forma exclusiva para os componentes de rede.

Basicamente todas as ações utilizadas para prover segurança em redes físicas, também se aplicam a redes virtuais como:

- Utilizar firewalls para filtrar os dados entre máquinas virtuais
- Utilizar VLANs para segregar o tráfego entre grupos de portas e diminuir os domínios de colisão.
- Utilizar IPS para analisar o tráfego que está em suas redes.
- Utilizar serviços de diretório de acesso (LDAP) para impedir que usuários sem permissão consigam acessar dispositivos não permitidos.
- Utilizar protocolos de comunicação seguros.
- Utilizar VPNs para acesso externo a rede interna.
- Utilizar endpoints para seus servidores de virtualização, de forma a torna-los resilientes.
- Manter servidores virtuais e máquinas virtuais com suas atualizações em dia.

2.4 VULNERABILIDADES EM AMBIENTES VIRTUAIS

As vulnerabilidades em ambientes virtuais serão classificadas nesse trabalho em dois tipos: Vulnerabilidades de rede, que buscam ter acesso a uma máquina e para isso devem passar pela rede e vulnerabilidades de sistema, onde através de falhas de isolamento uma máquina virtual consegue realizar um ataque diretamente na outra máquina virtual através do hypervisor. Geralmente uma vulnerabilidade de sistema somente pode ser explorada se o atacante já está em posse de uma máquina, para isso ele precisa explorar falhas de rede primeiro.

2.4.1 Vulnerabilidades de Rede

2.4.1.1 Denial of Service

Denial of Service é caracterizado quando usuário busca impedir que um grupo de usuários utilize um serviço ou recurso provido pela rede ou infraestrutura.[27] Esse tipo de ataque pode ser realizado de diversas maneiras, alguns exemplos são:

- Um usuário obtém acesso para criar máquinas virtuais e cria várias máquinas de forma a esgotar os recursos disponibilizados pela infraestrutura.
- Um usuário abre conexões para com uma máquina específica esgotando as portas da máquina impedindo que outros usuários possam utilizar de seus serviços.
- Vários dispositivos infectados enchem a rede de pacotes com o intuito de inutilizar ou deteriorar a rede.

Ataques de Denial of Service se tornaram populares nos últimos anos sendo registrados como 18% dos ataques da base CVE segundo o site CVE details.[28]

2.4.1.2 Sniffing

Sniffing ocorre quando alguém tem a capacidade de observar o que se passa pela rede capturando seu tráfego geralmente utilizando ferramentas chamadas de sniffers.[29] Esse ataque permite que o atacante tenha maior familiaridade com o ambiente procurando por vulnerabilidades que permitam que ele vá ainda mais longe.

Para realizar um ataque de sniffing o atacante precisa ter acesso a rede e também poder escutar os pacotes que trafegam nela. Ataques de sniffing são feitos colocando a interface da máquina atacante para capturar todos os pacotes que estiverem passando pela rede. Enquanto normalmente uma interface apenas capturaria pacotes com endereço MAC de destino a ela, uma máquina realizando sniffing coloca sua interface para capturar qualquer pacote que for ouvido pela interface de rede. Esse modo de captura é chamado de modo promíscuo. Geralmente a captura dos pacotes é salva em um dump que pode ser salvo em diversos formatos inclusive plain text (txt). Um dos formatos mais utilizados é o pcap que é dedicado a formatação para captura de pacotes de rede.

Um ataque de sniffing é utilizado de forma a observar o comportamento da rede ou dos componentes dela a fim de obter informações para a realização de outros ataques.

2.4.1.3 Spoofing

Spoofing ocorre quando um dispositivo assume a identidade de outro dispositivo na rede. Spoofing é geralmente utilizado para redirecionar comunicações na rede ou mascarar a verdadeira identidade do atacante na rede. Existem diversas formas de realizar ataques de spoofing, a mais comum é com a utilização de ARP poisoning onde um dispositivo utiliza da divulgação de um endereça MAC que não é o seu na rede e se passa por outro dispositivo, podendo assim receber as requisições destinadas ao outro dispositivo e agir com base nelas. Outra forma é enviar pacotes com o endereço MAC alterado, mascarando a real identidade de onde os pacotes estão sendo enviados.

Ataques de spoofing são um passo inicial para a realização de outros ataques como Man-In-The-Middle onde uma máquina conversa com um agente intermediário achando que está conversando com o receptor final. Outra utilização de ataques de spoofing é para mascarar a identidade do atacante forjando uma identidade falsa ou até mesmo assumindo a identidade de um componente conhecido da rede. O spoofing é muito usado para roubo e interceptação de dados, em outros casos até mesmo para derrubar um serviço ou desviar um trafego.

2.4.1.4 Ataques de Varredura - Port Scan

Ataques de varredura procuram enviar requisições aos dispositivos que se encontram na rede na procura por portas que estejam abertas e oferecendo serviços. Tais ataques visam obter informações sobre os dispositivos que se encontram na rede para a partir dessas informações explorar vulnerabilidades.

Um atacante realizando um ataque de varredura enviará pacotes para um ou mais componentes da rede em uma ou mais portas e observar se houveram respostas e qual o tipo de resposta que foi dada. Com essas informações ele consegue dizer quais portas estão abertas em qual máquina e que tipo e versão do serviço está disponível naquela porta, assim como o tipo do sistema operacional entre outras informações. Ataques de varredura coletam dados e subsidiam que outros ataques sejam preparados de forma personalizada para cada máquina.

2.4.2 Vulnerabilidades de Sistema

2.4.2.1 Privilege Escalation

Privilege escalation é utilizar de uma falha de isolamento para obter acesso a um contexto com o privilégio mais amplo que o que você está. Isso geralmente ocorre por existirem códigos que não necessitam de acesso a uma zona privilegiada terem tais acessos permitindo ao atacante utilizar disso para ter acesso a um contexto privilegiado dentro da máquina. Uma forma característica de obter esse acesso é quando o atacante consegue acesso a escrita fora dos limites da memória atingindo a parte privilegiada, assim colocando o seu código em um contexto privilegiado.

2.4.2.2 Hyperjacking

Hyperjack é um ataque caracterizado por assumir o controle do VMM e a partir daí explorar o ambiente virtual. Como o VMM é responsável pela monitoração do ambiente - ligar e desligar máquinas, controle dos recursos, em alguns casos monitorar aplicações dentro das máquinas virtuais e até mesmo criar ou deletar máquinas ou realizar cópias delas - então obter acesso ao VMM significa ter o poder de impactar o ambiente virtual em operações de monitoramento. Proteger tal capacidade é fundamental para um ambiente saudável. Esse tipo de ataque é feito explorando vulnerabilidades que permitam tomar o controle do VMM ou executar comandos por meio dele, seja presencialmente ou de forma remota. Isso pode ser feito através de rootkits instalados diretamente no hardware que contém o VMM ou por meio de falhas de escalação de privilégios. Esse tipo de ataque é caracterizado como host-to-guest, ou do hospedeiro para o hóspede.[30]

2.4.2.3 VM Escape

Outro ataque que se utiliza de privilege escalation é VM Escape, onde uma máquina virtual encontra uma brecha no isolamento, normalmente através dos códigos dos dispositivos virtuais, permitindo que uma VM acesse o domínio de outra ou que uma VM acesse o recurso diretamente sem a intervenção do VMM que está hospedada utilizando desse acesso para executar comandos no host. Ao obter acesso ao VMM uma VM obtém privilégios de administrador e pode comprometer de diversas formas o ambiente. Ataques assim são caracterizados como guest-to-guest, VM para VM, ou guest-to-host, VM para VMM, no segundo caso. Problemas de VM Escape podem ser resolvidos configurando de forma adequada o acesso aos recursos e a interação entre o VMM e a máquina virtual.[14][31]

2.5 TRABALHOS RELACIONADOS

O artigo: "Virtual network security: threats, countermeasures, and challenges" [32] publicado em Journal of Internet Services and Applications no ano de 2015 traz o tema segurança de redes virtualizadas e apresenta de forma teórica ameaças, contramedidas e alguns desafios a respeito desse tema. Tal artigo vai classificar de forma taxonômica diversas ameaças e contramedidas. O enfoque está nas ameaças que podem ser encontradas em redes virtuais e contramedidas que devem ser realizadas para conter tais ameaças. Ao final do trabalho os autores mencionam alguns desafios na área de segurança em redes virtuais como a dificuldade de implementar medidas de "nonrepudiation", a heterogeneidade das infraestruturas de rede e a que as plataformas de virtualização geralmente não oferecem as medidas de segurança adequadas.

O artigo: "Um Mecanismo para Isolamento Seguro de Redes Virtuais Usando a Abordagem Híbrida Xen e OpenFlow" [33] publicado no XIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais no ano de 2013 traz uma abordagem de segurança para redes virtuais utilizando de SDN através da mesclagem do protocolo OpenFlow e a plataforma de virtualização Xen. Esse artigo foca na criação de um mecanismo que utiliza de tags para realizar o controle sobre as redes virtuais criadas sobre o Xen. A aplicação vai separar o plano de controle do plano de dados e utilizar de VLANs para fazer a segregação e a proteção da rede. Dessa forma os fluxos são mapeados considerando o marcador na etiqueta de VLAN como critério de classificação. Como trabalho futuro eles propõem a troca da marcação com VLAN para MPLS (Multiprotocol Label Switching).

O artigo: "Uma Arquitetura Elástica para Prevenção de Intrusão em Redes Virtuais usando Redes Definidas por Software" [34] publicado nos Anais do 32º Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos no ano de 2014 traz uma abordagem de segurança para redes virtuais a partir da alocação dinâmica de máquinas virtuais de análise de pacotes e sistemas de detecção de intrusos (IDS). A abordagem neste trabalho busca integrar os dados obtidos por máquinas virtuais que analisam a rede e os módulos do OpenFlow em uma arquitetura de virtualização Xen. De acordo com a demanda das redes virtuais são criadas ou destruídas máquinas de análise de trafego. Esse comportamento adaptativo é o que eles chamam de arquitetura elástica.

O artigo: "NICE: Network Intrusion Detection and Countermeasure Selection in Virtual Network Systems"[35] publicado pelo IEEE em 2013 busca um modelo para um sistema que detecta um ataque em um ambiente virtual e seleciona a melhor contramedida para esse ataque. O enfoque do trabalho é para máquinas virtuais que se encontram na nuvem de forma a prevenir ataques de negação de serviço ou ataques de zombie exploration.

Por outro lado, este trabalho foca na avaliação das principais soluções de virtualização a respeito de ataques como sniffing, spoofing e port scan a partir de máquinas dentro da rede virtual. O objetivo é analisar até que ponto a virtualização de servidores pura consegue conter ou prevenir esses ataques sem a utilização de redes definidas por software ou máquinas virtuais. Os três ataques realizados para os testes nesse trabalho foram escolhidos por serem ataques que provem informação ou dão suporte a outros ataques. Ao final terão algumas discussões sobre a integração de funcionalidades aos virtualizadores de forma a incrementar a segurança do ambiente providenciado por eles. O diferencial deste trabalho em relação aos trabalhos apresentados a cima é a abordagem sem a utilização de agentes externos para providenciarem a segurança, mas a análise de funções ou que já existem ou que poderiam ser integradas ou kernel dos virtualizadores. Além disso as tecnologias de virtualização utilizadas nesse trabalho são das empresas que representam a liderança no mercado de virtualização atualmente.

3 DESCRIÇÃO DO CENÁRIO

A fim de testar a segurança foi montado um cenário que está descrito nesse capítulo. O mesmo cenário foi utilizado para a realização de todos os testes descritos na seção 3.5.

3.1 TOPOLOGIA DAS REDES

Para um melhor entendimento sobre o trabalho estão apresentadas nessa seção as topologias utilizadas para a criação dos ambientes que foram estudados nesse trabalho. Como a virtualização trabalha com a abstração de recursos físicos, apresentando para as máquinas virtuais um recurso lógico, serão apresentadas as topologias física e lógica utilizadas como modelo para os criar os ambientes com duas diferentes soluções de virtualização.

3.1.1 Topologia Física

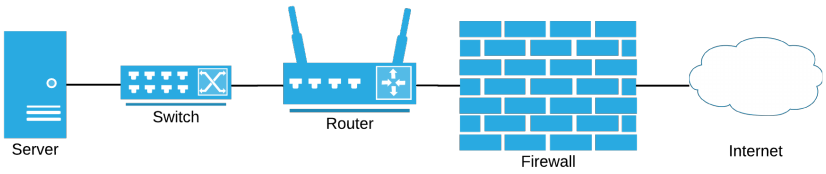

Figura 3.1: Topologia física simplificada da rede.

A virtualização realiza abstração de recursos físicos, então mesmo que os recursos apresentados as máquinas no hypervisor sejam virtuais, eles precisam existir fisicamente. Dessa forma a virtualização é uma camada criada sobre uma topologia física.

Para os ambientes criados nesse trabalho a topologia física em cada caso é composta por um servidor e uma infraestrutura de rede física com switches, roteadores e firewall a qual o servidor se conecta. O gerenciamento sobre o ambiente não foi total. Por conta do servidor ser um servidor na nuvem, era possível gerenciar o servidor, mas não os componentes da rede física a qual ele se conecta.

Um exemplo simplificado e funcional de topologia física de rede paravirtualização é encontrado na figura 3.1. Essa topologia permite o funcionamento da rede apesar de não ser muito resiliente. Possui um firewall para fazer o controle de entrada e saída do ambiente, um roteador para gerenciar as rotas no ambiente, um switch para conectar os componentes e um servidor virtualizado com os recursos de processamento, memória e armazenamento a serem abstraídos e entregues as máquinas virtuais.

Em ambientes corporativos existiriam outros componentes para agregar mais funções ao ambiente, componentes como storage ou IPS/IDS ou outros ativos de rede para gerar redundância ou segmentações na rede. O ambiente apresentado é um ambiente simplificado e pode ser escalado em tamanho e complexidade com a adição de outros componentes.

3.1.2 Topologia Virtual

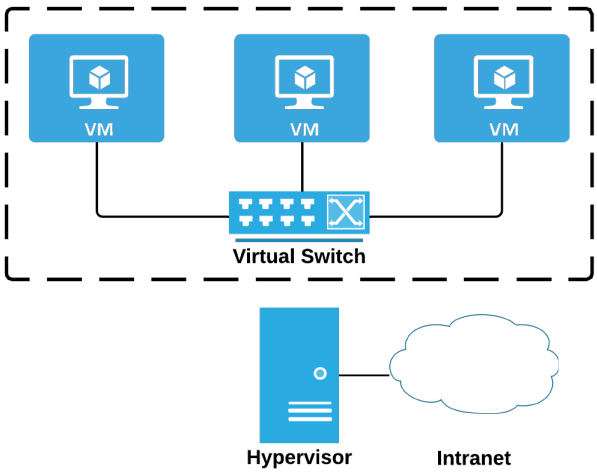

Figura 3.2: Topologia lógica simplificada da rede virtual.

Acima da topologia física, com a instalação de um virtualizador para gerenciar os recursos dos servidores, é criada uma camada virtual que é representada na topologia física da seção 3.1.1 apenas pelo servidor. Sobre o servidor são criados switches virtuais e máquinas virtuais em um primeiro passo da virtualização. Esses switches e máquinas virtuais são abstrações dentro dos servidores e não podem ser vistos apenas observando a topologia física e por isso são representados de forma lógica em uma topologia lógica da rede.

Os switches e máquinas virtuais usam os recursos da rede física para se comunicar uns com os outros. O funcionamento dos switches virtuais é parecido com o funcionamento dos switches da rede física. Switches virtuais trabalham como switches físicos de camada 2. Tráfegos entre componentes em um mesmo switch virtual são encaminhados pelos switches virtuais. Tráfegos entre componentes em diferentes switches virtuais precisam ser roteados por um roteador, seja ele físico ou virtual.

Os switches virtuais conseguem segregar o tráfego sobre eles com a utilização de VLANs, mas necessitam que os componentes na rede física forneçam as VLANs para que isso seja propagado para diferentes switches virtuais ou outros servidores. Dessa forma a configuração mais comum é manter os switches físicos em modo trunk e determinar as VLANs tags nos switches virtuais. Dessa forma uma máquina em um segmento virtual em um switch poderá se comunicar com uma máquina no mesmo segmento virtual em outro switch, e vice-versa, por meio do encaminhamento dos pacotes através dos componentes de rede da rede física.

Um exemplo simplificado de topologia lógica é encontrado na figura 3.2. A rede física é representada como uma nuvem e chamada de intranet ou rede interna e a representação é feita apenas a partir do servidor. Dentro do servidor é criada uma estrutura com switches virtuais e máquinas virtuais. Os switches virtuais utilizam como forma de se conectar a rede física as placas de rede físicas dos servidores e as máquinas virtuais se conectam as portas dos switches virtuais através de placas de rede virtuais a rede.

A topologia utilizada neste trabalho é a descrita na figura 3.2, onde existem 3 máquinas virtuais conectadas por um único switch virtual em um único grupo de portas ou VLAN. As máquinas virtuais serão: uma máquina atacante, uma máquina servidor que provê serviços aos componentes da rede e uma máquina cliente que consumirá os serviços do servidor. Todos os testes serão executados em cima dessa topologia sem adicionar ou remover componentes dela.

3.1.3 Criação das Máquinas para os Testes

Para os testes propostos na seção 3.5, foram criadas três máquinas virtuais. Segue a lista de máquinas criadas e seus propósitos:

- Uma máquina virtual Kali Linux versão 2019.2. Utilizada para a realização dos ataques.
- Uma máquina virtual Ubuntu Server versão 18.04. Utilizada como servidor web como serviço para a rede.
- Uma máquina virtual Ubuntu Desktop versão 18.04. Utilizada como estação de trabalho para consumir o serviço web disponibilizado.

3.2 SOLUÇÕES DE VIRTUALIZAÇÃO

Existem diversas soluções de virtualização de servidores na arquitetura x86 disponíveis no mercado. O Gartner classificou em sua última avaliação, em 2016, oito soluções de virtualização de servidores. Dentre essas oito empresas, duas tem se mantido como líderes no nicho de mercado desde 2011, elas são a VMware e a Microsoft.[36] Por conta desse histórico de anos na liderança essas foram as duas soluções escolhidas para compor o cenário na construção da camada de virtualização.

3.2.1 VMware vSphere

A VMware é a pioneira no mercado de virtualização de servidores na arquitetura x86. Fundada em 1998 vem trabalhando com virtualização de servidores a mais de 15 anos. Atualmente focada em soluções de nuvem e tem como foco pavimentar o caminho pra a transformação digital das empresas. Sua solução de virtualização de servidores é o VMware vSphere, também chamado de ESXi, que atualmente se encontra na versão 6.7. A solução da VMware é classificada como virtualização sobre o hardware (Hardware-Layer Virtualization) logo as máquinas não sabem que são virtualizadas.

A versão do VMware ESXi no ambiente VMware é a versão 6.7.0-816169922. Mais detalhes podem ser obtidos a partir da tabela 3.1

3.2.2 Microsoft Hyper-V

A Microsoft entrou para o quadrante de líder de mercado em virtualização de servidores x86 em 2011 e desde então tem se desenvolvido e se mantido no quadrante junto com a VMware. A solução de virtualização de servidores da Microsoft é chamada de Hyper-V. Tal funcionalidade foi incorporada aos sistemas operacionais Windows Servers e está disponível desde o Windows Server 2008. Atualmente a versão mais nova do Windows Server é o Windows Server 2019. A solução da Microsoft é classificada como paravirtualizada (paravirtualization) e realiza algumas modificações no sistema operacional das máquinas virtuais a fim de otimizar a performance da máquina melhorando a comunicação entre máquina virtual e virtualizador.

A versão do Hyper-V Manager no ambiente Microsoft é a versão 10.0.17763.1 build 17763. Mais detalhes podem ser obtidos a partir da tabela 3.1.

3.3 INSTALAÇÃO E CONFIGURAÇÃO DAS SOLUÇÕES

Nessa seção serão abordados os passos de instalação de cada uma das soluções. Ambas as soluções foram instaladas em máquinas virtuais na nuvem, mas o processo de instalação em um servidor físico é o mesmo. As versões instaladas podem ser verificadas na tabela 3.1.

Tabela 3.1: Versões dos virtualizadores utilizados para a criação do ambiente de testes.

	VMware	**Microsoft**
Hypervisor Name	ESXi	Hyper-V
Version	6.7.0-8169922	10.0.17763 build 17763
Product Name	VMware vSphere ESXi	Microsoft Windows Server 2019 Datacenter Evaluation with Hyper-V

3.3.1 Instalação e Configuração do ESXi

Para instalação do ESXi foi feito o download da imagem do hypervisor no site da VMware [37]. A versão baixada foi a versão VMware vSphere 6.7. A instalação foi feita conforme documentação oficial da VMware [38].

O Hypervisor é instalado como o sistema operacional da máquina física. Ele vai abstrair os recursos físicos disponíveis no hardware e gerenciar o acesso das máquinas virtuais a eles. A instalação do ESXi é feita através de interface gráfica. Uma vez realizado o boot na mídia é só seguir os passos de configuração que o servidor irá instalar a solução e reiniciar. Uma vez reiniciado deve configurar a rede de gerenciamento nele através. Esse passo pode ser feito pressionando "F2" na tela inicial, entrando com a senha e indo até "Configure Management Network".

Após instalado o ESXi, um switch virtual é automaticamente criado com dois grupos de portas. Um grupo de portas é para a gerência do hypervisor e o outro é um grupo para máquinas virtuais. Para conter as máquinas virtuais foi criado um outro virtual switch standard de nome "Internal" sem uma interface de uplink com um grupo de portas chamado de "Internal". O virtual switch foi criado com as configurações padrão, tais configurações podem ser revisadas nas tabelas 3.2 e 3.3.

A administração do ESXi após a configuração da rede de gerenciamento pode ser feita pela interface web através de um navegador com o protocolo HTTPS e o IP atribuído a interface de gerenciamento do ESXi. Um exemplo seria: "https://192.168.168.192".

Tabela 3.2: Configurações obtidas via CLI para o switch utilizado na solução da VMware através do comando *esxcli network vswitch standard list*

	vSwitch
Name	Internal
Class	cswitch
Num Ports	2816
Used Ports	1
Configured Ports	1024
MTU	1600
CDP Status	listen
Beacon Enabled	false
Beacon Interval	1
Beacon Threshold	3
Beacon Required By	
Uplinks	
Portgroups	Internal

Para finalizar a fim de que a solução de virtualização se comunique melhor com as máquinas virtuais foi instalado o pacote de serviços e módulos do open-vm-tools em cada uma das máquinas virtuais.[39] O pacote de serviços tem como objetivo obter melhores informações sobre a máquina, permitindo o virtualizador gerenciar melhor a VM. Além disso ele realiza a instalação de drivers para ajudar na comunicação e apresentação das máquinas virtuais.

Tabela 3.3: Configurações obtidas via web console para o switch utilizado na solução da VMware através da console de configuração do vSwitch.

	Virtual Switch "Internal"
MTU	1600
Link discovery Mode	Listen
Link discovery Protocol	Cisco discovery protocol (CDP)
Security Promiscuos mode	Alterado conforme os testes
Security MAC address changes	Alterado conforme os testes
Security Forged transmits	Alterado conforme os testes
NIC teaming Load balancing	Route based on originating port ID
NIC teaming Network failover detection	Link status only
NIC teaming Notify switche	Yes
NIC teaming Failback	Yes
NIC teaming Failover order	
Traffic shaping Status	Disabled

A versão do pacote open-vm-tools instalado em cada máquina está registrada na tabela 3.4.

Tabela 3.4: Resumo de configurações das máquinas virtuais criadas no ambiente VMware.

	Máquina Atacante	**Máquina Desktop**	**Máquina Server**
Sistema operacional Description	Kali GNU/Linux Rolling	Ubuntu Desktop 18.04.2 LTS	Ubuntu Server 18.04.2 LTS
Sistema operacional Release	2019.2	18.04	18.04
IP	192.168.1.214	192.168.1.216	192.168.1.208
MAC	00:0C:29:47:05:42	00:0C:29:2B:AB:4E	00:0C:29:58:C1:D8
VMware Tools Version	2:10.3.10-1	2:10.3.5-7~ubuntu0.18.04.1	2:10.3.5-7~ubuntu0.18.04.1

A figura 3.3 representa graficamente as configurações de rede de cada máquina virtual criada no ambiente VMware. Essa configuração será utilizada no ambiente VMware em todos os testes apresentados posteriormente na seção 3.5.

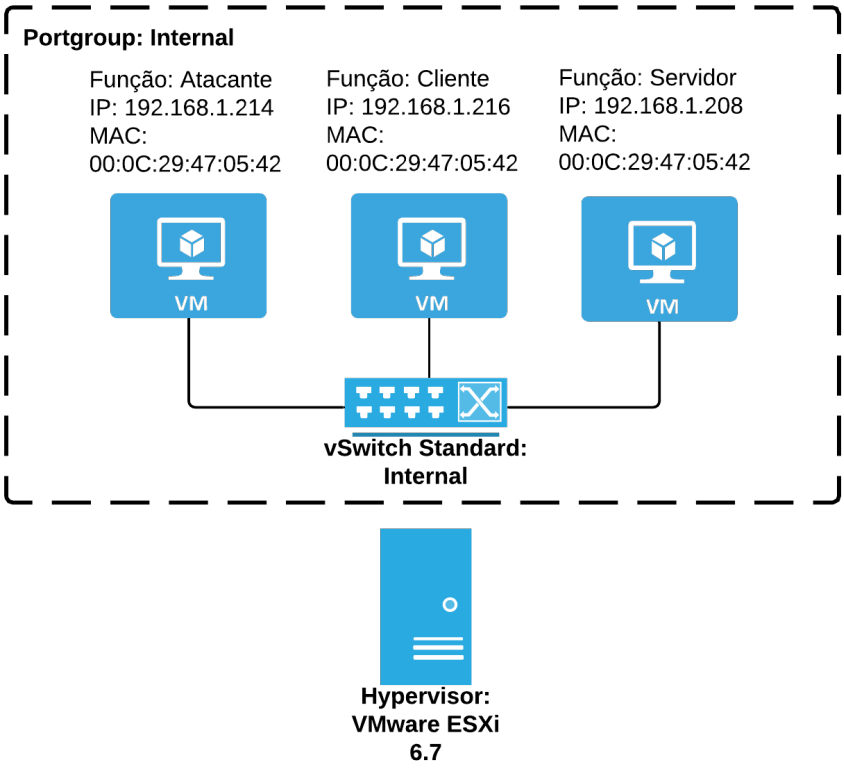

Figura 3.3: Resumo das configurações dos endereços de rede das máquinas virtuais no ambiente VMware.

3.3.2 Instalação e Configuração do Hyper-V

Para a instalação do Hyper-V foi utilizada a imagem disponibilizada pelo provedor de serviço da nuvem. A versão instalada do Windows Server foi a versão Windows Server 2019 Datacenter. A instalação foi feita conforme a documentação oficial da Microsoft.[40]

Após instalado o Windows Server 2019 com Desktop Experience, ou interface gráfica, o Hyper-V foi adicionado a partir do recurso de Adicionar Recursos ao Windows. A rede virtual foi configurada junto com a adição do novo recurso utilizando a placa de rede do servidor para a criação do comutador virtual do tipo "External". A fim de dar conectividade as máquinas virtuais foi criado um comutador do tipo "Internal" e feita uma configuração para que ele pudesse utilizar a internet por meio do comutador externo criado na adição do recurso do Hyper-V a partir de compartilhamento na rede. Dessa forma o comutador interno realiza um NAT para sair para a internet por meio do comutador externo. Para ativar essa funcionalidade de compartilhamento, após criadas as redes virtuais acesse as conexões de rede e altere a propriedade de compartilhamento da rede externa para compartilhar a conexão com a rede interna conforme mostrado na figura 3.4. Todas as máquinas virtuais se encontram no comutador interno.

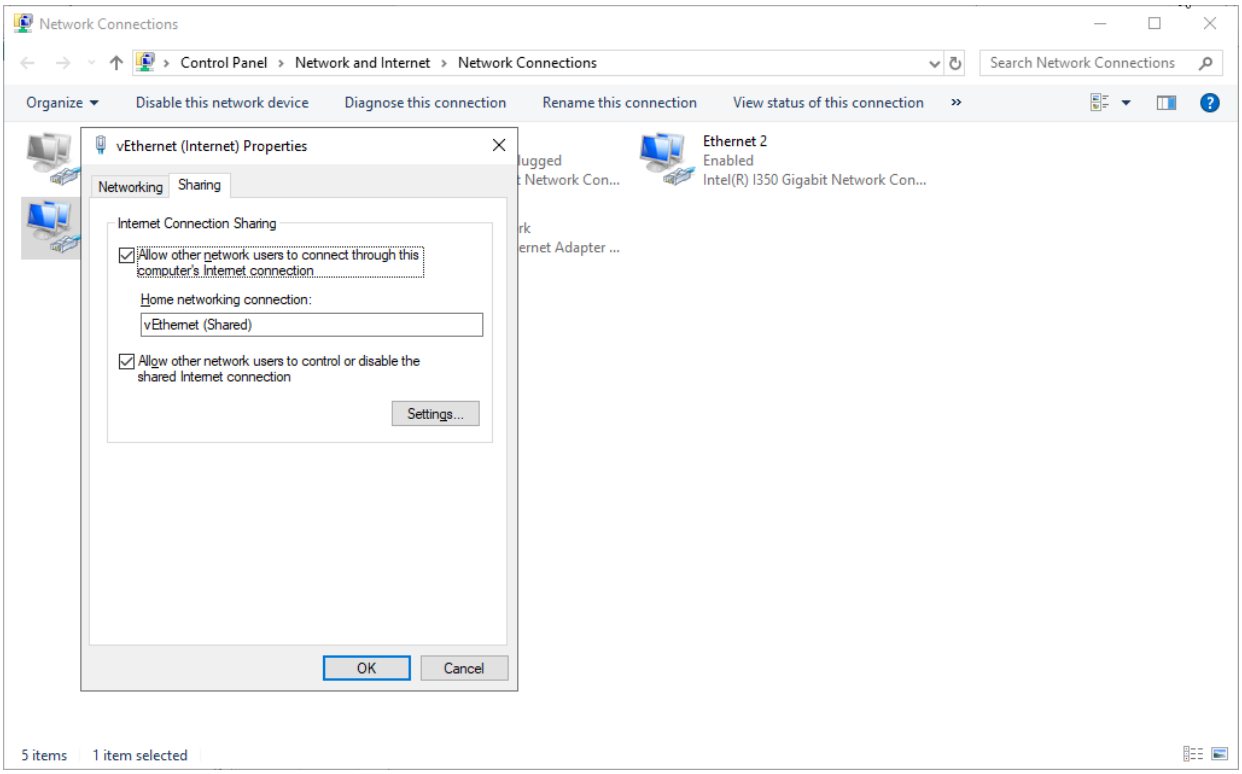

Figura 3.4: Apresentação das configurações de compartilhamento de conexão.

O switch virtual criado para dar conectividade às máquinas foi configurado com as configurações padrão e adicionadas as extensões Microsoft Windows Filtering Platform e Microsoft NDIS Capture. Todas as extensões podem ser verificadas nas figuras 3.5 e 3.6. Na tabela 3.5 tem as configurações feitas na interface gráfica para o virtual switch "Shared".

Para finalizar o pacote de serviços do Hyper-V, Linux Integration Services, foi instalado em cada uma das máquinas virtuais. Esse pacote é instalado automaticamente nos sistemas operacionais suportados pelo Hyper-V. O objetivo do pacote de serviços do Hyper-V é permitir um melhor gerenciamento do virtualizador sobre as máquinas virtuais a partir da obtenção de dados sobre a máquina.

```
PS C:\Users\Administrator> Get-VMSwitch shared

Name   SwitchType NetAdapterInterfaceDescription
----   ---------- ------------------------------
Shared Internal


PS C:\Users\Administrator> Get-vmswitchextension

cmdlet Get-VMSwitchExtension at command pipeline position 1
Supply values for the following parameters:
VMSwitchName[0]: shared
VMSwitchName[1]:


Id                   : E7C3B2F0-F3C5-48DF-AF2B-10FED6D72E7A
Name                 : Microsoft Windows Filtering Platform
Vendor               : Microsoft
Version              : 10.0.17763.1
ExtensionType        : Filter
ParentExtensionId    :
ParentExtensionName  :
SwitchId             : 0daa282a-993d-444b-9cd2-909f303b8f21
SwitchName           : Shared
Enabled              : True
Running              : True
CimSession           : CimSession: .
ComputerName         : WIN-U0I2PULLKKU
IsDeleted            : False

Id                   : EA24CD6C-D17A-4348-9190-09F0D5BE83DD
Name                 : Microsoft NDIS Capture
Vendor               : Microsoft
Version              : 10.0.17763.1
ExtensionType        : Monitoring
ParentExtensionId    :
ParentExtensionName  :
SwitchId             : 0daa282a-993d-444b-9cd2-909f303b8f21
SwitchName           : Shared
Enabled              : True
Running              : False
CimSession           : CimSession: .
ComputerName         : WIN-U0I2PULLKKU
IsDeleted            : False
```

Figura 3.5: Configurações obtidas via CLI para o switch utilizado na solução da Microsoft através dos comandos *Get-VMSwitch* e *Get-VMSwitchExtension*.

Tabela 3.5: Configurações obtidas via console do gerenciador (UI) para o switch utilizado na solução da Microsoft através da console de configuração do vSwitch.

	Virtual Switch "Shared"
Name	Shared
Notes	
Connection type	Internal network
VLAN ID	
Extensions **Microsoft Windows Filtering Platform**	Enabled
Extensions **Microsoft NDIS Capture**	Enabled

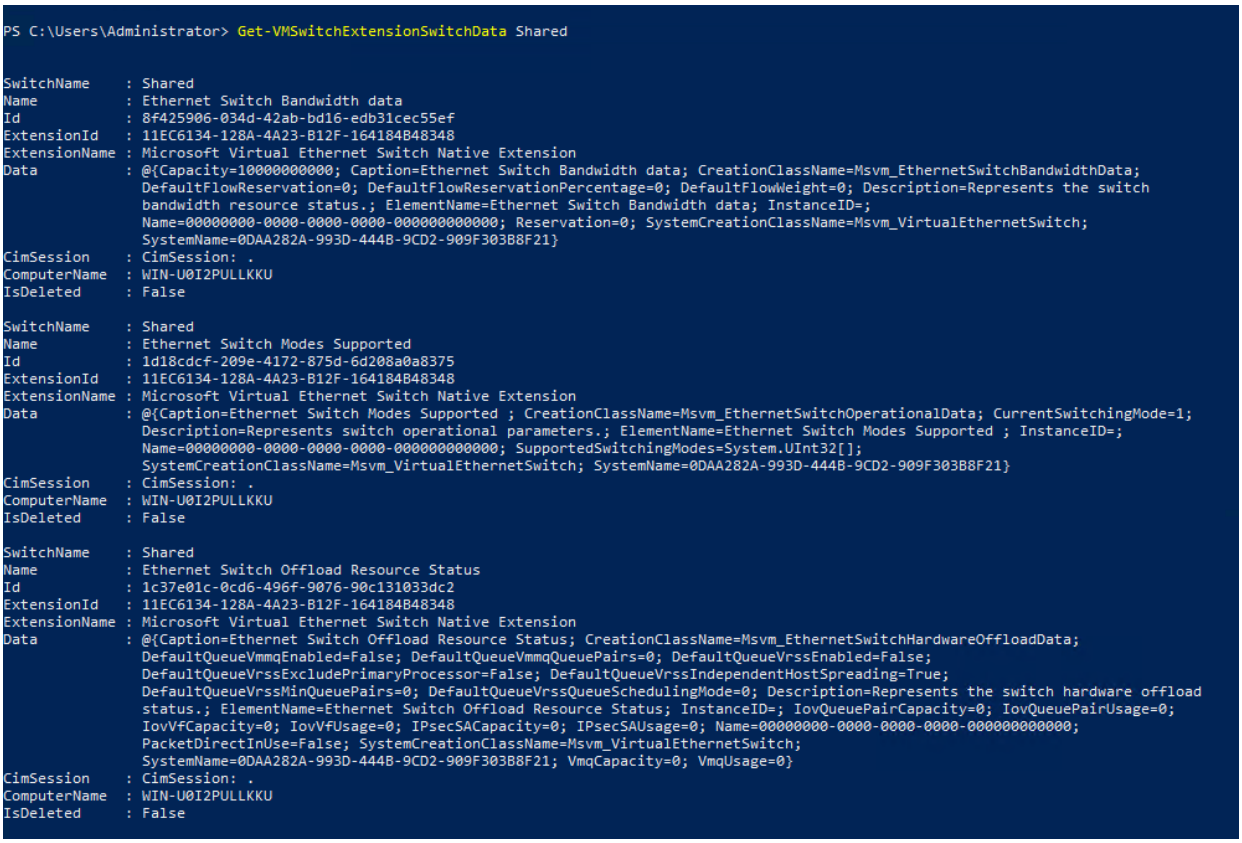

Figura 3.6: Configurações obtidas via CLI para o switch utilizado na solução da Microsoft através do comando *Get-VMSwitchExtensionSwitchData*.

A versão do linux integration services instalada em cada máquina pode ser obtida na tabela 3.6.

Tabela 3.6: Resumo de configurações das máquinas virtuais criadas no ambiente Microsoft.

	Máquina Atacante	**Máquina Desktop**	**Máquina Server**
Sistema operacional Description	Kali GNU/Linux Rolling	Ubuntu Desktop 18.04.2 LTS	Ubuntu Server 18.04.2 LTS
Sistema operacional Release	2019.2	18.04	18.04
IP	192.168.137.226	192.168.137.34	192.168.137.227
MAC	00:15:5D:86:66:07	00:15:5D:86:66:08	00:15:5D:86:66:09
Linux Integration Services Version	4.19.0-kali4-amd64 SMP mod_unload modversions	4.18.0-15-generic mod_unload	4.15.0-45-generic SMP mod_unload

A figura 3.7 representa graficamente as configurações de rede de cada máquina virtual criada no ambiente Microsoft. Essa configuração será utilizada no ambiente Microsoft em todos os testes apresentados posteriormente na seção 3.5.

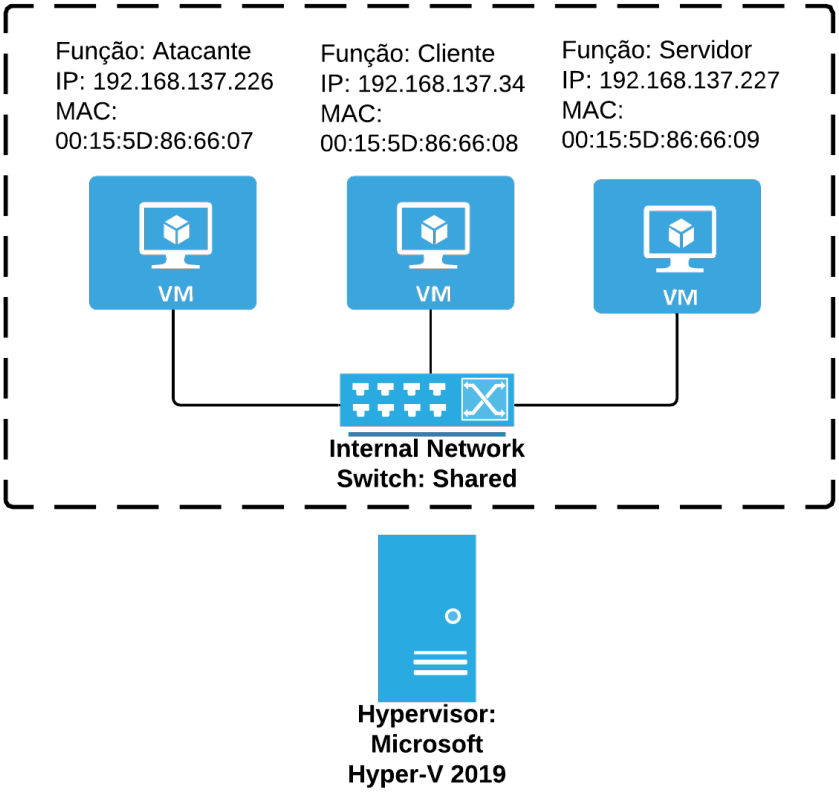

Figura 3.7: Resumo das configurações dos endereços de rede das máquinas virtuais no ambiente Microsoft.

3.4 OBSERVAÇÕES SOBRE TÓPICOS ENCONTRADOS NAS DOCUMENTAÇÕES DAS SOLUÇÕES

3.4.1 Observações para a Solução da VMware

Algumas observações a respeito da solução da VMware com base em sua documentação:

- A VMware chama seus switches virtuais básicos de vSphere Standard Switch ou vSwitch. Segundo a documentação os vSwitches funcionam de forma muito semelhante a switches físicos. Eles detectam as máquinas virtuais logicamente conectadas a eles através de placas de redes virtuais, ou vNIC, e fazem o encaminhamento dos tráfegos da rede para os devidos destinos. Os vSwitches se conectam com os switches físicos na rede utilizando placas de redes físicas dos servidores. Sem que exista uma placa de rede física dedicada para um vSwitch as máquinas virtuais conectadas a eles poderão conversar entre si, mas não com máquinas conectadas a outros switches, pois não tem acesso a rede física.[41][42]

- Existe um recurso que permite criar segmentos de rede a partir de VLANs em um switch virtual. Quando esse recurso está ativado as máquinas virtuais que pertencem a um grupo de portas em uma VLAN não se comunicam com máquinas virtuais em um grupo de portas em uma outra VLAN.[43]

- Existe um recurso que permite criar segmentos de rede com várias VLANs. Quando esse recurso está ativado, as máquinas virtuais que pertencem a esse grupo de portas em modo trunk podem apenas se comunicar com as máquinas virtuais que estejam em um grupo de portas com pelo menos uma das VLANs em trunk. [43]

- Existe um recurso de segurança que pode impedir que uma máquina virtual escute a rede colocando sua interface virtual em modo promiscuo. Quando o recurso que controla o modo promiscuo está configurado para rejeitar a comunicação feita entre máquinas virtuais em um mesmo host, que acontece na memória do hypervisor, não é percebida por outras máquinas virtuais dentro do host.[44][45]

- Existe um recurso de segurança que pode impedir que uma máquina virtual mude seu endereço MAC. Quando o recurso que controla a permissão para uma máquina virtual trocar ou não seu endereço MAC está configurado para rejeitar a troca, a interface se torna inativa até que o endereço na placa de rede no sistema operacional seja o mesmo configurado nas configurações iniciais da máquina virtual no hypervisor.[44][46]

- Existe um recurso de segurança que pode impedir que uma máquina virtual envie pacotes com o campo do endereço MAC diferente daquele que está definido em sua placa de rede. Quando este recurso está configurado para rejeitar tráfegos forjados é feita uma comparação entre o endereço MAC configurado no adaptador de rede e o endereço MAC do remetente no pacote a ser transmitido. Caso esses endereços sejam diferentes o pacote é interceptado pelo switch virtual.[44][47]

3.4.2 Observações para a Solução da Microsoft

Após realizada a implementação do ambiente Hyper-V foram observados alguns pontos:

- Existe um recurso que provê proteção contra ARP spoofing e Neighbor Discovery spoofing. Esse recurso está incluído no comutador virtual e impede que uma máquina virtual utilize de falsificação do protocolo ARP para roubar IPs de outra VMs. Também fornece proteção contra-ataques por IPv6 que visam a falsificação por meio da descoberta de vizinhos ND.[48]
- Existe um recurso que impede mensagens DHCP de servidores não confiáveis cheguem a máquina virtual, realizando assim um DHCP Guard. Esse recurso deve ser configurado no adaptador de rede junto com a lista de servidores DHCP confiáveis. Uma vez configurado as máquinas só poderão receber um IP dos servidores DHCP listados na configuração.[48]
- Existe um recurso que permite o controle de acesso as portas do switch virtual. Através do Power Shell é possível criar filtros baseados em endereços MAC ou IP. Esse recurso é chamado de Access Control List (ACL) e trabalha com regras de entrada e saída para acesso as máquinas ou a rede.[48]
- Existe um recurso que permite que uma appliance virtual seja implementada e que o tráfego de diversas VLANs seja redirecionado para essa appliance permitindo uma configuração em modo trunk. Dessa forma máquinas nessas VLANs em trunk podem se comunicar.[48]
- Existe um recurso que permite o monitoramento do tráfego que passa pelo switch. Esse recurso depende da instalação do recurso "Network Monitor" em uma máquina virtual e a configuração de port mirroring nas máquinas virtuais para direcionar o tráfego de suas placas de rede virtuais para a placa de rede da máquina de monitoramento.[48]
- Existe um recurso que permite criar segmentos de rede a partir de VLANs em um switch virtual. Quando esse recurso está ativado as máquinas virtuais que pertencem a um grupo de portas em uma VLAN não se comunicam com máquinas virtuais em um grupo de portas em uma outra VLAN.[40]

3.5 TESTES A SEREM EXECUTADOS SOBRE O AMBIENTE

3.5.1 Ataques Realizados

Dentre os ataques mencionados na seção 2.4 apenas 3 serão utilizados para os testes nesse trabalho: Sniffing, spoofing e port scan. A escolha desses três ataques foi feita por eles serem ataques que podem prover informação para a execução de outros ataques, máscarar a identidade do atacante ou ser o passo inicial de outros ataques.

Os testes serão executados segundo as seguintes premissas:

1. A intenção é analisar a segurança da rede virtual dentro do host.
2. A rede física é preparada para conter as ameaças que cheguem a ela.
3. O atacante já está em posse de uma máquina virtual com conectividade a rede virtual.
4. O atacante tem permissão de administrador na máquina que ele tem acesso.
5. As máquinas dentro da rede virtual não têm acesso à internet.
6. O foco é ataques de rede, assim ataques baseados em explorar vulnerabilidades de sistema não serão abordados.
7. O atacante não tem nenhum tipo de permissão sobre a infraestrutura de virtualização.
8. Todos os testes serão feitos com todas as máquinas no mesmo segmento de rede.
9. Somente serão utilizadas medidas de prevenção que existam na configuração dos virtualizadores.
10. O nível de virtualização se encontra apenas na virtualização de servidores.

3.5.1.1 Sniffing

Para a realização do ataque de sniffing, foi ativado o recurso de captura de pacotes Wireshark na máquina Kali Linux com a interface de rede em modo promíscuo. Enquanto o servidor e o cliente trocavam requisições HTTP, o sniffer escutava o meio de comunicação e capturava os pacotes que ele podia ouvir.

O ataque será feito com as seguintes configurações:

- Uso de uma máquina ubuntu server como servidor web;
- Uso de uma máquina ubuntu desktop para consumir o serviço web.
- Uso de um Kali linux versão 2019.2 como sistema operacional para uso da aplicação sniffer;
- Uso de Wireshark versão 2.6.8-1.1 para a captura dos pacotes atuando como sniffer;

Caso a máquina Kali Linux consiga obter os pacotes HTTP enviados entre as máquinas servidor e cliente o ataque será considerado bem-sucedido, caso contrário dado como falha.

O ataque será realizado com base nos passos registrados de forma resumida na figura 3.8. A baixo temos um passo a passo um pouco mais detalhado.

1. Na solução de virtualização serão configuradas as medidas de proteção disponíveis contra sniffing.
   (a) Na solução da VMware configurado para rejeitar o modo promiscuo.

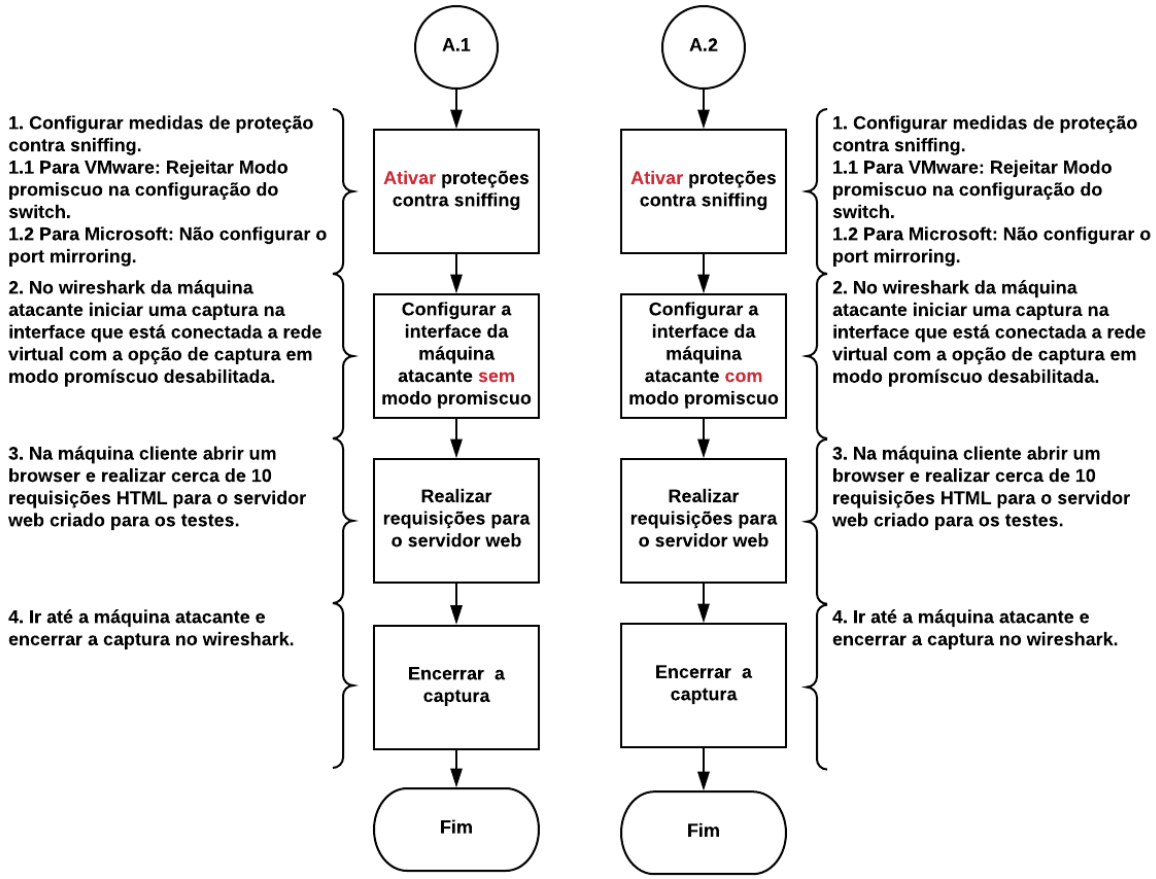

Figura 3.8: Fluxogramas resumidos para os testes de sniffing. Fluxo A.1 realiza os testes sem a interface em modo promíscuo. Fluxo A.2 realiza os testes com a interface em modo promíscuo.

i. No switch virtual edite as configurações de segurança em relação ao modo promiscuo para "Reject".

(b) Na solução da Microsoft não foi configurado o recurso de port mirroring na placa de rede em nenhuma máquina virtual.

2. Na máquina kali linux será utilizado o wireshark a fim de interceptar as comunicações entre a máquina ubuntu desktop e a máquina ubuntu server.

3. Será iniciada a captura de pacotes no wireshark na máquina kali linux.

   (a) No wireshark configure a captura para capturar pacotes na interface conectada a rede virtual.

   (b) Na configuração da captura habilite o modo promíscuo.

4. Serão tocadas requisições HTTP entre o cliente e o servidor.

   (a) Na máquina ubuntu desktop, abra o navegador e realize uma consulta HTML ao endereço do servidor web criado para os testes.

   (b) Repita a consulta cerca de 10 vezes para gerar um volume maior de dados.

5. Será encerrada a captura dos pacotes.

6. Será iniciada uma nova captura de pacotes no wireshark na máquina kali linux.

   (a) No wireshark configure a captura para capturar pacotes na interface conectada a rede virtual.

   (b) Na configuração da captura desabilite o modo promíscuo.

7. Serão tocadas requisições HTTP entre o cliente e o servidor.

   (a) Na máquina ubuntu desktop, abra o navegador e realize uma consulta HTML ao endereço do servidor web criado para os testes.

   (b) Repita a consulta cerca de 10 vezes para gerar um volume maior de dados.

8. Será encerrada a captura dos pacotes.

A contraprova será realizada com base nos passos registrados na figura 3.9. A baixo temos um passo a passo um pouco mais detalhado.

1. Na solução de virtualização serão retiradas as medidas de proteção disponíveis contra Sniffing.

   (a) Na solução da VMware configurado para aceitar o modo promiscuo.

      i. No switch virtual edite as configurações de segurança em relação ao modo promiscuo para "Reject".

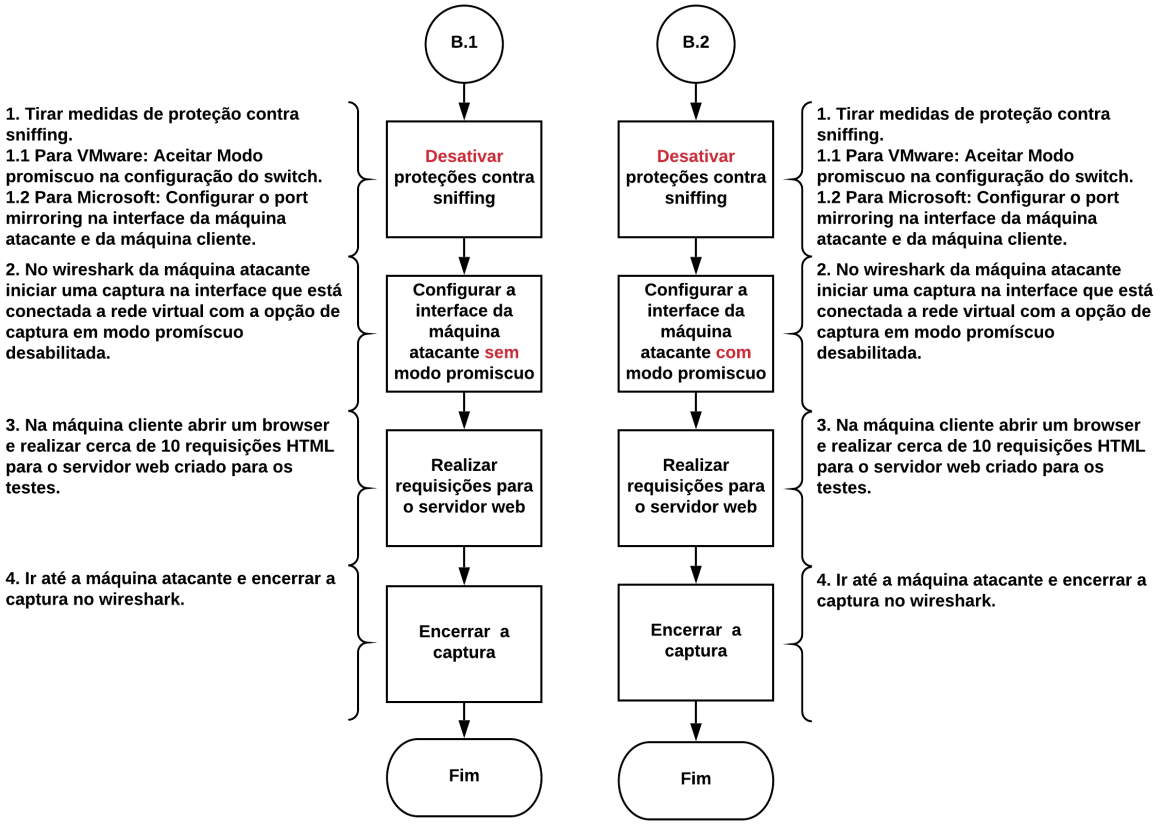

Figura 3.9: Fluxogramas resumidos para as contraprovas dos testes de sniffing. Fluxo B.1 realiza as contraprovas sem a interface em modo promíscuo. Fluxo B.2 realiza as contraprovas com a interface em modo promíscuo.

(b) Na solução da Microsoft foi configurado o recurso de port mirroring na placa de rede das máquinas virtuais.

i. Na placa de rede da máquina atacante configure o port mirroring como "Destinantion".

ii. Na placa de rede da máquina cliente configure o port mirroring como "Source".

2. Na máquina kali linux será utilizado o wireshark a fim de interceptar as comunicações entre a máquina ubuntu desktop e a máquina ubuntu server.

3. Será iniciada a captura de pacotes no wireshark na máquina kali linux.

   (a) No wireshark configure a captura para capturar pacotes na interface conectada a rede virtual.

   (b) Na configuração da captura habilite o modo promíscuo.

4. Serão tocadas requisições HTTP entre o cliente e o servidor.

   (a) Na máquina ubuntu desktop, abra o navegador e realize uma consulta HTML ao endereço do servidor web criado para os testes.

   (b) Repita a consulta cerca de 10 vezes para gerar um volume maior de dados.

5. Será encerrada a captura dos pacotes.

6. Será iniciada uma nova captura de pacotes no wireshark na máquina kali linux.

   (a) No wireshark configure a captura para capturar pacotes na interface conectada a rede virtual.

   (b) Na configuração da captura desabilite o modo promíscuo.

7. Serão tocadas requisições HTTP entre o cliente e o servidor.

   (a) Na máquina ubuntu desktop, abra o navegador e realize uma consulta HTML ao endereço do servidor web criado para os testes.

   (b) Repita a consulta cerca de 10 vezes para gerar um volume maior de dados.

8. Será encerrada a captura dos pacotes.

3.5.1.2 Spoofing

Para a realização do ataque de spoofing, a máquina Kali Linux foi colocada sobre o mesmo segmento de rede que a máquina Ubuntu Server e a máquina Ubuntu Desktop. A máquina Kali Linux assumiu a identidade do servidor Ubuntu utilizando de ARP poisoning em um ataque de man-in-the-middle (MITM). A máquina Ubuntu Desktop fez requisições HTTP para o servidor Ubuntu enquanto a máquina Kali Linux assumia a identidade dele na rede.

O ataque será feito com as seguintes configurações:

- Uso de uma máquina ubuntu server como servidor web;
- Uso de uma máquina ubuntu desktop para consumir o serviço web.
- Uso de um Kali linux versão 2019.2 como plataforma para o ataque;
- Uso do recurso arpspoof versão 2.4 disponível no Kali Linux;

Caso a página HTTP se torne indisponível, o ataque será considerado bem-sucedido, caso contrário dado como falha.

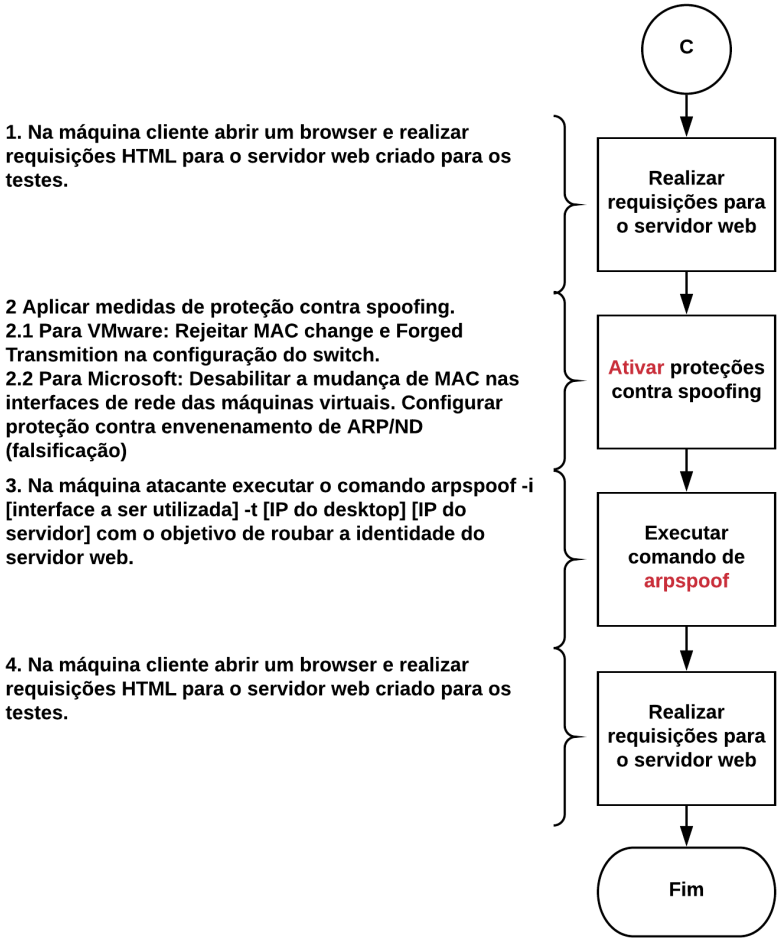

Figura 3.10: Fluxograma resumido para os testes de spoofing.

O teste será realizado com base nos passos registrados na figura 3.10. A baixo temos um passo a passo um pouco mais detalhado:

1. Serão feitas requisições HTTP da máquina ubuntu desktop para a máquina ubuntu server.
   (a) Na máquina ubuntu desktop, abra o navegador e realize uma consulta HTML ao endereço do servidor web criado para os testes.

2. Na solução de virtualização serão configuradas as medidas de proteção disponíveis contra ARP Spoofing.

   (a) Na solução da VMware:

      i. No switch virtual da solução da VMware configurado "Reject" para mudança de endereço MAC (MAC Address Change)

      ii. No switch virtual da solução da VMware configurado "Reject" parar transmissões forjadas (Forged Transmits).

   (b) Na solução da Microsoft:

      i. A proteção contra envenenamento de ARP/ND (falsificação) está incluída no comutador virtual.[48]

      ii. Não habilitar na placa virtual da máquina atacante a permissão para troca de endereço MAC.

3. Na máquina kali linux será utilizada a função de arpspoof para que a máquina kali linux se passe pela máquina ubuntu server a fim de interceptar as comunicações entre a máquina ubuntu desktop e a máquina ubuntu server.

   (a) Na máquina kali linux abra o terminal

   (b) Execute o comando *arpspoof -i [interface a ser utilizada] -t [IP do desktop] [IP do servidor]*, alterando os parâmetros conforme as características das máquinas.

4. Serão feitas requisições HTTP da máquina ubuntu desktop para a máquina ubuntu server.

   (a) Na máquina ubuntu desktop, atualize o navegador e realize uma consulta HTML ao endereço do servidor web criado para os testes.

A contraprova será realizada com base nos passos registrados na figura 3.11. A baixo temos um passo a passo um pouco mais detalhado.

1. Serão feitas requisições HTTP da máquina ubuntu desktop para a máquina ubuntu server.

   (a) Na máquina ubuntu desktop, abra o navegador e realize uma consulta HTML ao endereço do servidor web criado para os testes.

2. Na solução de virtualização serão retiradas as medidas de proteção disponíveis contra ARP Spoofing.

   (a) Na solução da VMware:

      i. No switch virtual da solução da VMware configurado "Accept" para mudança de endereço MAC (MAC Address Change)

      ii. No switch virtual da solução da VMware configurado "Accept" para transmissões forjadas (Forged Transmits).

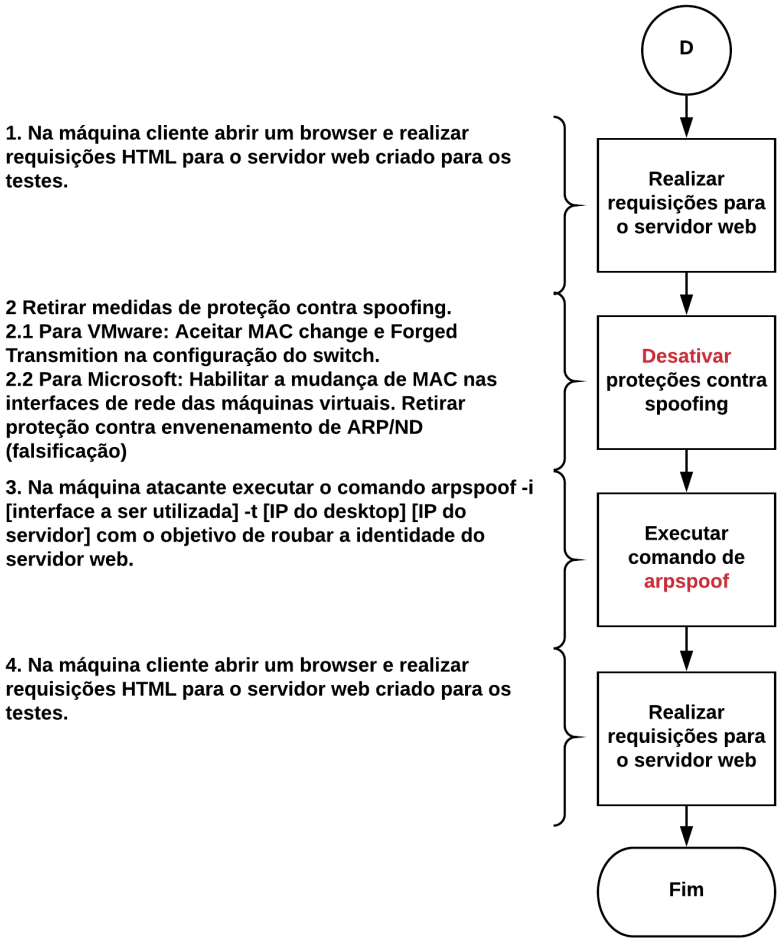

Figura 3.11: Fluxograma resumido para a contraprova dos testes de spoofing.

(b) Na solução da Microsoft:

i. A proteção contra envenenamento de ARP/ND (falsificação) está incluída no comutador virtual.[48] Não foi encontrada forma de desabilitar.

ii. Habilitar na placa virtual da máquina atacante a permissão para troca de endereço MAC.

3. Na máquina kali linux será utilizada a função de arpspoof para que a máquina kali linux se passe pela máquina ubuntu server a fim de interceptar as comunicações entre a máquina ubuntu desktop e a máquina ubuntu server.

(a) Na máquina kali linux abra o terminal

(b) Execute o comando *arpspoof -i [interface a ser utilizada] -t [IP do desktop] [IP do servidor]*, alterando os parâmetros conforme as características das máquinas.

4. Serão feitas requisições HTTP da máquina ubuntu desktop para a máquina ubuntu server.

(a) Na máquina ubuntu desktop, atualize o navegador e realize uma consulta HTML ao endereço do servidor web criado para os testes.

3.5.1.3 Port Scan

Para a realização do ataque de port scan, a máquina Kali linux executará a ferramenta NMAP a fim de descobrir o máximo de informações sobre a rede.

O ataque será feito com as seguintes configurações:

- Uso de um Kali linux versão 2019.2 como plataforma para o ataque;
- Uso do recurso NMAP versão 7.70 disponível no Kali Linux;
- As máquinas ubuntu desktop e ubuntu server estarão na mesma rede.

O ataque será realizado com base nos passos registrados na figura 3.12. A baixo temos um passo a passo um pouco mais detalhado.

1. Na solução de virtualização serão configuradas as medidas de proteção disponíveis nos switches virtuais e nas placas de rede.

(a) Na solução da VMware:

i. No switch virtual da solução da VMware configurado "Reject" para modo promiscuo (Promiscuos)

ii. No switch virtual da solução da VMware configurado "Reject" para mudança de endereço MAC (MAC Address Change)

iii. No switch virtual da solução da VMware configurado "Reject" para transmissões forjadas (Forged Transmits).

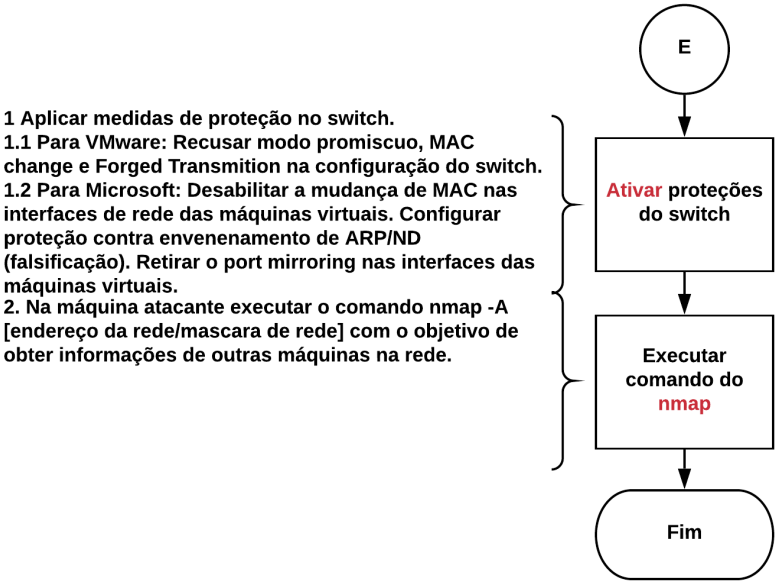

Figura 3.12: Fluxograma resumido para os testes de port scan.

(b) Na solução da Microsoft:

i. Não foi configurado o port mirroring na interface de rede das máquinas virtuais.

ii. A proteção contra envenenamento de ARP/ND (falsificação) está incluída no comutador virtual.[48] Não foi encontrada forma de desabilitar.

iii. Desabilitar na placa virtual da máquina atacante a permissão para troca de endereço MAC.

2. A partir da máquina kali linux será realizada a varredura da rede utilizando o recurso NMAP.

(a) Abra o terminal na máquina kali linux.

(b) Execute o comando nmap -A [endereço da rede/ máscara de rede]. Substitua os parâmetros conforme as configurações da rede.

A contraprova será realizada com base nos passos registrados na figura 3.13. A baixo temos um passo a passo um pouco mais detalhado.

1. Na solução de virtualização serão retiradas as medidas de proteção disponíveis nos switches virtuais e nas placas de rede.

(a) Na solução da VMware:

i. No switch virtual da solução da VMware configurado "Accept" para modo promiscuo (Promiscuos)

ii. No switch virtual da solução da VMware configurado "Accept" para mudança de endereço MAC (Mac Address Change)

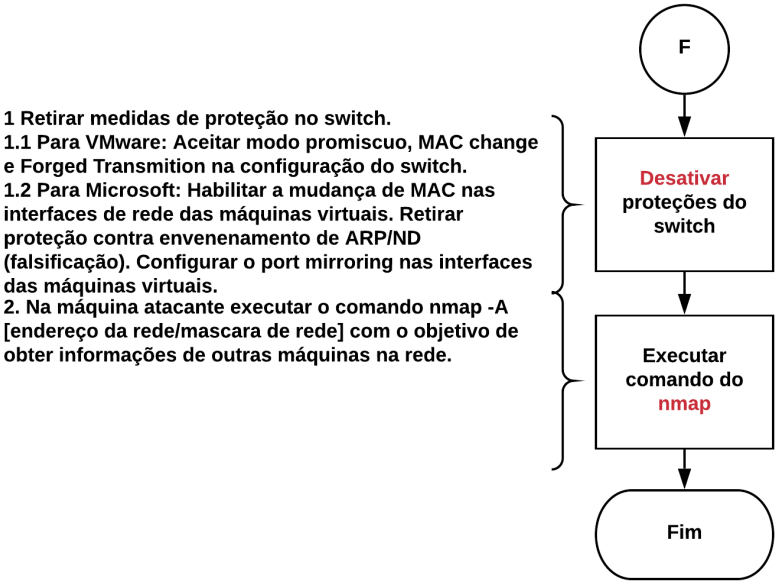

Figura 3.13: Fluxograma resumido para as contraprovas dos testes de port scan.

iii. No switch virtual da solução da VMware configurado "Accept" para transmissões forjadas (Forged Transmits).

(b) Na solução da Microsoft:

i. Na placa de rede da máquina atacante configure o port mirroring como "Destinantion".

ii. Na placa de rede da máquina cliente configure o port mirroring como "Source".

iii. Na placa de rede da máquina servidor configure o port mirroring como "Source".

iv. A proteção contra envenenamento de ARP/ND (falsificação) está incluída no comutador virtual.[48] Não foi encontrada forma de desabilitar.

v. Desabilitar na placa virtual da máquina atacante a permissão para troca de endereço MAC.

2. A partir da máquina kali linux será realizada a varredura da rede utilizando o recurso NMAP.

(a) Abra o terminal na máquina kali linux.

(b) Execute o comando nmap -A [endereço da rede/máscara de rede]. Substitua os parâmetros conforme as configurações da rede.

Caso a ferramenta NMAP consiga descobrir informações de serviços e sistema operacional sobre as outras duas máquinas virtuais o ataque será considerado bem-sucedido.

3.6 RELATO DE COMPORTAMENTO CONFORME DOCUMENTAÇÃO ANALISADA

Com base no que foi descoberto na documentação dos produtos, aqui está o comportamento esperado em relação aos ataques apresentados na seção 3.5 e executados para a realização dos testes.

3.6.1 Comportamento da solução da VMware

Com base no que foi observado na documentação, foram assumidas as seguintes hipóteses teóricas a respeito do comportamento da solução da VMware:

3.6.1.1 Comportamento para sniffing

Como a comunicação é feita apenas em memória para tráfegos entre máquinas em um mesmo servidor, sem o modo promíscuo habilitado e caso a máquina em escuta seja uma máquina virtual, não é possível escutar a comunicação que passa pela rede virtual. Logo ao realizar uma captura de pacotes apenas seriam capturados os pacotes com destino à interface da máquina em escuta ou pacotes transmitidos com destino em broadcast. Caso a máquina em escuta não seja uma máquina virtual, mas esteja na rede física, é possível realizar a captura dos pacotes entre quaisquer máquinas que estejam em switches virtuais diferentes. Uma vez que o tráfego precisa ser redirecionado para rede física a fim de ser encaminhado e roteado se necessário até o devido destino. Dessa forma um sniffer no mesmo segmento de rede dos servidores consegue capturar os pacotes da comunicação entre as máquinas virtuais.

3.6.1.2 Comportamento para spoofing

Como é feita uma verificação entre o endereço MAC no adaptador de rede virtual e o endereço MAC na configuração da placa de rede virtual quando o recurso de rejeitar mudanças de endereço MAC está habilitado, o hypervisor consegue impedir que trocas de endereço MAC na configuração da máquina virtual, sejam propagadas pela rede. Como é feita uma verificação entre o endereço MAC da origem descrito no pacote e o endereço MAC do adaptador de rede quando o recurso de rejeitar transmissões forjadas está habilitado, o hypervisor consegue impedir que máquinas virtuais gerenciadas por ele efetuem spoofing a partir de ARP Poisoning. Caso a máquina à efetuar o spoofing esteja fora do ambiente virtual, o hypervisor não será capaz de detectar a ameaça. Logo caso não existam outras medidas para conter ataques de ARP Poisoning existirá uma vulnerabilidade de rede na rede física que influencia no ambiente virtual.

3.6.1.3 Comportamento para port scan

Configurações de segmentação de rede podem diminuir o impacto de port scans na rede, contudo não existem medidas de segurança de visam impedir a realização de port scan documentadas na documentação oficial do fabricante. Logo os ataques de descoberta de rede serão bem-sucedidos.

3.6.2 Comportamento da solução da Microsoft

Com base no que foi observado, foram assumidas as seguintes hipóteses teóricas a respeito do comportamento da solução da Microsoft:

3.6.2.1 Comportamento para sniffing

Como a comunicação é feita em memória para tráfegos entre máquinas em um mesmo servidor, caso a máquina em escuta seja uma máquina virtual e o espelhamento de porta não esteja habilitado nas configurações de rede da máquina atacante e na máquina da qual se deseja capturar os pacotes, não é possível escutar a comunicação que passa pela rede virtual. Logo ao realizar uma captura de pacotes apenas seriam capturados os pacotes com destino à interface da máquina em escuta ou pacotes transmitidos em broadcast. Caso a máquina em escuta não seja uma máquina virtual, mas esteja na rede física, é possível realizar a captura dos pacotes entre quaisquer máquinas que estejam em comutadores virtuais diferentes. Uma vez que o tráfego precisa ser redirecionado através da rede física, um sniffer no mesmo segmento de rede dos servidores consegue capturar os pacotes da comunicação entre as máquinas virtuais.

3.6.2.2 Comportamento para spoofing

Como é feita uma verificação entre o endereço MAC no adaptador de rede virtual e o endereço MAC na configuração da placa de rede virtual quando o recurso de rejeitar mudanças de endereço MAC está habilitado, o hypervisor consegue impedir que trocas de endereço MAC na configuração da máquina virtual, sejam propagadas pela rede. Além disso o como existe uma proteção contra envenenamento de ARP/ND (falsificação) incluída no switch não será possível realizar ataques de ARP spoofing. Caso a máquina a efetuar o spoofing esteja fora do ambiente virtual, o hypervisor não será capaz de detectar a ameaça. Logo caso não existam outras medidas para conter ataques de ARP Poisoning existirá uma vulnerabilidade de rede na rede física que influencia no ambiente virtual.

3.6.2.3 Comportamento para port scan

Configurações de segmentações de rede podem diminuir o impacto de port scans na rede. A criação de ACL é uma opção, mas é feita de forma totalmente manual tendo que identificar o ataque e então construir uma ACL que impeça a comunicação entre as duas máquinas. Dessa forma os ataques de varredura de rede serão bem-sucedidos.

4 RESULTADOS E ANÁLISE DOS TESTES

Neste capítulo serão apresentados os resultados obtidos após os testes documentados na seção 3.5. Será feita também uma análise sobre os resultados obtidos. Para uma melhor organização, para cada teste será utilizada uma seção.

4.1 ATAQUES DE SNIFFING

Para os testes de sniffing foram postos o sniffer, o servidor web e o cliente web na mesma rede, conforme figura 3.3 e 3.7 para a solução da VMware e Microsoft respectivamente.

Enquanto o servidor e o cliente trocavam requisições HTTP, o sniffer escutava o meio de comunicação e capturava os pacotes que ele podia ouvir. Para mais informações sobre como foi realizado o ataque consultar a seção 3.5.1.1

4.1.1 Na solução da VMWARE: ESXi

Com os ataques de sniffing na solução da VMware, foram obtidos os seguintes resultados:

Ao realizar o ataque com as proteções ativadas no switch virtual o atacante não conseguiu capturar a comunicação entre as máquinas ubuntu desktop e ubuntu server. Esse comportamento foi observado tanto com a interface da máquina kali linux sem o modo promiscuo habilitado quanto com modo promiscuo habilitado.

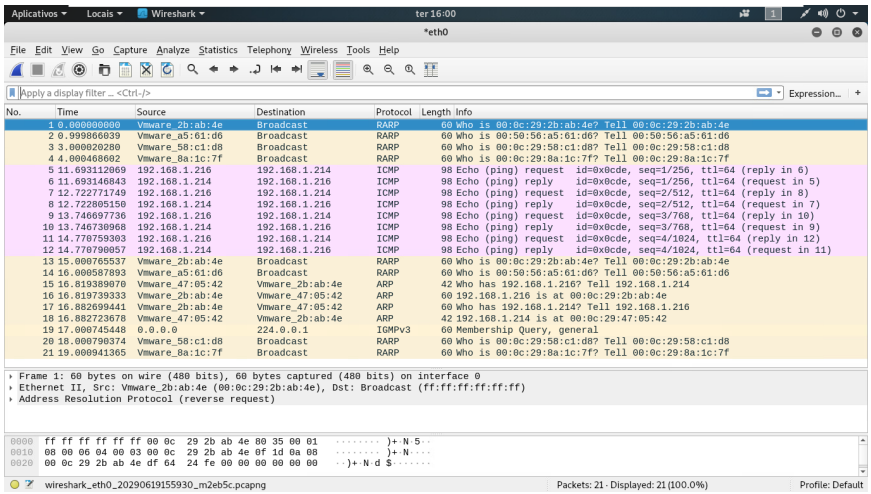

Figura 4.1: Configuração da interface em modo promiscuo.

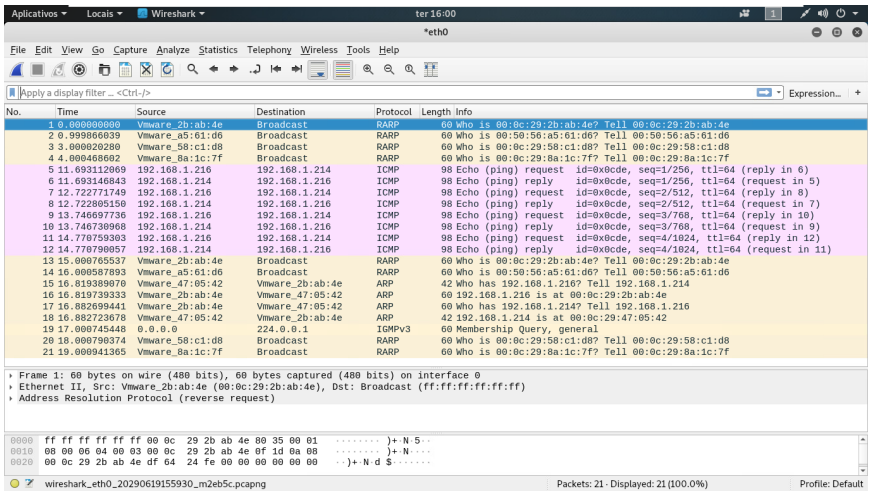

Figura 4.2: Captura de pacotes com a interface em modo promiscuo e o switch virtual configurado para rejeitar o modo promiscuo.

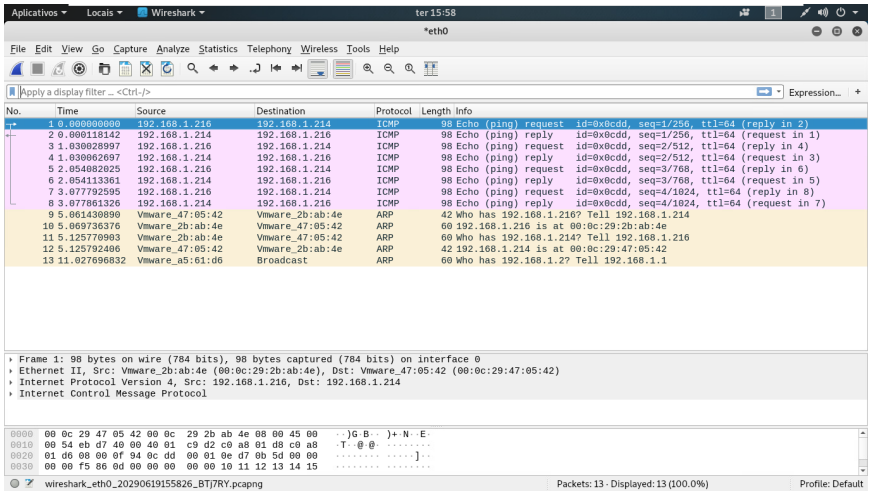

Figura 4.3: Captura de pacotes com a interface em modo promiscuo e o switch virtual configurado para rejeitar o modo promiscuo.

As figuras 4.2 e 4.3. mostram que os únicos tráfegos que puderam ser capturados foram os tráfegos com destino a máquina atacante, tráfegos com destino em broadcast ou tráfegos gerados pela máquina atacante. As informações de endereçamento das máquinas podem ser encontradas na tabela 3.4.

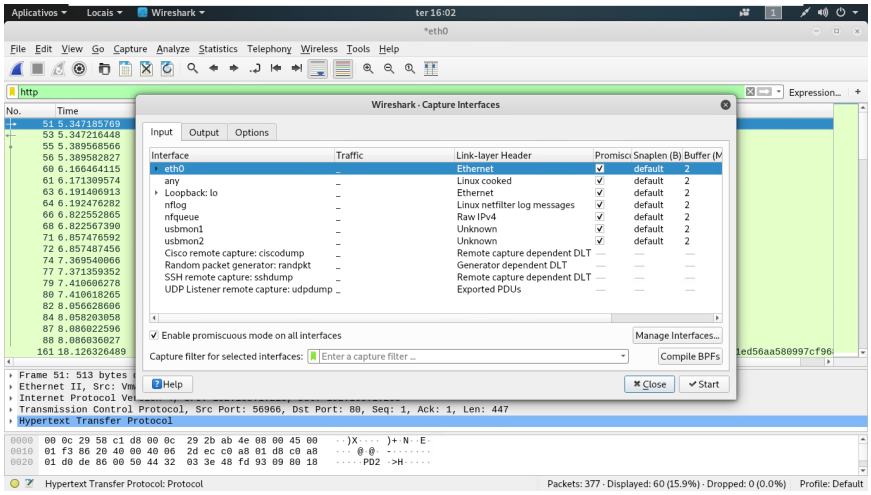

Figura 4.4: Configuração da interface em modo promiscuo.

Ao realizar a contraprova, permitindo o modo promíscuo no virtual switch, foi possível capturar os pacotes da comunicação entre o ubuntu desktop e o ubuntu server quando a interface da máquina atacante estava configurada em modo promiscuo, observe as figuras 4.4 e 4.5.

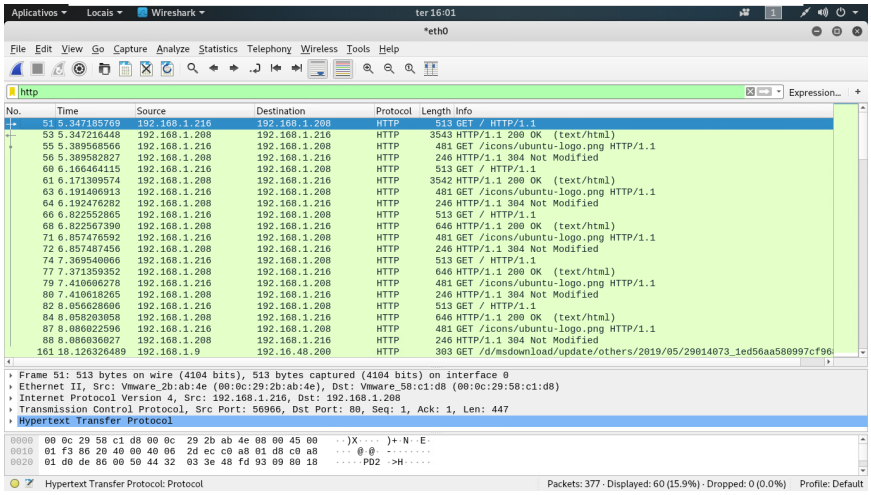

Figura 4.5: Captura de pacotes com a interface em modo promiscuo e o switch virtual configurado para aceitar o modo promiscuo.

Na figura 4.5 a máquina de endereço IP 192.168.1.216 é o ubuntu desktop que realiza várias requisições HTTP para a máquina de endereço IP 192.168.1.208 que é o ubuntu server que contém um apache versão 2.14 instalado. A máquina kali está realizando a captura através do wireshark. Por estar na mesma rede ela obtém os dados da comunicação entre as outras máquinas. Mais informações de endereçamento estão descritas na tabela 3.4.

Com os ataques de sniffing na solução da VMware, foi possível observar que:

A solução da VMware utiliza de mapeamento virtual da rede em memória. Os switches virtuais e as placas de rede virtuais são mapeadas e o tráfego entre as máquinas é realizado na memória do servidor. Dessa forma quando duas máquinas virtuais precisam se comunicar o pacote é entregue do endereço mapeado em memória da placa de rede virtual da primeira máquina virtual direto para o endereço mapeado em memória da placa de rede virtual da segunda máquina. Logo máquinas que estejam em um mesmo segmento da rede virtual não são capazes de observar a comunicação.

Por conta desse modo de funcionamento do ambiente virtual não é possível realizar a captura de pacotes a respeito de comunicações que não são destinadas ou remetidas pela máquina atacante. Como a comunicação ocorre diretamente entre duas máquinas os pacotes não serão observados pela interface virtual da máquina atacante, dado que o endereço das interfaces virtuais mapeado em memória na comunicação entre as máquinas ubuntu server e ubuntu desktop não é o endereço da máquina atacante kali linux.

Na solução da VMware para que se torne possível a captura de pacotes na rede virtual é preciso que seja habilitada uma configuração onde todo e qualquer pacote que seja gerado nas interfaces virtuais das máquinas no segmento da rede virtual seja entregue em todas as interfaces virtuais mapeadas na memória. Dessa forma é criado um barramento virtual de onde todas as máquinas podem observar o tráfego da rede.

Apesar de não ser possível capturar pacotes através de ataques a rede virtual apenas ativando o modo promíscuo na interface da máquina atacante, existem outras formas de realizar a captura de pacotes. Essas formas serão posteriormente apresentadas e discutidas na seção 4.4 nesse mesmo capítulo.

4.1.2 Na solução da MICROSOFT: HYPER-V

Com os ataques de sniffing na solução da Microsoft, foram obtidos os seguintes resultados:

Ao realizar o ataque com as proteções ativadas a máquina atacante não conseguiu capturar a comunicação entre as máquinas ubuntu desktop e ubuntu server. Isso ocorreu tanto com a interface da máquina kali linux sem ou com o modo promiscuo habilitado.

Os únicos tráfegos que puderam ser capturados foram os tráfegos com destino a máquina atacante de endereço IP 192.168.137.226, tráfegos com destino em broadcast ou tráfegos gerados pela máquina atacante, observe as figuras 4.3 e 4.7. Mais informações sobre o endereçamento da máquina virtual podem ser obtidas através da tabela 3.6

Ao realizar a contraprova permitindo o modo promíscuo no virtual switch, foi possível capturar os pacotes da comunicação entre o ubuntu desktop e o ubuntu server. Para isso a interface da máquina atacante estava configurada com o port mirroring como destino e a máquina ubuntu desktop estava configurada com o port mirroring como fonte.

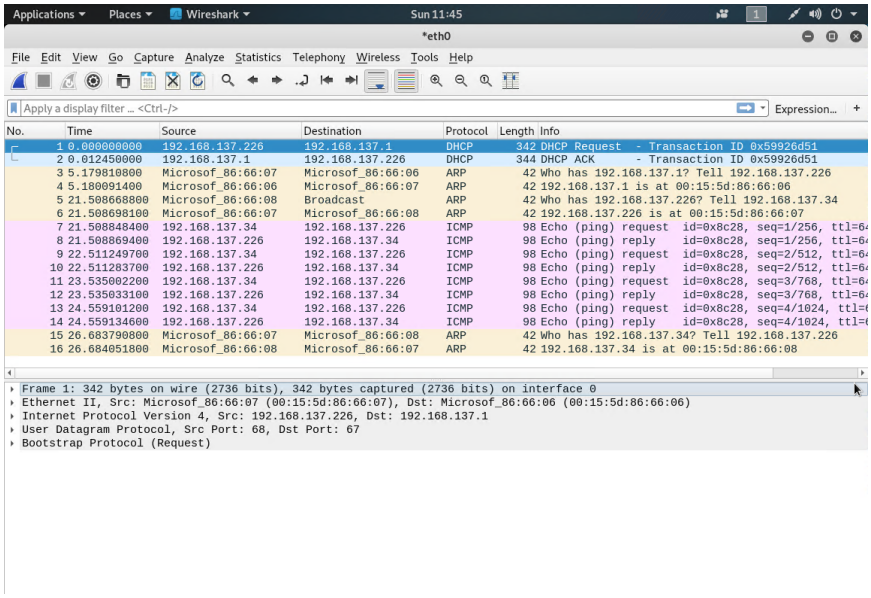

Figura 4.6: Captura de pacotes com a interface em modo promiscuo e o switch virtual configurado para rejeitar o modo promiscuo.

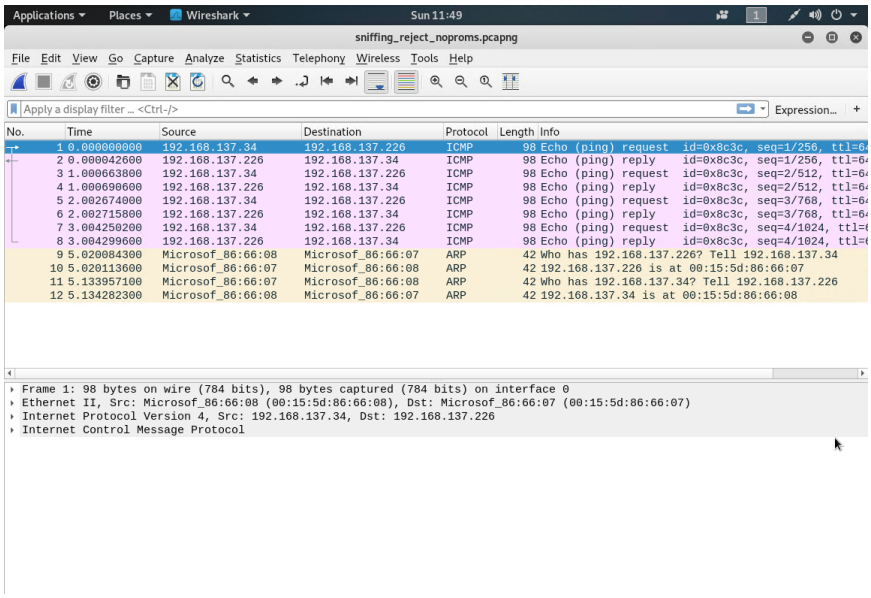

Figura 4.7: Captura de pacotes com a interface em modo promiscuo e o switch virtual configurado para rejeitar o modo promiscuo.

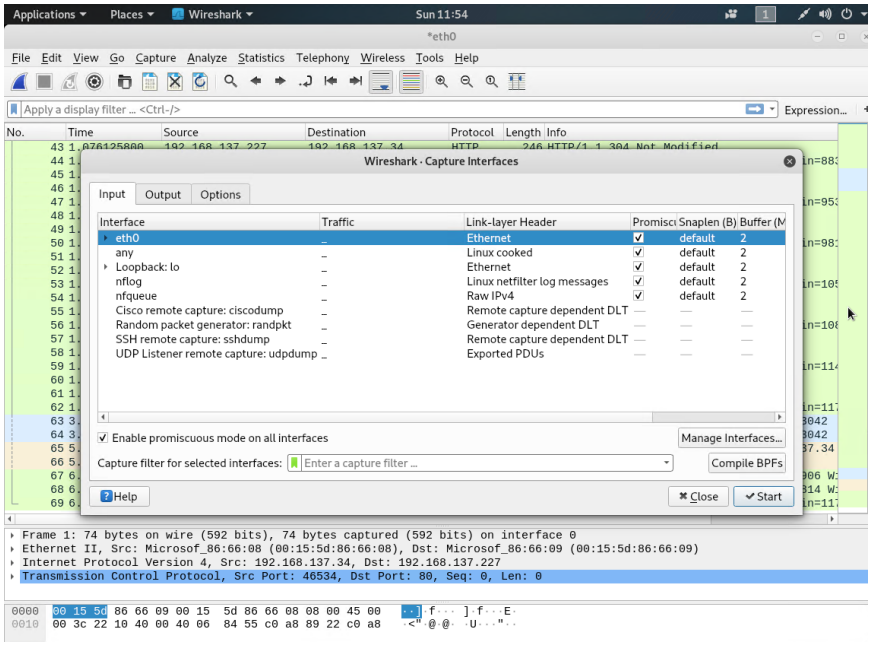

Figura 4.8: Configuração da interface em modo promiscuo.

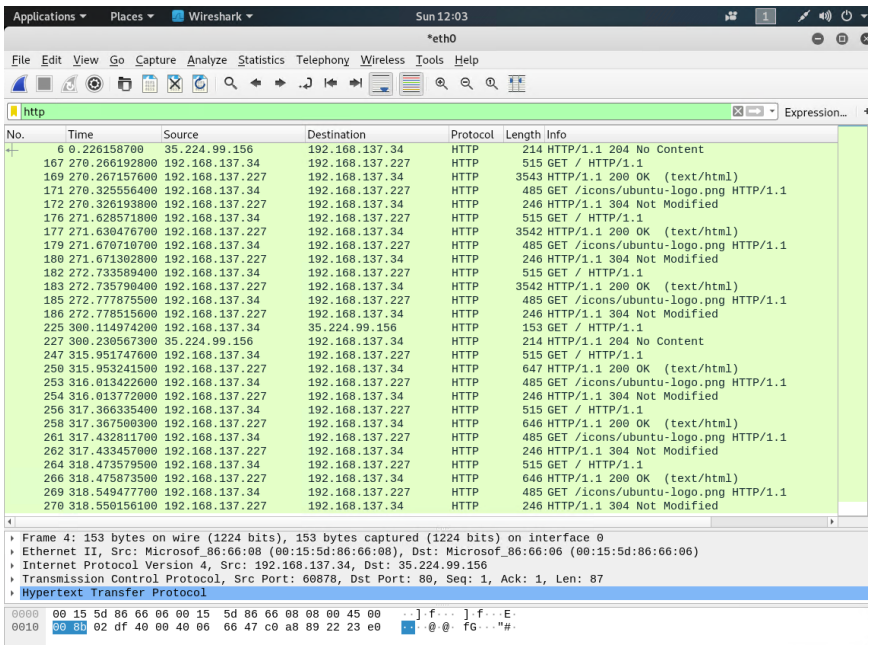

Figura 4.9: Captura de pacotes com a interface em modo promiscuo e o switch virtual configurado para aceitar o modo promiscuo.

As figuras 4.8 e 4.9 mostram a configuração da máquina atacante em modo promíscuo e a captura dos pacotes HTTP trocados entre a máquina ubuntu desktop de endereço IP 192.168.137.34 e a máquina ubuntu server de endereço IP 192.168.137.227.

Com os ataques de sniffing na solução da Microsoft, foi possível observar que:

A solução da Microsoft trabalha também com o mapeamento das interfaces de rede virtuais em memória. Os comutadores virtuais e as interfaces de rede virtuais das máquinas virtuais tem seus endereços mapeados na memória. Dessa forma, quando uma máquina virtual vai se comunicar com outra máquina virtual a comunicação sai do endereço mapeado para a interface da primeira máquina e segue para o endereço mapeado da segunda máquina. Assim outras máquinas por mais que estejam no mesmo endereço de rede não conseguem capturar os pacotes da comunicação, uma vez que a comunicação não aparecerá no endereço mapeado para a interface de rede delas. Por conta desse funcionamento característico de ambientes virtuais, a máquina kali linux não pode observar nenhum pacote da comunicação entre as máquinas ubuntu server e ubuntu desktop.

Para que seja possível observar o tráfego de outras máquinas é preciso configurar port mirroring na solução da Microsoft. O port mirroring é feito na interface de rede virtual de cada máquina. Na configuração se diz quem vai ser a fonte de tráfego e quem será a máquina de monitoramento. Com essa configuração os pacotes gerados na interface de rede da máquina virtual configurada como fonte não só irão para as máquinas de destino, mas serão copiados e entregues a interface de rede virtual da máquina de monitoramento. Sendo assim possível que uma máquina não participante da comunicação observe tráfegos entre duas ou mais máquinas.

Apesar de não ser possível capturar pacotes através de ataques a rede virtual apenas ativando o modo promíscuo na interface da máquina atacante, existem outras formas de realizar a captura de pacotes. Essas formas serão posteriormente apresentadas e discutidas na seção 4.4 nesse mesmo capítulo.

4.2 ATAQUES DE SPOOFING

Para os testes de spoofing foram postos a máquina atacante, o servidor web e o cliente web na mesma rede. O atacante realizou um ataque de ARP poisoning contra a máquina cliente assumindo a identidade do servidor web. Informações sobre o cenário utilizado para esses testes podem ser obtidos através das figuras 3.3 e 3.7 para VMware e Microsoft respectivamente.

4.2.1 Na solução da VMWARE: ESXi

Com os ataques de spoofing na solução da VMware, foram obtidos os seguintes resultados:

Ao realizar o ataque com as proteções ativadas foi possível realizar o ataque. A página web fica indisponível enquanto o comando arpspoof estiver ativo, observe a figura 4.10.

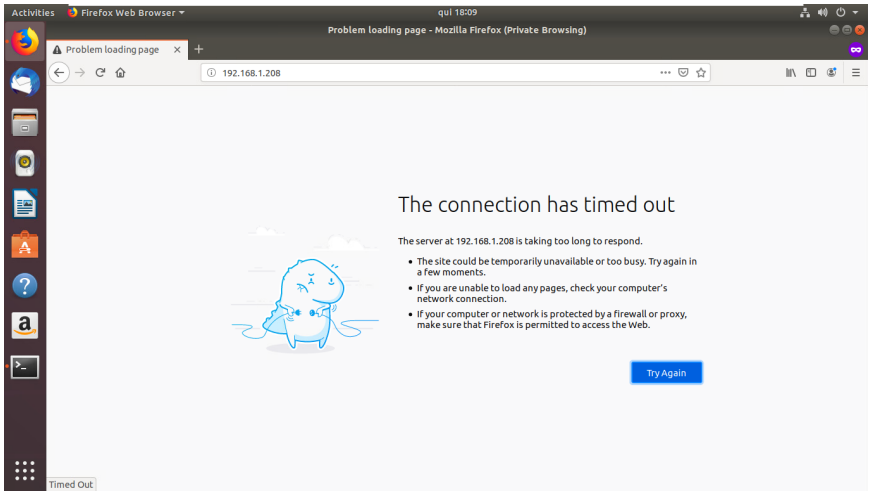

Figura 4.10: Página web fora do ar durante ataque de ARP spoofing.

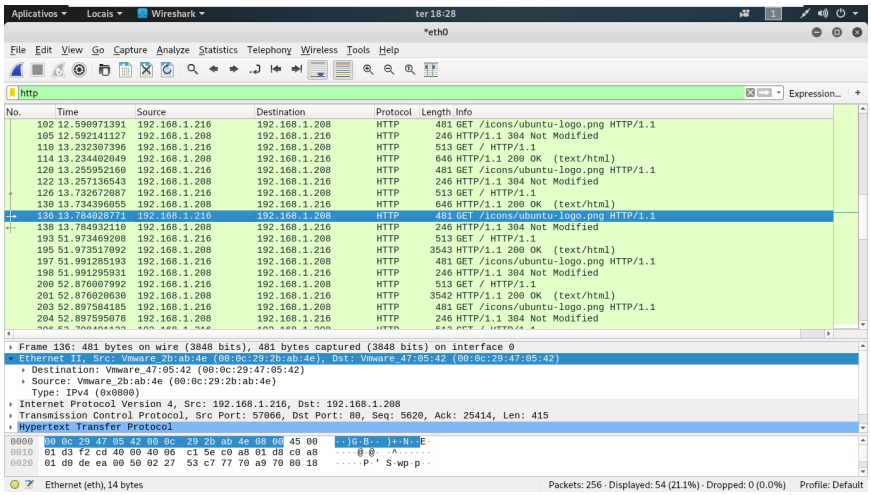

Figura 4.11: Captura de pacotes. O direcionamento das requisições HTTP está sendo para o atacante por conta do ataque de ARP spoofing enquanto as proteções estão ativas.

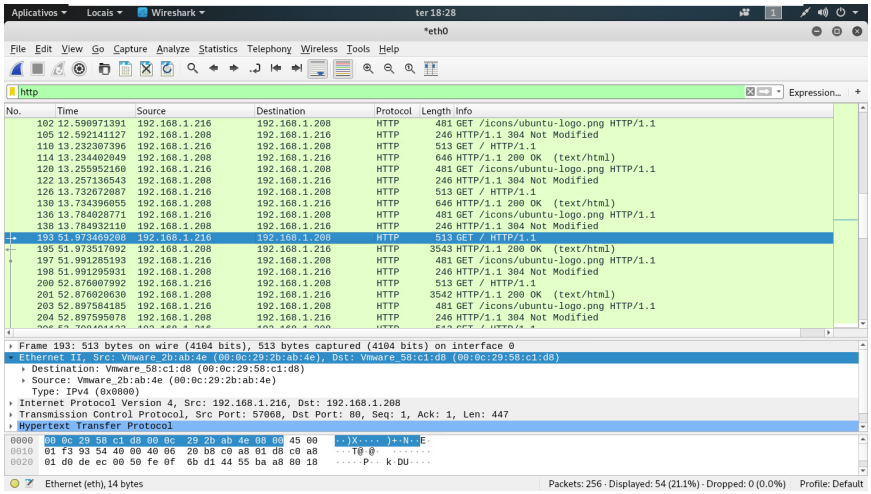

Figura 4.12: Captura de pacotes. Após finalizado o ataque de ARP spoofing o direcionamento volta a ser para o servidor.

A fim de observar o que acontecia foi ativado o recurso de encaminhamento de pacotes com o comando sysctl net.ipv4.ip_forward=1 na máquina kali linux, executado o comando arpspoof novamente e capturados os pacotes durante o ataque. Enquanto o comando estava ativo as requisições HTTP eram feitas para o kali linux de endereço MAC 00:0C:29:47:05:42, a partir do ubuntu desktop de endereço MAC 00:0C:29:2B:AB:4E e quando o comando era desativado a comunicação voltava a ser direta entre o ubuntu desktop e o ubuntu server de endereço MAC 00:0C:29:58:C1:D8, observe as figuras 4.11 e 4.12 respectivamente. Os endereços MAC das máquinas kali linux, ubuntu desktop e ubuntu server podem ser confirmados na tabela 3.4.

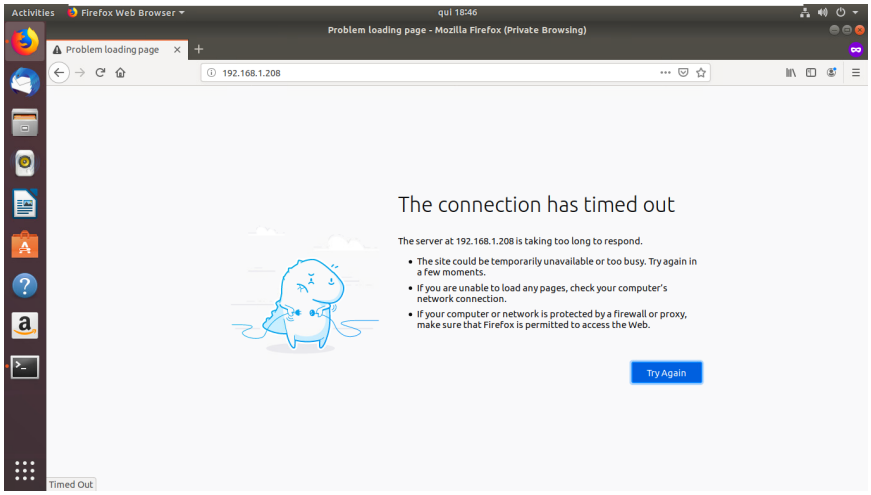

Figura 4.13: Página web fora do ar durante ataque de ARP spoofing.

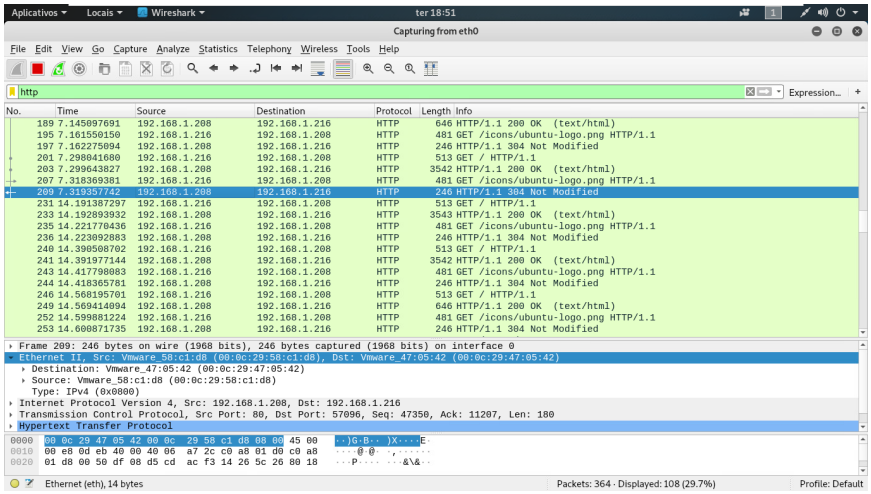

Figura 4.14: Captura de pacotes. Com as configurações de proteção desabilitadas para a realização da contraprova, o atacante recebe as requisições HTTP da máquina ubuntu desktop durante o ataque de ARP spoofing.

Ao realizar a contraprova desabilitando as proteções foi possível realizar o ataque assim como havia sido possível com elas habilitadas, observe as figuras de 4.13 a 4.15. Enquanto o comando estava ativo as requisições HTTP eram feitas para o kali linux de endereço MAC 00:0C:29:47:05:42, a partir do ubuntu desktop de endereço MAC 00:0C:29:2B:AB:4E e quando o comando era desativado a comunicação voltava a ser direta entre o ubuntu desktop e o ubuntu server de endereço MAC 00:0C:29:58:C1:D8.

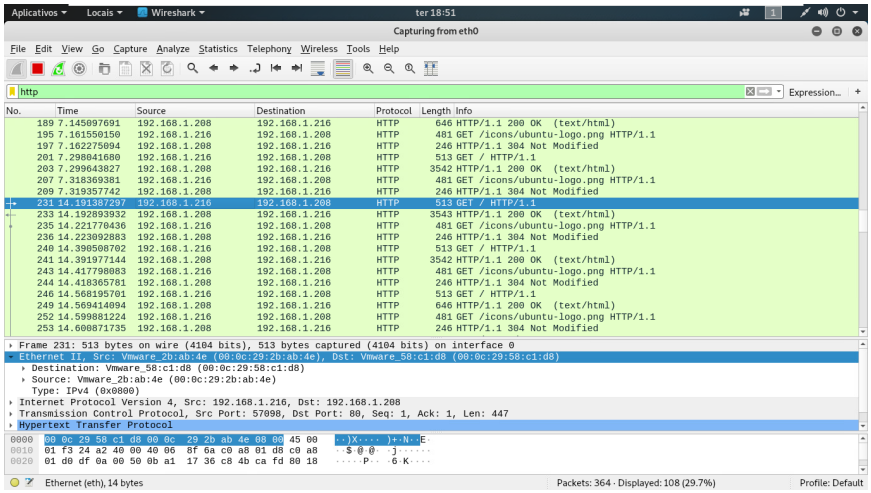

Figura 4.15: Captura de pacotes. Com as configurações de proteção desabilitadas para a realização da contraprova, o ubuntu server retorna a receber as requisições HTTP da máquina ubuntu desktop após finalizado o ataque de ARP spoofing.

Com os ataques de spoofing na solução da VMware, foi possível observar que:

Na documentação oficial do fabricante VMware está escrito que é possível dar segurança ao tráfego de camada 2 do virtual switch a partir da proteção contra troca endereço MAC e da interceptação de pacotes forjados com um MAC distinto daquele que está descrito na interface de rede virtual.

Durante um ataque de ARP spoofing o atacante vai se utilizar do protocolo ARP a fim de manipular a tabela ARP de dispositivos e assumir a identidade que não é a sua. Dessa forma prevenir que o MAC seja alterado e que pacotes forjados não possam ser enviados pela rede é uma medida de proteção contra alguns ataques de ARP spoofing, mas não todos.

Conforme os resultados obtidos a partir de um ataque de ARP spoofing utilizando a técnica de man-in-the-middle é possível interceptar tráfegos na rede o que torna a rede virtual não segura mesmo com as proteções disponíveis habilitadas. Isso é possível porque os recursos de segurança apenas monitoram trocas de endereço MAC. Ao associar um IP que não é o seu ao seu próprio MAC, assumindo a identidade de outra máquina, ela não identificará isso como uma violação de segurança o que permite realizar uma série de ataques na rede. Caso a proteção contra pacotes forjados se estendesse também ao endereço IP a segurança na rede virtual seria melhor.

Como é possível realizar essa troca de identidade a solução da VMware se torna vulnerável a ataques de ARP spoofing. Como um ataque de ARP spoofing pode ser utilizado como meio para realização de outros ataques a abrangência de vulnerabilidades da rede virtual aumenta por exemplo para alguns tipos de ataques de sniffing. Se eu consigo dizer a uma máquina que ela deve enviar pacote para a minha interface virtual então o mecanismo de proteção contra sniffing não funcionará dado que para ele será uma comunicação autentica entre duas máquinas. O pacote sairá da interface virtual da primeira máquina e será entregue diretamente na interface virtual da segunda máquina sendo capturado pelo sniffer.

Existem métodos de identificação de spoofing. Esses métodos serão apresentados e discutidos na seção 4.4.

4.2.2 Na solução da Microsoft: HYPER-V

Com os ataques de spoofing na solução da Microsoft, foram obtidos os seguintes resultados:

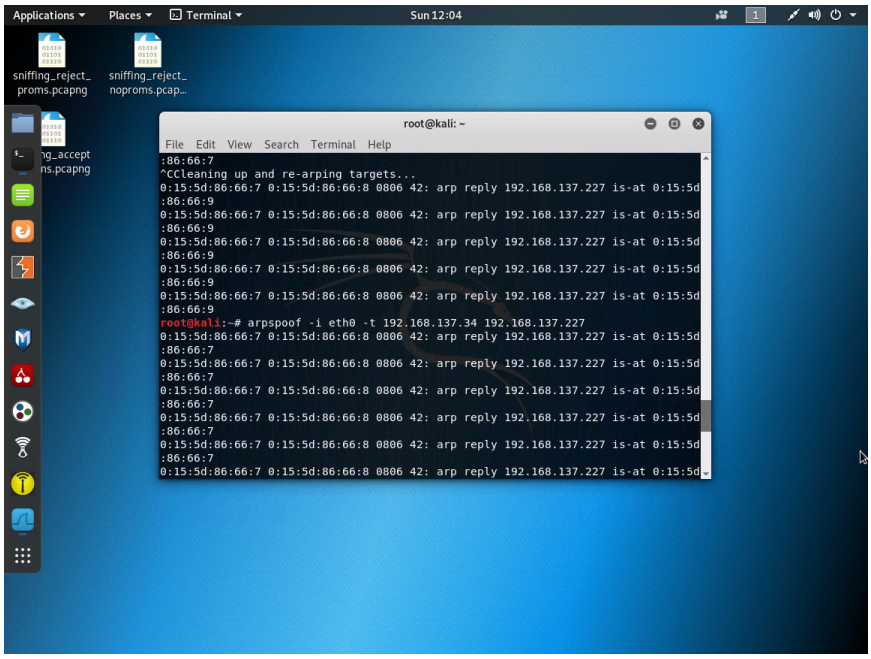

Figura 4.16: Ataque de ARP spoofing. Atacante assumindo a identidade do servidor web.

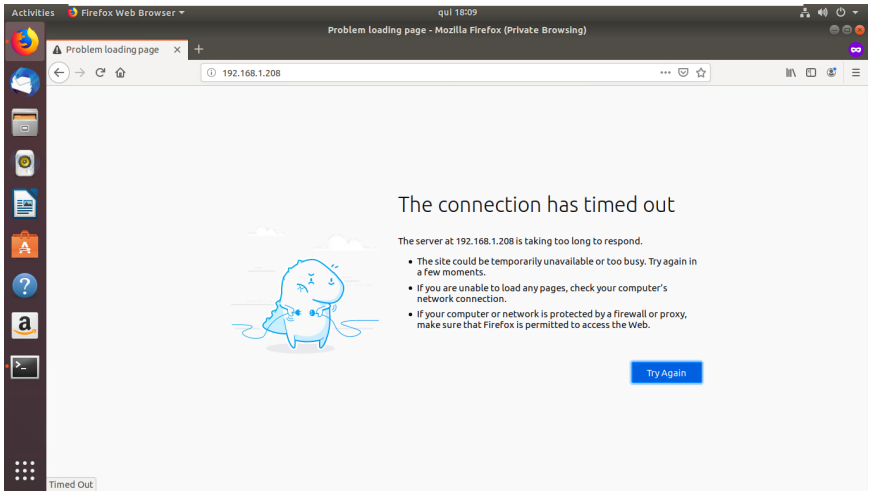

Figura 4.17: Página fora do ar durante ataque de ARP spoofing.

Ao realizar o ataque com as proteções ativadas foi possível assumir a identidade da máquina ubuntu server de endereço IP 192.168.137.227. A página web fica indisponível enquanto o comando arpspoof estiver ativo, observe as figuras 4.16 e 4.17.

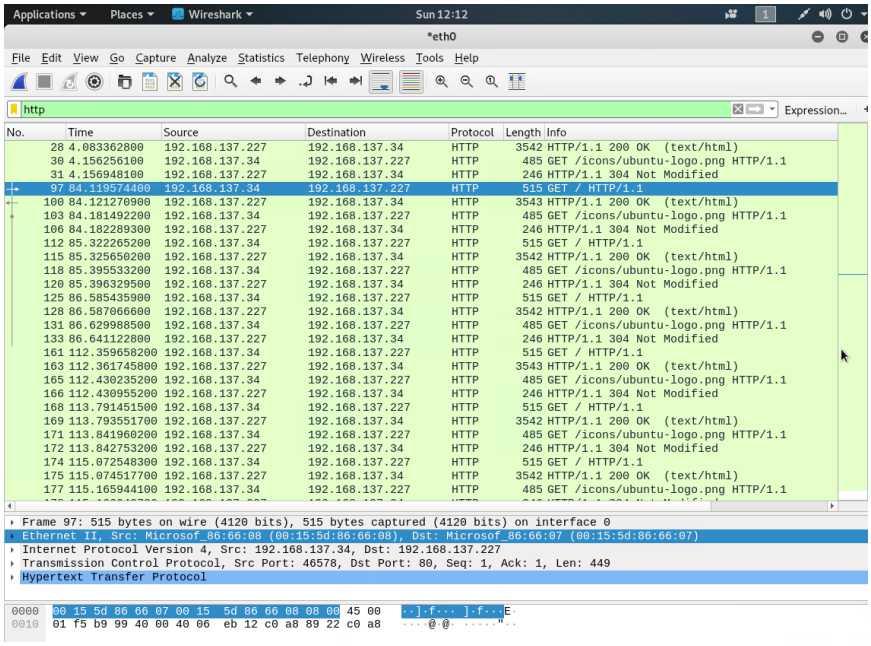

Figura 4.18: Captura de pacotes. Com as configurações de proteção desabilitadas para a realização da contraprova, o atacante recebe as requisições HTTP da máquina ubuntu desktop durante o ataque de ARP spoofing.

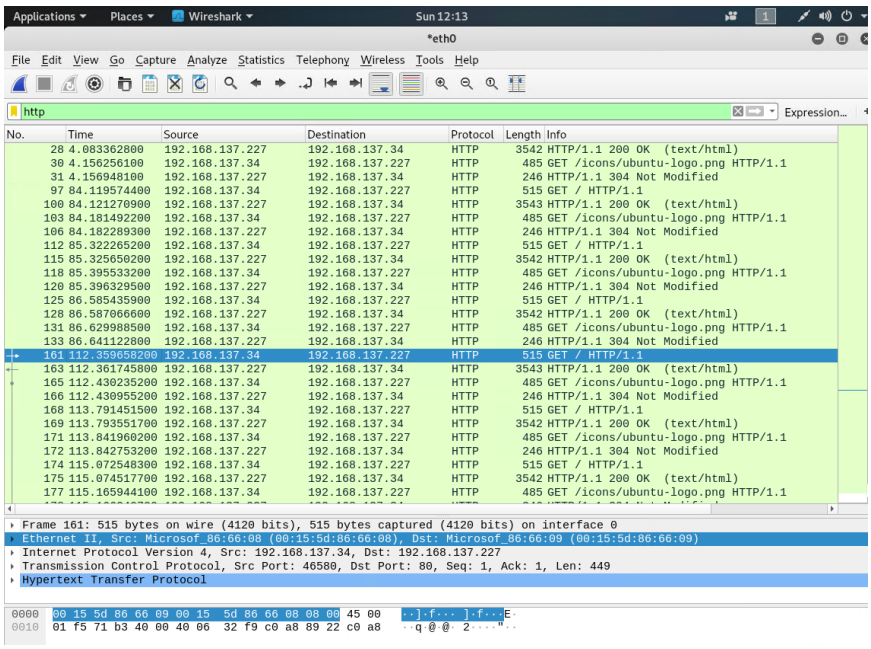

Figura 4.19: Captura de pacotes. Com as configurações de proteção desabilitadas para a realização da contraprova, o ubuntu server retorna a receber as requisições HTTP da máquina ubuntu desktop após finalizado o ataque de ARP spoofing.

Ao realizar a contraprova permitindo a troca de endereço MAC foi possível assumir a identidade da máquina ubuntu server assim como havia sido possível com elas habilitadas. A fim de observar o que acontecia foi ativado o recurso de encaminhamento de pacotes com o comando sysctl net.ipv4.ip_forward=1 na máquina kali linux, executado o comando arpspoof novamente e capturados os pacotes durante o ataque. Enquanto o comando estava ativo as requisições HTTP eram feitas para o kali linux de endereço MAC 00:15:5D:86:66:07 a partir do ubuntu desktop de endereço MAC 00:15:5D:86:66:08 e quando o comando era desativado a comunicação voltava a ser direta entre o ubuntu desktop e o ubuntu server de endereço MAC 00:15:5D:86:66:09, observe as figuras 4.18 e 4.19 respectivamente. Os endereços MAC das máquinas kali linux, ubuntu desktop e ubuntu server podem ser confirmados na tabela 3.6.

A proteção contra envenenamento de ARP/ND (falsificação) mencionada na documentação como incluída no switch não foi desabilitada por não haver nenhuma opção nas configurações nem do comutador virtual nem da máquina virtual.

Com os ataques de spoofing na solução da Microsoft, foi possível observar que:

Na documentação oficial do fabricante Microsoft está escrito que um dos principais recursos incluídos no comutador virtual deles é proteção contra envenenamento de ARP/ND (falsificação). Contudo essa proteção não foi suficiente para um ataque de ARP spoofing como o descrito na seção 3.5.1.2. A fabricante cumpre na proteção contra a troca de endereço MAC, uma vez que ao se utilizar a ferramenta macchanger para trocar o MAC da máquina atacante a máquina virtual fica sem acesso à rede. Mas apenas isso não é suficiente para proteger a rede virtual contra ARP spoofing ou ARP poisoning.

Observar apenas a troca do endereço MAC não garante que sua rede estará segura. Se for associado qualquer IP ao MAC existente da máquina virtual, a proteção deixa de existir. Regras de Access Control List podem ser criadas para prevenir que esses tipos de ataques ocorram. O problema é que ao se criar regras manualmente é gerado um problema gerencial no ambiente demandando tempo e a aplicação delas a toda e qualquer máquina que venha a ser criada no ambiente. O ideal é que tais regras fossem criadas automaticamente e atribuídas as placas de rede virtuais de todas as máquinas logo após a criação da máquina virtual como se subentende a partir da documentação.

Assim como na solução da VMware, é possível realizar a troca de identidade e sendo assim outros ataques podem ser utilizados também na solução da Microsoft, incluindo um ataque se sniffing como o mencionado para a solução da VMware. Existem métodos de identificação de spoofing. Esses métodos serão apresentados e discutidos na seção 4.4.

4.3 PORT SCAN

4.3.1 Na solução da VMWARE: ESXi

Com o ataque de port scan na solução da VMware, foi possível observar que o NMAP conseguiu uma série de informações sobre a rede inclusive o tipo de sistema operacional e os serviços que rodavam dentro das máquinas. Observe a figura 4.20 por exemplo, o NMAP retorna que a máquina de endereço IP 192.168.1.208 é um LINUX 3.X|4.X com um Apache 2.4.29 em execução.

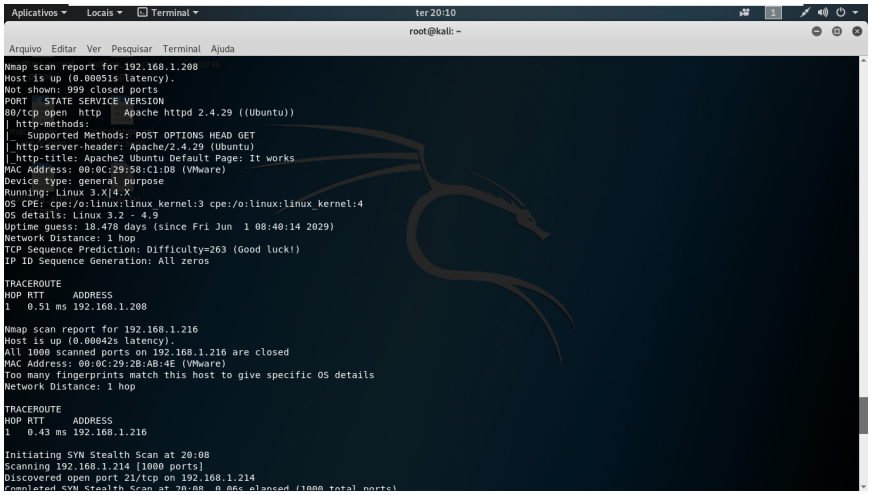

Figura 4.20: Realização de varredura na rede retorna informações sobre sistema operacional, serviços, portas abertas, entre outros.

Como a solução de virtualização da VMware não faz análise do tráfego nas redes virtuais, ataque como port scan ou até mesmo Denial of Service que poderiam ser identificados e prevenidos não são. As medidas de proteção nas soluções de virtualização podem até diminuir o alcance desses ataques com a utilização de segmentação de rede, mas dentro de um mesmo segmento os ataques não são impedidos.

Agregar inteligencia computacional com análise dos dados da rede pode ser uma solução para alguns tipos de ataques. Contudo para realizar isso é necessário o consumo de recursos ou até mesmo impactar na performance das máquinas virtuais. Sendo assim é preciso balancear segurança e performance e encontrar qual a verdadeira necessidade conforme as regras de negócio de cada organização. Isso será discutido posterior mente na seção 4.4.

4.3.2 Na solução da MICROSOFT: HYPER-V

Com os ataques de port scan na solução da Microsoft, foi possível observar que o NMAP obteve uma série de informações sobre a rede inclusive os tipos de sistemas operacionais das máquinas e os serviços que elas prestavam. Observe a figura 4.21 por exemplo, o NMAP retorna que a máquina de endereço IP 192.168.137.227 é um LINUX 3.X|4.X com um Apache 2.4.29 em execução.

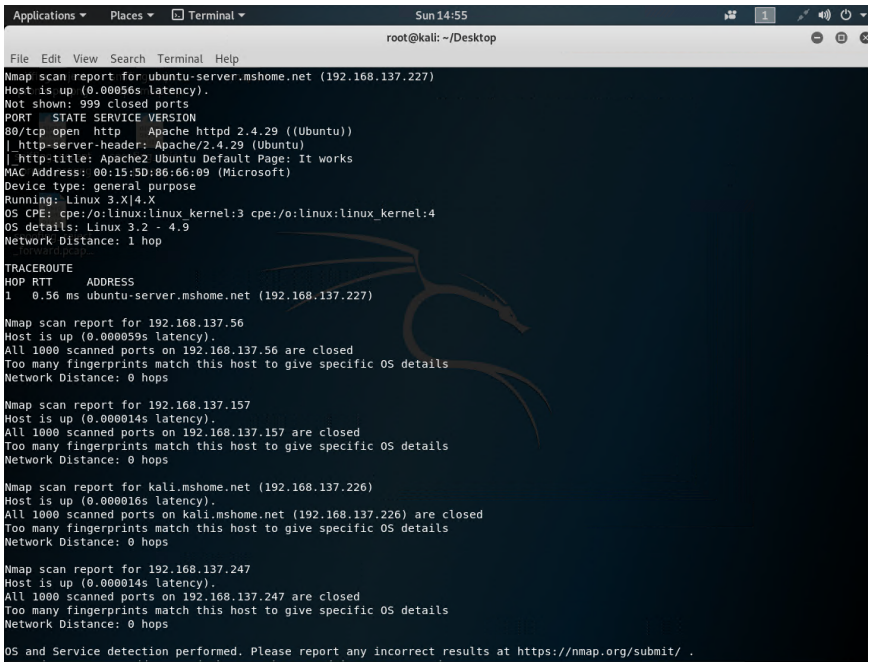

Figura 4.21: Realização de varredura na rede retorna informações sobre sistema operacional, serviços, portas abertas, entre outros.

A solução da Microsoft não realiza a análise dos tráfegos assim como a solução da VMware e se encontra vulnerável a ataques de port scan também. A utilização de ACLs podem ser utilizadas para impedir a comunicação entre uma máquina realizando port scan e a rede, mas para isso esse comportamento deve ser identificado e a regra de ACL deve ser criada manualmente o que dificulta a proteção.

A automatização na identificação e criação de regras pode ser um caminho para proteção nesse tipo de ataque. Isso será discutido posterior mente na seção 4.4.

4.4 SÍNTESE DOS RESULTADOS E DISCUSSÕES

4.4.1 Sobre Sniffing em Redes Virtuais

Quando a virtualização é realizada existe uma abstração dos recursos e um dos recursos que é abstraído é o recurso de rede. Dessa forma as máquinas virtuais passam a utilizar uma rede virtual para enviar seus pacotes de dados. Essa rede é criada dentro da memória do virtualizador e existe fisicamente apenas em memória através do mapeamento das interfaces de rede virtuais em endereços de memória. Sendo assim uma máquina virtual que deseja enviar um pacote de dados para outra máquina virtual em um mesmo servidor o faz através da memória deste. O pacote é enviado através de uma placa de rede virtual diretamente para outra placa de rede virtual sem acessar um barramento físico. Por conta disso sniffers não conseguem interceptar a comunicação na rede virtual dado que nenhum dado que não seja para eles chegará até a sua placa de rede virtual.

Embora esse comportamento ocorra para máquinas em um mesmo virtualizador, ele não ocorre para máquinas em hosts diferentes. Caso as máquinas em virtualizadores diferentes estejam se comunicando, uma máquina na rede física conseguiria capturar os dados sendo enviados de uma para a outra. Quando uma máquina precisa enviar um pacote para uma máquina em outro virtualizador, o hypervisor irá enviar o pacote em texto aberto para o switch na rede física e este irá encaminhar o pacote para o destino apropriado. Ao chegar no outro virtualizador o pacote é enviado por meio da memória a outra máquina virtual. Esse comportamento é o mesmo para máquinas em um mesmo servidor, porém em um switch virtual diferente. Os switches virtuais não realizam operações de roteamento, logo precisam enviar os pacotes para a rede física para que eles sejam roteados para o destino correto. Portanto, caso a máquina atacante se encontre dentro da rede virtual ela não será capaz de observar o tráfego não direcionado a ela. Mas caso esteja na rede física poderá observar tráfegos entre máquinas em diferentes servidores ou switches virtuais no mesmo segmento que ela.

Como uma opção para permitir que outras máquinas tenham acesso ao que ocorre na rede virtual, os switches virtuais têm opções para enviar os pacotes a todas as interfaces de rede virtuais, atuando assim de forma muito semelhante a um barramento físico e permitindo que sniffers possam escutar a rede.

As duas soluções escolhidas têm formas diferentes de permitir a captura de pacotes. Enquanto a VMware prefere aplicar as regras diretamente no switch virtual, a Microsoft prefere aplicar na placa de rede da máquina virtual. A solução da VMware em sua forma mais básica ativa a regra no switch fazendo com que ele se assemelhe com um hub virtual, enquanto a solução da Microsoft estabelece regras de port mirroring enviando os pacotes das máquinas configuradas como fonte para as portas de destino. A forma da fabricante VMware utilizar o recurso torna a rede mais insegura uma vez que qualquer máquina conectada ao switch virtual terá todos os pacotes chegando a sua interface virtual. Já na solução da Microsoft apenas máquinas configuradas como destino no port mirroring terão os pacotes chegando as suas interfaces virtuais.

Para que um ataque de sniffing seja bem sucedido e a comunicação entre duas máquinas seja ouvida é necessário ter acesso ou visibilidade do estado da memória do virtualizador e não acesso a rede virtual. Sendo assim uma forma de se observar o tráfego na rede virtual é utilizando ferramentas que realizam dump de memória. Após obtidas as informações nos dumps é necessário tratar esses dados e analisar de forma a identificar a estrutura mapeada em memória transformando para um formato que possa ser apresentado ao atacante. Esse é um ataque muito complexo uma vez que deve se obter acesso a memória de um sistema virtualizado e a partir daí fazer uma coleta e tratamento de dados para então obter informações úteis.

Existem algumas patentes criadas com o fim de caracterizar soluções que realizam o monitoramento de redes virtuais. Elas têm focado na criação de aplicações que sejam executadas dentro dos virtualizadores, kernel-based, que consigam através de portas de teste de acesso, test access port (TAP), se comunicar com o virtualizador e realizar o monitoramento da rede capturando os pacotes juntamente com os controladores da rede.[13][12]

A forma como redes virtuais são criadas e tratadas em ambientes virtuais impedem algumas formas de capturar pacotes na rede, porém a proteção contra sniffing pode ser burlada através de ataques de spoofing. Quando um atacante assume a identidade de outra máquina, a interface de rede virtual para qual serão enviados os pacotes será a da própria máquina atacante. Assim os pacotes serão entregues da placa de rede virtual da máquina remetente para a placa de rede virtual da máquina atacante pelo mesmo método utilizado em uma comunicação entre quaisquer outras duas máquinas. Logo a máquina atacante poderá intermediar a troca de pacotes entre a máquina remetente e a máquina de destino capturando, modificando ou interceptando eles. Sendo assim por mais que a forma como o tráfego é lidado no modelo virtual impeça ataques de sniffing apenas ouvindo a rede, eles podem ser feitos enganando o endereçamento para que os pacotes sejam redirecionados para uma máquina atacante por meio de spoofing.

4.4.2 Sobre Spoofing em Redes Virtuais

Ambos os fabricantes analisados neste trabalho tiveram problema em proteger suas redes contra o ataque de ARP spoofing da ferramenta arpspoof presente no Kali linux. A VMware implementa algumas proteções contra a troca de endereço MAC na interface de rede virtual e contra a criação de pacotes forjados onde o campo MAC não esteja em conformidade com o endereço registrado na placa de rede. Isso impede que máquinas criem pacotes falando que tem outro MAC, mas não impede que elas digam que tem outro IP através de ARP responses. O mesmo ocorre com a Microsoft. Existe proteção contra a troca de MAC que impede a troca de MAC, mas não tem nenhum controle quando uma máquina utiliza de ARP responses para roubar a identidade de outra máquina. Na documentação a Microsoft afirma: "Estes são alguns dos principais recursos incluídos no Comutador Virtual Hyper-V: Proteção contra envenenamento de ARP/ND (falsificação): fornece proteção contra uma VM mal-intencionada que usa falsificação de protocolo ARP para roubar endereços IP de outras VMs. Fornece proteção contra ataques que podem ser iniciados para IPv6 usando falsificação ND (Descoberta de Vizinhos).", porém o ataque realizado foi exatamente o que está descrito que seria impedido na primeira parte da afirmação: "... fornece proteção contra uma VM mal-intencionada que usa falsificação de protocolo ARP para roubar endereços IP de outras VMs".

Existem sistemas que conseguem detectar ataques de ARP spoofing. O SNORT, que é um sistema de detecção de invasão de rede open source, possui regras para a identificação deste tipo de tráfego.[49] Em uma de suas formas de identificação ele escuta o tráfego na rede e busca por máquinas que estejam realizando o envio de respostas ARP sem que tenha ocorrido uma requisição ARP. Uma máquina que esteja enviando respostas ARP sem requisições está muito provavelmente realizando ARP spoofing. Esse tipo de verificação poderia ter impedido o ataque de ARP spoofing feito nesse trabalho. Apesar do SNORT não poder dizer de onde para onde vai o ataque, em um sistema virtualizado o virtualizador saberia de qual máquina o tráfego estaria saindo e em direção a qual máquina podendo assim impedir que o ataque ocorresse. Utilizando regras de detecção de intrusos e regras de controle de acesso como a ACL da solução da Microsoft seria possível automatizar a criação de regras para impedir ataques de ARP spoofing na rede virtual.

Os hypervisors tem poder computacional para realizarem essas verificações de tráfego. Atualmente existem IPS e IDS como appliances virtuais que consomem os recursos do virtualizador. Colocar um sistema de prevenção de intrusos diretamente no kernel pode consumir mais recursos, mas melhoraria a segurança em ambientes virtuais. Por outro lado, a verificação de todos os pacotes gerados na rede poderia gerar um problema de performance nas máquinas uma vez que todo pacote deveria ser analisado para que realmente se garantisse a segurança. Uma abordagem equilibrada procurando realizar análise aleatória da rede pode ser uma solução que balanceia a questão segurança versus performance. Na análise aleatória nem todos pacotes seriam analisados. De forma aleatória são escolhidos pacotes e eles são analisados. Também pode se usar uma análise adaptativa onde enquanto o tráfego não estiver alto todos os pacotes são analisados. Quando o tráfego aumentar passa a se utilizar uma análise aleatória ou estatística. Dessa forma não existiria a necessidade de se implementar IPS ou IDS para detectar ameaças a rede virtual. Em relação ao tráfego que vem da rede física para a rede virtual, seria possível analisar esse tráfego também impedindo que ataques partissem da rede física para a rede virtual.

Uma forma de proteger a rede contra ataques de ARP spoofing é criando filtros ou regras que só permitam que um pacote seja enviado se os dados de endereçamento dele estejam em conformidade com o que está registrado no virtualizador. Os hypervisors tem pacotes de serviço que permitem a eles obter diversas informações sobre uma máquina como por exemplo o endereço MAC de suas interfaces de rede e os IPs atribuídos a essas interfaces. Utilizando essas informações para criar regras de ACL, por exemplo na solução da Microsoft, impediria ataques de ARP spoofing. A criação dessas regras pode ser feitas automaticamente quando a máquina for criada, receber um novo IP ou trocar a placa de rede tudo isso poderia ser monitorado pelo pacote de serviços. Um dos problemas desse tipo de configuração é que o pacote de serviços precisaria estar instalado e a todo momento se comunicando com a solução de virtualização para impedir que as regras sejam forjadas ou enganadas.

4.4.3 Sobre Port Scan em Redes Virtuais

As soluções de virtualização em seu core não possuem proteção contra port scan. Não existe uma análise de pacotes de forma automatizada nas redes virtuais por conta do virtualizador em seu modelo mais básico. Existem formas de criar filtros para impedir alguns tipos de comunicação, mas tais filtros são criados de forma manual e não tem inteligência para identificar ataques como por exemplo port scan que já é um ataque com formas de prevenção conhecidas, realizando a detecção a partir de filtros de tráfego. Se uma fonte está enviando pacotes para um mesmo destino em diferentes portas em um intervalo muito pequeno entre as requisições isso é provavelmente um ataque de port scan. Tal tipo de verificação poderia ser feita pelo virtualizador a fim de proteger a rede virtual que está dentro dele sem a necessidade de utilização de IPS ou NIPS em máquinas virtuais.

O módulo de Network Intrusion Prevention poderia atuar dentro do virtualizador e com ele ativo seria possível detectar e prevenir diversos ataques na rede virtual diretamente na saída da interface de rede virtual de cada uma das máquinas virtuais. Ele poderia identificar os padrões de comportamento que se diferem do comportamento normal da máquina virtual e até mesmo comportamentos maliciosos como port scan, ARP poisoning ou denial of service dentro da rede virtual. Como o virtualizador possui diversas informações sobre as máquinas virtuais, o módulo também teria essas informações, como endereços MAC, tipos de serviços que elas executam, sistema operacional, entre outros. Dessa forma ele seria capaz de identificar também qual máquina realiza qual tipo de ataque e o destino do ataque, podendo agir de forma preventiva impedindo pacotes maliciosos de trafegarem na rede. Em relação a rede física poderia ser analisado o tráfego de entrada para a rede virtual e feitas verificações sobre os pacotes que desejam entrar na rede.

Dois dos grandes problemas quando se trata de implementar ferramentas de segurança é a relação entre segurança e performance ou segurança e recursos. Realizar tarefas de análise sobre a rede gera uma latência média na rede. Como os pacotes teriam de passar por análise para apenas depois serem encaminhados pela rede o tempo de análise precisa ser incluído no tempo de transmissão. Além disso, recursos de processamento e memória precisariam ser dedicados a realização dessas análises o que retiraria parte dos recursos disponíveis para as máquinas virtuais. Por outro lado, existem soluções de NIPS que são implementadas em máquinas virtuais. Uma vez tendo esse tipo de solução incluída no kernel não seria necessária a implementação de máquinas virtuais. Seriam consumidos menos recursos do que uma máquina virtual por ser apenas mais um processo no virtualizador e não um sistema operacional inteiro de uma máquina virtual. Contudo como o processo estará sendo executado em cada um dos virtualizadores, em um cluster o recurso destinado a realização das análises pode ultrapassar o recurso destinado a uma solução em máquina virtual.

5 CONCLUSÃO E TRABALHOS FUTUROS

5.1 CONCLUSÃO

O uso da virtualização vem crescendo e novas tecnologias vem se desenvolvendo a partir dela. A criação de máquinas virtuais e do compartilhamento de recursos de um único hardware entre elas gerou um modelo flexível que tem se ajustado as necessidades de diversos tipos de soluções. Por mais que o meio onde existem as redes virtuais seja diferente do meio das redes físicas as ameaças do modelo físico podem ser ameaças para o modelo virtual também. Sendo assim a rede virtual precisa se preocupar com a segurança das máquinas que se encontram nela e assim como a rede física implementar medidas de segurança de forma a impedir que tais ataques sejam bem-sucedidos. Para isso o uso das informações que os virtualizadores podem obter sobre as máquinas e o controle que eles exercem sobre os recursos são essenciais. Identificar ataques a partir da análise da rede na memória com a integração de módulos de IPS no próprio kernel da solução de virtualização é um caminho otimizado onde cada virtualizador analisa as redes virtuais que estão dentro dele e a entrada da rede física para a rede virtual.

A abordagem das soluções de virtualização a partir da criação de políticas de segurança sobre as interfaces de rede não se mostrou uma abordagem segura. Dois dos três testes realizados apresentaram falhas sendo que um deles apenas foi impedido por conta da abordagem e poderia ser efetuado de outras formas. Uma abordagem voltada a políticas de controle de acesso também não se mostra eficiente, uma vez que a detecção da ameaça não é feita pela solução e sim por um profissional e a implementação das regras é manual e gera um problema de gestão. Caso a abordagem fosse adicionada inteligencia computacional afim de identificar ameaças e aplicar contramedidas de forma automática o modelo seria mais seguro e eficiente.

O uso de módulos de detecção e prevenção de intrusos pode ser vinculado ao kernel e agir como um processo dentro da camada de virtualização ao invés da utilização de máquinas virtuais dedicadas a isso. Se cada virtualizador for responsável pela análise do tráfego dentro dele os recursos utilizados para tal análise podem ser reduzidos se comparados com aos recursos dedicados a uma máquina virtual. Dessa forma não teria a necessidade de implementação de máquinas virtuais dedicadas a esse tipo de funcionalidade.

A segurança em ambientes virtuais tem sido focada no uso de aplicações externas, quando o próprio virtualizador tem mais informações e mais controle para poder lidar com ameaças.

5.2 TRABALHOS FUTUROS

Este trabalho abordou a segurança apenas dentro do ambiente virtual. Um ambiente real tem a componente virtual e a componente física. A análise em conjunto do ambiente virtual e ambiente físico e em como o ambiente virtual pode contribuir para a segurança do ambiente físico pode ser um trabalho futuro.

Com a virtualização sugiram também os conceitos de computação em nuvem. A computação em nuvem utiliza da virtualização para prover seus serviços, a segurança na nuvem tem sido um tema recorrente que pode ser tratado como um trabalho futuro.

Com o surgimento da nuvem também surgiu um conceito de segurança provida como serviço. Nuvens de serviço de segurança analisam o tráfego do datacenter, filtram o tráfego e enviam de volta para o datacenter. Esse conceito é um conceito novo que não foi abordado e pode ser abordado em trabalhos futuros.

A incorporação de um módulo de segurança nos virtualizadores é uma opção para garantir a segurança nesses ambientes. Contudo até que ponto a segurança impacta na performance das soluções de virtualização. A análise do impacto da performance da segurança em soluções de virtualização pode ser um trabalho futuro.

REFERENCIAS

1 XIA, W.; WEN, Y.; FOH, C. H.; NIYATO, D.; XIE, H. A survey on software-defined networking. *IEEE Communications Surveys & Tutorials*, IEEE, v. 17, n. 1, p. 27–51, 2015.

2 HAN, B.; GOPALAKRISHNAN, V.; JI, L.; LEE, S. Network function virtualization: Challenges and opportunities for innovations. *IEEE Communications Magazine*, IEEE, v. 53, n. 2, p. 90–97, 2015.

3 GOLDBERG, R. P. *Architectural principles for virtual computer systems*. [S.l.], 1973.

4 GOLDBERG, R. P. Architecture of virtual machines. In: ACM. *Proceedings of the workshop on virtual computer systems*. [S.l.], 1973. p. 74–112.

5 GOLDBERG, R. P. Survey of virtual machine research. *Computer*, IEEE, n. 6, p. 34–45, 1974.

6 POPEK, G. J.; GOLDBERG, R. P. Formal requirements for virtualizable third generation architectures. *Communications of the ACM*, ACM, v. 17, n. 7, p. 412–421, 1974.

7 DREPPER, U. The cost of virtualization. *Queue*, ACM, v. 6, n. 1, p. 28–35, 2008.

8 MADNICK, S. E.; DONOVAN, J. J. Application and analysis of the virtual machine approach to information system security and isolation. In: ACM. *Proceedings of the workshop on virtual computer systems*. [S.l.], 1973. p. 210–224.

9 FISCHER, A.; BOTERO, J. F.; BECK, M. T.; MEER, H. D.; HESSELBACH, X. Virtual network embedding: A survey. *IEEE Communications Surveys & Tutorials*, IEEE, v. 15, n. 4, p. 1888–1906, 2013.

10 SURI, S.; CHILKOTI, H. *Application delivery control module for virtual network switch*. [S.l.]: Google Patents, 2011. US Patent 7,962,647.

11 NOGUEIRA, J.; MELO, M.; CARAPINHA, J.; SARGENTO, S. Virtual network mapping into heterogeneous substrate networks. In: IEEE. *2011 IEEE symposium on computers and communications (ISCC)*. [S.l.], 2011. p. 438–444.

12 SMITH, M.; ELANGOVAN, A.; FAZZONE, P. *Traffic forwarding for virtual machines*. [S.l.]: Google Patents, 2013. US Patent 8,589,919.

13 TRIPATHI, S.; DROUX, N. G.; BELGAIED, K. *Managing traffic on virtualized lanes between a network switch and a virtual machine*. [S.l.]: Google Patents, 2012. US Patent 8,174,984.

14 SAHOO, J.; MOHAPATRA, S.; LATH, R. Virtualization: A survey on concepts, taxonomy and associated security issues. In: IEEE. *Computer and Network Technology (ICCNT), 2010 Second International Conference on*. [S.l.], 2010. p. 222–226.

15 IDC. *International Data Corporation IDC Forecasts Network Functions Virtualization Infrastructure (NFVI) Revenues to Reach $5.6 Billion in 2022*. Acessado: 13, fevereiro. 2019. Disponível em: <https://www.idc.com/getdoc.jsp?containerId=prUS44231418>.

16 Open Networking Foundation. *Open Networking Foundation Site*. Acessado: 25, janeiro. 2019. Disponível em: <https://www.opennetworking.org/>.

17 MCKEOWN, N.; ANDERSON, T.; BALAKRISHNAN, H.; PARULKAR, G.; PETERSON, L.; REXFORD, J.; SHENKER, S.; TURNER, J. Openflow: enabling innovation in campus networks. *ACM SIGCOMM Computer Communication Review*, ACM, v. 38, n. 2, p. 69–74, 2008.

18 KREUTZ, D.; RAMOS, F. M.; VERISSIMO, P. E.; ROTHENBERG, C. E.; AZODOLMOLKY, S.; UHLIG, S. Software-defined networking: A comprehensive survey. *Proceedings of the IEEE*, Ieee, v. 103, n. 1, p. 14–76, 2015.

19 MIJUMBI, R.; SERRAT, J.; GORRICHO, J.-L.; BOUTEN, N.; TURCK, F. D.; BOUTABA, R. Network function virtualization: State-of-the-art and research challenges. *IEEE Communications Surveys & Tutorials*, IEEE, v. 18, n. 1, p. 236–262, 2016.

20 European Telecommunications Standards Institute. *European Telecommunications Standards Institute Site NFV Release 3*. Acessado: 25, janeiro. 2019. Disponível em: <https://www.etsi.org/technologies/nfv?jjj=1548509224459>.

21 SINGH, A.; KORUPOLU, M.; MOHAPATRA, D. Server-storage virtualization: integration and load balancing in data centers. In: IEEE PRESS. *Proceedings of the 2008 ACM/IEEE conference on Supercomputing*. [S.l.], 2008. p. 53.

22 VERAS, M. Datacenter: componente central da infraestrutura de ti. *Rio de Janeiro: Brasport*, 2009.

23 CUPPENS, F.; CUPPENS-BOULAHIA, N.; ALFARO, J. Misconfiguration management of network security components. In: *IASTED International Conference on Communication, Network, and Information Security (CNIS 2005)*. [S.l.: s.n.], 2005. p. 1–10.

24 FOSTER, I.; KESSELMAN, C.; TSUDIK, G.; TUECKE, S. A security architecture for computational grids. In: ACM. *Proceedings of the 5th ACM conference on Computer and communications security*. [S.l.], 1998. p. 83–92.

25 MOLVA, R. Internet security architecture. *Computer Networks*, Elsevier, v. 31, n. 8, p. 787–804, 1999.

26 OKUHARA, M.; SHIOZAKI, T.; SUZUKI, T. Security architecture for cloud computing. *Fujitsu Sci. Tech. J*, v. 46, n. 4, p. 397–402, 2010.

27 SHEA, R.; LIU, J. Understanding the impact of denial of service attacks on virtual machines. In: IEEE PRESS. *Proceedings of the 2012 IEEE 20th International Workshop on Quality of Service*. [S.l.], 2012. p. 27.

28 CVE. *Vulnerabilities By Type*. Acessado: 13, fevereiro. 2019. Disponível em: <https://www.cvedetails.com/vulnerabilities-by-types.php>.

29 WU, H.; DING, Y.; WINER, C.; YAO, L. Network security for virtual machine in cloud computing. In: IEEE. *Computer Sciences and Convergence Information Technology (ICCIT), 2010 5th International Conference on*. [S.l.], 2010. p. 18–21.

30 VAUGHAN-NICHOLS, S. J. Virtualization sparks security concerns. *Computer*, IEEE, v. 41, n. 8, p. 13–15, 2008.

31 PEARCE, M.; ZEADALLY, S.; HUNT, R. Virtualization: Issues, security threats, and solutions. *ACM Computing Surveys (CSUR)*, ACM, v. 45, n. 2, p. 17, 2013.

32 BAYS, L. R.; OLIVEIRA, R. R.; BARCELLOS, M. P.; GASPARY, L. P.; MADEIRA, E. R. M. Virtual network security: threats, countermeasures, and challenges. *Journal of Internet Services and Applications*, v. 6, n. 1, p. 1, 2015.

33 MATTOS, D. M. F.; FERRAZ, L. H. G.; DUARTE, O.; JANEIRO-RJ-BRASIL, R. de. Um mecanismo para isolamento seguro de redes virtuais usando a abordagem hıbrida xen e openflow. *XIII SBSeg*, v. 13, p. 128–141, 2013.

34 LOBATO, A. G. P.; FIGUEIREDO, U. da R.; LOPEZ, M. A.; DUARTE, O. Uma arquitetura elástica para prevenç ao de intrusao em redes virtuais usando redes definidas por software. *XXXII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos-SBRC 2014*, p. 1–14, 2014.

35 CHUNG, C.-J.; KHATKAR, P.; XING, T.; LEE, J.; HUANG, D. Nice: Network intrusion detection and countermeasure selection in virtual network systems. *IEEE transactions on dependable and secure computing*, IEEE, v. 10, n. 4, p. 198–211, 2013.

36 GARTNER. *Gartner Magic Quadrant for x86 Server Virtualization Infrastructure*. Acessado: 01, maio. 2019. Disponível em: <https://www.gartner.com/en/documents/3400418>.

37 VMWARE. *VMware Página Oficial VMware*. Acessado: 01, maio. 2019. Disponível em: <https://www.vmware.com/>.

38 VMWARE. *VMware Docs VMware vSphere Documentation*. Acessado: 13, fevereiro. 2019. Disponível em: <https://docs.vmware.com/en/VMware-vSphere/index.html>.

39 VMWARE. *GitHub open-vm-tools*. Acessado: 19, junho. 2019. Disponível em: <https://github.com/vmware/open-vm-tools>.

40 MICROSOFT. *Microsoft Windows IT Pro Center, Windows Server, Virtualization*. Acessado: 07, maio. 2019. Disponível em: <https://docs.microsoft.com/pt-br/windows-server/virtualization/hyper-v-virtual-switch/hyper-v-virtual-switch>.

41 VMWARE. *VMware Docs Networking Concepts Overview*. Acessado: 19, junho. 2019. Disponível em: <https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.networking.doc/GUID-2B11DBB8-CB3C-4AFF-8885-EFEA0FC562F4.html>.

42 VMWARE. *VMware Docs vSphere Standard Switches*. Acessado: 19, junho. 2019. Disponível em: <https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.networking.doc/GUID-350344DE-483A-42ED-B0E2-C811EE927D59.html>.

43 VMWARE. *VMware Docs VLAN Configuration*. Acessado: 19, junho. 2019. Disponível em: <https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.networking.doc/GUID-7225A28C-DAAB-4E90-AE8C-795A755FBE27.html>.

44 VMWARE. *VMware Docs Securing vSphere Standard Switches*. Acessado: 19, junho. 2019. Disponível em: <https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.security.doc/GUID-3507432E-AFEA-4B6B-B404-17A020575358.html>.

45 VMWARE. *VMware Docs Promiscuous Mode Operation*. Acessado: 19, junho. 2019. Disponível em: <https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.security.doc/GUID-92F3AB1F-B4C5-4F25-A010-8820D7250350.html>.

46 VMWARE. *VMware Docs MAC Address Changes*. Acessado: 19, junho. 2019. Disponível em: <https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.security.doc/GUID-942BD3AA-731B-4A05-8196-66F2B4BF1ACB.html>.

47 VMWARE. *VMware Docs Forged Transmits*. Acessado: 19, junho. 2019. Disponível em: <https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.security.doc/GUID-7DC6486F-5400-44DF-8A62-6273798A2F80.html>.

48 MICROSOFT. *Microsoft Windows IT Pro Center, Windows Server, Virtualization, Hyper-V Virtual Switch*. Acessado: 23, junho. 2019. Disponível em: <https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v-virtual-switch/hyper-v-virtual-switch#bkmk_func>.

49 SNORT. *Snort Site oficial*. Acessado: 13, fevereiro. 2019. Disponível em: <https://www.snort.org/>.