Universidade Federal do Maranhão
Centro de Ciências Exatas e Tecnologia
Curso de Ciência da Computação

Rodolfo Fernando Oliveira do Nascimento

Segurança de Redes: Estudo de caso com o Framework Kathará

São Luís
2024

Universidade Federal do Maranhão
Centro de Ciências Exatas e Tecnologia
Curso de Ciência da Computação

Segurança de Redes: Estudo de caso com o Framework Kathará

Monografia apresentada ao curso de Ciência da Computação da Universidade Federal do Maranhão, como parte dos requisitos para obtenção do grau de Bacharel em Ciência da Computação.

Orientador: Prof. Dr. Mário Antonio Meireles Teixeira

São Luís
2024

Ficha gerada por meio do SIGAA/Biblioteca com dados fornecidos pelo(a) autor(a).
Diretoria Integrada de Bibliotecas/UFMA

Nascimento, Rodolfo Fernando Oliveira do.
Segurança de redes : estudo de caso com o framework kathará / Rodolfo Fernando Oliveira do Nascimento. - 2024.
54 p.

Orientador(a): Mário Antonio Meireles Teixeira.
Monografia (Graduação) - Curso de Ciência da Computação, Universidade Federal do Maranhão, Online, 2024.

1. Ambientes virtuais. 2. Ensino de redes. 3. Kathará. 4. Redes de computadores. 5. Segurança de redes. I. Teixeira, Mário Antonio Meireles. II. Título.

Rodolfo Fernando Oliveira do Nascimento

Segurança de Redes: Estudo de caso com o Framework Kathará

Monografia apresentada ao curso de Ciência da Computação da Universidade Federal do Maranhão, como parte dos requisitos para obtenção do grau de Bacharel em Ciência da Computação.

Aprovado em ___de_____de_____

BANCA EXAMINADORA

_____

Prof. Dr. Mário Antonio Meireles Teixeira
Universidade Federal do Maranhão
Orientador

_____

Prof. Dr. Tiago Bonini Borchartt
Universidade Federal do Maranhão
Banca Examinadora

_____

Profa. Dra. Simara Vieira da Rocha
Universidade Federal do Maranhão
Banca Examinadora

São Luís
2024

AGRADECIMENTOS

Aos meus pais e meu irmão, sua presença e amor incondicional na minha vida sempre. Este trabalho é a prova de que os esforços deles pela minha educação não foram em vão e valeram a pena.

Aos meus amigos que sempre estão ao meu lado e desejando meu sucesso. Agradeço o apoio de todos.

Por fim, ao meu professor orientador Mário pelas valiosas contribuições dadas durante todo o trabalho.

RESUMO

Este trabalho propõe um estudo sobre vulnerabilidades em redes de computadores, com foco especial na análise e simulação utilizando entre outras ferramentas, o software kathará, que é uma ferramenta de simulação de ambientes virtuais. O estudo de caso se baseia na simulação de ambientes virtuais realistas proporcionando uma abordagem prática para analisar vulnerabilidades, permitindo experimentações controladas em cenários que reproduzem fielmente os problemas que podem ser encontrados em ambientes reais, bem como contribuir para compreensão e mitigação de ameaças em redes de computadores, proporcionando conhecimentos valiosos, nesse contexto que é essencial para garantir proteção contra possíveis ataques a infraestrutura de TI.

Palavras-chave: Redes de computadores; Segurança de redes; Kathará; Ambientes virtuais; Ensino de redes

ABSTRACT

This work proposes a study on vulnerabilities in computer networks, with a special focus on analysis and simulation using, among other tools, the kathara software, which is a tool for simulating virtual environments. The case study is based on the simulation of realistic virtual environments, providing a practical approach to analyzing vulnerabilities, allowing controlled experimentation in scenarios that faithfully reproduce problems that can be found in real environments, as well as contributing to the understanding and mitigation of threats in networks. computers, providing valuable knowledge, in this context which is essential to guarantee protection against possible attacks on IT infrastructure.

Keywords: Computer networks; Network security; Kathara; Virtual environments; Network learning

LISTA DE ILUSTRAÇÕES

Figura 1 - Criptografia de Chave simétrica 15
Figura 2 - Criptografia de Chave assimétrica 16
Figura 3 - Ataques passivo e ativo 19
Figura 4 - Filtro de Pacotes Tradicionais 22
Figura 5 - Gateway de Aplicação 24
Figura 6 - Arquitetura do kathará. 25
Figura 7 - Redes interconectadas por um roteador. 27
Figura 8 - Kathará executando a emulação dos dispositivos da topologia 28
Figura 9 - Estrutura do diretório e arquivos de configuração 29
Figura 10 - Topologia utilizada no experimento 31
Figura 11 - Busca por portas abertas na rede 33
Figura 12 - Página inicial da aplicação 34
Figura 13 - Acesso dados do sqlserver 35
Figura 14 - Serviço web afetado 36
Figura 15 - Bloqueio de tráfego icmp 38
Figura 16 - Tentativa de acesso a porta tcp bloqueada 39
Figura 17 -Topologia utilizada no laboratório 40
Figura 18 - Tabela ARP do atacante 41
Figura 19- Injeção de pacote com o nemesis 43
Figura 20 - Ataque man-in-the-middle em execução 43
Figura 21 - Topologia utilizada no laboratório 45
Figura 22 - Inicialização do servidor VPN 49
FIgura 23 - Execução do cliente VPN 50

LISTA DE TABELAS

Tabela 1 - Descrição dos equipamentos 31
Tabela 2 - Lista de endereços MAC 42
Tabela 3 - Descrição de equipamentos utilizados no laboratório 45

LISTA DE ABREVIATURAS E SIGLAS

DHCP	*Dynamic Host Configuration Protocol*
DNS	*Domain Name System*
GPL	*General Public License*
IP	*Internet Protocol*
ISP	*Internet Service Provider*
HTTP	Hypertext Transfer Protocol
LAN	*Local Area Network*
MAC	*Media access control*
OSPF	*Open Shortest Path First*
SSL	*Secure Sockets Layer*
TCP	*Transmission Control Protocol*
TLS	*Transport Layer Security*

SUMÁRIO

1 INTRODUÇÃO 10
1.1 Relevância do Tema 10
1.2 Objetivo 10
1.2.1 Objetivos específicos 10
1.3 Estrutura do trabalho 11
2 SEGURANÇA DE REDES 12
2.1 Definição 12
2.2 Criptografia 13
2.2.1 Sistemas de Criptografia de Chave Simétrica 14
2.2.2 Sistemas de Criptografia de Chave Assimétrica 16
2.3 Ataques 17
2.4 Firewall 21
2.4.1 Filtros de pacotes tradicionais 21
2.4.2 Filtros de pacotes com estado 23
2.4.3 Gateways de aplicação 23
3 SOFTWARE DE VIRTUALIZAÇÃO DE REDES: KATHARÁ 24
3.1 Introdução 24
3.2 Framework Kathará 25
3.3 Criação de redes virtuais 27
4 ESTUDOS DE CASO: LABORATÓRIOS 30
4.1 Visão Geral 30
4.2 Servidor Web 30
4.2.1 Cenário de Rede 30
4.2.2 Descrição do Laboratório 32
4.3 Servidor Web com Firewall 36
4.4 Man-in-the-Middle 39
4.4.1 Cenário de rede 39
4.4.2 Descrição do Laboratório 40
4.5 VPNs 44
4.5.1 Cenário de Rede 44
4.5.2 Descrição do laboratório 46
5 CONCLUSÃO 51
REFERÊNCIAS 53

1 INTRODUÇÃO

1.1 Relevância do Tema

Em uma era em que a sociedade está cada vez mais interligada por meio da tecnologia, as redes de computadores desempenham um papel vital, facilitando a comunicação e o funcionamento eficiente de diversas aplicações. Contudo, a complexidade crescente desse ambiente digital também abre espaço para ameaças cibernéticas, tornando essencial uma compreensão aprofundada das vulnerabilidades presentes nesse ecossistema.

A interconectividade global e a diversidade de tecnologias utilizadas aumentaram a superfície de ataque, demandando uma análise detalhada das vulnerabilidades específicas que podem ser exploradas por agentes maliciosos.

A simulação é uma abordagem prática e eficaz para analisar vulnerabilidades em condições controladas, permitindo a experimentação sem riscos em ambientes simulados que reproduzem com fidelidade os desafios encontrados em redes reais.

1.2 Objetivo

Este trabalho tem como objetivo apresentar um estudo de caso sobre as vulnerabilidades inerentes a redes de computadores, utilizando o software kathará como ferramenta para a análise, além de explorar o potencial dessa ferramenta para o ensino de redes de computadores.

1.2.1 Objetivos específicos

- Analisar desafios na segurança de redes;
- Utilizar o software kathará na análise de vulnerabilidades de redes de computadores;
- Ampliar a perspectiva educacional da área de redes com o kathará;
- Desenvolver estudos de casos práticos.

1.3 Estrutura do trabalho

Este trabalho contém 5 capítulos, e é dividido em suas respectivas seções e subseções, no capítulo 2 é feito o referencial teórico onde são abordados os princípios de segurança de redes, como a sua definição, os tipos de criptografia, introduz sobre os tipos de ataques e apresenta o conceito de firewall.

No capítulo 3 é apresentado o software de simulação de redes kathará, bem como seu funcionamento e sua composição.

No capítulo 4 é discorrido sobre os estudos de caso utilizando o kathará para emular os ambientes virtuais, oferecendo uma análise detalhada das vulnerabilidades em redes de computadores.

Por fim, o capítulo 5 recapitula os elementos cruciais abordados ao longo do trabalho, desde a identificação de vulnerabilidades em redes de computadores até a aplicação prática desses conceitos em estudos de casos específicos utilizando o kathará. Além disso, são apresentadas as considerações finais seguidas por melhorias para trabalhos futuros na área de segurança de redes.

2 SEGURANÇA DE REDES

2.1 Definição

A segurança de redes é um elemento essencial num mundo cada vez mais conectado. Com os avanços da tecnologia e a multiplicação de dispositivos interligados, como smartphones, tablets e dispositivos inteligentes, as redes tornaram-se um alvo cada vez mais atraente para os cibercriminosos. A falta de segurança de redes pode ter consequências graves, como o roubo de dados sensíveis, a interrupção de serviços, danos à reputação de uma organização e perdas financeiras significativas (MORAES, 2010, p. 78).

Ela é um conjunto de medidas e práticas destinadas a proteger os sistemas informáticos, os dispositivos e os dados interligados contra ameaças internas e externas. Como toda segurança de TI, envolve a implementação de políticas, procedimentos e tecnologias para garantir a integridade, a confidencialidade e a disponibilidade das informações na rede (MORAES, 2010, p. 78).

Também, a segurança de rede abrange diferentes áreas e aspectos, como a proteção contra acessos não autorizados, ciberataques, malware, roubo de dados, intrusão e interrupção de serviços. A segurança das redes tem como objetivo prevenir, detectar e responder eficazmente às ameaças, minimizar os riscos e mitigar os danos potenciais (MORAES, 2010, p. 79).

Além disso, a segurança das redes é essencial para proteger informações sensíveis, manter a confiança dos utilizadores e facilitar as operações num ambiente cada vez mais complexo e propenso a ciberameaças (MORAES, 2010, p. 79).

Existem vários tipos de segurança de rede que visam proteger sistemas e dados de diferentes tipos de ameaças. Alguns dos principais são listados a seguir (MORAES, 2010, p. 88):

- Firewalls: Barreiras de segurança que monitoram e controlam o tráfego da rede com base em regras predefinidas, protege a rede bloqueando o acesso não autorizado e filtrando pacotes de dados maliciosos.

- Criptografia: Codificação de informações para que apenas as partes autorizadas possam aceder às mesmas. É utilizada para para proteger a confidencialidade dos dados durante a transmissão através de uma rede e garantir que apenas o destinatário correto possa desencriptar.
- Rede privada virtual (VPN): Estabelece uma ligação segura e criptografada entre um dispositivo remoto e a rede da empresa. Amplamente utilizada para proteger comunicações através das redes públicas, permitindo que os utilizadores usem de forma segura os recursos da empresa.
- Sistemas de detecção e prevenção de intrusões (IDS/IPS): Monitoram o tráfego de rede para detectar atividades suspeitas ou maliciosas; o IDS identifica potenciais ameaças e o IPS bloqueia ou responde a essas ameaças em tempo real.
- Autenticação e controle de acesso: Garante que apenas os utilizadores autorizados possam ter contato com os recursos da rede. Estes incluem palavras-passe (senhas), autenticação de dois fatores, certificados digitais e políticas de acesso baseada em funções.
- Antivírus ou antimalware: São usados para detectar e bloquear e remover ameaças como vírus, worms, cavalos de tróia e spyware para proteger as redes de programas maliciosos.

2.2 Criptografia

A criptografia, uma combinação das palavras gregas *kriptos* (oculto) e *grapho* (grafia), é a encriptação de mensagens que apenas o emissor e o receptor sabem traduzir. Basicamente, utiliza-se uma chave contendo parâmetros para traduzir o valor do texto para o modo cifrado e, por outro lado, existe uma chave correspondente contendo parâmetros para decifrar essa mensagem, que pode ser a mesma do emissor ou a versão inversa (GURGEL et al., 2015, p. 165).

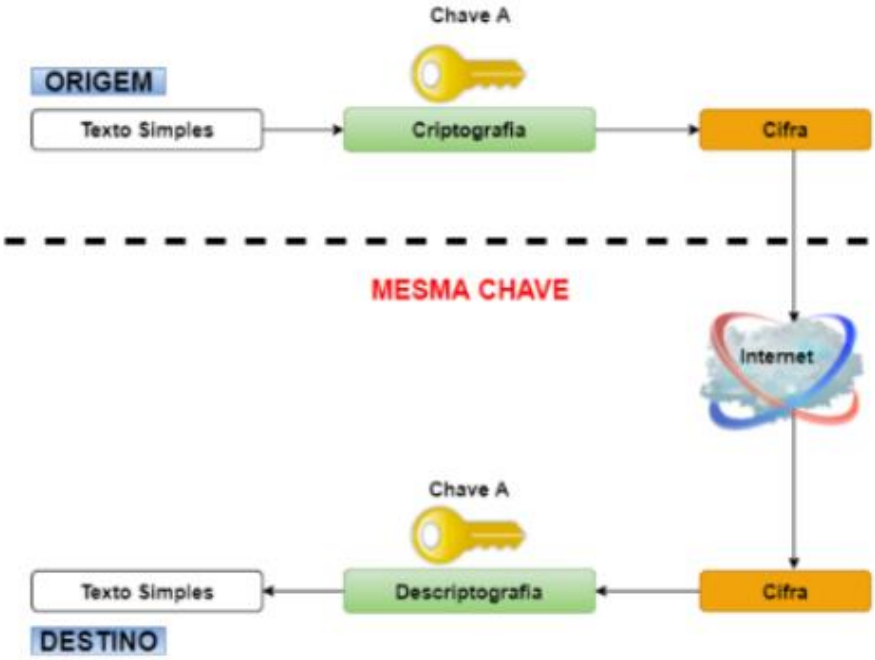
Sendo uma ciência matemática e não computacional, a criptografia existe há mais tempo do que os computadores. Por conseguinte, as suas aplicações existem há séculos ao longo da história da humanidade.

Atualmente, existem essencialmente duas formas de utilizar e distribuir chaves criptográficas. Uma consiste em utilizar a mesma chave para cifrar e decifrar mensagens, a outra consiste em utilizar chaves diferentes. Por esta razão, para além de várias outras características incluídas na criptografia moderna, a criptografia pode ser subdividida em dois grupos principais: Sistemas de Criptografia de Chave Simétrica e Sistemas de Criptografia de Chave Assimétrica (GURGEL et al., 2015, p. 165).

2.2.1 Sistemas de Criptografia de Chave Simétrica

Os sistemas de chave simétrica ou secreta/privada (Figura 1) consistem nos conceitos mais tradicionais de criptografia e pressupõem que a cifragem e a decifragem de uma mensagem utilizam uma chave única conhecida apenas pelas pessoas envolvidas na transmissão. Esta chave secreta é idealmente mais segura se não for transmitida eletronicamente. Isto porque, se existir uma forma segura de transmitir esta chave, os dados da mensagem podem ser enviados. Se a chave for trocada diretamente, é garantido um maior grau de segurança (GURGEL et al., 2015, p.167).

Figura 1 - Criptografia de Chave simétrica



Fonte: Macoratti, 2010.

A vantagem da criptografia simétrica (criptografia de chave privada) é a velocidade de cifragem e decifragem das mensagens, e a sua eficiência tem sido confirmada no uso cotidiano, como nas transações seguras pela Internet, em que muitas comunicações exigem a troca temporária de senhas (GURGEL et al., 2015, p. 167).

Uma desvantagem da aplicação da criptografia simétrica é o número de chaves necessárias quando mais de duas pessoas estão envolvidas. Por exemplo, duas pessoas precisam de uma chave para trocar uma mensagem secreta, enquanto 10 pessoas precisariam de 45 chaves secretas. Esse número é derivado da função de que n pessoas precisam de n* ((n-1) / 2) chaves secretas (GURGEL et al., 2015, p.168).

2.2.2 Sistemas de Criptografia de Chave Assimétrica

Os sistemas assimétricos (Figura 2) surgiram em 1976 e foram propostos por Whitfield Diffie e Martin E. Hellman. Esse sistema se desvia dos métodos tradicionais de criptografia descritos anteriormente no texto Sistema Simétrico, que utiliza a mesma chave para criptografar e descriptografar mensagens. Os sistemas assimétricos utilizam duas chaves, uma pública e outra restrita. Estas chaves estão

interligadas e totalmente relacionadas, pelo que a encriptação com uma chave pública só pode ser desencriptada com a chave correspondente à sua chave privada (GURGEL et al., 2015, p.170).

Figura 2 - Criptografia de Chave assimétrica

Fonte: Macoratti, 2010.

Simulando uma comunicação entre dois utilizadores, designados por emissor e receptor, para garantir a segurança dos dados ao enviar mensagens utilizando um sistema de encriptação assimétrica, o emissor deve encriptar a mensagem a enviar utilizando a chave pública do receptor. Neste caso, o remetente deve cifrar a mensagem utilizando a chave pública do destinatário e, em seguida, cifrá-la novamente utilizando a chave privada do remetente. Ao receber a mensagem, o destinatário deve primeiro desencriptar a mensagem utilizando a chave pública do suposto remetente e verificar a origem da mensagem. O próximo passo é decifrar a mensagem usando a chave privada e acessar os dados da mensagem (GURGEL et al., 2015, p. 170).

Os algoritmos que implementam a criptografia de chave pública são os padrões RSA e de curva elíptica. E a desvantagem desse método em relação ao método de

chave simétrica é que ele é mais lento, mesmo quando o número de chaves secretas trocadas é reduzido (GURGEL et al., 2015, p.171).

2.3 Ataques

Embora possam parecer significar a mesma coisa, ameaças e ataques são distintos. Uma ameaça é algo que prejudica o funcionamento de uma rede ou sistema, enquanto um ataque é uma técnica utilizada para explorar as suas vulnerabilidades (GURGEL et al., 2015, p. 157). Em outras palavras, sabe-se que uma rede deve manter o seu funcionamento perante os três pilares da segurança da informação, e a subversão de qualquer um deles significa que a rede está a ser atacada.

Para proteger uma rede, não é necessário apenas conhecer as ameaças, mas também conhecer os tipos de ataques a que a rede pode estar sujeita (GURGEL et al., 2015, p. 157). Conhecendo os tipos de ataques, fica mais fácil encontrar contramedidas.

A definição dos tipos de ataques mais conhecidos permite ter em mente o tipo de segurança que a rede necessita, tornando mais fácil e eficiente a criação da política de segurança que uma determinada rede precisa.

Para entender por que a segurança da informação é importante em qualquer situação, seja na proteção de dados pessoais ou na proteção de dados de grandes empresas, é preciso conhecer os tipos de ataques mais utilizados por pessoas mal intencionadas. Segundo Geus e Nakamura (2003, p. 8), a evolução constante da tecnologia cria novas formas de proteção, que por sua vez criam novas formas de ataque.

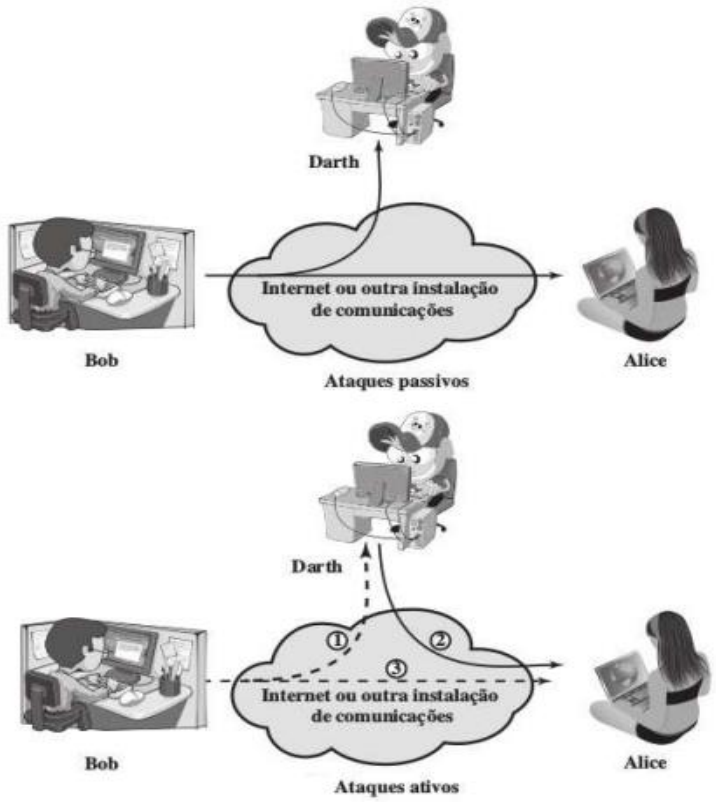
Assim como a tecnologia está em constante mudança, o mesmo acontece com as técnicas de ataque. Por mais que as redes precisem ser constantemente atualizadas, alguns utilizadores não querem "perder" este tempo. Então, conhecer os tipos de ataques e as técnicas necessárias para proteger a rede ajudará a melhorar a rede e a tornar mais visível a desenvoltura da equipe (GEUS & NAKAMURA, 2003, p. 12).

De acordo com Stallings (2005, p. 379), o advento dos computadores demonstrou a necessidade de proteger os ficheiros e as informações armazenadas. Os diferentes tipos de ataques têm características diferentes ou semelhantes, mas o objetivo de obter informação é o mesmo.

Como se pode ver na Figura 3, os ataques podem ser divididos em dois modos: ativo e passivo. No modo passivo de ataque, o atacante utiliza os dados deduzidos para os seus próprios fins, mas não afeta ou altera os dados originais da entidade legítima. E no modo de ataque ativo, o atacante utiliza subterfúgios para interceptar dados, alterá-los e devolvê-los ao seu caminho original, de modo a que essas alterações não sejam notadas pela entidade legítima ou por terceiros (FIRMINO, 2019).

Os ataques passivos envolvem essencialmente a recolha de informações de terceiros de forma não autorizada para verificar a presença de dados sensíveis que, se utilizados, trariam algum benefício para o atacante. Isto inclui a intercepção de dados, chamadas telefônicas, e-mails, etc. (FIRMINO, 2019).

Figura 3 - Ataques passivo e ativo



Fonte: Stallings, 2015.

Assim, pode-se dizer que os ataques passivos estão relacionados com a interceção, monitorização e análise de pacotes, enquanto os ataques ativos estão relacionados com a adulteração, fraude, replicação e bloqueio (Firmino, 2019).

De acordo com Firmino (2019), os principais tipos de ataques são: código malicioso (malware) programas especificamente concebidos para realizar atividades nocivas ou maliciosas em um computador:

- Vírus: um programa ou parte de um programa, normalmente um programa informático malicioso, que se propaga inserindo cópias de si mesmo e tornando-se parte de outros programas ou arquivos. O vírus depende da execução de um programa ou ficheiro hospedeiro para se tornar ativo.
- Worm: Um programa que pode se propagar automaticamente através de uma rede e enviar cópias de si mesmo de um computador para outro. Ao contrário dos vírus, os worms não se propagam adicionando cópias de si mesmo para

outros programas ou arquivos, mas executando as suas cópias diretamente ou explorando vulnerabilidades em programas instalados nos computadores.

- Bots e botnets: São programas maliciosos que possuem um mecanismo para comunicar com um atacante e permitir o controle remotamente. os computadores infectados por bots são muitas vezes referidos como computadores zumbi porque podem ser controlados remotamente sem que o usuário perceba isso. um botnet é uma rede formada por centenas ou milhares de computadores zumbi, que podem ampliar as ações nocivas realizadas pelo bot.
- Trojans: Um programa que não só executa a sua função aparentemente concebida, mas também executa outras funções, normalmente maliciosas, sem o consentimento do usuário. Por definição, um cavalo de Tróia distingue-se de um vírus ou worm na medida em que não infecta outros arquivos nem propaga automaticamente cópias de si próprio.
- Spyware: Um programa concebido para monitorar a atividade do sistema e transmitir a terceiros as informações que recolhe pode ser utilizado tanto de forma legítima como maliciosa.
- Análise de rede (scan): Uma técnica que envolve pesquisa exaustiva de uma rede para identificar computadores ativos e recolher informações sobre eles. Com base nas informações recolhidas, podem ser associadas possíveis vulnerabilidades e serviços e programas disponíveis instalados nos computadores alvos detectados.
- Falsificação de correio eletrônico (e-mail spoofing): Técnica em que os campos do cabeçalho de uma mensagem de correio eletrônico são alterados para fazer parecer que a mensagem foi enviada de uma fonte específica, quando na realidade foi enviada de uma fonte diferente.
- interceptação de tráfego (sniffing): A utilização de programas específicos, denominados sniffers, para inspecionar os dados trocados em redes informáticas. Os atacantes podem obter informações sensíveis, como palavras passe (senhas), números de cartões de crédito e o conteúdo de arquivos confidenciais através de conexões não encriptadas e não seguras.
- Força bruta: Adivinhar nomes de usuários e senhas por tentativa e erro e depois executar processos para conectar a páginas web, computadores e serviços em nome deste usuário, com os mesmos privilégios que ele.

- Alteração de páginas (Defacement): Alterar o conteúdo de páginas Web em domínio Web .
- negação de serviço (DoS e DDoS): Técnica da qual um atacante utiliza um computador para tornar inoperacional um serviço, computador ou rede ligados à internet. Quando utilizado em forma coordenada e distribuída, ou seja, quando um grande número de computadores é utilizado em um ataque, é chamado de negação de serviço distribuído (DDoS).

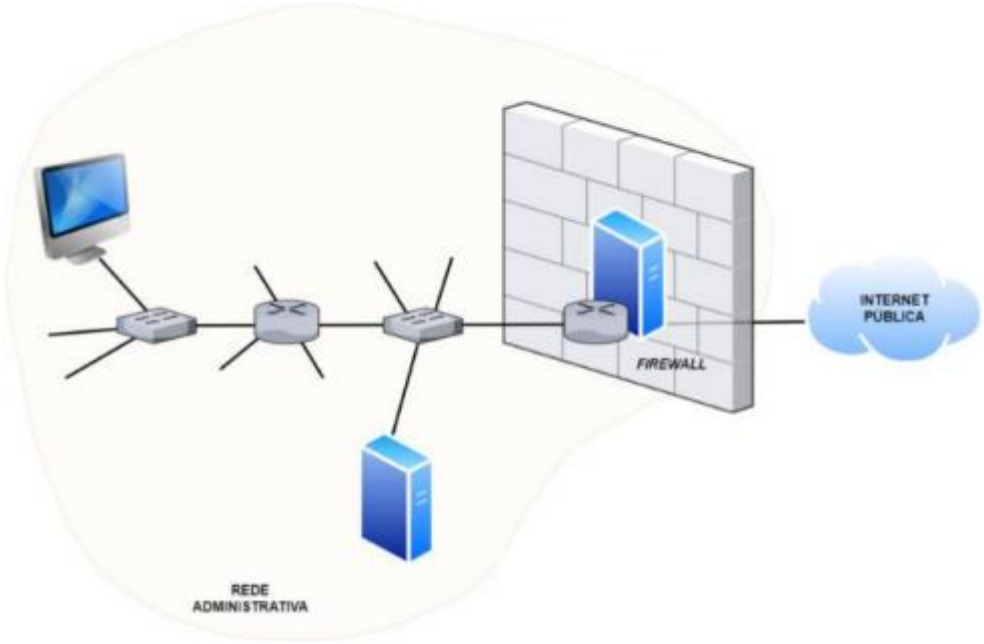
2.4 Firewall

Segundo Kurose e Ross (2013), firewall é uma combinação de hardware e software que isola a rede interna de uma organização da Internet, permitindo a passagem de alguns pacotes e bloqueando outros. Os firewalls permitem aos administradores de rede controlar o acesso entre recursos de rede externos e geridos, gerindo o fluxo de tráfego. Além disso, os firewalls também podem ser classificados em três categorias.

2.4.1 Filtros de pacotes tradicionais

Conforme mostrado na Figura 4, todo o tráfego de e para a Internet passa por um roteador de borda que conecta sua rede interna ao ISP. A filtragem de pacotes é feita aqui. Isso significa que o filtro de pacotes examina cada datagrama e, com base em certas regras definidas pelo administrador, decide se ele deve ser permitido ou deve permanecer.

Figura 4 - Filtro de Pacotes Tradicionais



Fonte: Kurose,Ross, 2013.

Segundo Kurose e Ross (2013), estas regras baseiam-se também nos endereços IP de origem e de destino, no tipo de protocolo do campo do datagrama (IP, TCP, UDP, ICMP, OSPF, entre outros), nas portas TCP ou UDP de origem e de destino e nos bits de bandeira TCP (SYN, ACK, etc.), com base no tipo de mensagens ICMP, regras diferentes para datagramas que entram e saem da rede e regras diferentes para interfaces de roteadores.

De acordo com Kurore e Ross (2014), os administradores de rede configuram firewalls com base em políticas organizacionais. Essas políticas podem ter em conta não só as preocupações de segurança da organização, mas também a produtividade dos utilizadores e a utilização da largura de banda.

2.4.2 Filtros de pacotes com estado

Os filtros de pacotes com estado, tal como a filtragem tradicional, utilizam um conjunto de regras de filtragem e informações de estado derivadas de ligações e sessões para o processo de filtragem. A filtragem tradicional é realizada apenas no primeiro pacote de uma conexão ou sessão. Por outras palavras, apenas o primeiro pacote pertencente a uma sessão ou ligação é verificado em relação ao conjunto de regras. Se este pacote for permitido, o SPF cria uma entrada para esta conexão ou sessão na tabela de estados (LIMA, 2000).

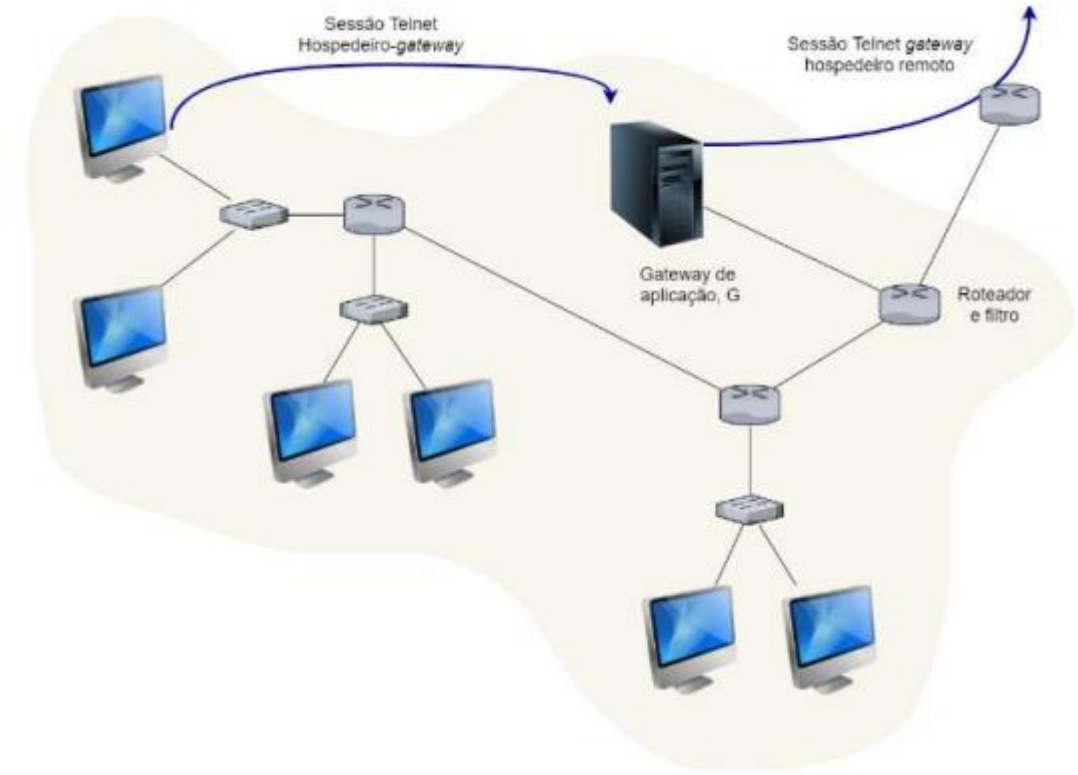
A partir deste momento, os demais pacotes de uma conexão ou sessão só são permitidos se houver uma entrada na tabela de estados para esta conexão ou sessão. Existem tabelas de estados que acompanham o progresso de cada conexão ou sessão que passa pelo filtro num determinado momento (LIMA, 2000).

2.4.3 Gateways de aplicação

Um gateway de aplicação é um servidor através do qual todos os dados da aplicação (de entrada e de saída) devem passar. Vários gateways de aplicação podem ser executados no mesmo host, mas cada gateway é um servidor separado com seus próprios processos (ROSS, 2014).

Como exemplo, supõe-se um tipo de firewall que permite que apenas utilizadores restritos executem telnet (LIMA, 2000) para o exterior e impede que todos os clientes externos executem telnet para o interior (Figura 5).

Figura 5 - *Gateway* de Aplicação



Fonte: Kurose, Ross, 2013.

Como pode ser visto na figura 5 acima, essa política pode ser aplicada pela execução da combinação de um filtro de pacotes (em um roteador) com um gateway de aplicação de telnet.

3 SOFTWARE DE VIRTUALIZAÇÃO DE REDES: KATHARÁ

3.1 Introdução

Em um ambiente de rede, muitas vezes é necessário realizar testes para verificar o funcionamento de equipamentos físicos e implementar novas funcionalidades.

Executar esses testes pode ser uma tarefa complicada, pois poderá afetar configurações e funcionamento de serviços que estão sendo executados nesse

ambiente, impossibilitando sua realização em ambiente de produção, seria possível ainda a utilização de uma bancada de testes, mas adquirir equipamentos físicos somente para teste é um gasto de capital desnecessário.

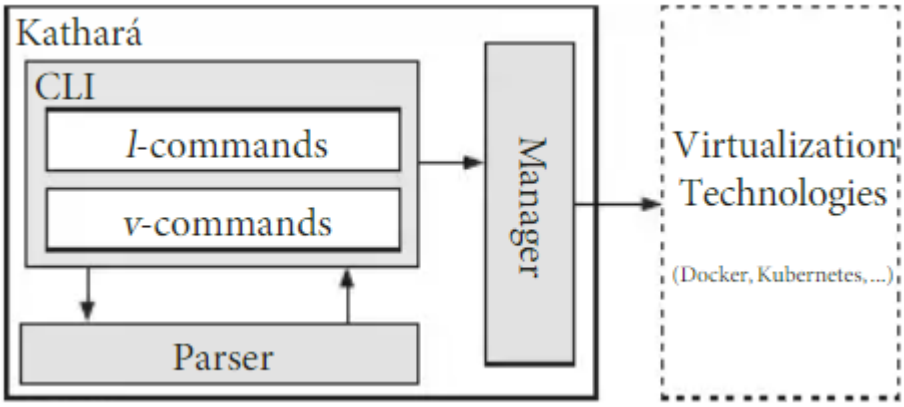
Consequentemente, ambientes virtuais de rede foram desenvolvidos e eles permitem que o usuário crie computadores virtuais para realização de experimentos, testes e configurações de equipamentos físicos como roteadores, servidores, switches e diversos outros tipos de dispositivos.

Neste capítulo será definido o modelo do framework kathará. Será mostrada sua arquitetura, e ainda suas principais características.

3.2 Framework kathará

O framework kathará foi desenvolvido utilizando softwares de código aberto e lançado sob licença GPL versão 3 (Kathará). É uma ferramenta de emulação de rede que utiliza containers docker como base para criar ambientes de rede virtuais.O framework foi desenvolvido a partir do netkit, desenvolvido na Roma Tre Universitá no ano de 1999. Tendo assim compatibilidade e herdando os seus recursos. Na figura 6 é possível observar a arquitetura do kathará e seus componentes.

Figura 6 - Arquitetura do kathará.



Fonte: Scazzariello, Ariemma, Caiazzi, 2020.

De acordo com (SCAZZARIELLO; ARIEMMA; CAIAZZI, 2020) o kathará é baseado nos conceitos de dispositivo, domínio de colisão e cenários de rede.

- Dispositivo: São dispositivos virtuais que simulam dispositivos de redes reais, como roteadores, servidores de DNS e servidores web. Esses dispositivos virtuais são máquinas virtuais de rede e possuem, processadores virtuais, memória RAM e discos virtuais. Eles são usados para testar e simular cenários de rede sem a necessidade do dispositivo físico real.
- Domínio de colisão: Uma LAN de camada 2 virtual que funciona como uma conexão virtual que interliga dispositivos, similar a uma conexão física entre as interfaces desses dispositivos. Sua função principal é encaminhar todos os pacotes recebidos de uma interface para todas as outras interfaces dentro do mesmo domínio de colisão, sem realizar qualquer modificação nos pacotes. Assim como os hubs não tomam decisões de encaminhamento com base no MAC nem segmenta ou filtra o tráfego, simplesmente encaminha os dados para todos os dispositivos conectados. Pode ser útil em vários cenários, mas pode levar a congestionamento de rede.
- Cenários de rede: Conjuntos de dispositivos interconectados por meio de domínios de colisão em uma rede simulada. fornece uma representação simplificada de uma rede complexa, composta por vários dispositivos e domínios de colisão. No contexto do kathará, um cenário de rede é representado como um diretório que inclui um arquivo que descreve a topologia lógica e a arquitetura física dos dispositivos, há arquivos e pastas que contêm a configuração específica desse dispositivo.

Segundo (SCAZZARIELLO; ARIEMMA; CAIAZZI, 2020) a arquitetura do kathará é composta por três componentes principais, a CLI (interface de linha de comando), parser (analisador) e o manager (gerenciador) mostrada anteriormente na figura 6.

- CLI (interface de linha de comando): A CLI é a interface que os usuários interagem para controlar e configurar o kathará ela fornece comandos para criar, configurar e gerenciar cenários de redes virtuais. Os usuários podem utilizar a CLI para iniciar e parar um único dispositivo, podem iniciar e parar todo um cenário de rede e ainda fazer o troubleshooting dos dispositivos.

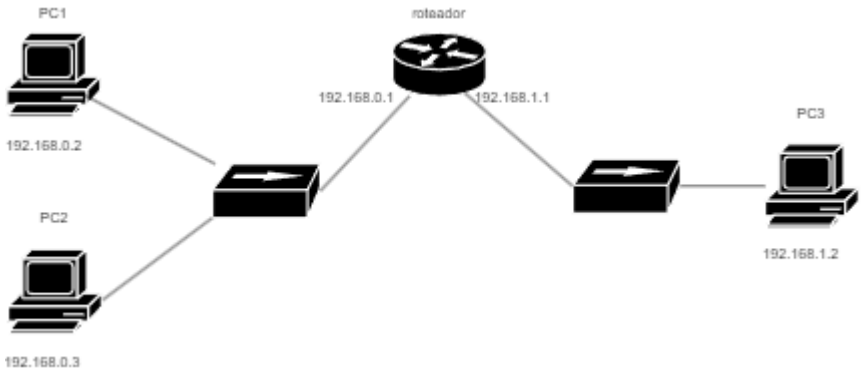
- Parser (analisador): O parser é responsável por analisar os comandos e configurações fornecidos pelos usuários por meio da CLI. Ele interpreta o comando e traduz as instruções em ações que o kathará deve realizar. o parser desempenha papel fundamental na tradução das intenções do usuário em comandos compreensíveis para o sistema.
- Manager (gerenciador): O gerenciador é o componente que controla e coordena todas as operações dentro do kathará. Ele supervisiona a criação e a execução dos cenários de rede, garantindo que os dispositivos virtuais sejam configurados corretamente e que as interações de rede ocorram conforme os comandos especificados pelo usuário na CLI. O gerenciador também lida com tarefas como a inicialização e a limpeza dos cenários de rede virtuais.

3.3 Criação de redes virtuais

A criação de uma rede virtual no kathará é realizada através de um arquivo de configuração. Nesse arquivo, todos os dispositivos que compõem a rede virtual devem ser corretamente listados, além disso o arquivo de configuração precisa ter necessariamente a extensão “.conf".

A figura 7 mostra um cenário de rede com 3 hosts conectados (PC1, PC2, PC3) e um roteador fazendo a divisão em 2 domínios de broadcast.

Figura 7 - Redes interconectadas por um roteador.

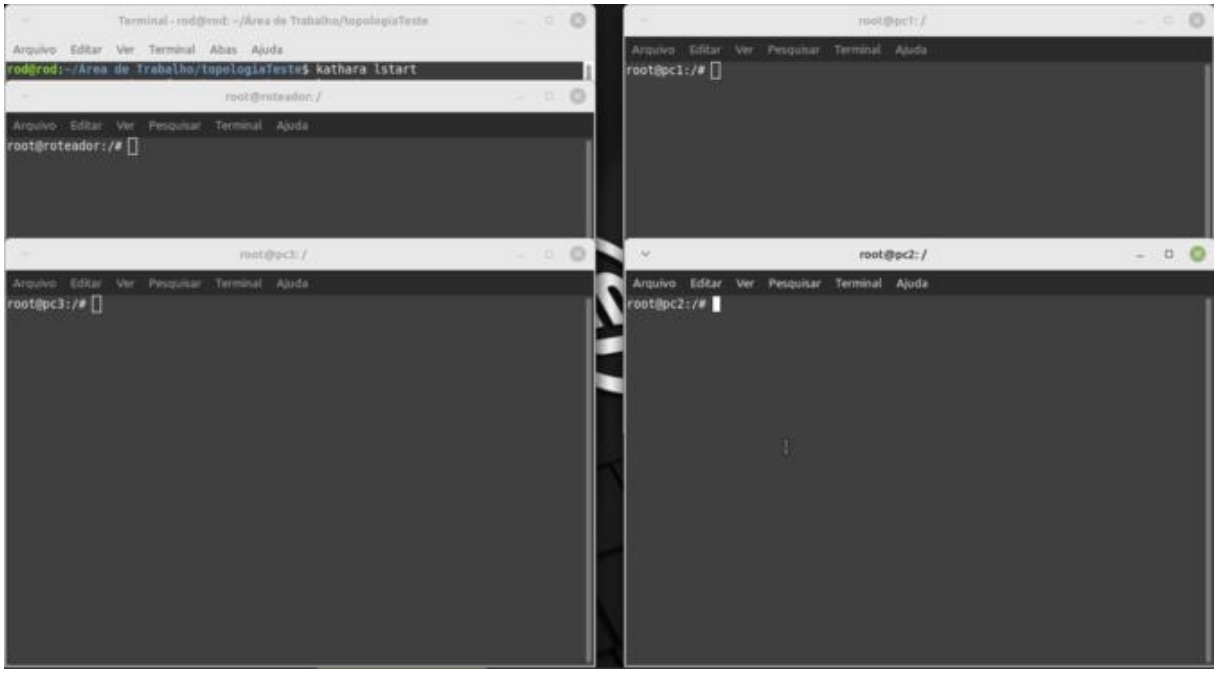


Fonte: Autor

A figura 8 mostra a execução do cenário da figura 7 mostrada anteriormente. Onde foi declarado que dispositivos fazem parte da rede virtual a ser executada,

podendo ser dispositivos finais, roteadores ou mesmo hubs. Ao mesmo tempo que esses equipamentos têm suas interfaces de rede ligadas e configuradas com ips e máscaras de rede e rotas estáticas e default gateway.

Figura 8 - Kathará executando a emulação dos dispositivos da topologia



Fonte: Autor

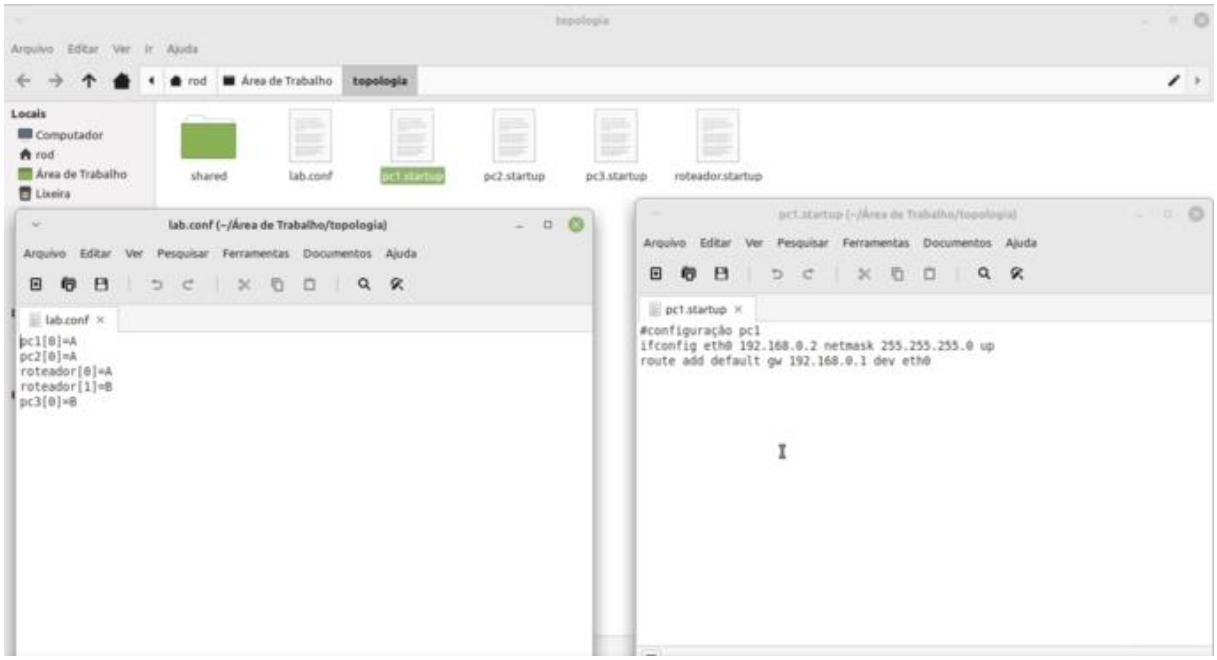
Um ambiente virtual do kathará é formado por um conjunto de arquivos e diretórios que são previamente configurados pelo usuário, esses arquivos incluem as configurações que cada dispositivo emulado deve ter. Essa abordagem é comum em ambientes de simulação de rede, onde os ambientes são pré-configurados para criar ambientes para realização de testes específicos, cada arquivo de configuração contém informações como:

- Configuração de interfaces de rede: Especificações sobre quais interfaces de rede virtuais devem ser criadas em cada dispositivo virtual e como eles são interconectados.
- Configuração de endereços IP: Definição do endereçamento ip, máscaras de sub-redes e gateway padrão de cada dispositivo virtual.

- Configuração de roteamento: Configuração de roteamento, para direcionar o tráfego em redes distintas.
- Configuração de serviços de rede: Ativação e configuração de serviços de rede, tal como, DNS, DHCP, servidores web, banco de dados, etc.
- Configurações de segurança: Definições de regras de firewall, permissões de acesso, e diversas outras configurações de segurança.
- Outras configurações específicas do cenário: Qualquer outra configuração ou personalização necessária para atender aos objetivos do laboratório virtual.

Essa abordagem permite aos usuários criar rapidamente cenários de rede complexos e realistas sem a necessidade de configurar cada dispositivo virtual manualmente toda vez que for iniciar o ambiente virtual, em substituição, os arquivos pré-configurados facilitam a implantação de testes mais específicos de forma consciente e permitindo uma melhor agilidade e eficiência.

Figura 9 - Estrutura do diretório e arquivos de configuração



Fonte: Autor

Na figura 9 é possível visualizar a estrutura do laboratório e um arquivo de configuração da topologia, e outro arquivo contendo a configuração de rede de um dispositivo ao ser inicializado.

4 ESTUDOS DE CASO: LABORATÓRIOS

4.1 Visão Geral

Estudar sobre segurança de redes de computadores pode não ser uma tarefa tão trivial, é possível estudar em livros, artigos, revistas, mas a parte prática é de suma importância para o complemento entendimento. Entretanto, estudos práticos vão necessitar de alguns equipamentos físicos que demandam um aumento na complexidade da infraestrutura que não vai ser atendida por somente um dispositivo final.

O kathará é uma ferramenta que permite a execução desses experimentos de redes de computadores e vai possibilitar uma experiência mais próxima possível do real podendo ser executada em um simples computador com a ferramenta instalada.

Neste capítulo será apresentado alguns estudos de caso abrangendo os conceitos

4.2 Servidor Web

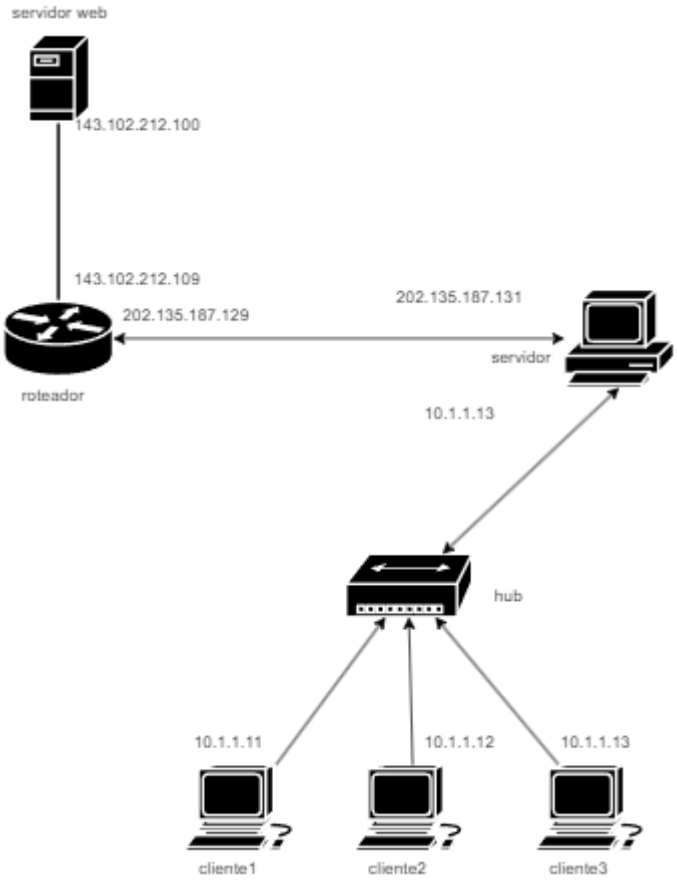
O objetivo deste experimento é simular vulnerabilidades em aplicações web conforme visto na seção 2.3. Tal qual a mitigação delas é fundamental para garantir a segurança e a integridade das operações.

4.2.1 Cenário de Rede

A escolha por esse cenário ocorre devido à facilidade de entendimento da disposição dos equipamentos utilizados, uma vez que há um roteador fazendo a divisão da rede, cada equipamento ficará em uma rede distinta, e o servidor ficará responsável pela conexão de acesso dos clientes.

Este cenário está ilustrado na figura 10 e será utilizado em todos os experimentos desta seção. A tabela 1 descreve todos os equipamentos ilustrados na topologia.

Figura 10 - Topologia utilizada no experimento



Fonte : autor

Tabela 1 - Descrição dos equipamentos

Dispositivo	Funcionalidade
Roteador	Ponto de comunicação entre a rede interna e a aplicação web
Internet	Utilizado para hospedar a aplicação web simulando um ambiente fora da rede interna
Servidor	Utilizado para disponibilizar serviços para os clientes da rede interna
Hub	Utilizado para fazer a interligação de todos os dispositivos da rede interna

Cliente 1	Utilizado para conexão com a aplicação web simulando uma requisição HTTP
Cliente 2	Utilizado para conexão com a aplicação web simulando uma requisição HTTP
Cliente 3	Utilizado para conexão com a aplicação web simulando uma requisição HTTP

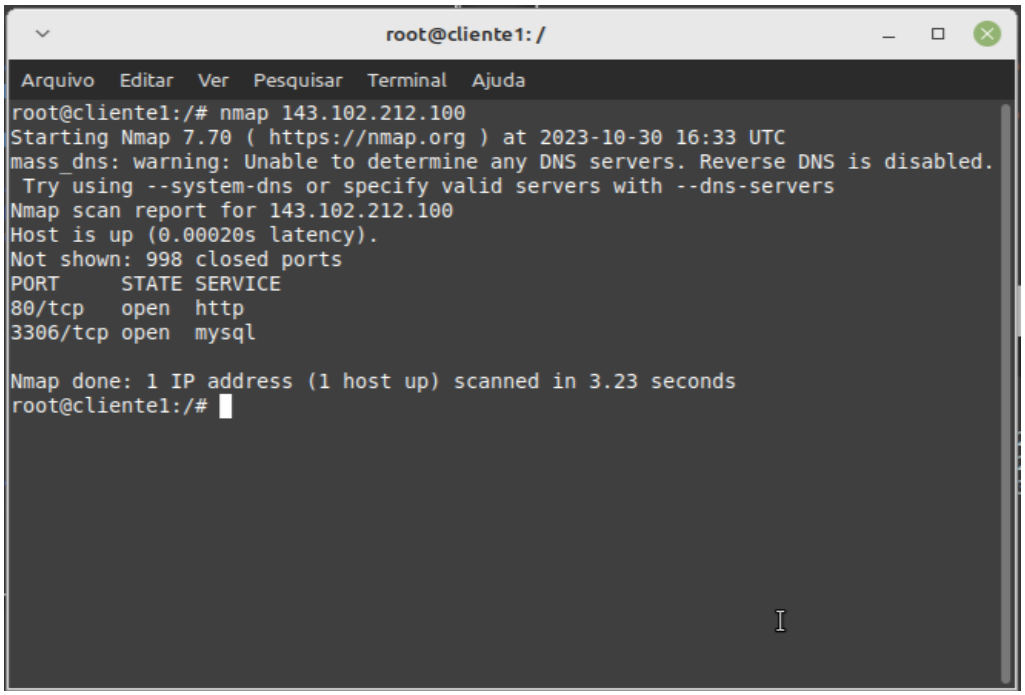
4.2.2 Descrição do Laboratório

Esse experimento consiste em configurar três dispositivos finais como clientes que vão consumir uma aplicação web que ficará no dispositivo internet com o IP 143.102.212.100 ficando com a seguinte disposição, o primeiro cliente ficou com o IP 10.1.1.11, o segundo cliente ficou configurado com o IP 10.1.1.12 e o terceiro cliente ficou com o IP 10.1.1.13, os seus respectivos gateways ficaram configurados na porta eth0 do servidor com o IP 10.1.1.1. No cliente 1 execute o comando:

```
1  root@cliente1:/#  nmap 143.102.212.100
```

Onde o Nmap (network mapper) é utilizado para buscar portas abertas sendo executado no terminal do cliente1, nesse caso foi informado somente um endereço IP, mas poderia ser utilizado o número da porta como parâmetro. o Nmap fará uma varredura em conjunto padrão de portas para identificar quais portas estão abertas e quais estão sendo utilizadas como mostra a figura 11.

Figura 11 - Busca por portas abertas na rede



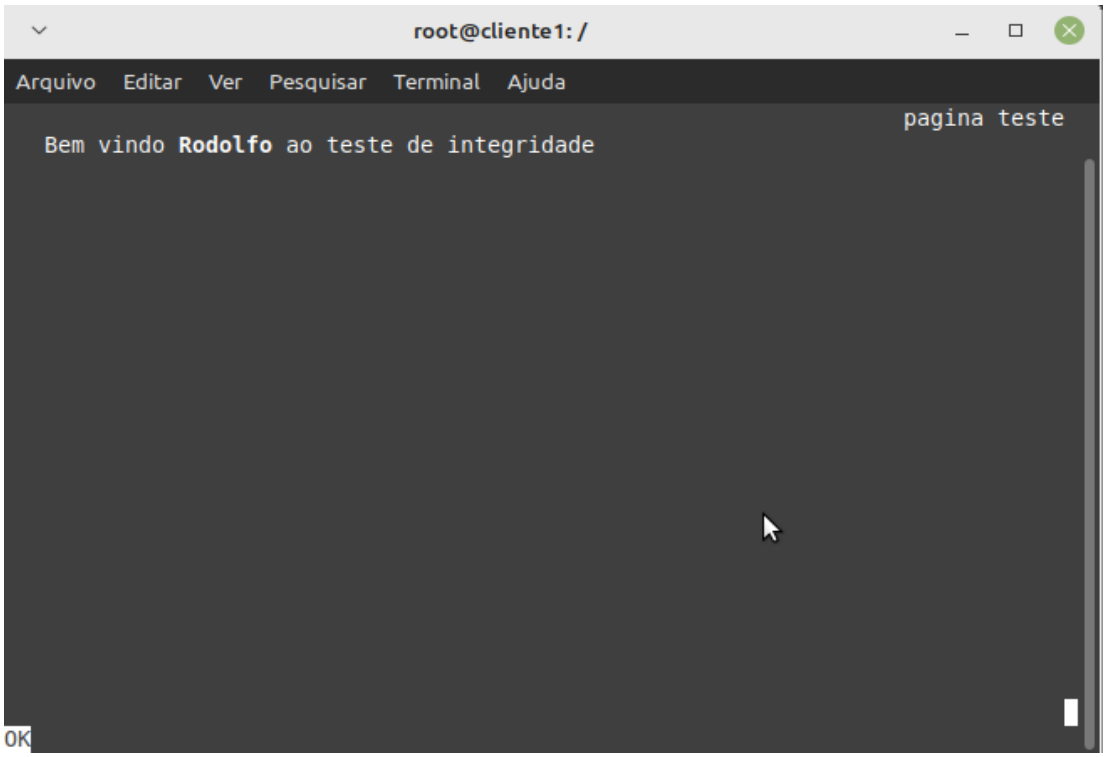
Fonte: Autor

Após portas abertas e com senhas fáceis serem encontradas, o dispositivo é acessado em busca de serviços vulneráveis o que aumenta a eficácia do ataque, a principal ameaça que pode decorrer a partir da exploração dessas vulnerabilidades são: captura de dados da rede local que estão em tráfego, perda da disponibilidade do dispositivo e ainda exposição a ataques DDoS. no cliente 1 execute o comando a seguir :

```
1  root@cliente1:/# links 143.102.212.100
```

Onde está executando um comando para acessar a aplicação web utilizando o navegador links, alocada no dispositivo internet que está executando o servidor apache 2, a figura 12 mostra a página web executada.

Figura 12 - Página inicial da aplicação



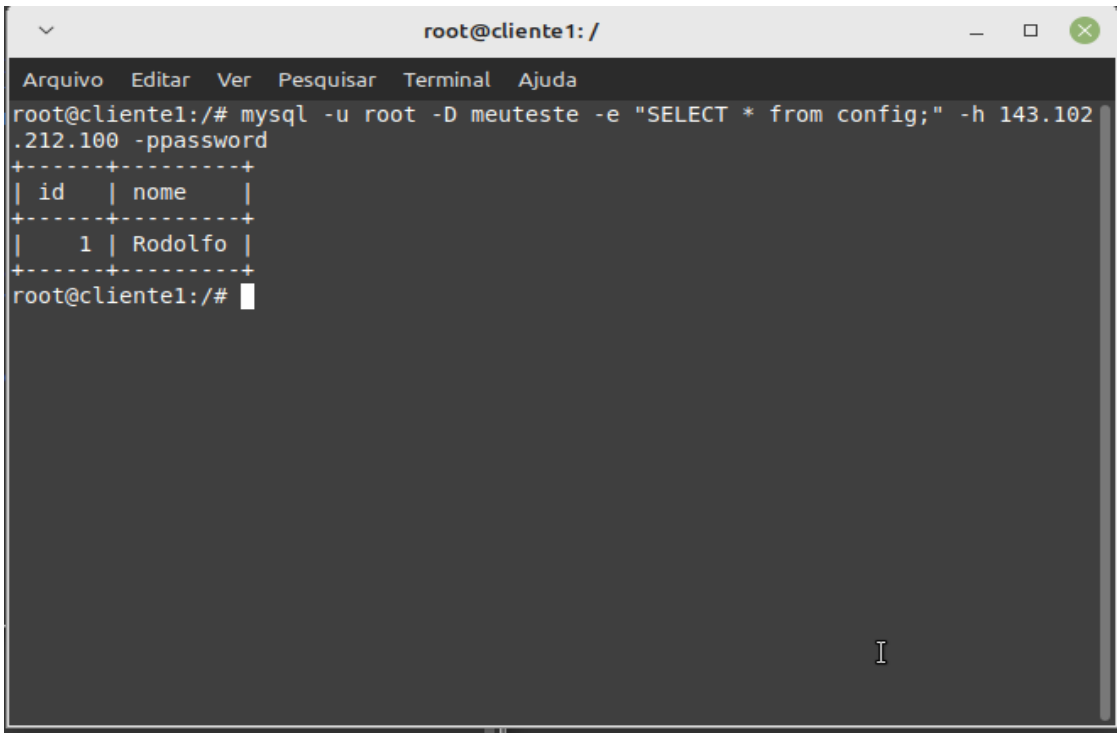
Fonte: Autor

O escaneamento da rede que foi feito utilizando o Nmap revelou diversas portas vulneráveis, após identificar os alvos o ataque pode ser realizado utilizando a fragilidade de configuração no servidor de banco de dados, é comum encontrar banco de dados com configurações e contas no padrão default a partir dessa vulnerabilidade vai ser explorada, no cliente 1 execute o comando:

```
1 root@cliente1:/# mysql -u root -D meuteste -e "SELECT * from config;" -h 143.102.212.100 -
2 ppassword
```

Onde está tentando conectar ao shell do servidor de banco de dados onde o parâmetro -u especifica o nome de usuário do servidor de banco de dados que no caso remete ao usuário root, como a senha e password foi possível ao atacante se conectar conforme mostra a figura 13.

Figura 13 - Acesso dados do sqlserver



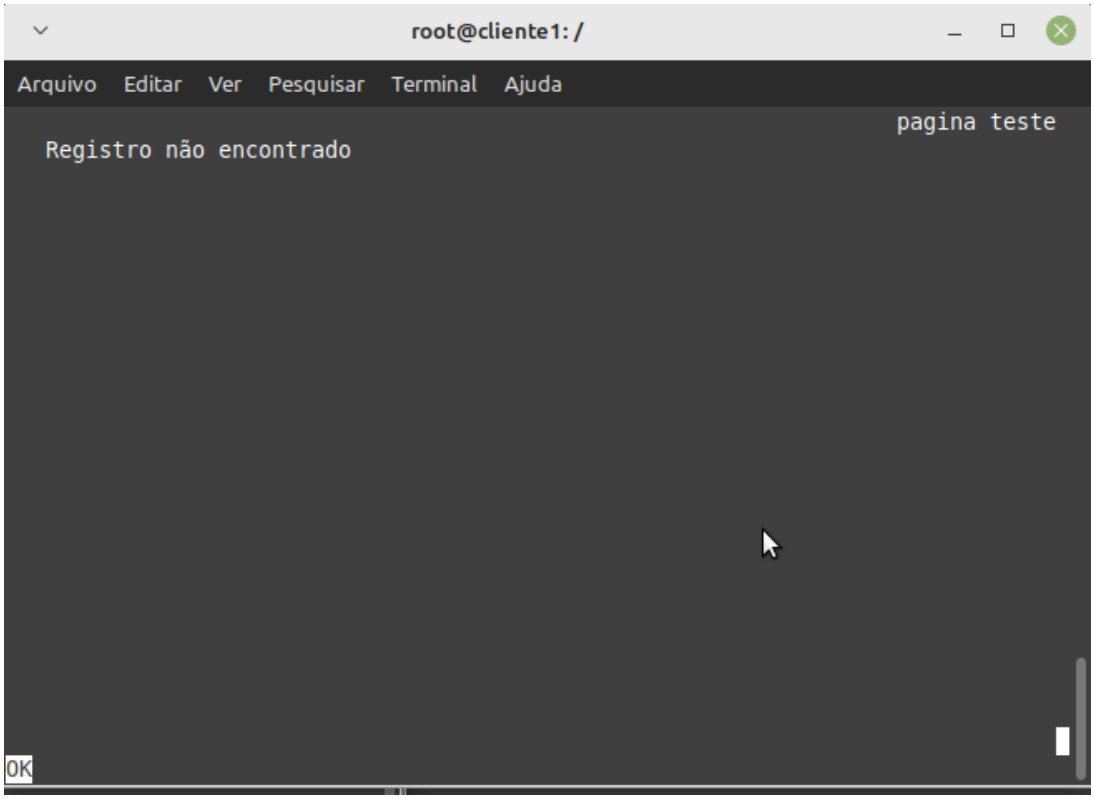
Fonte: Autor

O modo de ataque é semelhante ao executado anteriormente, é feita a conexão com o servidor de banco de dados, a página é exposta a um ataque usando o usuário root e a senha padrão em caso de sucesso o tem-se acesso ao servidor, mas dessa vez a disponibilidade do serviço será afetada no cliente 1 execute o comando:

```
1 root@cliente1:/# mysql -u root -D meuteste -e "DELETE FROM confing WHERE id =1;" -h
2 143.102.212.100 -ppassword
```

Onde é feito o DROP da tabela utilizando a senha já conhecida, afetando a disponibilidade do serviço conforme mostra a figura 14.

Figura 14 - Serviço web afetado



Fonte: Autor

4.3 Servidor Web com Firewall

Considerando as vulnerabilidades encontradas no laboratório anterior, nessa seção será implementado uma solução com uso de um firewall. será utilizado o iptables que é uma ferramenta em linha de comando utilizada para controlar filtros de pacotes do linux, e é parte do subsistema de rede do kernel linux. A principal utilidade do iptables é controlar tráfego em uma rede, decidindo quais pacotes serão permitidos ou bloqueados com base em regras, essas regras podem ser organizadas em tabelas e cada tabela é composta por cadeias (chains). Existem três tabelas fundamentais no iptables que são:

- Tabela Filter: Essa é a tabela padrão que é usada para a filtragem de pacotes, o administrador define as regras para encaminhar pacotes, aceitar ou rejeitar.
- Tabela NAT: Essa é a tabela usada para a tradução de endereços de rede e portas, muito utilizada quando se quer atribuir diversos endereços privados para endereços públicos roteáveis.

- Tabela Mangle: essa tabela é usada para alterar pacotes, por exemplo, modificando campos do cabeçalho IP.

As cadeias (chains) são regras que são aplicadas sequencialmente em pacotes de rede que podem ser:

- INPUT: Contém regras para pacotes que possuem como destino o próprio firewall.
- OUTPUT: Contém regras que são para os pacotes que são gerados pelo próprio firewall.
- FORWARDING: contém regras para pacotes que são roteador através de outros dispositivos e que vão passar pelo firewall para chegar ao seu destino.

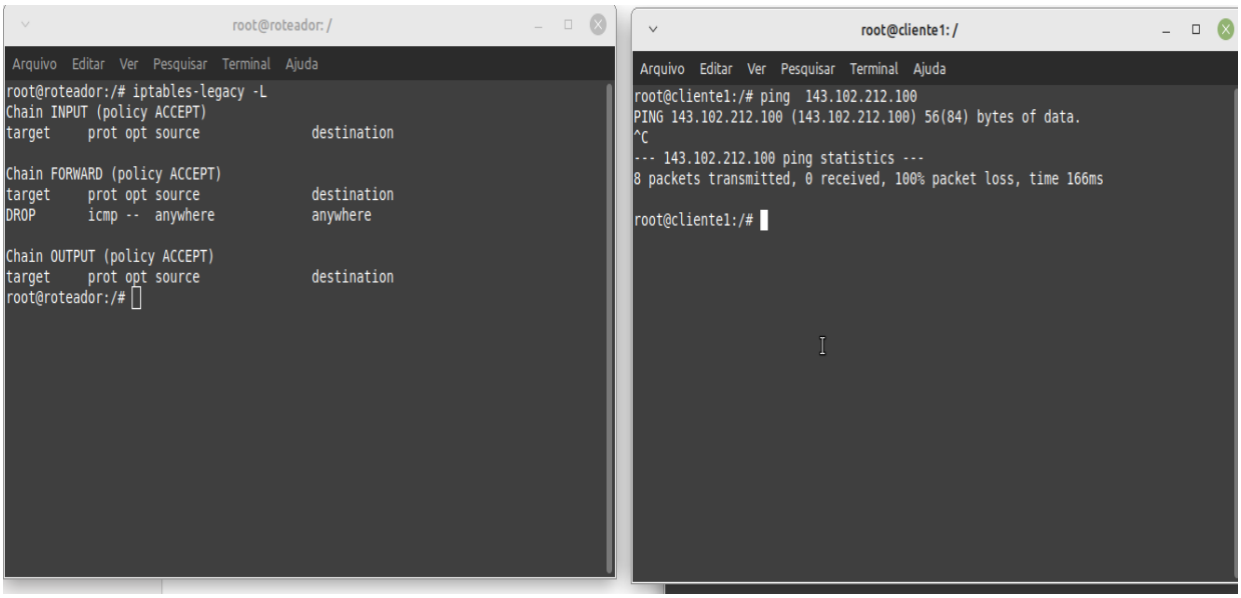
4.3.1 Descrição do laboratório

Esse laboratório consiste em implementar um firewall para mitigar algumas vulnerabilidades encontradas anteriormente. A topologia do laboratório será a mesma utilizada na seção anterior com a adição de um firewall entre as bordas. No cliente 1 execute o seguinte comando:

```
1 iptables-legacy -A FORWARD -p icmp -j DROP
```

Onde essa regra impede o roteamento de tráfego de pacotes ICMP (internet control message protocol) , que pode ser utilizado pelo atacante para tornar o alvo indisponível, pois vai estar respondendo todas as requisições consumindo assim todos os seus recursos. A figura 15 mostra a aplicação dessa regra.

Figura 15 - Bloqueio de tráfego icmp



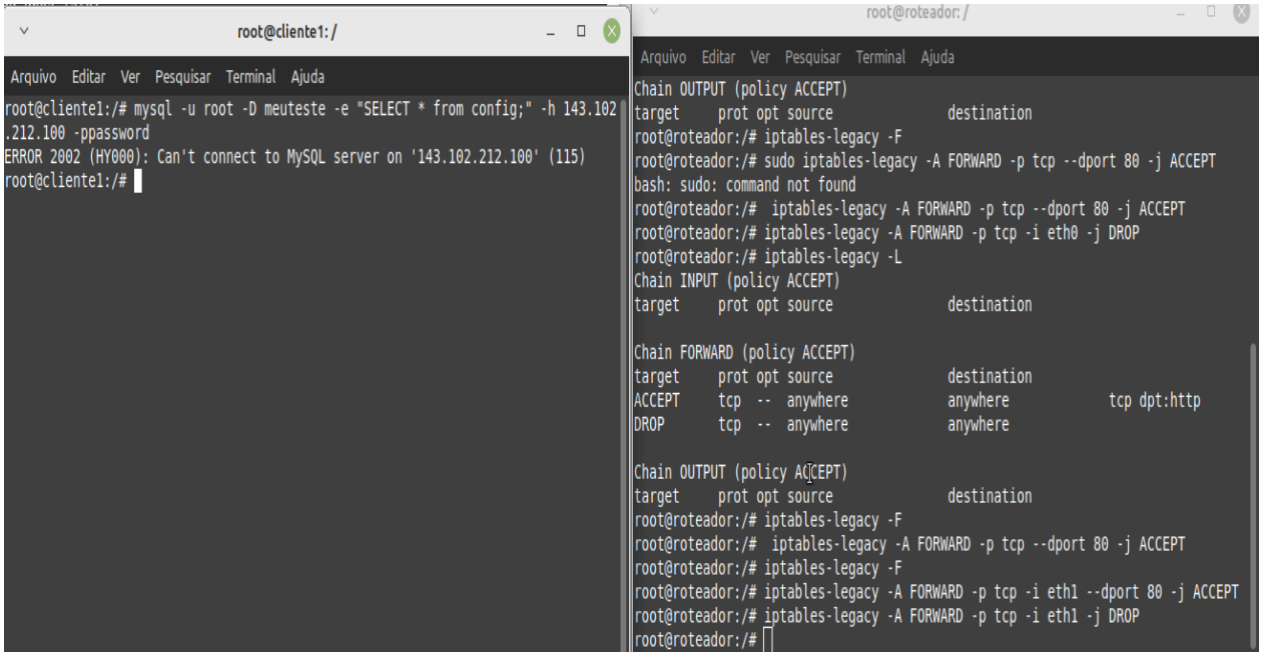
Fonte: Autor

Em seguida é necessário estabelecer medidas de segurança para o tráfego de pacotes TCP, para que somente as portas necessárias e confiáveis sejam permitidas todas as outras portas serão bloqueadas e só serão liberadas caso o administrador permita, o que minimiza erros de configuração de segurança. No cliente 1 execute os seguintes comandos:

```
1 iptables-legacy -A FOWARD -p tcp -i eth1 --dport 80 -j ACCEPT
2 iptables-legacy -A FOWARD -p tcp -i eth1 -j DROP
```

Onde o acesso ao servidor web é permitido roteamento na porta 80 usando o protocolo TCP que encapsula o protocolo HTTP, encaminhado proveniente da interface de rede eth1, posteriormente todo o tráfego TCP que chega a interface é bloqueado. A figura 16 ilustra a tentativa de acesso do atacante à porta TCP que corresponde ao servidor de banco de dados da aplicação web.

Figura 16 - Tentativa de acesso a porta tcp bloqueada



Fonte: Autor

Ao aplicar regras de firewall é importante entender o impacto que elas podem ocasionar no seu ambiente de rede e das suas implicações de segurança. Além disso, é importante garantir que serviços importantes fiquem disponíveis, por exemplo, serviços de acesso remoto para gerência como o SSH (secure socket shell) que utiliza a porta 22.

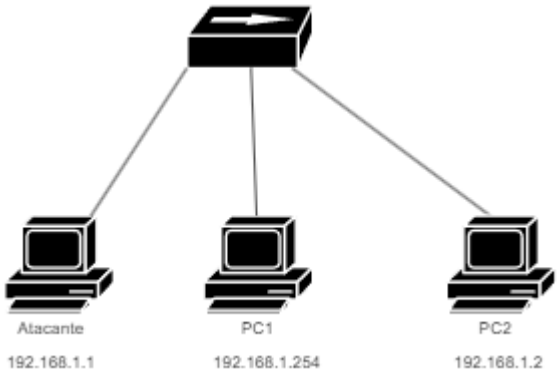
4.4 Man-in-the-Middle

O objetivo desse laboratório é simular um ataque Man-in-the-middle ou ataque de homem de meio, que consiste na interceptação de dados enquanto ocorre a comunicação entre dispositivos, onde o atacante se insere no meio da comunicação com o objetivo de modificar, retransmitir ou mesmo rejeitar.

4.4.1 Cenário de rede

Neste laboratório vai ser utilizado um cenário com três dispositivos, PC1, PC2 e atacante, todos sendo endereçados na mesma LAN, a figura 17 ilustra a topologia de rede e os endereços IP das máquinas.

Figura 17 -Topologia utilizada no laboratório



Fonte: Autor

4.4.2 Descrição do Laboratório

Esse laboratório consiste em simular um “ataque de ARP spoofing” ou “ARP poisoning”. A tabela ARP (address resolution protocol) tem função de associar endereços IP a endereços MAC em uma rede local. No ARP spoofing o atacante envia mensagens ARP falsificadas para um computador na rede, fazendo com que o mesmo atualize sua tabela ARP incorretamente com um endereço escolhido pelo atacante. Isso leva a associação de um IP legítimo de um dispositivo ou gateway para um controlado pelo atacante. Com o controle do atacante sobre a tabela ARP ele pode interceptar ou redirecionar o tráfego na rede local ao seu critério que podem ser:

- Observar a comunicação: O atacante monitora o tráfego entre a vítima e outros dispositivos na rede, que podem ser dados sensíveis, senhas e informações confidenciais.

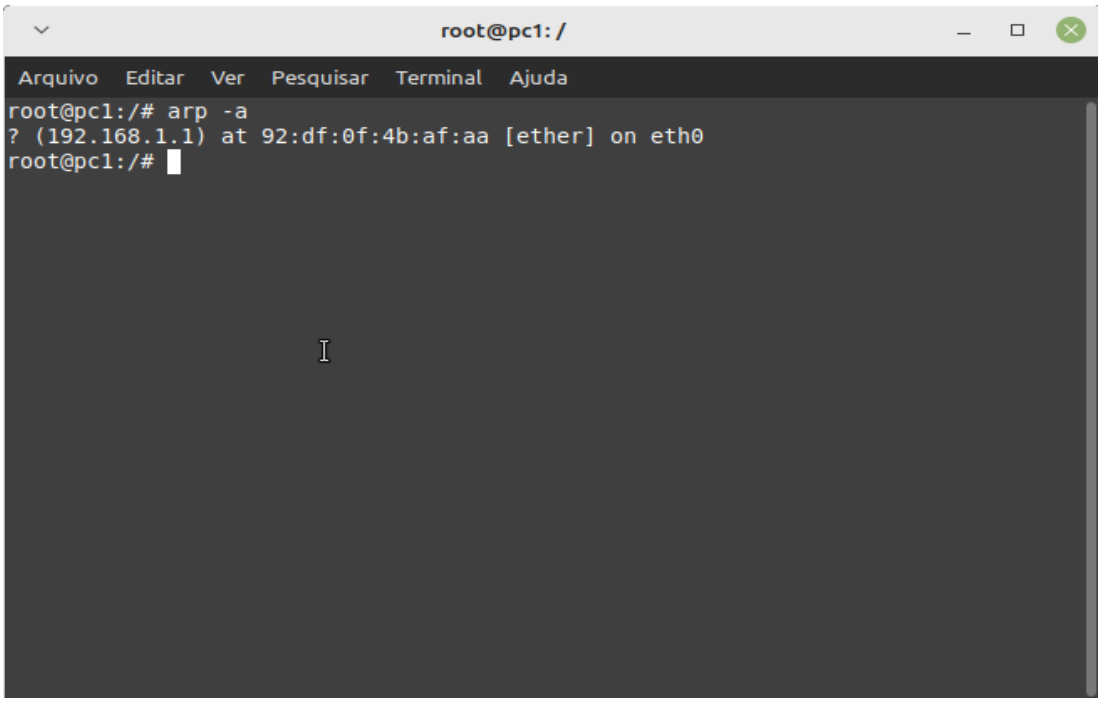
- Ataque de man-in-the-middle: O atacante se posiciona entre a vítima e o dispositivo a ser conectado, ficando no meio da comunicação sem autorização, podendo ainda injetar dados na comunicação entre a vítima e outros dispositivos.

para observar observar esses cenários execute o seguinte comando no dispositivo atacante:

```
1 ping 192.168.1.254
2 arp -a
```

Onde é feita a comunicação entre o dispositivo atacante e o alvo desejado, em seguida é listada a sua tabela ARP conforme mostra a figura 18.

Figura 18 - Tabela ARP do atacante



Fonte: Autor

Em seguida é necessário ter conhecimento do endereço MAC e seus respectivos IPs, a tabela 2 mostra a correspondência dos endereços IPs e o endereço MAC de seus respectivos dispositivos.

Tabela 2 - Lista de endereços MAC

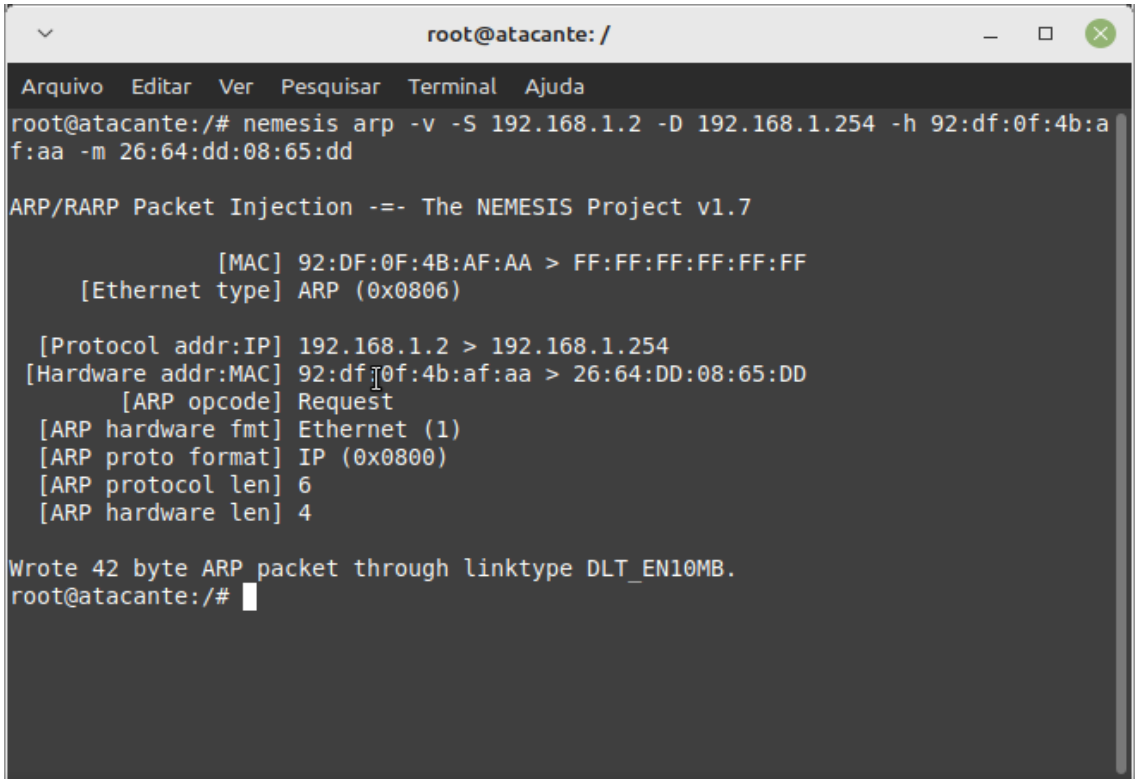
Dispositivo	IP	MAC
Atacante	192.168.1.1	92:df:0f:4b:af:aa
PC1	192.168.1.254	26:64:dd:08:65:dd
PC2	192.168.1.2	1e:a0:ab:e3:c9:a7

A tabela ARP ajuda a desempenhar a comunicação entre dispositivos: quando um host envia um pacote IP para outro dispositivo, é feita a consulta na tabela ARP onde é obtido um endereço MAC que corresponde a esse endereço IP, caso este endereço o IP não esteja rede é feita a solicitação por meio do mac da interface de gateway que encaminhará o pacote para outra rede. No dispositivo atacante execute o seguinte comando:

```
1 nemesis arp -v -S 192.168.1.2 -D 192.168.1.254 -h 92:df:0f:4b:af:aa -m 26:64:dd:08:65:dd
```

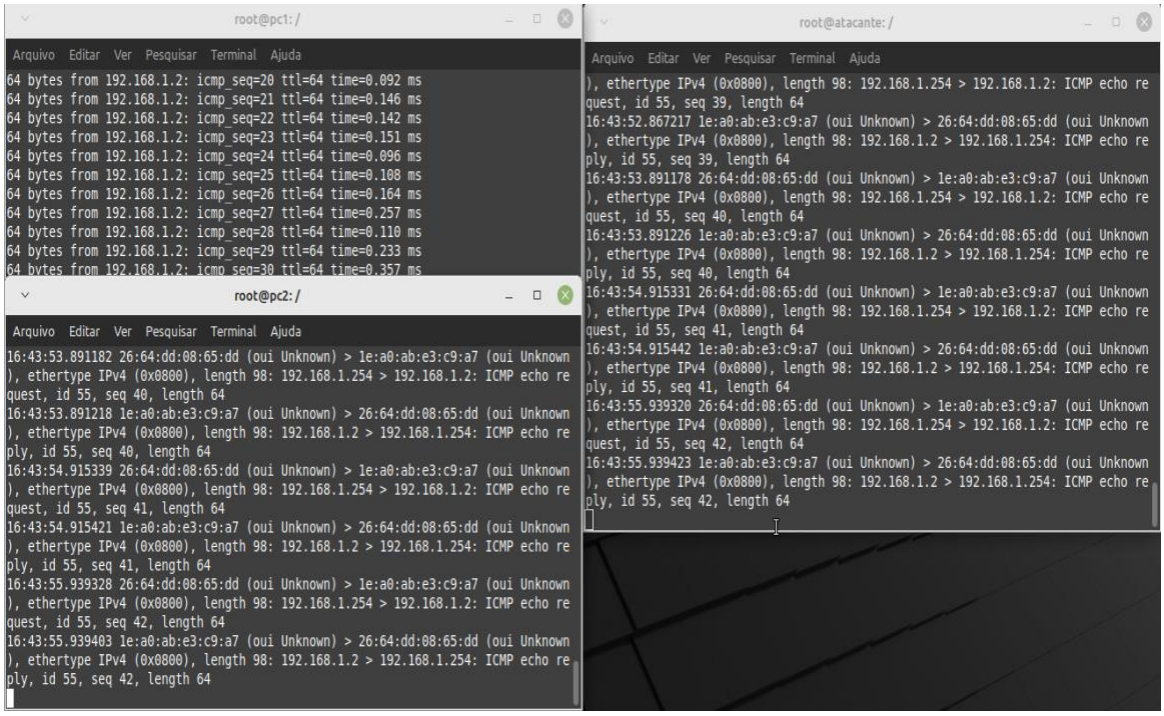
Onde o comando usa o nemesis que é uma ferramenta de injeção de pacotes e permite a criação de pacotes personalizados. Em que o -s indica o IP que o atacante deseja falsificar, e o -D indica o IP de destino ao qual quer se enganar, o -h especifica o MAC do atacante e por fim o -m indica o endereço MAC que será afetado. A figura 17 mostra a execução da ferramenta nemesis.

Figura 19- Injeção de pacote com o nemesis



Fonte: Autor

Figura 20 - Ataque man-in-the-middle em execução



Fonte: Autor

A figura 20 apresenta os pacotes interceptados pela máquina atacante de endereço IP 192.168.1.1 no momento da execução do ping, entre a máquina PC1 endereço 192.168.1.254 e a máquina PC2, endereço 192.168.1.2, observa-se que o dispositivo atacante durante o ataque, irá interpretar a comunicação, a ocorrência é clara pois todas as comunicações foram interceptadas conforme destacado na figura 20.

4.5 VPNs

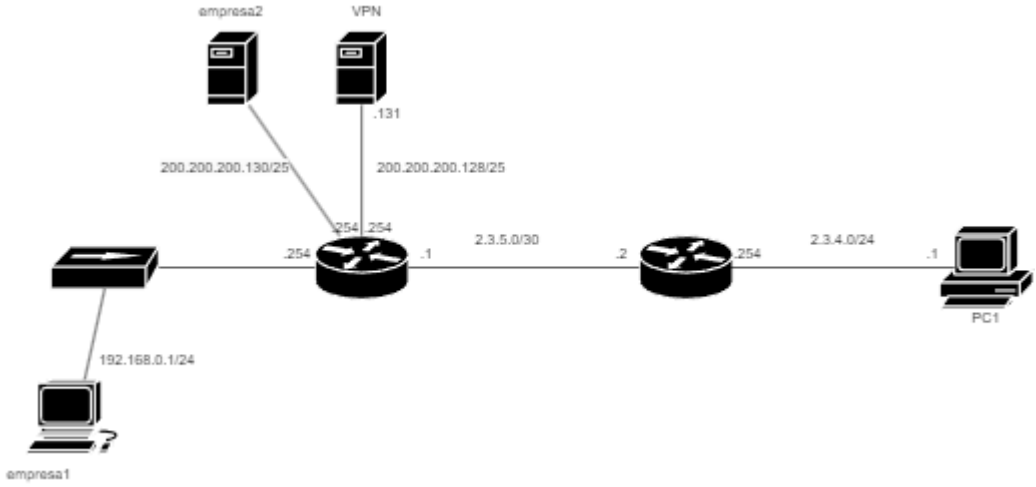
Neste laboratório o objetivo é simular uma rede utilizando uma conexão VPN, que vai permitir a comunicação entre dois pontos distintos utilizando uma rede segura. Uma conexão VPN (virtual private network) adiciona criptografia na conexão no tráfego que circula entre as redes. Isso significa que, mesmo que o tráfego esteja por redes públicas, como por exemplo a Internet, ele vai ser protegido contra acesso não autorizado, isso é fundamental durante o tráfego de informações sensíveis. Existem vários protocolos e métodos para implementação de VPNs, sendo os dois mais comuns:

- IPSec: Oferece um conjunto de protocolos para a segurança de comunicação em nível de IP e é implementado na camada na de rede.
- SSL/TLS: Atua na camada de transporte e aplicação e provê uma conexão segura baseada nos princípios de confidencialidade, integridade e disponibilidade, sendo que o SSL é um protocolo proprietário, contudo a IETF produz especificações públicas do TLS.

4.5.1 Cenário de Rede

A Topologia utilizada no experimento representa uma rede de uma empresa, o lado direito simula uma rede de fora que representa a internet, o roteador 1 funciona como gateway entre a rede interna da empresa e a internet, essa é uma representação típica, pois o roteador 1 atua como firewall e controla o tráfego entre as duas redes. Este cenário está ilustrado na figura 21. A tabela 3 descreve os equipamentos utilizados neste laboratório.

Figura 21 - Topologia utilizada no laboratório



Fonte: Autor

Tabela 3 - Descrição de equipamentos utilizados no laboratório

Dispositivo	Funcionalidade
Roteador 1	Ponto de comunicação entre a rede interna e externa
VPN	Utilizado para intermediar a conexão de uma conexão fora da rede interna
Roteador 2	Utilizado para encaminhar pacotes da rede externa
Hub	Utilizado para fazer a interligação de todos os dispositivos da rede interna
Empresa 2	Utilizado para hospedar serviços fora da rede interna
Cliente1	Utilizado para conexão com a rede interna fazendo uma requisição ao servidor VPN
Empresa 1	Utilizado para simular equipamentos da rede interna

4.5.2 Descrição do laboratório

Uma conexão VPN permite o acesso de uma rede de fora da rede interna de uma empresa ou organização fornecendo uma criptografia para a conexão, neste laboratório vamos configurar o dispositivo pc1 para acessar a rede interna interna, compreendendo os dispositivos conectados ao roteador 1, mas antes o acesso acesso à rede deve ser bloqueado por meio de regras de firewall, no roteador 1 execute o comando:

```
1 iptables-legacy -A FORWARD -o eth0 -d 192.168.0.0/24 -j DROP
```

Onde o acesso à rede interna por meio do dispositivo pc1 foi bloqueado, a conexão será feita por meio de uma conexão vpn utilizando o openvpn que é uma ferramenta open source licenciado sob a GPL (general public license), vai ser criado um servidor VPN no dispositivo VPN, portanto os computadores que desejaram se conectar a rede deverão se conectar ao servidor VPN. O openVPN utiliza chaves assimétricas e certificados para fazer a autenticação dos usuários, vai ser utilizado um conjunto de scripts do openVPN para gerar uma autoridade certificadora (CA) e certificados.

No servidor VPN execute os seguintes comandos no diretório /etc/openvpn/easy-rsa/vars e altere as seguintes linhas:

```
set_var KEY_COUNTRY "BRASIL"
set_var KEY_PROVINCE "MARANHAO"
set_var KEY_CITY "Sao Luis"
set_var KEY_ORG "UFMA"
set_var KEY_EMAIL "admin@exemplo.com"
set_var KEY_OU "Organizacao"
```

Onde foi configurada a entidade certificadora da conexão para criptografar o tráfego entre o servidor e o cliente. No servidor VPN execute os seguintes comandos:

```
1 ./easyrsa init-pki
```

```
2 ./easyrsa build-ca nopass
```

Onde foi executado um script easyrsa para iniciar o gerenciamento da autoridade certificadora e em seguida foi construído a CA com os respectivos arquivos:

- ca.crt: é distribuído entre o cliente e servidor e cada parte confia na CA para validar os seus respectivos certificados, onde todos os participantes estão se comunicando com entidades legítimas, evitando interceptação da comunicação por atacantes, que não serão capazes de fornecer um certificado válido e portanto não terão a conexão autenticada e a comunicação não será estabelecida.
- ca.key: é a chave privada correspondente ao certificado público da CA, essa chave é usada para assinar os certificados de servidor e cliente, garantindo o princípio básico de autenticidade.

No servidor VPN execute os seguintes comandos para gerar arquivos que vão ser usados durante o processo de criptografia.

```
1 
2 ./easyrsa gen-req server nopass
3 ./easyrsa sign-req server server
4 ./easyrsa gen-req client nopass
5 ./easyrsa sign-req client client
```

Onde serão geradas solicitações de chaves e certificados para o servidor e cliente, e em seguida assinar essas solicitações para criar os certificados correspondentes. Essa sequência de comandos é padrão para configurar um ambiente com openVPN usando o easyrsa para gerar os certificados, as chaves privadas associadas a esses certificados devem ser protegidas adequadamente pois os certificados são uma parte crítica da autenticação e segurança em uma rede VPN. no servidor VPN execute o seguinte comando:

```
1 ./easyrsa gen-dh
```

Onde o comando é usado para gerar os parâmetros Diffie-Hellman (DH) esses parâmetros DH são usados durante a negociação de chaves entre o servidor

openVPN e os clientes. O processo Diffie-Hellman permite que o servidor e cliente concordem sobre uma chave de sessão compartilhada sem que ela seja transmitida pela rede. A geração dos parâmetros DH pode levar algum tempo, pois envolve muitos cálculos matemáticos, após a conclusão do processo de geração de parâmetros DH, eles vão ser utilizados no arquivo de configuração do servidor openVPN. A segurança deste arquivo é fundamental e necessário a proteção do mesmo e regenerá-lo periodicamente. No servidor VPN execute o seguinte comando:

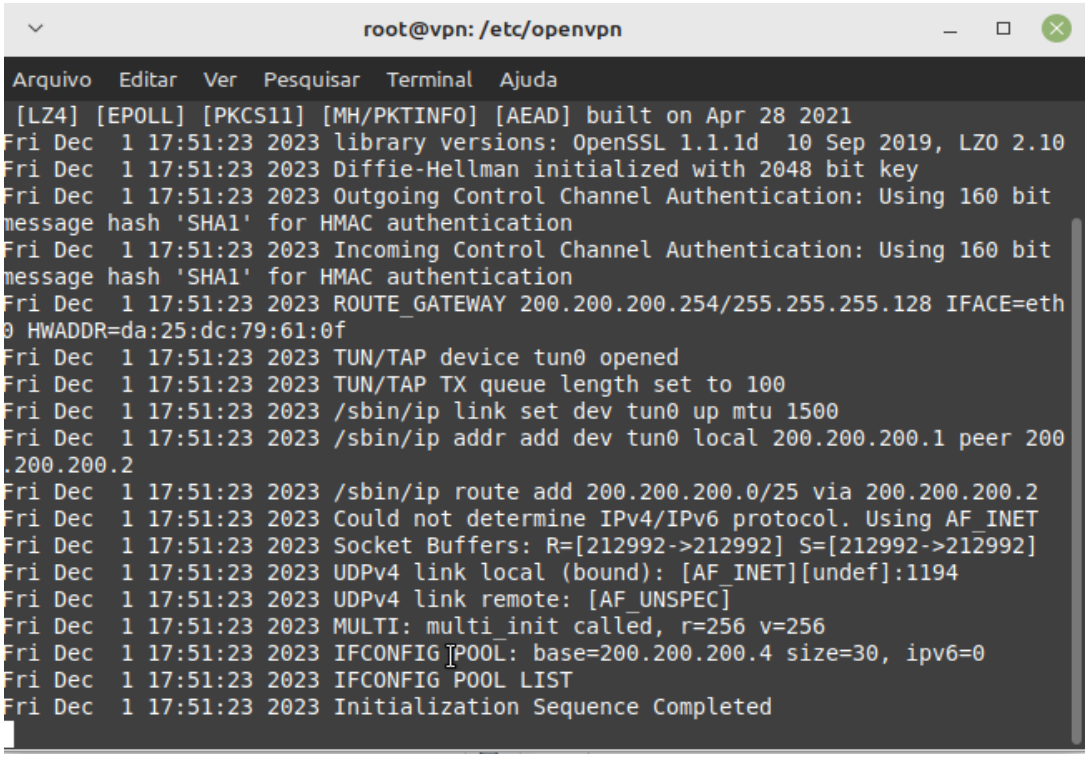
```
1 openvpn --genkey --secret ta.key
```

Onde o comando é usado para gerar uma chave de autenticação TLS (Transport Layer Security) para o openVPN ela é utilizada para garantir a integridade dos pacotes transmitidos entre o cliente e o servidor openVPN. A chave de autenticação é importante para garantir que os dados transmitidos entre o cliente e servidor não foram alterados por um atacante, ela adiciona uma camada adicional de segurança, ela deve ser ativada no arquivo de configuração do servidor openvpn e no cliente, a segurança deste arquivo é crucial para a implementação do openvpn e deve distribuído de forma segura entre entre o servidor e o cliente. no servidor openVPN execute o comando:

```
1 openvpn server.conf
```

No qual é usado para iniciar o servidor openVPN com base nas configurações especificadas, esse arquivo contém todas as informações necessárias para iniciar o servidor openVPN. A figura 22 mostra a execução do serviço no servidor VPN.

Figura 22 - Inicialização do servidor VPN



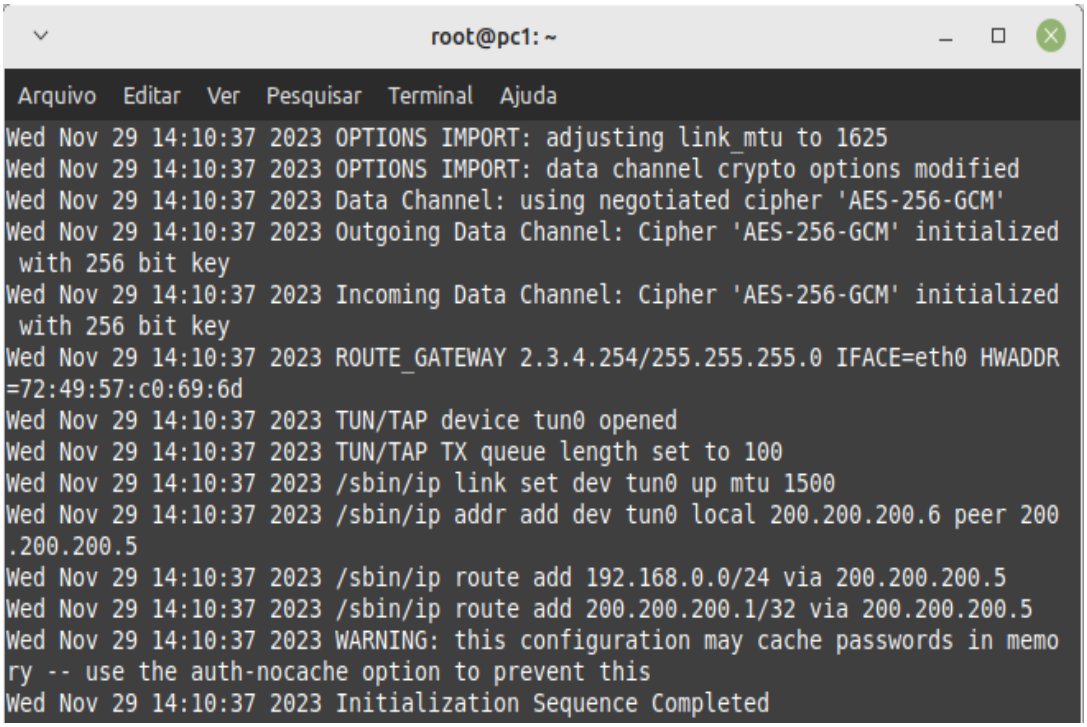
Fonte: Autor

Onde a sub rede da VPN foi configurada com o endereço IP 200.200.200.0/25 isso significa que, os dispositivos na VPN incluindo o cliente (PC1), serão atribuídos IPs dentro dessa faixa de endereço quando estiverem conectados. No PC1 execute o seguinte comando:

```
1 openvpn client.conf
```

No qual é usado para iniciar um cliente openVPN utilizando as configurações já especificadas no arquivo de configuração, contendo as informações sobre o servidor openVPN, configurações de autenticação, opções de criptografia e diversas outras. O arquivo deve estar corretamente configurado para que a conexão seja estabelecida com êxito, conforme mostra a figura 23.

FIgura 23 - Execução do cliente VPN



Fonte: Autor

Onde o PC1 recebe automaticamente um endereço da subrede 200.200.200.0/25 para se conectar ao servidor VPN, esse processo ocorre automaticamente durante o processo de conexão com o servidor VPN.

Em resumo, a VPN proporciona uma camada de segurança crucial ao permitir acesso remoto à rede interna de uma organização, mantendo a confidencialidade e integridade dos dados durante a comunicação através de redes públicas.

5 CONCLUSÃO

Neste trabalho, foi realizado um estudo sobre algumas vulnerabilidades encontradas em redes de computadores, utilizando o software de simulação de rede kathará.

Tendo como objetivo principal fornecer simulações sobre vulnerabilidades encontradas no mundo real de forma fiel aos desafios que podem ser encontrados em ambientes de rede. Essa abordagem permitiu uma análise detalhada das ameaças encontradas.

Tendo em vista que altos custos de implantação, manutenção e aquisição de dispositivos para laboratórios podem ser problemas impeditivos para instituições ofertarem disciplinas de redes de computadores. Levando em consideração esses problemas, parte o objetivo deste trabalho, algo que pode ser tangível utilizando o software kathará para criação de ambientes virtuais que são capazes de simular dispositivos e cenários de rede, permitindo a experimentação do aluno, além de evitar o aumento de despesas de capital, já que é utilizado somente um computador para tal.

Ao longo deste trabalho foi apresentado o software de simulação de redes kathará que pode ser aplicado ao ensino de disciplinas de redes de computadores, permitindo uma experimentação prática e dinâmica, permitindo que os alunos explorem e aprendam em um ambiente virtual seguro. Proporcionando uma oportunidade de aplicar teorias aprendidas em sala de aula em situações reais, oferecidas pelos estudos de caso, fortalece não apenas a teoria, mas também habilidades práticas essenciais para profissionais de redes de computadores.

Como trabalho futuro poderia empregar a análise de laboratórios mais complexos e com vulnerabilidades que poderiam desencadear ameaças muito mais graves, não apenas aprofundaria o entendimento das vulnerabilidades, mas também contribuiria para o desenvolvimento contínuo de estratégias de seguranças mais robustas e eficazes.

REFERÊNCIAS

FIRMINO, M. **Segurança de redes:** Introdução à Segurança da Informação. IFRN, 2019. Disponível em: https://docente.ifrn.edu.br/josemacedo/disciplinas/2019/2019.1/introducao-a-seguranca-da-informacao. Acesso em: 13 ago. 2023.

GEUS, P. L. de; NAKAMURA, E. T. **Segurança de redes em ambientes cooperativos.** 2. ed. São Paulo: Futura, 2003.

GURGEL, P. H. M. et al. **Redes de Computadores:** Da teoria à prática com Netkit. 1. ed. Rio de Janeiro: Elsevier, 2015.

KATHARÁ, **A Lightweight Network Emulation System**. Acessado em 03-10-2023. Disponível em : <https://www.kathara.org/>

LIMA, M. B. Firewalls - Uma introdução à segurança. **Revista do Linux**, Curitiba, p. 16, 2000.

MACORATTI, J. C. Minicurso: **Criptografia na plataforma.NET**. 2010. Disponível em: http://www.macoratti.net/Cursos/Cripto/net_cripto4.htm. Acesso em: 13 ago. 2023.

MORAES, A. F. de. **Segurança em Redes:** Fundamentos. 1 ed. São Paulo: Érica, 2010.

M. Scazzariello, L. Ariemma and T. Caiazzi, "**Kathará: A Lightweight Network Emulation System**," NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium, Budapest, Hungary, 2020, pp. 1-2, doi: 10.1109/NOMS47738.2020.9110351.

ROSS, Keith W.; KUROSE, James F. **Redes de Computadores e a Internet uma abordagem top-down**. São Paulo - SP - Brasil: Pearson, 2013.

STALLINGS, W. **Criptografia e segurança de redes: princípios e práticas**. 6. ed. São Paulo: Pearson Education do Brasil. 2015.

STALLINGS, W. **Redes e sistemas de comunicação de dados:** teoria e aplicações corporativas. 5. ed. Rio de Janeiro: Elsevier, 2005.