FACULDADE DE TECNOLOGIA DE AMERICANA "MINISTRO RALPH BIASI"

Curso Superior de Tecnologia em Segurança da Informação

Gustavo Amancio da Costa

Miqueias Sales de Lima

EXPLORAÇÃO DE VULNERABILIDADES EM SISTEMAS OPERACIONAIS LINUX

Americana, SP

2023

FACULDADE DE TECNOLOGIA DE AMERICANA "MINISTRO RALPH BIASI"

Curso Superior de Tecnologia em Segurança da Informação

Gustavo Amancio da Costa

Miqueias Sales de Lima

EXPLORAÇÃO DE VULNERABILIDADES EM SISTEMAS OPERACIONAIS LINUX

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

Americana, SP.

2023

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana Ministro Ralph Biasi- CEETEPS Dados Internacionais de Catalogação-na-fonte

COSTA, Gustavo Amancio

Exploração de vulnerabilidades em sistemas operacionais Linux. / Gustavo Amancio Costa, Miqueias Sales Lima – Americana, 2023.

62f.

Monografia (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana Ministro Ralph Biasi – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Dr. José Luis Zem

1. LINUX - sistema operacional 2. Redes de computadores 3. Segurança em sistemas de informação. I. COSTA, Gustavo Amancio, II. LIMA, Miqueias Sales III. ZEM, José Luis IV. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana Ministro Ralph Biasi

CDU: 681.3.066LINUX
681519
681.518.5

Elaborada pelo autor por meio de sistema automático gerador de ficha catalográfica da Fatec de Americana Ministro Ralph Biasi.

Gustavo Amancio da Costa
Miqueias Sales de Lima

EXPLORAÇÃO DE VULNERABILIDADES EM SISTEMAS OPERACIONAIS LINUX

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Curso Superior de Tecnologia em Segurança da Informação pelo Centro Paula Souza FATEC - Faculdade de Tecnologia de Americana - Ministro Ralph Biasi.
Área de concentração: Segurança da Informação.

Americana, 28 de novembro de 2023.

Banca Examinadora:

José Luis Zem
Doutorado
Fatec Americana - Faculdade de Tecnologia de Americana Ministro Ralph Biasi

Benedito Luciano Antunes de França
Mestrado
Fatec Americana - Faculdade de Tecnologia de Americana Ministro Ralph Biasi

Henrj Alves de Godoy
Ph.D.
Fatec Americana - Faculdade de Tecnologia de Americana Ministro Ralph Biasi

AGRADECIMENTOS

Gostaríamos de expressar nossa sincera gratidão a toda equipe docente da Faculdade de Tecnologia de Americana e a todos que contribuíram para o funcionamento desta instituição. Seu comprometimento, dedicação e apoio foram fundamentais para o nosso crescimento acadêmico. Suas aulas inspiradoras e trabalho incansável nos bastidores fizeram uma diferença significativa em nossa jornada. Levaremos suas lições e inspiração adiante em nossas vidas.

DEDICATÓRIA

Dedicamos este projeto de conclusão de curso a todas as pessoas especiais que estiveram ao nosso lado ao longo desta jornada. As nossas famílias, que sempre acreditaram em nós, nos apoiaram nos momentos de desafio e celebraram conosco nas conquistas. Vocês foram a nossa base sólida, a luz que iluminou o caminho. Aos nossos amigos, que compartilharam risos, noites de estudo e conselhos preciosos. Juntos, construímos memórias que levaremos para toda a vida. Aos nossos professores e orientadores, que dedicaram seu tempo e conhecimento para nos guiar neste percurso acadêmico. Suas orientações foram fundamentais para o nosso crescimento. E a todos os outros familiares, colegas e mentores que de alguma forma contribuíram para esta jornada, o nosso profundo agradecimento. Este projeto é o resultado do esforço coletivo e do amor que recebemos de cada um de vocês. Com humildade e gratidão, dedicamos a todos este trabalho, na esperança de que ele contribua para um mundo melhor. Muito obrigado por fazerem parte da nossa história e por tornarem este momento tão especial. Vocês são a nossa inspiração e motivação constante. Com carinho e gratidão.

RESUMO

A crescente dependência das organizações em redes de computadores para operações críticas tem gerado uma necessidade urgente de avaliar e fortalecer a segurança dessas redes. Este projeto de conclusão de curso tem como objetivo principal investigar e analisar as vulnerabilidades em redes de computadores, com ênfase na identificação e exploração dessas fraquezas. O projeto abordará diversas etapas essenciais, incluindo a identificação de vulnerabilidades comuns, análise de suas causas e potenciais impactos, e a criação de cenários práticos de exploração para demonstrar as consequências de tais ameaças. Serão utilizadas ferramentas de segurança e técnicas de teste de penetração para avaliar a resiliência das redes e sistemas sob ataque. Além disso, a pesquisa também abordará medidas preventivas e corretivas, destacando a importância de localizar vulnerabilidades existentes e solucioná-las, configurações adequadas e a implementação de práticas recomendadas para mitigar vulnerabilidades. Ao final do projeto, espera-se não apenas aumentar a compreensão das vulnerabilidades em redes de computadores, como também fornecer recomendações práticas para proteger essas infraestruturas críticas contra ameaças cibernéticas. O conhecimento adquirido terá implicações significativas na melhoria da Segurança da Informação e na proteção de dados sensíveis em ambientes empresariais e acadêmicos. Este projeto contribuirá para o avanço do conhecimento na área de Segurança da Informação, fornecendo *insights* valiosos sobre as táticas e estratégias empregadas por invasores cibernéticos, bem como orientações para reforçar a resiliência das redes de computadores em um cenário de ameaças em constante evolução.

Palavras Chaves: Segurança da informação; *pentest*; redes.

ABSTRACT

The increasing reliance of organizations on computer networks for critical operations has generated an urgent need to assess and strengthen the security of these networks. This graduation project aims to investigate and analyze vulnerabilities in computer networks, with a focus on identifying and exploiting these weaknesses. The project will address several essential stages, including the identification of common vulnerabilities, analysis of their causes and potential impacts, and the creation of practical exploitation scenarios to demonstrate the consequences of such threats. Security tools and penetration testing techniques will be used to assess the resilience of networks and systems under attack. Furthermore, the research will also cover preventive and corrective measures, highlighting the importance of applying security patches, proper configurations, and the implementation of best practices to mitigate vulnerabilities. By the end of the project, it is expected not only to increase the understanding of vulnerabilities in computer networks but also to provide practical recommendations to protect these critical infrastructures against cyber threats. The knowledge gained will have significant implications for improving information security and safeguarding sensitive data in business and academic environments. This project will contribute to advancing knowledge in the field of Information Security, providing valuable insights into the tactics and strategies employed by cyber intruders, as well as guidance for enhancing the resilience of computer networks in a constantly evolving threat landscape.

Keywords: *Information security; pentest*; *LAN*.

LISTA DE FIGURAS

LISTA DE QUADROS

SUMÁRIO

INTRODUÇÃO

O primeiro conceito de teste de penetração (*pentest*) surgiu em 1960 (Espinosa, 2023), quando a crescente indústria de tecnologia percebeu que o uso compartilhado de um mesmo sistema, que na época era o de tempo compartilhado, estava crescendo muito, algo que só aumentaria nos próximos anos. Com isto, a probabilidade de danos à integridade do sistema ocorrerem era alta, pois o progresso da computação faria com que ainda mais pessoas estivessem conectadas, o que resultaria na perda de controle e monitoramento dessas conexões. Assim, o mais correto a se fazer seria desenvolver meios de se proteger de acessos indevidos e programas que danificassem o funcionamento do sistema.

A partir disso, se formaram os primeiros times de testes de invasão, que ficaram conhecidos como "*Tiger Teams*", os primeiros destes trabalharam para o governo e para o exército dos Estados Unidos da América (EUA). Em 1971 a Força Aérea dos EUA solicitou um teste de segurança em seus sistemas de tempo compartilhado (Espinosa, 2023).

Um dos primeiros sistemas que apresentavam diversas vulnerabilidades era o de tempo compartilhado, a maneira que eles funcionavam era da seguinte forma, a unidade central de processamento, em inglês *central processing unit* (CPU), era compartilhada entre vários terminais em uma rede, todos os usuários utilizavam o mesmo processador por um determinado período. O usuário tinha a impressão de que todo o processamento estava sendo utilizado para ele, mas na realidade ele estava esperando em uma fila em que disponibilizaria o processamento por um curto período e seguiria para o próximo terminal. Por este sistema ser compartilhado, havia uma ausência de confidencialidade nos programas, os usuários conseguiam acessar as informações de outros terminais que compartilhavam o mesmo processamento, por isso, era necessário realizar um teste de invasão para identificar as vulnerabilidades e mitigá-las (Padhyay, 2023).

I APRESENTAÇÃO

Atualmente no cenário tecnológico mundial muitos dados são compartilhados na rede, *crackers* estão a todo momento buscando maneiras de ter acesso a essas informações compartilhadas por empresas, onde as pessoas são o elo mais fraco.

Nesse contexto, a pergunta do problema da pesquisa é: como empresas podem aplicar o *pentest* para melhorar as suas defesas contra os ataques cibernéticos, e saber por onde essas informações estão sendo vazadas e expostas?

Serão utilizados nesta pesquisa os conhecimentos adquiridos nas disciplinas de Fundamentos de Perícia Forense em Segurança da Informação, Administração de Sistemas Operacionais de Redes, Segurança em Sistemas Operacionais e Redes de Computadores, Diagnóstico e Solução de Problemas de Tecnologia da Informação e Criptografia do curso de Segurança da Informação da Faculdade de Tecnologia (FATEC) de Americana.

1.1 Objetivos

Como objetivo principal desta pesquisa tem-se o de destacar a relevância do teste de penetração no contexto da Segurança da Informação, delineando suas aplicações apropriadas tanto para organizações quanto para estudantes da área. O enfoque recai na identificação de vulnerabilidades em redes específicas, visando aprimorar as defesas contra ameaças cibernéticas e softwares maliciosos.

Para atingir esse desiderato, conduzir-se-á uma revisão bibliográfica acerca das práticas dos testes de penetração (*pentesting)* e das ferramentas correlatas, destinada a prover compreensão aos profissionais e estudiosos de Segurança da Informação sobre a natureza e as abordagens desse procedimento. O trabalho almeja, adicionalmente, apresentar estatísticas elucidativas das vulnerabilidades mais comuns em redes de computadores e serviços online. A abordagem metodológica, centrada na tentativa de invasão de alvos previamente mencionados, visa revelar as principais fragilidades em sua segurança, permitindo intervenções corretivas antecipadas, salvaguardando assim a integridade, confidencialidade e disponibilidade das informações.

Outro ponto de destaque consiste na demonstração da prática do *pentest*, elucidando suas razões fundamentais de aplicação, princípios subjacentes, categorias de testes, bem como as fases e técnicas inerentes à prática de invasão. Ao término desse exame teórico, será delineado um cenário prático, viabilizando a visualização concreta da identificação de vulnerabilidades em uma rede específica com máquinas Linux, acompanhado de sugestões para resolução das deficiências de segurança identificadas.

1.2 Metodologias

A abordagem metodológica adotada nesta pesquisa é, de maneira geral, qualiquantitativa, visando fornecer uma perspectiva abrangente que abrange tanto informações qualitativas quanto quantitativas. Inicialmente, através de uma pesquisa bibliográfica, será abordado o que é o *pentest*, delineando a forma apropriada de utilização de suas ferramentas para aprimorar a Segurança da Informação. Serão também abordados aspectos legais pertinentes à sua aplicação, alertando sobre práticas proibidas por lei.

Em uma fase subsequente, será conduzida uma pesquisa documental em fontes especializadas sobre testes de penetração, com o propósito de adquirir dados sobre metodologias de invasão de sistemas. Pretende-se, igualmente, coletar e analisar informações referentes aos níveis de implementação das ferramentas de defesa comumente empregadas por empresas, identificando pontos de vulnerabilidade essenciais para a obtenção de elevados níveis de confidencialidade. Além disso, serão apresentadas estatísticas abrangentes sobre falhas de segurança frequentemente identificadas na *Internet*.

Por fim, será apresentado um cenário prático, no qual serão empregadas ferramentas específicas para a identificação de vulnerabilidades, sendo propostas soluções concretas para os problemas detectados.

1.3 Justificativas

De acordo com o *Blog Central Server*, no artigo intitulado “As 5 vulnerabilidades mais comuns em *web* sites e como evitá-las", postado em 9 de janeiro de 2015, adverte os leitores das vulnerabilidades que existem em sites e como elas podem nos causar prejuízo, sendo assim, demonstra também como evitá-las.

Durante a prática de identificação de vulnerabilidades em sites, exemplifica-se o uso da ferramenta disponível no site *builtwith* (Builtwith, 2023), este recurso revela a composição de um site, expondo os nomes dos serviços em execução na página e suas respectivas versões. Para ilustrar, considera-se o caso em que um site utiliza a linguagem de programação *Personal Home Page* (PHP) na versão 5.6, ao submeter o *Uniform Resource Locator* (URL) deste site ao *builtwith*, torna-se possível a realização de uma prática frequentemente empregada por invasores, a de pesquisar na *Internet* vulnerabilidades já conhecidas para determinado serviço na versão mencionada. Portanto, uma das primeiras abordagens do atacante será conduzir uma breve pesquisa na *Internet* para identificar as vulnerabilidades conhecidas do PHP na versão 5.6, possibilitando, assim, sua exploração.

Na perspectiva de defesa contra potenciais ataques, identificar as falhas já conhecidas pelo público é essencial, ao perceber a presença dessas vulnerabilidades em seu próprio site, é de extrema importância realizar a atualização do serviço e mitigar as brechas de segurança correspondentes.

Gonçalves (2022), em sua publicação intitulada “Conheça as 10 principais vulnerabilidades *web* de 2021”, no *blog* 4Linux, postada em 27 de janeiro de 2022, apresenta diversas vulnerabilidades encontradas *Internet* afora.

As vulnerabilidades mais comumente encontradas em sistemas e redes podem variar de senhas fracas, senhas fáceis de adivinhar ou que não são trocadas regularmente é que são um risco de segurança, softwares desatualizados ou não corrigidos que podem ter vulnerabilidades conhecidas que podem ser exploradas por atacantes, o *phishing*, que se caracteriza por tentativas de enganar os usuários para que revelem informações confidenciais, como senhas e informações de login.

Falhas de segurança em aplicativos são as que podem permitir que um invasor execute comandos maliciosos no sistema ou roubar informações confidenciais, os

ataques de força bruta que podem ser interpretados como tentativas repetitivas de adivinhar senhas ou outras informações de autenticação.

O *Malware* como vírus, trojans e *ransomware*, podem infectar sistemas e redes e causar danos significativos, os acessos físicos não autorizados a sistemas e redes pode permitir que invasores roubem ou danifiquem informações confidenciais.

Soldateli (2023), em sua publicação intitulada “Foi hackeado em 2022? Conheça as vulnerabilidades mais exploradas”, no *site* Olhar Digital, postada em 6 de janeiro de 2023, é advertido aos leitores sobre as vulnerabilidades mais exploradas por criminosos cibernéticos durante o ano de 2022.

Rijnetu (2023) em seu artigo “100+ *essential penetration testing statistics* [2023 *edition*]” no blog Pentest Tools, apresenta diversas estatísticas que estão relacionadas ao *penetration testing,* sendo elas:

> 75% das empresas realizam testes de penetração para medir sua postura de segurança ou por motivos de conformidade. 57% delas o fazem para apoiar um programa de gerenciamento de vulnerabilidades. [...]A maioria dos testadores de penetração utiliza uma variedade de ferramentas de segurança durante as atividades, sendo que 78% utilizam tanto ferramentas gratuitas quanto comerciais, enquanto 11% delas dependem de ferramentas gratuitas e de código aberto. [...]Em termos das características mais importantes em ferramentas de software de testes de penetração pagas, 77% das empresas disseram que relatórios são essenciais. 67% adquirem extensas bibliotecas de ameaças, enquanto 61% estão interessados em capacidades de testes multi vetoriais. [...]Os *scanners* de vulnerabilidades podem identificar mais de 50.000 vulnerabilidades únicas externas e/ou internas. [...]Servidores, aplicações *web* e bancos de dados são as três principais áreas de foco para testes de penetração automatizados. [...]Apenas 29% das organizações automatizaram 70% ou mais de seus testes de segurança. [...]44% incluíram testes e revisões de segurança como parte dos fluxos de trabalho de codificação.

Com tantas brechas de segurança encontradas *Internet* afora, que causam prejuízos financeiros a tantas empresas, e que afetam também a integridade emocional das pessoas, porque quando um invasor quando consegue ter acesso a um sistema e vaza as informações que nele estão, a privacidade das pessoas que detinham informações pessoais nela são expostas, se tornando alvos de golpes e humilhações.

Pelos motivos expostos, justifica-se a importância desta pesquisa, porque, ter métodos que ajudem a melhorar as defesas de redes e serviços se torna ainda mais

essencial com o crescimento da tecnologia pelo mundo. O conhecimento em testes de invasão é uma das ferramentas para aprimorar a cibersegurança. Empresas poderão aprender, com os resultados obtidos nas tentativas de invasão da rede e dos seus serviços, aplicando métodos, para reduzir as vulnerabilidades encontradas.

II LEVANTAMENTO TEÓRICO

As redes com o passar dos tempos foram se tornando muito complexas, com muitos dispositivos começando a fazer parte delas, com isto, o conhecimento necessário para aumentar as defesas foram cada vez se tornando maior, não sendo apenas um profissional responsável por toda ela, pois da primeira camada do modelo OSI até a última existem brechas que precisam ser observadas individualmente por equipes especializadas (Santos, 2019).

Na camada de enlace e de redes, fica como responsável a equipe de infraestrutura, que uma empresa irá designar para implementar configurações nos seus roteadores e *switchs*, que irão servir como barreiras, impedindo ataques, conexões indesejadas e negar o acesso a usuários não autorizados, um exemplo disto são as ACLs, implementadas em roteadores, que podem impedir conexões de determinados IPs, ou de determinados protocolos (Cisco, 2019).

Uma equipe especializada em softwares, como antivírus, configurações de *firewalls* e ferramentas de escaneamento de redes irão utilizar seus conhecimentos e mecanismos para encontrar as vulnerabilidades que há na rede em que estão operando, ao encontrar alguma, irão procurar métodos para mitigá-las ou se conseguirem, eliminá-las. Sendo criando regras que limitem acessos, ou manipulando ferramentas de escaneamento em uma rede, o usuário precisa estar em constante aprendizado, pois a área de Tecnologia da Informação (TI) como um todo, está sempre se atualizando e evoluindo rapidamente, trazendo também junto novos desafios para os profissionais de Segurança da Informação, sendo estes desafios, novas vulnerabilidades, *exploits*, softwares maliciosos, entre diversos caminhos que um invasor têm para alcançar seus objetivos (Gazola, 2021).

Os testes de penetração é uma parte principal na evolução da maturidade de uma empresa em relação a sua segurança cibernética (Raidbr, 2023), o objetivo dos *pentests* é identificar vulnerabilidades em sistemas e redes para que possam ser corrigidas antes que sejam exploradas por hackers mal-intencionados. Para se tornar um *pentester*, é necessário ter habilidades em testes de penetração, avaliação de vulnerabilidades e técnicas de *hacking* ético (invasores de sistemas que o fazem com objetivos de descobrir vulnerabilidades e reportá-las, sem intenções de causar danos e lucrar por meios ilegais), além de experiência em segurança cibernética.

Uma maneira de adquirir essas habilidades e conhecimentos é através de certificações em segurança cibernética. Existem várias certificações que podem ser úteis para aqueles que desejam se tornar *pentesters*, cada uma com seu próprio foco e objetivos, alguns exemplos são a CEH ANSI (*Certified Ethical Hacker*), CEH Practical (*Certied Ethical Hacker Practical*), ECSA (*Security Analyst*) e entre outras (Antonio, 2022).

2.1 Segurança da Informação

A Segurança da Informação é a área da Tecnologia da Informação que foca em manter as informações que estão armazenadas ou em transição nas redes de computadores protegidas, ou seja, que elas possam ser utilizadas da maneira que é esperado, da maneira que elas foram originalmente planejadas para serem, sem intervenções de usuário não autorizados, sem serem destruídas ou modificadas.

Para que a Segurança da Informação consiga seus objetivos, é preciso implementar políticas, documentos que nele estão descritos as regras que os colaboradores de uma organização devem seguir e como informações de importância devem ser tratadas, sendo também necessário que esteja neste documento o modo como implementar estas decisões, que primeiro precisam da autorização da alta gerência antes de serem postas em prática, pois uma empresa precisa atingir os objetivos que ela mesmo propõe, também restrições físicas, que é a de proibir pessoas não autorizadas de entrar em partes da empresa em que estão documentos e servidores, e por último, fazer campanhas de boas práticas, incentivando os colaboradores a seguir recomendações de segurança, como a de não compartilhar suas senhas, fazer *backup* de suas informações, utilizar senhas fortes e não repeti-las entre outras boas práticas (Apeti, 2023).

Para que a Segurança da Informação consiga fazer com que haja esta proteção, ela segue seis pilares, que se cumprido todos eles, a confiança no processo em que a informação faz parte é aumentada (Pedra, 2023).

2.1.1 Confidencialidade

A propriedade da confidencialidade é uma consideração prévia à discussão tecnológica, sendo observada historicamente na sociedade. A preocupação em preservar informações importantes de acesso por outros indivíduos é inerente, especialmente quando há segredos que revelam dados pessoais e sensíveis sobre uma pessoa, nesse contexto, é necessário manter tais informações em confidencialidade.

Em computadores isto se dá também, empresas mantém em seus bancos de dados diversas informações pessoais de clientes e funcionários, em que, hipótese alguma pode ser exposto, sendo necessários utilizar maneiras para mantê-las em total confidencialidade.

A primeira etapa para se garantir a confidencialidade é a de abordar informações que exijam confidencialidade de uma maneira diferente de outras, se questionando se elas são inicialmente necessárias serem armazenadas, pois ter que gerar um grande esforço para se proteger algo que não é de fato essencial é perda de tempo e dinheiro. A outra etapa é a de utilizar ferramentas para restringir acesso ao valioso, como por exemplo *firewalls*, que irão limitar acessos a usuários não autorizados, como também a criptografia, que mesmo que haja um vazamento, os dados estarão criptografados (Kurose, 2013).

Kurose (2013) em seu livro “Redes de Computadores: Uma Abordagem Top-Down”, apresenta a definição de confidencialidade:

> Confidencialidade. Apenas o remetente e o destinatário pretendido devem poder entender o conteúdo da mensagem transmitida. O fato de intrusos conseguirem interceptar a mensagem exige, necessariamente, que esta seja cifrada de alguma maneira para impedir que seja entendida por um interceptador. Esse aspecto de confidencialidade é, provavelmente, o significado mais comumente percebido na expressão comunicação segura. Estudaremos técnicas de criptografia para cifrar e decifrar dados.

2.1.2 Integridade

A integridade refere-se à garantia de que os dados não foram corrompidos ou modificados de forma não autorizada durante a transmissão ou armazenamento.

Em contextos de redes de computadores, a integridade é um dos princípios-chave de segurança e é fundamental para garantir que os dados permaneçam inalterados desde a origem até o destino. Para proteger a integridade dos dados, várias técnicas e mecanismos de segurança, como criptografia e verificação de integridade (hashes), são frequentemente utilizados. Além disso, a integridade dos dados também está relacionada ao controle de acesso, que garante que apenas entidades autorizadas possam modificar os dados (Kurose, 2013).

Kurose (2013) em seu livro “Redes de Computadores: Uma Abordagem Top-Down”, apresenta uma analogia para se entender integridade:

> Integridade de mensagem. Alice e Bob querem assegurar que o conteúdo de sua comunicação não seja alterado, por acidente ou por má intenção, durante a transmissão. Extensões das técnicas de soma de verificação que encontramos em protocolos de transporte e de enlace confiáveis podem ser utilizadas para proporcionar integridade à mensagem.

2.1.3 Disponibilidade

A disponibilidade é um dos princípios-chave da cibersegurança e se concentra na garantia de que os sistemas, recursos e serviços de uma rede de computadores estão prontamente acessíveis e operacionais quando necessário. Isso significa que os usuários devem poder confiar na disponibilidade contínua de recursos, sem interrupções não planejadas.

Para garantir a disponibilidade, são implementadas várias práticas e estratégias. Isso inclui a redundância de componentes críticos, como servidores e links de rede, de modo que, em caso de falha, os sistemas alternativos possam assumir a operação. Além disso, o monitoramento constante da rede é vital para identificar rapidamente problemas e falhas, permitindo uma resposta imediata.

Além disso, a disponibilidade também está relacionada à segurança cibernética. Medidas de segurança, como *firewalls*, sistemas de detecção de intrusões e autenticação forte, são usadas para proteger os sistemas contra os ataques que poderiam afetar a disponibilidade. Em caso de incidentes de segurança, é importante ter planos de resposta a incidentes para minimizar o impacto na disponibilidade dos recursos.

Além disso, os planos de recuperação de desastres são desenvolvidos para restaurar a disponibilidade em caso de eventos graves, como desastres naturais ou falhas catastróficas. Esses planos podem envolver cópias de segurança de dados, sistemas de espelhamento e outros mecanismos de recuperação (Kurose, 2013).

2.1.4 Autenticidade

A autenticidade no contexto de tecnologia é a propriedade que uma informação consiga provar ser realmente o que ela é, quando ela está sendo transportada, precisa chegar em seu destino da mesma maneira em que ela foi enviada, não sendo confundida com outra, permanecendo com mesmo conteúdo, pois se em um ataque, um atacante conseguir interceptar determinada mensagem, ele pode modificar o conteúdo dela, não sendo mais a mensagem original, também a mensagem precisa ter um prazo de validade, quando expirado, não se torna mais válido (Alves, 2019).

Uma maneira de certificar que uma mensagem é autêntica é utilizando o *hash*, um processo que transforma diversos dados em uma linha de alguns caracteres, em que qualquer mudança no conteúdo original, mesmo que seja um bit, fará que o *hash* será diferente, não sendo possível gerar *hashes* iguais, assim, é possível sempre que um documento é finalizado, se gera um *hash*, para que quando for transportado para outro computador, faça a comparação do *hash* emitido originalmente com o que será feito na máquina que recebeu o arquivo, comprovando ser o mesmo (Donohue, 2014).

O certificado digital é outra forma em que se garante a autenticidade, em páginas *web* podemos localizar no canto superior esquerdo o comprovante de que o *site* em questão é verdadeiramente o mesmo quem ele se diz ser, pois, há um determinado tipo de golpe realizado por agentes maliciosos que desenvolvem *sites* que são idênticos a de uma outra página, por exemplo a de um banco, assim o usuário despercebido, insere seus dados em um formulário que envia esta informação de extrema importância para "mãos erradas", sendo assim é fundamental verificarmos se uma página emite um certificado válido.

Os certificados também são utilizados para carimbar um documento, provando que ele é autêntico, a maneira que as ferramentas de autenticidade funcionam é composta por várias etapas, a principal delas é emissão de chaves públicas e privadas, que são utilizadas para codificar e decodificar o arquivo, para que dois lados

possam compartilhar arquivos de forma segura, é preciso que tenham um par de chaves de cada lado (Pereira, 2014).

2.1.5 Legalidade

No que se diz a legalidade na Segurança da Informação, é o estado que uma empresa se encontra em que ela esteja cumprindo as leis vigentes no seu presente momento referentes a dados pessoais, fazendo isto para que não sofra punições dos órgãos reguladores, que fiscalizam as empresas em busca daquelas que tratam os dados pessoais de funcionários, clientes e fornecedores de maneira incorreta, sendo assim, é necessário que as empresas analisem as leis atualmente vigentes e faça planos para se enquadrar nelas (Guedes, 2020).

A Lei Carolina Dieckmann (12.737/2012) é a lei que aborda questões sobre a invasão de dispositivos, nela está previsto que acessar computadores ou celulares alheios sem a permissão dos donos é crime, sendo assim, é importante que os *pentesters* garantam que antes de iniciar seus testes, seja aprovado pelos proprietários que o teste ocorra, assim não ocorrendo nenhuma irregularidade (Fachini, 2023).

A Lei Geral de Proteção de Dados (LGPD), é a lei que vigora no Brasil, ela é a que diz a maneira que as empresas precisam tratar os dados pessoais que ela armazena, é nesta hora em que todo o investimento que uma empresa aplica em defesa cibernética é recompensado, pois, se uma empresa que não acata os regulamentos da LGPD, ou quando determinado ataque acontece e um vazamento das informações ocorre, os órgãos regulamentadores irão puni-la com multas que podem chegar até 50 milhões de reais, entre outras punições (Donda, 2020).

2.1.6 Irretratabilidade

A irretratabilidade, também conhecida como não repúdio, é o conceito que é preciso que uma informação quando enviada precisa ter uma maneira de confirmar qual a sua origem, podendo saber qual o dono daquela informação, para que em um

caso de ilegalidade, os proprietários da informação não consigam negar ter vindo deles, assim sendo possível serem julgados e punidos.

A maneira de se atingi-la é com a junção de métodos de integridade e autenticidade, utilizando uma assinatura digital, será registrado o autor de determinada mensagem, a partir de algoritmos de *hash,* juntamente com criptografia utilizando chaves assimétricas, será preservado a autoria dela, fazendo com que se não seja possível negar a origem dela (Oliveira, 2023).

2.2 Algumas ameaças e suas vulnerabilidades em sistemas Linux

A *Internet* está repleta de ameaças, *softwares* maliciosos e invasores, tentando a todo tempo explorar vulnerabilidades, que são brechas de segurança existentes em programas e sistemas, que quando conseguem, causam prejuízos a empresas e pessoas, há diversos *scripts* já desenvolvidos, fáceis de serem utilizados por pessoas que não tem conhecimento técnico, disponíveis a qualquer um, que conseguem infectar máquinas e danificá-las, criptografando seus dados, corrompendo-os ou utilizando seu processamento para outros fins.

A lista de vulnerabilidades que podem ser exploradas é imensa, sendo que todos os dias se descobre uma nova, a questão do mundo tecnológico em que vivemos é a de que precisamos estar prontos para ataques, principalmente minimizar os danos, pois a chance de nenhum ataque ter sucesso durante diversos anos em que uma empresa atua é muito pequeno (Fraga, 2019).

Segundo Santos (2015), em seu artigo intitulado “Análise de vulnerabilidade em rede, com teste de intrusão, utilizando a distribuição Kali Linux”, citas os três tipos de vulnerabilidades que podem ser exploradas:

> Muitos e diferentes são os caminhos que podem ser utilizados pelos adversários para invadir um sistema de uma organização. Cada vulnerabilidade é uma fraqueza e permite que o invasor obtenha informações de determinado sistema. Sendo elas:
>
> - Erros de programação – Grande parte das vulnerabilidades surge do erro de tamanho do *buffer*, uma região da memória reservada para escrita e leitura dos dados.
> - Configuração inadequada – Aplicativos de segurança como o *firewall*, devem ser corretamente

configurados, ou podem ser brechas para ataques maliciosos.
- Falha humana – Execução de arquivos maliciosos manualmente.

No quadro 1 é possível ver as vulnerabilidades que foram encontradas no teste prático que será apresentado mais adiante e suas explicações.

Quadro 1 - Vulnerabilidades encontradas no teste prático

Portas abertas	Máquinas Linux que não possuem um *firewall* configurado podem estar correndo um grande risco de serem atacadas, pois, por deixarem as portas de serviços que não estão sendo utilizadas abertas, atacantes podem explorar este descuido para danificá-la ou acessá-la.
Senhas fracas	É preciso que sempre ao cadastrar um usuário em qualquer sistema, seja colocado uma senha de acesso que tenha diversos caracteres diferentes, utilizando com por exemplo letras maiúsculas e minúsculas, caracteres especiais e números.
Sobrecarga de recurso	Além de fechar as portas de serviços que não estão sendo utilizadas, é preciso proteger as que estão sendo utilizadas, se um servidor *web* está hospedando uma página, é preciso bloquear que ela receba pacotes ICMP.

Fonte: Autoria própria (2023)

2.3 Algumas ferramentas e técnicas que podem ser utilizadas no *pentest*

Existem diversas ferramentas utilizadas em "*pentest*", elas têm como objetivo trazer informações ou servir como maneira de se ter acesso a um sistema, elas são

utilizadas juntas para se conseguir atingir os objetivos de um *pentester* (Profissionais TI, 2020).

No quadro 2 é possível ver as ferramentas que foram utilizadas no teste prático que será mostrado mais adiante juntamente com suas explicações.

Quadro 2 - Ferramentas utilizadas no teste prático

Nmap	O Nmap é uma ferramenta utilizada para se escanear uma rede, conseguindo descobrir quais computadores estão nela, os seus endereços e se há portas de serviços abertas nesses *hosts,* sendo ele disponível no Kali Linux por padrão (Profissionais TI, 2020).
Hydra	O Hydra é uma ferramenta de força bruta, ou seja, ela tem como objetivo fazer diversas tentativas até conseguir ter acesso a um sistema, no método de tentativa e erro, ele pode fazer isto contra diversos protocolos, como FTP, HTTP, HTTP, SMB e entre outros, sendo ele disponível no Kali Linux por padrão (Shivanandhan, 2022).
Slowhttptest	*Slowhttptest* é um tipo de ferramenta de ataque de negação de serviço que permite que uma única máquina derrube o servidor *web* de outra máquina com largura de banda mínima e efeitos colaterais em serviços e portas não relacionados, ela é uma ferramenta que já é disponível no Kali Linux por padrão.

Fonte: Autoria própria (2023)

Keshri (2021), em sua publicação intitulada "*Top 5 Penetration Testing Methodologies and Standards*", no site "Astra", postada em 15 de setembro de 2021, é apresentado um *ranking* das metodologias de testes de penetração que ela acha serem as melhores e mais completas, ou seja, as que melhor conseguem trazer o caminho para se realizar todo o processo da invasão e documentação dos resultados.

As metodologias do *pentest* são guias para se conseguir ter um melhor direcionamentos quando se deseja implementá-lo, com caminhos que já foram testados e avaliados, sendo assim, não sendo necessário desenvolver uma maneira nova do zero, pois já existem diversas que podem em muito, facilitar no processo de coletar e documentar as fraquezas tecnológicas que cercam uma rede.

No quadro 3 é possível ver algumas metodologias que *pentesters* podem utilizar para guiá-los ao iniciar um *pentest*, como também suas explicações e do que consistem.

Quadro 3 - Metodologias que podem ser utilizadas no *pentest*

***Open Source Security Testing Methodology Manual* (OSSTMM)**	A OSSTMM define um conjunto de práticas para a realização de testes de penetração em redes, servidores e aplicativos. Ela é considerada uma das metodologias mais completas e abrangentes em termos de avaliação de segurança.
***Penetration Testing Execution Standard* (PTES)**	A PTES é uma metodologia de *pentest* que consiste em 7 fases: pré-engajamento, inteligência de ameaças, análise de vulnerabilidades, exploração, pós-exploração, relatórios e encerramento.
***Information Systems Security Assessment Framework* (ISSAF)**	ISSAF é uma metodologia de *pentest* que envolve a coleta de informações, análise de vulnerabilidades, exploração de vulnerabilidades e pós-exploração.

Fonte: Autoria própria (2023)

III TESTE PRÁTICO

Kali (2023), em seu site oficial, demonstra as capacidades que seu sistema operacional é capaz de proporcionar, as diversas maneiras que ele pode ser utilizado, como aprender mais sobre ele, suas ferramentas e sendo ainda o melhor de tudo, que o Kali Linux é uma distribuição gratuita, ele será a parte principal do teste prático, a base de todo o processo, pois nele contém todas as ferramentas que precisam para fazer os ataques.

3.1 Desenvolvimento

A construção de um teste de invasão se inicia com a preparação do ambiente, os invasores utilizam diversas ferramentas e técnicas para se ganhar acesso ou danificar redes ou serviços, sendo a primeira delas o sistema operacional Kali Linux, uma distribuição dos sistemas operacionais GNU/Linux baseada em Debian desenvolvido e mantido pela *Offensive Security Ltd*, especializada em teste de penetração, pesquisa de segurança, computação forense e engenharia reversa, com ele se torna muito mais fácil de se praticar técnicas relacionadas à cibersegurança, pois por padrão o Kali já possui diversos softwares de coleta de informações, análise de vulnerabilidades, análise de aplicações *web*, avaliação de *database*, ataque de força bruta, ataque à redes sem fio, engenharia reversa, ferramentas de *exploitation*, *Sniffing & Spoofing*, post *exploitation*, forense e engenharia social.

O Kali Linux pode ser utilizado em diversas formas, por ser um sistema operacional versátil e leve, é possível utilizar um *bootable pendrive* com o Kali instalado nele e iniciá-lo antes do sistema operacional que está na máquina, sendo muito útil para investigações forenses, pois quando se deseja extrair as informações que existem na memória de um computador, é preciso tomar as devidas precauções, porque é muito provável que se existe informações valiosas e comprometedoras em um disco rígido, há também ferramentas para protegê-lo de acessos não autorizados, como encriptação de seus dados, por este motivo, o Kali oferece suas ferramentas de forense que podem ajudar a manipular a memória de um computador.

Fraga (2019), apresenta maneiras de se ter privacidade no ambiente em que estão sendo realizados os testes de invasão, utilizando o navegador Tor, *proxychains* e uma VPN, ele também explica como utilizar estas ferramentas no Kali.

3.2 Aprovação do teste

A segunda etapa para a construção do ambiente é de ter a aprovação para se iniciar o teste, porque como foi dito anteriormente, está determinado nas leis que escanear redes e acessar informações de outras pessoas é crime, portanto, sempre antes de se escanear uma rede e testar as ferramentas nelas, é preciso ter a aprovação de seu dono, para que não ocorra nenhuma irregularidade.

Quando um *pentester* é chamado por uma empresa para realizar os testes de invasão é necessário que ele crie o roteiro dos testes, quais ferramentas serão utilizadas, o escopo entre outras especificações, isso, juntamente com os profissionais de tecnologia da informação da empresa, ao final, será levado a alta gerência para que seja aprovado, assim podendo iniciar a procura pelas vulnerabilidades.

É importante também definir qual será o tipo de teste de penetração que será utilizado, pois há diversos deles, alguns não é dado nenhuma informação ao invasor sobre a rede, outros, o invasor recebe as informações para que facilite a procura pelas fraquezas (Writer, 2023).

3.3 Documentar as descobertas

A terceira etapa é a de tomar notas de todas as informações adquiridas nos testes, sendo a parte mais importante de todo o processo do *pentest*, pois o objetivo desta prática é a de solucionar os problemas que foram encontrados, os clientes que requisitam uma invasão controlada em sua rede esperam que ao final dela, seja apresentado as falhas para que haja um plano de melhoria e de aperfeiçoamento das ferramentas de defesa, como por exemplo, se durante o teste de penetração for realizado um escaneamento na rede e fossem encontradas portas de serviços abertas, o *pentester* iria gerar anotações sobre quais são elas e suas especificações, a partir disto, outro grupo seria responsável por trazer soluções para esta falha

encontrada, podendo ser a de fechar estas portas ou protegê-las de acessos não autorizados, como por exemplo implementando um *firewall* nesta rede.

3.4 Cenário prático

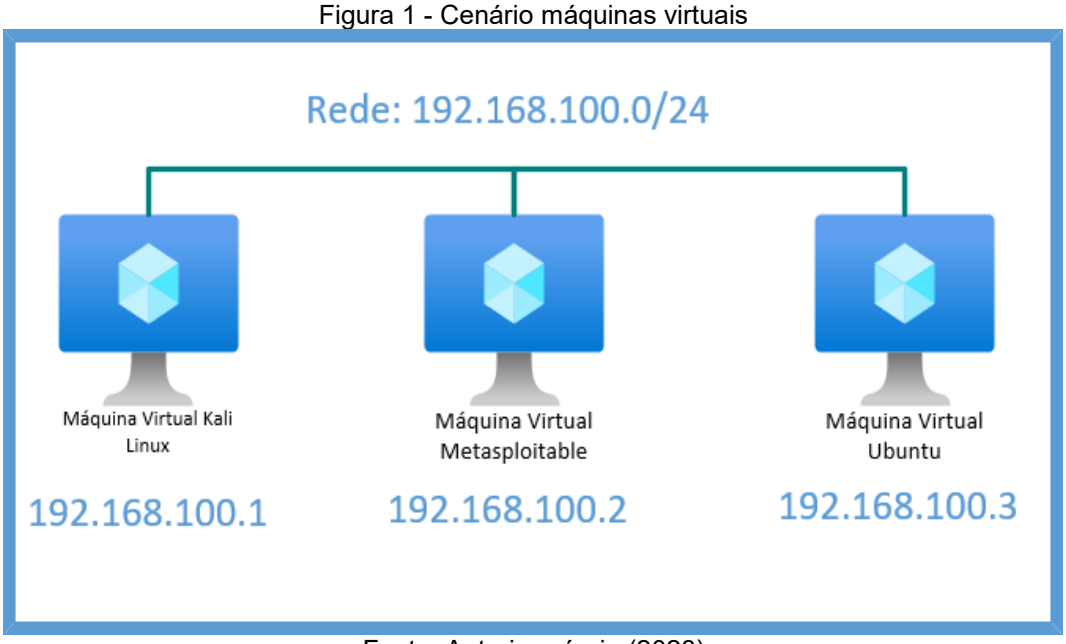
Foi desenvolvido um cenário formado por três máquinas virtuais utilizando o programa de virtualização VirtualBox da Oracle (Oracle, 2023), a máquina Metasploitable (Rapid7user, 2019) que será atacada, máquina Kali (Kali, 2023) que será utilizada para fazer o ataque e uma máquina Ubuntu (Ubuntu, 2023) que será utilizada para acessar os serviços da Metasploitable.

As duas máquinas estão se comunicando na mesma rede, utilizando a configuração de rede interna nas placas de rede de ambos, em um cenário real seria como se dois computadores estivessem conectados com o cabo de rede à um *switch,* as máquinas não têm acesso à *Internet*, mas para que seja possível instalar os requisitos necessários para o teste e a mitigação, será utilizado um segundo adaptador de rede em modo NAT, apenas para instalar os pacotes e logo depois será desativado.

Para fins práticos e acadêmicos, todas as vulnerabilidades da máquina que será invadida já são conhecidas, sendo assim, o cenário foi criado para que os testes fossem objetivos e funcionassem, para que fosse possível entender como o sistema funciona e como utilizar as ferramentas.

Na Figura 1 é apresentada a máquina Kali que possui endereço IP 192.168.100.1, a Metasploitable que possui o endereço 192.168.100.2 e a Ubuntu possui o endereço 192.168.100.3, todos os IPs foram inseridos manualmente, estando na mesma rede.

Figura 1 - Cenário máquinas virtuais



Fonte: Autoria própria (2023)

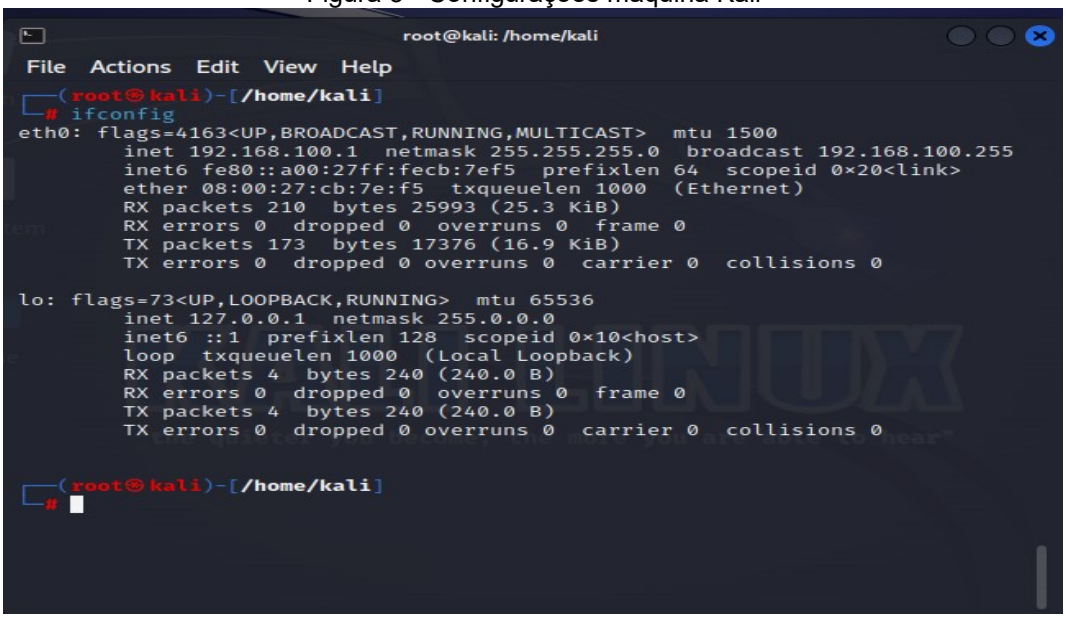
Na Figura 2 é possível ver a interface gráfica do Kali Linux.

Figura 2 - Desktop Kali

Fonte: Autoria própria (2023)

Na Figura 3 é possível ver o comando “*ifconfig*”, que é utilizado para mostrar as placas de rede da máquina, a eth0 e a *loopback.*

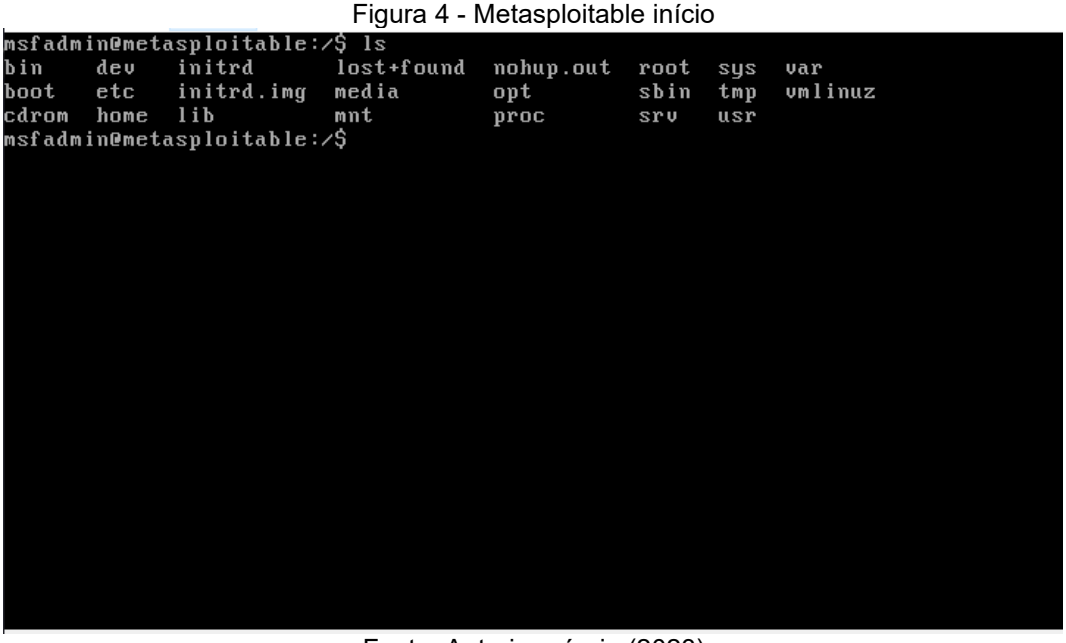
Figura 3 - Configurações máquina Kali



Fonte: Autoria própria (2023)

Na Figura 4 é possível ver o terminal da máquina Metasploitable, as distribuições Linux são comumente utilizadas pelos usuários direto do seu terminal, onde são inseridos os comandos, tendo assim um controle total do sistema operacional, como por exemplo, o “ls” visto na figura, com ele é possível mostrar arquivos e diretórios.

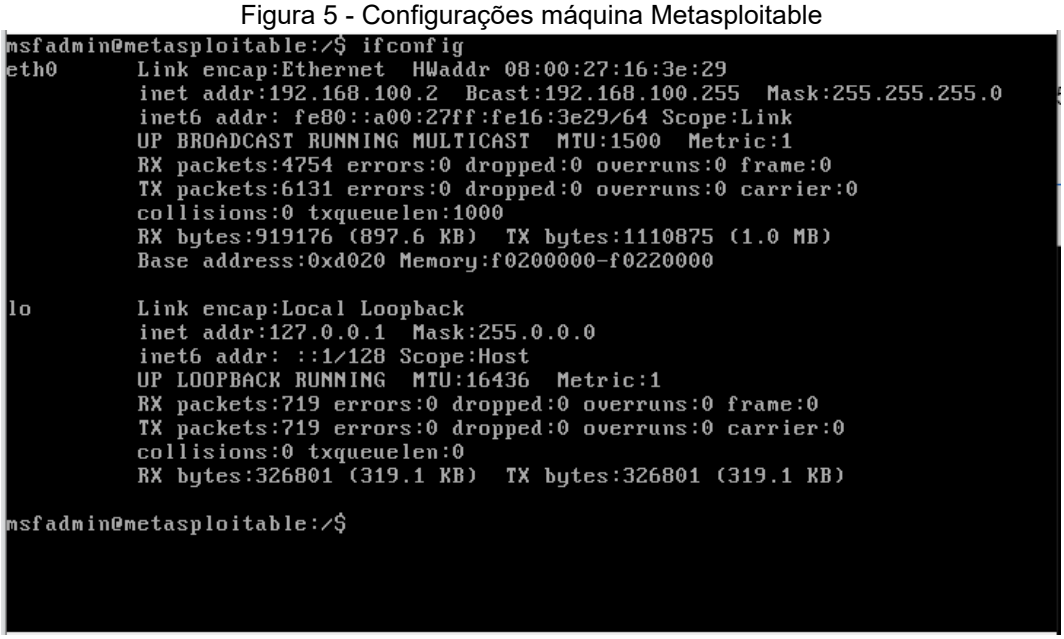
Figura 4 - Metasploitable início



Fonte: Autoria própria (2023)

Na Figura 5 é possível ver que com o comando “*ifconfig*” são mostradas as placas de rede da máquina Metasploitable também.

Figura 5 - Configurações máquina Metasploitable



Fonte: Autoria própria (2023)

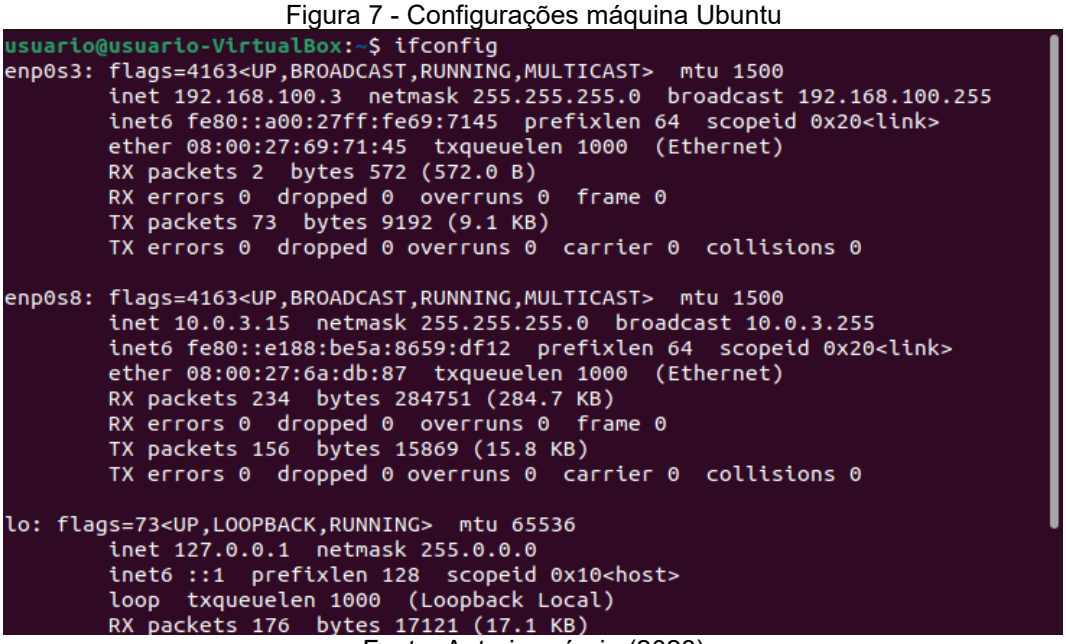
Na Figura 6 é possível ver a interface gráfica do Ubuntu.

Figura 6 - Desktop Ubuntu

Fonte: Autoria própria (2023)

Na Figura 7 é possível ver que com o comando “*ifconfig*” são mostradas as placas de rede da máquina Ubuntu também.

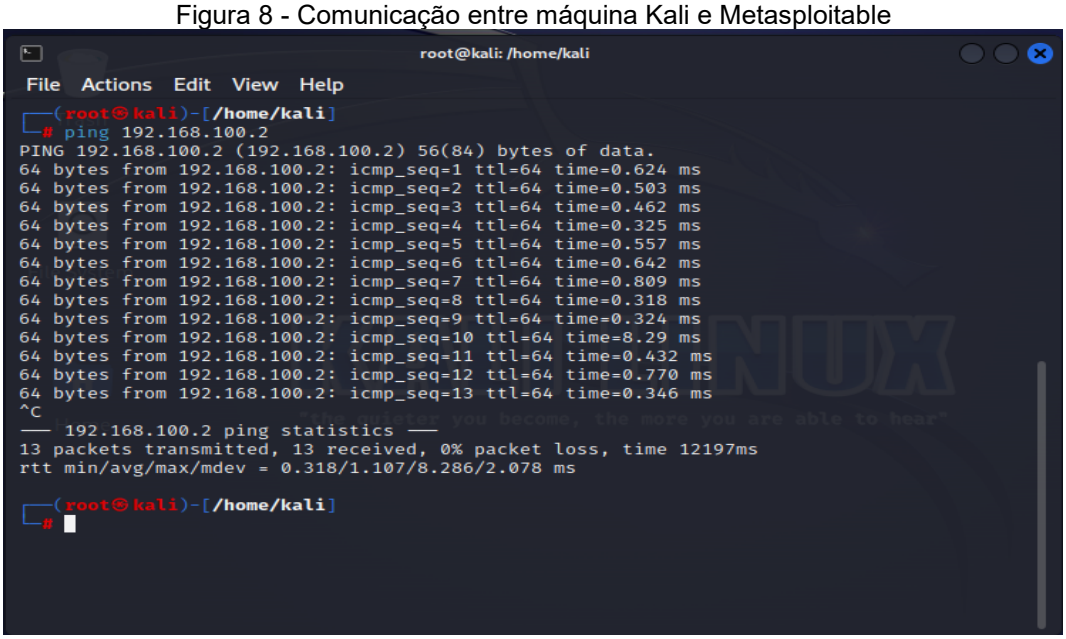
Figura 7 - Configurações máquina Ubuntu



Fonte: Autoria própria (2023)

Na Figura 8 é possível ver que utilizando o comando "*ping*" tendo como alvo o IP da máquina vizinha Metasploitable, há um retorno das mensagens enviadas, nos revelando haver comunicação entre ambas.

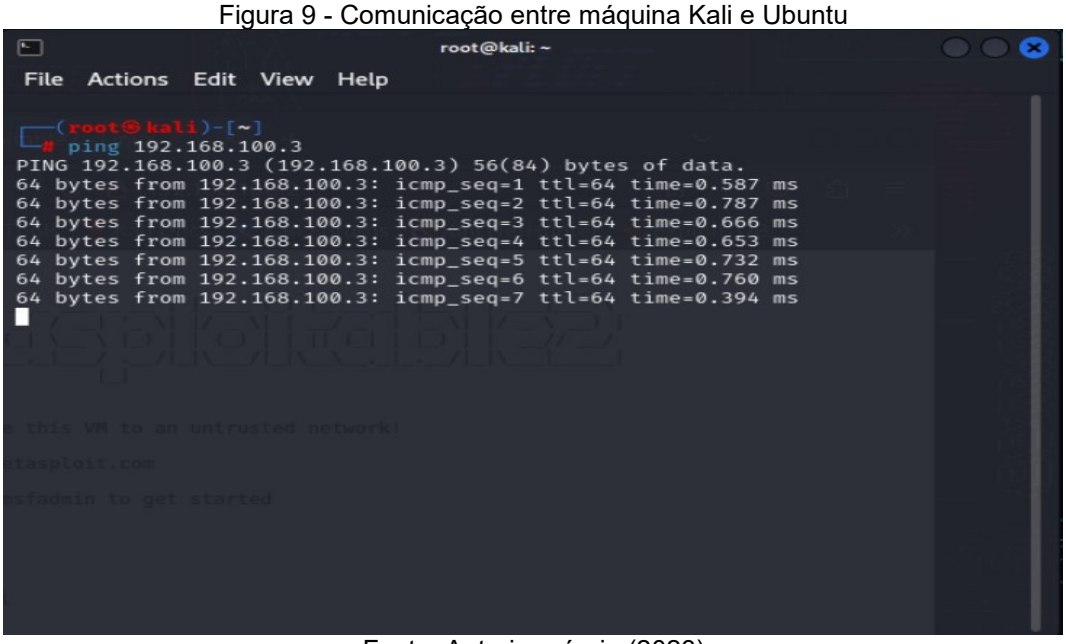
Figura 8 - Comunicação entre máquina Kali e Metasploitable



Fonte: Autoria própria (2023)

Na Figura 9 é possível ver que utilizando o comando "*ping*" tendo como alvo o IP da máquina vizinha Ubuntu, há um retorno das mensagens enviadas, nos revelando haver comunicação entre ambas.

Figura 9 - Comunicação entre máquina Kali e Ubuntu



Fonte: Autoria própria (2023)

3.5 Testes para localizar as vulnerabilidades

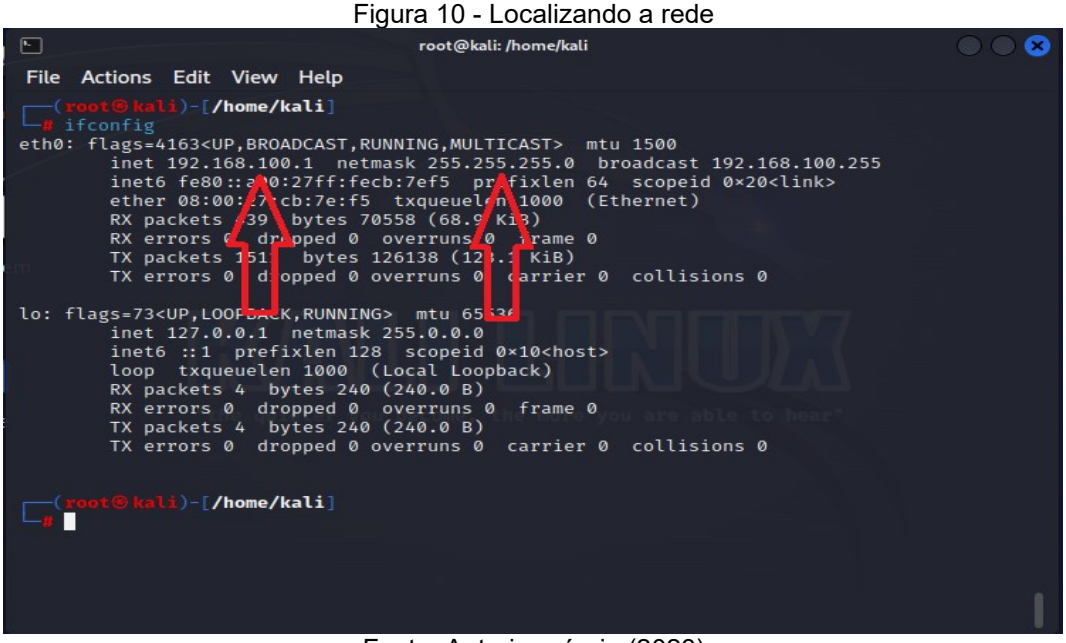
Foram realizados testes e ataques a partir da máquina Kali com o alvo na Metasploitable, localizando suas vulnerabilidades e as explorando, com o intuito de, após o teste, solucioná-las.

3.5.1 Nmap

O Nmap é uma ferramenta que é utilizada para escanear redes, utilizando-o, é possível descobrir quais máquinas estão conectadas na mesma rede, seus IPs e suas portas.

Na Figura 10 é utilizado o “*ifconfig”*, com isto, é descoberto em qual rede a máquina atacante está, para que seja feita a varredura.

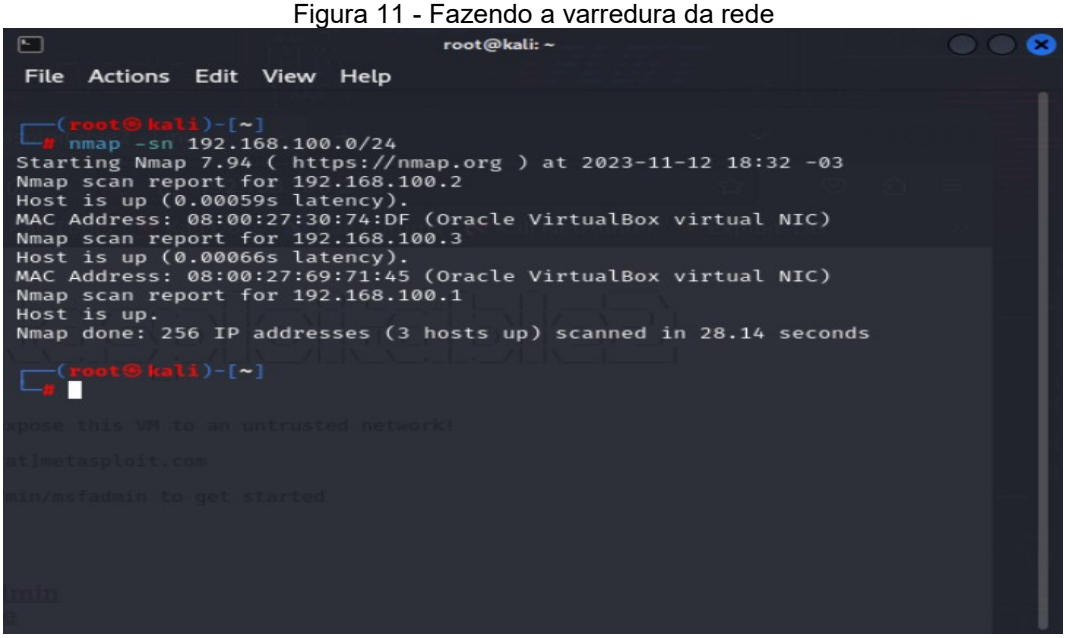
Figura 10 - Localizando a rede



Fonte: Autoria própria (2023)

Na Figura 11 é possível ver o comando do Nmap utilizado para fazer uma varredura da rede, “-sn” significando *Scan Network,* ou seja, escanear a rede, com isto temos o resultado de três IPs, o da máquina atual Kali e de mais duas máquinas que foram descobertas nesta rede, a do IP 192.168.100.2 e a do IP 192.168.100.3.

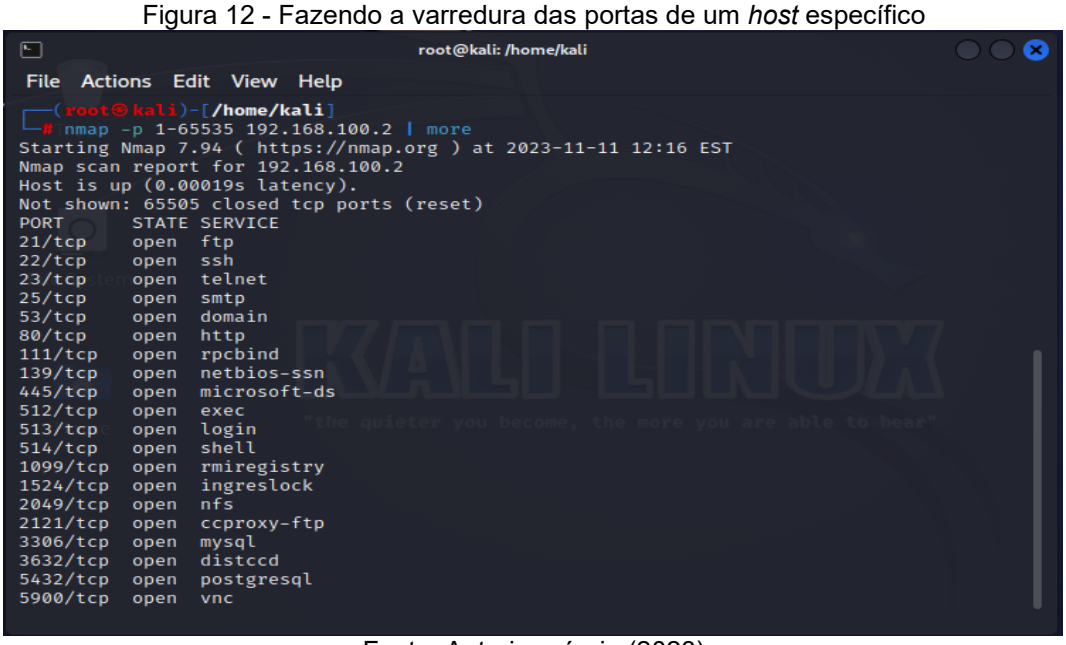
Figura 11 - Fazendo a varredura da rede



Fonte: Autoria própria (2023)

Na Figura 12 se consegue ver que é utilizado o comando do Nmap para escanear as portas de um IP específico, sendo este IP o que foi descoberto na varredura anterior, o “-p” é utilizado para escolher quais portas serão escaneadas, indo da 1 até a 65535 (que é o limite de portas existentes), é incrementado ao comando o “| more”, pois a quantidade de portas abertas eram muitas, assim com este comando não são mostradas todas, finalizado o processo, é mostrado na tela as portas de serviço TCP/UDP que estão abertas e podem ser exploradas.

Figura 12 - Fazendo a varredura das portas de um *host* específico



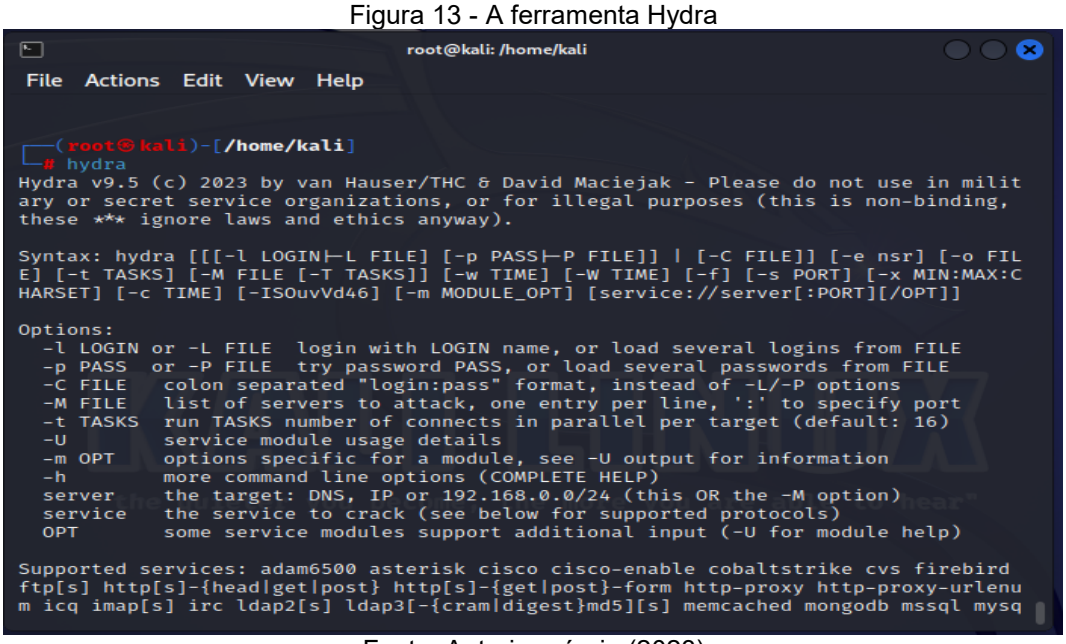
Fonte: Autoria própria (2023)

3.5.2 Hydra

Hydra é uma ferramenta que pode ser utilizada para fazer força bruta em *Secure Socket Shell* (SSH), isto é, ela vai tentar diversos possíveis usuários e diversas possíveis senhas para se conectar remotamente a outra máquina que está na rede, pois não sabendo as credenciais, é necessário fazer um processo de tentativa e erro, até que se consiga o acesso.

Na Figura 13 é possível ver as possibilidades do Hydra, uma ferramenta que está disponível por padrão no Kali, digitando “hydra“ no terminal, é possível ver as opções disponíveis que podem ser utilizadas.

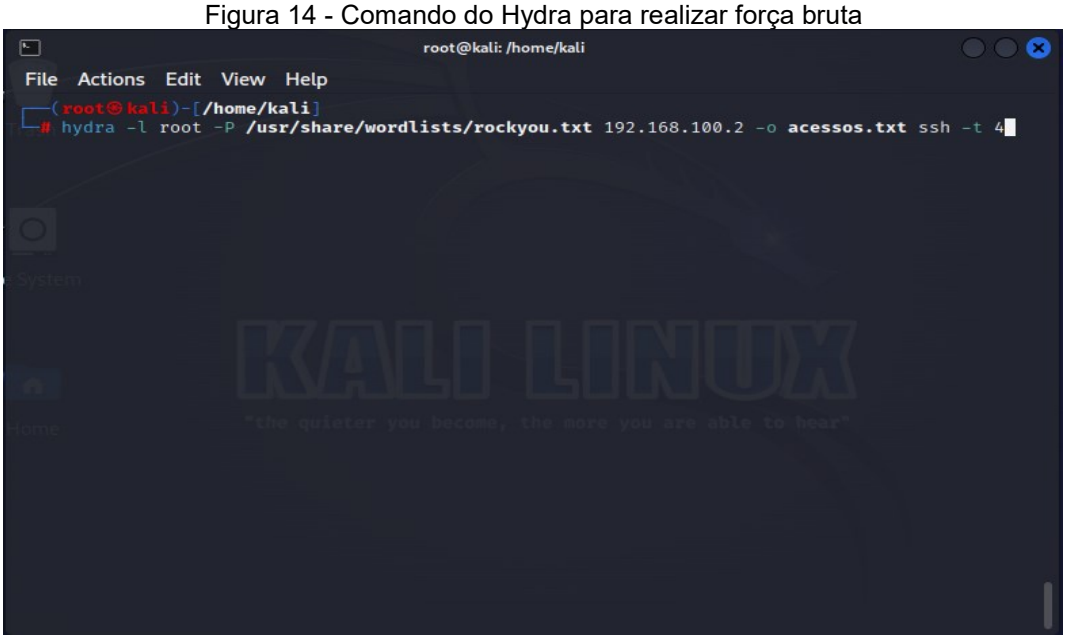
Figura 13 - A ferramenta Hydra



Fonte: Autoria própria (2023)

Na Figura 14 é possível ver o comando da ferramenta Hydra para se fazer força bruta em SSH e os seus parâmetros.

Figura 14 - Comando do Hydra para realizar força bruta



Fonte: Autoria própria (2023)

No quadro 4 é possível ver os parâmetros utilizados para se fazer o ataque de força bruta.

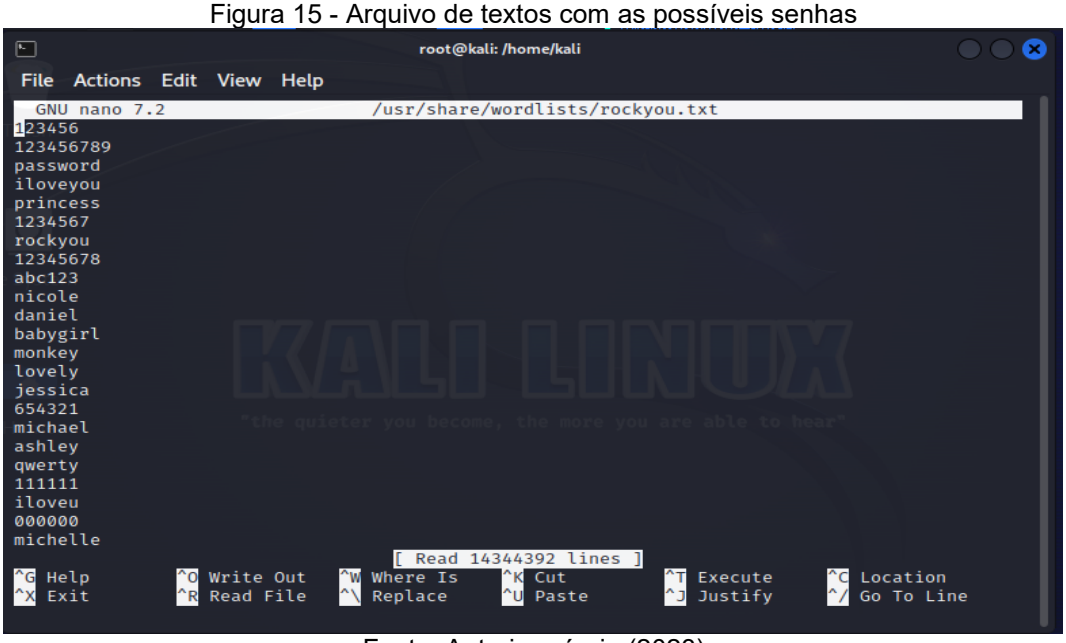
Quadro 4 - Opções de parâmetros para o ataque de força bruta

-l root	Com este comando é possível escolher um usuário que será utilizado para se tentar adivinhar a sua senha, o usuário *root* é comum em sistemas Linux, por este motivo, a chance de que tenha um usuário com este nome é grande.
-P /usr/share/wordlists/rockyou.txt	Com este comando é possível escolher um arquivo que será utilizado para tentar as possíveis senhas, o Hydra por padrão disponibiliza um arquivo de textos com diversas senhas que são comuns de serem utilizadas.
192.168.100.2	Como alvo será colocado o IP que foi descoberto na varredura do Nmap.
-o acessos.txt	Com este comando é possível direcionar para um arquivo o resultado de sucesso do ataque, se ele conseguir acertar o usuário e senha, será escrito no “acessos.txt” as credenciais corretas.
ssh -t 4	Com este comando é que se escolhe qual serviço será atacado e a quantidade de *tasks* máximas.

Fonte: Autoria própria (2023)

Na Figura 15 é possível as diversas senhas que estão armazenadas no arquivo de texto “*rockyou.txt*”, essas senhas podem ser encontradas em diversos locais da *Internet*, sendo utilizadas pelas pessoas por serem fáceis de serem lembradas, mas sendo vulneráveis a ataques de força bruta.

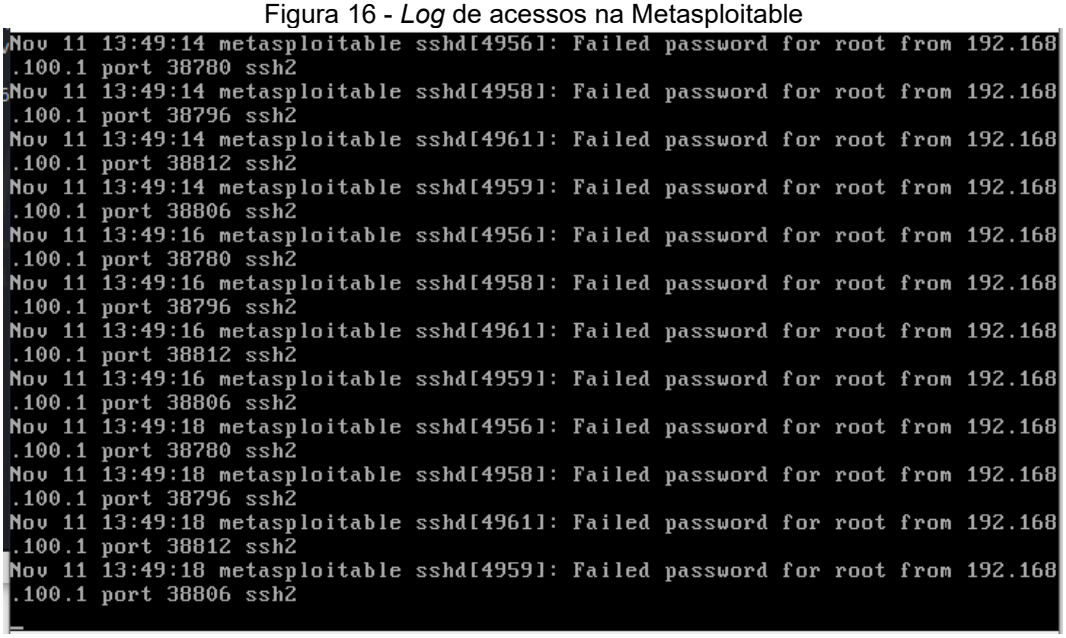
Figura 15 - Arquivo de textos com as possíveis senhas



Fonte: Autoria própria (2023)

Na Figura 16 é mostrado o resultado do comando "*tail -f /var/log/auth.log*" na máquina Metasploitable, enquanto ocorre o ataque de força bruta feito pela Hydra, é possível ver as tentativas que falharam sendo registradas, por tentarem uma senha errada do usuário *root*.

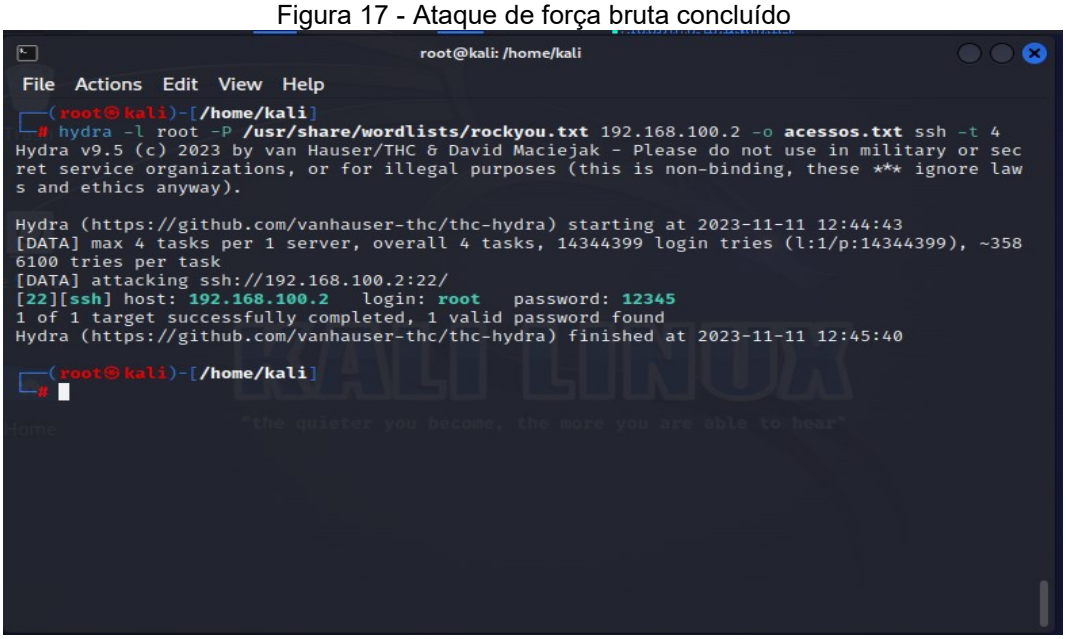
Figura 16 - *Log* de acessos na Metasploitable



Fonte: Autoria própria (2023)

Na Figura 17, após diversas tentativas, o Hydra conseguiu o acesso remoto à máquina Metasploitable, descobrindo qual a senha do usuário *root*.

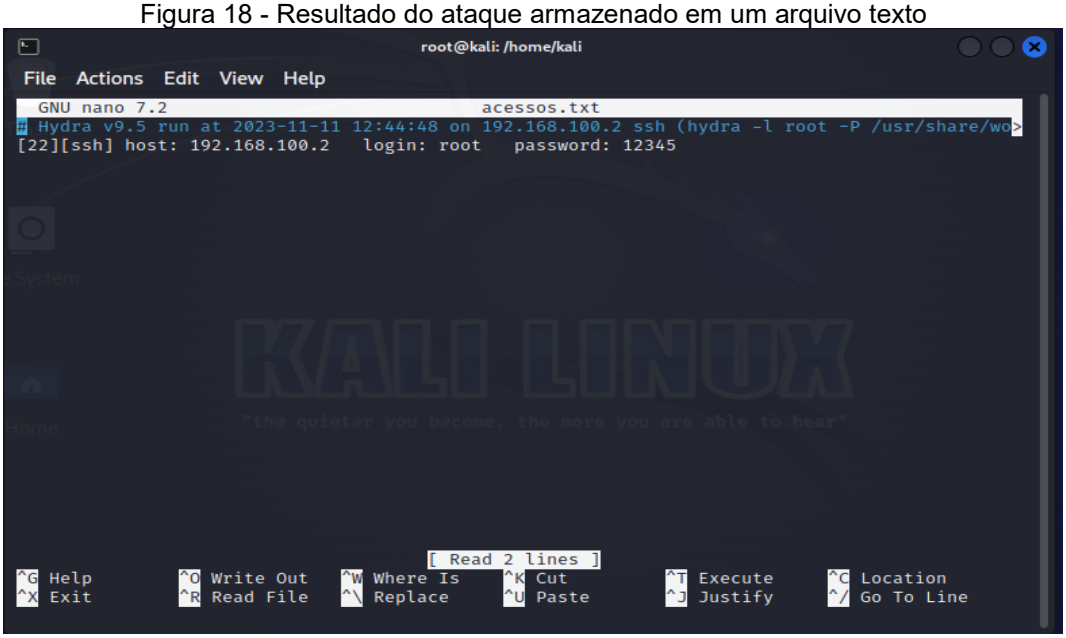
Figura 17 - Ataque de força bruta concluído



Fonte: Autoria própria (2023)

Na Figura 18 é possível ver o resultado do ataque sendo armazenado no arquivo “acessos.txt”, para que quando o atacante desejar, ele consiga acessar remotamente esta máquina.

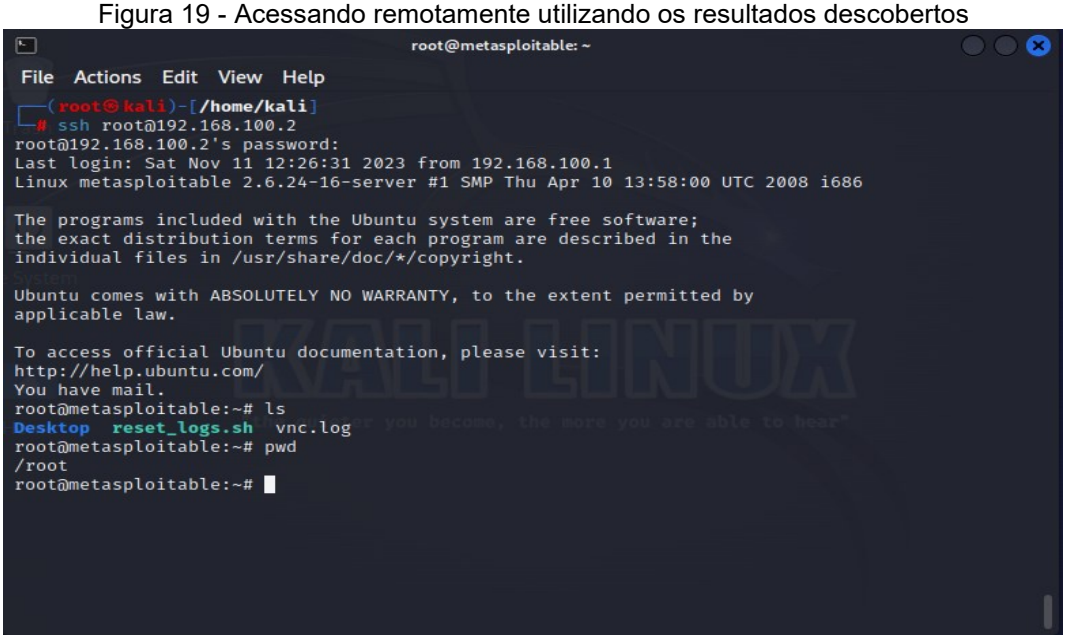
Figura 18 - Resultado do ataque armazenado em um arquivo texto



Fonte: Autoria própria (2023)

Na Figura 19 é possível ver o acesso remoto por meio do SSH a máquina que foi atacada, acessando por meio das credenciais descobertas no ataque anterior, usuário: “root” e senha: ”12345”.

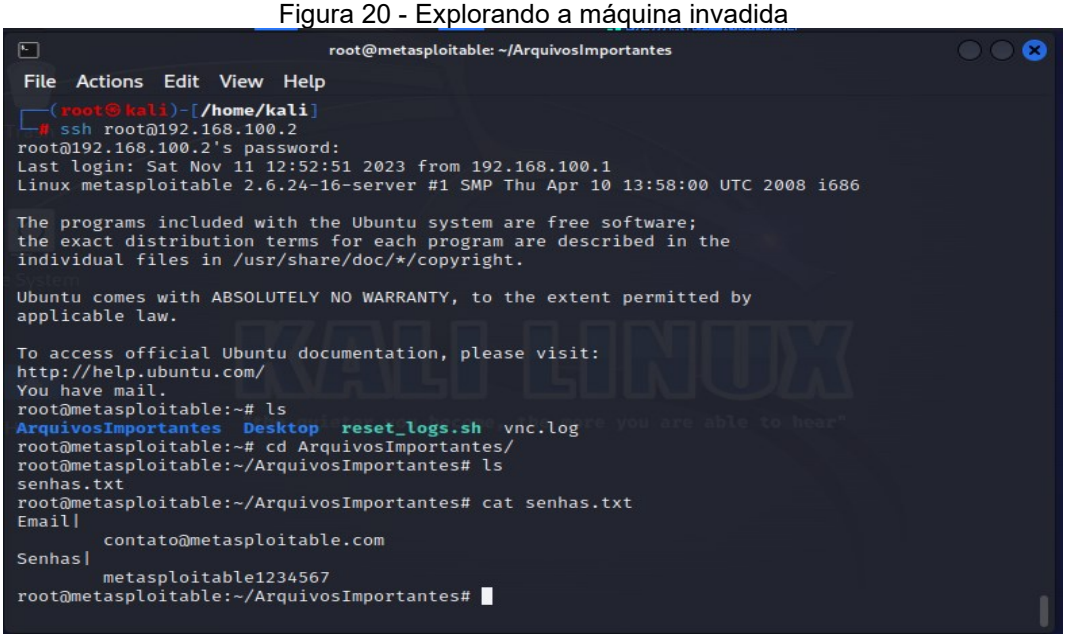
Figura 19 - Acessando remotamente utilizando os resultados descobertos



Fonte: Autoria própria (2023)

Na Figura 20 é possível ver o atacante acessando a máquina invadida, com isto, se consegue explorar o sistema, listando as informações armazenadas nele.

Figura 20 - Explorando a máquina invadida



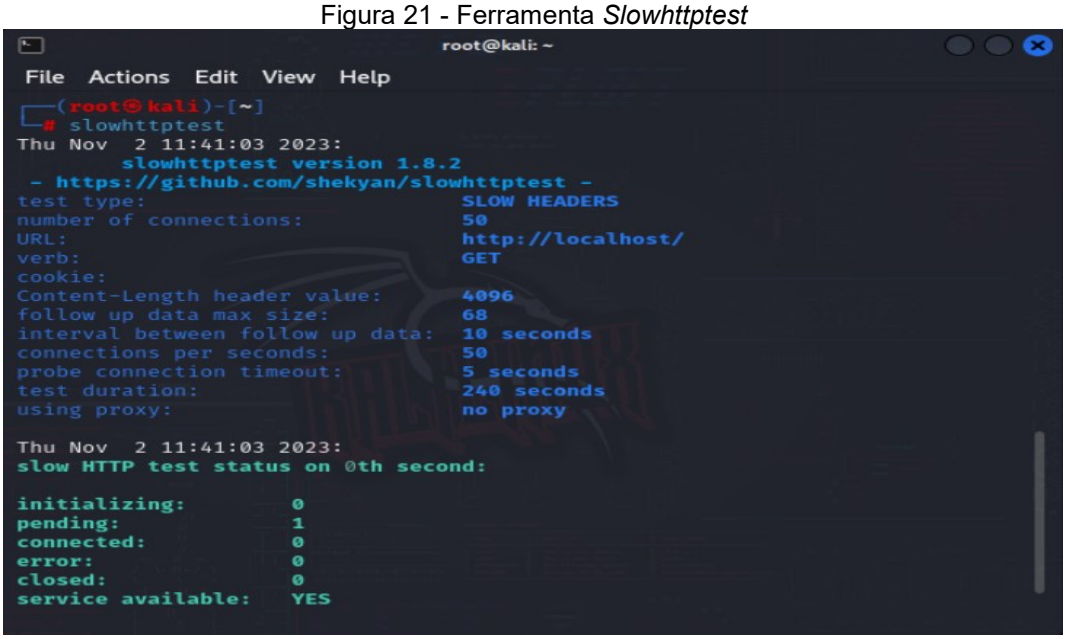
Fonte: Autoria própria (2023)

3.5.3 *Slowhttptest*

A partir do *Slowhttptest* será possível atacar o serviço *web* http que está hospedado na máquina Metasploitable, utilizando o DoS, que é um envio de diversas mensagens de *ping* para o serviço, até que ele não consiga se manter funcionando corretamente.

Na Figura 21 é possível visualizar a ferramenta *Slowhttptest* em sua versão 1.8.2 que é utilizada para explorar vulnerabilidades *web*.

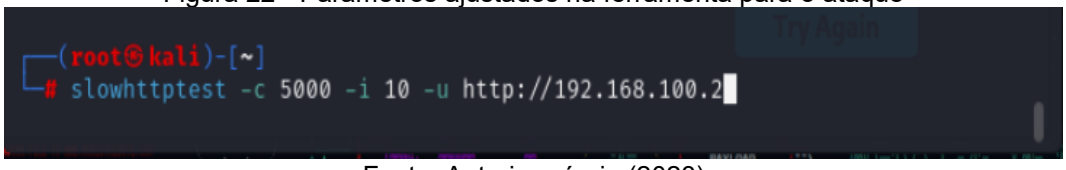
Figura 21 - Ferramenta *Slowhttptest*



Fonte: Autoria própria (2023)

Na Figura 22 é possível visualizar os parâmetros já ajustados para efetuar um ataque DoS na URL http://192.168.100.2/.

Figura 22 - Parâmetros ajustados na ferramenta para o ataque



Fonte: Autoria própria (2023)

No quadro 5 é possível ver os possíveis parâmetros que se pode utilizar para fazer o ataque DoS pelo *Slowhttptest*.

Quadro 5 - Opções de parâmetros para o ataque DoS

-c	Tamanho da solicitação HTTP em bytes.
-X	Método HTTP da solicitação.
-g	Número de solicitações para enviar por conexão.
-o	Arquivo de saída para salvar os resultados do teste.
slow read stats	Ativa a coleta de estatísticas de leitura lenta.
-r	Número de conexões para abrir por segundo.
-w	Tempo de espera para uma resposta HTTP em segundos.
-y	Tempo de espera para uma conexão em segundos.
-n	Número total de conexões para abrir.
-z	Número de solicitações para enviar.
-k	Mantém as conexões abertas após o teste.
-u	*User-Agent* HTTP a ser usado.
-p	Porta TCP para se conectar.

Fonte: Autoria própria (2023)

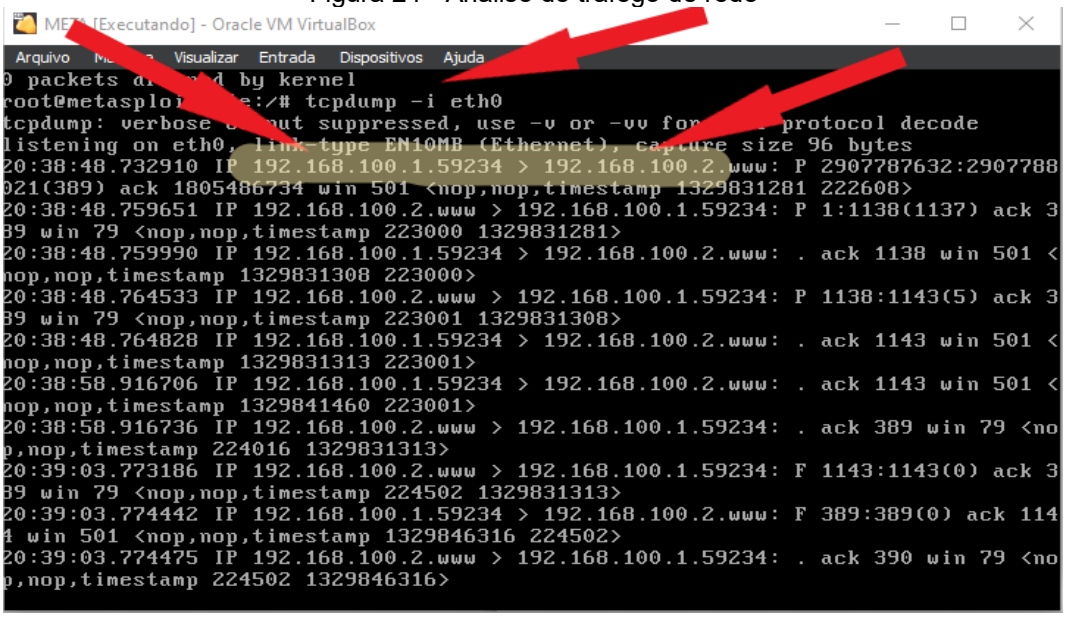
Na Figura 23 é possível visualizar a página *web* hospedada no servidor, podendo ser acessada normalmente momentos antes da execução do ataque.

Figura 23 - Página *web* que será alvo de ataque DoS

Fonte: Autoria própria (2023)

Na Figura 24 através do comando "*tcpdump -i eth0*" executado no servidor que permite realizar um monitoramento no tráfego de rede, podemos observar o tráfego na página *web* vindo da máquina Kali Linux antes do ataque DoS.

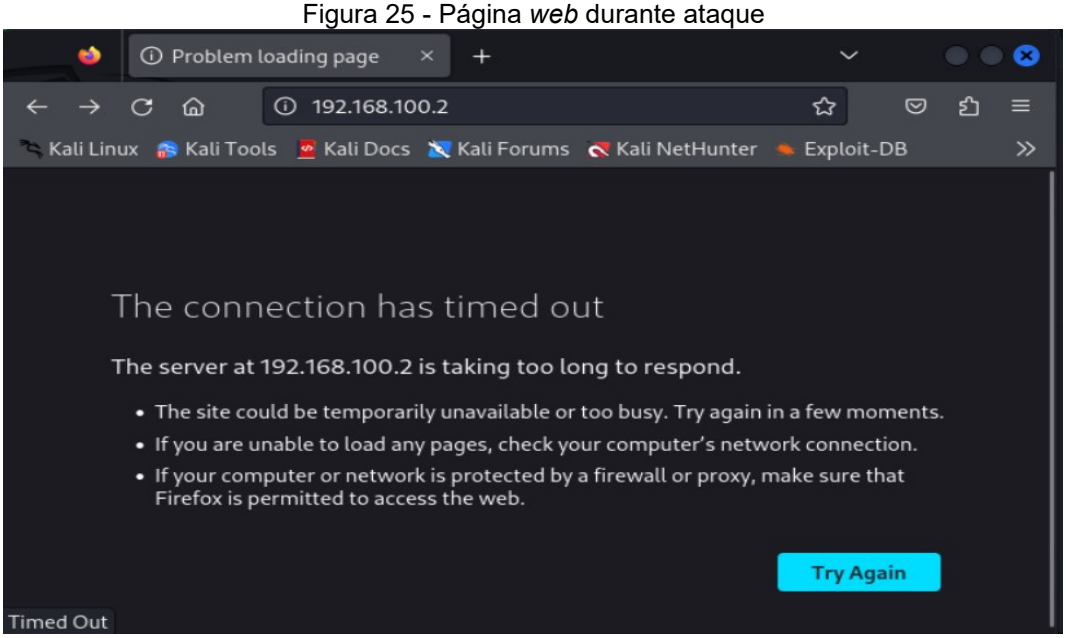
Figura 24 - Análise de tráfego de rede



Fonte: Autoria própria (2023)

A Figura 25 mostra o efeito causado pelo ataque DoS que deixou a página *web* indisponível durante o ataque.

Figura 25 - Página *web* durante ataque



Fonte: Autoria própria (2023)

3.6 Resultados

O *pentest* tem como objetivo localizar as vulnerabilidades existentes em redes, sistemas e computadores, para que, após localizar e documentar quais são elas, propor soluções para estes problemas, sendo assim, a partir dos resultados que foram obtidos com os testes anteriores, será apresentado maneiras de eliminar as vulnerabilidades encontradas nos testes anteriores e mitigar os danos.

3.6.1 Implementando senhas fortes

Com o teste de força bruta utilizando a ferramenta Hydra, foi possível ver que por ter uma senha simples sendo utilizada para acessar o SSH, a máquina está suscetível ao ataque de força bruta, sendo assim, para que seja evitado esse ataque é preciso alterar a senha do usuário root para uma complexa e difícil de adivinhar, é possível também utilizar outros métodos para proteger o serviço SSH, como utilizar chaves públicas e chaves privadas, nessa solução a troca da senha por uma mais complexa já será uma grande mudança para aprimorar a defesa de segurança.

Uma senha ideal é uma que tenha um tamanho maior e uma diversidade de caracteres que dificulte de ser adivinhada.

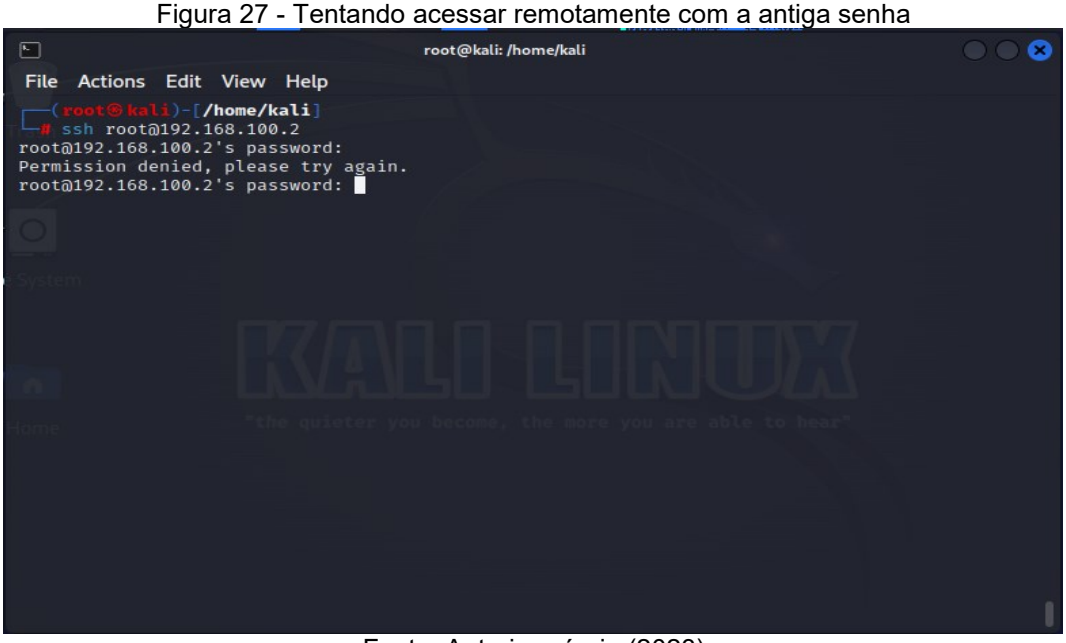
Na Figura 26 é possível ver o comando “*passwd root*”, que é utilizado para trocar a senha do usuário “*root*”, colocando uma senha complexa, sendo ela à “$%dF44aDr$5h7&&f”.

Figura 26 - Alterando senha do usuário root

Fonte: Autoria própria (2023)

Na Figura 27 se consegue ver que a senha utilizada anteriormente não é mais possível, sendo agora necessário inserir a senha “$%dF44aDr$5h7&&f”, que demoraria diversos anos para que fosse quebrada pelo ataque de força bruta.

Figura 27 - Tentando acessar remotamente com a antiga senha



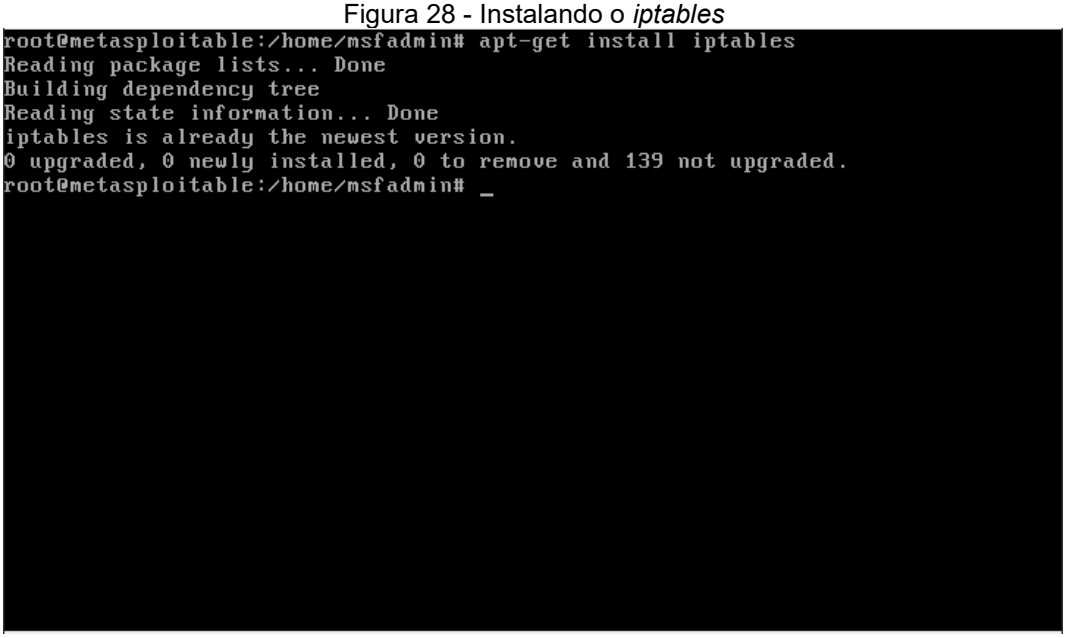
Fonte: Autoria própria (2023)

3.6.2 Implementando um *firewall*

Como foi possível ver pelo escaneamento feito pelo Nmap, a máquina Metasploitable está com diversas portas de serviço TCP/UDP abertas, sendo que elas não estão sendo utilizadas e podem ser exploradas, por isso é necessário fechá-las, por meio de um *firewall*.

Na Figura 28 podemos ver o comando *"apt-get install iptables*" sendo utilizado para instalar o *firewall* que é comumente utilizado em sistemas Linux, o *iptables*.

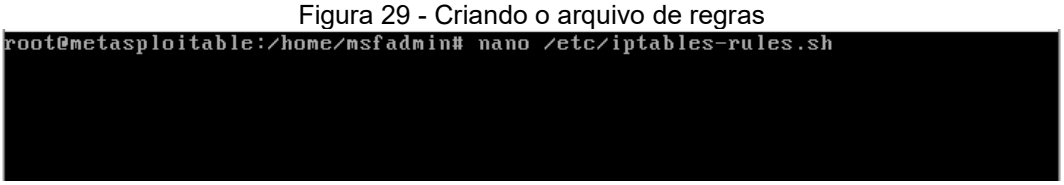
Figura 28 - Instalando o *iptables*



Fonte: Autoria própria (2023)

Na Figura 29 podemos ver o comando "*nano /etc/iptables-rules.sh*" que é utilizado para criar o arquivo que será utilizado para inserir as regras.

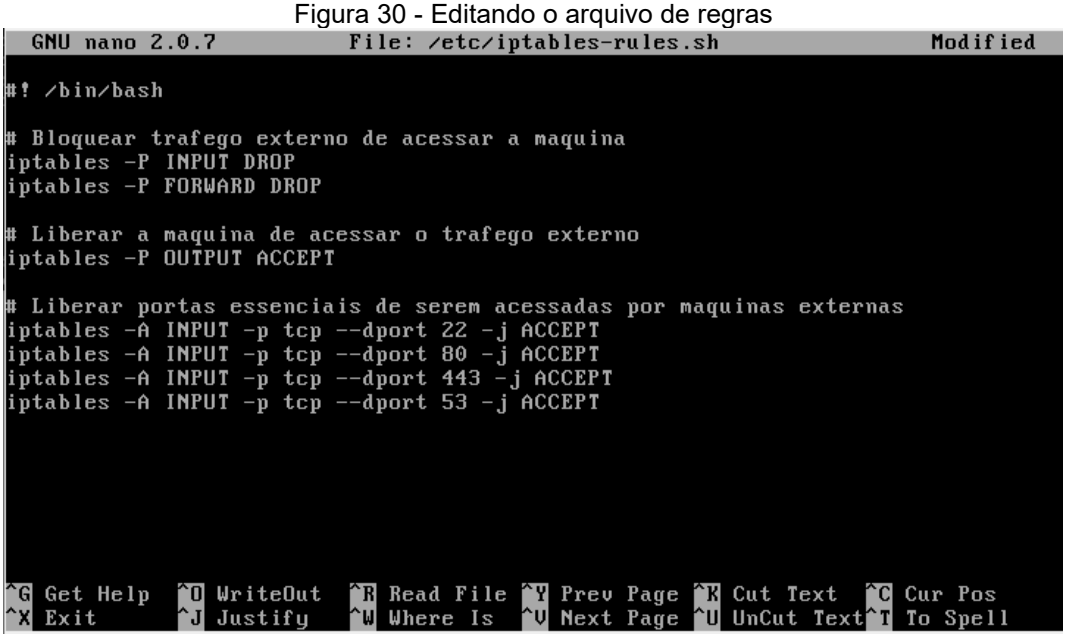
Figura 29 - Criando o arquivo de regras



Fonte: Autoria própria (2023)

Na Figura 30 é possível ver as regras para se bloquear as portas de serviço TCP/UDP, na primeira parte do arquivo é colocado três linhas que servem para bloquear todas as portas de serem acessadas por fontes externas, mas sendo possível a máquina em que está sendo configurado o *firewall* acessar as máquinas externas, no final do arquivo há quatro linhas que liberam a porta de serviços essenciais de serem acessadas por máquinas externas.

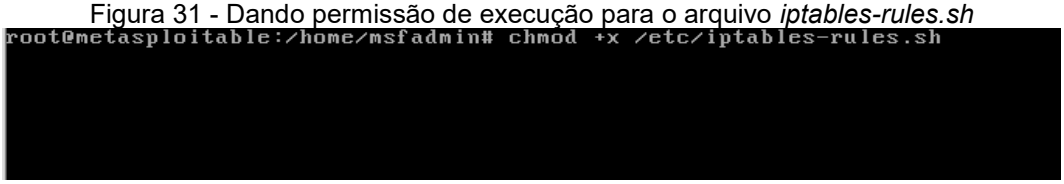
Figura 30 - Editando o arquivo de regras



Fonte: Autoria própria (2023)

Na Figura 31 podemos ver o comando "*chmod +x /etc/iptables-rules.sh*" que é utilizado para dar permissão de execução ao arquivo de regras.

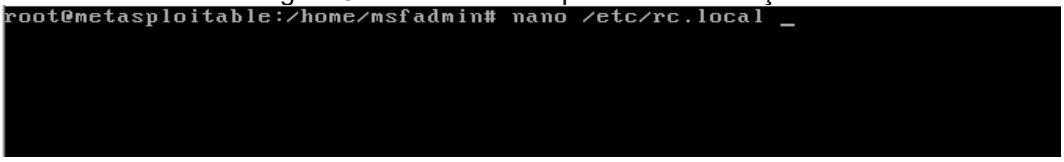
Figura 31 - Dando permissão de execução para o arquivo *iptables-rules.sh*



Fonte: Autoria própria (2023)

Na Figura 32 vemos o comando "*nano /etc/rc.local*" sendo utilizado para editar o arquivo que faz com que as regras criadas anteriormente sejam inicializadas juntas com o sistema.

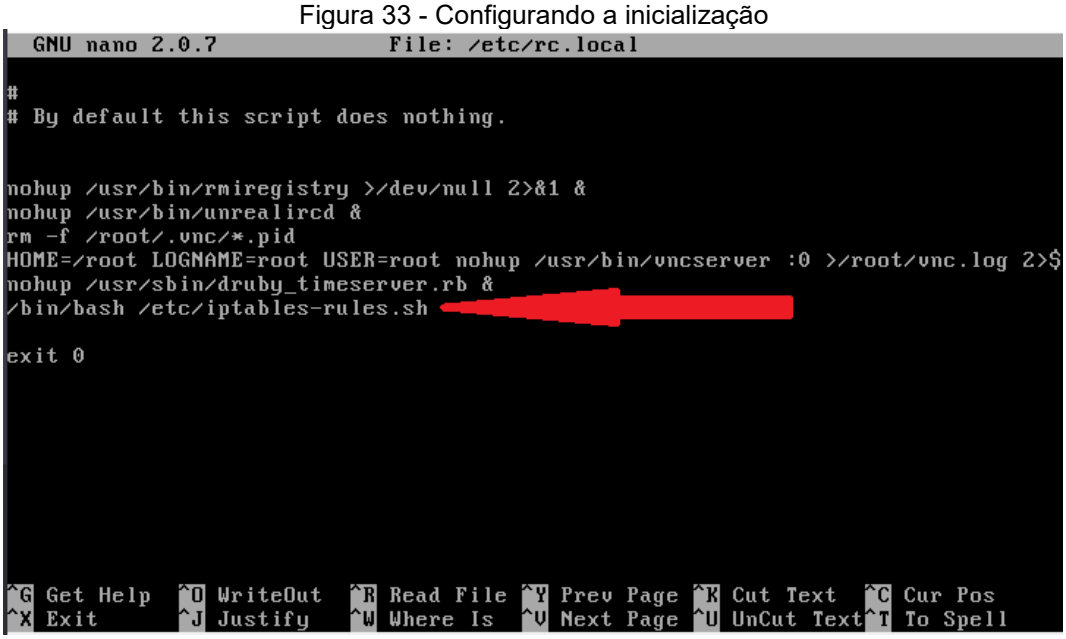
Figura 32 - Editando o arquivo de inicialização



Fonte: Autoria própria (2023)

Na Figura 33 é possível ver que foi inserido no final do arquivo "*rc.local*" a linha que faz com que o arquivo de regras seja inicializado e suas regras aplicadas.

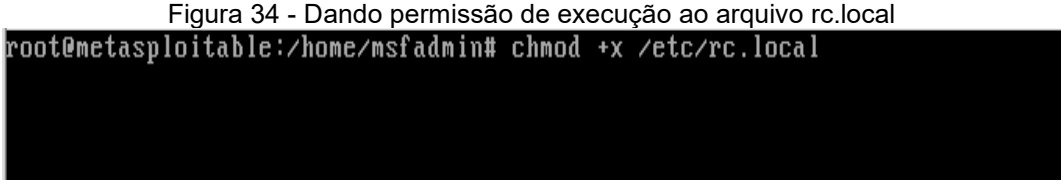
Figura 33 - Configurando a inicialização



Fonte: Autoria própria (2023)

Na Figura 34 vemos o comando "*chmod +x /etc/rc.local*" que é utilizado para dar permissão de execução ao arquivo de inicialização.

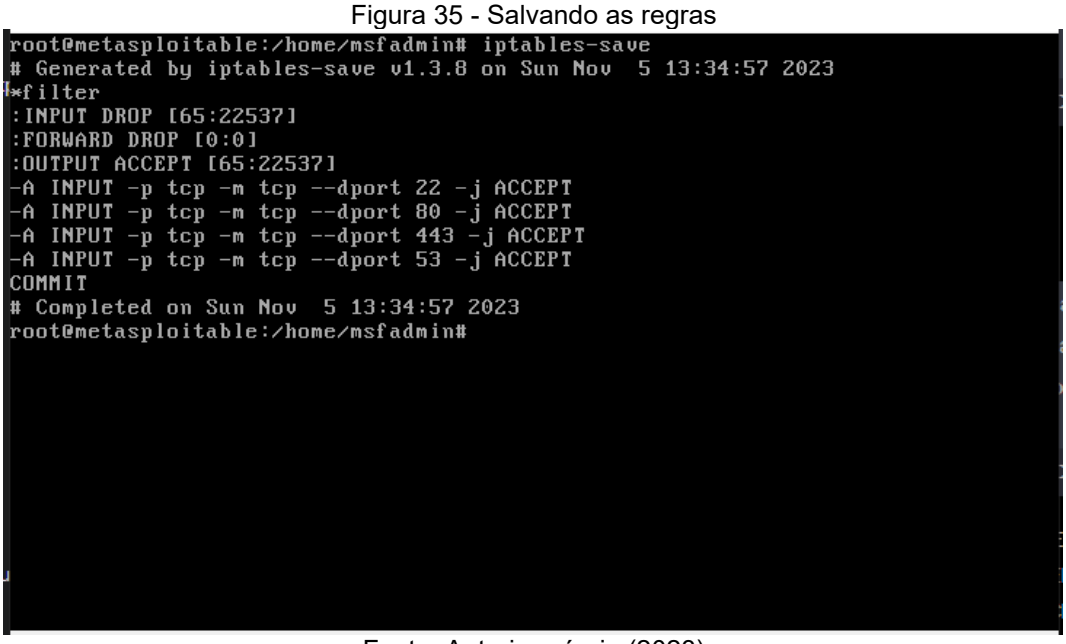
Figura 34 - Dando permissão de execução ao arquivo rc.local



Fonte: Autoria própria (2023)

Na Figura 35 é possível ver o comando "*iptables-save*" que é utilizado para salvar as configurações feitas anteriormente.

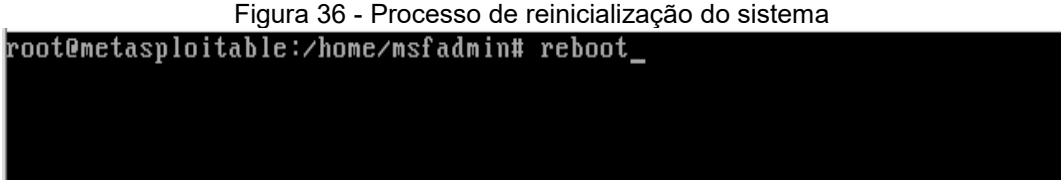
Figura 35 - Salvando as regras



Fonte: Autoria própria (2023)

Na Figura 36 é possível ver o comando "*reboo*t" utilizado para reiniciar o sistema e fazer com que as regras de *firewall* funcionem.

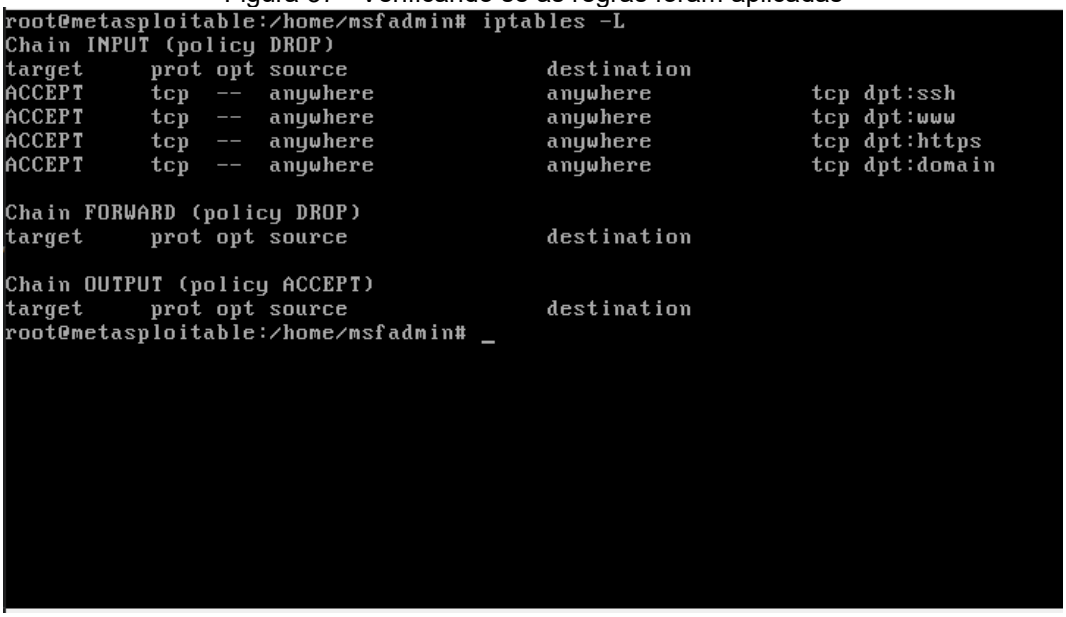
Figura 36 - Processo de reinicialização do sistema



Fonte: Autoria própria (2023)

Na Figura 37 é possível notar que com o comando "*iptables -L*" são mostradas as regras feitas anteriormente e que foram aplicadas e estão em funcionamento.

Figura 37 - Verificando se as regras foram aplicadas



Fonte: Autoria própria (2023)

Na Figura 38 vemos o escaneamento do Nmap sendo feito novamente, mas que agora há apenas as portas essenciais abertas, se for necessário que um serviço precise que algumas portas sejam abertas, pode-se adicionar uma nova regra no *firewall,* não se esquecendo de protegê-las antes de serem abertas.

Figura 38 - Testando o escaneamento após a configuração do *firewall*

Fonte: Autoria própria (2023)

3.6.3 Barrando ICMP

Para que o ataque DoS não tenha efeito no serviço *web* é preciso barrar os *pings* de serem respondidos pelo servidor, para isto será preciso adicionar algumas regras no *firewall* que foi desenvolvido anteriormente.

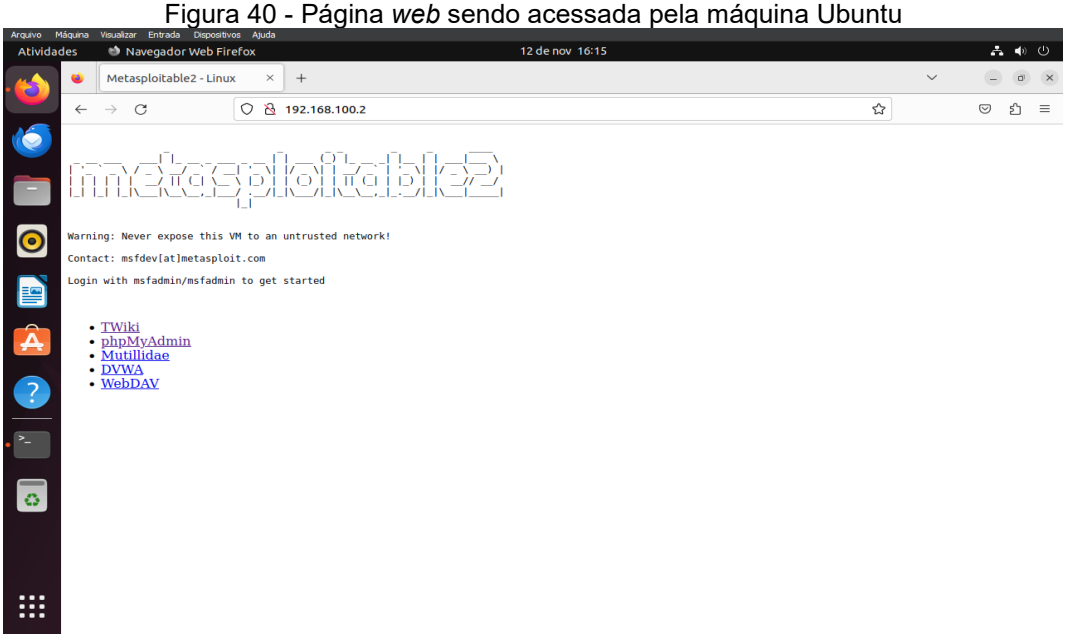
Vemos na Figura 39 a aplicação de regras no *firewall iptables* para mitigar o ataque DoS, é uma tática de segurança da informação que consiste em limitar o número de conexões ou solicitações que um determinado endereço IP pode fazer em um determinado intervalo de tempo.

Figura 39 - Aplicação de regras no firewall iptables para mitigar ataque DoS

Fonte: Autoria própria (2023)

A Figura 40 mostra que a página *web* do servidor Metasploitable está acessível na máquina do usuário Ubuntu durante o ataque de negação de serviços, mostrando que as novas regras do *firewall* impediram que ela fosse derrubada.

Figura 40 - Página *web* sendo acessada pela máquina Ubuntu



Fonte: Autoria própria (2023)

CONSIDERAÇÕES FINAIS

Com o decorrer desta pesquisa foi notório a importância do estudo da Segurança da Informação, para que as tecnologias usadas pelas empresas estejam seguras e funcionando como deveriam.

Ao fim deste trabalho foi possível entender do que se trata o *pentest,* como ele é utilizado para encontrar vulnerabilidades, sua busca contínua por brechas de segurança, sua análise do ambiente para que seja possível documentar o que foi descoberto e propor soluções, com o intuito de aumentar a as defesas cibernéticas nos computadores de uma rede.

Foi possível entender que as vulnerabilidades são comumente causadas por configurações erradas, que geram diversos meios para causar danos à máquina, mas foi possível também observar a facilidade de implementar métodos para combater as ameaças, porque sistemas operacionais Linux são abertos para configurá-los, fazendo com que haja muitas formas de solucionar os problemas de segurança.

Também foi enfatizado a conscientização de boas práticas, trazendo à tona o compromisso que todos os colaboradores de uma empresa têm com a confidencialidade e a integridade das informações que eles detêm.

Em suma, a cibersegurança necessita que haja um olhar atento às mudanças que ocorrem, localizar vulnerabilidades existentes em serviços dos sistemas operacionais Linux é de extrema importância, muitos servidores são baseados nele, pois como foi visto anteriormente, se não houver uma mitigação contra um ataque DoS, uma página na *Internet* pode sofrer o ataque e ficar sem funcionar por um longo período, causando prejuízo ao seu proprietário.

REFERÊNCIAS

ALVES, Patrícia. Como garantir autenticidade da assinatura digital. **Linkedin**, 2019. Disponível em: https://www.linkedin.com/pulse/como-garantir-autenticidade-da-assinatura-digital-patrícia-silva/?originalSubdomain=pt. Acesso em: 12 out. 2023, às 13h17min.

ANTONIO, Joas. Pentest, as certificações mais conhecidas. **Academia de forense digital**, 2022. Disponível em: https://academiadeforensedigital.com.br/pentest-as-certificacoes-mais-reconhecidas/. Acesso em: 14 mai. 2023, às 20h38min.

APETI. Os 5 pilares da segurança da informação. **Apeti**, 2023. Disponível em: https://apeti.org.br/blog/os-5-pilares-da-seguranca-da-informacao. Acesso em: 01 out. 2023, às 23h10min.

BUILTWITH. Find out what websites are Built With. **Builtwith**, 2023. Disponível em: https://builtwith.com. Acesso em: 21 mar. 2023, às 19h07min.

PROFISSIONAIS TI. 10 ferramentas mais usadas para Pentest (Testes de Invasão). **Profissionais TI**, 2020. Disponível em: https://www.profissionaisti.com.br/10-ferramentas-mais-usadas-para-pentest/. Acesso em: 21 mai. 2023, às 21h38min.

BLOG CENTRAL SERVER. As 5 vulnerabilidades mais comuns em web site e como evitá-las. **Blog Central Server,** 9 jan. 2015. Disponível em: https://blog.centralserver.com.br/as-5-vulnerabilidades-mais-comuns-em-web-sites-e-como-evita-las/. Acesso em: 07 abr. 2023, às 20h17min.

ESPINOSA, Christian**.** Penetration Testing History. **The Secure Blog:** insights to give you and edge in your worplace and your life, 2023. Disponível em: https://christianespinosa.com/blog/penetration-testing-history/#:~:text=Penetration%20testing%20first%20became%20a,risk%20to%20the%20system%27s%20security. Acesso em: 20 fev. 2023, às 22h50min.

CISCO. Configuring Security Access Control Lists. **Cisco**, 2019. Disponível em: https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/www.cisco.com/content/en/us/td/docs/interfaces_modules/services_modules/ace/vA2_3_0/configuration/security/guide/securgd/acl.html.xml. Acesso em: 30 set. 2023, às 20h25min.

DONDA, Daniel. **Guia prático de implementação da LGPD**: tudo que sua empresa precisa saber para estar em conformidade. 1. ed. São Paulo: Labrador, 2020.

DONOHUE, Brian. Hash: o que são e como funcionam. **Kaspersky**, 2014. Disponível em: https://www.kaspersky.com.br/blog/hash-o-que-sao-e-como-funcionam/2773/. Acesso em: 12 out. 2023, às 23h17min.

FACHINI, Tiago. Lei Carolina Dieckmann: Tudo o que você precisa saber sobre. **Projuris**, 2023. Disponível em: https://www.projuris.com.br/blog/lei-carolina-dieckman-tudo-o-que-voce-precisa-saber-sobre/. Acesso em: 02 dez. 2023, às 08h59min.

FRAGA, Bruno. **Técnicas de invasão**: aprenda as técnicas usadas por hackers em invasões reais. 1. ed. São Paulo: Labrador, 2019.

GAZOLA, Rodrigo. Dicas para uma boa análise de vulnerabilidade na rede de computadores de seu cliente. **Addee**, 2021. Disponível em: https://addee.com.br/blog/analise-de-vulnerabilidade/. Acesso em: 30 set. 2023, às 21h37min.

GONÇALVES, Samuel. Conheça as 10 principais vulnerabilidades web de 2021. **4Linux**, 2022. Disponível em: https://blog.4linux.com.br/conheca-as-10-principais-vulnerabilidades-web-de-2021/. Acesso em: 07 abr. 2023, às 23h10min.

GUEDES, Marylene. Pilares da Segurança da Informação. **Treinaweb**, 2020. Disponível em: <https://www.treinaweb.com.br/blog/pilares-da-seguranca-da-informacao>. Acesso em: 12 out. 2023, às 21h57min.

KALI. Kali Linux features. **Kali**, 2023. Disponível em: https://www.kali.org/features/. Acesso em: 05 mar. 2023, às 20h20min.

KESHRI, Aakanchha. Top 5 penetration testing methodologies and standards. **Astra**, 2021. Disponível em: https://www.getastra.com/blog/security-audit/penetration-testing-methodology/. Acesso em: 05 mar. 2023, às 19h27min.

KUROSE, J. F.; ROSS, K. W. **Computer networking:** A top-down approach: International edition. 6. ed. [s.l.] Pearson Education, 2013.

OLIVEIRA, Arlei. Os pilares da Segurança da Informação - Confidencialidade, Integridade e Disponibilidade. **Linkedin**, 2023. Disponível em: https://www.linkedin.com/pulse/os-pilares-da-segurança-informação-integridade-e-arlei-oliveira/?originalSubdomain=pt. Acesso em: 22 out. 2023, às 21h33min.

ORACLE. Welcome to VirtualBox.org! **Virtualbox**, 2023. Disponível em: https://www.virtualbox.org. Acesso em: 22 out. 2023, às 23h10min.

PADHYAY, Rajkumaru. Time sharing operating system. **Geeks for geeks**, 2023. Disponível em: https://www.geeksforgeeks.org/time-sharing-operating-system/. Acesso em: 20 fev. 2023, às 22h14min.

PEDRA, David. Segurança da informação: o que é e como criar uma política para proteção de dados. **Siteware**, 2023. Disponível em: https://www.siteware.com.br/seguranca/seguranca-da-informacao/. Acesso em: 01 out, 2023, às 19h10min.

PEREIRA, F. S. CERTIFICAÇÃO DIGITAL**:** aplicação tecnológica para autenticidade de documentos arquivísticos digitais. **Brasil escola**, 2014. Disponível em: https://monografias.brasilescola.uol.com.br/administracao-financas/certificacao-digital-aplicacao-tecnologica-para-autenticidade-de-documentos.htm. Acesso em: 12 out. 2023, às 21h21min.

RAIDBR. Importância do Pentest para as organizações. **Raidbr**, 2023. Disponível em: https://www.raidbr.com.br/importancia-do-pentest#:~:text=Entender%20a%20importância%20do%20pentest%20é%20simples%3A%20testar%20periodicamente%20os,possíveis%20novas%20oportunidades%20de%20cibersegurança. Acesso em: 02 dez. 2023, às 08h33min.

RAPID7USER. Metasploitable. **Sourceforge**, 2019. Disponível em: https://sourceforge.net/projects/metasploitable/. Acesso em: 22 out. 2023, às 19h31min.

RIJNETU, Loana. 100+ essential penetration testing statistics [2023 edition]. **Pentest tools**, 2023. Disponível em: https://pentest-tools.com/blog/penetration-testing-statistics. Acesso em: 21 mai, 2023, às 23h20min.

SANTOS, Andréia. **Análise de vulnerabilidade em rede, com teste de intrusão, utilizando a distribuição Kali Linux**. Orientador: Fábio Cristiano de Oliveira. 2015. 46 f. TCC (Graduação) – Licenciatura em Computação, Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano, Petrolina. 2015. Disponível em: https://releia.ifsertao-pe.edu.br/jspui/bitstream/123456789/352/1/TCC%20-%20ANÁLISE%20DE%20VULNERABILIDADE%20EM%20REDE%2c%20COM%20TESTE%20DE%20INTRUSÃO%2c%20UTILIZANDO%20A%20DISTRIBUIÇÃO%20KALI%20LINUX.pdf. Acesso em: 12 out. 2023, às 20h31min.

SANTOS, Raphael. Modelo OSI: entenda como funciona esse sistema de camadas. **Hosts green**, 2019. Disponível em: https://blog.hosts.green/modelo-osi/. Acesso em: 30 set, 2023, às 21h23min.

SHIVANANDHAN, Manish. How to Use Hydra to Hack Passwords – Penetration Testing Tutorial. **Freecodecamp**, 2022. Disponível em: https://www.freecodecamp.org/news/how-to-use-hydra-pentesting-tutorial/. Acesso em: 28 out. 2023, às 21h17min.

SOLDATELI, F. L. Foi hackeado em 2022? Conheça as vulnerabilidades mais exploradas. **Olhar digital**, 2023. Disponível em: https://olhardigital.com.br/2023/01/06/seguranca/foi-hackeado-em-2022-conheca-as-vulnerabilidades-mais-exploradas/. Acesso em: 07 abr. 2023, às 20h37min.

UBUNTU. Ubuntu Desktop. **Ubuntu**, 2023. Disponível em: https://ubuntu.com/download. Acesso em: 12 nov. 2023, às 15h47min.

Writer. 10 Passos Essenciais para Realizar um Teste de Penetração Bem-Sucedido. **Nobug**, 2023. Disponível em: https://nobug.com.br/10-passos-essenciais-para-realizar-um-teste-de-penetracao-bem-sucedido/. Acesso em: 02 dez. 2023, às 10h02min.