Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

RICARDO ALVES DE OLIVEIRA SOBRINHO

Análise de Vulnerabilidades em Sistemas Operacionais

Assis/SP
Ano 2024

Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

RICARDO ALVES DE OLIVEIRA SOBRINHO

Análise de Vulnerabilidades em Sistemas Operacionais

Trabalho de Conclusão de Curso apresentado ao curso de analise e desenvolvimento de sistema do Instituto Municipal de Ensino Superior de Assis – IMESA e a Fundação Educacional do Município de Assis – FEMA, como requisito parcial à obtenção do Certificado de Conclusão.

Orientando(a): Ricardo Alves de Oliveira Sobrinho
Orientador(a): Dr. Fábio Éder Cardoso

Assis/SP
Ano 2024

Oliveira Sobrinho, Ricardo Alves de

O482a Análise de vulnerabilidades em sistemas operacionais / Ricardo Alves de Oliveira Sobrinho. -- Assis, 2024.

35p.

Trabalho de Conclusão de Curso (Graduação em Análise e Desenvolvimento de Sistemas) -- Fundação Educacional do Município de Assis (FEMA), Instituto Municipal de Ensino Superior de Assis (IMESA), 2024.

Orientador: Prof. Dr. Fábio Eder Cardoso.

1. Segurança da informação. 2. Tolerância a falhas. 3. Educação. I Cardoso, Fábio Eder. II Título.

CDD 003

Análise de Vulnerabilidades em Sistemas Operacionais

RICARDO ALVES DE OLIVEIRA SOBRINHO

Trabalho de Conclusão de Curso apresentado ao Instituto Municipal de Ensino Superior de Assis, como requisito do Curso de Graduação, avaliado pela seguinte comissão examinadora:

Orientador: Dr. Fábio Éder Cardoso

Examinador: M.e. Claudinei Moreira da Silva

Assis/SP
Ano 2024

RESUMO

O objetivo central deste trabalho é investigar a segurança da informação no contexto dos sistemas educacionais, utilizando ferramentas de análise de vulnerabilidades para avaliar a robustez dos sistemas operacionais. Com o intuito de verificar a eficácia das defesas e identificar potenciais falhas, foi realizada uma exploração de vulnerabilidades em sistemas operacionais Microsoft Windows, por meio do Metasploit Framework. Ao longo do estudo, a curiosidade científica foi direcionada para entender como esses testes de segurança se comportam em ambientes Windows, buscando fornecer uma análise detalhada da segurança oferecida por esses sistemas. Assim, este projeto tem como foco o estudo e a implementação de testes de vulnerabilidade, com o objetivo de avaliar a real segurança dos sistemas operacionais utilizados.

Palavras-Chave: Penstest, Penetration Testing, Ensino, Falha, Defesa, Hacker.

SUMÁRIO

1. INTRODUÇÃO

A área educacional é um pilar extremamente importante da sociedade, na qual é composto por diversos sistemas tecnológicos que auxiliam os profissionais, entretanto, esses sistemas podem apresentar vulnerabilidades, comprometendo todo o processo de trabalho

Em razão disso, este trabalho objetiva a análise de vulnerabilidades desses sistemas, identificando as falhas e, contribuindo na implementação de segurança para evitar problemas futuros.

Dando início ao desenvolvimento deste TCC, trouxe como ideia inicial identificar, instalar e implementar ferramentas e procedimentos técnicos de testes de invasão em uma rede de sistemas dentro de um ambiente controlado por meio de simulação, e, com isso, identificar como tais testes influenciam no código e apresentam as falhas de segurança.

Como produto final, após adquirir expertise com uso das ferramentas de *pentest*, poderá ser implementado, com devida autorização legal, todo o processo em alguma instituição de ensino com a finalidade de identificar fragilidades nas aplicações.

Neste cenário, os autores pesquisados desenvolveram estudos de caso abordando aplicações web e em grandes empresas. No presente trabalho, objetiva explorar estudos que levam em conta a intrusão de sistemas na área educacional.

Em consonância ao apresentado por Weidman (2014, p. 30), teste de invasão (ou *Pentesting*) pode ser interpretado como uma simulação de ataques reais destinada a avaliar os riscos e impactos associados a brechas de segurança identificadas (caso sejam exploradas).

A autora também frisa que diferentemente das auditorias de segurança e de análise de vulnerabilidade, na qual a busca é focada em analisar e identificar vulnerabilidades sem necessariamente explora-las, um teste de invasão vai além disso onde se utiliza métodos e técnicas de invasão não somente para identificar possíveis brechas de segurança e sim diagnosticar profundamente quando viável, com a finalidade de avaliar o que os possíveis invasores poderiam obter ao serem bem sucedidos descobrindo tal falha.

Para que se realize testes em um sistema, é necessário ter um ambiente preparado, pois os testes que são feitos em um ambiente de produção, pois podem causar certa indisponibilidade nos serviços que esse sistema oferece.

O teste de invasão, ou *pentest*, é uma atividade em que são empregadas diversas técnicas para descobrir vulnerabilidades, em sistemas. O *pentest* tem como objetivo descobrir o maior número possível de vulnerabilidade e, para que isso aconteça, é necessário, um ambiente preparado. Isso porque o uso de ferramentas automatizadas e, até mesmo, os testes feitos manualmente podem causar indisponibilidade do serviço, entre outras implicações. (ALMEIDA JR, 2021, p.31).

De acordo com Weidman (2014, p.31-35), uma invasão possui 7 fases:

1) Preparação: Os testes de invasão têm início com a fase de preparação (*pre-engagement*), que envolve conversar com o cliente a respeito de seus objetivos para o teste de invasão, o mapeamento do escopo (a extensão e os parâmetros do teste) e assim por diante. Quando o pentester e o cliente chegarem a um acordo sobre o escopo, a formatação do relatório e outros assuntos, o teste de invasão propriamente dito terá início.
2) Coleta de informações: o pentester procura informações disponíveis publicamente sobre o cliente e identifica maneiras em potencial de conectar-se com seus sistemas. Na fase de modelagem das ameaças (*threat-modeling*), o pentester usa essas informações para determinar o valor de cada descoberta e o impacto sobre o cliente caso a descoberta permita que alguém invada um sistema. Essa avaliação permite ao pentester desenvolver um plano de ação e métodos de ataque.
3) Modelagem de ameaças: De acordo com o conhecimento obtido na fase de coleta de informações, prosseguiremos para a modelagem das ameaças. Nesse ponto, procura-se pensar como os invasores e desenvolvem planos de ataque de acordo com as informações coletadas. Por exemplo, se o cliente desenvolver um *software* proprietário, um invasor poderá devastar a empresa ao obter acesso aos seus sistemas de desenvolvimento internos, em que o código-fonte é desenvolvido e testado, e vender os segredos comerciais da empresa a um concorrente. De acordo com os dados encontrados durante a fase de coleta de informações, desenvolveremos estratégias para invadir os sistemas de um cliente.
4) Análise de vulnerabilidades: Antes que o *pentester* possa começar a atacar os

sistemas, ele realiza uma análise de vulnerabilidades (*vulnerability analysis*). Nessa fase, o *pentester* procura descobrir vulnerabilidades nos sistemas que poderão ser exploradas na fase de exploração de falhas (*exploitation*). Um *exploit* bem-sucedido pode conduzir a uma fase de pós-exploração de falhas (*post-exploitation*), em que se tira vantagem do resultado da exploração de falhas, de modo a descobrir informações adicionais, obter dados críticos, acessar outros sistemas e assim por diante.

5) Exploração de falhas: Neste ponto, são executados exploits contra as vulnerabilidades descobertas (às vezes, usando uma ferramenta como o Metasploit) em uma tentativa de acessar os sistemas de um cliente.
6) Pós-exploração de falhas: Na fase de pós-exploração de falhas, após o sistema ter sido invadido é onde se reúnem as informações mais interessantes e de valores, caso haja a necessidade de um cargo maior é preferível que procure uma maneira de elevar o nível. Por exemplo, podemos fazer um dump das hashes de senha para ver se podemos revertê-las ou usá-las para acessar sistemas adicionais. Também podemos tentar usar o computador explorado para atacar sistemas que não estavam anteriormente disponíveis a nós se efetuarmos um pivoteamento para esses sistemas.
7) Geração de relatórios: Na última fase é onde será feito o relatório da invasão, é onde o cliente é informado sobre todas as descobertas significativas. É passado tudo de correto que o cliente fez, e os pontos a qual ele precisa melhorar sua postura quanto a segurança, como corrigir os problemas e assim por diante

Todas essas fases consistem no processo de sucesso de um teste de invasão, onde os pentesters não só identificam, como avaliam, exploram todas as possibilidades mapeadas que um possível invasor possa realizar.

O presente trabalho está dividido em 4 secções. A seção 1, esta Introdução, apresenta os objetivos e as justificativas para a execução do trabalho. A seção 2 aborda os estudos de todos os testes de invasão que iremos usar. Na seção 3 estão os resultados dos testes e como exploramos as falhas no sistema. Enfim na seção 4, apresentam-se as conclusões obtidas a partir da realização deste trabalho e direciona para trabalhos futuros.

1.1. OBJETIVOS

1.1.1. Objetivos Gerais

O presente trabalho tem como objetivo geral identificar como procedimentos de invasão influenciam no código de um sistema, dessa forma analisa-se se o mesmo apresenta falhas ou não. Os testes são feitos todos em um sistema controlado e simulado.

1.1.2. Objetivo Específico

Para atender aos propósitos deste trabalho, este projeto se propõe a:

1- Implementar as ferramentas e procedimentos técnicos de invasão em uma rede de sistemas, todos os testes serão executados em um ambiente controlado e simulado para evitar possíveis problemas.
2- Em decorrência da implementação, irá ser feita uma análise de como o código se comportou enquanto os testes eram executados e se o mesmo apresentou alguma falha de segurança.
3- Depois de feita a implementação e análise das possíveis falhas no código do sistema, o time de desenvolvimento do orgão a qual nos disponibilizou o código será contactado, com o intuito de que os mesmos solucionem o problema.

1.2. JUSTIFICATIVA

A implementação de um teste de penetração *(pentest)* é essencial para garantir a segurança de uma organização. Quando é implementado simulações de ataques reais, no processo grande parte das organizações apresentam vulnerabilidades e falhas na

infraestrutura do sistema, isso nos traz uma análise mais detalhada de como está a segurança do sistema.

Ao revelar possíveis pontos fracos, os testes de penetração permitem que as equipes de segurança tomem ações preventivas e corretivas eficazes, reduzindo o risco de exploração por hackers mal-intencionados. Além de proteger dados sensíveis e informações da instituição, esta abordagem aumenta a confiabilidade de uma organização em razão a ameaças cibernéticas. Além disso, ao demonstrar compromisso com a segurança, aumenta-se a confiança de clientes e parceiros, solidificando a reputação da instituição no mercado.

1.3. MOTIVAÇÃO

A motivação para a realização desse trabalho está no reconhecimento de que com o passar dos anos a tecnologia evoluiu em um patamar tão grande que virou indispensável a análise mais profunda de redes de sistemas. Dessa forma, o presente trabalho de conclusão de curso segue na direção de estudar e implementar um pentest em um ambiente controlado e simulado.

1.4. PERSPECTIVA DE CONTRIBUIÇÃO

Após a finalização deste presente trabalho, espera-se que ele possa contribuir com o setor de segurança em sistemas educacionais, de uma forma que faça com que as outras instituições de ensino reflitam sobre se o sistemas a qual elas utilizam são realmente seguros. Espera-se também que a instituição a qual faremos os testes solucione os problemas identificados evitando futuros problemas de hackers maliciosos.

1.5. METODOLOGIA

A presente pesquisa será de natureza aplicada, do tipo exploratório, com procedimentos experimentais, utilizando ambientes controlados e simulados para adquirir conhecimentos que permeiam os procedimentos de análise de vulnerabilidade por meio de *Pentest*.

Para embasar os aspectos teóricos e práticos deste trabalho, será realizada exploração na literatura científica, abrangendo artigos e livros sobre redes de computadores e segurança da informação, a fim de adquirir os conhecimentos necessários para a execução eficiente da pesquisa.

Em decorrência dos estudos efetuados, será decidido qual metodologia de *pentest* a ser utilizada, bem como técnicas e tecnologias para implementar os processos de analise de vulnerabilidades.

2. REDES DE COMPUTADORES

Definição

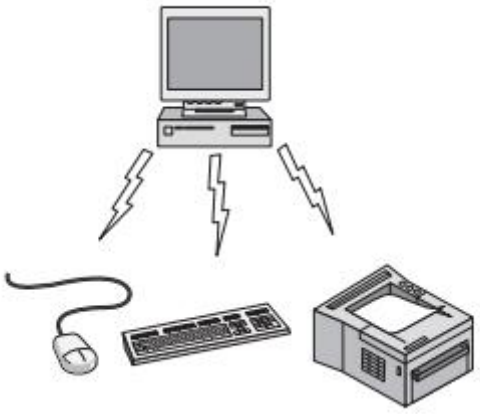
Tanenbaum (2018) diz que uma rede de computadores é composta por um conjunto de computadores e qualquer outro dispositivo conectado um com o outro, onde compartilham recursos, dados e aplicações. O tamanho dessas redes pode variar em termos de topologia, tipo de conexão e protocolos de comunicação. Pode-se afirmar que uma rede de computadores faz com que os dispositivos de comuniquem entre eles, onde compartilham arquivos, impressões e conexões à Internet.

Tipos de Redes

A criação dos tipos de redes tem como intuito de atender a demanda, de acordo com Tanenbaum em *Rede de computadores* (2011) ‘’ [...] À medida que cresce nossa capacidade de colher, processar e distribuir informações, torna-se ainda maior a demanda por formas mais sofisticadas de processamento de informação’’ (TANENBAUM, 2011, p.01), por consequência, o compartilhamento de recursos e a conectividade atuam em diferentes contextos e escalas. Em seguida são apresentados neste artigo, os modelos de redes de computadores, para ilustrá-los, as leituras de *Rede de computadores* de Tanenbaum e *Comunicação de dados e Rede de computadores* de Forouzan foram fundamentais para elaborar a explicação do funcionamento de cada uma.

PAN (Personal Area Network)

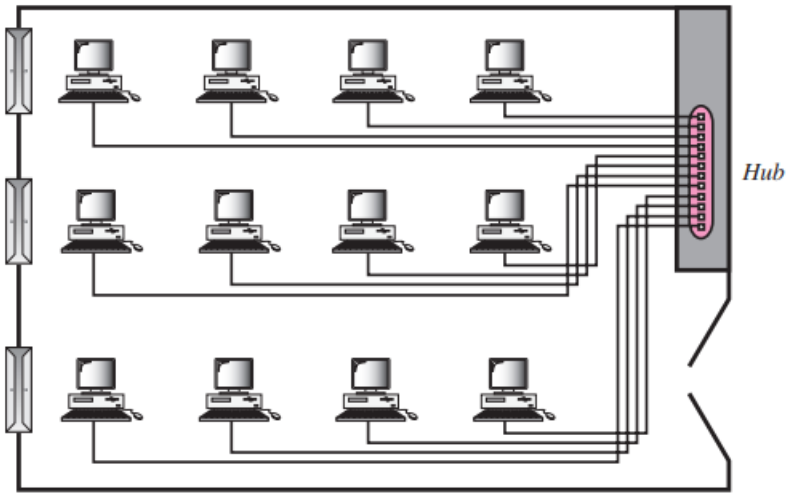
A Rede PAN, como o próprio nome diz, são redes pessoais. Seu tamanho é de apenas alguns metros e são muitas das vezes utilizadas para conectar dispositivos pessoais como *smartphones*, *tablets* ou *notebooks*. Um bom exemplo de rede PAN são os periféricos *Bluetooth*. Segundo Tanenbaum (2011) o uso deste recurso facilita a conexão por conta da ausência de cabos, com isto, aparentando uma grande vantagem na operação para os usuários.



FONTE: TANENBAUM (2011, p.11) Figura 1.5 Configuração de rede pessoal Bluetooth.

LAN (Local Area Network)

A rede LAN é uma rede local de tamanho menor, como: casas, escritórios, ou uma pequena fábrica. Este tipo de rede normalmente é muito utilizada para conectar computadores pessoais e eletrônicos (televisores ou impressoras) nas quais os mesmos trocam informações e compartilhem recursos. Conforme Forouzan (2010) um exemplo comum desta rede é ‘’ [...] encontrado em diversos ambientes empresariais, interliga um grupo de trabalho de computadores com tarefas relacionadas, como estações de trabalho da engenharia ou PCs da contabilidade’’. (FOROUZAN, 2010, p.14)



FONTE: FOROUZAN (2010, p.14) Figura 1.10 LAN isolada conectando 12 computadores a um hub em um gabinete.

MAN (Metropolitan Area Network)

A rede MAN é uma rede metropolitana maior que a rede CAN[1], mas em comparação com a rede WAN[2] é menor. As MANs têm o tamanho proporcional de uma cidade ou de um campus. Um exemplo de rede MAN é uma empresa que possui dois escritórios na mesma cidade, mas quer mantê-los interligados, desta forma eles a utilizam. Tanenbaum (2011) exemplifica que a rede de televisão a cabo comporta um sistema da rede MAN.

De acordo com o autor:

> [...] Esses sistemas cresceram a partir de antigos sistemas de antenas comunitárias usadas em áreas com fraca recepção do sinal de televisão pelo ar. Nesses primeiros sistemas, uma grande antena era colocada no alto de colina próxima e o sinal era, então, conduzido até as casas dos assinantes. (TANENBAUM, 2011, p.14)

Topologia de Rede

O termo topologia é utilizado no meio tecnológico para referir-se a forma como é feita a estruturação de uma rede de computadores. Ela se torna necessária quando há vários computadores conectados em uma mesma rede. Forounzan (2010) explica que uma topologia física é a maneira como uma rede é organizada fisicamente. Enquanto isso a topologia lógica é a maneira como os dados fluem em uma rede, quando se junta uma topologia física com uma topologia lógica geramos uma topologia de rede completa.

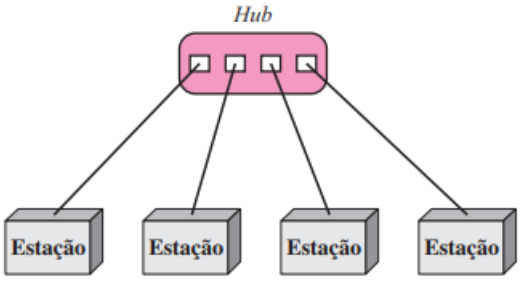
Topologia Estrela

O funcionamento da topologia de estrela é algo muito simples. A sua forma se assemelha como uma estrela com suas cinco pontas, onde cada ponta tem um dispositivo conectado a um *hub* bem ao meio da estrela. Toda informação que for enviada precisa passar pelo *hub* até chegar ao outro dispositivo, segundo Forouzan [...] os dispositivos não são ligados diretamente entre si. Diferentemente de uma topologia de malha, uma topologia estrela não permite tráfego direto entre os dispositivos.'' (FOROUZAN, 2010, p.10). Por fim, a troca de informação direta entre computadores não existe, toda informação é necessária passar primeiramente pelo *hub*.

---

[1] A rede CAN é uma rede de campus (Campus Area Network) na qual é utilizada por instuições de ensino superior na qual abrange a área total da mesma.

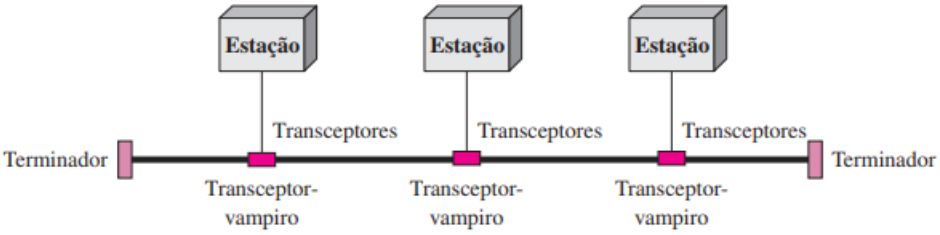
[2] A rede WAN é uma rede que abrange uma grande área geográfica. Tanenbaum (2011) exemplifica isso fazendo referência a dois escritórios que se localizam na Austrália, mas são muito distantes um do outro, porém são interconectados e conseguem trocar informações por meio de uma rede WAN.



FONTE: FOROUZAN (2010, p.44) Figura 1.6 Topologia estrela conectando quatro estações

Topologia Barramento

Também conhecida como topologia *backbone*, *bus* ou linha, como os próprios nomes sugerem, a ‘’ topologia de barramento é multiponto. Um longo cabo atua como um *backbone* que interliga todos os dispositivos da rede’’ (FOROUZAN, 2010, p.11). Em vista disso, a topologia é organizada por meio de um único cabo central que vai de uma ponta a outra da rede, na qual todos os dispositivos são conectados a esta “linha”, logo, o transporte de dados flui por meio do cabo central até chegar ao destino.



FONTE: FOROUZAN (2010, p.44) Figura 1.7 Topologia de barramento conectando três estações

Topologia Anel

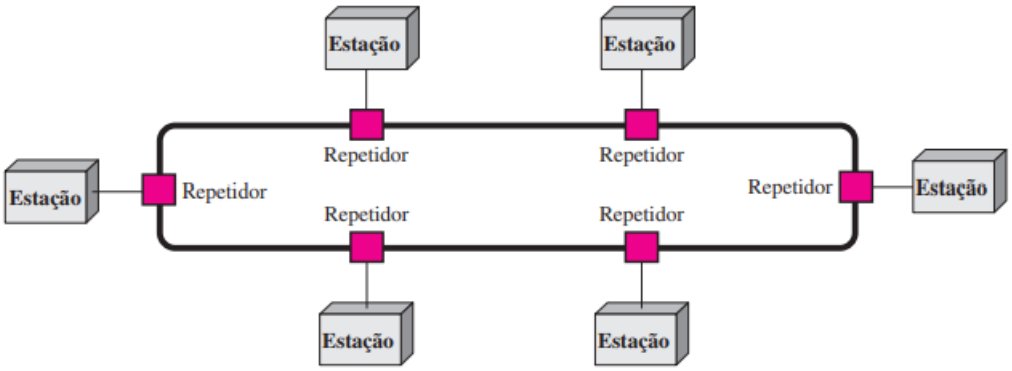
Na topologia anel todos os nós que formam o anel são feitos todos em um padrão circular. A forma com que as informações transitam é bem simples: Todas as informações passam por todos os dispositivos à medida que percorrem o anel. Quando este tipo de topologia é implementada em uma grande rede, é imprescindível o uso de repetidores para que não ocorra a perda de dados durante o tráfego.

Segundo Forouzan:

> Cada dispositivo é ligado apenas aos seus vizinhos imediatos (tanto em termos físicos como lógicos). Acrescentar ou eliminar um dispositivo exige apenas a mudança de duas conexões. Os únicos fatores limitantes são as questões relacionadas ao meio de transmissão e ao tráfego (comprimento máximo do anel e o número máximo de dispositivos). Além disso, o isolamento de falhas é

> simplificado. Em um anel, geralmente, um sinal está circulando o tempo todo. Se um dispositivo não receber um sinal dentro de um período especificado, ele pode emitir um alarme. Esse alarme alerta o operador da rede sobre o problema e sua localização. (FOROUZAN, 2010, p.12)

Em síntese, as topologias em anel podem ser configuradas como *half-duplex* na qual as informações fluem em uma direção somente ou *full-duplex* onde as mesmas podem transitar nas duas direções.



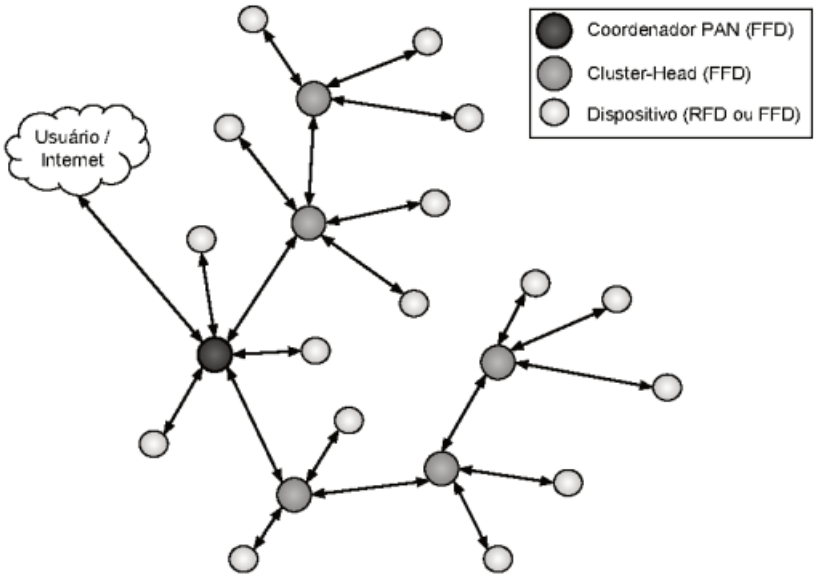
FONTE: FOROUZAN (2010, p.45) Figura 1.8 Topologia de anel conectando seis estações

Topologia Árvore

Um nó central conecta hubs secundários, que possuem uma relação pai-filho com os dispositivos. O eixo central funciona como o tronco de uma árvore. Nas junções das ramificações estão os hubs secundários ou nós de controle, e os dispositivos conectados são anexados a essas ramificações.

De acordo com o autor Siedersberger:

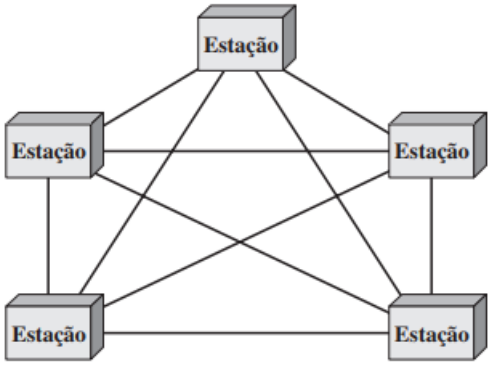
> A topologia em agrupamentos em árvore é um caso especial de par a par, onde os nodos são agrupados e coordenados de forma centralizad por coordenadores de agrupamento, conhecidos como *cluster-heads* (CHs).Os CHs são responsáveis pela formação, comunicação e sincronização de seu respectivo agrupamento, e são interconectados através de relação de pai e filho, formando uma estrutura de rede hierárquica em árvore. (Siedersberger, 2019, p.32)



FONTE: SIEDESBERGER (2019, p.32) Figura 2: Exemplo de topologia em agrupamentos em árvores.

Topologia Malha (Mesh)

Na topologia de Malha, os nós estão todos interligados No modo *full-mesh*, cada dispositivo na rede está diretamente ligado a todos os outros. Em uma topologia de malha parcial, a maioria dos dispositivos se conecta diretamente entre si. Desta maneira são oferecidos múltiplos caminhos para a entrega de dados, permitindo que os dados sejam enviados pela rota mais curta disponível. De acordo com Forouzan, a topologia de malha contém duas vantagens: A primeira é o uso de links dedicados que ‘’ [...] garante que cada conexão seja capaz de transportar seu próprio volume de dados, eliminando, portanto, os problemas de tráfego que possam ocorrer quando os links tiverem de ser compartilhados por vários dispositivos (FOROUZAN, 2010, p.10); a segunda vantagem é de que ‘’ uma topologia de malha é robusta. Se um link se tornar inutilizável, ele não afeta o sistema como um todo.’’ (FOROUZAN, 2010, p.10). Além disso, o próprio autor indica que a topologia de malha apresenta a vantagem de manter a segurança e privacidade.



FONTE: FOROUZAN (2010, p.43) Figura 1.5 Topologia de malha completamente conectada (cinco dispositivos)

3. SEGURANÇA DA INFORMAÇÃO

De acordo com Hintzbergen*, et al*. (2015) a segurança da informação se concentra em adotar práticas e tecnologias para proteger dados contra várias ameaças, como acessos não autorizados, perda de integridade e interrupções de serviços. O objetivo principal é garantir que as informações permaneçam seguras e não sejam comprometidas, o que poderia causar danos significativos a indivíduos e organizações.

Os pilares da segurança da informação são princípios fundamentais que trazem uma garantia na proteção e integridade dos dados dentro de uma empresa, dentre esses pilares, existem os fundamentais, sendo eles: Confidencialidade, Integridade e Disponibilidade (Hintzbergen, *et al.,* 2015, p. 33)

A confidencialidade, diz respeito aos limites de quem pode obter certa informação (Hintzbergen, *et al.,* 2015, p. 33). Uma empresa de tecnologia restringe o acesso a certas informações para os funcionários na parte de vendas, já os funcionários que fazem parte da segurança possuem um acesso total as informações.

A Confidencialidade garante ‘’que o nível necessário de sigilo seja aplicado em cada elemento de processamento de dados e impede a divulgação não autorizada’’ (Hintzbergen, *et al*., 2015, p.33). Esse nível de confidencialidade deve ser mantido enquanto os dados estiverem em sistemas e dispositivos na rede, durante a transmissão e até a chegada ao seu destino final.

Quando se pensa em integridade na área da segurança da informação, se refere o quanto deve estar completa a informação que é repassada ou recebida, esta, não precisa estar necessariamente correta, mas precisa estar completa.

Empresas que reforçam a integridade dos seus sistemas, trazem uma maior segurança para o seu sistema contra atacantes ou erros de usuários, para que os mesmos não comprometam a integridade do sistema ou dos dados. De acordo com Hintzbergen *et al*. (2018) Quando um invasor penetra no seu sistema e insere um cavalo de troia, ou um vírus a integridade do seu sistema está comprometida. Isso pode, consequentemente, comprometer a integridade das informações armazenadas no sistema, resultando em corrupção, modificação maliciosa ou substituição de dados por informações incorretas. Para mitigar essas ameaças, é essencial implementar controles de acesso rigorosos, sistemas de

detecção de intrusão e técnicas de *hashing.*

Conforme Hintzbergen *et al.* (2015) em disponibilidade há três características: A primeira se denomina como oportunidade na qual a informação sempre estará disponibilizada quando houver momentos necessários; Em segundo, a continuidade que mesmo havendo casos de falha a equipe consegue realizar a continuidade do trabalho; Em terceiro – por último – a robustez cujo sistema tem capacidade de suportar toda equipe trabalhando.

Hintzbergen *et al.* exemplifica dizendo que “tanto uma falha de disco quanto um ataque de negação de serviço causam violação da disponibilidade. Qualquer atraso que exceda o nível de serviço esperado para um sistema pode ser descrito como uma violação da disponibilidade” (HINTEZBERGEN, 2015, p.36).

Conforme Hintzbergen et al. (2015) descreve, a disponibilidade do sistema pode ser comprometida por falhas em dispositivos ou softwares. Dispositivos de backup devem estar prontos para substituir o quanto antes os sistemas que são essenciais, e é necessário que aqueles que são capacitados estejam disponíveis para realizar os ajustes necessários e restaurar o sistema. Fatores ambientais como calor, frio, umidade, eletricidade estática e contaminantes também podem impactar o sistema. Portanto, os sistemas devem ser protegidos contra esses fatores, devidamente aterrados e monitorados com atenção.

4. PENTESTING

4.1. FINALIDADE DE UM PENTEST

Pentest (teste de invasão) é algo muito importante, onde profissionais da área de segurança da informação simulam ataques em sistemas para encontrar vulnerabilidades.

O intuito de efetuar esses testes é identificar essas vulnerabilidades o quanto antes e corrigi-las, para evitar que *hackers* mal-intencionados tomem vantagem e venham roubar informações importantes ou até mesmo extorquir a empresa em troca dessas informações.

4.2. TIPOS DE PENTEST

Nos dias atuais, existem três tipos de Pentest, cada um trazendo um tipo de análise e uma forma de abordar o sistema a qual será testado.

4.2.1. Black Box

Neste modelo, pode-se ilustrar usando o próprio nome, uma espécie de “caixa preta” onde o testador tem pouco ou nenhum conhecimento prévio do sistema a ser invadido, pois a empresa a qual está sendo feito o *pentest* optou por não fornecer informações internas do sistema. A intenção do *black box* é imitar um atacante que realiza um *exploit* sem nenhuma informação de como funciona o sistema atacado, trazendo assim uma simulação mais realista sobre o que o invasor poderia descobrir e explorar, diante disso, Moreno (2015) demonstra um exemplo recorrente sobre o *black box,* como o autor afirma ‘’ Um exemplo clássico de cenário de black-box é quando um script kid encontra um site na internet que sofre de algum bug conhecido, como SQL Injection, e por meio de um programa especial consegue acesso ao painel administrativo do site’’.(MORENO, 2015, p. 54)

4.2.2. White Box

Em contra partida, em relação ao *Black Box*, Segundo Moreno (2015) no *pentest* White Box ‘’o auditor de segurança terá total conhecimento da infraestrutura da rede testada: diagrama e mapeamento da rede, endereços IP usados, firewalls, código-fonte das aplicações etc’’. (MORENO, 2015, p. 55). Em decorrência disto é efetuada uma auditoria de segurança interna mais profunda, na qual o testador tem acesso a diagramas de rede, códigos-fonte e outras informações importantes, devido a está quantia massiva de informações importantes fornecidas esse teste resulta uma análise mais detalhada das vulnerabilidades.

4.2.3. Grey Box

Enquanto isso, o *gray box* é uma espécie de mistura dos anteriores – *black box* e *white box* - na qual tem o objetivo minimamente diferenciado, conforme Monteiro (2015) o *gray box* é ‘’[...] um sistema de web em que o auditor terá acesso parcial às informações’’ (MORENO, 2015, p. 56) - tendo acesso apenas ao usuário e uma senha, no entanto, sem acesso ao código-fonte – Sendo assim simulando uma pessoa interna que possui um nível de acesso e conhecimento do sistema, neste tipo de modelo é avaliado o quão bem um sistema suporta esses ataques internos.

5. MATERIAIS E MÉTODOS

Neste artigo é apresentado uma metodologia de exploração de vulnerabilidade que ocorre na porta “445” dos sistemas operacionais Microsoft. Neste sentido foi utilizando a ferramenta *Metasploits Framework* onde todos os testes foram efetuados em um ambiente controlado por meio de simulação, logo, o teste foi seguro e não afetou o sistema do computador. Os recursos utilizados para realizar essa prática são: Virtual Box, sistemas operacionais *Kali Linux* e Windows XP. O método utilizado fundamenta-se em usar uma ferramenta de virtualização Virtual Box para emular um ambiente Virtual do Kali Linux (Invasor) Windows Xp (Sistema Alvo).

> O Oracle VM VirtualBox permite que você execute mais de um SO ao mesmo tempo. Dessa forma, você pode executar software escrito para um SO em outro, como software Windows no Linux ou Mac, sem precisar reinicializar para usá-lo. Como você pode configurar quais tipos de *hardware virtual* devem ser apresentados a cada SO, você pode instalar um SO antigo, como DOS ou OS/2, mesmo que o hardware do seu computador real não seja mais suportado por esse SO. (ORACLE VM, 2024, p.2)

Segundo a documentação do Kali Linux (2024) é um sistema operacional distribuído pela Linux, seu código é aberto e baseado em Debian, o que permite que os usuários efetuem testes de invasão.

O Virtual box possui uma opção de configuração de *hardware* para cada máquina virtual, para preparar as máquinas que vão ser utilizadas é necessário selecionar a que irá configurar e em seguida apertar em “Configurações”, desta maneira algumas opções serão mostradas como, Geral, Sistema, Monitor, Armazenamento, Áudio, **Rede**, Portas Seriais, USB, Pastas Compartilhadas, Interface de Usuário, a que nos importa é a opção “Rede”. Para se configurar a rede do sistema que irá realizar o ataque, é necessário a configuração de duas placas de rede, uma como rede interna (intnet) e outra como NAT (*Network Adress Translation*). Na máquina alvo na qual possui o Windows XP, irá ser feita a configuração da placa de rede somente como rede interna(intnet). Para explicar esses conceitos de “NAT” e “Rede Interna”, pode-se exemplificar por meio de duas cúpulas, na rede interna a comunicação é feita somente entre as máquinas, porém impede o acesso a rede externa, como acessar a Internet. Por outro lado na rede NAT, é utilizada somente para acesso a rede externa, mas impede que as maquinas se comuniquem na mesma rede local.

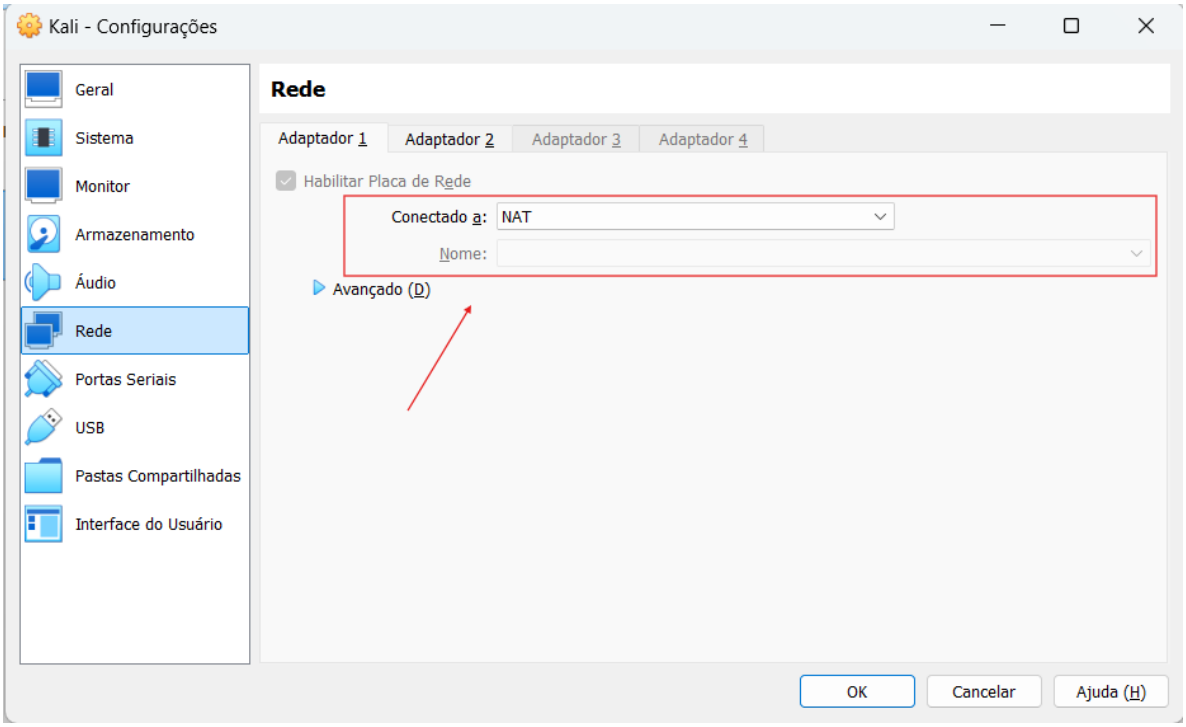


Figura 1 – Configuração de placa rede NAT do Kali Linux.

Fonte: do autor

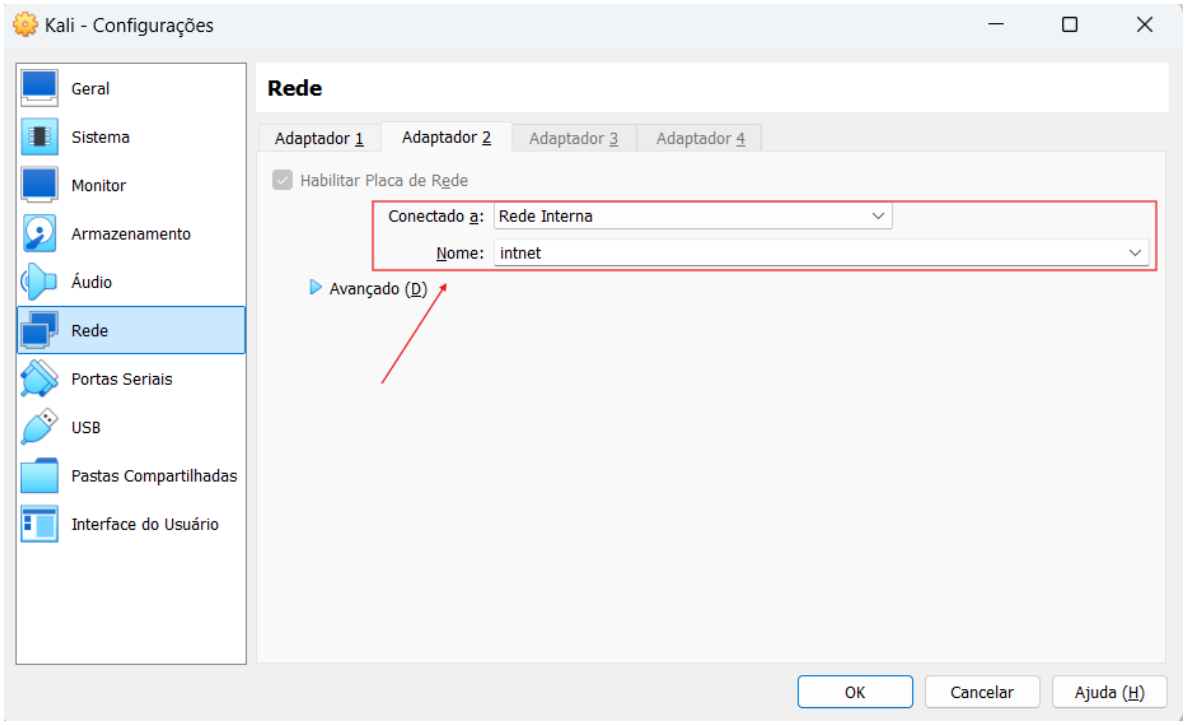


Figura 2 – Configuração de placa rede interna do Kali Linux.

Fonte: do autor

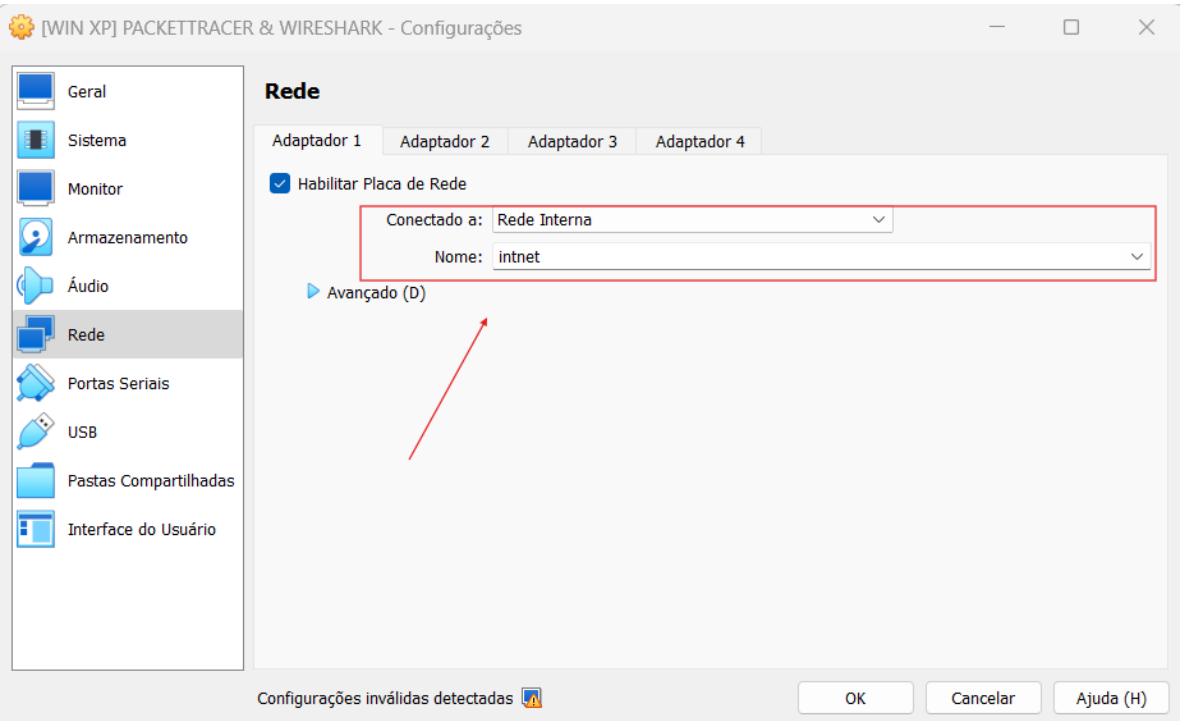


Figura 3 – Configuração de placa rede interna do Windos XP.

Fonte: do autor

Antes de iniciar a prática, na qual o sistema operacional Windows XP será analisado, é necessário configurar o Endereço IP, Máscara de sub-rede e Gateway padrão, além de configurar o endereço do servidor DNS. Isso é feito indo em “Status de Conexão local” depois “Propriedades” em seguida “Protocolo TCP/IP” e “Propriedades” Novamente, desta maneira chega-se onde é necessário para configuração.

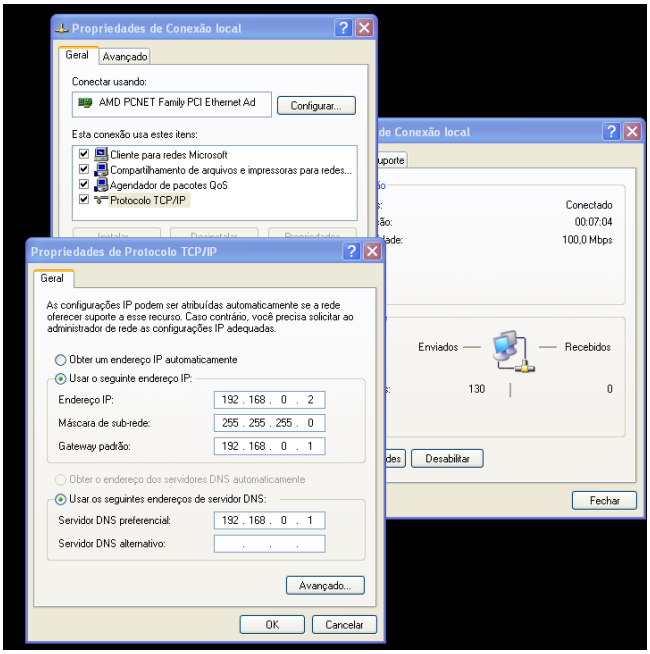


Figura 4 – Configuração dos endereços.

Fonte: do autor

No Sistema Operacional Kali Linux é necessário atualizar manter o sistema atualizado, desta maneira os seus aplicativos e *frameworks* são atualizados, fazendo com o que trazendo assim uma maior segurança nos testes.

Para configurar o Kali Linux, deve-se entrar como super usuário para ter total acesso e configurar o sistema de forma livre. Em seguida é verificado o status da interface de rede, como mostrado na Figura 5, onde é possível observar que a interface de rede "*eth1"* possui a configuração de acesso a Internet e a interface de rede "*eth0"* tem acesso a rede interna.

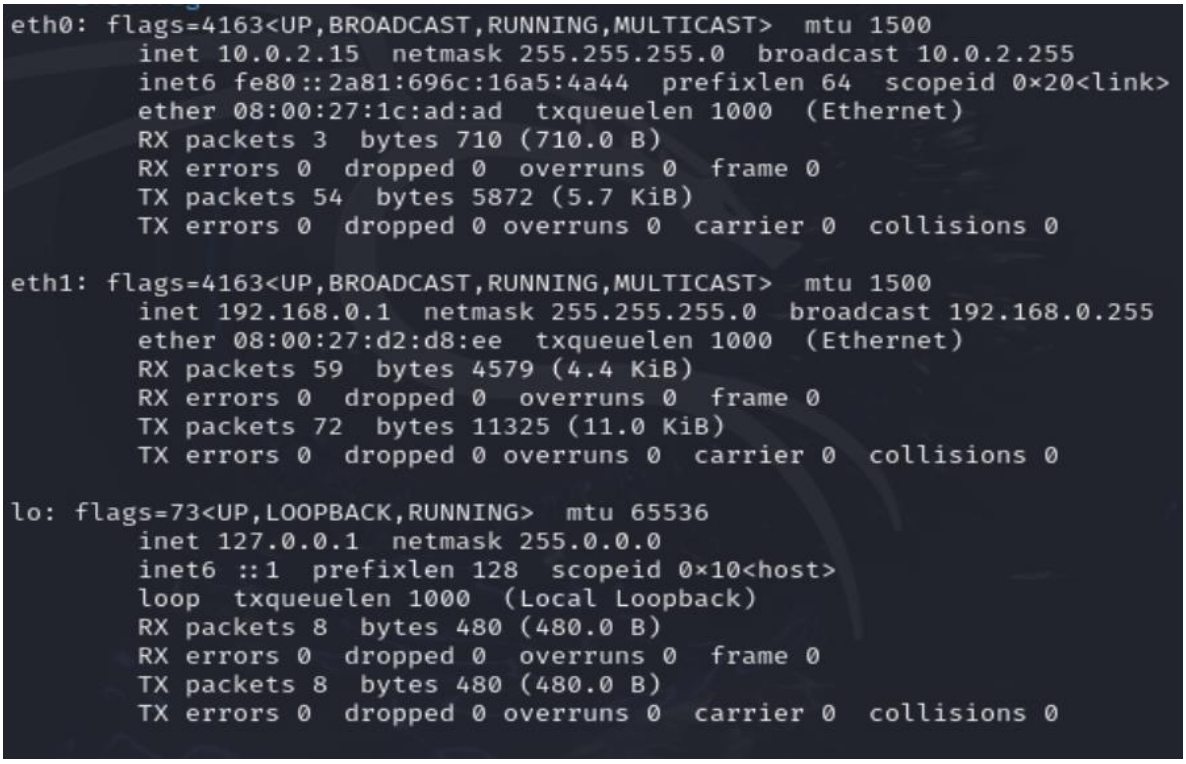


Figura 5 – Verificando status da rede do Kali

Fonte: do autor

Em caso da verificação do status tiver algum problema, onde o endereço IP da interface “eth1” não estiver configurado é necessário editar a interface de forma manual. Deve-se fazer a configuração da rede por meio dos seguintes comandos: “*ifconfig eth1 down*”, conforme ilustra a figura 6. Em seguida digitar o comando “*ifconfig eth1 192.168.0.1”* *(*Figura 7*). D*esta maneira o próprio kali já irá colocar a mascara de rede e o broadcast.

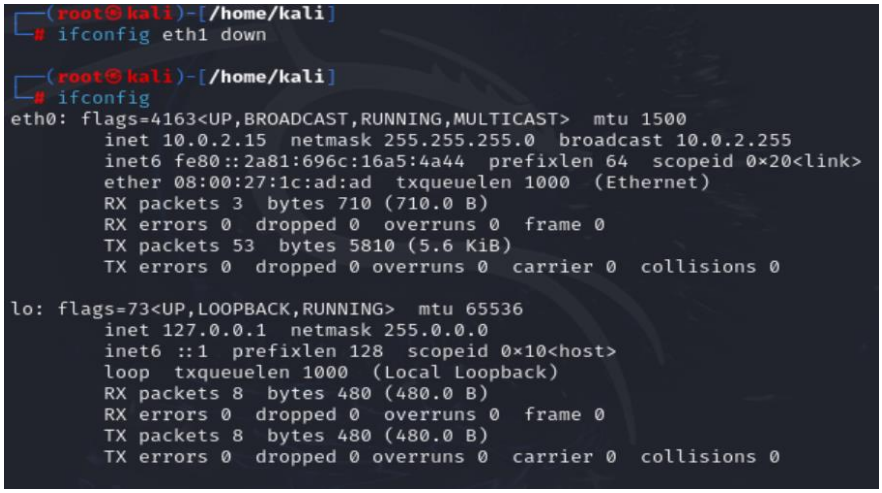


Figura 6 – Configurando Manualmente a Rede.

Fonte: do autor

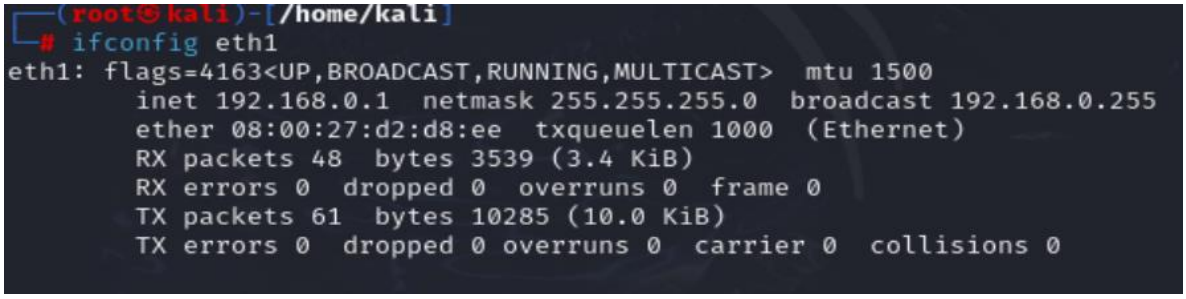


Figura 7 – Inserindo IP na rede eth1.

Fonte: do autor

Após concluir a configuração das duas máquinas virtuais, é importante testar a comunicação entre elas. Para isso, utilize o comando “ping”, seguido pelo endereço IP da máquina com a qual se deseja estabelecer a conexão. Por exemplo, no terminal do Kali coloca-se o ip da máquina a ser invadida para saber se a mesma possui conexão com o Kali como referido na Figura 8.

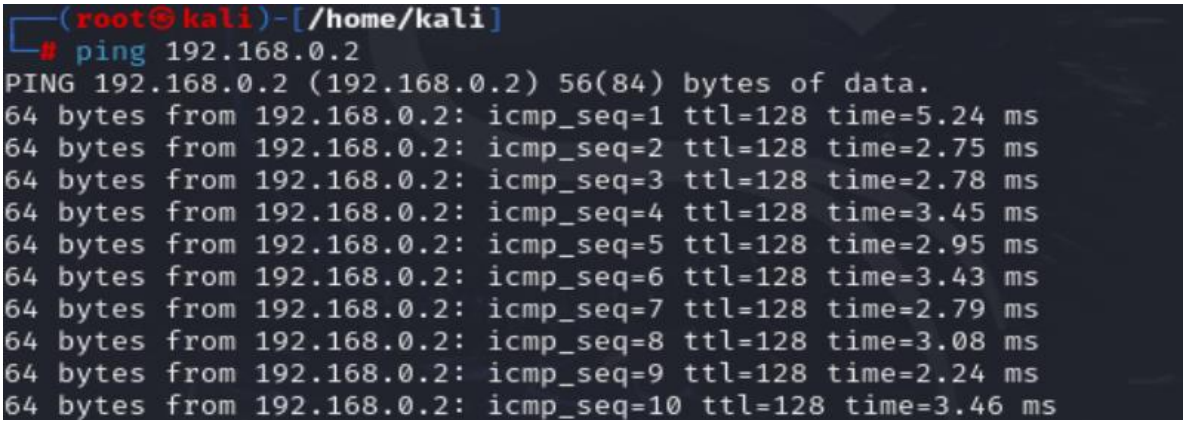


Figura 8 – Pingando o Windows xp.

Fonte: do autor

Após a confirmação que se possui uma conexão com a máquina a ser invadida e o Kali, é efetuada uma varredura utilizando o comando “nmap 192.168.0.2”, conforme ilustra a figura 9 que é responsável por verificar todas as portas e mostrar quais estão abertas e prontas para serem invadidas.

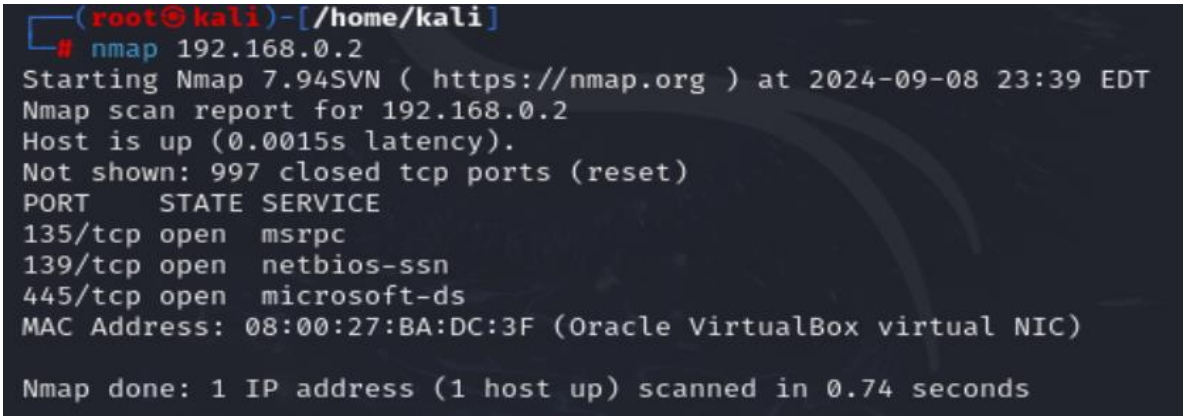


Figura 9 – Varredura de Portas utilizando nmap.

Fonte: do autor

Para realizar o teste de vulnerabilidade proposto neste trabalho, foi utilizada a ferramenta Metasploit Framework. Para iniciá-la, é necessário estar logado como superusuário no sistema Kali e, em seguida, executar o comando “msfconsole”. Isso abrirá a interface do Metasploit. Como observado na Figura 10.

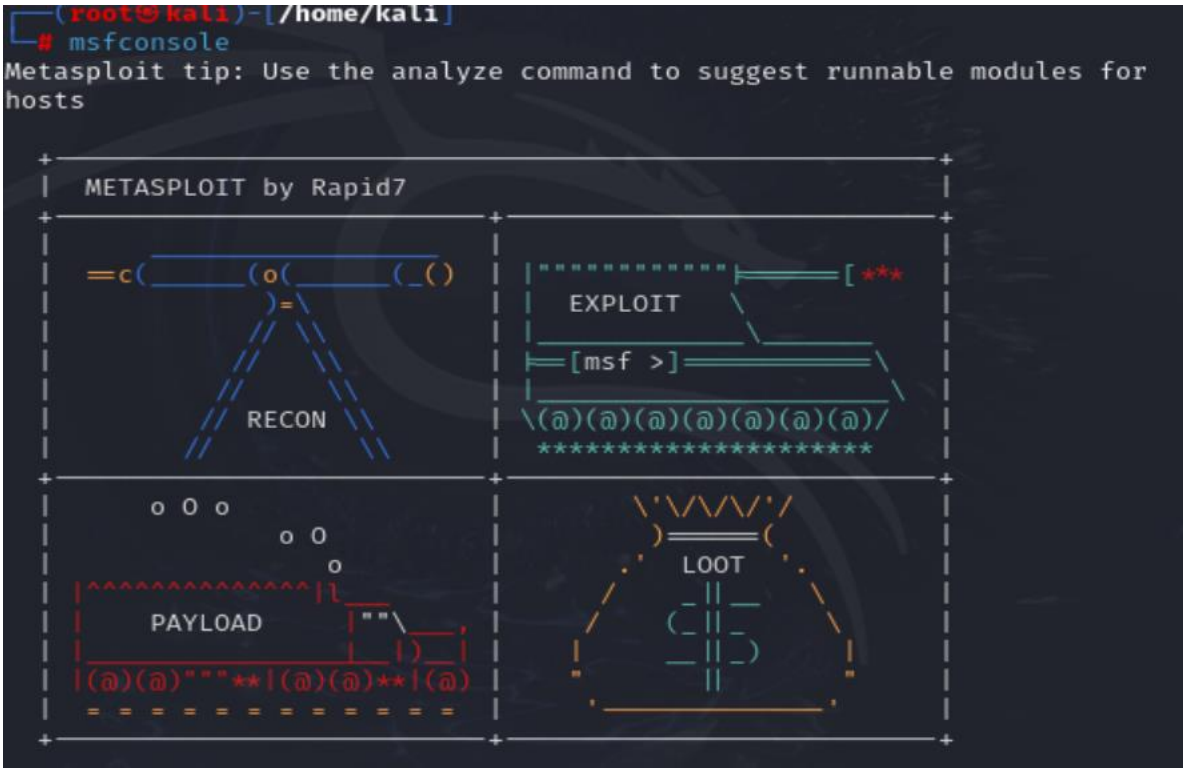
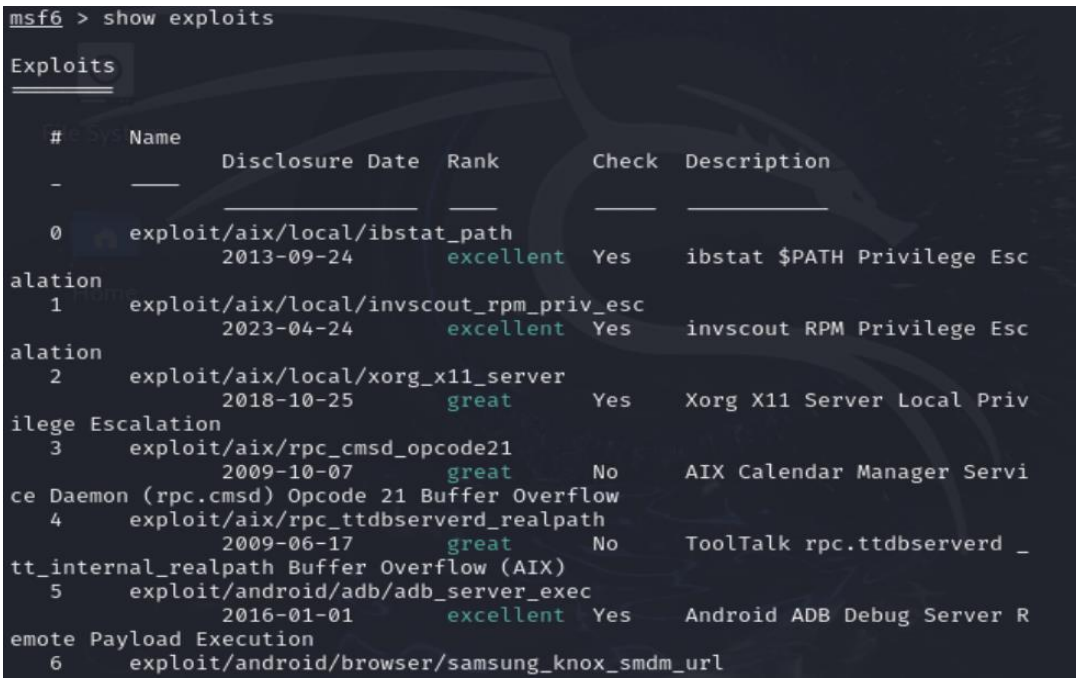


Figura 10 – Iniciando metasploit.

Fonte: do autor

Após isso será listado todos os *exploits* por meio do comando “*show exploits*” (Figura 11) na qual será mostrada uma infinita gama de *exploits* a serem utilizados, porém o *exploit*

que utilizado neste teste é descrito por meio do seguinte comando "*use exploit/windows/smb/ms8_067_netapi*", desta maneira ele já seta que iremos utilizar este *exploit* como observado na Figura 12.



. Figura 11 – Mostrando os exploits

Fonte: do autor

Figura 12 – Setando o exploit a ser usado.

Fonte: do autor

O próximo passo agora, é escolher um *Payload*, que seja compatível com o *exploit* que está sendo utilizado. No caso será utilizado o Payload tcp meterpreter conforme ilustra a figura 13.

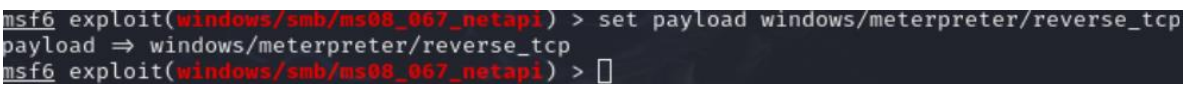


Figura 13 – Setando o payload compatível.

Fonte: do autor

Em seguida é feita a configuração da variável LHOST (Kali Linux), o IP a ser coloca vai ser o ip padrão "192.168.0.1", depois se faz a mesma coisa com a RHOST que é

configurada com o IP da máquina a ser invadida, IP esse que é “192.168.0.2” o mesmo ip que foi testado a conexão com o ping, como é descrito na Figura 14.

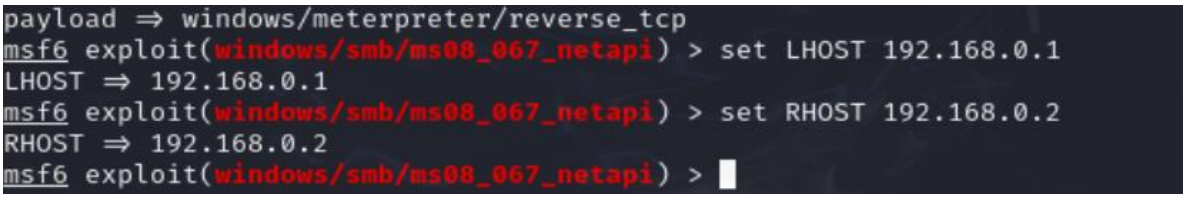


Figura 14 – Configurando LHOST e RHOST.

Fonte: do autor

Agora que tudo está pronto e configurado será realizado o ataque, para isso basta digitar o comando “*exploit*”, conforme demonstra a figura 15, após isso já se possui acesso total a maquina atacada, sendo assim é possível fazer o que quiser.

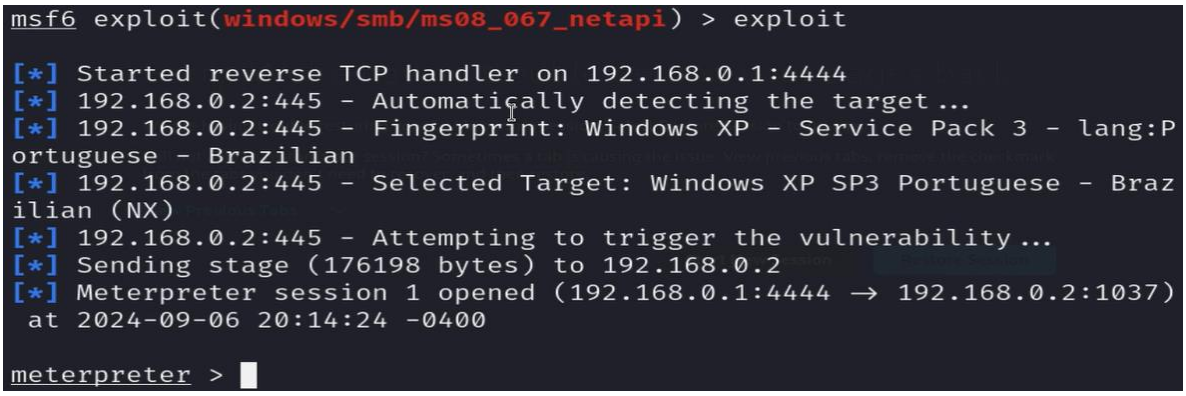


Figura 13 – Invasão Sucessida

Fonte: do autor

Para ilustrar as figuras seguir descrevem a invasão e o acesso do diretório “C:/Windows/system32” e criação do diretório chamado “terror”. Na qual mostra o qual poderoso pode ser esta invasão, seria possível até mesmo apagar a system32 do suposto computador o que prejudicaria totalmente a maquina a tornando impossível de ser utilizada.

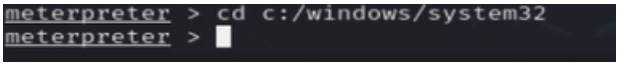


Figura 14 – Acessando o diretório

Fonte: do autor

Figura 15 – Criando o diretório “terror”

Fonte: do autor

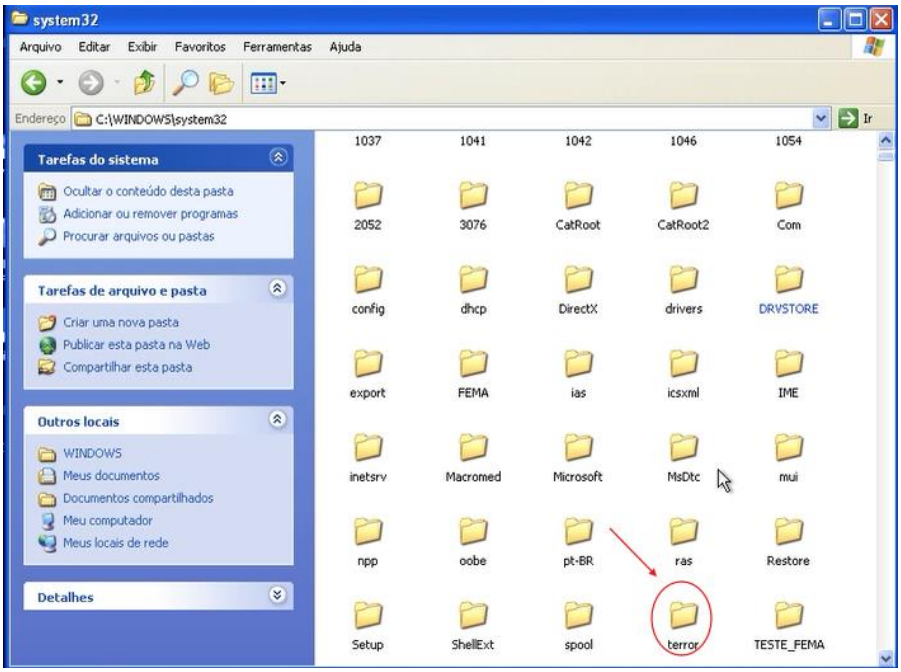


Figura 16 – Constatação da criação do diretório “terror”

Fonte: do autor

6. CONCLUSÃO

Este estudo teve como foco investigar as vulnerabilidades em sistemas operacionais por meio de testes de invasão (pentesting) em ambientes controlados. Utilizando ferramentas como o Metasploit Framework, foram identificadas fragilidades nos sistemas analisados, ressaltando a importância de testes de segurança contínuos para assegurar a integridade e confiabilidade dos sistemas.

Observou-se que até mesmo sistemas amplamente utilizados, como o Windows XP, possuem vulnerabilidades que podem ser exploradas de forma relativamente simples por hackers mal-intencionados, caso não sejam corrigidas. Os testes realizados permitiram o acesso a arquivos críticos e a manipulação significativa do sistema, evidenciando a gravidade das falhas encontradas.

Portanto, este trabalho reforça a necessidade de implementar políticas de segurança cibernética mais rigorosas e de realizar testes de vulnerabilidade regularmente, especialmente em sistemas utilizados por instituições educacionais, que são frequentemente alvos de ataques. Espera-se que este estudo incentive outras instituições de ensino a refletirem sobre a segurança de seus sistemas e a adotarem medidas preventivas para mitigar os riscos identificados.

A continuidade deste tipo de pesquisa, com a aplicação de testes em sistemas operacionais mais recentes e em ambientes produtivos, poderá contribuir significativamente para o aprimoramento das práticas de segurança da informação, minimizando os riscos de ataques cibernéticos e garantindo a proteção de dados sensíveis.

7. REFERÊNCIA

ALMEIDA JR., José Augusto, **Pentest em aplicações web**: Avalie a segurança contra ataques web com testes de invasão no Kali Lunix.São Paulo:Casa do Código,2021.

WEIDMAN, GEORGIA. **Testes de Invasão**: Uma introdução prática ao hacking. Novatec Editora Ltda. São Paulo, 2014.

OLIVEIRA, Danilo; LIMA, Bruno Inacio. Pentest: o que é e para que serve o teste de segurança de rede de sistema. Disponível em: https://olhardigital.com.br/2023/08/23/seguranca/pentest-o-que-e-e-para-que-serve-o-teste-de-seguranca-de-rede-e-sistema/#:~:text=No%20entanto%2C%20ao%20contr%C3%A1rio%20de,sejam%20exploradas%20por%20criminosos%20cibern%C3%A9ticos. Acesso em: 27 de março. 2024.

TANENBAUM**,** ANDREW S. e WETHERALL David J.**. Redes de Computadores***.* 5.ed. Pearson, 2011.

MORENO, Daniel. **Introdução ao Pentest**. [*S. l.*]: Novatec, 2015.

SIEDERSBERGER, Daniel. **Abordagens para Formação de topologia em agrupamentos em árvore para RSSF de larga escala**. p.118. Dissertação de Mestrado. Universidade Federal de Santa Catarina, Centro Tecnológico, Programa de Pós Graduação em Engenharia de Automação e Sistemas, Florianópolis, 2019.

HINTZBERGEN, Jule, HINTZBERGEN, Kess, SMULDERS, André, BAARS, Hans. **Fundamentos de Segurança da Informação**: Com base na ISO 27001 e na ISSO 27002. 3.ed. Brasport Livros e Multimídia. 2015.

FOUROUZAN, Behrouz. Comunicação de Dados e Redes de Computadores. 4.ed. AMG Editora. 2010.

ORACLE. User Manual. Disponível em: https://download.virtualbox.org/virtualbox/UserManual.pdf. Acesso em: 07 de setembro. 2024.

Kali Linux. What is Kali Linux?. Disponível em: https://www.kali.org/docs/introduction/what-is-kali-linux/#about-kali-linux. Acesso em: 07 de setembro. 2024.