PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA POLITÉCNICA E DE ARTES
CURSO DE ENGENHARIA DE COMPUTAÇÃO

ANÁLISE DE PENTEST COMO FERRAMENTA PARA SEGURANÇA DA INFORMAÇÃO

DOUGLAS MARTINS FERREIRA

GOIÂNIA, GO
2024

DOUGLAS MARTINS FERREIRA

ANÁLISE DE PENTEST COMO FERRAMENTA PARA SEGURANÇA DA INFORMAÇÃO

Trabalho de Conclusão de Curso apresentado à Escola Politécnica e de Artes, da Pontifícia Universidade Católica de Goiás, referente a parte dos requisitos para a obtenção do título de Bacharel em Engenharia de Computação.

Orientador(a): Prof. Me. Cláudio Martins Garcia

GOIÂNIA, GO
2024

Dedicatória

Dedico este projeto à minha família e amigos que sempre estiveram presentes direta ou indiretamente em todos os momentos de minha formação.

A todos os meus professores da graduação, que foram de fundamental importância na construção da minha vida profissional.

Agradecimentos

A conclusão deste trabalho só foi possível graças ao apoio incondicional de minha família, que sempre esteve ao meu lado nos momentos mais desafiadores. Aos meus pais, pela paciência, amor e incentivo constante, e ao meu irmão, por compreenderem minhas ausências e me motivarem a seguir em frente. Sou profundamente grato por terem acreditado em mim e em minha capacidade de alcançar esse objetivo, mesmo quando eu mesmo duvidei. Esse suporte foi essencial para que eu pudesse superar cada obstáculo ao longo dessa jornada.

Aos meus amigos, agradeço pela parceria, pelas conversas animadoras e pelo conforto em momentos de tensão, tornando o percurso mais leve e agradável. Aos professores, expresso minha imensa gratidão por compartilharem seu conhecimento, orientações e palavras de incentivo, fundamentais para o desenvolvimento deste trabalho. Sua dedicação e paciência foram essenciais para que eu pudesse crescer academicamente e pessoalmente. A todos que, direta ou indiretamente, contribuíram para essa conquista, o meu mais sincero obrigado.

"O homem não é nada além
daquilo que a educação faz dele."
(Kant)

Resumo

Este trabalho tem como objetivo apresentar o cenário da segurança da informação, descrevendo suas bases e fundamentos, com foco principal em pentest. Serão abordados os conceitos, metodologias e ferramentas utilizadas durante o procedimento. Neste trabalho, também são apresentadas as limitações legais envolvidas nesse processo, que consiste na simulação de um ataque. O desenvolvimento do trabalho será baseado na análise dos métodos e das diversas ferramentas utilizadas na realização do pentest.

Com a digitalização da informação, o pentest se mostra como uma ferramenta essencial para a validação dos processos de segurança já implementados, averiguando a eficácia e as vulnerabilidades que possam existir.

O pentest caracteriza-se como um processo preventivo que busca identificar as vulnerabilidades do alvo por meio de uma simulação de ataque, tendo como objetivo principal a identificação e análise dessas vulnerabilidades. Durante o procedimento, são gerados relatórios para cada etapa, que, ao final, comporão o relatório final, descrevendo o que foi identificado e propondo as soluções a serem aplicadas para sua resolução.

No decorrer do trabalho, serão apresentados e descritos os procedimentos e métodos utilizados na realização do pentest, assim como uma descrição das ferramentas e funcionalidades presentes em cada uma delas. Além disso, serão apresentados os resultados obtidos por meio da aplicação prática dos conceitos e técnicas descritos neste trabalho.

Palavras-chave: Segurança da informação, pentest, ataques, ferramentas, segurança.

Abstract

This work aims to present the information security landscape, describing its foundations and principles, with a primary focus on penetration testing (pentest). It will cover the concepts, methodologies, and tools used during the process. This study also addresses the legal limitations involved in this process, which consists of simulating an attack. The development of this work will be based on the analysis of the methods and various tools used in conducting pentests.

With the digitization of information, pentesting proves to be an essential tool for validating already implemented security processes, assessing their effectiveness and identifying potential vulnerabilities.

Pentesting is characterized as a preventive process that seeks to identify the target's vulnerabilities through an attack simulation, with the main objective of identifying and analyzing these weaknesses. During the procedure, reports are generated for each phase, which will ultimately compose the final report, describing the identified issues and proposing solutions to address them.

Throughout this work, the procedures and methods used in performing pentests will be presented and described, along with a description of the tools and functionalities of each. Additionally, the results obtained through the practical application of the concepts and techniques described in this study will also be presented.

Keywords: Information security, penetration testing, attacks, tools, security.

Lista de Figuras

Lista de abreviaturas e siglas

CID - confidencialidade, Integridade, Disponibilidade

DDoS - Distributed Denial of Service

DNS - Domain Name System

DoS - Denial of Service

IBGE - Instituto Brasileiro de Geografia e Estatística

IDS - Intrusion Detection System

IP - Internet Protocol

IPS - Intrusion Prevention System

ISO - International Organization for Standardization

ISSAF - Information Systems Security Assessment Framework

LGPD - Lei Geral de Proteção de Dados

OSSTMM - Open-Source Security Testing Methodology Manual

OWASP - Open Web Application Security Project

PTES - Padrão de Execução de Teste de Penetração

PTW - Pyshkin, Tews, Weinmann

Pentest - Penetration testing

RaaS - Ransomware-as-a-Service

SEToolkit - Social Engineer Toolkit

SO - Sistema Operacional

TI - Tecnologia da Informação

VPN - virtual private network

Sumário

1 INTRODUÇÃO

Com o passar dos anos e o desenvolvimento da tecnologia, a forma como as informações são armazenadas mudou completamente. O que antes era armazenado em pilhas de papéis e arquivos com centenas, talvez milhares, de pastas agora pode ser guardado no bolso de qualquer pessoa.

A digitalização da informação certamente trouxe uma mudança completa no que diz respeito ao armazenamento de dados. Porém, essa facilidade trouxe consigo a necessidade de garantir a segurança dessas informações. No mundo atual, a informação possui um valor inestimável. Dados pessoais, informações internas, planejamentos futuros, informações governamentais são exemplos de dados armazenados em meios digitais que precisam de proteção.

Para garantir a segurança desses dados, é necessário aplicar técnicas de defesa e métodos de segurança digital. Essa defesa é baseada em testes de segurança regulares que identificam e solucionam possíveis vulnerabilidades, tornando, assim, os sistemas de segurança mais confiáveis.

Dentre essas técnicas e métodos, destaca-se o teste de penetração (Pentest), um conjunto de testes de vulnerabilidade implementados para fortalecer a segurança dos sistemas de armazenamento de informações e que será abordado como o tópico principal deste trabalho.

1.1 Objetivos

A seguir estão dispostos os objetivos almejados durante a execução deste trabalho.

1.1.1 Objetivo Geral

O objetivo geral deste trabalho é introduzir a área de conhecimento da segurança da informação, tendo como foco principal a utilização de pentest como ferramenta para garantir a segurança de redes e dados.

A análise será focada na identificação dos métodos e ferramentas utilizados e no entendimento de como se dá o processo de pentest.

Por fim, obter aprofundamento técnico sobre pentest através da aplicação prática dos conceitos analisados.

1.1.2 Objetivos Específicos

- Contextualizar a segurança da informação.
- Introduzir os conceitos e definições básicos sobre segurança da informação.
- Apresentar o conceito e definição de pentest como técnica de segurança.
- Apresentar as metodologias e ferramentas utilizadas no procedimento.
- Aprofundar na utilização das ferramentas e metodologias apresentadas.

1.2 Justificativa

Com o avanço da tecnologia de armazenamento de dados e a frequente digitalização da informação, vem se tornando uma necessidade e uma obrigação legal a proteção e manutenção destes dados e informações. A utilização de técnicas de defesa e mitigação de riscos se tornou uma necessidade básica quando se trata da manipulação e conservação de dados.

Com isso em vista este trabalho visa expor a importância do pentest como ferramenta de segurança e explorar suas metodologias e ferramentas.

1.3 Metodologia

Quanto a sua natureza, este trabalho é um resumo de assunto, buscando sintetizar a área de conhecimento em questão para o âmbito acadêmico. O intuito dessa pesquisa nesse presente trabalho é aprofundar conceitos que já foram estudados e aperfeiçoar conceitos pouco explorados. (WAZLAWICK, 2014).

Quanto aos objetivos é uma pesquisa descritiva, pois serão analisados dados e informações sobre pentest com o objetivo de adquirir maior entendimento sobre eles. (WAZLAWICK, 2014).

Quanto aos seus procedimentos técnicos é classificado por uma pesquisa bibliográfica (WAZLAWICK, 2014).

Primeiramente será realizada uma pesquisa bibliográfica. Esta pesquisa se caracteriza como o estudo de um conjunto de conhecimentos e informações que estão presentes em diversas obras já existentes e a partir desses conhecimentos conduzir o pesquisador na busca por novos conhecimentos. Ela se fundamenta na leitura de obras já publicadas servindo como base para outras pesquisas (FACHIN,2017).

2 REFERENCIAL TEÓRICO

A fim de apresentar e introduzir os conceitos e definições abordados neste trabalho estão dispostos abaixo os textos utilizados como referência para o mesmo.

2.1 Segurança da informação

A maneira como a informação se propaga pelo mundo mudou drasticamente nos últimos séculos, o envio de cartas que poderiam levar dias ou até mesmo meses para serem entregues para enviar mensagens de texto instantâneas via internet que são entregues no mesmo segundo em que são enviadas.

Da mesma forma, a maneira como se armazena informação também se modificou. O que antes era armazenado em pilhas de papéis e pastas agora pode ser armazenado no bolso de qualquer pessoa comum. A digitalização da informação foi certamente um dos maiores avanços conquistados pela humanidade.

O processo de digitalização da informação fez surgir a necessidade de garantir a segurança das informações. O que antes só podia ser acessado fisicamente agora pode ser acessado remotamente com a criação das redes de computadores e a conexão à internet.

Para garantir que estas informações permanecem seguras e que criminosos e pessoas mal intencionadas não tenham acesso a esses dados, desenvolve-se a área conhecida como segurança da informação.

A Segurança da Informação como o próprio nome sugere é a área responsável pela proteção de informações de computadores e outros dispositivos tanto de usuários comuns quanto de organizações. Esta área de atuação visa a proteção das informações contra criminosos utilizando normas padronizadas internacionalmente e nacionalmente para garantir a segurança de computadores, celulares, câmeras de vigilância, redes de computadores etc.

Mas o que de fato é informação? Segundo Maurício Rocha Lyra (2015) informação pode ser definida da seguinte forma:

> “De uma forma simples e direta, a Informação pode ser definida por um conjunto de dados tratados e organizados de tal maneira que tragam algum significado ou sentido dentro de um dado contexto.”

Tendo em vista essa definição podemos concluir que informação é um conjunto de dados organizados de forma a fazer sentido seja em forma de texto, tabelas, gráficos etc.

De acordo com o conceito de dados e informação se pode descrever segurança da informação das seguintes formas:

> “Podemos definir segurança da informação como uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade.” (Sêmola, 2013, p. 41)

> “Preservação da confidencialidade, integridade e disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas” (ABNT NBR ISO/IEC 27001:2006)

Analisando as definições expostas acima pode-se observar que para ambas as definições é comum três conceitos básicos: confidencialidade, integridade e disponibilidade (CID). Esses três conceitos são apresentados por alguns autores como os três pilares ou princípios da segurança da informação.

Confidencialidade diz respeito a garantir que toda informação será protegida de acordo com o grau de sigilo que seu conteúdo requerer, garantindo o acesso

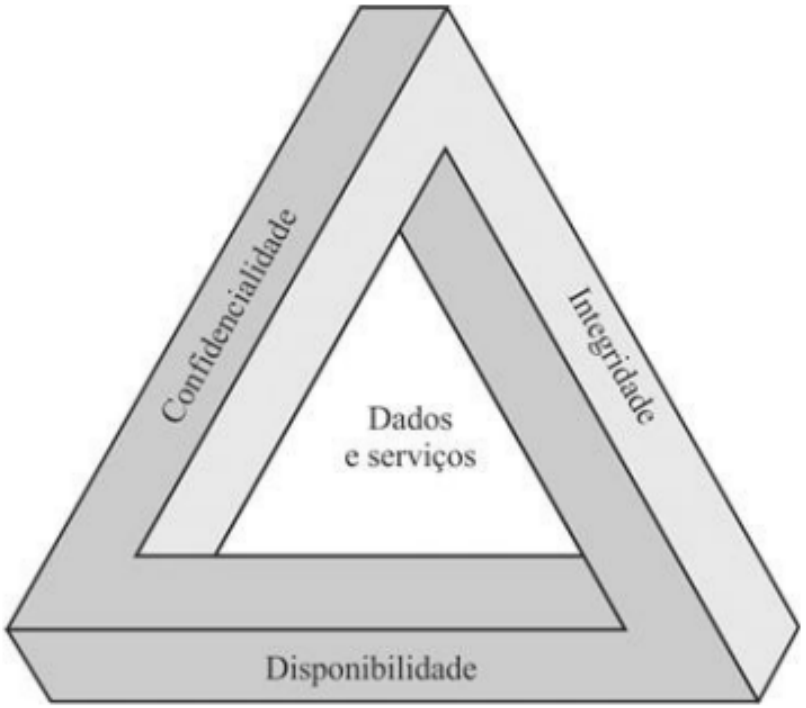
apenas para a quem a informação se destina. Um exemplo é a utilização de criptografia de dados.

Integridade é garantir que toda informação será mantida na mesma condição em que foi disponibilizada, protegendo de alterações indevidas e garantindo a autenticidade e originalidade da informação.

Disponibilidade garante que toda informação gerada ou adquirida esteja disponível sempre que necessário para acesso pelos usuários autorizados.

A Figura 2.1 representa a relação entre estes três pilares principais:

Figura 2.1 - A tríade de requisitos de segurança



Fonte:(STALLINGS; BROWN, 2014)

A Figura 2.1 representa a disposição dos três pilares da segurança da informação em relação aos dados e serviços.

Maurício Rocha Lyra (2015) cita que existem ainda três aspectos complementares para garantia da segurança da informação sendo estes:

> “Autenticação: Garantir que um usuário é de fato quem alega ser. Não repúdio: Capacidade do sistema de provar que um usuário executa uma determinada ação. Lyra (2015, p.4)

> Legalidade: Garantir que o sistema esteja aderente à legislação. Privacidade: Capacidade de um sistema de manter anônimo um usuário, impossibilitando o relacionamento entre o usuário e suas ações. Lyra (2015, p.4)
>
> Auditoria: Capacidade do sistema de auditar tudo o que foi realizado pelos usuários, detectando fraudes ou tentativas de ataque. Lyra (2015, p.4)"

De acordo com as definições apresentadas pelos autores há também a definição de ativo que se refere a todo elemento que compõem o processamento e a manipulação da informação além da própria informação. A ISO/IEC 27001:2005 define ativo como "qualquer coisa que tenha valor para a organização".

2.1.1 Mecanismos de proteção e técnicas de defesa

Existem diferentes mecanismos que podem ser utilizados para garantir a segurança de sistemas e redes de computadores, seja através de *software* ou *hardware*.

Esses mecanismos tem como objetivo prevenir, identificar e interromper ataques aos sistemas, de forma a garantir a segurança dos dados e informações.

Sêmola (2013) divide os mecanismos de defesa em 3 tipos de acordo com suas características:

Preventivos - Tem como objetivo evitar que os incidentes ocorram através de mecanismos de conduta como políticas de segurança, procedimentos detalhados, controles de acesso etc.

Detectivas - Utilizadas para detectar indivíduos ou condições que possam gerar ameaças ao sistema e evitar que os mesmos explorem as vulnerabilidades.

Corretivas - Medidas tomadas para interceptar e interromper ataques e ameaças como equipes de emergência, restauração de *backup*, plano de recuperação etc.

Entre os diversos mecanismos de defesa existem:

Firewall é um sistema de segurança que, quando implementado em *software* ou em *hardware,* funciona como um filtro restringindo o tráfego da internet para, de ou em uma rede privada. O *Firewall* é configurado para liberar ou bloquear pacotes de dados e acesso a portas de acordo com as especificações necessárias para a

rede, podendo ser mais restritivo ou mais abrangente. Geralmente é configurado de forma manual.

Uma rede privada virtual (VPN - *virtual private network*) é uma técnica adotada para se obter uma conexão segura, criptografada, protegendo a identidade do dispositivo que realiza a conexão com o serviço de internet. O VPN funciona como um intermediador entre o pacote de dados e o usuário, evitando o rastreamento através da interceptação dos pacotes. Fornece também um endereço de IP temporário ao dispositivo preservando o endereço IP real.

Antivírus são *softwares* utilizados em sistemas operacionais com o objetivo de proteger os mesmos de programas maliciosos com os mais diversos tipos de vírus de computadores. O antivírus atua realizando a análise dos programas em execução em busca de códigos maliciosos. Quando detectado, o antivírus interrompe a execução do programa para realizar a análise do código com base no banco de dados de códigos maliciosos fornecido pelo fabricante do sistema.

Criptografia consiste em converter dados para um código ilegível conhecido como cifra. Esse método funciona utilizando uma chave de criptografia gerada matematicamente que encripta os dados, ou seja, transforma os dados em uma sequência de códigos ilegíveis. A força ou potência desta técnica depende diretamente do tamanho ou comprimento da chave utilizada. Este comprimento é medido em bits.

Sistema de detecção de intrusão (IDS - *Intrusion Detection System*) e sistema de prevenção de intrusão (IPS - *Intrusion Prevention System*) são sistemas que examinam o tráfego de dados pela rede para detectar e prevenir acessos não autorizados na mesma, prevenindo a exploração de vulnerabilidades por agentes não autorizados. Esses sistemas comparam os pacotes da rede com um banco de dados de ameaças e sinalizam os pacotes correspondentes. Enquanto o IDS é um sistema de monitoramento, o IPS é um sistema de controle de intrusão que impede que o pacote de dados seja entregue de acordo com seu conteúdo.

Autenticação é o processo de verificar a autenticidade das informações, garantindo que apenas usuários autorizados tenham acesso às informações e sistemas. Funciona por meio de verificação de credenciais. Caso as mesmas sejam autênticas, o acesso é liberado. Um modelo comumente utilizado é o sistema de *login* utilizando usuário e senha. Porém existem outros métodos possíveis, como a verificação biométrica ou facial, a forma de verificação varia de acordo com a

escolha do responsável pelo sistema podendo ser implementado até mesmos múltiplos procedimentos e um mesmo sistema.

2.1.1 Ameaças e vulnerabilidades

Sêmola (2013) descreve ameaças como agentes ou condições que comprometem as informações e seus ativos através da exploração de vulnerabilidades, provocando a perda da confidencialidade, integridade e disponibilidade das informações. Estes agentes podem ser pessoas, eventos, meio ambiente, sistemas, etc.

No que se refere às ameaças elas podem ser distinguidas entre ativas ou passivas, segundo Lyra (2015):

Ativas: “Envolvem alteração de dados”.

Passivas: “Envolvem invasão e/ou monitoramento, mas sem alteração de informações”.

De acordo com Mascarenhas Neto (2019) ainda é possível classificar as ameaças quanto a intencionalidade sendo:

Naturais sendo provenientes de fenômenos naturais como enchentes, incêndios naturais, tempestades eletromagnéticas etc.

Involuntárias ameaças inconsistentes provocadas muitas vezes por desconhecimento, entre as causas então queda de energia, acidentes, erros etc.

Voluntárias ameaças intencionais provocadas por agentes humanos como hackers, espiões, ladrões etc.

As vulnerabilidades estão diretamente ligadas aos pontos fracos dos ativos, ou seja, podem ser consideradas como fragilidades apresentadas pelos ativos. Essas fragilidades podem ser erros de configuração ou falhas de procedimentos geradas de maneira intencional ou não. Quando exploradas por ameaças as vulnerabilidades geram os chamados incidentes de segurança. Segundo a ABNT NBR ISO/IEC 27001:2006 incidente de segurança pode ser definido da seguinte forma:

> “Um simples ou uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma

> grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação".

A ocorrência de um incidente de segurança acarreta no rompimento de um ou mais princípios da segurança da informação. Stallings e Brown (2014) listam algumas ameaças e os princípios de segurança da informação com os quais elas se relacionam.

Revelação não autorizada ocorre quando uma ou mais entidades não autorizadas obtêm acesso a dados restritos, ferindo assim o princípio da confidencialidade. Alguns tipos de ataques resultantes desta ameaça podem ser: exposição, interceptação, inferência e intrusão.

Fraude e Usurpação, fraude seria a disseminação de informações falsas por parte de uma entidade com o objetivo de enganar o receptor das informações. Já a usurpação é o roubo ou tomada de controle sobre informações por uma entidade não autorizada, ambos os casos ferindo o princípio da integridade. Alguns tipos de ataques resultantes destas ameaças podem ser: personificação, falsificação e apropriação indevida.

Disrupção ocorre quando a interrupção da disponibilidade das informações por meio da interferência de um agente não autorizado ferindo o princípio da disponibilidade. Alguns tipos de ataques resultantes desta ameaça podem ser: incapacitação e obstrução.

Mascarenhas Neto (2019) dividem as vulnerabilidades em categorias de acordo com suas características sendo elas:

Físicas - Instalações que não seguem as normas e regulamentações adequadas, controle de acesso deficiente em ambientes com informações sensíveis etc.

Naturais - *Hardware* alocado em locais suscetíveis a desastres naturais, como incêndios, enchentes, terremotos, tempestades e outros.

Hardware - Computadores suscetíveis a poeira, umidade e acesso indevido, recursos protegidos de maneira inadequada podem acarretar falhas de *hardware*.

Software - Erros de codificação, instalação e configuração de aplicativos e sistemas podem acarretar falhas, acessos indevidos, perda de dados e vazamento de informações.

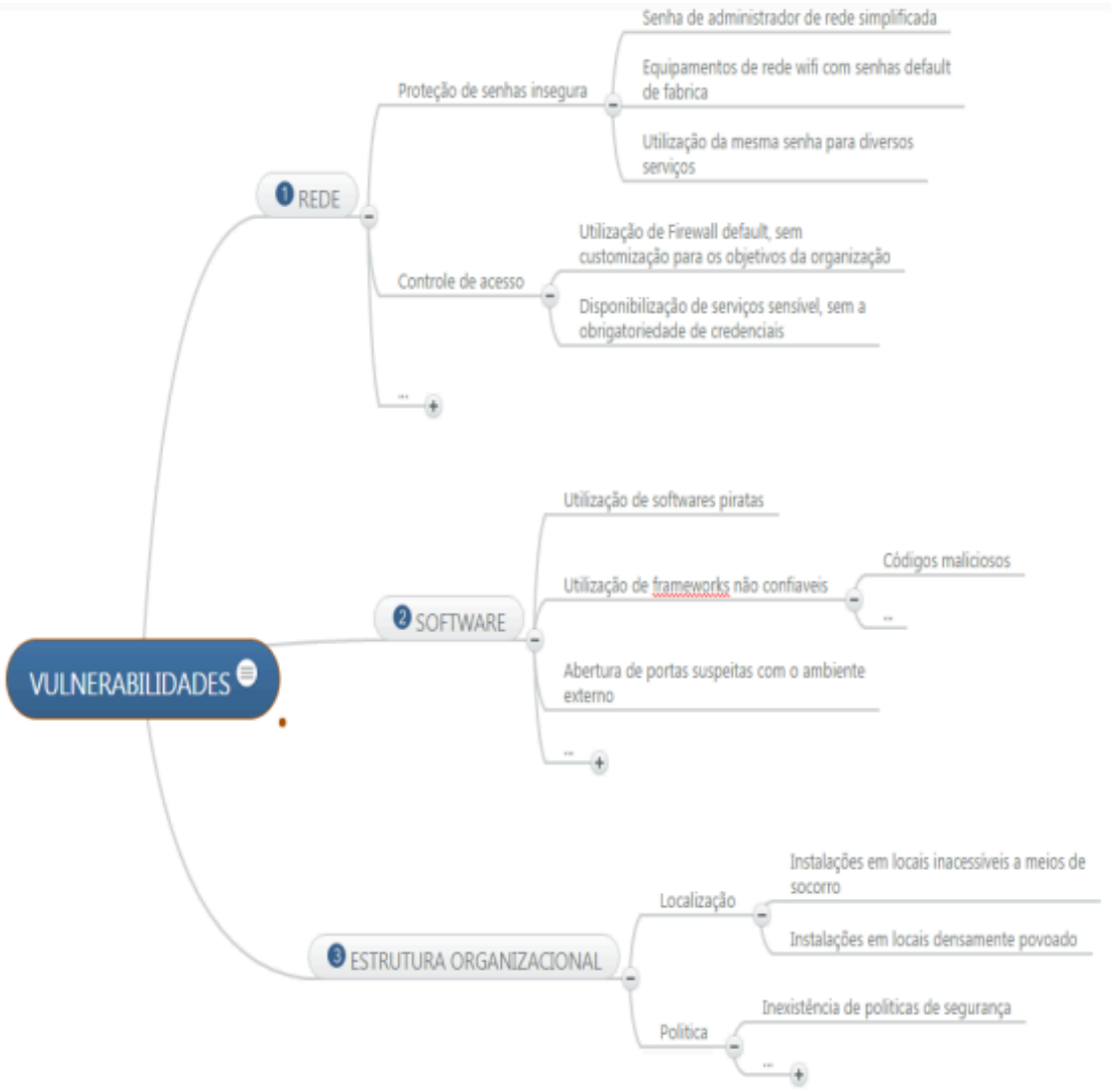
Mídias - Discos, fitas, relatórios impressos podem ser danificados. Falhas de energia podem ocasionar mal funcionamento de equipamentos e comprometer conjuntos de dados.

Comunicação - A comunicação telefônica é vulnerável a acessos indevidos e falhas de infraestrutura que impeçam a comunicação.

Humanas - Treinamento inadequado, não verificação de antecedentes, problemas anteriores, má-fé ou descontentamento de funcionários podem acarretar no compartilhamento indevido de informações ou interferência nos dados.

Ainda segundo Mascarenhas Neto (2019) a identificação das vulnerabilidades permite realizar o cálculo de probabilidade das ameaças se concretizaram em determinados cenários, podendo ser representado na árvore tipológica da figura 2.2:

Figura 2.2 - Exemplo de árvore de vulnerabilidades



Fonte:(Mascarenhas Neto, 2019)

A Figura 2.2 apresenta um exemplo de árvore de vulnerabilidades e como é feita a distribuição das vulnerabilidades em relação a sua origem

2.2 Normas técnicas e Legislação

Abordaremos as normas e legislações que regulamentam e delimitam a área de atuação da segurança da informação.

2.2.1 Normas técnicas de segurança

A área da segurança de informação como todas as áreas de conhecimento possui um conjunto de normas e especificações a serem seguidas com o objetivo de garantir a eficiência e competência dos procedimentos realizados.

Neste cenário se destaca a série ISO/IEC 2700x onde se encontram as normas internacionais para segurança de TI (tecnologia da Informação) e segurança da informação em organizações privadas, públicas e sem fins lucrativos. As ISO 2700x tratam de diversos tópicos na área da segurança da informação, cada uma especificando as normas e procedimentos para determinadas operações.

Algumas normas da série ISO/IEC 2700x de grande importância para a área de segurança da informação são:

ISO 27001 - Requisitos para sistemas de gestão de segurança da informação. A Norma define requisitos, regras e métodos a serem seguidos para garantir a segurança das informações. A ISO oferece um modelo para implementar, monitorar e melhorar a proteção para a organização, analisando, identificando e controlando riscos potenciais para a empresa.

ISO 27002 - Orientação sobre controles de segurança da informação. A ISO é uma diretriz com recomendações para a implementação das medidas da ISO 27001. Contendo orientações precisas para que não ocorra negligências na implementação das medidas.

ISO 27000 - Visão geral e vocabulário dos sistemas de gestão da segurança da informação. Contém termos e definições utilizados na série de normas ISO 2700x.

ISO 27701 - Orientação sobre gestão de proteção de dados. A norma é especificamente relacionada à privacidade dos dados, especificando um sistema de

gestão de proteção de dados para tratar o processamento e a segurança das informações.

ISO 27005 - Orientação sobre gestão de riscos de segurança da informação. Oferece orientações sobre gestão de riscos de segurança e aborda conceitos apresentados na ISO 27001.

ISO 27017 - Guia de medidas de segurança da informação em serviços em nuvem. Oferece orientações relacionadas a medidas de segurança na computação em nuvem.

ISO 27033 - Orientação sobre segurança de rede. Apresenta uma visão geral, conceitos e diretrizes para implementação da segurança de redes nas organizações.

ISO 27039 - Orientação sobre sistemas de detecção de intrusão (IDPS).

A implementação das práticas presentes nas ISO/IEC 2700x garantem que a rede ou o sistema em questão sigam os padrões internacionais de segurança para minimização de riscos e ameaças, garantindo assim a confiabilidade do mesmo.

2.2.2 Legislação

No Brasil assim como em outros países há um conjunto de leis e definições nacionais que regulamentam o uso da internet, definindo os limites do que é legalmente aceitável dentro do âmbito digital, da mesma forma definindo o que é caracterizado como crime digital, também referido como crime cibernético.

Crime digital é toda ação definida como ilegal perante as leis realizadas contra qualquer pessoa ou organização que usa um computador, seus sistemas e seus aplicativos *online* ou *offline*.

Dentre as leis que regulamentam os crimes digitais no Brasil destacam-se:

- Lei Nº 12.737, de 30 de novembro de 2012. Foi a primeira lei a tipificar atos de crimes digitais como invasão de computadores, violação de dados e interrupção de serviços.
- Lei nº 12.965, de 23 de abril de 2014. Também chamado de marco civil da internet, esta lei surgiu para regulamentar os direitos e deveres dos usuários da rede, esta lei se tornou essencial para a proteção das informações dos usuários na rede, garantindo que essas informações só serão acessadas perante ordem judicial. A lei também garante a possibilidade de retirar um determinado conteúdo do ar.

- Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD), esta é hoje uma das leis mais importantes quando se trata da proteção de dados e informações seja em meio digital ou físico.

> “Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.” (Brasil, 2018).

Ou seja, a LGPD busca proteger a captação, armazenamento e compartilhamento de dados pessoais dos usuários.

- Decreto nº 11.491, de 12 de abril de 2023. Este decreto promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001. Neste decreto estão estabelecidas as medidas legais a serem adotadas no caso de crime digital divididas em: crimes contra a confidencialidade, integridade e disponibilidade de dados e sistemas de computador, crimes informáticos, crimes relacionados ao conteúdo da informação, violação de direitos autorais e de direitos correlatos e outras formas de responsabilidade e sanções.

2.3 Ataques

Ataques são ações contra a infraestrutura de segurança das organizações ou indivíduos visando explorar falhas e vulnerabilidades da mesma. Quando bem sucedidos os ataques podem causar sérios danos à organização alvo.

Segundo comunicado à imprensa Fortnet (2023) relata que no decorrer do ano de 2022, o Brasil foi o segundo país que mais sofreu com ataques cibernéticos na américa latina com um total de 103 bilhões de ataques sofridos no período do ano de 2022, ficando atrás apenas do México com 187 bilhões de ataques registrados.

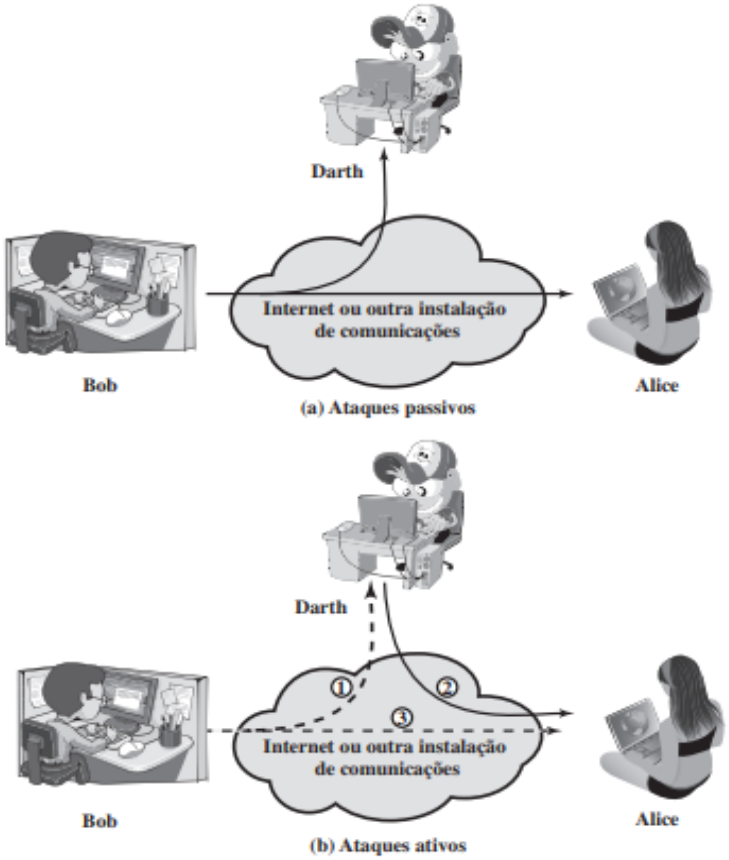
Alguns pontos destacados no relatório são:

> “A contínua destruição em massa do malware wiper mostra a evolução destrutiva dos ataques cibernéticos.
>
> Ataques de ransomware permanecem em níveis máximos, sem evidência de desaceleração em âmbito global e com novas variantes habilitadas por Ransomware-as-a-Service (RaaS).
>
> Os malwares mais utilizados no período foram criados há mais de um ano, o que mostra que os atacantes se beneficiam em termos de eficácia e economia de custos ao reutilizar e reciclar códigos.
>
> A vulnerabilidade Log4j continua a causar danos em organizações de todos os setores, principalmente em Tecnologia, Governo e Educação.” (Fortnet, 2023).

O relatório apresentado pela Fortner mostra o cenário preocupante em que se encontra o Brasil quando se observa o cenário de crimes cibernéticos. De acordo com IBGE (2023) no censo realizado no ano de 2022 o Brasil possui uma população de aproximadamente 203 milhões de pessoas, o que leva ao número de 507 casos de ataques cibernéticos por habitante no país.

De acordo com Stallings (2015) os ataques podem ser divididos em ataques passivos e ataques ativos.

Figura 2.3 - Ataques à segurança



Fonte:(Stallings, 2015)

Na Figura 2.3 (a) é demonstrado o funcionamento de um ataque do tipo passivo, com um indivíduo interceptando a comunicação entre dois *hosts*. Figura 2.3 (b) apresenta um ataque do tipo ativo, onde o indivíduo intercepta e altera o conteúdo dos dados enviados entres os *hosts*.

2.3.1 Ataques passivos

Este método de ataque geralmente se baseia na utilização de escutas e interceptações de transmissões para obter informações que estão sendo transmitidas. Stallings (2015) cita dois tipos de ataques passivos.

Vazamento de conteúdo como o nome sugere é a captação e divulgação de conteúdo sensível ou confidencial, podendo ser obtido através de escutas telefônicas, mensagens por correio eletrônico ou transferência de arquivos.

Análise de tráfego é um método mais sutil visando basicamente o monitoramento de tráfego de informações entre interlocutores. Mesmo que não se obtenha acesso direto às informações trocadas entre os interlocutores pode-se obter informações úteis como a frequência com que se comunicam e o tamanho das informações trocadas.

Ataques passivos são consideravelmente difíceis de serem detectados já que não envolvem alterações nos dados. No geral o tráfego de informações se dá de maneira aparentemente normal de forma que nem o emissor e nem o receptor das informações consigam perceber que há uma interferência no tráfego da informação.

2.3.2 Ataques ativos

Ataques ativos geralmente realizam alguma alteração no fluxo de dados ou criam um fluxo de dados falso. Também há possibilidade de interromper o fluxo de dados. Stallings (2015) divide este modelo de ataque em quatro categorias: disfarce, repasse, modificação de mensagem e negação de serviço.

Disfarce ocorre quando o invasor assume a identidade de uma entidade pertencente ao sistema (caminho 2 da figura 2.3b). Este tipo de ataque geralmente envolve algum dos outros tipos de ataques ativos, por exemplo ao assumir uma identidade no sistema o invasor ganha acesso e modifica informações internas.

Repasse é a captura passiva de um fluxo de dados e a retransmissão subsequente com o objetivo de produzir um efeito não autorizado.

Modificação de mensagens assim como o nome sugere é a alteração de partes das mensagens enviadas entre os interlocutores ou até mesmo o reordenamento e adiamento do envio das mensagens com o objetivo de interferir no resultado final do processo.

Negação de serviço consiste em impedir ou inibir o uso ou gerenciamento dos sistemas de comunicação do alvo. Um exemplo deste tipo de ataque é o sequestro de bancos de dados. Neste ataque o criminoso invade os sistemas internos da organização, através de algoritmos de criptografia que encripta as informações do banco de dados da mesma, impedindo assim o acesso aos dados.

Ao contrário dos ataques passivos que são difíceis de se detectar, mas possuem diferentes métodos para prevenção, os ataques ativos são mais fáceis de

serem detectados, porém devido às inúmeras vulnerabilidades possíveis em um sistema a interrupção dos mesmos é um processo mais complexo e de urgência.

2.3.3 Tipos de ataque

Novas ferramentas, técnicas e métodos de ataque surgem frequentemente, assim como novas falhas em sistemas são encontradas. O fácil acesso ao conhecimento graças a internet tornou ataques cibernéticos algo que até mesmo pessoas sem grandes conhecimentos da área podem realizar.

Ataques à segurança da informação podem ser classificados de acordo com a técnica utilizada e o objetivo do atacante. Mascarenhas Neto (2019) apresenta alguns dos ataques mais comuns a segurança, sendo ele:

- **Engenharia Social** - Utiliza de persuasão e enganação para obter informações que possam comprometer a segurança da organização, assim obtendo acesso não autorizado a recursos e informações restritas.
- **Negação de Serviço (DoS e DDoS)** - Ataques DoS (*Denial of Service*) tem como objetivo interromper um serviço ou um computador sobrecarregando o processamento do mesmo ou sobrecarregando o tráfego de dados na rede em que ele está conectado. Ataques DDoS (*Distributed Denial of Service*) seguem o mesmo conceito, porém utilizando um conjunto de computadores para derrubar um serviço ou outro conjunto de computadores.
- ***Phishing* (*Phishing Scam, Scam*)** - O principal objetivo é a captura de informações sensíveis dos alvos, geralmente através de fraudes eletrônicas, utilizando-se de *e-mails* e páginas *web* falsas.
- ***Pharming*** - é uma variação de *Phishing* que explora vulnerabilidades em *browsers*, SOs (Sistemas Operacionais) e servidores DNS (*Domain Name System*) redirecionando usuários para páginas *web* falsas.
- **IP *Spoofing*** - Tenta assumir a identidade de outro computador enviando pacotes de dados com endereços IPs falsos de outra máquina.

- ***Malware*** - Se refere a todos os tipos de programas que executam ações maliciosas em um computador, como: vírus, cavalos de Tróia, *adware*, *spyware*, *backdoors*, *keyloggers*, *worms*, *bots* e *rootkits*.
- **Ataques de força bruta** - utiliza criptoanálise de maneira exaustiva para descobrir senhas de ativos de rede, servidores, serviços *web* etc.

Estes são alguns dos métodos de ataque mais comumente utilizados em ataques a ativos em organizações, os métodos variam dependendo das ferramentas e objetivos do atacante em relação ao alvo.

2.4 Pentest

A segurança da informação é dividida em diversas áreas: monitoramento, pesquisa, gestão de segurança, defesa, dentre outros.

A defesa em segurança da informação é composta por diversos mecanismos, técnicas e métodos que podem ser aplicados por uma organização para garantir sua segurança de seus sistemas. O Pentest por sua vez é um dos métodos utilizados para testar e avaliar os mecanismos e técnicas de defesa implementados por organizações e apontar possíveis falhas e melhorias a serem aplicadas para garantir o máximo de segurança possível para estes sistemas.

2.4.1 Conceito

Penetration testing ou Pentest pode ser traduzido com teste de penetração ou teste de intrusão. Consiste em uma série de testes realizados em uma rede, sistema, *software*, *hardware*, sites, etc., com o objetivo de identificar, mapear e expor as possíveis vulnerabilidades encontradas. O processo de Pentest é de extrema importância principalmente em grandes organizações pois permite tratar as vulnerabilidades do sistema seja através de correções diretas ou com a criação de mecanismos de defesa direcionados para estas vulnerabilidades, garantido assim a segurança dos ativos e das informações da organização.

O objetivo do Pentest não é conseguir acesso aos sistemas explorando falhas, e sim mapear as falhas existentes nos sistemas para que as devidas medidas de

segurança possam ser aplicadas, seja por substituição de *hardware* ou atualização de sistemas com *patches* de segurança.

No processo de execução do Pentest após cada tentativa de invasão seja ela bem-sucedida ou não, é gerado um relatório detalhado com os erros, falhas, vulnerabilidades encontradas, métodos e ferramentas utilizadas durante a tentativa de invasão. Esse relatório é apresentado à equipe da organização alvo que deverá, a partir daí, implementar soluções para corrigir e tratar as falhas de segurança encontradas.

Dentro da área de Pentest existe ainda um programa conhecido com *bug bounty* em que não existe vínculo contratual entre a organização alvo e o profissional (*hacker*) que realizará a tentativa de invasão. Neste sistema a empresa paga recompensas em dinheiro para *hackers* que encontrarem falhas e *bugs* em seus sistemas e reportar para que possam ser corrigidas. Algumas empresas utilizam este programa como forma de melhorar a segurança de seus sistemas e aplicações.

2.4.2 Tipos de Pentest

O pentest pode ser classificado em tipos de acordo com as condições em que é realizado. Segundo Moreno (2015) o pentest pode ser dividido nos seguintes tipos:

Black-Box também chamado de teste da caixa preta ou teste cego. O auditor tentará acessar a infraestrutura da rede sem nenhum conhecimento prévio da estrutura ou organização da rede.

Este é o cenário mais comum se tratando de ataques de invasão externo, já que os invasores virão de fora da rede e não terão conhecimento da estrutura da mesma.

A metodologia *black-box* é sub categorizada em:

- *Blind* - Neste cenário o auditor não possui nenhuma informação da rede a ser testada e o alvo sabe que será atacado e quais testes serão realizados
- *Double Blind* - Neste cenário o auditor não possui informações da rede e o alvo não sabe que será atacado e nem mesmo os testes que serão realizados

Este modelo é eficiente considerando o cenário em que o atacante não possui conhecimento da rede, porém se torna superficial se o atacante possuir informações da estrutura da rede.

White-box também chamado de teste da caixa branca ou teste não cego, neste cenário o auditor terá total conhecimento da infraestrutura da rede a ser testada. Este modelo simula o caso de um ataque interno à rede ou um ataque em que o atacante tem conhecimento sobre a mesma.

A metodologia *white-box* é sub categorizada em:

- *Tardem* - Neste contexto o auditor tem total conhecimento da rede a ser testada, o alvo sabe que será atacado e quais testes serão realizados.
- *Reversal* - Neste contexto o auditor tem total conhecimento da rede e o alvo não sabe que será atacado, nem mesmo os testes que serão realizados.

Este método é mais específico e detalhado, já que o auditor tem conhecimento total da rede possibilitando elaborar um plano de ataque mais detalhado e efetivo para o teste de segurança.

Gray-box também chamado de teste da caixa cinza ou teste parcialmente cego, neste cenário o auditor terá conhecimento parcial da rede alvo sendo uma mescla entre *black-box* e *white-box*.

A metodologia *gray-box* é sub categorizada em:

- *Gray-box* - Neste contexto o auditor tem conhecimento parcial da rede e o alvo sabe que será atacado e quais testes serão realizados no processo.
- *Double Gray-box* - Neste contexto o auditor tem conhecimento parcial da rede e o alvo não sabe que será atacado e nem quais testes serão executados.

2.5 Vantagens do Pentest

De acordo com as legislações em vigência é responsabilidade da empresa manter seguro os dados de seus usuários e funcionários além é claro de suas informações internas.

Segundo Moreno (2015) pentest deve fazer parte do escopo de um projeto de rede, considerando que haverá a possibilidade da rede ser atacada por indivíduos mal intencionados. O atacante poderá utilizar diversos métodos e explorar diversas falhas e uma vez acessada indevidamente, a rede pode sofrer sérios danos e perdas.

Ao realizar um teste de penetração em uma rede é possível se garantir um maior nível de segurança para a mesma, já que durante o processo um auditor capacitado irá detectar falhas e vulnerabilidades que podem comprometer a rede. Essas falhas serão listadas para que a equipe responsável possa realizar as correções ou tomar as medidas preventivas cabíveis de forma a garantir a segurança dos dados e informações que circulam pela rede.

Os benefícios dessa prática se estendem e diversificam de várias maneiras. Entre as vantagens, destacam-se:

- Avaliação crítica da eficácia da segurança cibernética;
- Identificação escalável de vulnerabilidades e lacunas no sistema de segurança;
- Abordagem preventiva, não apenas corretiva, na implementação de medidas contra cibercriminosos;
- Adoção proativa de novas práticas e medidas de Segurança da Informação;
- Reforço da reputação da marca, tanto interna quanto externamente, em relação à segurança de dados.

É importante ressaltar que o Teste de Vulnerabilidade proporciona uma tranquilidade adicional para os clientes, especialmente em uma era em que a transformação digital está intimamente ligada à conformidade com a Lei Geral de Proteção de Dados (LGPD). O Pentest, de acordo com os requisitos da legislação vigente, oferece segurança abrangente, contribuindo para a conformidade e proteção dos dados.

2.6 Riscos do Pentest

Se tratando de pentest não existem desvantagens na realização deste procedimento já que o mesmo consiste em um procedimento preventivo e corretivo para problemas já existentes, porém existem alguns riscos incluídos neste processo.

Afinal, o pentest consiste basicamente na realização de uma invasão a rede auditada e mesmo que não intencionalmente pode gerar alguns problemas e transtornos devido à natureza do procedimento. Entre os possíveis problemas pode-se listar:

- Indisponibilidade de sistemas e/ou dados da rede;
- Perda permanente de dados;
- Corrupção de arquivos e dados.

Por este motivo, ao se realizar este procedimento deve-se garantir que haja a possibilidade de restaurar o sistema e seus dados em caso de necessidade.

3 MÉTODOS E FERRAMENTAS

Existem diferentes métodos e ferramentas a serem utilizados no processo de Pentest, cada qual com sua finalidade e objetivo, a seguir serão abordadas algumas delas.

3.1 Metodologia

.

Na área de pentest existem diversas metodologias que podem ser utilizadas como guias no processo de testagem de uma rede, apesar de cada rede possui suas próprias características o que leva a um processo personalizado para cada caso, as metodologias podem ser utilizadas como guias indicando a sequência de etapas a serem realizadas para o pentest.

Cada metodologia possui como foco uma determinada área de teste, algumas sendo utilizadas em aplicações web, outras em redes sem fio etc. Auxiliando assim a garantir um foco direcionado totalmente ao modelo de rede a ser testado.

Algumas metodologias utilizadas são descritas abaixo.

Metodologia ISSAF

Essa metodologia busca os resultados de uma auditoria da forma mais rápida possível, podemos dividir essa metodologia em quatro principais etapas:

- Planejamento - Nesta etapa são definidas informações como os alvos que serão testados na auditoria, objetivos a serem cumpridos, propósito do teste etc;
- Avaliação - Consiste na realização do teste e anotação e organização dos resultados obtidos;
- Tratamento - Decisão em relação ao que será feito sobre as vulnerabilidades encontradas;
- Acreditação - Etapas finais para emissão do certificado ISSAF para a empresa.

Metodologia OWASP

Essa metodologia é direcionada para testes em servidores e aplicações web. A seguir estão listados alguns testes realizados em ambiente web:

- Injeção - Consistindo em injetar códigos ou comandos no sistema com o objetivo de retornar dados privados.
- Quebra de sistemas de autenticação/sessão - Manipular e quebrar sistemas de autenticação, por exemplo telas de *login*.
- Referência direta a objetos - Manipulação de dados diretamente na página, permitindo ataques de injeção ou acesso a áreas restritas.
- *Directory Traversal* - Capacidade de leitura e acesso a diretórios e arquivos proibidos.
- *File Upload* - Envio de arquivos para o servidor web. Pode ser enviado um arquivo malicioso que permita o controle da página web.
- Configurações falhas - Teste de intrusão em serviços e não somente em aplicações web.
- Exposição de dados sensíveis – Dados sensíveis sem sistemas de proteção ou métodos criptográficos adequados.
- CSRF – Falhas em sistemas de autenticação que permitem ações não autorizadas.

- Controle de acesso quanto à função – Acesso a páginas restritas sem sistemas de autenticação.
- Utilização de componentes vulneráveis – Uso de módulos e frameworks conhecidamente vulneráveis, como o Joomla e o WordPress.
- Manutenção do acesso – Instalação de páginas maliciosas no servidor para posterior acesso.
- Negação de serviço – Testes de stress com o objetivo de sobrecarregar o alvo com excesso de dados.

Metodologia OSSTMM

O objetivo dessa metodologia é avaliar a segurança digital considerando o objetivo do negócio, baseando-se em métodos científicos para garantir a segurança da informação. Testes seguindo este modelo passam por três estágios:

- Pré-teste - Estágio inicial da avaliação de segurança, pode ser dividido em:
  - Conformidade: A avaliação deve seguir as leis vigentes no país, regras industriais e políticas da empresa a ser auditada.
  - Regras de boa conduta: Regras gerais de boa conduta para realização da avaliação de segurança.
  - Detectar riscos e ameaças: Detectar tudo que possa comprometer a segurança dos dados ou ter efeito negativo para a empresa auditada.
- Teste - Realizar testes de segurança para garantir a segurança e confiabilidade do sistema auditado.
- Pós-teste - Escrita e apresentação dos resultados em um relatório final.

Metodologia Backtrack

Esta metodologia pode ser ajustada de acordo com as necessidades da auditoria para se encaixar melhor no cenário desejado, ela pode ser dividida em:

- Planejamento do projeto
- *Footprinting*
- *Fingerprinting*
- Enumeração
- Mapeamento de vulnerabilidades
- Exploração do alvo
- Engenharia social (opcional)
- Escalonamento de privilégios
- Manutenção do acesso
- DoS – Negação de serviço
- Documentação técnica
- Redes sem fio (opcional)

Metodologia PTES

Este é um dos métodos mais recentes para a condução de Testes de Penetração, visando estabelecer-se como uma norma-padrão para a execução desse tipo de serviço.

O PTES (Padrão de Execução de Teste de Penetração) fragmenta os testes em fases distintas, que incluem:

- Predefinição
- Coleta de inteligência
- Modelagem de ameaças
- Análise de vulnerabilidades
- Exploração
- Publicar exploração
- Relatório

3.1.1 Etapas gerais

O Pentest pode ser dividido de forma geral em 3 etapas comuns: planejamento, execução e após execução. A partir das descrições apresentadas nas referências bibliográficas utilizadas na elaboração deste documento as características destas etapas podem ser descritas da seguinte maneira:

Planejamento: Levantamento inicial das informações utilizadas na modelagem dos testes a serem realizados, onde se verificam detalhes relacionados a infraestrutura, equipamentos necessários, recursos a serem utilizados, planos de gerenciamento, requisitos, ameaças de interesse, metas, objetivos a serem alcançados, responsabilidades técnicas etc.

Nesta etapa são definidos os testes a serem realizados. Testes externos consistem em verificar se é possível acessar a rede interna da empresa auditada superando os procedimentos de segurança que isolam a rede de conexões não autorizadas de terceiros. Durante a invasão externa devem ser verificadas as vulnerabilidades e a eficiência de firewalls, proxys, sistemas de detecção de intrusão e quaisquer outros sistemas de proteção existentes na rede. Testes internos tem como base o invasor já possuindo acesso interno à rede, simulando ataques com diferentes níveis de acesso à rede, buscando maneiras de escalar privilégios e conseguir acessos anteriormente não possuídos pelo usuário representado no teste. Durante o teste busca-se vulnerabilidades que possam ser exploradas e os possíveis danos causados pelas mesmas, analisando a eficiência dos sistemas de proteção interna de dados como validações de acesso por exemplo.

Execução: como sugerido pelo nome é a etapa onde são realizados os testes. Durante esta etapa é realizado o processo de identificação e exploração de riscos e vulnerabilidades. Atividades características desta etapa são a obtenção de informação, identificação de vulnerabilidades e pôr fim ao ataque.

Pós Execução: Aqui são analisadas as vulnerabilidades encontradas na fase etapa anterior, identificando cada uma das vulnerabilidades encontradas estabelecendo possíveis ações para mitigação das mesmas. Nesta etapa é gerado o relatório final apresentando toda a documentação gerada durante a execução das etapas anteriores

3.2 Ferramentas

Os *softwares* utilizados nesta área variam principalmente em funcionalidades sendo direcionados para objetivos e contextos específicos, alguns são direcionados para testes em interfaces web, outros para redes *wireless* e assim por diante, existe uma grande diversidade de *softwares* quando se refere a testes de segurança.

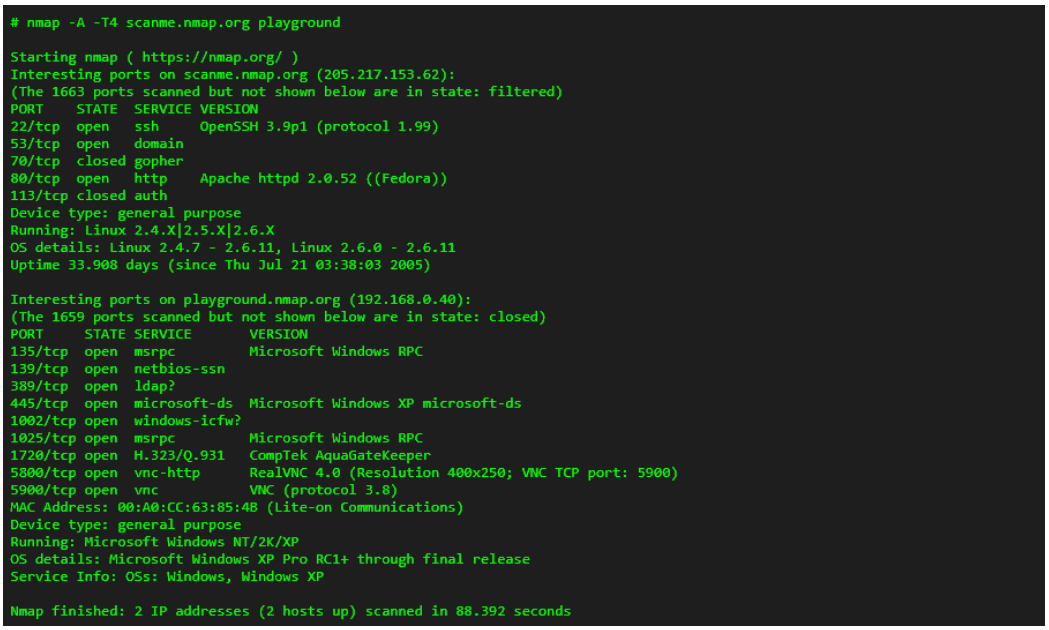
Dentre as diversas ferramentas existentes pode-se citar algumas comumente utilizadas nesta área:

- **Kali Linux**
  Kali Linux é um sistema operacional baseado em Debian. Debian é uma distribuição Linux utilizada como base não só para o Kali como para o Ubuntu entre outros. Kali é um sistema operacional desenvolvido e mantido pela empresa OffSec, uma empresa de cibersegurança.
  O Kali é um sistema operacional criado como uma ferramenta para profissionais da segurança da informação para uso forense e realização de pentest, sendo um sistema operacional completamente customizado para atender a tal finalidade. Embora possa ser utilizado como qualquer outro sistema operacional comum, o Kali é voltado completamente para a área da segurança possuindo diversas ferramentas direcionadas a essa finalidade instalada de forma nativa.
  Existem, até momento em que este documento é escrito oito, maneiras de se utilizar o Kali sendo elas instalando como sistema operacional principal do computador, utilizando uma máquina virtual, Instalação em processadores ARM, dispositivos mobile, rodando o sistema diretamente da nuvem, modo live que permite rodar o sistema diretamente de um pen drive, containers e via WSL no Windows.

- **Nmap** - Uma das ferramentas mais antigas e completas disponíveis, esta ferramenta foi sendo aprimorada com o passar do tempo, sendo uma das ferramentas básicas nesta área de atuação.
  Essencialmente, o Nmap é uma ferramenta de varredura de rede que utiliza pacotes IP para identificar todos os dispositivos conectados a uma rede. O programa fornece detalhes sobre todos os IPs ativos em suas

redes, possibilitando a verificação individual de cada endereço IP. O Nmap também oferece informações sobre a rede como um todo. Ele pode gerar uma lista de *hosts* ativos e portas abertas, além de identificar o sistema operacional de cada dispositivo conectado. Essa capacidade torna-o uma ferramenta valiosa para o monitoramento contínuo do sistema.

Figura 3.1 – Captura de Nmap scan



Fonte: nmap.org

Figura 3.1 - Apresenta um scan realizado com a ferramenta nmap no site oficial da ferramenta.

- **Metasploit** - Essa ferramenta tem como objetivo criar um ambiente de pesquisa e estabelecer um campo de exploração de vulnerabilidades. Isso possibilita a descoberta de erros de programação que podem resultar em falhas de segurança.

  Após obter um panorama completo das vulnerabilidades, o próximo passo envolve o desenvolvimento do *exploit*, usando técnicas como engenharia reversa ou programação. Em seguida, o *exploit* é executado e testado em diversos cenários para confirmar a existência das vulnerabilidades. Os *exploits* visam as vulnerabilidades identificadas,

executando o *payload* (código malicioso) e, assim, estabelecendo uma sessão de SSH ou Telnet. Isso possibilita o controle remoto do computador atacado.

Figura 3.2 – Captura de Metasploit

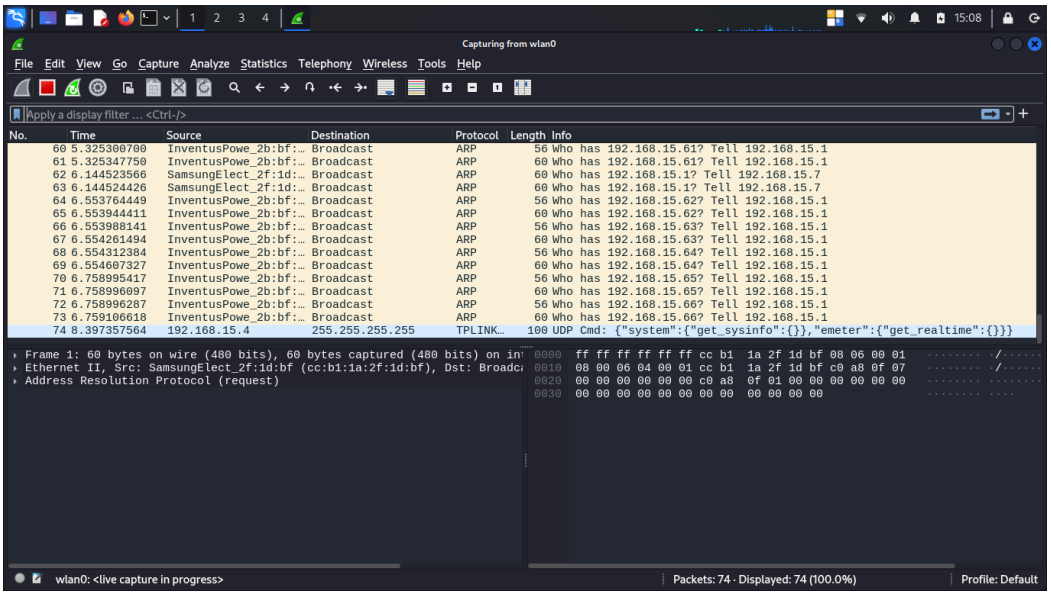
Fonte: docs.metasploit.com

Figura 3.2 - Página inicial da ferramenta Metasploit.

- **Wireshark** - O Wireshark é uma ferramenta de análise de pacotes e *sniffer* de rede. Ele registra o tráfego de rede na rede local, armazenando esses dados para análise posterior. O Wireshark é capaz de capturar o tráfego de rede em diversos protocolos, incluindo *Ethernet*, *Bluetooth*, redes sem fio (IEEE.802.11), *token ring*, conexões *frame relay*, entre outros.

  Uma característica notável do Wireshark é a capacidade de filtrar os registros antes ou durante a captura, permitindo concentrar a atenção no que é relevante durante o monitoramento da rede. Essa flexibilidade de filtragem é uma das razões pelas quais o Wireshark se tornou a ferramenta padrão para análise de pacotes.

Figura 3.3 - Captura de Wireshark



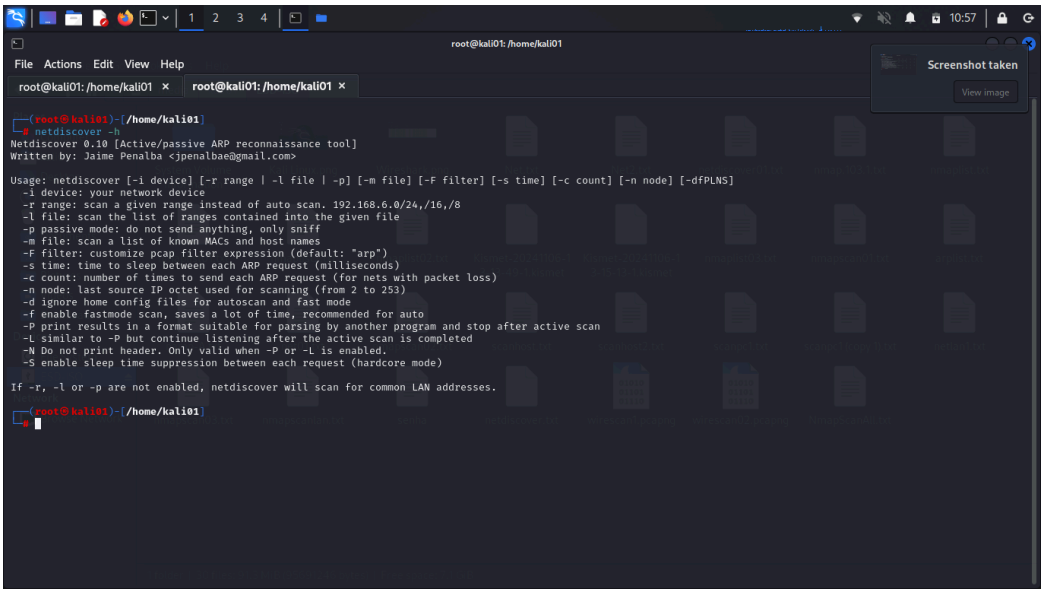
Fonte: Autor

Figura 3.3 - Captura de tela da ferramenta Wireshark durante monitoramento de rede.

- **Netdiscover** – Uma ferramenta de reconhecimento de endereços passivo/ativo, desenvolvido para com foco em redes sem fio que não possuem servidor DHCP, com foco principal em *wardriving*. Pode ser utilizado tanto em detecção passiva de *hosts* ativos quanto ativamente enviando solicitações ARP.

  Netdiscover inspeciona o tráfego ARP das redes em busca de endereços de rede utilizados pelos hosts conectados, trazendo também informações sobre os endereços MAC e os fornecedores dos mesmos.

Figura 3.4 - Captura de Netdiscover

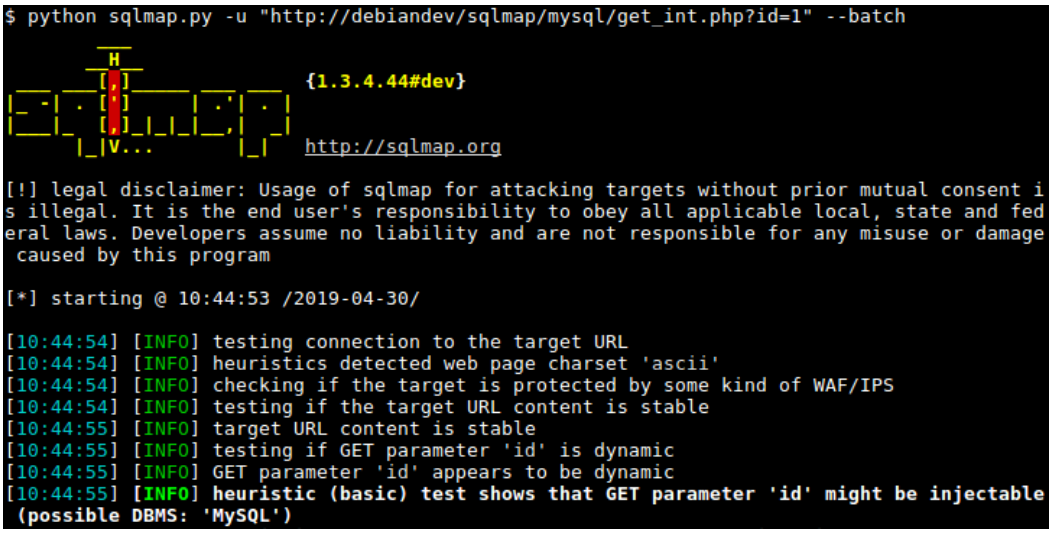


Fonte: Autor

Figura 3.4 - Captura de tela mostrando os comandos disponíveis para uso na ferramenta Netdiscover.

- **SQLmap** - O SQLMAP é uma ferramenta para ajudar na detecção de falhas de SQL *Injection*. Ele automatiza o envio de vários parâmetros maliciosos ao alvo, buscando vulnerabilidades de SQL *Injection*.
  Um Ataque de *Injeção* de SQL acontece quando comandos do banco de dados SQL são inseridos para apagar, coletar ou modificar dados no banco de dados. Isso ocorre quando os dados fornecidos pelo usuário não são validados corretamente e são interpretados como uma forma de inserção de comandos SQL. A vulnerabilidade de SQL *Injection* é bastante ampla, afeta tudo que se relaciona com algum banco de dados.

Figura 3.5 – Captura de SQLmap



Fonte: sqlmap.org

Figura 3.5 - Funcionamento da ferramenta em teste realizado pelo fabricante.

- **SEToolkit** - A engenharia social é uma técnica eficaz utilizada por invasores cibernéticos para obter acesso não autorizado a informações sensíveis. Para auxiliar os profissionais de segurança na identificação e mitigação dessas ameaças, foi desenvolvida a *Social-Engineer-Toolkit* (SEToolkit). Trata-se de uma ferramenta gratuita e de código aberto empregada em ataques de engenharia social, como *phishing*, falsificação de números de telefone, envio de SMS, e outras técnicas.

- **Maltego** - O Maltego é um serviço que tem a capacidade de encontrar informações sobre pessoas e empresas na internet, permitindo a combinação de dados para criar perfis em redes sociais, servidores de e-mail, entre outros.

  Ele é capaz de coletar diversas informações, como:

  Informações de rede: Verificação e coleta de dados sobre hosts de rede, portas abertas e protocolos utilizados.

  Informações de domínio: Coleta de dados relacionados a domínios, incluindo registros DNS, registros de e-mail e registros de nomes de host.

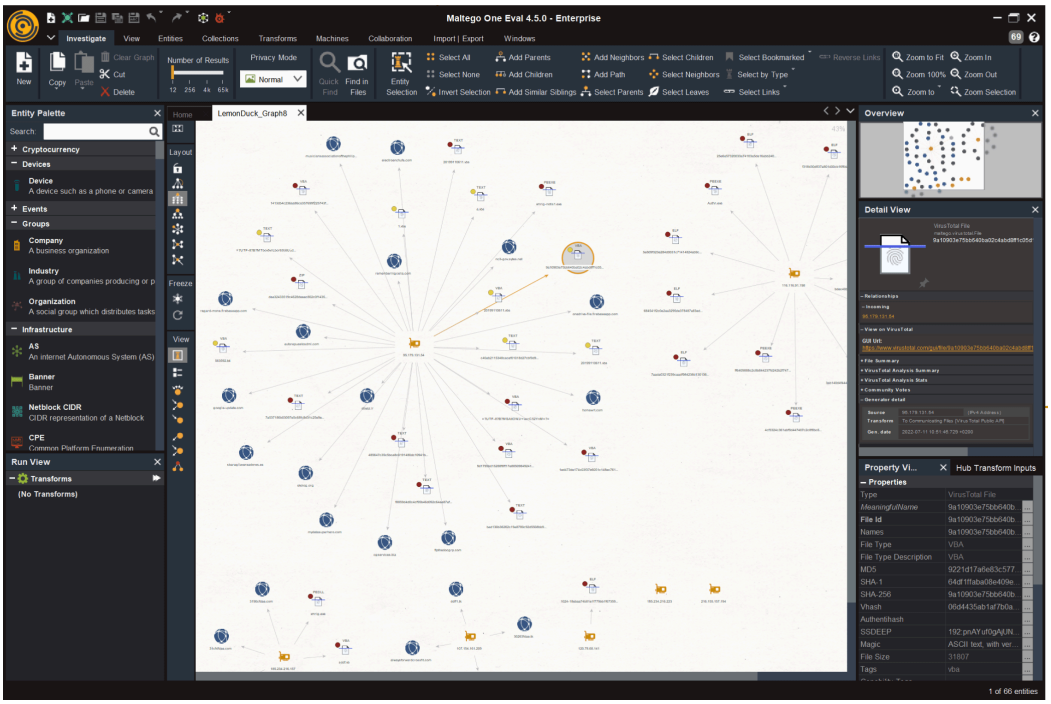
Informações de e-mail: Coleta de informações sobre endereços de e-mail, como nomes de domínio, provedores de e-mail e registros DNS.

Informações de redes sociais: Assim como no exemplo anterior, o Maltego pode obter dados de redes sociais, como perfis, postagens, amigos, seguidores e conexões.

Informações sobre pessoas e organizações: Coleta de dados sobre indivíduos e organizações, incluindo nomes, endereços, números de telefone, endereços de e-mail, sites e perfis de redes sociais.

Informações sobre malware: Coleta de dados relacionados a *malware*, como nomes de arquivos, impressões digitais, comportamento e padrões de ataque.

Figura 3.6 – Captura de Maltego



Fonte: maltego.com

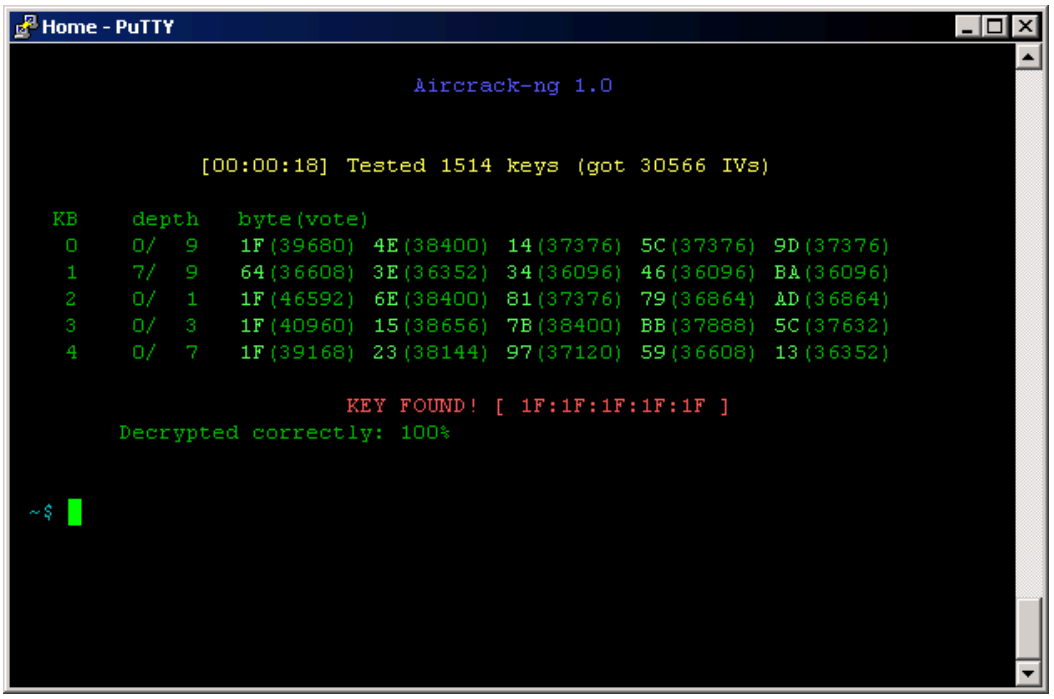
Figura 3.6 - Captura de tela realizada durante a utilização da ferramenta pelo fabricante.

- **Aircrack-ng** - O Aircrack-ng é um programa desenvolvido para quebrar chaves WEP e WPA/WPA2-PSK do IEEE 802.11.

  Para recuperar a chave WEP, o Aircrack-ng precisa capturar um número suficiente de pacotes criptografados usando o airodump-ng. Essa parte

do pacote Aircrack-ng utiliza dois métodos principais. O primeiro é a abordagem PTW (Pyshkin, Tews, Weinmann). A principal vantagem da abordagem PTW é que requer muito poucos pacotes de dados para quebrar a chave WEP. O segundo método é o método FMS/KoreK, que utiliza vários ataques estatísticos para descobrir a chave WEP, combinando-os com a força bruta.

Figura 3.7 – Captura de aircrack-ng

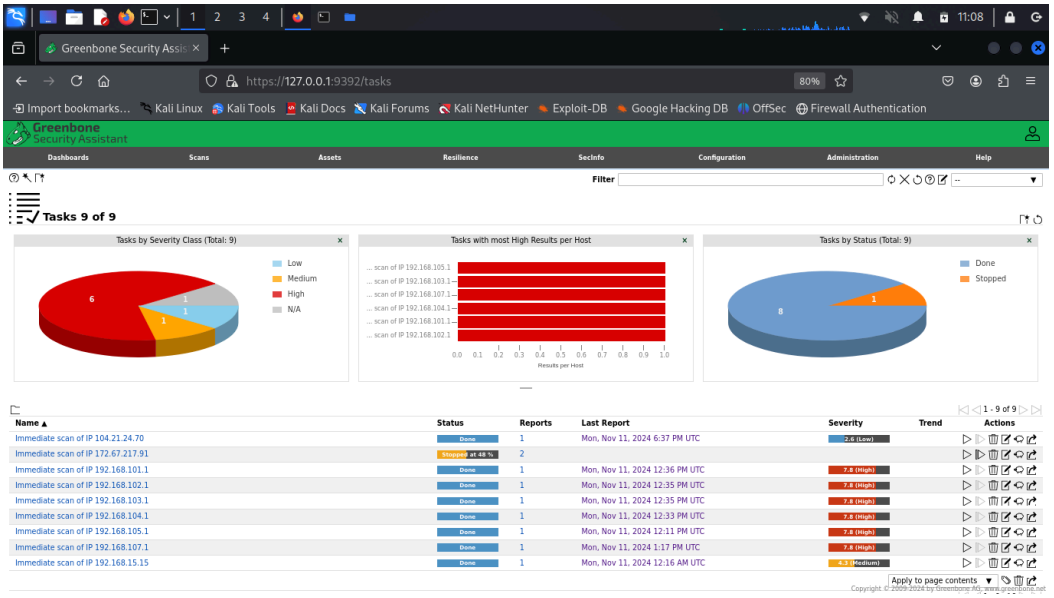


Fonte: aircrack-ng.org

Figura 3.7 - Captura de tela durante a utilização da ferramenta pelo fabricante.

- **OpenVAS** - O OpenVAS (*Open Vulnerability Assessment System*) é um *framework* composto por diversos serviços e ferramentas, proporcionando uma solução abrangente para a varredura e gerenciamento de vulnerabilidades.
  Ele oferece recursos como testes autenticados e não autenticados, suporte para diversos protocolos industriais e de Internet em diferentes níveis, ajuste de desempenho para varreduras em larga escala, e uma linguagem de programação interna poderosa que permite a implementação de qualquer tipo de teste de vulnerabilidade.

Figura 3.8 – Captura de OpenVAS



Fonte: Autor

4 APLICAÇÃO E ANÁLISE

A seguir será realizada uma aplicação prática dos conceitos e técnicas apresentados, buscando exemplificar de forma prática os processos utilizados durante a realização de um pentest.

Os testes realizados a seguir visam atingir os três pilares da segurança da informação. Serão realizados testes para validar estes três princípios, e por fim uma análise dos resultados obtidos no processo.

4.1 Caso de Teste

Devido a questões legais e técnicas que envolvem o processo de realização de um pentest completo após análise de locais potenciais, e minuta de contrato de Pentest para autorização de verificação, Anexo I, optou-se pela utilização dos laboratórios de informática internos do curso de Computação de forma a auxiliar em sua administração, como cenário para os testes e análises.

O objetivo dos testes será realizar uma análise de vulnerabilidade na rede do laboratório como a intenção de obter informações e acessos na rede, a verificação foi realizada do ponto de vista de um usuário interno que possui informações sobre

a estrutura interna dos laboratórios caracterizando um pentest do tipo Gray-box, pois apesar de possuir algumas informações sobre a rede essas informações são limitadas, os testes serão conduzidos levando em conta o seguinte cenário de execução apresentado a seguir:

Cenário Infraestrutura interna – O cenário é voltado para realização de teste a estrutura física dos laboratórios buscando obter acesso aos mesmos e sua infraestrutura e posteriormente obter acesso a rede e suas dependências, objetiva-se obter acesso a rede interna cabeada infiltrando-se e explorando em busca de possíveis vulnerabilidades que se mostrem ao alcance.

Este ataque consiste em um ataque interno tendo em vista que o atacante possui acesso às dependências da instituição e conhecimento relativo à rede e suas estruturas locais.

4.2 Análise de Vulnerabilidades

Como mencionado, neste cenário o atacante possui acesso a rede interna e algum conhecimento prévio sobre ela, o objetivo principal é a exploração da rede em busca de vulnerabilidades que possam comprometer a estrutura da rede interna da instituição.

4.2.1 Análise da rede

A rede foi observada com o uso da ferramenta Netdiscover em modo passivo para monitorar as trocas de pacotes entre os hosts, bem como no emprego do comando traceroute foi identificado que todos os pacotes de dados foram direcionados para fora da rede dos laboratórios. Utilizando a ferramenta Nmap se obteve o conjunto de informações sobre estes hosts, bem como portas abertas e serviços em execução, incluindo Firewall.

4.2.2 Análise de vulnerabilidades da rede

Com as informações obtidas a partir da utilização do Nmap e também, do monitoramento de pacotes na rede, dentre elas endereços IP, endereço MAC, máscara de rede, portas e serviços, sistema operacional e Firewall, utilizando a

ferramenta OpenVas foi realizado um scanner de vulnerabilidades nos hosts do laboratório.

Após a execução da varredura a ferramenta gerou um relatório contendo as vulnerabilidades encontradas, bem como a descrição de cada uma delas e o nível de impacto para a segurança representado por cada uma.

4.3 Análise de Segurança

Além da segurança digital a segurança da informação também deve se ater a segurança física da rede e demais equipamentos nela presentes, como ferramenta para teste de segurança o pentest também deve avaliar esse requisito.

Em vista disso também foi analisada a segurança da estrutura física dos laboratórios, considerando a manutenção dos três pilares da segurança da informação como base de análise.

4.3.1 Segurança da unidade

Os laboratórios da instituição estão em um edifício localizado no complexo de prédios destinados à utilização pelos alunos.

4.3.2 Ataques contra estrutura física

Foram analisados os ataques possíveis de execução no comprometimento da estrutura física da rede, e soluções potenciais para estes problemas.

4.4 Resultado geral da análise

Com base nos resultados encontrados no processo de análise de vulnerabilidades e de segurança realizados nos laboratórios foi possível visualizar e compreender a estrutura de segurança adotada na instituição e as falhas presentes no mesmo, bem como elaborar documento entregue à Direção da Escola Politécnica e de Artes para melhoria do serviço.

5 CONCLUSÃO

Através das informações apresentadas e dos estudos realizados neste trabalho, foi possível verificar a importância da aplicação de boas práticas e técnicas de segurança para garantir a confiabilidade, integridade e disponibilidade dos dados.

Por meio de análises feitas foi possível constatar que assim como o processo de digitalização da informação traz novas possibilidades e facilidades para manipulação de dados, ela traz consigo novos desafios quanto à segurança destes dados.

A utilização do pentest como ferramenta de verificação de segurança acaba por se tornar uma das maneiras mais confiáveis de se garantir a segurança de redes, permitindo uma visualização precisa das falhas e vulnerabilidades presentes na mesma pela perspectiva do atacante, dando assim uma visão ampla em relação aos meios e métodos a serem empregados para garantir a seguridade da rede.

No processo de análise apesar das limitações existentes foi possível concluir o objetivo de realizar uma varredura em busca de vulnerabilidades nos laboratórios, encontrando tanto as vulnerabilidades digitais quanto as físicas e gerar relatório gerencial para Escola Politécnica e de Artes.

Visando o aprofundamento no tema estudado, trabalhos futuros podem ser realizados centrados nas etapas subsequentes como o processo de ataque propriamente e manutenção de acesso, em vista da ausência desses processos no atual trabalho.

Por meio do estudo das metodologias e ferramentas utilizadas foi possível compreender o processo por trás de um ataque, seja ele interno ou externo, visualizando suas etapas e compreendendo o funcionamento das ferramentas utilizadas de acordo com o contexto em que o ataque irá ocorrer.

Por fim foi possível compreender a importância e complexidade por trás deste método de testagem e suas ferramentas, atingindo assim os objetivos propostos. A compreensão desta área de atuação é de grande importância, os conhecimentos adquiridos certamente servirão como base para o aprofundamento nos estudos desta área.

BIBLIOGRAFIA

ABNT. ABNT NBR ISO/IEC 27002:2013 - Tecnologia da informação - Técnicas de segurança - Código de práticas para controles de segurança da informação. Rio de Janeiro: ABNT, 2013.

ABNT. ABNT NBR ISO/IEC 27005:2011 - Gestão de riscos para a segurança da informação - Diretrizes. Rio de Janeiro: ABNT, 2011.

BRASIL. Decreto nº 11.491, de 12 de abril de 2023. Institui o Programa Nacional de Segurança Cibernética (PNSC). Diário Oficial da União: seção 1, Brasília, DF, ano 161, n. 71, p. 1, 13 abr. 2023.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Cria o crime de invasão de dispositivo informático. Diário Oficial da União, Brasília, DF, 30 nov. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 19 out. 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2023].

BRASIL. Presidência da República. Lei nº 12.965, de 23 de abril de 2014. Dispõe sobre o Marco Civil da Internet. Diário Oficial da União: seção 1, Brasília, DF, ano 151, n. 80, p. 1-9, 24 abr. 2014.

Controle Net. O que é FreeBSD e quais são suas aplicações?. Controle Net. Disponível em: https://www.controle.net/faq/o-que-e-freebsd-e-quais-sao-suas-aplicacoes. Acesso em: 10 nov. 2024.

Criptografia e Segurança de Redes - 6ª Ed. / William Stallings. São Paulo: Pearson, 2014.

FORTINET. FortiGuard Labs reports destructive wiper malware increases over 50 percent. Fortinet, 2023. Disponível em: https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2023/fortiguard-labs-reports-destructive-wiper-malware-increases-over-50-percent. Acesso em: 20 out. 2023.

Fundamentos de segurança da informação com base na ISO/IEC 27001 e na ISO/IEC 27002 / José Carlos de Oliveira. 1. ed. São Paulo: Novatec, 2019.

Gestão de Segurança da Informação: uma visão executiva / Marcos Semola. 1. ed. São Paulo: Novatec, 2013.

Governança da Segurança da Informação / Maurício Rocha Lyra. 1. ed. São Paulo: Novatec, 2015.

IBGE. Censo 2022. IBGE, 2023. Disponível em: https://censo2022.ibge.gov.br/panorama. Acessado em: 20 out. 2023

IBM. O que é VMware?. IBM, 2024. Disponível em: https://www.ibm.com/br-pt/topics/vmware. Acessado em: 10 nov. 2024

MORENO, Daniel. Introdução ao Pentest. 1. ed. Rio de Janeiro: Novatec, 2015.

MORENO, Daniel. Pentest em redes sem fio. 1. ed. Rio de Janeiro: Novatec, 2017.

Posesa. Crimes Cibernéticos: o que são, leis aplicáveis e mais. Posesa. Disponível em <https://posesa.com.br/crimes-digitais-leis-aplicaveis/>. Acesso em: 19 out. 2023.

Prolinx. Pentest: Conheça As Principais Metodologias E Padrões. Prolinx, 2022. Disponivel em https://prolinx.com.br/pentest/#pentest-metodologias. Acesso em: 22 out. 2023.

PUC Go. PUC em dados. PUC Go, 2021. Disponivel em https://www.pucgoias.edu.br/puc-em-dados/2021-1/. Acesso em: 25 out. 2024

Sackel, André. Normas para a segurança da informação: Uma visão geral. DQS do Brasil. Disponível em <https://www.dqsglobal.com/pt-br/academy/blog/normas-para-a-seguranca-da-informacao-uma-visao-geral>. Acesso em: 19 out. 2023.

Segurança da informação - Uma visão sistêmica para implantação em organizações / Pedro Tenório. 1. ed. Rio de Janeiro: Elsevier, 2019.

Segurança de Computadores - Princípios e Práticas - 2ª Ed. / William Stallings. São Paulo: Pearson, 2014.

WEIDMAN, Georgia. Testes de Invasão Uma introdução prática. 1. ed. Rio de Janeiro: Alta Books, 2014.

6 ANEXO I – MODELO DE CONTRATO PARA PENTEST

CONTRATO DE REALIZAÇÃO DE SERVIÇOS DE TESTE DE INTRUSÃO (PENTEST)

CONTRATADO:

Sr., brasileiro, _____, portador do RG nº _____ e inscrito no CPF sob nº _____.

CONTRATANTE:

_____ , estabelecida na Rua _____, inscrita no CNPJ sob nº _____, neste ato representada pelo Sr/Sra. _____, brasileiro, _____, portador do RG nº _____ e inscrito no CPF sob nº _____.

As partes acima identificadas têm, entre si, justo e acertado o presente Contrato de Realização de Serviços de Teste de Intrusão (Pentest), que se regerá pelas cláusulas seguintes e pelas condições descritas no presente.

1. DO OBJETO

O presente contrato tem por objeto, a realização de Teste de Intrusão (Pentest), a ser realizado pelo CONTRATADO junto à CONTRATANTE, sendo que referidos testes somente poderão ser realizados nos dias e horários acordados, discriminados na Cláusula 2ª.

O CONTRATADO conduzirá um PENETRATION TESTING contra a infraestrutura, sistema e redes internas da instituição.

Tais testes consistem em simulações de ataques reais, resultando na descoberta de falhas da configuração e/ou vulnerabilidades. Vulnerabilidades estas que possam vir

a permitir que a CONTRATANTE sofra impactos com ataques direcionados, perdendo a disponibilidade, integridade e confidencialidade de informações e sistemas.

2. DA EXECUÇÃO DOS SERVIÇOS

2.1 Escopo

O PENETRATION TESTING escolhido foi do tipo BLACKBOX (Sem conhecimento de informações), ou seja, a única informação oferecida pela CONTRATANTE será o acesso às instalações e à rede.

O CONTRATADO tem permissão de explorar o Escopo em sua integralidade.

2.2 Limitações do Escopo

A CONTRATANTE determina as seguintes limitações à realização dos referidos testes:

- Ataques DoS e DDoS (Negação de Serviço), uma vez que, retirar o site de funcionamento, pode ocasionar grandes perdas e prejuízos ao negócio.
- Atacar sistema crítico localizado no IP _____ ou URL _____.

2.3 Janela de testes

Referidos testes, deverão ser realizados dentro do horário comercial, ou seja, de segunda à sexta-feira das 09:00 às 18:00 horas.

Todas as fases do teste poderão ser acompanhadas e supervisionadas a critério da CONTRATANTE. Caso opte pelo acompanhamento, tal supervisão somente poderá

ser realizada pelo responsável indicado e qualificado pela CONTRATANTE na Cláusula 3ª.

O teste de invasão deverá obedecer às seguintes fases:

1 Planejamento;
2 Descoberta;
3 Ataque (exploração);
4. Relatório de recomendações;
5. Reunião para apresentação do relatório de recomendações e descrição das atividades executadas durante o teste.

3. DAS RESPONSABILIDADES

A responsabilidade do CONTRATADO restringe-se à apenas detectar e apontar os riscos existentes com relação à integridade e vulnerabilidade dos sistemas da CONTRATANTE.

O trabalho desenvolvido pelo CONTRATADO **não** tem como objetivo corrigir as possíveis vulnerabilidades, tampouco, proteger a CONTRATANTE contra-ataques internos e externos.

As recomendações feitas pelo CONTRATADO devem ser validadas antes de serem colocadas em produção, o CONTRATADO não se responsabilizará por erros de implementações.

Será de responsabilidade da CONTRATANTE, garantir a segurança ao acesso dos relatórios entregues pela CONTRATADO, bem como a indicação dos responsáveis pelo acompanhamento da realização dos referidos testes, sendo a pessoa indicada pela CONTRATANTE, devidamente qualificada abaixo:

Responsável nomeado pela CONTRATANTE:

Nome: _____
CPF: _____
RG: _____
Telefone: _____
E-mail:_____
Ciente: _____

Ao CONTRATADO cabe a responsabilidade de garantir o sigilo total em relação às informações, falhas e outros dados sensíveis encontrados durante o procedimento de Teste de Intrusão (Pentest). O CONTRATADO assume a responsabilidade de manter as informações derivadas do procedimento em total e absoluto sigilo por parte do mesmo, cabendo ao CONTRATANTE a decisão de divulgação ou não destas informações.

4. DO PRAZO CONTRATUAL

O presente contrato terá validade única e exclusivamente durante o período de realização da atividade contratada, ou seja, até a conclusão da disciplina CMP 1072 TRABALHO DE CONCLUSÃO DE CURSO II por parte do CONTRATADO, a partir da data da assinatura do presente contrato, podendo ser prorrogado por comum acordo entre as partes até a conclusão dos serviços contratados.

O presente contrato poderá ser rescindido ocorrendo pelo menos uma das seguintes situações:

a) por mútuo consentimento;

b) por qualquer das partes, mediante manifestação por escrito com antecedência mínima de 7 (sete) dias, se a outra parte descumprir quaisquer obrigações assumidas no presente Contrato.

5. DA AUTORIZAÇÃO

Para que seja alcançado o objetivo da atividade CONTRATADA e, para que esta possa ser realizada em sua integralidade, a CONTRATANTE, neste ato, AUTORIZA a CONTRATADA, a realizar o Teste de Intrusão (pentest), objeto do presente contrato, devendo-se sempre, ambas as partes, assegurar a segurança das informações obtidas e fornecidas, bem como, cumprirem com seus deveres de confidencialidade de informações.

6. DAS CONDIÇÕES GERAIS

Este Contrato constitui o único documento que regula os direitos e obrigações das partes, com relação aos serviços contratados, ficando expressamente cancelado ou revogado, todo e qualquer entendimento ou ajuste porventura existente que não esteja explicitamente consignado neste Contrato.

Caso as partes envolvidas deixem de exigir em qualquer tempo o cumprimento de quaisquer cláusulas ou condições deste contrato, a parte prejudicada não ficará impedida de, quando o entender, fazer com que a parte inadimplente cumpra rigorosamente todas as condições contratuais.

E, por estarem justos e contratados, cientes e de acordo com todas as cláusulas e condições do presente Contrato de Realização de Serviços de Teste de Intrusão (Pentest), assinam este instrumento em duas vias para um só efeito na presença das testemunhas abaixo.

Goiânia, ____ de _____ de 20___

_____ _____

CONTRATADO CONTRATANTE

Testemunha:

Nome:_____

RG:_____

CPF:_____