PONTIFÍCA UNIVERSIDADE CATÓLICA DE GOIÁS

ESCOLA POLITECNICA

GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

PENTEST BASEADO EM IMAGENS ENCASE: UMA ANÁLISE DE VULNERABILIDADES EM SERVIDORES WEB

LÍDIA PAULA DE OLIVEIRA SILVA

GOIÂNIA

2024

LÍDIA PAULA DE OLIVEIRA SILVA

PENTEST BASEADO EM IMAGENS ENCASE: UMA ANÁLISE DE VULNERABILIDADES EM SERVIDORES WEB

Trabalho de Conclusão de Curso apresentado á Escola Politécnica da Pontifícia Universidade Católica de Goiás, como parte dos requisitos para conclusão do curso de Ciências da Computação.

Orientador(a): Prof. Mestre Claudio Martins Garcia

GOIÂNIA

2024

Sumário

LÍDIA PAULA DE OLIVEIRA SILVA

PENTEST BASEADO EM IMAGENS ENCASE: UMA ANÁLISE DE VULNERABILIDADES EM SERVIDORES WEB

Trabalho de Conclusão de Curso aprovado em sua forma final pela Escola Politécnica, da Pontifícia Universidade Católica de Goiás, para obtenção do título de Bacharel em Ciências de Computação, em _____/_____/_____.

_____

Prof. Ma. Ludmilla Reis Pinheiro Dos Santos
Coordenadora de Trabalho de Conclusão de Curso

Banca examinadora:

_____

Orientador(a): Prof. Me Claudio Martins Garcia

_____

Prof. Dr Nilson Cardoso Amaral

_____

Prof. Me Olegário Correa Da Silva Neto

GOIÂNIA
2024

RESUMO

Este trabalho apresenta a criação de um laboratório de estudo de Pentest utilizando imagens EnCase, demonstrando sua eficácia no desenvolvimento de habilidades técnicas e práticas em segurança da informação. O laboratório proporciona um ambiente controlado e realista para a aplicação de técnicas de teste de penetração, essencial para a formação de profissionais qualificados. Propõe-se, para trabalhos futuros, a implementação de redes mais robustas, simulações de ataques avançados, e o estudo de tecnologias de segurança avançadas, visando aprofundar o conhecimento e preparar os alunos para os desafios do mercado de cibersegurança.
Palavras-chave: Pentest, segurança da informação, imagens EnCase, laboratório de testes, prevenção de intrusão.

Abstract

This work presents the creation of a Pentest study laboratory using EnCase images, demonstrating its effectiveness in developing technical and practical skills in information security. The laboratory provides a controlled and realistic environment for the application of penetration testing techniques, essential for the training of qualified professionals. It is proposed, for future work, the implementation of more robust networks, simulations of advanced attacks, and the study of advanced security technologies, aiming to deepen knowledge and prepare students for the challenges of the cybersecurity market.

Keywords: *Pentest, information security, EnCase images, testing laboratory, intrusion prevention.*

1 Introdução

O *pentest*, ou teste de penetração, é uma prática que simula ataques reais a sistemas de clientes específicos, visando identificar riscos e brechas de segurança (Weidman, 2014)

Durante esses testes, o profissional responsável, também conhecido como *pentester*, procura identificar possíveis vulnerabilidades exploráveis por invasores, compreendendo como tais invasores poderiam obter informações do sistema em caso de sucesso (Weidman, 2014)

Os testes de penetração podem variar de acordo com o sistema analisado, sendo comuns em redes cabeada e sem fio, aplicações web, revisão de código-fonte e desenvolvimento de programas exploratórios para outras vulnerabilidades em softwares (Monteiro, 2015)

Embora as técnicas de *pentest* sejam empregadas na prevenção de invasões, é crucial destacar que essas mesmas técnicas e ferramentas podem ser exploradas de forma maliciosa, resultando em danos à vítima (Monteiro, 2015)

A invasão de sistemas é tipificada como acesso não autorizado a um sistema informatizado, com o propósito de obter, alterar ou destruir dados. A Lei Geral de Proteção de Dados (LGPD) regula o uso de dados e prevê penalidades, incluindo processos administrativos e criminais, além de penas de reclusão de um a quatro anos (Monteiro, 2015).

Devido a isso, foram criadas leis que regulamentam o uso dos dados de terceiros e a forma como eles são manipulados. De acordo com a Lei Geral de Proteção de Dados (LGPD), o infrator pode enfrentar processos administrativos e criminais, além de pena de reclusão, que pode variar de um a quatro anos de reclusão. Além disso, existem medidas que podem levar ao aumento da pena, podendo chegar a oito anos de reclusão e multa.

Em caso de conhecimento prévio pela empresa responsável de falhas que possam resultar no vazamento de dados, a LGPD impõe sanções administrativas, incluindo multas de até 2% do faturamento anual, limitadas a 50 milhões (Lei nº 13.709, de 14 de agosto de 2018)

Entretanto, quando falamos sobre roubo de dados e questões relacionadas, o senso comum nos traz a visão de uma pessoa atrás de um computador, usando várias técnicas avançadas e complexas. No entanto, a forma mais usada para obtenção de dados é mais simples do que se imagina. (MITNICK, 2003)

Ao abordar o roubo de dados, é essencial considerar a engenharia social, descrita por Kevin MITNICK em 'A Arte de Enganar'. Essa técnica envolve a habilidade do atacante em manipular

pessoas, utilizando charme e educação para estabelecer afinidade e confiança, sendo uma abordagem eficaz para a obtenção de informações-alvo (MITNICK, 2003).

Desta forma a abordagem escolhida para que seja possível o estudo de técnicas de *pentest* foi a utilização de imagens encase, uma vez que essas imagens são copias estáticas de um sistema. (Raedts,2007)

Com a utilização dessas copias do sistema, é possível explorar os seus ecossistemas sem se preocupar com as possíveis reações que poderiam ocorrer no mundo real, além de com essa abordagem é possível ter uma experiencia mais vivida, mas sem desrespeitar a LGPD.

Essa cópia pode ser adquirida a partir de um processo de cópia de um sistema ou através de sites como o do professor Ali Hadi ou em sites como o CFREDS, um site administrado pelo *National Institute of Standards and tecnology* que disponibilizam imagens encase de forma publica para que qualquer pessoa possa as utilizar para estudo.

1.1 Motivação

A segurança cibernética se tornou um pilar fundamental na era digital, protegendo informações confidenciais e sistemas críticos contra-ataques cibernéticos cada vez mais sofisticados. Nesse contexto, os testes de penetração (*PenTest*) assumem um papel crucial na identificação e mitigação de vulnerabilidades em sistemas de informação.

Este Trabalho de Conclusão de Curso (TCC) propõe a investigação e aplicação de *pentest* baseados em imagens encase para analisar vulnerabilidades em servidores web. A escolha de imagens encase permite o estudo de *pentest* em ambientes que simulam o mundo real, onde o *pentester*, dependendo da abordagem utilizada, terá o mínimo ou nenhuma informação prévia sobre o sistema. Essa metodologia é essencial para reproduzir as condições reais de um ataque cibernético, proporcionando uma análise mais precisa e eficaz das vulnerabilidades.

A utilização de imagens encase também oferece um ambiente controlado e seguro para a realização dos testes, evitando riscos associados ao uso de dados reais, que poderiam violar normas de proteção de dados.

Portanto, a motivação para a realização deste TCC é dupla: aprimorar a compreensão e aplicação prática dos testes de penetração em condições que imitam o mundo real, e assegurar que as organizações estejam em conformidade com as exigências legais e normativas de proteção de dados. Ao explorar e aplicar técnicas avançadas de *pentest* utilizando imagens

encase, este trabalho contribuirá para o fortalecimento da segurança cibernética e a proteção das informações sensíveis em um cenário de ameaças crescentes.

1.2 Objetivo Geral:

Investigar e aplicar *pentest* baseados em imagens encase para analisar vulnerabilidades em servidores web, contribuindo para a aprimoramento da segurança de infraestruturas web.

1.2.1 Objetivos Específicos:

Aprimorar o conhecimento teórico sobre *pentest*, imagens encase, segurança de servidores web e metodologias de pesquisa científica.

Analisar a viabilidade da aplicação de *pentest* baseados em imagens encase para servidores web, considerando aspectos técnicos, práticos e éticos.

Desenvolver um plano de *pentest* baseado em imagens encase para servidores web, incluindo técnicas de coleta de dados, análise de vulnerabilidades e geração de relatórios.

Implementar o plano de *pentest* em um ambiente virtual utilizando imagens Encase de um servidor web real.

Identificar e documentar as vulnerabilidades encontradas no servidor web durante o *pentest*.

Propor medidas de mitigação para as vulnerabilidades identificadas, considerando aspectos técnicos, financeiros e de tempo.

1.3 Laboratório de Estudo em Imagens Encase

A utilização de imagens encase como laboratório de estudo para *pentest* de servidores web oferece diversas vantagens:

- **Segurança:** Elimina o risco de comprometer a infraestrutura real durante os testes.
- **Repetibilidade:** Permite realizar testes repetidamente sob as mesmas condições, facilitando a comparação de resultados e a avaliação da efetividade das medidas de segurança.
- **Flexibilidade:** Possibilita a simulação de diversos cenários de ataque, incluindo ataques sofisticados e direcionados.
- **Eficiência:** Permite otimizar o tempo e os recursos necessários para realizar *pentest*, pois não há necessidade de configurar e gerenciar ambientes reais.

- **Controle:** Oferece maior controle sobre o ambiente de teste, permitindo que os profissionais de segurança se concentrem em áreas específicas de interesse.

1.4 Metodologia

A metodologia de pesquisa deste Trabalho de Conclusão de Curso (TCC) será composta pelas seguintes etapas:

1. Revisão Bibliográfica: Será realizada uma revisão bibliográfica abrangente para aprofundar o conhecimento sobre testes de penetração (*pentest*), imagens encase. Esta etapa visa fundamentar teoricamente o estudo e identificar as melhores práticas e abordagens utilizadas na área.
2. Estudo de Caso: Um estudo de caso será conduzido para demonstrar a aplicação prática de *pentest* baseados em imagens encase na identificação de vulnerabilidades em servidores web. Este estudo permitirá avaliar a eficácia e a aplicabilidade das técnicas em um cenário que simula condições reais de segurança cibernética.
3. Análise de Dados: Os dados coletados durante o estudo de caso serão analisados detalhadamente para identificar as vulnerabilidades presentes no servidor web. A análise incluirá a classificação das vulnerabilidades, a avaliação de seu impacto potencial e a identificação de padrões de segurança.
4. Discussão dos Resultados: Os resultados obtidos serão discutidos em relação à viabilidade e eficácia de *pentest* baseados em imagens encase para avaliar a segurança de servidores web. Esta discussão abordará os pontos fortes e as limitações da abordagem, bem como sugestões para pesquisas futuras e melhorias na metodologia.

Essa estrutura metodológica permitirá uma abordagem sistemática e rigorosa para investigar a aplicação de *pentest* com imagens encase, contribuindo para o avanço do conhecimento na área de segurança cibernética e fornecendo insights valiosos para a prática profissional.

2 Revisão Bibliográfica

2.1 Marco Civil da Internet

Com o avanço da internet no Brasil, foi promulgada em 2014 a Lei nº 12.965, conhecida como Marco Civil da Internet, que estabelece os princípios, garantias, direitos e deveres para o uso da internet no país.

A Lei nº 12.965, conhecida como Marco Civil da Internet, foi promulgada em 2014 e estabelece os princípios, garantias, direitos e deveres para o uso da internet no país. Entre eles estão:

I - Inviolabilidade da intimidade e da vida privada, com proteção e indenização por dano material ou moral decorrente de sua violação;

II - Inviolabilidade e sigilo do fluxo de suas comunicações pela internet, exceto por ordem judicial, conforme estabelecido em lei;

III - Inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;

VII - Não fornecimento a terceiros de seus dados pessoais, incluindo registros de conexão e acesso a aplicações de internet, exceto mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei.

Nos artigos 10 e 11, determina-se que toda guarda e registro de acesso a aplicações web devem obedecer às leis vigentes no país, mesmo que ocorram no exterior. Isso ocorre porque qualquer ato ocorrido em território brasileiro deve respeitar a legislação brasileira vigente. Ainda é importante ressaltar que nenhum dado privado pode ser disponibilizado para terceiros sem ordem judicial.

No artigo 12, são abordadas as consequências das infrações às normas dos artigos 10 e 11, sem prejuízo das demais sanções cíveis, criminais ou administrativas. Essas sanções podem ser aplicadas de forma isolada ou acumulativa e incluem:

I - Advertência, com indicação de prazo para adoção de medidas corretivas;

II - Multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no último exercício, excluídos os tributos, considerando a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;

III - Suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou

IV - Proibição do exercício das atividades que envolvam os atos previstos no art. 11.

Parágrafo único: No caso de empresa estrangeira, sua filial, sucursal, escritório ou estabelecimento situado no país responde solidariamente pelo pagamento da multa mencionada no caput.

2.2 Lei Geral de proteção de dados

Com a criação da primeira lei para regulamentação da internet no Brasil, em 2014, conhecida como Marco Civil da Internet, foi criada também a Lei Geral de Proteção de Dados, que trata sobre como deve ser feito o tratamento de dados pessoais, de forma digital ou não, para pessoas naturais ou jurídicas.

Essa lei tem como objetivo proteger os direitos fundamentais da pessoa natural à liberdade, à privacidade e ao livre desenvolvimento da personalidade.

No artigo 2º da LGPD, são estabelecidos os fundamentos para a proteção de dados, sendo eles:

I - o respeito à privacidade;

II - a autodeterminação informativa;

III - a liberdade de expressão, de informação, de comunicação e de opinião;

IV - a inviolabilidade da intimidade, da honra e da imagem;

V - o desenvolvimento econômico e tecnológico e a inovação;

VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e

VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Indo para o artigo 6°, é definido que deverá seguir os princípios de:

I - Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

2.2.1 Requisitos para o Tratamento de Dados Pessoais

Junto com a lei também foram determinados requisitos para que seja feito tratamentos com os dados pessoais coletados, no artigo 7° está previsto que só será permitido o tratamento de dados uma vez que seja dado o consentimento do titular, como também para que seja feito cumprir obrigações legais ou regulatória pelo controlador ou então para outros processos legais, mas nunca indo contra direitos e liberdades fundamentais do título que venha a exigir a proteção dos dados pessoais, como também para a proteção de credito.

Mas ainda na clausula 4° é previsto que em casos de dados que foram manifestados como públicos pelo seu titular não é necessário o seu consentimento para o uso desses dados.

Logo em seguida no art 8° é definida com forma de consentimento deve ser registrada de forma escrita ou então de outra forma que demonstre que a aceitação do titular.

2.2.2 Tratamento de Dados Pessoais Sensíveis

Os chamados dados pessoais sensíveis são todos os dados que possam revelar origem racial ou étnica, convicções religiosas ou filosóficas, opiniões políticas, filiação sindical, questões genéticas, biométricas e sobre a saúde ou a vida sexual de uma pessoa. (SERPRO,2018)

Devido a isso, existem regras que devem ser seguidas para seu tratamento correto. Essas regras são previstas no artigo 11º da lei, que prevê que os dados pessoais sensíveis só podem ser usados nos seguintes casos:

I - Quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;

b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

e) proteção da vida ou da incolumidade física do titular ou de terceiros;

f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (Redação dada pela Lei nº 13.853, de 2019) Vigência

g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

§ 1º Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica.

§ 2º Nos casos de aplicação do disposto nas alíneas "a" e "b" do inciso II do caput deste artigo pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 desta Lei.

§ 3º A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências.

§ 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir: (Redação dada pela Lei nº 13.853, de 2019) Vigência

I - a portabilidade de dados quando solicitada pelo titular; ou (Incluído pela Lei nº 13.853, de 2019) Vigência

II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo. (Incluído pela Lei nº 13.853, de 2019) Vigência

§ 5º É vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários. (Incluído pela Lei nº 13.853, de 2019) Vigência

2.3 Propriedades e princípios de segurança da computação

De acordo com Carlos Maziero, em seu livro Sistemas Operacionais: Conceitos e Mecanismos, para garantir a segurança de um sistema de computação, é necessário garantir algumas propriedades fundamentais às informações e recursos existentes no sistema. Essas propriedades são:

- **Confidencialidade**: os recursos presentes no sistema só podem ser acessados por pessoas autorizadas.
- **Disponibilidade**: os recursos devem estar disponíveis a todo momento para que os usuários autorizados possam utilizá-lo.
- **Integridade**: os recursos só serão modificados por pessoas autorizadas.
- **Autenticidade**: os dados e informações contidas no sistema são autênticos e genuínos, garantindo que correspondam exatamente ao que representam no mundo real, como a origem dos dados dos arquivos ou a identidade dos usuários.
- **Irretratabilidade**: este recurso garante que qualquer alteração feita no sistema seja registrada e que seja possível identificar o autor da alteração.

Para garantir esses princípios básicos, existem algumas medidas que podem ser tomadas na elaboração de um sistema de computador, como:

- **Privilégio mínimo**: cada usuário deve ter o mínimo possível de privilégios ou permissões de acesso para que possa realizar suas atividades.
- **Separação de privilégios**: esse conceito consiste em ser necessário mais de um controle ou regra para que seja feita determinada ação, tornando assim mais robusta sua proteção, pois mesmo que um atacante burle uma parte do sistema ainda não poderá acessar determinado recurso.
- **Mediação completa**: todos os acessos que sejam feitos de forma direta ou de forma indireta devem passar por mecanismos de verificação de segurança. Além de estarem organizados de forma que não seja possível burlá-los.
- **Default seguro**: o mecanismo de segurança deve saber identificar caso ocorra algum acesso que não seja permitido ou malicioso, fazendo com que esse acesso seja negado.

2.4 Pentest

O teste de penetração, também conhecido como *pentest*, é uma bateria de testes realizada de forma metodológica que podem ser aplicados em sistemas operacionais, redes de

computadores, websites, redes sem fio, bancos de dados, aplicativos e programas. (WEIDMAN,2014)

Com o objetivo de descobrir, mapear e expor possíveis vulnerabilidades, as corporações podem criar meios de defesa adequados com esse conhecimento em mãos. (MORENO,2015)

A meta do *pentest* é encontrar falhas para corrigi-las. Ele não é usado para obter acesso não autorizado a um sistema ou servidor. (MORENO,2015)

Ao final de cada bateria de testes, é necessário criar um relatório com as vulnerabilidades encontradas e as correções necessárias. Esse relatório deve ser entregue ao cliente que solicitou o *pentest*. (MORENO,2015)

Para a aplicação do *pentest* existem várias metodologias, sendo elas SSTMM e OWASP as mais conhecidas e utilizadas. (MORENO,2015)

2.5 Categoria de *pentest*

Existem três tipos de categoria de *pentest*, onde cada categoria se diferencia do nível de conhecimento do auditor pela infraestrutura da rede e todo o seu funcionamento, sendo elas: *black-box*, *white-box* e *gray-box*. (MORENO,2015)

2.5.1 *Black-box*

Esse cenário ocorre quando, nesse tipo de teste, o auditor de segurança não possui nenhum conhecimento prévio sobre o mapeamento da infraestrutura do alvo. (MORENO,2015)

Sendo esse o cenário mais típico de ataques de invasão externas, pois os invasores muitas vezes não possuem informações sobre a infraestrutura. Usando scripts automatizados é possível encontrar falhas e vulnerabilidades escaneando redes e assim ir se aprofundando em como conseguir mais informações e dados da vítima. (MORENO,2015)

Ainda existem duas subcategorias de teste *black-box*: *blind*, onde o auditor não possui nenhuma informação e o alvo sabe o que será atacado e quais os testes que serão feitos; e *double blind*, onde o auditor não possui nenhuma informação e o alvo não sabe que será atacado ou quais os testes e metodologias usadas. (MORENO,2015)

2.5.2 *White-box*

Neste cenário, ao contrário do *black-box*, o auditor possui todas as informações necessárias sobre a infraestrutura da rede a ser testada. (MORENO,2015)

Esse tipo de teste é bastante eficiente para analisar possíveis vulnerabilidades existentes em caso de ataques internos, como por exemplo, quando um funcionário quer prejudicar a empresa, obter um dado para benefício próprio ou quando o auditor faz uma revisão no código-fonte. (MORENO,2015)

Nessa categoria, também existem duas subcategorias:

- ***Tandem***: o auditor possui todas as informações da rede a ser testada e o alvo sabe o que será atacado e quais testes serão feitos, também apelidado como caixa de cristal.
- ***Reversa***: o auditor possui total conhecimento da rede a ser testada, porém o alvo não sabe que será atacado.

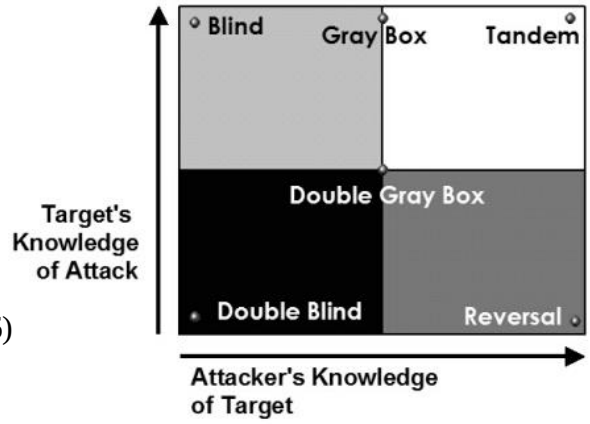
Por possuir todas as informações sobre a rede alvo, os testes de caixa branca tendem a ter um plano de teste mais específico e detalhado. Devido a isso, os testes de *white-box* costumam ter um tempo maior e possuem um maior custo que os testes de *black-box*, porém seu resultado se mostra muito mais efetivo. (MORENO,2015)

2.5.3 *Gray-box*

A *gray-box*, também conhecida como teste de caixa cinza ou apenas teste meio cego, é uma categoria de teste em que o auditor possui um conhecimento parcial da rede testada, combinando os testes de caixa preta com os testes de caixa branca. Assim como as outras categorias, a *gray-box* possui duas subcategorias:

Gray-box: o auditor tem conhecimento parcial e o alvo sabe o que será atacado e os testes a serem realizados.

Double gray-box: o auditor tem conhecimento parcial do sistema e o alvo não sabe que será atacado ou então os testes que serão feitos.



Fonte: (HERZOG, 2010, p. 36)

2.6 Metodologias de *pentest*

Devido aos vários tipos de sistemas que podem ser testados, é necessário que exista várias metodologias de *pentest*, cada uma com sua própria efetividade, dependendo do cenário e escopo do projeto. (RUFINO,2015)

Sendo elas:

• OSSTMM (*Open Source Security Testing Methodology Manual*).

• ISSAF (*Information Systems Security Assessment Framework*).

• OWASP (*Open Web Application Security Project Top Ten*).

• WASC-TC (*Web Application SecurityConsortium Threat Classification*).

As duas primeiras metodologias são aplicáveis a sistemas em geral, enquanto as duas últimas são específicas para servidores web. (RUFINO,2015)

A escolha da metodologia é uma etapa importante, pois é através dela que serão definidos os passos do teste, de acordo com o escopo do projeto. (RUFINO,2015)

2.7 Metodologia OSSTMM

O OSSTMM é uma metodologia de *pentest* aberta e livre. Ela foi desenvolvida pela ISECOM (*Institute for Security Open Methodologies*), uma organização internacional que promove a segurança da informação. (BERTOGLIO,2015)

A metodologia OSSTMM é baseada em um ciclo de vida que consiste em cinco fases:

1. **Reconhecimento:** O testador coleta informações sobre o alvo, como endereços IP, portas abertas, serviços em execução, sistemas operacionais, arquitetura de rede, políticas de segurança etc.
2. **Mapeamento de rede:** O testador identifica a topologia de rede do alvo, incluindo os hosts, firewalls, dispositivos de segurança etc.
3. **Identificação de vulnerabilidades:** O testador identifica vulnerabilidades técnicas nos sistemas e aplicações do alvo, como vulnerabilidades de softwares, vulnerabilidades de configuração, vulnerabilidades de hardware etc.
4. **Exploração:** O testador explora as vulnerabilidades identificadas para obter acesso não autorizado ao alvo.
5. **Relatório:** O testador gera um relatório que descreve os resultados do teste de penetração, incluindo recomendações de remediação. (ISECOM,2010).

A metodologia OSSTMM é uma ferramenta valiosa para profissionais de segurança da informação que desejam realizar *pentest* de forma mais eficaz. Ela fornece uma estrutura abrangente e flexível que pode ser adaptada para atender às necessidades específicas de cada projeto. (ISECOM,2010)

2.8 Metodologia ISSAF

A metodologia ISSAF é um framework que pode modelar os requisitos de controle interno para que seja feita a segurança das informações e assim poder avaliar o nível de segurança da rede interna de uma empresa além de também para sistemas e aplicações. (BERTOGLIO,2015)

Essa metodologia possui três áreas de atuação, que se dividem em várias outras atividades, sendo elas: planejamento e preparação, avaliação e relatório e por fim a fase de limpeza e destruição de artefatos. (BERTOGLIO,2016)

O processo de planejamento e preparação é o processo inicial, onde é definido o ambiente onde será feito os testes, planejamento de testes e ferramentas a serem usadas, contratos e todo o âmbito legal, os prazos e requisitos a serem alcançados. (BERTOGLIO,2016)

Já a fase de avaliação e relatório é onde acontece a aplicação do *pentest* em si, onde essa etapa é dividida em nove atividades sendo elas:

1. **Coleta de informações**: Primeira etapa e a mais importante, onde é feita toda a coleta das informações sobre o alvo que será feito os testes. Em alguns casos a principal e única fonte de informação sobre o alvo é a internet. O objetivo geral dessa etapa é achar todas as possíveis formas de ataque, tendo assim uma visão geral do alvo.
2. **Mapeamento da rede:** Essa etapa consiste em conseguir informações mais especificas sobre a rede alvo, a partir da coleta feita anteriormente, essa etapa é feita para conseguir produzir a topologia de rede usada pelo alvo e poder traçar as estratégias de ataque. O auditor busca identificar todos os hosts vivos, sistemas operacionais usados, firewalls, sistema de detecção de intrusão, servidores de serviços e toda a sua topologia de rede.
3. **Identificação de vulnerabilidade:** Já de posse dos dados da infraestrutura e da topologia de rede, já é possível buscar as falhas existentes na rede, servidor, serviço entre outros recursos que o alvo pode vir a usar. Podendo começar a utilizar de ferramentas e técnicas para poder identificar possíveis falhas e vulnerabilidades no sistema.
4. **Penetração:** É a etapa onde o auditor testa as vulnerabilidades antes identificadas
5. **Acesso e Escalada de Privilégio:** Essa atividade é possível após conseguir acesso interno através das atividades anteriores e conseguir ir escalando o privilégio de acesso a rede alvo.
6. **Enumeração:** Conseguindo ter acesso aos privilégios de acesso são feitos os monitoramentos e análises de tráfego, coleta de cookie, coleta de e-mails, identificação de rotas de rede e mapeamento das redes internas.
7. **Comprometer usuários remotos:** Nessa etapa é comprometido o acesso de usuários remotos a rede interna do alvo.
8. **Manutenção de acesso:** Após obter acesso ao alvo, o auditor deve manter os meios de comunicação com a rede. Essa comunicação é importante para que o auditor possa continuar realizando seus testes, como exploração de vulnerabilidades e coleta de informações. Para diminuir as chances de ser detectado, é necessário que a comunicação seja realizada por um canal secreto.

9. **Cobrindo rastros:** E para finalizar essa atividade tem como objetivo esconder ferramentas que foram utilizadas durante o comprometimento da rede do alvo. (BERTOGLIO,2016)

E por fim temos a última fase da metodologia que é a fase de Relatório, Limpeza e Destruição de Artefatos, onde é feiro o processo pós invasão do teste. Essa etapa consiste na elaboração de um relatório completo sobre as vulnerabilidades encontradas e a destruição efetiva dos artefatos construídos durante a fase de avaliação. (BERTOGLIO ,2015)

2.9 OWASP

OWASP, é uma organização internacional sem fins lucrativos, formada por desenvolvedores, profissionais de segurança e acadêmicos. Que juntos tem a missão de compartilhar seu conhecimento e ferramentas para melhorar a segurança na web, tornando os sistemas web mais seguros.

Essa organização possui como principais recursos: o OWASP Top 10, que consiste em um documento com os dez principais riscos de segurança da web; OWASP *Cheat Sheet Series*, que ensina a como evitar as vulnerabilidades mais comuns de segurança; OWASP *Testing Guide*, que possui um guia de testes de segurança que podem ser feitos em aplicações web; OWASP *Code Review Guide*, um guia de como fazer uma revisão de código que garanta maior segurança ao sistema. (OWASP,2021)

2.9.1 Top 10 OWASP

Possuindo sua última atualização em 2021, o top 10 OWASP possui os dez principais riscos de segurança na web, na sua alteração de 2021 foram acrescentadas três novas vulnerabilidades, enquanto as demais tiveram apenas uma mudança de posição.

2.9.1.1 Broken Access Control

Essa forma de ataque consiste em burlar os controles de acesso do usuário, permitindo que o atacante tenha acesso a informações que deveriam estar ocultas ao usuário. Permitindo assim a possibilidade de modificação e até mesmo a destruição de dados.

Algumas formas de ser feito isso é através de alteração na URL (*Uniform Resource Locator*) modificando seus parâmetros ou tentando uma navegação forçada ou então usando ferramentas próprias de ataque para que seja possível modificar as solicitações feitas pela API

(*Application Programming Interface*), manipulação de metadados como a adulterar o token de acesso. (OWASP,2021)

2.9.1.2 Cryptographic Failures

Alguns dados como senhas, números de cartão de crédito, registros de saúde e segredos comerciais necessitam de uma forma de proteção extra, visto que como previsto na LGPD em caso de vazamento desses dados as empresas podem sofrer punições legais.

Por isso alguns desses dados não podem trafegar na internet de forma pura, sendo necessário à sua criptografia, porém em alguns casos mesmo utilizando desse mecanismo de defesa as vezes é usado de forma errada, como por exemplo a utilização de algoritmos de criptografia fracos ou antigos. Ou até mesmo utilizar de funções hash obsoletas como o MD5(Algoritmo de Resumo de Mensagem) ou então o SHA1(Algoritmo de Hash Seguro) está entre as falhas de criptografia mais comuns. (OWASP,2021)

2.9.1.3 Injection

Esse problema de segurança acontece quando uma API recebe uma entrada de dados de uma fonte não confiável, a forma mais típica de fazer esses ataques é através de queries sql (*Structed Query Language*), *NoSql*, comandos de sistema operacional.

Um dos principais fatores que pode trazer essa vulnerabilidade para um sistema é a falta de validação nos dados que são fornecidos pelo usuário, podem inserir um código malicioso em qualquer entrada de dados. (OWASP,2021)

2.9.1.4 Insecure Design

Adicionada ao OWASP em 2021 esse problema de segurança é relacionado a um problema mais complexo, visto ainda antes da implementação do código-fonte, essa falha diz respeito ao design e arquitetura definida para um sistema, ela traz com sigo as chamadas enumerações de fraquezas comuns notáveis, mais conhecidas como CWEs.

Entre elas está incluso: a CWE-209:Geração de mensagens de erro contendo informações confidenciais, CWE-256:Armazenamento desprotegido de credenciais, CWE-501: Violação de limite de confiança e por último a CWE-522:Credenciais insuficientemente protegidas.

O design inseguro possui com sigo diferentes fraquezas, podendo ser expressa como “design de controle ausente ou ineficiente”, com tudo não podemos dizer que ele é a causa de

todas as falhas existentes no top 10. Mesmo com um design seguro pode vir a ter defeitos de implementação que gere outras vulnerabilidades. (OWASP,2021)

2.9.1.5 Security Misconfiguration

Além de ser possível ter vulnerabilidades que surgem do código-fonte ou do design de projeto escolhido, uma forma de gerar vulnerabilidades em um sistema é através de alguns erros de configuração no ambiente de produção, sendo algumas delas: falta de endurecimento de segurança de forma apropriada, permissões configuradas de forma incorreta nos serviços de nuvem, recursos desnecessários habilitados ou instalados, como por exemplo portas, serviços ou privilégios desnecessários.

Utiliza de softwares desatualizados ou vulneráveis ou então possui sistemas atualizados, porém os recursos de segurança estão desabilitados ou não estão configurados de maneira correta. (OWASP,2021)

2.9.1.6 Vulnerable and Outdated Components

Essa vulnerabilidade está mais ligada os softwares de terceiros usados para criar seu próprio sistema, uma vez que não é viável criar tudo do zero para fazer seu sistema, as empresas acabam usando ferramentas e softwares de outras.

Devido a isso algumas ações que podem deixar um sistema web vulnerável é a falta do conhecimento das versões destes softwares de terceiros, utilização de softwares que já foram descontinuados, assim trazendo vulnerabilidades por não possuírem mais suporte nem atualizações.

Isso vale tanto para os sistemas operacionais, como também para servidores, sistemas de gerenciamento de banco de dados, APIs e todos os componentes usados pelo sistema.

2.9.1.7 Identification and Authentication Failures

Nesta vulnerabilidade está presente uma falha na confirmação de identidade do usuário, autenticação e gerenciamento de sessão.

O sistema fica suscetível a falhas de autenticação caso permita senhas que sejam padrão, fracas ou conhecidas, permitindo assim que seja feito ataques de força bruta de forma muito mais fácil, usar processos de recuperação de credenciais e senhas fracos e ineficazes, expor o identificador de sessão na URL, reutilizar o identificador de sessão após login bem-sucedido.

2.9.1.8 Software and Data Integrity Failures

Outra categoria adicionada em 2021, essa categoria de vulnerabilidade está relacionada a suposições em relação a atualização dos softwares utilizados, dados críticos e pipelines CI/CD (Integração e entrega contínuas) sem verificar sua integridade.

O software fica propenso a esse tipo de vulnerabilidade quando o aplicativo utiliza de plugins, bibliotecas ou módulos de fontes não confiáveis, ou então ao utilizar de um pipeline inseguro. Muitos aplicativos agora incluem uma funcionalidade de atualizações automáticas, onde não é feita nenhuma verificação de integridade nessa nova versão, permitindo que a integridade dessa atualização seja verificada.

Assim, invasores podem enviar suas próprias versões de atualização e assim distribuindo e executando junto com as demais atualizações.

2.9.1.9 Security Logging and Monitoring Failures

Essa categoria tinha sido retirada no top 10 de 2017 e agora retorna para o top 10 em 2021, ela diz respeito ao monitoramento e registro dos logs, uma vez que os possuindo é possível detectar algum acesso estranho ou indevido.

Esse sistema de registro, detecção e monitoramento é de bastante importância, uma vez que é através dele que é possível ter uma resposta ativa contra qualquer movimentação e acesso suspeito.

Alguns erros nos sistemas de log como eventos auditáveis por exemplo: logins, logins com falha e transações de alto valor, não são registrados, os avisos de erro; avisos e erros geram mensagens de log inexistentes, inadequadas ou pouco claras; os logs de aplicativos, APIs não são monitorados quanto a atividades suspeitas; os logs são armazenados apenas localmente; o aplicativo não pode detectar, escalar ou alertar sobre ataques ativos em tempo real ou quase em tempo real.

2.9.1.10 Server-Side Request Forgery

Também adicionada no top 10 de 2021, essa categoria ocorre quando um aplicativo web tenta buscar um recurso sem validar a URL fornecida pelo usuário, fazendo com que o invasor possa obrigar o aplicativo a enviar uma solicitação criada para um destino inesperado, mesmo que seja protegido por um firewall, vpn ou outro tipo de lista de controle de acesso à rede.

Devido aos aplicativos web mais modernos permitir que os usuários finais tenham recursos mais convenientes, realizar a busca de uma URL está mais comum. Com isso o SSRF está se tornando uma forma de ataque mais comum, além do aumento da gravidade desse ataque devido aos serviços em nuvem e a complexidade das suas arquiteturas.

2.10 WASC-TC

A metodologia WASC-TC é uma metodologia de classificação de ameaças para aplicações web. Ela foi desenvolvida pelo Web Application Security Consortium (WASC), uma organização internacional que promove a segurança de aplicações web, assim como o OWASP. (BERTOGLIO,2016)

Na metodologia WASC-TC as ameaças a aplicações web são divididas em três categorias:

- **Ameaças externas:** Ameaças que são originadas de fora da aplicação web, como ataques de hackers ou malware.
- **Ameaças internas:** Ameaças que são originadas de dentro da aplicação web, como usuários mal-intencionados ou erros de programação.
- **Ameaças físicas:** Ameaças que são originadas do ambiente físico, como roubo de dados ou sabotagem.

Cada categoria é dividida em subcategorias, que são ainda divididas em técnicas de ataque. As subcategorias do WASC-TC são:

2.10.1 Ameaças externas

- **Ataques de exploração:** Ameaças que exploram vulnerabilidades conhecidas em aplicações web.
- **Ataques de engenharia social:** Ameaças que enganam os usuários para que eles forneçam informações confidenciais ou executem ações maliciosas.
- **Ataques de distribuição de malware:** Ameaças que distribuem malware para comprometer aplicações web.
- **Ataques de infraestrutura:** Ameaças que atacam a infraestrutura de uma aplicação web, como servidores, redes ou sistemas de banco de dados.

2.10.2 Ameaças internas

- **Usuários mal-intencionados:** Ameaças que são originadas de usuários mal-intencionados, como funcionários, parceiros ou clientes.
- **Erros de programação:** Ameaças que são originadas de erros de programação nas aplicações web.

2.10.3 Ameaças físicas

- **Roubo de dados:** Ameaças que envolvem o roubo de dados físicos, como mídias removíveis ou equipamentos de armazenamento.
- **Sabotagem:** Ameaças que envolvem a destruição deliberada de aplicações web.

Dentro de cada uma dessas subcategoria é dividido em técnicas de ataque. Sendo elas:

2.10.3.1 Ataques de exploração

- ***SQL injection*:** Uma técnica de ataque que injeta código SQL malicioso em uma aplicação web.
- ***Cross-site scripting (XSS)***: Uma técnica de ataque que injeta código JavaScript malicioso em uma aplicação web.
- ***Cross-site request forgery (CSRF)***: Uma técnica de ataque que força um usuário a realizar uma ação não intencional em uma aplicação web.

2.10.3.2 Ataques de engenharia social

- ***Phishing***: Um ataque que envia e-mails ou mensagens de texto falsos para enganar os usuários para que eles forneçam informações confidenciais.
- ***Social engineering*:** Um ataque que utiliza técnicas de persuasão para enganar os usuários para que eles executem ações maliciosas.

2.10.3.3 Ataques de distribuição de *malware*

- ***Malware:*** Um software malicioso que pode ser usado para comprometer uma aplicação web.
- ***Phishing*:** Um ataque que envia e-mails ou mensagens de texto falsos para distribuir malware.

2.10.3.4 Ataques de infraestrutura

- **DDoS:** Um ataque que inunda uma aplicação web com tráfego falso.
- **DoS:** Um ataque que impede o acesso a uma aplicação web.

2.10.3.5 Usuários mal-intencionados

- **Usuários com privilégios elevados:** Usuários que possuem privilégios elevados em uma aplicação web.
- **Usuários com acesso físico:** Usuários que possuem acesso físico a um servidor ou dispositivo de armazenamento.

2.10.3.6 Erros de programação

- **Vulnerabilidades de autenticação:** Vulnerabilidades que permitem que usuários não autorizados acessem uma aplicação web.
- **Vulnerabilidades de autorização:** Vulnerabilidades que permitem que usuários autorizados acessem recursos que não deveriam acessar.
- **Vulnerabilidades de integridade:** Vulnerabilidades que permitem que dados sejam modificados ou apagados sem autorização.

2.10.3.7 Roubo de dados

- **Roubos de mídias removíveis:** Roubos de mídias removíveis, como *pendrives* ou CDs, que contenham dados confidenciais.
- **Roubos de equipamentos de armazenamento:** Roubos de equipamentos de armazenamento, como servidores ou laptops, que contenham dados confidenciais.

2.10.3.8 Sabotagem

- **Destruição de equipamentos:** Destruição de equipamentos, como servidores ou switches, que hospedam aplicações web.
- **Interferência elétrica:** Interferência elétrica que pode interromper o funcionamento de aplicações web.

2.11 Imagens Encase

Dito pela primeira vez pelo Dr. Henry Lee, “Nunca toque, altere ou altere nada até que tenha sido documentado, identificado, medido e fotografado.”, acabou se tornando uma máxima na área forense e não seria diferente na área de perícia digital.

Porém, na área da computação existe uma vantagem que as demais áreas não possuem, sendo ela a capacidade de fazer uma cópia 100% idêntica das evidências. (Raedts,2007)

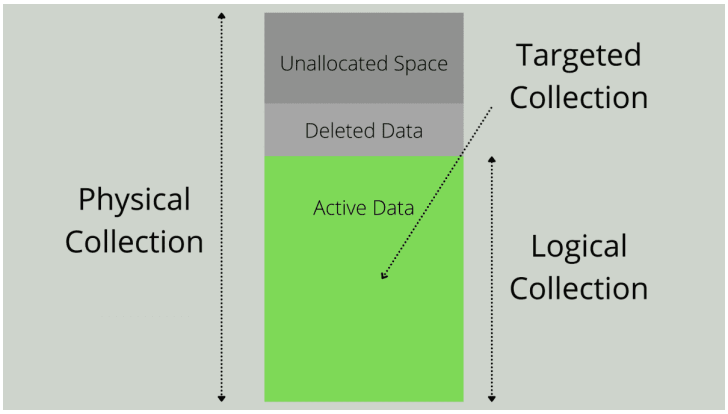
Para a criação dessas copias existem várias formas de fazê-la, porém todas tem um princípio em comum, a fonte de onde será feita a cópia deve ter alguma forma de bloquear funções de escrita, dessa forma só pode ser possível ler a unidade, mas nunca gravar, pois ao fazer isso estará alterando a evidencia. Essas copias foram denominadas imagens encase (Raedts,2007)

A crescente quantidade e diversidade de dados digitais transformam o armazenamento e a gestão de evidências em um desafio cada vez mais complexo. Imagens de disco, outrora o foco principal, agora dividem espaço com fontes de prova como imagens de memória, imagens de rede e arquivos comuns.

Preservar essas informações é crucial para investigações digitais (Carrier & Spafford, 2004)

2.12 Tipos de imagem

As imagens encasem podem ser divididas em três grandes grupos: imagens físicas, as imagens logicas e as imagens direcionadas. O que define qual delas será usada é a natureza jurídica e o orçamento. (Main,2022)



Fonte: (Main, 2022)

2.12.1 Imagem física

Uma coleção de dispositivos físicos consiste em uma duplicação bit a bit do dispositivo, garantindo uma cópia exata. A criação de imagens físicas de dispositivos móveis é o método mais abrangente, capturando a maior quantidade possível de dados. (Main, 2022)

Esse processo permite obter todo o conteúdo físico de um disco. As imagens forenses físicas registram áreas excluídas, fragmentos de arquivos e possibilitam o acesso a dados apagados e criptografados. (Main, 2022)

Como em todos os tipos de coleções forenses, a coleta de dispositivos físicos apresenta vantagens e desvantagens. Entre as vantagens, destaca-se o acesso completo aos artefatos do dispositivo, como registros de eventos, arquivos e carimbos de data/hora. (Main, 2022)

Entre as desvantagens, está o aumento dos custos proporcionais à quantidade de dados coletados. (Main, 2022)

Para investigações de alto risco, como as internas ou criminais, o método mais defensável e rigoroso de coleta de dispositivos é a aquisição de uma imagem forense física dos dispositivos em questão.

Uma outra característica importante de uma imagem física é a possibilidade de gravá-la de volta em um disco. Como uma imagem física é uma cópia bit a bit de um dispositivo de armazenamento, é possível transferir essa imagem para outro dispositivo de armazenamento, criando uma réplica idêntica ao original. (Raedts, 2007)

Isso pode ser extremamente útil se for necessário inicializar o sistema original, por exemplo, para um exame ao vivo do sistema. O sistema funcionará exatamente como se a unidade original estivesse em uso. (Raedts, 2007)

2.12.2 Imagem Logica

Uma imagem logica é uma imagem no nível do sistema de arquivo, essa forma de imagem é comumente usada quando não é possível criar uma imagem física ou por determinações legais que permitem que seja feita a cópia apenas de uma determinada pasta. (Raedts, 2007)

Sendo assim a imagem logica consegue apenas recuperar itens que estão visíveis ao usuário, dessa forma caso o suspeito antes da criação da imagem excluir esse arquivo esse modelo de imagem não recupera itens e dados excluídos, nem coleta seus fragmentos. (Main, 2022)

2.12.3 Imagem Direcionada

Como o próprio nome já diz esse tipo de imagem é direcionada a cópia de arquivos e pastas especificas, uma vez que ela seja relevante para o caso. Esse é o método mais barato entre os três, uma vez que é usada uma coleta de uma menor quantidade de dados. (Main, 2022)

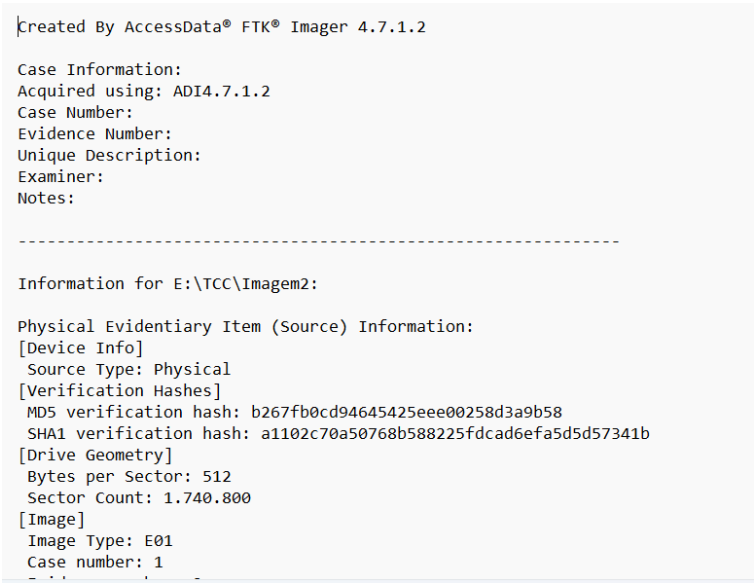
Vantagens das coleções forenses direcionadas: agilizam o processo de descoberta eletrônica devido ao tempo de processamento reduzido. Desvantagens: pode ser necessário retornar à fonte de coleta se dados adicionais, não incluídos na coleta direcionada original, forem necessários. (Main, 2022)

2.13 Formatos de Imagem

Ao criar uma imagem encase ela pode possuir vários formatos, esses formatos dependem principalmente de preferências pessoais e do software que será usado. Os formatos mais usados pelas ferramentas são: bruto (DD) e E01. (Raedts, 2007)

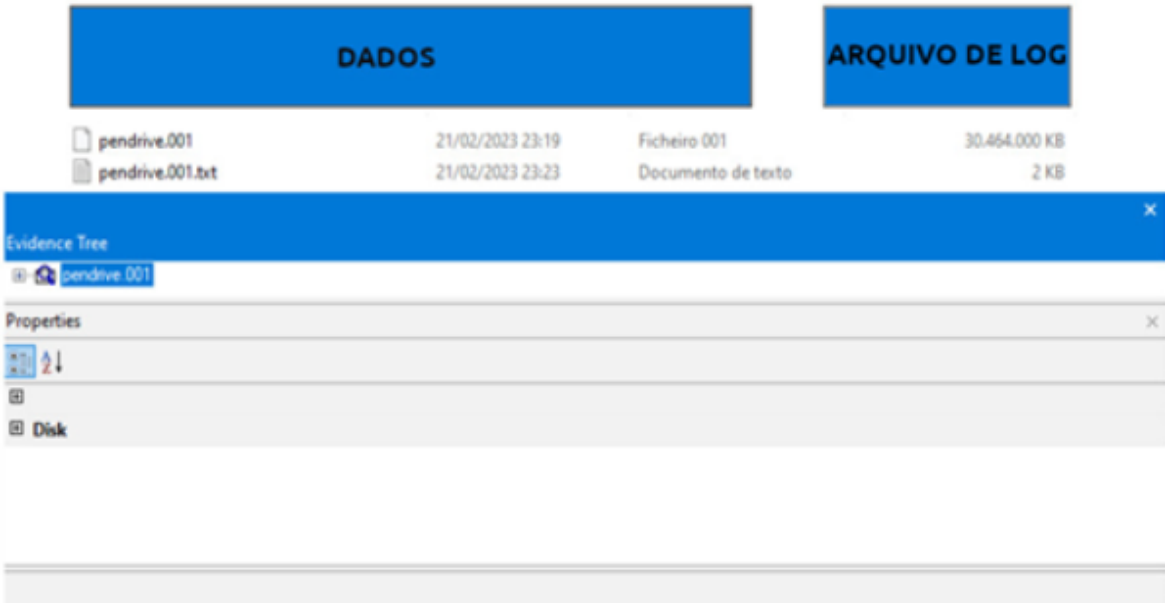
2.13.1 Bruto (DD)

O formato de imagem RAW é basicamente uma cópia bit a bit dos dados RAW do disco ou volume armazenado em um ou vários arquivos. Ele não possui os metadados, assim as ferramentas criam um arquivo de texto onde contém os detalhes da imagem, como: detalhes do arquivo de imagem, dados do hardware/software usado e dados de origem e destino como também valores *hash*. (Raedts, 2007)



```
Created By AccessData® FTK® Imager 4.7.1.2

Case Information:
Acquired using: ADI4.7.1.2
Case Number:
Evidence Number:
Unique Description:
Examiner:
Notes:

---------------------------------------------------------------

Information for E:\TCC\Imagem2:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Verification Hashes]
 MD5 verification hash: b267fb0cd94645425eee00258d3a9b58
 SHA1 verification hash: a1102c70a50768b588225fdcad6efa5d5d57341b
[Drive Geometry]
 Bytes per Sector: 512
 Sector Count: 1.740.800
[Image]
 Image Type: E01
 Case number: 1
```

Fonte: Própria



Fonte: Tsukahara,2023

2.13.2 E01

O arquivo de evidencias EnCase é ao lado do formato RAW E01 são os formatos de imagem mais usados. Esse formato possui um fluxo de bits armazenada em um ou vários arquivos, onde possuem os metadados do sistema copiado. (Raedts, 2007)

Fonte: Tsukahara,2023

Seus metadados possuem as seguintes informações: informações do caso, nome do examinador, notas, somas de verificação e o *hash* MD5, além de poder fazer a compactação e proteção por senha. Sendo esses dois últimos sua principal vantagem em relação aos outros modelos. (Raedts, 2007)

3 Ataques mais comuns

3.1 Engenharia Social

De acordo com a Agência Brasileira de Inteligência (ABIN), a engenharia social é uma técnica utilizada por indivíduos mal-intencionados para enganar, manipular e explorar a confiança das pessoas, levando-as a fornecer informações sensíveis voluntariamente, sem o uso de força.

Essa técnica pode ser aplicada para obter dados pessoais da própria vítima ou para acessar informações sobre a empresa em que ela trabalha (ABIN, 2021).

Os ataques de engenharia social normalmente envolvem diversas táticas para conquistar a confiança do alvo, aproveitando-se de características humanas como:

Fingir ser uma marca confiável: Os golpistas frequentemente se passam por empresas conhecidas e confiáveis com as quais as vítimas interagem regularmente. Isso faz com que as pessoas sigam instruções dessas "empresas" sem as devidas precauções. Muitos golpistas usam kits disponíveis para criar sites falsos que imitam os de grandes marcas (IBM, 2024).

Fingir ser uma agência governamental ou figura de autoridade: As pessoas tendem a confiar, respeitar ou temer figuras de autoridade. Os ataques de engenharia social exploram esse instinto com mensagens que parecem vir de agências governamentais (como o FBI ou a Receita Federal), figuras políticas ou até celebridades (IBM, 2024).

Induzir medo ou senso de urgência: Sob pressão ou medo, as pessoas tendem a agir rapidamente e sem cautela. Golpistas usam várias técnicas para criar esse sentimento, como alegar que uma transação de crédito foi recusada, que o computador foi infectado por um vírus ou que uma imagem no site da vítima infringe direitos autorais. Também exploram o medo de perder (FOMO), criando uma sensação de urgência (IBM, 2024).

Apelar à ganância: Um exemplo clássico é o golpe do Príncipe Nigeriano, onde um e-mail de um suposto membro da realeza nigeriana oferece uma grande recompensa financeira em troca de informações bancárias ou uma pequena taxa antecipada. Esse golpe combina ganância, falsa autoridade e urgência, e ainda arrecadava US$ 700 mil por ano em 2018 (IBM, 2024).

Apelar para a utilidade ou curiosidade: Golpistas também se aproveitam da boa vontade das vítimas, enviando mensagens que parecem ser de amigos ou redes sociais, oferecendo ajuda técnica, solicitando participação em pesquisas ou alegando que uma postagem se tornou viral. Essas mensagens frequentemente contêm links para sites falsos ou downloads de malware (IBM, 2024).

3.1.1 Phishing

O phishing é a técnica de engenharia social mais utilizada e conhecida. Os ataques de phishing baseiam-se em mensagens de texto ou de voz que visam manipular o alvo, induzindo-o a compartilhar dados confidenciais, baixar softwares mal-intencionados ou transferir dinheiro para outras pessoas (IBM, 2021).

A prática mais comum envolve o envio de uma série de e-mails que fingem ser de grandes empresas e instituições conhecidas, induzindo o alvo a clicar em links maliciosos que levam a sites falsos para roubar seus dados (IBM, 2021).

O spear phishing, por sua vez, é uma variante mais direcionada do phishing, com um alvo específico. Seu objetivo é obter acesso a informações de usuários, redes de computadores ou fundos corporativos. Para isso, o golpista acessa as redes sociais da vítima, criando uma mensagem personalizada que gera a confiança necessária para enganar a pessoa (IBM, 2021).

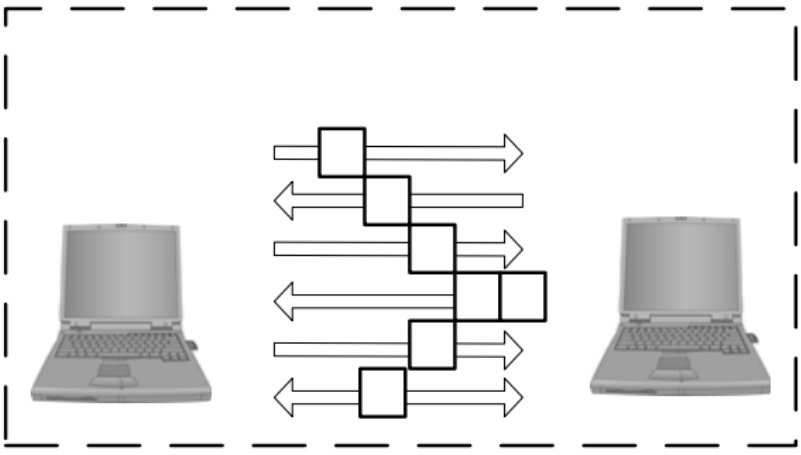
O phishing se consolidou como a principal ameaça cibernética da atualidade, sendo responsável por uma parcela significativa de ataques e violações de dados. De acordo com o *IBM Security X-Force Threat Intelligence Index* 2023, o phishing é o principal vetor de infecção por malware, presente em impressionantes 41% dos incidentes registrados.

Essa estatística alarmante se intensifica ao analisarmos o impacto financeiro das violações de dados. O relatório *Cost of a Data Breach* 2022 revela que o *phishing* é o principal vetor de ataque inicial que leva às violações mais onerosas, com um custo médio de US$ 4,76 milhões por incidente.

3.2 Associação Maliciosa

Devido a característica da rede *wi-fi* estar sendo compartilhada pelo ar não existe necessidade do atacante estar presente de forma física ou ter acesso aos equipamentos da rede-alvo, basta estar na área que abrange o sinal. (RUFINO.2011)

Esse tipo de ataque é caracterizado pelo atacante criar um *acess point*, fazendo com que o sistema entenda esse *acess point* como uma rede real e com isso o atacante possa interceptar os dados que são enviados. (DUARTE,2003)



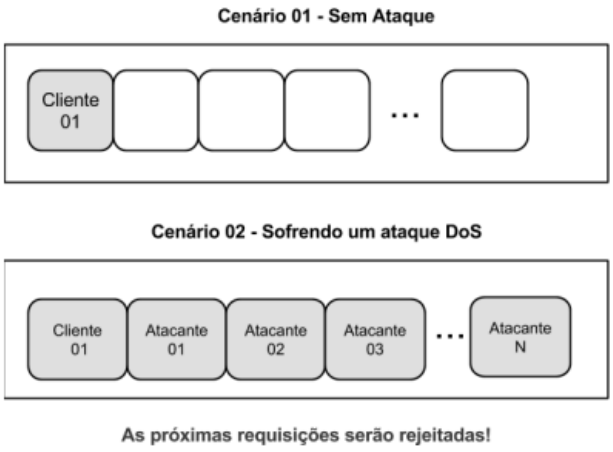
Fonte: (DUARTE,2003, p.38)

3.3 Negação de Serviço (DoS)

Esse ataque consiste em tornar um sistema ou aplicação indisponível para o acesso para os usuários. O atacante para atingir esse objetivo faz com que o servidor utiliza toda a sua capacidade de processamento enviando várias requisições simultâneas fazendo com que o servidor da aplicação fique indisponível e os usuários legítimos não tenham acesso ao sistema. (DANTAS,2015)

Um exemplo de ataque DoS de rede *Wi-Fi* ocorre quando um invasor se passa por um *acess point* (AP) com o mesmo SSID e endereço MAC de um AP válido. O invasor então inunda a rede com pedidos de dissociação. Esses pedidos forçam os clientes a se desassociar e se reconectar ao AP. Se o invasor enviar esses pedidos com frequência suficiente, os clientes não poderão permanecer conectados por muito tempo. (DUARTE,2003)

Ataque de Negação de Serviço Distribuído

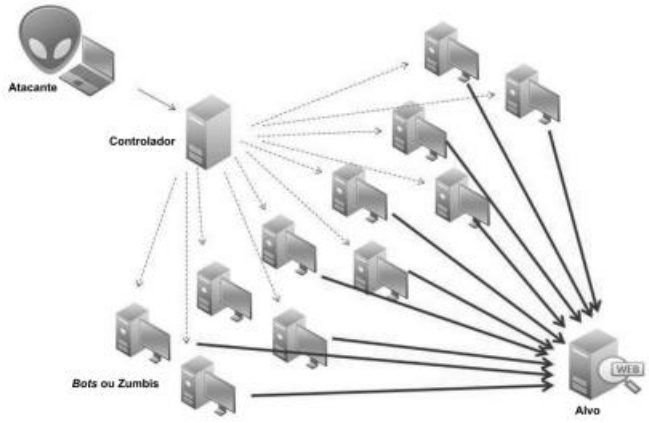


Fonte: (DANTAS,2015, p.22)

3.4 Ataque de Negação de Serviço Distribuído (DDoS)

O Ataque de Negação de Serviço Distribuído (DDoS) consiste em um conjunto de máquinas, denominadas *bots* ou zumbis, que foram infectadas por algum malware e podem ser controladas de forma remota. Esse grupo de máquinas infectadas é denominado como *botnet*. (DANTAS,2015)

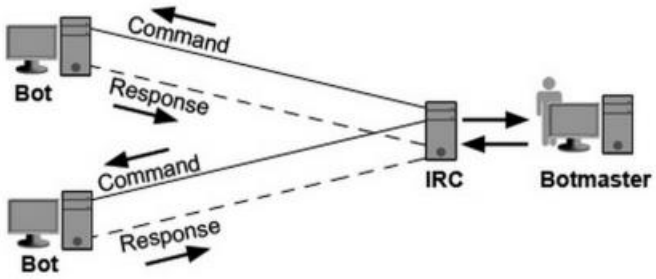
Esses *bots* quando o atacante queira fazer o ataque são acionados de forma remota, o denominado *botmaster* define o alvo e então os vários *bots* começam a enviar várias requisições fazendo com que o sistema fique inacessível para os usuários legítimos. (DANTAS,2015)



Fonte: (DANTAS,2015, p.23

A arquitetura desse ataque é formada por cinco atores principais, sendo eles:

1. **Atacante:** Usuário que conduz o ataque, denominado *botmaster*.
2. **Controlador:** É o serviço de comunicação utilizado na internet, utilizado tradicionalmente para ataques DDoS, o chamado IRC, o atacante utiliza desse protocolo para mandar os comandos para os *bot* e assim poder orquestrar o ataque, o conduzindo em massa.
3. **Máquinas Infectadas (*Bots*):** São as máquinas infectadas que serão usadas para mandar mensagens em massa para o alvo.
4. **Alvo:** Sistema ou aplicação que irá sofrer o ataque



Fonte: (DANTAS,2015, p.24)

4 Construção do laboratório

Para a configuração do laboratório, foi selecionada uma imagem encase pública disponibilizada pelo Professor Ali Hadi, Diretor de Pesquisa do *Leahy Center for Digital Forensics and Cybersecurity* e professor em tempo integral e diretor de programa do Programa de Computação e Forense Digital do *Champlain College* nos EUA.

No site pessoal do Professor Ali Hadi, é possível encontrar uma série de imagens encase para estudo gratuito. A imagem selecionada simula um servidor web de uma empresa que foi violado através do seu site. Foram aplicadas as técnicas simulando como poderia ser feito após o atacante já ter acesso ao servidor, pulando a etapa de acesso via site.

Optar por usar uma imagem pública Encase em vez de um ambiente real para este tipo de treinamento é crucial devido às rigorosas leis e regulamentações de proteção de dados, como a Lei Geral de Proteção de Dados (LGPD) e o Marco Civil da Internet. Essas legislações estabelecem regras claras sobre a violação de dados sem a devida autorização, impondo sanções severas para quem descumprir essas normas.

A utilização de dados reais em treinamentos de segurança cibernética ou análises forenses pode colocar em risco a privacidade e a segurança das informações de indivíduos e empresas. A LGPD, por exemplo, exige que o tratamento de dados pessoais seja realizado com base em uma justificativa legal e com o consentimento dos titulares dos dados. Qualquer violação a essas normas pode resultar em multas elevadas e danos à reputação das instituições envolvidas.

Ao empregar imagens públicas encase, como as disponibilizadas pelo Professor Ali Hadi, os pesquisadores e estudantes podem realizar análises e desenvolver suas habilidades em um ambiente controlado e seguro, sem infringir as leis de proteção de dados. Essas imagens simulam cenários reais de violação de segurança, permitindo que os profissionais pratiquem técnicas de testes de penetração de maneira ética e legal.

Fazendo com que possa explorar uma serie de brechas sem ter que se preocupar com uma resposta reativa do outro lado, estando assim livre para que possa aplicar todo tipo de técnica e poder aprofundar seus estudos.

Além disso, o uso de imagens públicas garante a integridade e a confiabilidade dos dados, uma vez que essas imagens são preparadas por especialistas com o objetivo de fornecer material educativo de qualidade. Isso proporciona um ambiente de aprendizado enriquecedor e seguro,

respeitando as normativas legais e protegendo os dados sensíveis de possíveis exposições ou abusos.

4.1 Montando a imagem

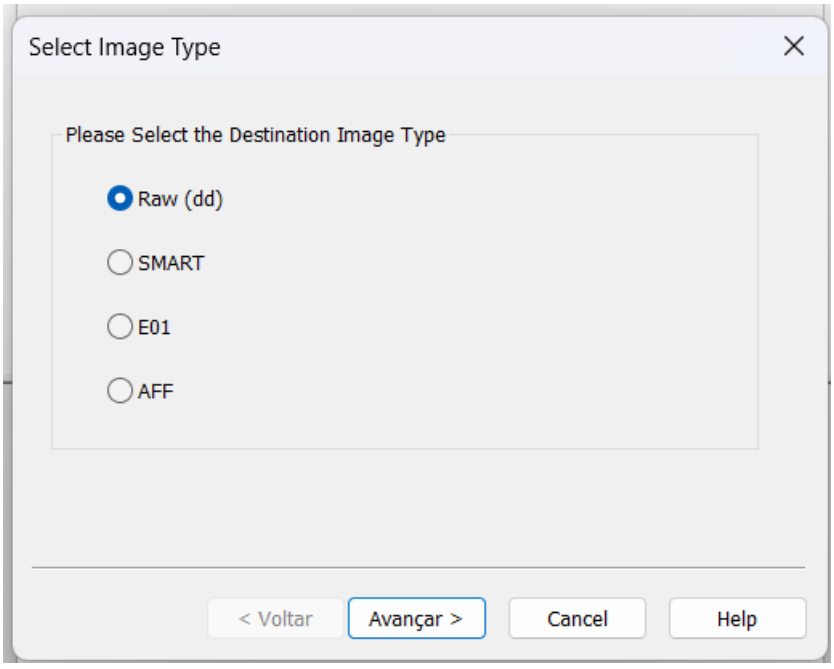
Considerando que a imagem em questão estava no formato E01, era necessário convertê-la para um formato utilizável, como .iso ou similar.

Para tal, foi utilizada a ferramenta FTK *Imager*, um software forense amplamente reconhecido na área, que permite visualizar todas as informações da imagem e os arquivos presentes nela, além de oferecer uma poderosa ferramenta de conversão de formatos.

Assim, a imagem E01 foi convertida para o formato raw, uma imagem bruta que representa uma cópia bit a bit da imagem original.

4.1.1 Conversão de tipo

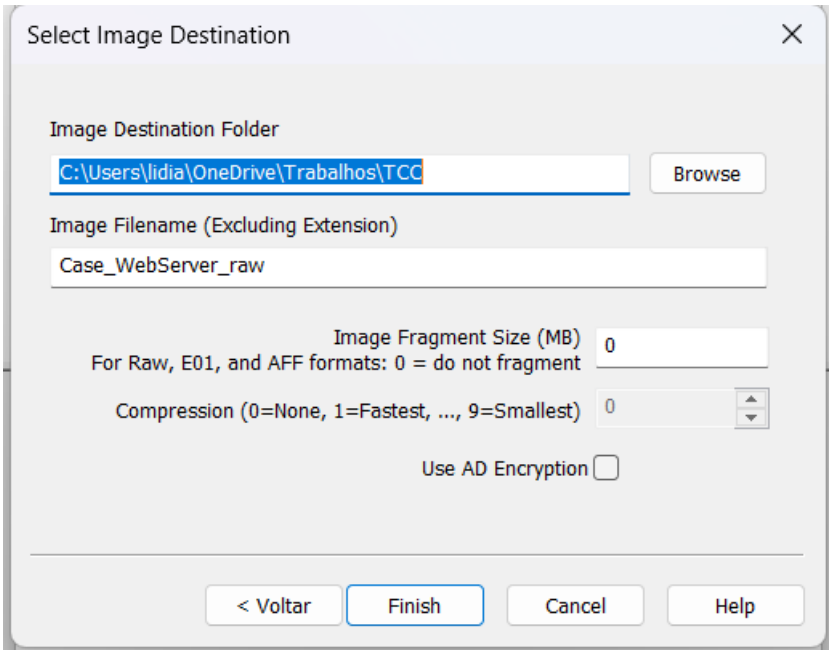
O processo de conversão de imagens forenses com o FTK *Imager* se destaca pela sua simplicidade. A ferramenta oferece uma ampla gama de formatos de destino, permitindo que o usuário escolha o mais adequado para suas necessidades. No caso em questão, optamos pelo formato *Raw*, também conhecido como dd.



Fonte: Própria

Após a seleção do formato de destino, o FTK *Imager* permite a adição de informações opcionais à imagem forense. Essas informações podem incluir comentários, descrições ou outros dados relevantes para a análise. No entanto, a inclusão de informações adicionais não é obrigatória.

O próximo passo consiste na seleção da imagem forense a ser convertida e do local onde a nova imagem será salva. O FTK *Imager* também oferece a opção de fragmentar a imagem em partes menores, facilitando o armazenamento e a transferência em mídias com capacidade limitada. No caso em questão, a fragmentação não foi necessária, portanto, o valor "0" foi inserido no campo correspondente.



Fonte: Própria

Após a configuração e o ajuste das opções de conversão, o FTK *Imager* inicia o processo de conversão da imagem forense. Ao final, um novo arquivo no formato Raw, também conhecido como dd, é gerado. Este arquivo possui o mesmo tamanho da imagem original, garantindo a preservação íntegra de todos os dados.

4.2 Criando uma máquina virtual com a imagem convertida

Com o arquivo raw da imagem forense em mãos, é possível criar uma máquina virtual utilizando o VirtualBox, permitindo a análise e investigação da imagem em um ambiente virtual seguro. Esse procedimento adiciona uma camada extra de proteção, pois permite isolar o

ambiente de teste, evitando qualquer risco de contaminação ou vazamento de dados para sistemas reais.

4.2.1 Criação de Máquinas Virtuais a partir de Imagens Raw com o VirtualBox

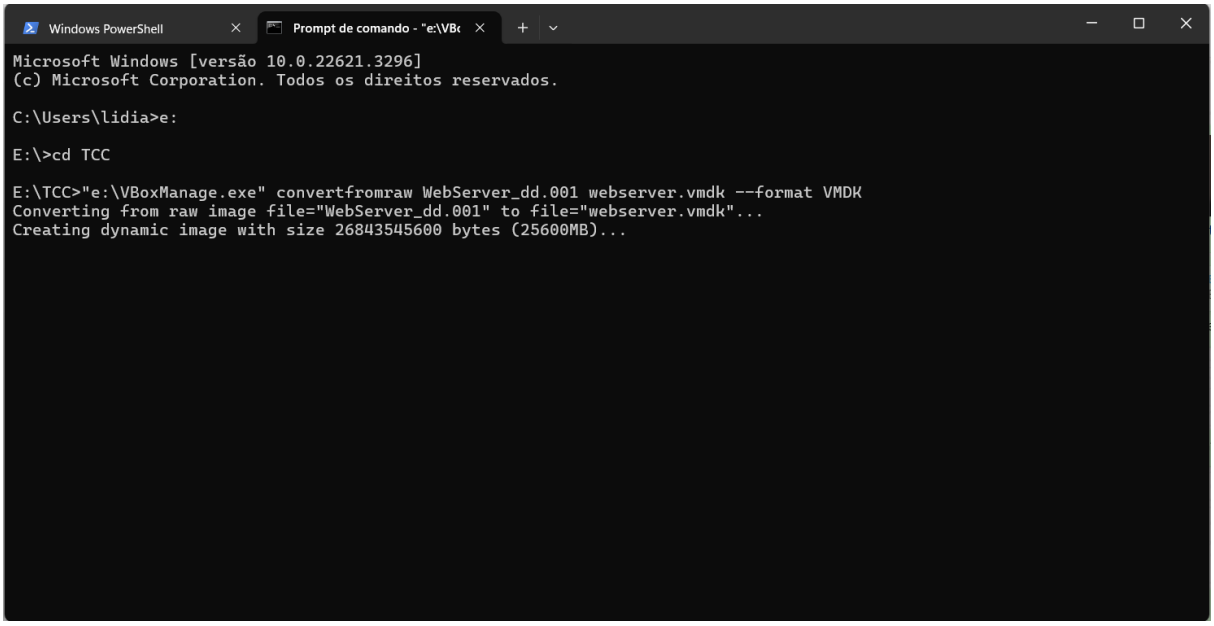
Para que seja feita essa conversão é necessário usar um comando do próprio VirtualBox,

- `VBoxManage convertfrom*`

Esse comando permite que sejam convertidos arquivos para um tipo que o VirtualBox consiga ler e assim fazer a máquina virtual, a sintaxe do comando é a seguinte:

```
VBoxManage convertfromraw <arquivo_raw.raw> <arquivo_vmdk.vmdk> <tipo>
```

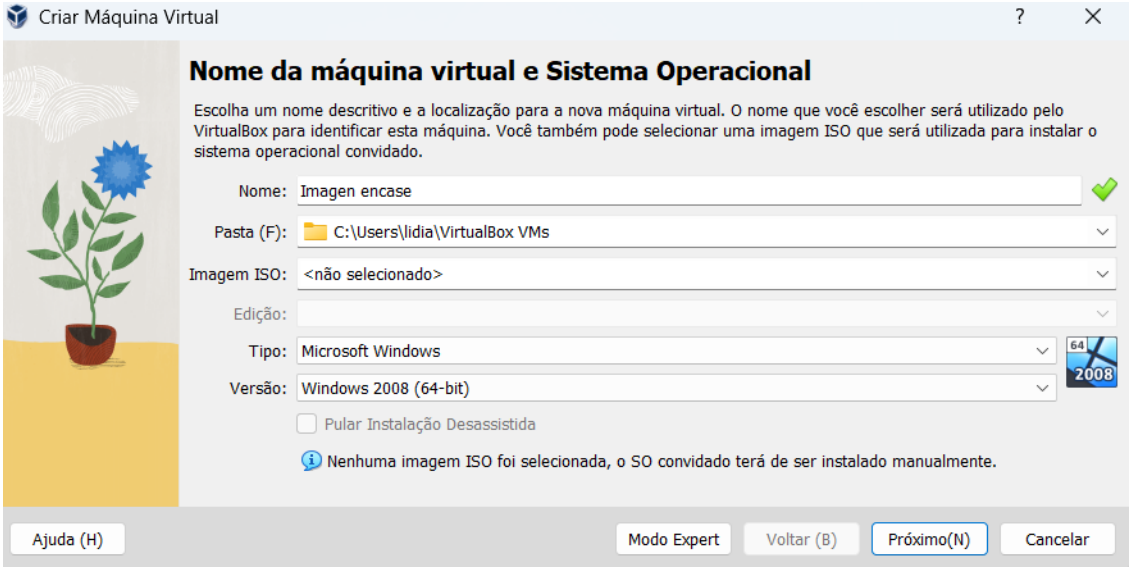
Foi substituído `<arquivo_raw.raw>` pelo nome real do arquivo raw da imagem forense, `<arquivo_vmdk.vmdk>` pelo nome desejado para o arquivo VMDK convertido e `<tipo>` pelo tipo de conversão (por exemplo, VMDK).



Fonte: Propria

Com o arquivo VMDK pronto é possível fazer a criação da máquina virtual dentro do VirtualBox. Para usar esse formato de arquivo é necessário fazer a criação de uma maquina virtual, informando seu nome e o sistema operacional que deve ser usado, nesse momento é importante que saiba qual é o sistema operacional que é usado na imagem, pois o VirtualBox com essa informação já faz a configuração padrão de virtualização necessária para o sistema operacional (SO).

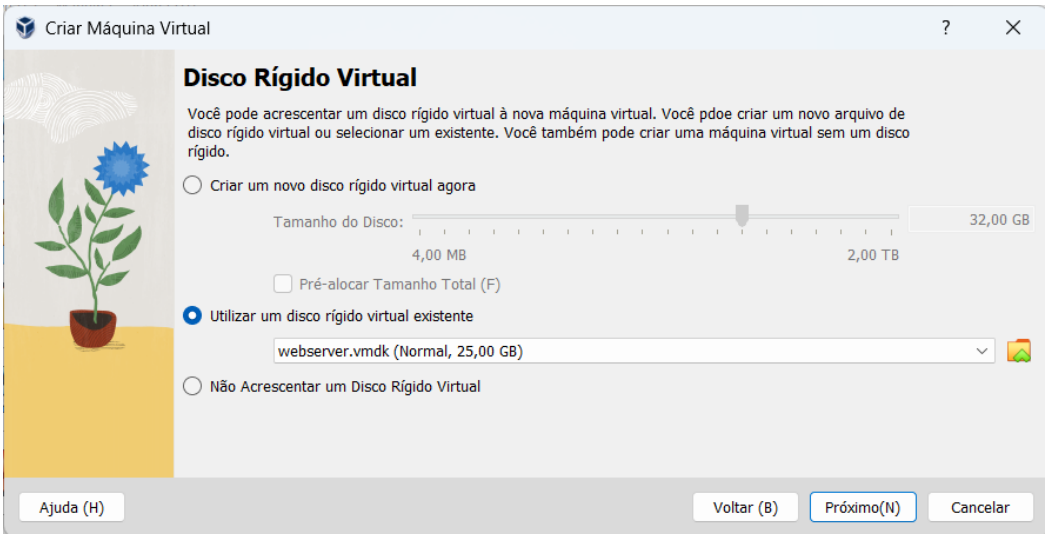
Caso selecione o SO incorreto poderá funcionar a máquina virtual, mas alguns recursos podem ter algum tipo de erro, sendo necessário criar outra máquina com o SO correto.



Fonte: Própria

Feito isso, o próximo passo é fazer a seleção da memoria e processador necessários, a quantidade de memória e processador depende de quanto o SO necessita e quanto de memória física está disponível na máquina hospedeira.

Com isso selecionado, o próximo passo é definir o disco rígido e é nesse momento que a imagem encase já com seu formato convertida é usada, selecionando a opção de um disco rígido já existente.

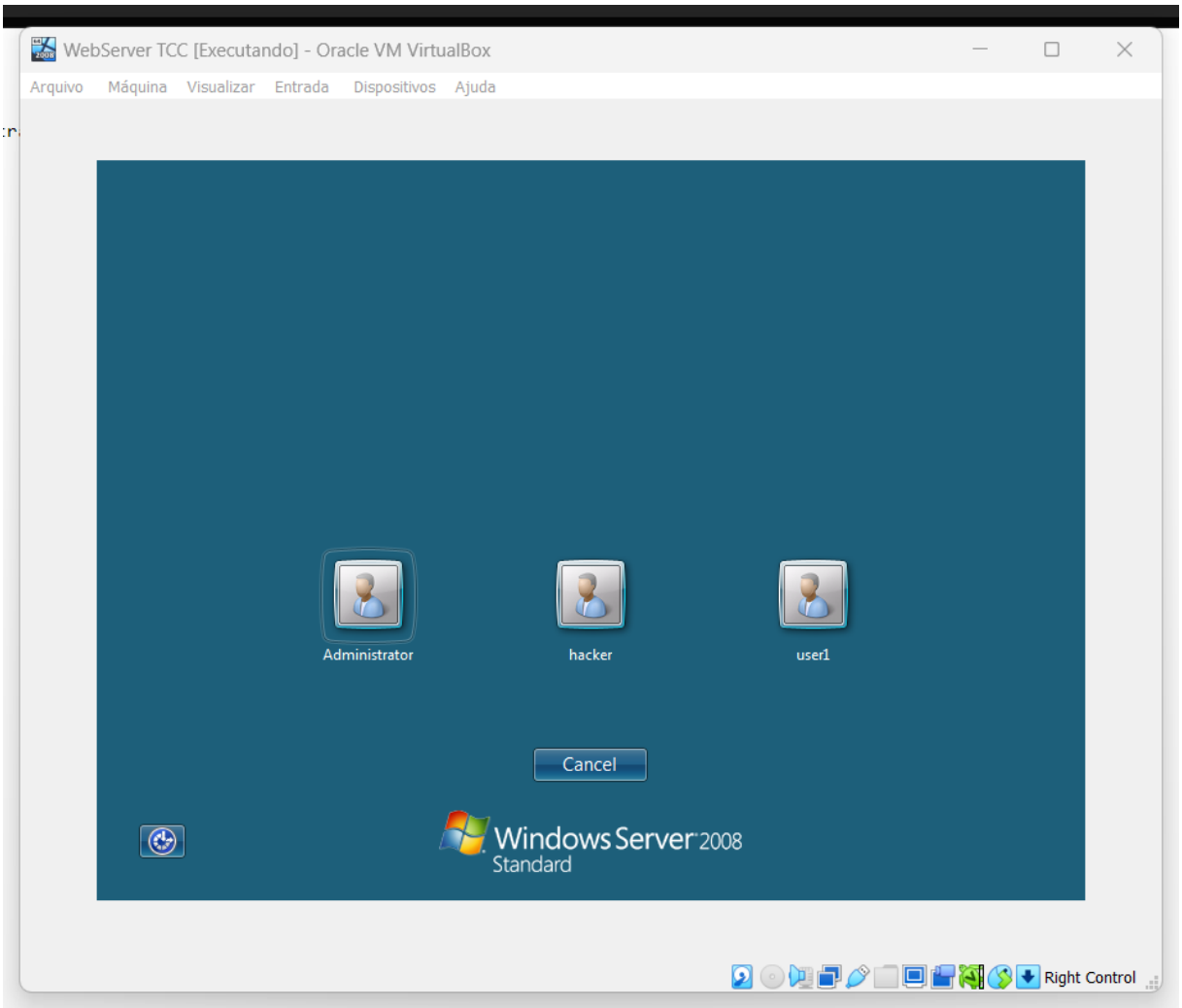


Fonte: Própria

4.3 Aplicando técnicas de *pentest*

Com a imagem em mãos e podendo ser explorada, de início foi feita um ataque de força bruta, onde usando um dicionário de senhas, onde é usadas as senhas mais comuns. A utilização dessa técnica não surtiu efeito, tanto ao tentar acessar a conta de administrador quanto a conta do user1.

Vendo que essa não seria uma abordagem efetiva, foi feita uma segunda abordagem, onde a ideia era utilizar um segundo sistema operacional para tentar montar os dados de diretórios do Windows.

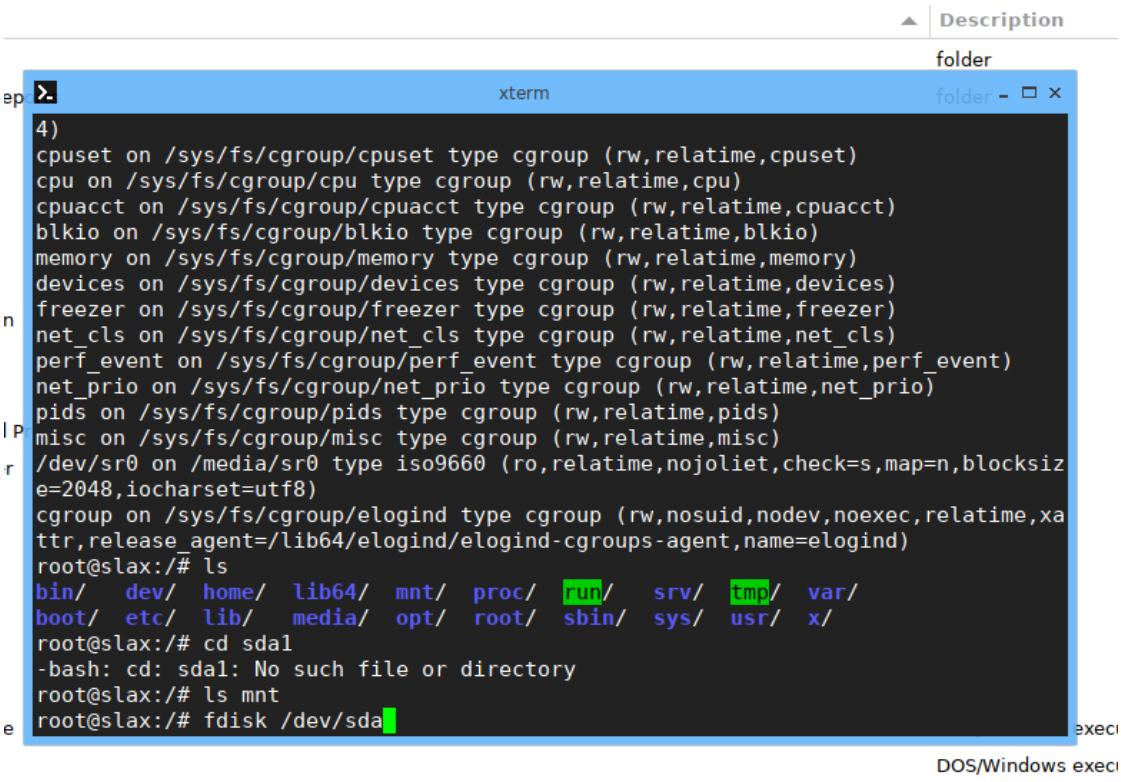


Fonte: Própria

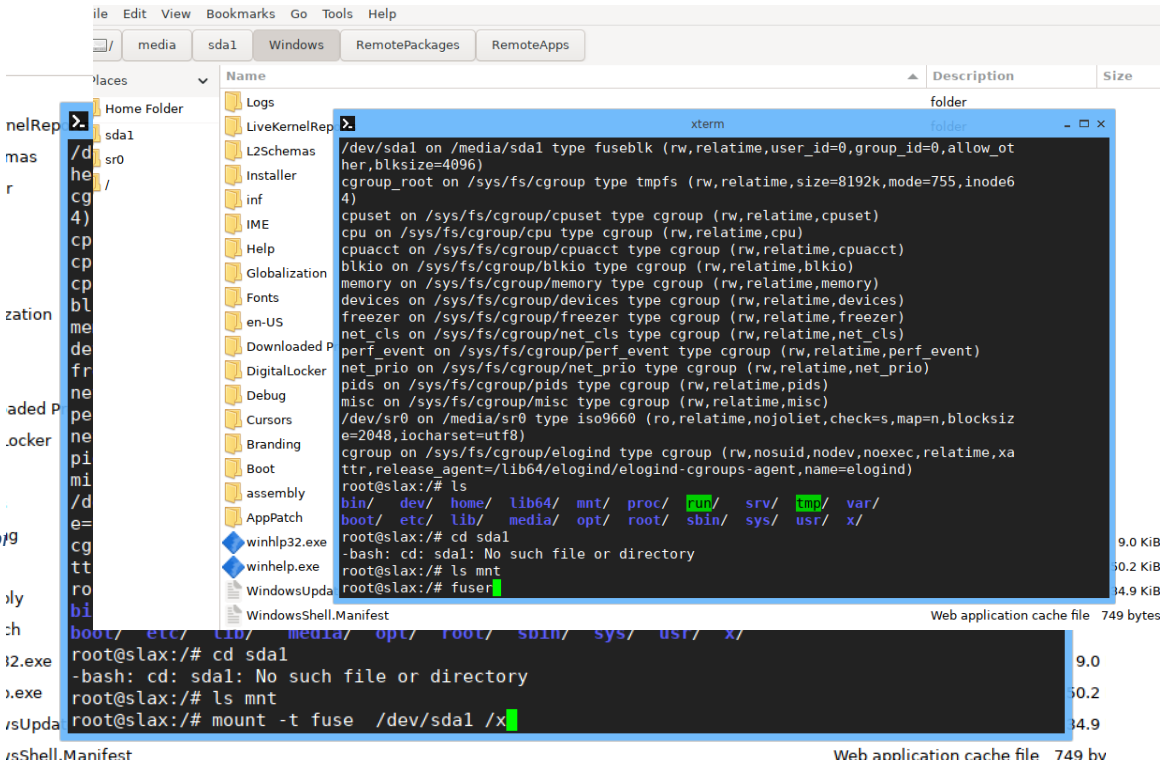
Para isso foi usado o Slax, que é um sistema operacional Linux compacto, rápido e moderno que combina design elegante com abordagem modular. Com a capacidade de

funcionar diretamente de uma unidade flash USB sem a necessidade de instalação. (Matejicek, 2024)

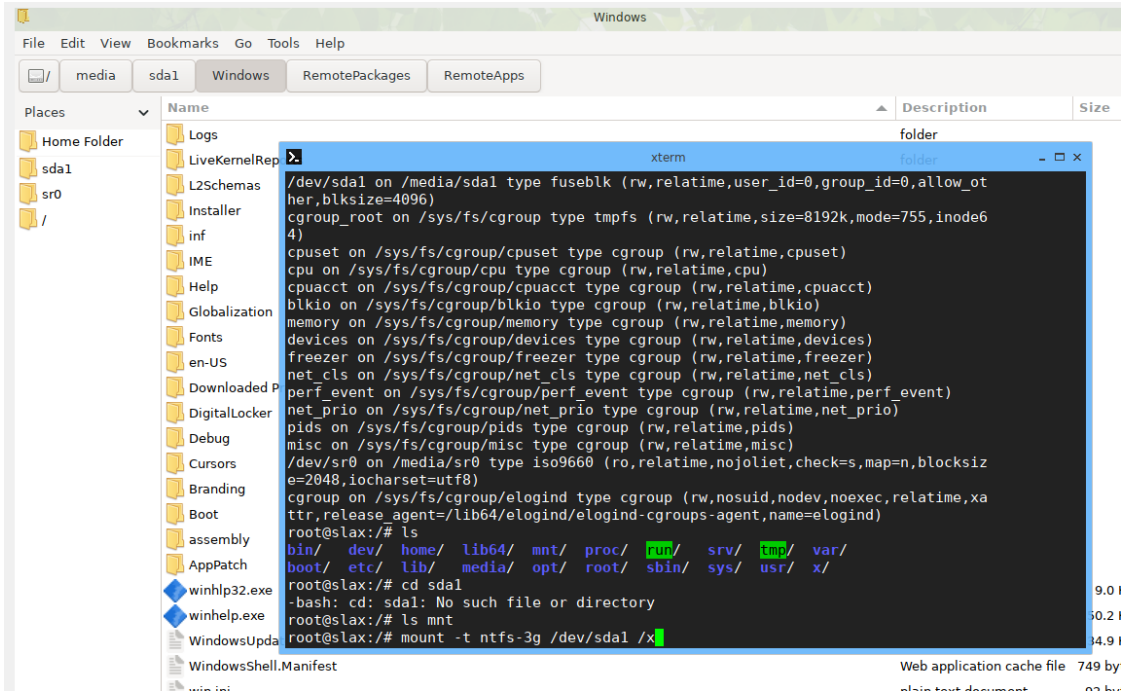
Uma vez o utilizando para dar boot através do próprio VirtualBox, ao inicializá-lo, abrindo o prompt de comando, foi possível, através de simples comandos montar os diretórios do Windows.



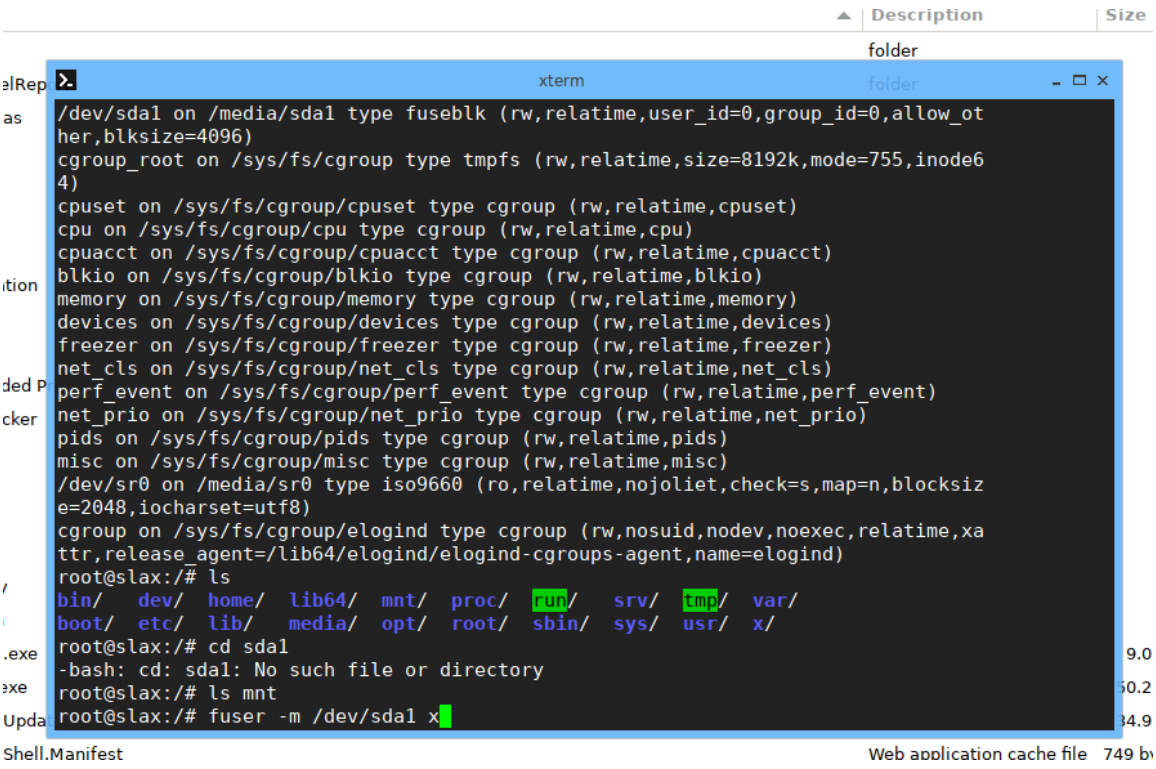
Fonte: Própria



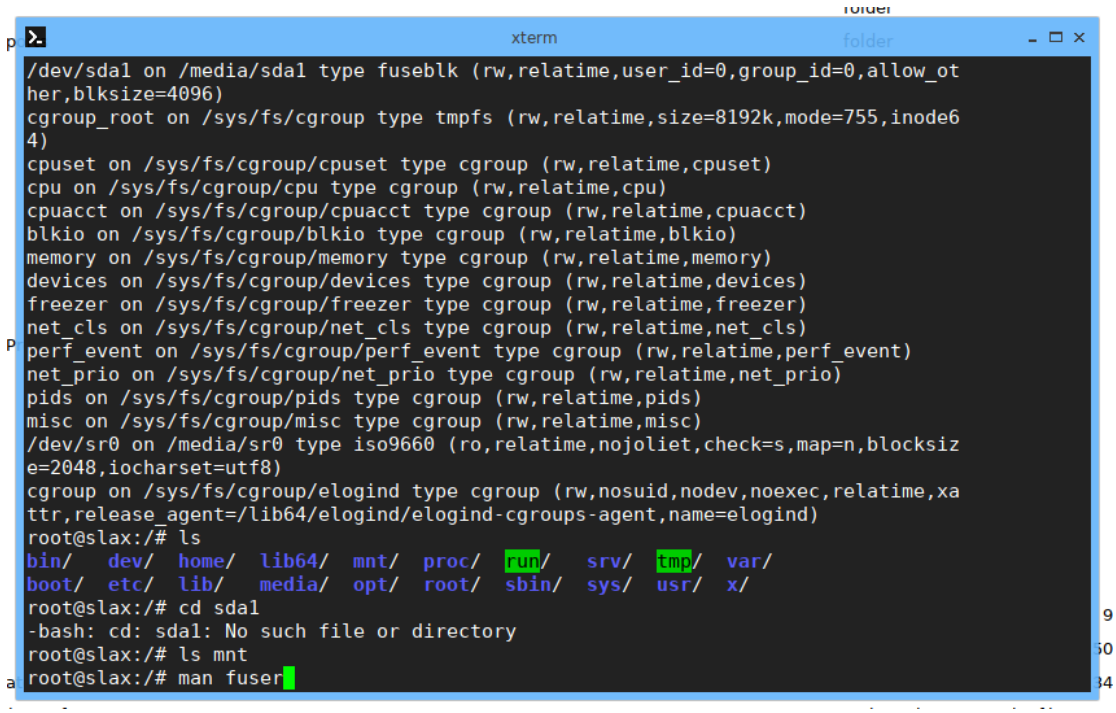
Fonte: Prop



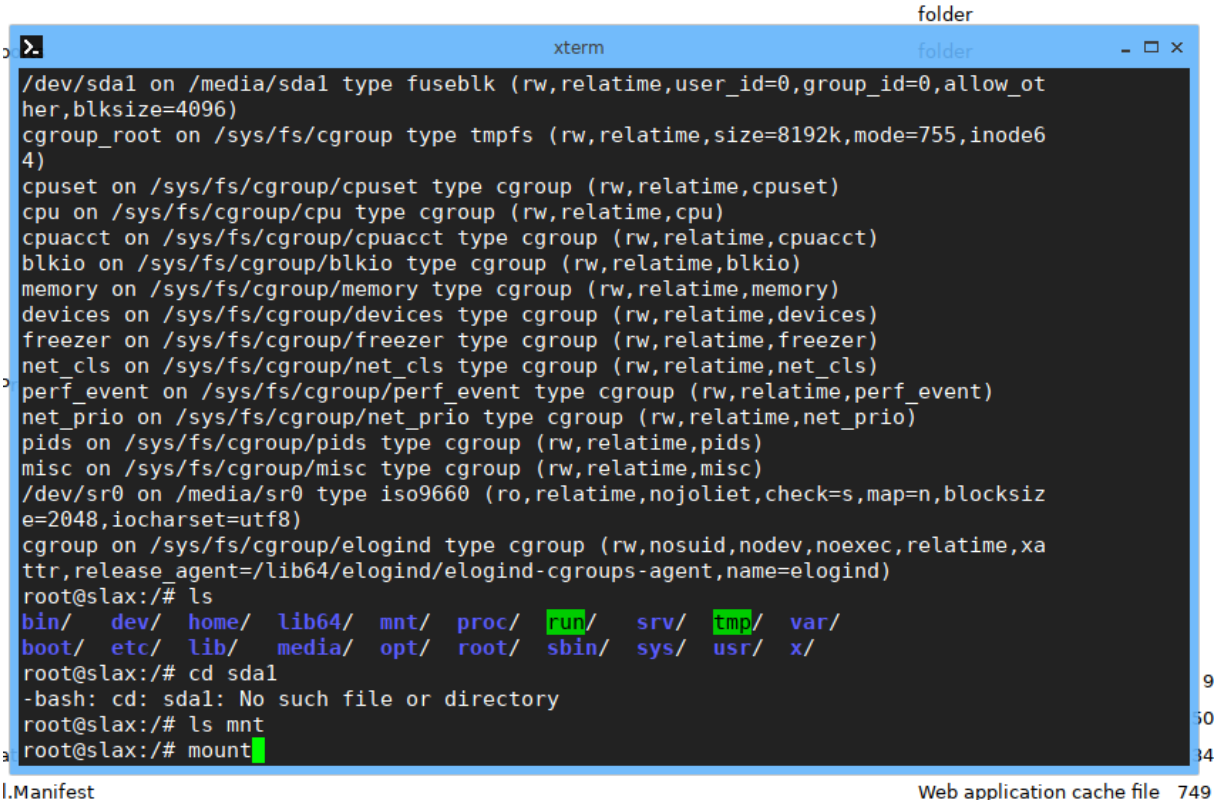
Fonte: Própria



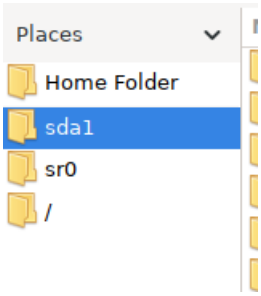
Fonte: Própria



Fonte: Própria

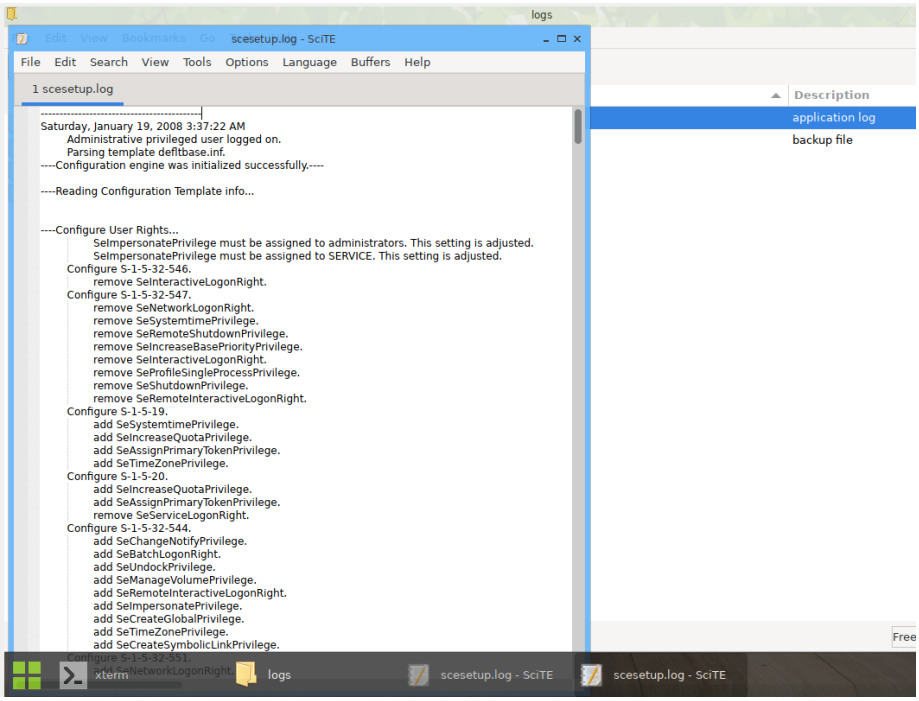


Depois de utilizar todos os comandos foi criada uma pasta com todos os diretórios do Windows server, apenas com isso já conseguiríamos violar o princípio de confidencialidade do sistema, a figura a seguir nos mostra as pastas que foram criadas.

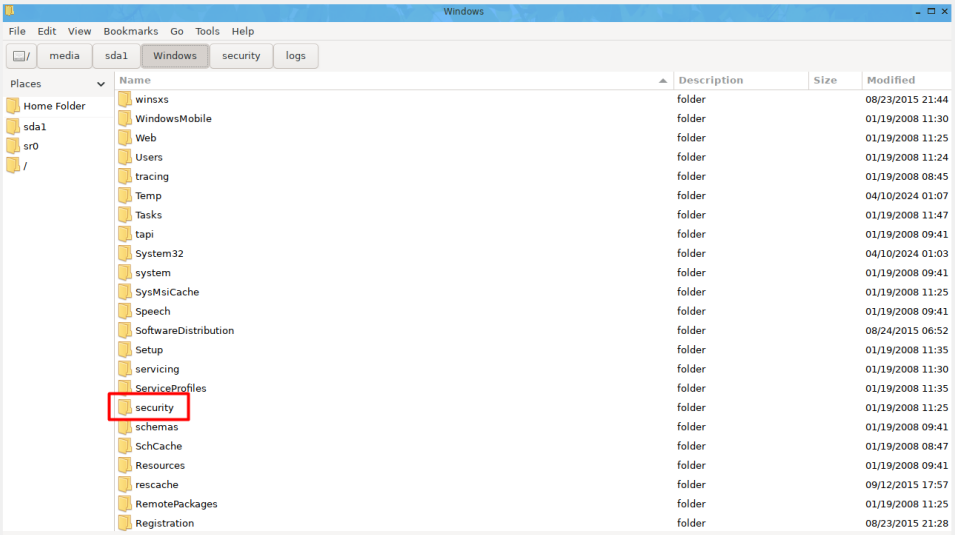


Fonte: Própria

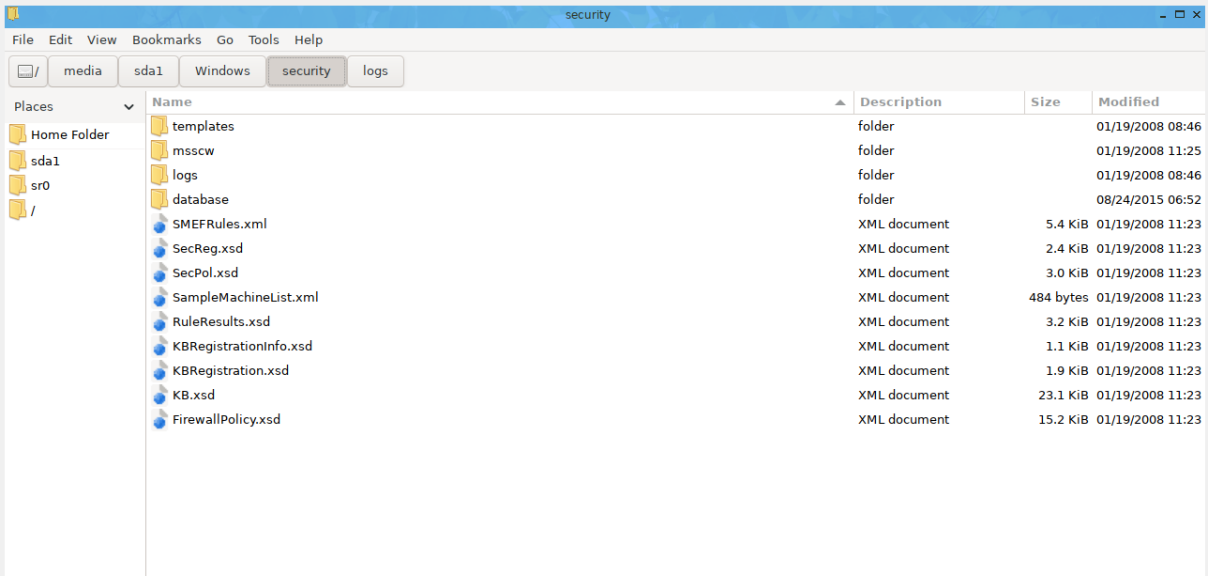
Dessa forma já temos acesso a grande parte das informações do servidor, ao analisar as pastas e arquivos foi possível encontrar dados sensíveis, como scripts de firewall, banco de dados e diversos arquivos de logs.



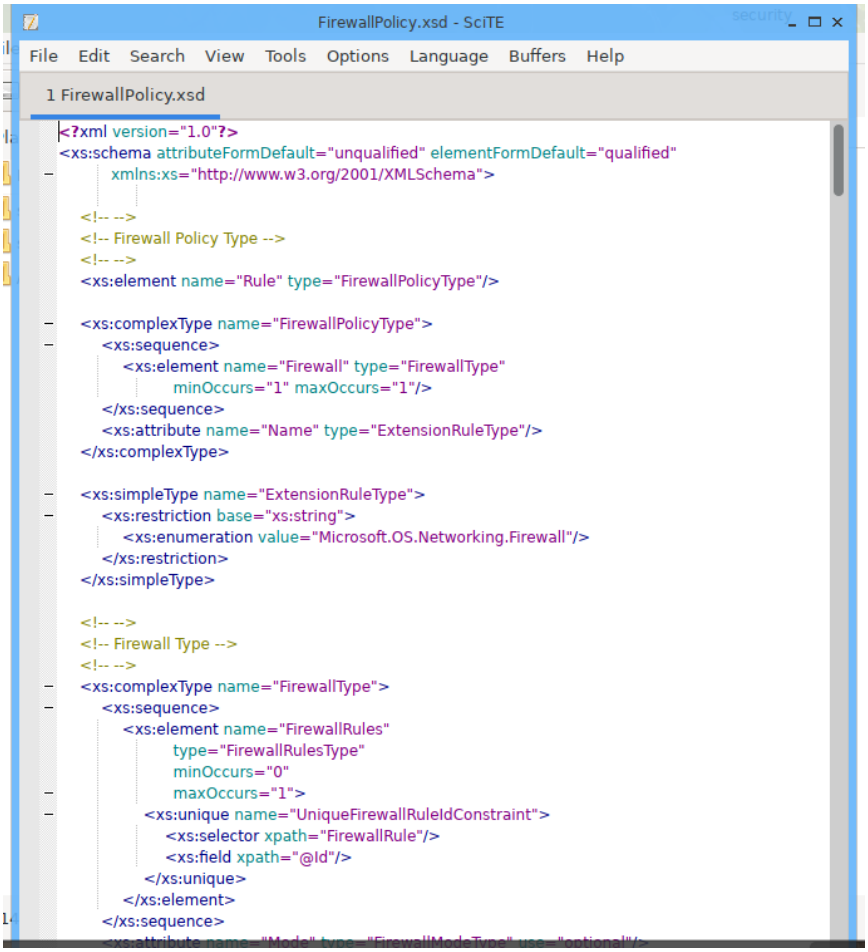
Fonte: Própria



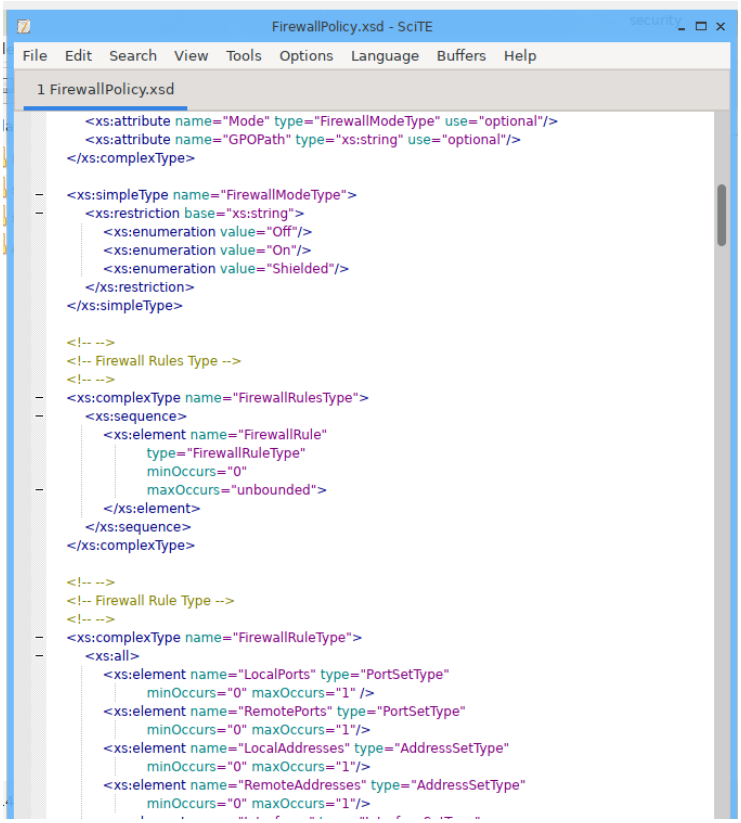
Fonte: Própria



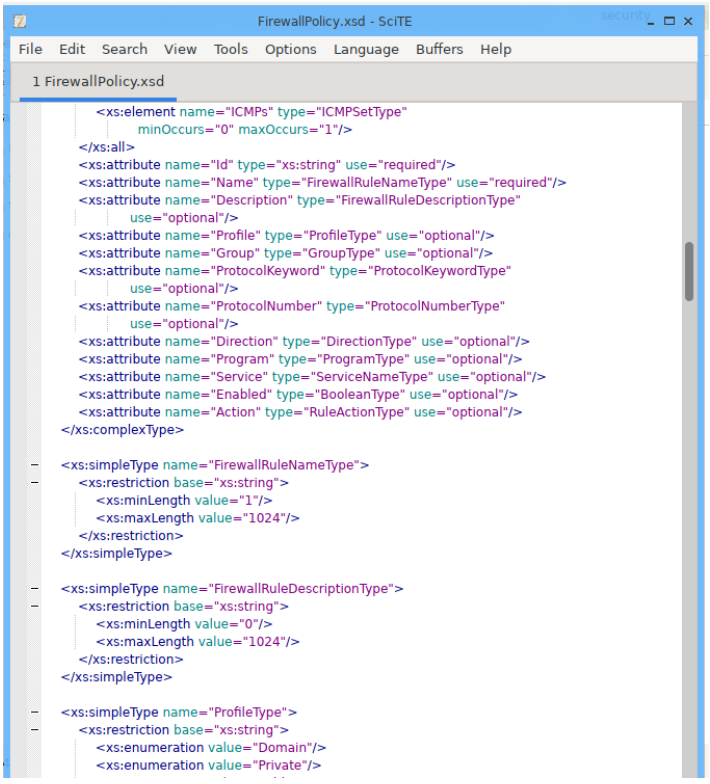
Ao acessar o arquivo FirewallPolicys.xsd é possível ter acesso a todo o sistema de políticas do firewall, esse arquivo não possui nenhuma proteção de leitura e escrita, sendo possível que qualquer pessoa o altere e possa abrir uma porta de acesso por ele.



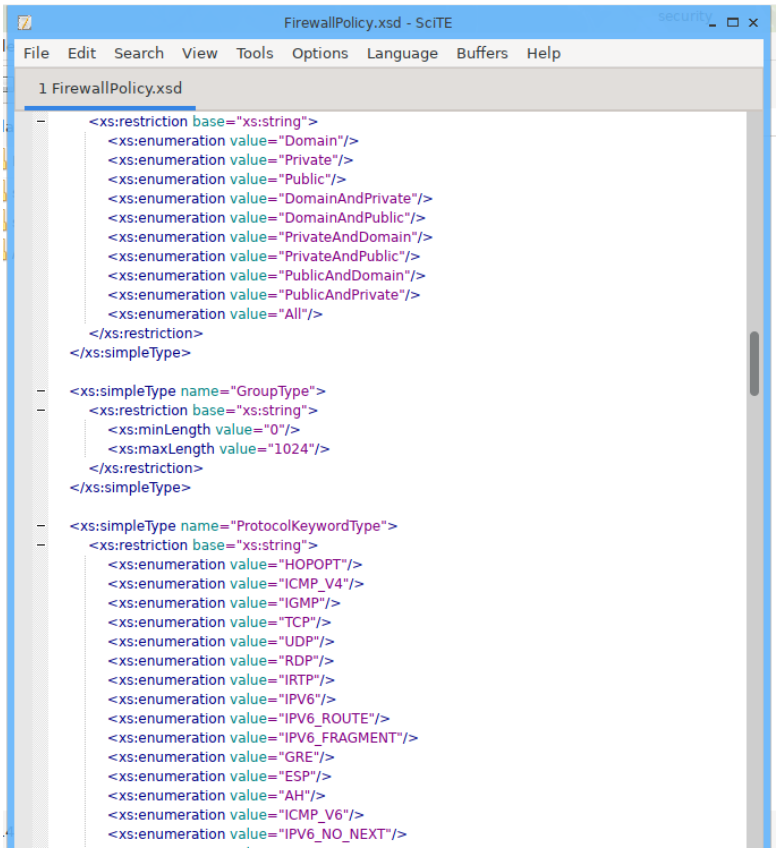
Fonte: Própria



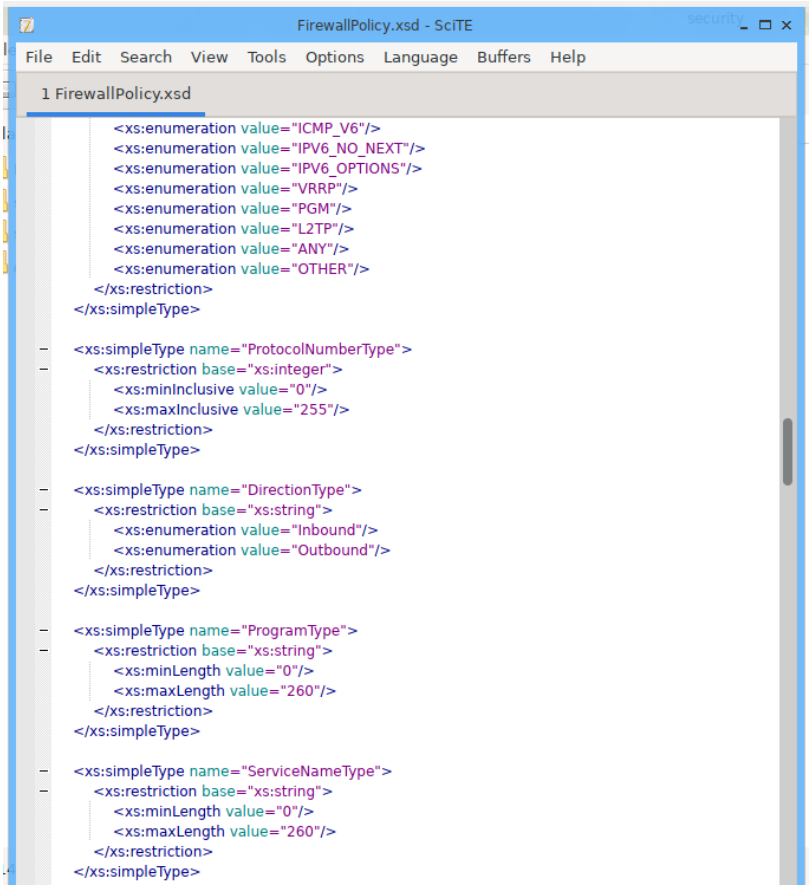
Fonte: Própria



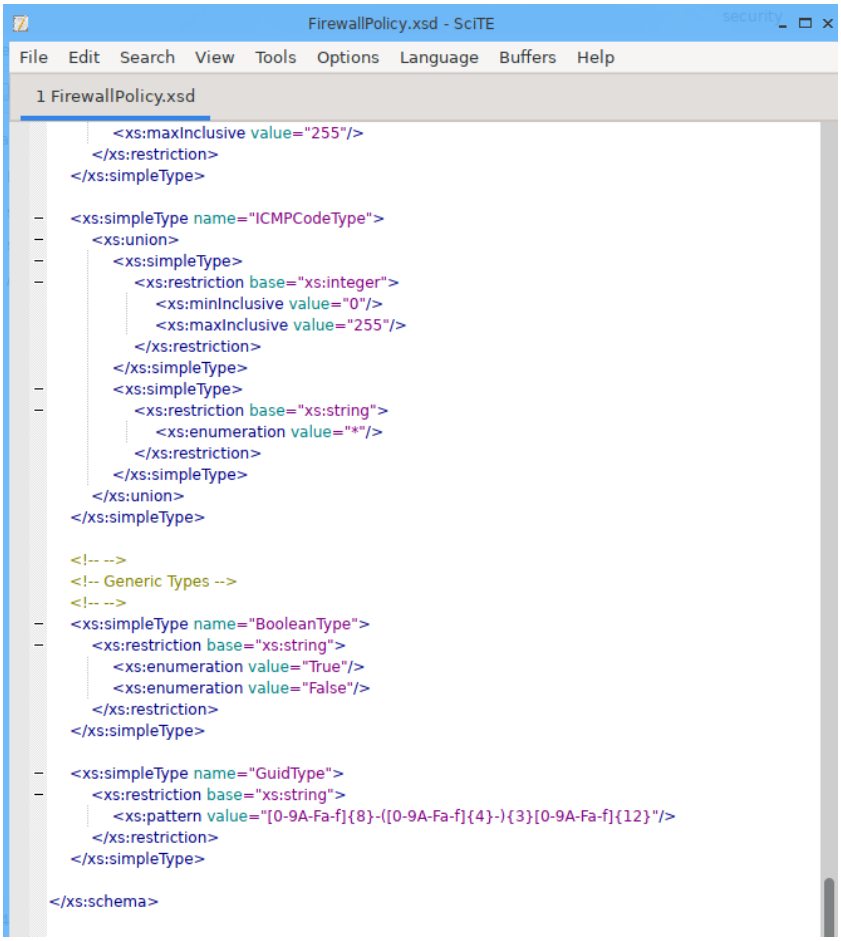
Fonte: Própria



Fonte: Própria

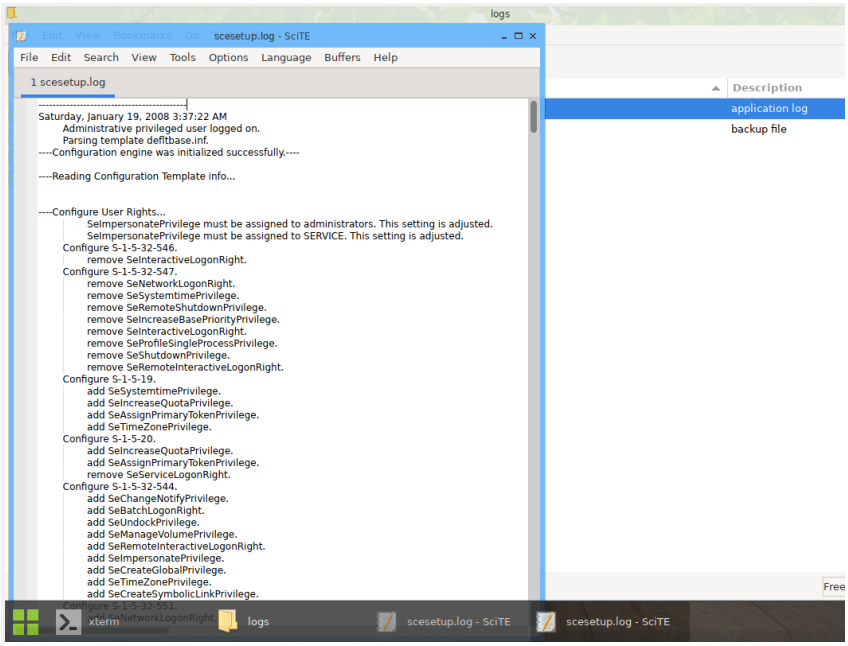


Fonte: Própria



Fonte: Própria

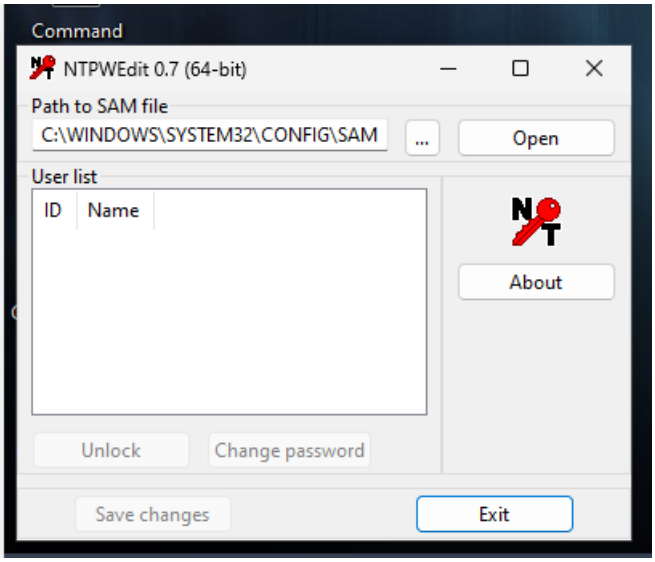
Além disso outros dados sensíveis podem ser acessados livremente, como arquivos de log, onde podemos conseguir várias informações de como o servidor trabalha e as transações feitas. Sendo esse um dos vários arquivos de log que podem ser encontrados apenas com essa técnica.



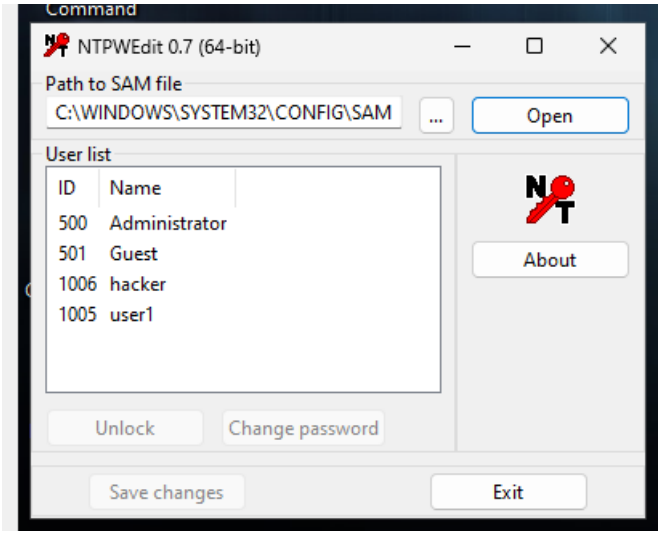
Fonte: Própria

Já utilizando essa tática já é possível ter acesso a vários dados importantes do servidor, mas querendo ter um acesso maior ao sistema foi utilizado o Hirens Boot, um sistema operacional baseado em Windows que possui várias ferramentas para a solução de problemas em computadores.

Uma dessas ferramentas é o NT Password Edit v0.7, uma ferramenta para redefinição de senha. Usando essa ferramenta foi possível redefinir a senha e poder acessar a conta de administrador.

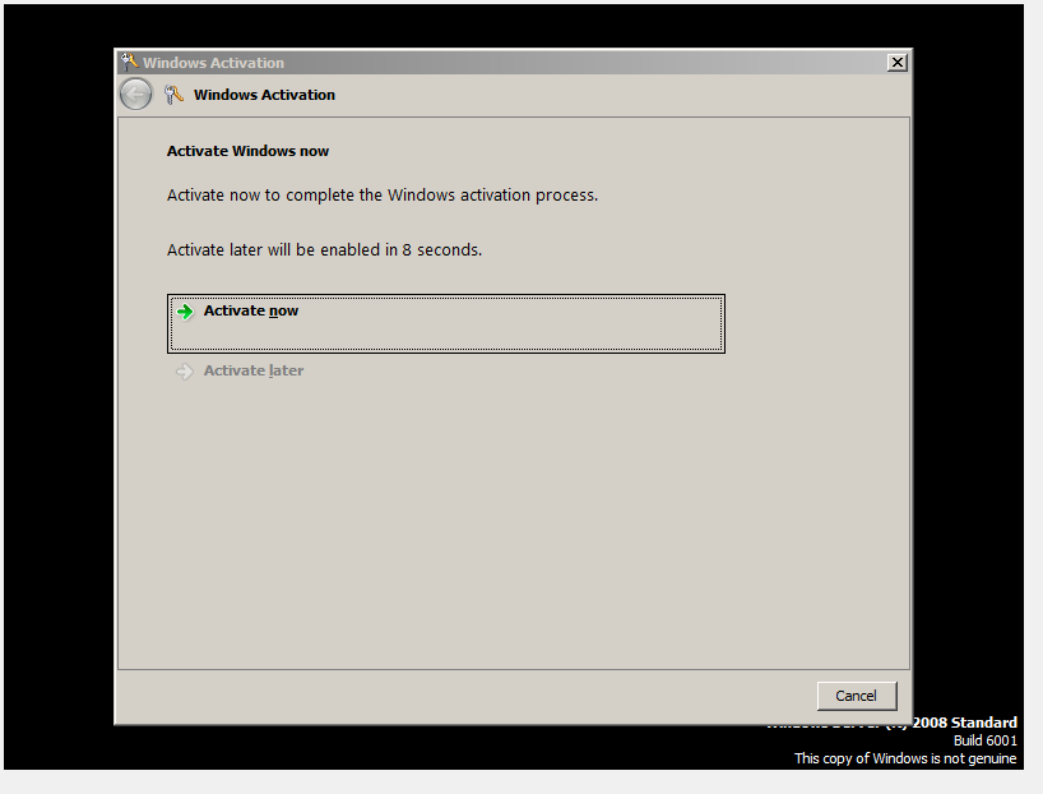


Fonte: Própria



Fonte: Própria

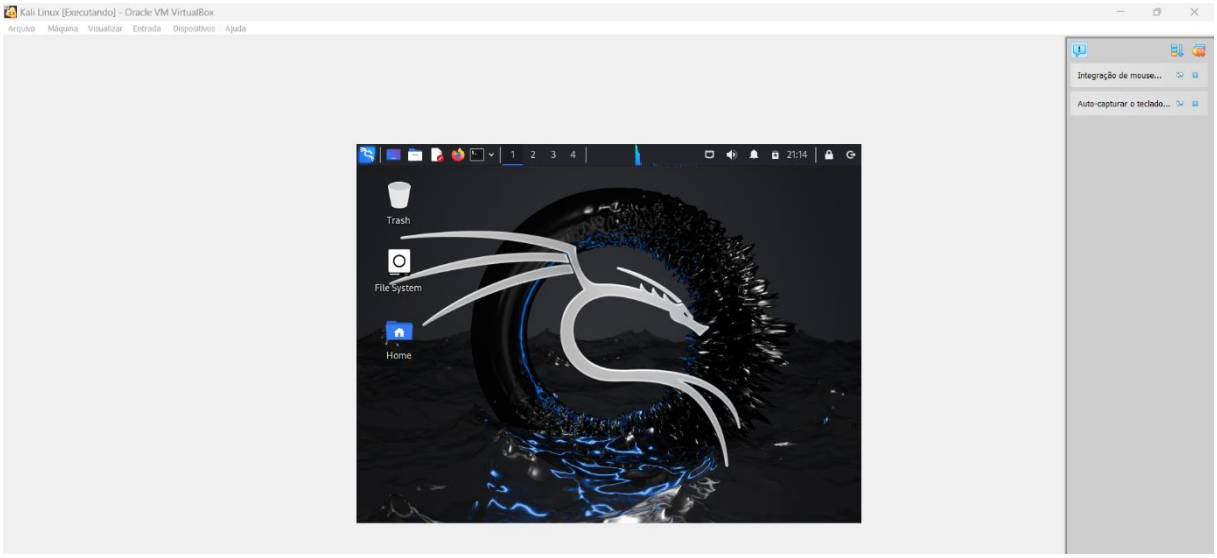
Ao logar foi possível em seu primeiro acesso notar que o sistema da imagem selecionada estava com o seu Windows desativado, assim já deixando que o sistema ficasse exposto.



Fonte: Própria

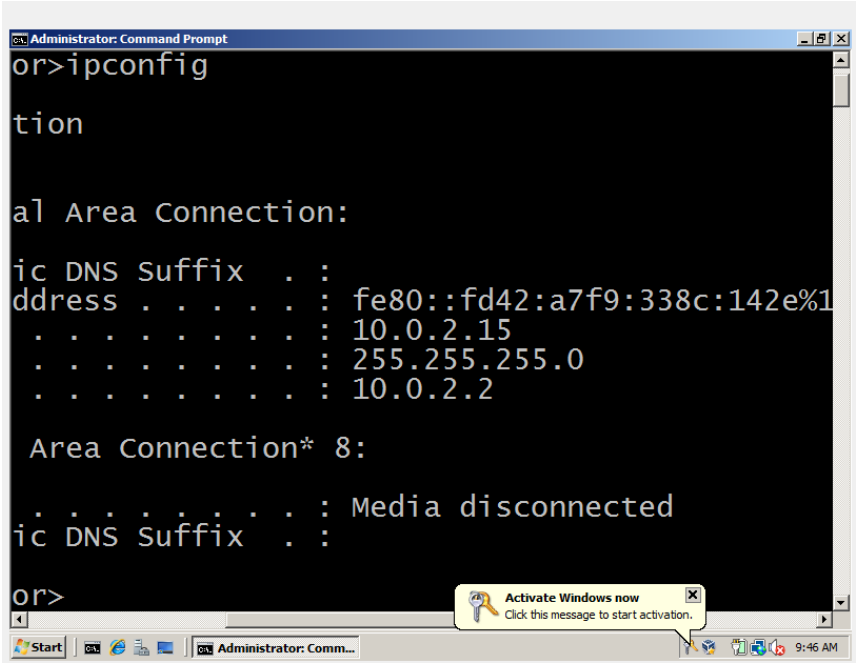
Feito isso o próximo passo foi criar uma segunda máquina virtual, onde essa estaria com o sistema operacional Kali Linux, esse sistema possui uma série de ferramentas voltadas para a área de invasão e *pentest*.

Esse sistema operacional pode ser baixado na sua versão como máquina virtual no próprio site do sistema operacional, precisando apenas importar para a hospedeiro, essa forma é mais prática e simples, pois já vem devidamente configurado. As credenciais de acesso e senha de root são informadas no próprio site. Uma vez importando com sucesso a máquina virtual ela já está pronta para uso.

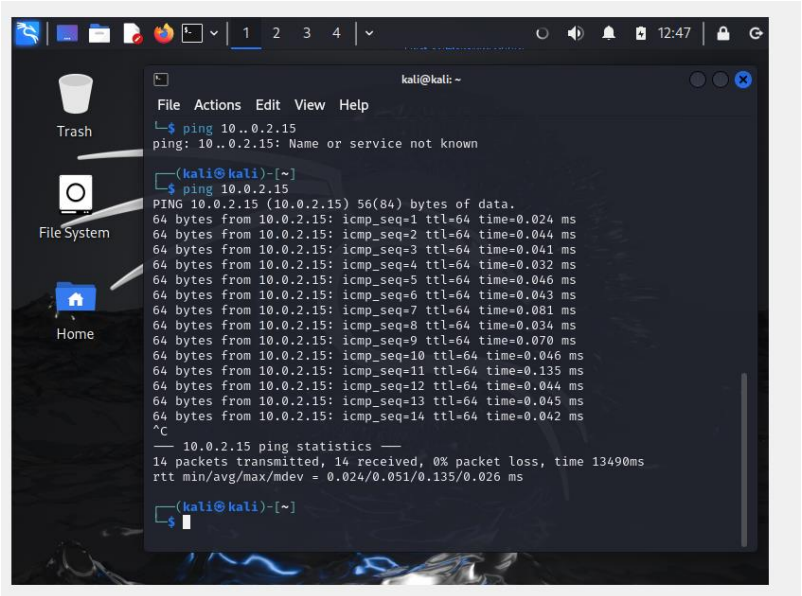


Com esse sistema ligado com a máquina virtual do servidor via rede NAT, dessa forma com as duas máquinas estando ligadas na mesma rede seria possível acessar o servidor e começar os testes.

Pode ser feito um teste para verificar que as duas máquinas estão conectadas na mesma rede ao através do Kali Linux tentar dá um *ping* na máquina que possui o servidor. Onde as duas máquinas estão se comunicando sem perca

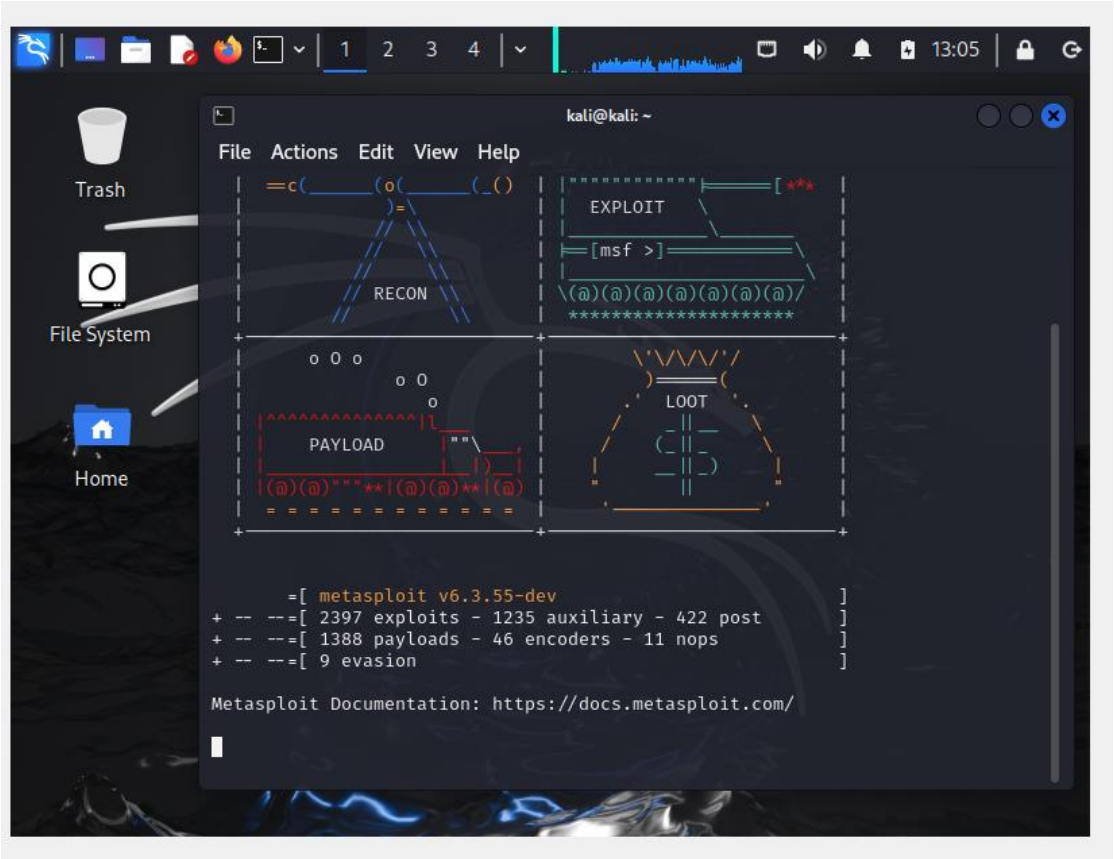


Fonte: Própria



Fonte: Própria

Desta forma já é possível fazer testes de penetração mais elaborados utilizando a rede para esse fim, como o framework *metasplot* que já vem pré-instalado no Kali Linux e possui várias ferramentas para que possa ser feitos os testes.



Fonte: Própria

5 CONCLUSÃO

A implementação de um laboratório de estudo de *Pentest* utilizando imagens encase demonstrou ser uma iniciativa altamente eficaz para o desenvolvimento das competências técnicas e práticas dos alunos em segurança da informação. Este ambiente controlado permite a aplicação realista de técnicas de teste de penetração, essencial para a formação de profissionais qualificados. As imagens encase oferecem um cenário detalhado e autêntico para o aprendizado, promovendo uma compreensão aprofundada das ameaças cibernéticas e das estratégias de mitigação. Assim, o laboratório não só atende às necessidades acadêmicas, mas também prepara os alunos para os desafios do mercado de trabalho na área de cibersegurança.

Além disso, o laboratório serve como uma plataforma para a inovação e o desenvolvimento contínuo de novas técnicas e metodologias de teste de penetração. A colaboração entre alunos e profissionais no ambiente do laboratório promove uma troca de conhecimentos valiosa, contribuindo para o avanço da pesquisa e das práticas em cibersegurança.

Desta forma é possível ter a continuidade desse estudo em trabalhos futuros fazendo a estruturação de uma plataforma onde se possa criar ambientes mais robustos e com tecnologias mais avançadas, criando um sistema de nível de conhecimento e dificuldade para que o estudante possa ir aprimorando suas técnicas.

REFERÊNCIA

ACADEMIA DE FORENSE DIGITAL. Imagens forenses: o que são e quais os tipos mais utilizados. Disponível em: https://academiadeforensedigital.com.br/imagens-forenses-o-que-sao-e-quais-os-tipos-mais-utilizados/. Acesso em: 10 jun. 2024.

AGÊNCIA BRASILEIRA DE INTELIGÊNCIA (ABIN). Engenharia social: guia para proteção de conhecimentos sensíveis. Disponível em: https://www.gov.br/abin/pt-br/institucional/acoes-e-programas/PNPC/boaspraticas/cartilha-engenharia-social-guia-para-protecao-de-conhecimentos-sensiveis. Acesso em: 10 jun. 2024.

ASHEMERY, Asem. DFIR Resources. Disponível em: https://www.ashemery.com/dfir.html. Acesso em: 5 fev. 2024.

BERTOGLIO, D. D.; ZORZO, A. F. Tramonto: Uma estratégia para recomendação de teste de penetração. In: Anais do XVI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg), 2016.

BERTOGLIO, D. D.; ZORZO, A. F. Um mapeamento sistemático sobre testes de penetração. Resumo Técnico: no. 84. Porto Alegre: Faculdade de Informática PUC-RS, 2015.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Diário Oficial da União, Brasília, DF, 23 abr. 2014.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018.

CARRIER, Brian; SPAFFORD, Eugene H. An event-based digital forensic investigation framework. Disponível em: https://dfrws.org/wp-content/uploads/2019/06/2004_USA_pres-an_event-based_digital_forensic_investigation_framework.pdf. Acesso em: 10 jun. 2024.

CHAD MAIN. Percipient. Overview: The Three Types of Forensic Collections – Physical vs. Logical vs. Targeted. 2022. Disponível em: https://percipient.co/overview-the-three-types-of-forensic-collections-physical-vs-logical-vs-targeted/. Acesso em: 14 fev. 2024.

CFReDS Portal. Disponível em: https://cfreds.nist.gov/all. Acesso em: 10 jun. 2024.

DANTAS, Y. G. Estratégia para o tratamento de ataque de negação de serviço na camada de aplicação em redes IP. 2015. Dissertação (Mestrado em Informática) – Universidade Federal da Paraíba, João Pessoa, 2015.

DUARTE, L. O. Análise de vulnerabilidades e ataques inerentes a redes sem fio 802.11x. 2003. Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) – Universidade Estadual Paulista, São José do Rio Preto, 2003. Disponível em: http://smeduquedecaxias.rj.gov.br/nead/Biblioteca/Formação%20Continuada/Tecnologia/cursos/seguranca/ataques%20e%20vulnerabilidades%20em%20redes%20sem%20fio.pdf. Acesso em: 15 nov. 2023.

EXTERRO. FTK Product Downloads. Disponível em: https://www.exterro.com/ftk-product-downloads/. Acesso em: 5 fev. 2024.

HERZOG, Pete. OSSTMM3: the open source security testing methodology manual – contemporary security testing and analysis. 2010. Disponível em: https://www.isecom.org/OSSTMM.3.pdf. Acesso em: 14 nov. 2023.

IBM. Engenharia Social. Disponível em: https://www.ibm.com/br-pt/topics/social-engineering. Acesso em: 10 jun. 2024.

KALI LINUX. Disponível em: https://www.kali.org/. Acesso em: 10 abr. 2024.

LEPESQUEUR, Alexandre M.; OLIVEIRA, Ítalo D. Pentest, Análise e Mitigação de Vulnerabilidades. 2006. Trabalho de Conclusão de Curso (Graduação em Engenharia de Redes de Comunicação) – Universidade de Brasília, Brasília, 2006.

Lee, H. C., Palmach, T., & Miller, M. T. (2001). *Henry Lee's Crime Scene Handbook*. San Diego, CA: Academic Press.

MAZIERO, C. A. Sistemas operacionais: conceitos e mecanismos. Curitiba: Editora da UFPR, 2019.

Metasploit. Disponível em: https://www.metasploit.com/. Acesso em: 10 jun. 2024.

MORENO, Daniel. Pentest em redes sem fio. 1. ed. São Paulo: Novatec Editora, 2016.

MORENO, D. Introdução ao pentest: aprenda a realizar testes de invasão de forma ética e profissional. São Paulo: Novatec Editora, 2015.

OWASP Top Ten. Disponível em: https://owasp.org/www-project-top-ten/. Acesso em: 31 out. 2023.

RAEDTS.BIZ. Forensics 101: What is a forensic image? 2017. Disponível em: https://www.raedts.biz/forensics/forensics-101-forensic-image/. Acesso em: 14 mai. 2024.

RUFINO, N. M. de O. Segurança em Redes sem Fio: Aprenda a proteger suas informações em ambientes Wi-Fi e Bluetooth. São Paulo: Novatec Editora, 2015. Disponível em: https://s3.novatec.com.br/capitulos/capitulo-9788575222430.pdf. Acesso em: 15 set. 2023.

SERPRO. Dados Sensíveis LGPD. Disponível em: https://www.serpro.gov.br/lgpd/menu/protecao-de-dados/dados-sensiveis-lgpd. Acesso em: 11 nov. 2023.

SLAX. Disponível em: https://www.slax.org/. Acesso em: 5 mar. 2024.

VIRTUALBOX. Disponível em: https://www.virtualbox.org/. Acesso em: 10 fev. 2024.

WEIDMAN, Georgia. Teste de invasão: uma introdução prática ao hacking. 1. ed. São Paulo: Novatec Editora, 2014.

APÊNDICE

Termo De Autorização De Publicação De Produção Acadêmica

O(A) estudante **Lidia Paula de Oliveira Silva** do curso Ciência da Computação matricula 2019.1.0028.0097-6, telefone (62) 99983-5830, e-mail lidia5000@hotmail.com, na qualidade de titular dos direitos autorais, em consonância com a Lei no 9.610/98 (Lei dos Direitos do autor), autoriza a Pontifícia Universidade Católica de Goiás (PUC Goiás) a disponibilizar o Trabalho de Conclusão de Curso intitulado ***Pentest* Baseado Em Imagens Encase: Uma Análise De Vulnerabilidades Em Servidores Web**, gratuitamente, sem ressarcimento dos direitos autorais, por 5 (cinco) anos, conforme permissões do documento, em meio eletrônico, na rede mundial de computadores, no formato especificado (Texto (PDF); Imagem (GIF ou JEPG): Som (WAVE, MPEG, AIFF, SNS); Vídeo (MPEG,MWV, AVI, QT); outros, específicos da área; para fins de leitura e/ou impressão pela internet, a título de divulgação da produção científica gerada nos cursos de graduação da PUC Goiás.

Goiânia, 26 de junho de 2024

Assinatura do(s) autor(es):_____

Nome completo do autor: Lidia Paula de Oliveira Silva

Assinatura do professor-orientador:_____

Nome completo do professor-orientador: Claudio Martins Garcia