DISSERTAÇÃO DE MESTRADO PROFISSIONAL

PROPOSTA DE CONTROLES DE SEGURANÇA PRIORITÁRIOS CONTRA ATAQUES EM REDES LOCAIS COM DISPOSITIVOS COMPACTOS

PAULO VICTOR DE ARAÚJO DA SILVA

Programa de Pós-Graduação Profissional em Engenharia Elétrica

DEPARTAMENTO DE ENGENHARIA ELÉTRICA
FACULDADE DE TECNOLOGIA
UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA
Faculdade de Tecnologia

DISSERTAÇÃO DE MESTRADO PROFISSIONAL

PROPOSTA DE CONTROLES DE SEGURANÇA PRIORITÁRIOS CONTRA ATAQUES EM REDES LOCAIS COM DISPOSITIVOS COMPACTOS

PAULO VICTOR DE ARAÚJO DA SILVA

Dissertação de Mestrado Profissional submetida ao Departamento de Engenharia Elétrica como requisito parcial para obtenção do grau de Mestre em Engenharia Elétrica

Banca Examinadora

Prof. Georges Daniel Amvame Nze, Ph.D, FT/UnB _____
Orientador

Prof. Fábio Lúcio Lopes Mendonça, Ph.D, FT/UnB _____
Examinador Interno

Prof. Ricardo Paranhos Pinheiro, Ph.D, UPE _____
Examinador externo

Prof. Daniel Alves da Silva, Ph.D, FT/UnB _____
Examinador interno suplente

FICHA CATALOGRÁFICA

SILVA, PAULO VICTOR DE ARAÚJO DA
PROPOSTA DE CONTROLES DE SEGURANÇA PRIORITÁRIOS CONTRA ATAQUES EM REDES LOCAIS COM DISPOSITIVOS COMPACTOS [Distrito Federal] 2025.
xvi, 78 p., 210 x 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2025).
Dissertação de Mestrado Profissional - Universidade de Brasília, Faculdade de Tecnologia.
Departamento de Engenharia Elétrica

1. Frameworks	2. Intrusões Físicas
3. Perímetro	4. Defesa em Profundidade
I. ENE/FT/UnB	II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

SILVA, P. V. A. (2025). *PROPOSTA DE CONTROLES DE SEGURANÇA PRIORITÁRIOS CONTRA ATAQUES EM REDES LOCAIS COM DISPOSITIVOS COMPACTOS*. Dissertação de Mestrado Profissional, Publicação: PPEE.MP.103. Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 78 p.

CESSÃO DE DIREITOS

AUTOR: PAULO VICTOR DE ARAÚJO DA SILVA
TÍTULO: PROPOSTA DE CONTROLES DE SEGURANÇA PRIORITÁRIOS CONTRA ATAQUES EM REDES LOCAIS COM DISPOSITIVOS COMPACTOS.
GRAU: Mestre em Engenharia Elétrica ANO: 2025

PAULO VICTOR DE ARAÚJO DA SILVA
Depto. de Engenharia Elétrica (ENE) - FT
Universidade de Brasília (UnB)
Campus Darcy Ribeiro
CEP 70919-970 - Brasília - DF - Brasil

DEDICATÓRIA

Dedico este trabalho à minha mãe, que, com todos os erros e acertos, fez o melhor que pôde para me conduzir até onde estou hoje.

Dedico-o também, de forma especial, à minha esposa Vivian, que me apoiou desde o primeiro momento em que considerei investir tempo e esforço nesta jornada acadêmica e de aprendizado. Sem ambas, nada disso teria sido possível.

AGRADECIMENTOS

Agradeço primeiramente a Deus, que me guia, sustenta, motiva e dá forças sobrenaturais para vencer os mais difíceis obstáculos da vida.

Ao meu amigo Dyego, que serviu de exemplo e inspiração para que este plano pudesse ter início.

Sou grato ao meu orientador, Prof. Dr. Georges Daniel Amvame Nze, que, com paciência, conhecimento e humildade, foi fundamental para o meu desenvolvimento e para a execução deste trabalho.

Também agradeço aos professores que tornaram minha formação possível: Prof. Dr. William Ferreira Giozza, Prof. Dr. Fábio Lúcio Lopes de Mendonça, Prof. Dr. Ricardo Staciarini Puttini, Prof. Dr. Rafael Rabelo Nunes e Prof. Dr. Robson de Oliveira Albuquerque.

Agradeço a todo o corpo administrativo do Programa de Pós-Graduação em Engenharia Elétrica (PPEE), em especial às colegas Tayná, Ludmilla, Julia e Cristiana, pela constante disposição em esclarecer dúvidas e auxiliar prontamente em todo tipo de demanda.

Sou igualmente grato ao período de trabalho duro e braçal que vivenciei, pois foi o melhor professor, ensinando-me o valor e a importância dos estudos.

RESUMO

As medidas de proteção para redes corporativas podem variar significativamente, indo de controles administrativos até controles técnicos, e identificar quais são apropriados para cada ameaça específica torna-se um desafio dentro de frameworks que reúnem dezenas ou centenas de salvaguardas. Nesse contexto, este trabalho examina um vetor particular e crescente de exploração: as intrusões físicas que inserem dispositivos compactos e espúrios nas redes alvo, capazes de realizar ponte, clonagem de endereços, sniffing, bypass de NAC e movimentação lateral. Tais técnicas possuem alto impacto e representam risco direto à continuidade de negócio, pois exploram fragilidades que vão além da segurança de perímetro.

Após um estudo aprofundado das formas de ataque, incluindo modelagem com árvore de ataque e análise de casos reais, esta pesquisa propõe um modelo estruturado de defesa em profundidade, fundamentado no NIST SP 800-53, para tratamento do problema. O trabalho utiliza a metodologia Design Science Research (DSR) para investigar o cenário, projetar e priorizar controles, e avaliar sua eficácia. O conjunto final inclui controles administrativos, operacionais e técnicos voltados à prevenção, detecção, mitigação e resposta, abrangendo, por exemplo, NAC/802.1X, SIEM/IDS, inventário e descoberta de ativos, bloqueios automáticos.

Parte desses controles foi implementada em laboratório por meio de provas de conceito, demonstrando sua aplicabilidade prática; adicionalmente, evidências de um cenário real permitiram analisar o impacto dos controles na redução de ataques e incidentes. Os resultados mostram avanços significativos frente a trabalhos correlatos e reforçam a importância de medidas multicamadas para lidar com ameaças que utilizam dispositivos compactos. Por fim, o estudo apresenta limitações, discute implicações práticas e aponta direções para pesquisas futuras.

Palavras-chave: Frameworks, Intrusões Físicas, Perímetro, Defesa em Profundidade.

ABSTRACT

Protection measures for corporate networks can vary significantly, ranging from administrative to technical controls, and identifying which ones are appropriate for each specific threat becomes a challenge within frameworks that contain dozens or even hundreds of safeguards. In this context, this work examines a particular and increasingly relevant exploitation vector: physical intrusions that insert compact and rogue devices into target networks, capable of performing bridging, address cloning, sniffing, NAC bypass, and lateral movement. Such techniques have high impact and pose a direct risk to business continuity, as they exploit weaknesses that go beyond perimeter security.

After an in-depth study of these attack methods, including attack-tree modeling and analysis of real cases, this research proposes a structured defense-in-depth model, grounded in NIST SP 800-53, to address the problem. The study employs the Design Science Research (DSR) methodology to investigate the scenario, design and prioritize controls, and evaluate their effectiveness. The final set includes administrative, operational, and technical controls aimed at prevention, detection, mitigation, and response, encompassing, for example, NAC/802.1X, SIEM/IDS, asset inventory and discovery mechanisms, and automated blocking.

Part of these controls was implemented in a laboratory through proofs of concept, demonstrating their practical applicability; additionally, evidence from a real-world scenario enabled an assessment of the controls' impact on reducing attacks and incidents. The results show significant advancements compared to related work and reinforce the importance of multilayered measures to address threats involving compact devices. Finally, the study presents limitations, discusses practical implications, and points to directions for future research.

SUMÁRIO

1 INTRODUÇÃO 1
1.1 OBJETIVOS DO TRABALHO 2
1.1.1 OBJETIVO GERAL 2
1.1.2 OBJETIVOS ESPECÍFICOS 2
1.2 PRINCIPAIS CONTRIBUIÇÕES 3
1.3 ESTRUTURA E ORGANIZAÇÃO DO TRABALHO 3
1.4 DELIMITAÇÃO DO PROBLEMA 4

2 FUNDAMENTAÇÃO TEÓRICA E TRABALHOS CORRELATOS 5
2.1 MITRE ATT&CK 6
2.2 CIS CONTROLS V8 E CYBOK 1.1.0 6
2.3 MODELO OSI 7
2.4 NETWORK ACCESS CONTROL (NAC) 8
2.5 SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) 9
2.6 INTRUSION DETECTION SYSTEM (IDS) E INTRUSION PREVENTION SYSTEM (IPS) 11
2.7 IEEE 802.1AE - MACSEC 12
2.8 FERRAMENTAS UTILIZADAS NOS LABORATÓRIOS DE PROVA DE CONCEITO 13
2.8.1 VMWARE WORKSTATION 13
2.8.2 VIRTUALBOX 14
2.8.3 GNS3 14
2.8.4 ZABBIX 14
2.8.5 ACTIVE DIRECTORY (AD) 14
2.8.6 PFSENSE 15
2.8.7 SNORT / SURICATA 15
2.8.8 WIRESHARK 15
2.9 TRABALHOS CORRELATOS 15
2.10 LACUNA CIENTÍFÍCA 18

3 METODOLOGIA 20
3.0.1 DIRETRIZES DO DESIGN SCIENCE RESEARCH 21
3.1 INVESTIGAÇÃO DO PROBLEMA - MODELAGEM DA AMEAÇA COM ATTACK-TREE 22
3.1.1 COMO O ATAQUE OCORRE 23
3.2 PROJETO DA SOLUÇÃO - SELEÇÃO PRELIMINAR DE CONTROLES 28
3.2.1 DEFINIÇÃO DOS CONTROLES 29
3.2.2 CRITÉRIOS DE PRIORIZAÇÃO DE CONTROLES PARA CADA CENÁRIO 31

4 PROVA DE CONCEITO (POC) PARCIAL DA SOLUÇÃO 33
4.1 CONTROLES IMPLEMENTADOS EM LABORATÓRIO 33

4.1.1 AC-2 (g) Monitorar o Uso das Contas 34
4.1.2 AC-17 [1] Empregar Mecanismos Automatizados para Monitorar e Controlar Métodos de Acesso Remoto 37
4.1.3 CM-7 (9) (b) Proibir o Uso ou Conexão de Componentes de Hardware não Autorizados 40
4.1.4 CM-8 (a) Desenvolver e Documentar um Inventário de Componentes do Sistema que Reflita com Precisão o Ambiente 43
4.1.5 IA-3 [1] Identificar e Autenticar Dispositivos | Autenticação de Rede Bidirecional 50
4.1.6 IR-4 (5) Implementar um Recurso para Desabilitar Automaticamente um Recurso Caso Violações de Segurança sejam Detectadas 54
4.1.7 SI-4 (1) Conectar e Configurar Ferramentas de Detecção de Intrusão em um Sistema de Detecção de Intrusão para Todo o Sistema 58
4.2 Síntese dos Ambientes e Recursos Utilizados nas Provas de Conceito 62
4.3 Limitações Práticas das Provas de Conceito 63
4.4 Porque Implementar Controles de Segurança em Ambiente de Testes 65

5 Análise de Resultados 66
5.1 Avanços Alcançados em Relação aos trabalhos correlatos 72

6 Conclusões e Trabalhos Futuros 73

Referências Bibliográficas 75

LISTA DE FIGURAS

2.1 Fluxo de Dados no Modelo OSI 7
2.2 Componentes Padrão de um NAC com IEEE 802.1X 9
2.3 Arquitetura Clássica de um SIEM. 10
2.4 IDS versus IPS. 12
2.5 Encapsulamento do Cabeçalho MACsec em um Quadro Ethernet. 13

3.1 Ciclo Regulador de Wieringa (Adaptado) 20
3.2 Estrutura Básica de uma Attack-Tree (Schneier). 22
3.3 Raspberry Pi 4 23
3.4 Mikrotik HAP Mini 23
3.5 Dispositivo encontrado abaixo do piso elevado 25
3.6 Formas de inserção do dispositivo 26
3.7 Visão Geral do Ataque 27
3.8 Árvore do Ataque 28

4.1 Arquitetura do laboratório para Monitoria de Contas de Usuários. 35
4.2 Interface Adaxes. 36
4.3 Adaxes - Último Logon de Usuário 37
4.4 Arquitetura do laboratório para Teste de Bloqueio de Tráfego 38
4.5 Teste de Conexão SSH Bem-sucedida 39
4.6 Regra de Firewall para Bloqueio de Conexões Indevidas 39
4.7 Teste de Conexão SSH Mal-sucedida 40
4.8 Dispositivos Listados por lsusb. 41
4.9 Eventos Relativos ao Dispositivo de Teste. 42
4.10 Monitorando Dispositivos Bloqueados. 42
4.11 Definição e Aplicação de Política por Linha de Comando. 43
4.12 Arquitetura do Laboratório Utilizada para Testes de Inventário. 44
4.13 Configuração do Arquivo do Agente Zabbix. 45
4.14 Comandos para Ativação do SNMPv2 no Switch EXOS. 45
4.15 Caminho para Criação de Instâncias de Host a Serem Monitorados. 46
4.16 Janela para Criação de Hosts para Monitoração. 46
4.17 Mapa do Inventário Monitorado Gerado no Zabbix. 47
4.18 Inserção do Hub e Dispositivo Espúrio como Clone de Host Legítimo. 48
4.19 Resultado do Script ARP-Scan para percepção de Host Clonado. 48
4.20 Definição do Comando para Execução de Script no Host. 49
4.21 Seleção de Script a ser Executado no Host. 49
4.22 MACsec atua na Camada 2 do Modelo OSI. 50
4.23 Comandos para Ativação e Configuração do MACsec no Linux. 51
4.24 Verificação do estado do MACsec no Debian. 52

4.25 Verificação do estado do MACsec no Parrot. 52
4.26 Verificação do estatísticas do MACsec no Debian. 52
4.27 Verificação do estatísticas do MACsec no Parrot. 53
4.28 Captura de Tráfego MACsec entre os Hosts. 53
4.29 Arquitetura do Laboratório para Teste de Bloqueio de Porta. 55
4.30 Estado da Porta Habilitado. 55
4.31 Dispositivo Legítimo Identificado. 56
4.32 Identificação do Dispositivo do Atacante. 56
4.33 Comandos Para Ativação do MAC-Locking. 57
4.34 Bloqueio de Porta Utilizada para o Ataque. 57
4.35 Arquitetura do Laboratório para Teste com IDS. 59
4.36 Formato de Regra do Snort. 60
4.37 Tela de Alertas do Snort com Evidências de Anomalias. 61
4.38 Tela de Alertas do Suricata com Evidências de Anomalias. 62

5.1 Grau de complexidade de implementação cada controle 69
5.2 Comparação de Ataques Ocorridos e Bem-sucedidos, Antes e Após Implementação de Controles em um Cenário Real 70
5.3 Distribuição de atuação de controles em relação aos incidentes registrados em 2024 71

LISTA DE TABELAS

2.1 Trabalhos Correlatos Avaliados 18

3.1 Diretrizes para Design Science 21
3.2 Proposta de Controles de Segurança 31

4.1 Informações consolidadas dos laboratórios implementados 63

1 INTRODUÇÃO

Nos últimos anos, ataques cibernéticos têm se tornado cada vez mais sofisticados, explorando redes corporativas não só a partir da Internet, mas também das próprias redes internas, utilizando dispositivos de baixo custo, tamanho compacto, técnicas para evitar detecção e engenharia social para comprometer grandes organizações (1).

Em 2018, a NASA sofreu uma invasão em sua rede, em que um dispositivo Raspberry Pi foi utilizado para acessar informações sigilosas sobre missões espaciais, expondo falhas graves no gerenciamento de inventário de dispositivos conectados à rede e detecção de dispositivos espúrios (2). De forma semelhante, em 2024, o Banco do Brasil registrou um prejuízo de R$ 40 milhões, após invasores instalarem dispositivos em cabos de dados para acessar sistemas internos e contas de correntistas, além de corromperem funcionários através de técnicas de engenharia social (3). Já o Instituto Nacional do Seguro Social (INSS) brasileiro também foi alvo de ataques que exploraram a rede interna, reforçando a necessidade de fortalecer políticas de controle de dispositivos e acessos para mitigar tais ameaças. Esses exemplos demonstram a crescente vulnerabilidade em infraestruturas organizacionais frente a dispositivos espúrios e ataques cibernéticos bem orquestrados (4).

Em outro caso real, conforme relato confidencial para fins acadêmicos, uma empresa pública brasileira do ramo financeiro vem sofrendo ataques cibernéticos recorrentes em que atacantes utilizam dispositivos compactos, como Raspberry Pi e equipamentos da marca Mikrotik. A organização reportou que encontrou, somente em 2023, 30 dispositivos e, embora medidas de segurança estejam em constante aprimoramento, os ataques foram particularmente difíceis de detectar, devido ao pequeno tamanho e à flexibilidade dos dispositivos utilizados pelos invasores. Os incidentes continuam sob investigação e acompanhamento.

Embora alguns desses ataques cheguem à mídia, muitos casos semelhantes provavelmente ocorrem sem qualquer notificação pública. Em geral, organizações evitam divulgar esses incidentes e preferem lidar com eles internamente, para evitar danos à reputação e para que outros atacantes não se sintam motivados a repetir os ataques. Contudo, a falta de visibilidade desses casos torna difícil a mensuração do verdadeiro impacto desse tipo de ameaça, sugerindo que o número de ocorrências possa ser muito maior do que o relatado.

Nesse cenário, somam-se ainda as preocupações relacionadas à privacidade e proteção de dados pessoais, já que incidentes envolvendo dispositivos compactos podem resultar em acesso, alteração ou divulgação não autorizada de informações sensíveis. Tanto a Lei Geral de Proteção de Dados (LGPD)(5), em vigor no Brasil, quanto o General Data Protection Regulation (GDPR)(6), aplicável na União Europeia, compartilham princípios fundamentais como a finalidade do tratamento, a necessidade de limitar a coleta ao mínimo indispensável, a transparência nas operações e a responsabilização das organizações. Esses pilares, comuns entre os dois modelos regulatórios, reforçam a importância de práticas de segurança que assegurem não apenas a proteção técnica dos sistemas, mas também a salvaguarda dos direitos dos titulares de dados. O descumprimento dessas diretrizes pode acarretar sanções legais significativas, além de comprometer a confiança e a reputação institucional.

Além de legislações voltadas especificamente à privacidade de dados, como a LGPD e o GDPR, é importante considerar marcos regulatórios mais abrangentes relacionados à cibersegurança organizacional e setorial. A NIS2 Directive, em vigor na União Europeia, amplia as exigências de segurança para setores essenciais e importantes, impondo obrigações de gestão de risco e resposta a incidentes, bem como prazos rígidos de notificação (7). Nos Estados Unidos, destaca-se o Federal Information Security Modernization Act (FISMA), que estabelece responsabilidades claras para órgãos federais na proteção de sistemas de informação e integra práticas de auditoria e gestão de riscos (8). No Brasil, iniciativas recentes como o Plano Nacional de Cibersegurança (PNCiber) reforçam a necessidade de uma abordagem estratégica e coordenada, orientando tanto a administração pública quanto setores privados críticos (9). Em conjunto, esses instrumentos evidenciam uma tendência global de fortalecer a resiliência cibernética por meio de marcos regulatórios que complementam frameworks técnicos, como o NIST SP 800-53, e impõem às organizações padrões mínimos de proteção diante de um cenário de ameaças em constante evolução.

Devido à ampla variedade de controles de segurança disponíveis, priorizar essas medidas para lidar com problemas específicos torna-se um desafio significativo, pois não existe um conjunto único de controles de segurança que enderece todos os riscos (10). Portanto, deve-se considerar o contexto em que o sistema esteja inserido e outras circunstâncias como obrigações regulatórias e políticas; a natureza das operações organizacionais; as funcionalidades específicas empregadas nos sistemas; processos negociais; interesses privados dos indivíduos; os tipos de informações processadas, armazenadas e transmitidas e; principalmente, o horizonte de ameaças enfrentadas por cada organização (10).

A implementação de múltiplos controles pode ainda criar uma sobrecarga operacional e dificultar a identificação de soluções eficazes para cada vulnerabilidade, além de gerar risco residual (11).

Considerando a dificuldade em priorizar de forma eficiente os controles de segurança indicados para cada cenário e o impacto dos ataques de intrusão com a utilização de dispositivos compactos e furtivos, este trabalho apresenta uma proposta de priorização de controles de segurança focados em prevenir, detectar e mitigar esse tipo de ataque, utilizando a metodologia Design Science Research (DSR).

1.1 OBJETIVOS DO TRABALHO

1.1.1 Objetivo Geral

Propor e validar um conjunto de controles de segurança prioritários para prevenir, detectar, mitigar e responder a ataques de intrusão física em redes locais por meio da inserção de dispositivos compactos (e.g., Raspberry Pi, Mikrotik), estruturado sob defesa em profundidade e fundamentado no NIST SP 800-53.

1.1.2 Objetivos Específicos

Modelar o ataque com attack-tree (cenários bridge, ligação direta e via hub/clone).

Selecionar controles alinhados ao problema (prevenção, detecção, mitigação e resposta), com base em critérios de risco, impacto e custo-benefício.

Implementar PoCs em laboratório para um subconjunto crítico de controles técnicos.

Avaliar eficácia dos controles com métricas objetivas e evidências de um cenário real.

Discutir limitações e propor trabalhos futuros (ampliação do escopo e automações).

1.2 PRINCIPAIS CONTRIBUIÇÕES

Metodológica: Utilização de DSR (Hevner/Wieringa) para construir e avaliar um artefato (portfólio priorizado de controles) focado em um vetor específico de ameaça (dispositivo compacto inserido fisicamente). Esta metodologia é indicada para construção de artefatos que solucionem problemas concretos do mundo real.

Prática: priorização guiada por NIST SP 800-53 com PoCs (SIEM/IDS, MACsec, NAC, inventário/-descoberta e bloqueios automáticos) e evidência em cenário real.

Científica: lacuna endereçada—poucos trabalhos tratam explicitamente de dispositivos compactos físicos em redes internas com validação prática multicamadas.

Reutilizável: critérios de priorização e roteiros de PoC transferíveis a contextos corporativos diversos.

1.3 ESTRUTURA E ORGANIZAÇÃO DO TRABALHO

O trabalho está dividido em 6 partes principais, incluindo esta introdução.

A parte 1 ou introdução contextualiza brevemente o cenário estudado e expõe a relevância do tema, objetivos geral e específico e principais contribuições desta pesquisa.

A seção 2 que apresenta a fundamentação teórica e os trabalhos correlatos que servem de base e ponto de partida para esta pesquisa, bem como para o completo entendimento dos assuntos aqui tratados.

A seção 3 apresenta a metodologia utilizada para construção da proposta de controles de segurança, bem como a própria relação de controles específicos para o problema investigado.

A seção 4 apresenta algumas provas de conceito, realizadas em laboratório, sobre controles-chave desta proposta .

Na seção 5, é realizada análise de resultados alcançados, com base na implementação de alguns dos controles de segurança em um cenário real.

As conclusões e sugestões para trabalhos futuros são abordados na seção 6.

1.4 DELIMITAÇÃO DO PROBLEMA

Foco em ataques internos com inserção física de dispositivos compactos em LANs corporativas, visando o salto inicial e movimentação lateral. O escopo prioriza prevenção, detecção e resposta na camada 2/3 (incluindo 802.1X/MACsec, NAC, inventário e IDS/SIEM), não abrangendo outros vetores como Wi-Fi público/war-driving, supply-chain de hardware ou ataques puramente lógicos via internet.

2 FUNDAMENTAÇÃO TEÓRICA E TRABALHOS CORRELATOS

A priorização de controles de segurança é um tema amplamente discutido no campo da segurança cibernética. A publicação especial (SP) do NIST, SP 800-53 em sua quinta revisão (2020), destaca que a seleção e priorização de controles deve ser guiada por uma análise de riscos criteriosa, que avalie a criticidade dos ativos, as ameaças associadas e o impacto potencial dos ataques. Por esse motivo, o objetivo principal dessa abordagem é garantir que os controles implementados estejam alinhados às necessidades específicas da organização, levando em consideração fatores como custo de implementação, eficácia na mitigação dos riscos e aderência aos requisitos regulatórios.

Considerando o caráter exploratório dessa pesquisa, no sentido de levantamento de controles para composição da proposta, foram avaliados alguns frameworks de segurança como CIS Controls V8 e CYBOK 1.1.0, contudo, após análise preliminar, foi percebido que o modelo mais abrangente em termos de quantidade de medidas de segurança é a publicação especial do NIST. Apesar do objetivo de criação do framework, em que o padrão SP 800-53 fosse mandatório para agências governamentais do Estados Unidos, atualmente, esse framework é reconhecido mundialmente como um guia abrangente de boas práticas recomendadas de segurança e serve de base para diversos governos e organizações públicas e privadas do mundo todo (10). Nesse sentido, o próprio NIST define esta publicação como um dos padrões mais abrangentes, em termos de controles de segurança cibernética (10). Esses controles são classificados por famílias, que são agrupamentos de controles, por área foco, como “Controle de Acesso”, “Gerenciamento de Configuração” e “Resposta a Incidentes”, por exemplo. A publicação NIST SP 800-53 reúne, em sua revisão 5, 1007 controles no total, organizados em 20 famílias.

Dessa forma, a opção pelo NIST SP 800-53 mostrou-se mais adequada aos objetivos deste trabalho, uma vez que o CyBOK (Cyber Security Body of Knowledge), embora seja uma importante iniciativa acadêmica que reúne e organiza o corpo de conhecimento em cibersegurança, possui caráter essencialmente conceitual, servindo mais como referência teórica do que como guia prescritivo de implementação de controles (12). Já o CIS Controls v8, por sua vez, apresenta uma abordagem prática e objetiva, composta por um conjunto menor de controles priorizados e facilmente aplicáveis, cujo foco principal é fornecer recomendações claras e de rápida adoção por organizações que buscam elevar seu nível básico de maturidade em segurança (13). Nesse contexto, o NIST SP 800-53 destaca-se por não ser apenas um repositório amplo de controles, mas por oferecer uma estrutura consolidada e reconhecida internacionalmente, que combina profundidade técnica com aplicabilidade prática. Sua adoção por diferentes setores ao longo dos anos reforça a credibilidade do framework, que se mostra particularmente valioso quando há necessidade de direcionar esforços de segurança de maneira estruturada e coerente. Assim, o NIST SP 800-53 apresenta-se como a base mais adequada para a priorização de medidas diante de ameaças específicas, como aquelas decorrentes do uso de dispositivos compactos em redes cabeadas.

Nesta seção, são apresentados a base teórica relativa aos controles avaliados, componentes da proposta, tecnologias relativas ao problema e ao cenário de segurança de redes, além disso, em trabalhos correlatos,

são apresentados alguns trabalhos com relação direta ao modelo proposto.

2.1 MITRE ATT&CK

O MITRE ATT&CK é uma base de conhecimento global que descreve táticas, técnicas e procedimentos (TTPs) usados por adversários reais em todas as fases de um ataque cibernético. Estruturado em táticas que representam objetivos do atacante e técnicas que mostram como esses objetivos são alcançados, o framework permite mapear comportamentos adversários, identificar lacunas defensivas e construir detecções baseadas em evidências práticas. Ele também relaciona grupos de ameaça persistente avançada (APT), malware e ferramentas utilizadas em campanhas reais, tornando-se fundamental para análises de inteligência, Red Teaming, criação de regras em SIEM/EDR/XDR e fortalecimento da defesa em profundidade. Por ser continuamente atualizado com base em incidentes reais, o MITRE ATT&CK se consolidou como referência para compreender como atacantes operam e para orientar a priorização de controles de segurança em diversos frameworks e arquiteturas, incluindo NIST SP 800-53, CIS Controls e Zero Trust.

2.2 CIS CONTROLS V8 E CYBOK 1.1.0

O CIS Controls v8 é um conjunto de salvaguardas priorizadas e práticas, desenvolvido pelo Center for Internet Security (CIS), com foco em oferecer ações objetivas para elevar rapidamente a maturidade de segurança organizacional. Diferente de frameworks mais extensos e normativos, o CIS destaca-se pela simplicidade e aplicabilidade, estruturando 18 controles (e 153 subcontroles) distribuídos em três níveis de implementação (IG1, IG2 e IG3), que permitem adaptar a adoção de acordo com a complexidade, recursos e nível de risco da organização. Seus controles abrangem desde inventário e gestão de ativos, recrudescimento de configurações, controle de acesso e gestão de vulnerabilidades, até monitoramento contínuo, proteção de redes e defesa de aplicações. Por ser direto e orientado a resultados, o CIS Controls é amplamente utilizado como guia inicial ou intermediário para equipes que precisam implementar rapidamente proteções eficazes, funciona como modelo resumido, quando comparado ao NIST SP 800-53, ao transformar princípios de segurança em controles-chave para problemas genéricos (13).

O CyBOK 1.1.0 (Cyber Security Body of Knowledge) é um compêndio acadêmico e conceitual que organiza, de forma estruturada, o corpo de conhecimento essencial em cibersegurança. Diferentemente de frameworks prescritivos de controles, o CyBOK funciona como uma referência teórica abrangente, reunindo princípios, fundamentos e domínios especializados que sustentam a prática profissional e a pesquisa científica em segurança da informação. Sua estrutura engloba áreas como criptografia, redes, análise de malware, gestão de risco, comportamento adversário, engenharia segura, privacidade e sistemas operacionais, oferecendo uma visão profunda e multidisciplinar sobre como ameaças surgem, evoluem e exploram fragilidades técnicas e humanas. Por sua natureza didática, o CyBOK apoia a formação de profissionais, serve como base para projetos acadêmicos e orienta a compreensão do ecossistema de riscos, complementando frameworks como NIST SP 800-53, MITRE ATT&CK e CIS Controls ao fornecer o embasamento conceitual sobre o qual essas práticas são construídas (12).

2.3 MODELO OSI

O modelo OSI (Open Systems Interconnection), proposto pela ISO em 1984, representa uma referência conceitual que organiza a comunicação em redes em sete camadas distintas, sem constituir uma arquitetura de rede propriamente dita (14). Ele estabelece funções específicas para cada camada, padronizando como os protocolos devem interagir para permitir a transmissão e recepção de dados entre sistemas heterogêneos. A relevância desse modelo está em oferecer uma visão estruturada, útil para compreender a lógica do tráfego de informações e a forma como cada protocolo atua dentro de um nível determinado.

As sete camadas são: física (transmissão de bits brutos), enlace de dados (agrupamento em quadros e detecção de erros), rede (roteamento de pacotes), transporte (garantia de entrega fim a fim), sessão (gerenciamento de conexões entre aplicações), apresentação (tradução e criptografia dos dados) e aplicação (protocolos voltados ao usuário, como HTTP e SMTP). Essa divisão permite que cada camada seja estudada e desenvolvida de maneira independente, mas sempre integrada ao funcionamento global da rede.

Abaixo, a figura 2.1 que demonstra como os dados fluem, conforme as setas da imagem, pelas camadas do modelo OSI e entre os hosts envolvidos numa comunicação.

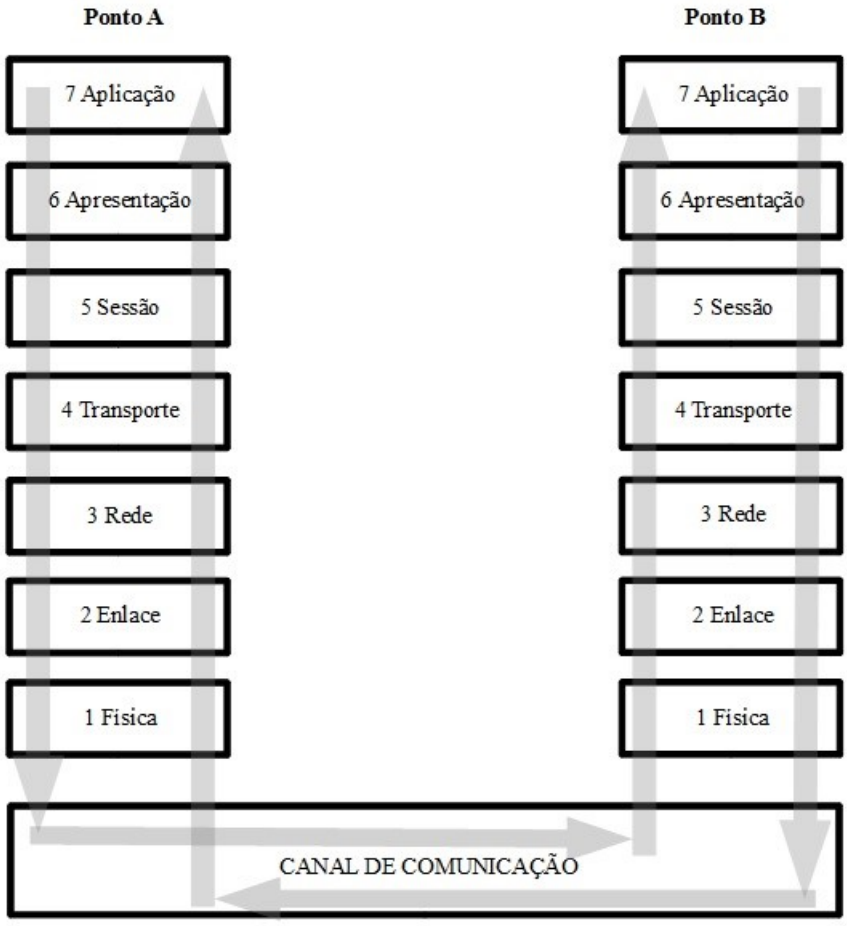

Figura 2.1: Fluxo de Dados no Modelo OSI

Fonte: Laboratório de Eletrônica(15)

O entendimento do modelo OSI é essencial para compreensão do fluxo de dados em redes de computadores e, no presente trabalho, é importante para entender como a conexão física de dispositivos espúrios pode contornar os controles de camadas superiores e explorar fragilidade de camadas inferiores, como as camadas de rede, enlace de dados e física.

No contexto deste trabalho, o modelo OSI ajuda a localizar precisamente onde a inserção física de um dispositivo espúrio impacta a defesa: a camada física permite o acoplamento furtivo; a camada de enlace (L2) é explorada por técnicas como bridge/hub-clone, MAC spoofing e duplicidade de endereços; e a camada de rede (L3) pode ser atingida por DHCP/ARP abuse e pivoting após o primeiro salto. Como os controles tradicionais tendem a se concentrar em camadas superiores (L4–L7), um atacante que se conecte antes do ponto de controle efetivo (ex.: porta de acesso sem 802.1X, segmentação frouxa ou ausência de MACsec) pode contornar políticas de aplicação e explorar fragilidades nas camadas inferiores, reforçando a necessidade de defesa em profundidade iniciando na borda L1/L2.

2.4 NETWORK ACCESS CONTROL (NAC)

O controle de acesso à rede (NAC – Network Access Control) consiste em aplicar políticas que assegurem que apenas usuários e dispositivos autenticados ou em conformidade com requisitos de segurança possam acessar a rede corporativa. Esse controle pode ser baseado em atributos como certificado digital, endereço físico ou impressão digital de dispositivos, reduzindo significativamente a superfície de ataque quanto mais rigorosas forem as verificações (16). Soluções NAC são especialmente relevantes em cenários de BYOD (Bring Your Own Device), visitantes, dispositivos IoT e ambientes corporativos que exigem autenticação constante.

Além da autenticação bidirecional entre cliente e rede, essas soluções permitem a aplicação de políticas complexas, como perfis de acesso diferenciados, segmentação de convidados e verificação de postura de segurança. O uso de NAC facilita a automação de rotinas, aumenta a visibilidade e o controle sobre quem está conectado, diferenciando usuários legítimos de possíveis atacantes. Tais ferramentas operam em dois modos: pré-admissão, em que a autenticação ocorre antes do acesso, e pós-admissão, em que o usuário já conectado precisa de autorização adicional para acessar novos recursos (16).

A figura 2.2 demonstra quais são os componentes padrão de um NAC, utilizando o protocolo IEEE 802.1X:

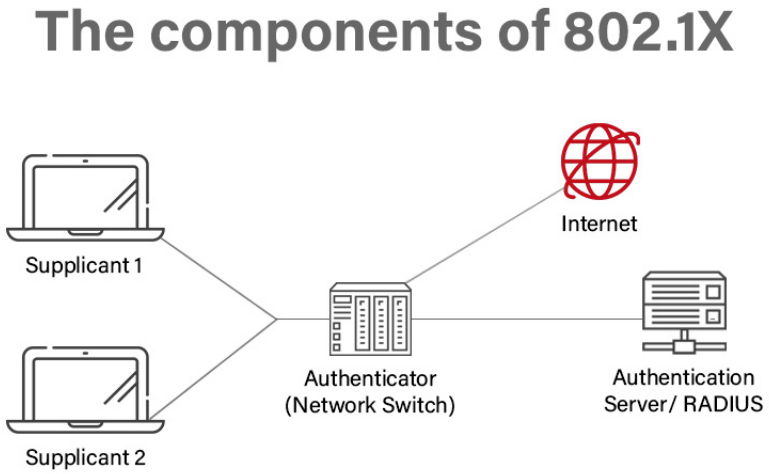

Figura 2.2: Componentes Padrão de um NAC com IEEE 802.1X

Fonte: CloudRadius.com(17)

Para o vetor de conexão física de dispositivos espúrios, o NAC é o primeiro gargalo efetivo: com 802.1X/EAP-TLS, verificação de postura, profiles e VLAN de quarentena, o invasor tende a permanecer não autorizado ou confinado. Contudo, cenários de bridge transparente entre o host legítimo e o switch podem "caronar" a autenticação do usuário (pass-through), exigindo contramedidas como port-security com sticky MAC/violation, detecção de duplicidade IP/MAC, MAB apenas como exceção e telemetria de porta integrada ao SOC. Assim, NAC robusto e bem posicionado reduz a superfície de ataque logo na porta de acesso, mas deve atuar em conjunto com automatizações de bloqueio e monitoramento contínuo para cobrir tentativas de bypass físico.

2.5 SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

SIEM é um sistema de gerenciamento de informações e eventos de segurança que, através da correlação de informações advindas de diversas fontes, tem a capacidade de reconhecer e abordar ameaças variadas, antes que elas se tornem incidentes (18).

Ferramentas SIEM atuais reúnem funções de gerenciamento de informações de segurança (SIM), gerenciamento de eventos de segurança (SEM) e gerenciamento de logs. Além disso, ferramentas mais modernas incorporam análise de comportamento de usuário e entidade (UEBA). SIEM pode ser considerado, atualmente, item básico nos centros de operações de segurança (SOCs) para monitoramento de eventos de segurança (18). Em linhas gerais, pode-se dizer que todas as soluções SIEM realizam agregação de dados, de fontes como servidores, endpoints e ativos de rede. Após a agregação, fazem classificação e correlação dos dados recebidos para transformar essas informações em conhecimentos sobre ameaças (18).

No caso de ataques como conexão de dispositivos espúrios, um SIEM receberia, após a devida configuração de alarmes e gatilhos, informações de switches e do próprio NAC. No caso de conexão direta do dispositivo em um ponto de rede, o endereço físico (MAC Address) do dispositivo pode ser coletado pelo SIEM, permitindo identificação do fabricante desse dispositivo. Nesse caso, um analista do SOC é alertado de que um Raspberry Pi, por exemplo, foi conectado à rede e necessita de atenção tempestiva.

Além de funções básicas já mencionadas, é muito comum encontrar soluções SIEM integradas com outras ferramentas para resposta automática a eventos indesejados. Os tipos de soluções que se integram com SIEM e podem realizar resposta automática são Extended Detection and Response (XDR) e Security Orchestration, Automation and Response (SOAR), do inglês, resposta e detecção estendida e resposta, automação e orquestração de segurança, respectivamente (18).

A figura 2.3 expõe a arquitetura clássica utilizada em muitos projetos de integração de SIEM nas organizações:

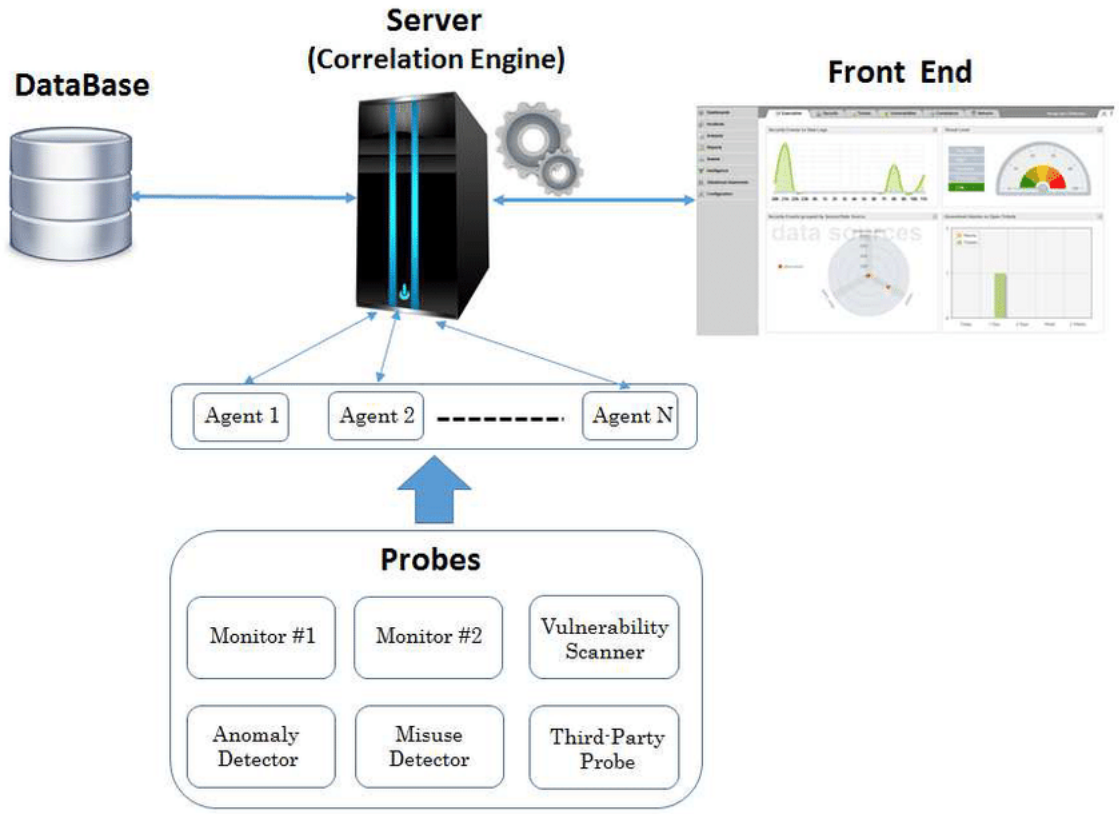

Figura 2.3: Arquitetura Clássica de um SIEM.

Fonte: ResearchGate(19)

Frente à inserção de um dispositivo compacto, o SIEM consolida sinais de rede e de acesso que denunciam o evento: logs de switch/NAC (autenticação falha, novo OUI de fabricante suspeito, flapping de MAC), telemetria L2/L3 (novos DHCP leases, ARP anômalo), e artefatos de C2 (túneis, reverse shells, DNS/HTTP inusitado). Com correlação e UEBA, é possível disparar alertas de "novo dispositivo em porta crítica", mudança de perfil de tráfego do usuário ou elevação súbita de conexões de saída. Integrado a SOAR/XDR, o SIEM pode isolar automaticamente a VLAN, aplicar ACL temporária ou instruir o shutdown

da porta suspeita, reduzindo o tempo de detecção e resposta para minutos no cenário estudado.

2.6 INTRUSION DETECTION SYSTEM (IDS) E INTRUSION PREVENTION SYSTEM (IPS)

Sistemas de detecção de intrusão ou detecção de intrusos são soluções que avaliam o tráfego da rede em busca de sinais que indiquem que há um atacante realizando alguma ação nos sistemas da organização. Já os sistemas de prevenção de intrusão são aqueles focados em atuar ativamente contra os intrusos, derrubando conexões, encerrando sessões, descartando pacotes ou acionando outras soluções. Geralmente, essas soluções atuam juntas e podem ser encontradas em sistemas de firewall de próxima geração (NGFW – Next Generation Firewall) ou integradas entre si em sistemas Intrusion Detection and Prevention System (IDPS) (20).

A detecção em IDS funciona, basicamente, de três formas: baseada em assinatura, em anomalias ou protocolo de estado. O método de detecção baseado em assinatura compara eventos observados com um banco de assinaturas para decidir se o evento pode ou não ser considerado uma intrusão. No método focado detectar anomalias, o sistema compara os eventos observados com uma linha de base de como deve ser o comportamento normal da rede, se o desvio exceder os gatilhos definidos pelos administradores, um alarme de intrusão é gerado. No último caso, protocolo de estado, o sistema compara valores pré-definidos de estado para protocolos chave, em caso de divergência, o desvio notado é apontado como intrusão (20).

É importante ressaltar que soluções de IPS e IDS podem ser baseadas em rede (NIDS), observando e atuando com base no tráfego de rede ou baseadas em host (HIDS), ou seja, avaliando comportamentos dentro de um sistema específico.

No contexto deste trabalho, sistemas de IDS e IPS têm grande relevância, visto que as atividades de detectar e responder a conexões não autorizadas são de extrema importância para proteção de redes contra esses ataques.

A figura 2.4 compara as formas de implementação e funcionamento entre IDS e IPS:

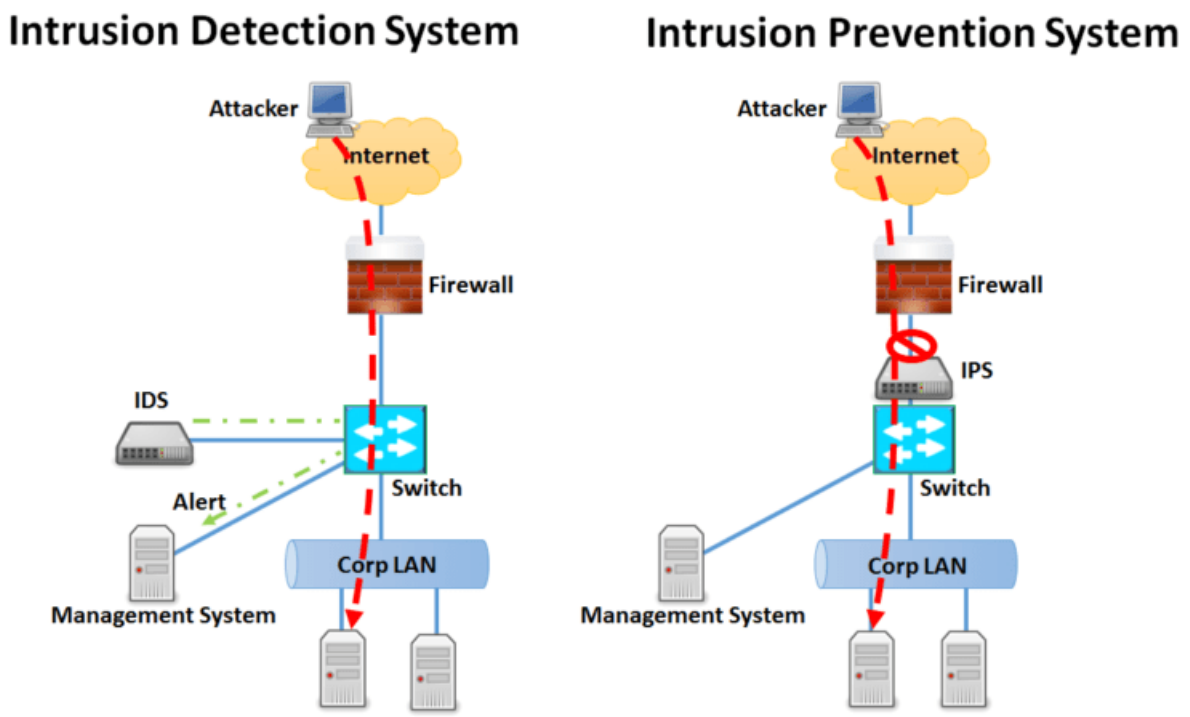

Figura 2.4: IDS versus IPS.

Fonte: TOPS Hong Kong(21)

No problema analisado, NIDS/HIDS complementam NAC e SIEM ao detectar padrões de exploração em L2/L3 e atividades pós-comprometimento: assinaturas para ARP spoofing/DHCP rogue, análise de anomalia para tráfego atípico de um ponto de acesso físico recém-ativado, e estado/protocolo para identificar túneis, SSH reverso, proxies e scanners comuns em kits de intrusão com Raspberry/Mikrotik. Quando posicionados na borda de acesso e em segmentos críticos, IDS/IPS podem bloquear (IPS) ou sinalizar rapidamente (IDS) tentativas de pivoting e exfiltração, oferecendo a camada de detecção e contenção necessária quando o atacante supera o controle inicial de acesso físico.

2.7 IEEE 802.1AE - MACSEC

O MACsec (Media Access Control Security), definido pelo padrão IEEE 802.1AE, é um protocolo de segurança que atua na camada 2 provendo confidencialidade, integridade e autenticação de origem para quadros Ethernet. Ele atua diretamente no enlace de dados, protegendo o tráfego ponto a ponto entre dispositivos conectados, como switches, roteadores e hosts (22).

Diferente de soluções de segurança em camadas superiores, o MACsec garante que os dados estejam protegidos desde o momento em que saem da interface de rede, impedindo que pacotes sejam interceptados, interpretados e modificados por atacantes locais. Essa proteção é feita por meio de criptografia simétrica (geralmente AES-GCM de 128 ou 256 bits)) e mecanismos de autenticação que asseguram que apenas dispositivos autorizados possam participar da comunicação.

A operação do MACsec depende de um protocolo auxiliar, o MKA (MACsec Key Agreement, definido no IEEE 802.1X-2010), responsável por negociar e distribuir as chaves criptográficas entre os dispositivos. Esse processo garante que a comunicação seja segura e dinâmica, mesmo em redes com múltiplos nós (22).

No contexto da segurança de redes corporativas, o MACsec é especialmente relevante em ambientes onde a proteção do tráfego interno é crítica, como data centers, redes industriais e infraestruturas críticas. Esse padrão pode ser utilizado em conjunto com outras soluções, como firewalls e sistemas de detecção de intrusão, compondo uma estratégia de defesa em profundidade.

A figura 2.5 mostra como o MACsec é encapsulado em um quadro Ethernet, conferindo criptografia ao payload transmitido:

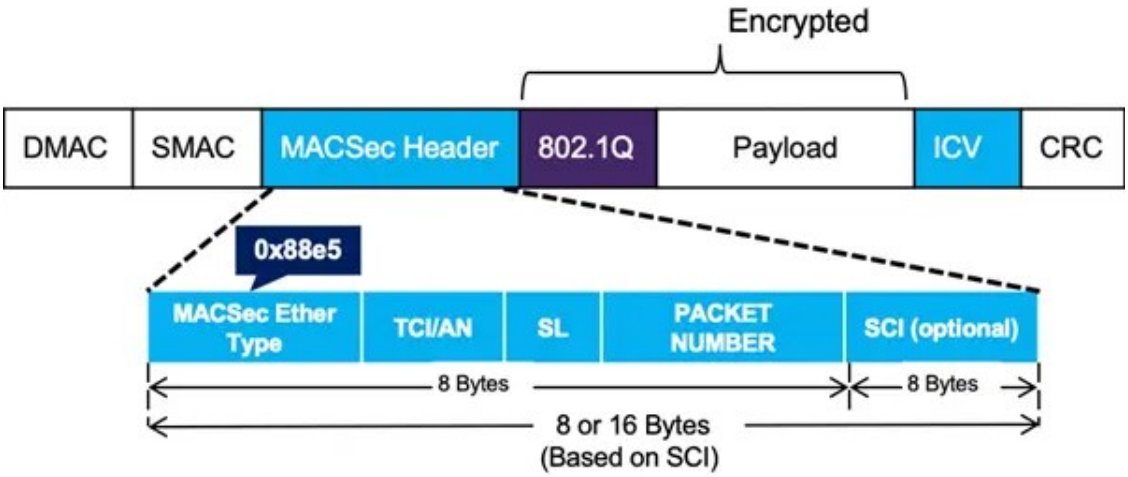

Figura 2.5: Encapsulamento do Cabeçalho MACsec em um Quadro Ethernet.

Fonte: Keysight Technologies(23)

Para ataques de interceptação e manipulação local após a inserção física, o MACsec mitiga sniffing, replay e tampering ao cifrar L2 ponto a ponto. Entretanto, se o agressor se interpõe entre o host e o switch por meio de bridge/hub-clone antes do estabelecimento do MACsec (ou se o MKA/802.1X estiver fraco/ausente), o tráfego pode ser encaminhado como pass-through, preservando a confidencialidade mas permitindo movimentação lateral e abuso de conectividade. Logo, para o cenário estudado, MACsec é essencial porém não suficiente: deve operar com 802.1X forte (EAP-TLS), NAC com políticas de porta, detecção de duplicidade e telemetria de borda integrada ao SOC, garantindo que a cifra em L2 venha acompanhada de autenticação, autorização e monitoramento ativo na porta de acesso.

2.8 FERRAMENTAS UTILIZADAS NOS LABORATÓRIOS DE PROVA DE CONCEITO

2.8.1 VMware Workstation

VMware é uma das principais plataformas de virtualização corporativa, amplamente utilizada em datacenters devido ao seu hypervisor bare-metal ESXi, que oferece alto desempenho, isolamento e confi-

abilidade. Junto ao vCenter Server, a solução permite gerenciamento centralizado e recursos avançados como migração ao vivo (vMotion), alta disponibilidade (HA), tolerância a falhas (FT), clusters distribuídos e integração com redes definidas por software (NSX) (24). Seu ecossistema suportado por grandes fabricantes de hardware e sua capacidade de operar em ambientes híbridos tornam o VMware workstation uma ferramenta útil para estudos práticos, operações corporativas críticas e operações de TI de alta complexidade.

2.8.2 VirtualBox

O VirtualBox é um hypervisor open-source desenvolvido pela Oracle, amplamente utilizado para testes, laboratórios acadêmicos e ambientes de desenvolvimento devido à sua facilidade de uso e compatibilidade com vários sistemas operacionais convidados. Com suporte a recursos como snapshots, redes virtuais, compartilhamento de pastas e diferentes formatos de disco virtual, ele se destaca como uma solução flexível, escalável e acessível para virtualização em desktops (25). Embora não ofereça os recursos corporativos encontrados em plataformas como VMware, o VirtualBox é ideal para experimentação, aprendizagem e simulações de pequena escala.

2.8.3 GNS3

O GNS3 (Graphical Network Simulator 3) é uma plataforma de simulação e emulação de redes que permite combinar dispositivos virtuais, imagens reais de equipamentos de fabricantes como Cisco e Juniper e máquinas virtuais em ambientes complexos (26). Ele é amplamente utilizado para estudos de certificações, validação de arquiteturas e experimentação de topologias avançadas, permitindo criar cenários realistas sem necessidade de hardware físico. Pela flexibilidade e integração com VirtualBox, VMware e contêineres, o GNS3 tornou-se uma ferramenta indispensável para engenheiros de rede, analistas de segurança e estudantes de infraestrutura.

2.8.4 Zabbix

O Zabbix é uma plataforma open-source de monitoramento de redes, servidores e aplicações, capaz de coletar métricas por agentes, SNMP, scripts personalizados e discovery automático. Ele fornece dashboards, triggers inteligentes, alertas, mapas e relatórios, permitindo uma visão ampla do comportamento de ambientes críticos (27). Graças à sua escalabilidade, o Zabbix é frequentemente adotado em grandes organizações e ambientes distribuídos, funcionando como peça-chave para detecção precoce de falhas, análise de capacidade e observabilidade operacional.

2.8.5 Active Directory (AD)

O Active Directory é o serviço de diretório corporativo da Microsoft que centraliza autenticação, autorização e gerenciamento de identidades em redes empresariais. Ele utiliza protocolos como Kerberos e LDAP para controlar usuários, grupos, permissões e políticas de segurança por meio de Objeto de Política

de Grupo (GPO), oferecendo integração com serviços Windows e soluções de nuvem como Azure Entra (antigo Azure AD). Como componente de praticamente todos os ambientes corporativos baseados em Windows, o AD desempenha papel fundamental na governança de identidade, SSO, reforço e implementação de modelos como Zero Trust (28).

2.8.6 pfSense

O pfSense é um firewall e roteador open-source baseado em FreeBSD, reconhecido por sua estabilidade e por oferecer, através de interface web, um conjunto avançado de funcionalidades como NAT, VLANs, VPNs (IPsec, OpenVPN, WireGuard), QoS, balanceamento e failover. Sua modularidade permite a instalação de pacotes como Snort, Suricata, Squid e pfBlockerNG, transformando-o em uma solução escalável para redes corporativas, provedores e laboratórios (29). O pfSense é amplamente adotado por combinar desempenho, segurança e baixo custo operacional.

2.8.7 Snort / Suricata

Snort e Suricata são IDS/IPS amplamente utilizados em segurança de redes, ambos capazes de detectar ataques e tráfego malicioso por meio de regras e inspeção profunda de pacotes. Snort, mantido pela Cisco, destaca-se por sua vasta base de assinaturas e longa maturidade na indústria (30). Suricata, desenvolvido pela Open Information Security Foundation (OISF), oferece arquitetura multicore, decodificadores avançados (HTTP, TLS, DNS) e saída EVE JSON para integração com SIEMs, sendo considerado uma evolução moderna para ambientes de alto desempenho (31). Essas ferramentas são fundamentais em SOCs, firewalls e sistemas de detecção de intrusão corporativos.

2.8.8 Wireshark

O Wireshark é a principal ferramenta de análise de pacotes da área de redes, permitindo capturar, decodificar e inspecionar protocolos em profundidade. Ele é amplamente utilizado para troubleshooting, investigação forense, testes de segurança e validação de configurações, oferecendo suporte a centenas de protocolos e filtros avançados (32). Sua interface intuitiva e precisão tornam o Wireshark indispensável para analistas de SOC, engenheiros de rede e profissionais de cibersegurança que necessitam compreender o comportamento real do tráfego em ambientes corporativos.

2.9 TRABALHOS CORRELATOS

Para Asalqour et al. (33), a implementação de um modelo bem definido de defesa em profundidade (Defense in Depth) tem potencial para funcionar como forte estratégia de segurança, uma vez que diferentes controles de segurança são implementados em série para impedir que técnicas complexas e variadas obtenham êxito contra todas as camadas. A proposta deste trabalho busca reunir controles com foco em prevenir, detectar e mitigar os ataques estudados e suas variações, com base nessa abordagem de segu-

rança. Um dos controles candidatos a constar na proposta, por exemplo, são os sistemas de prevenção e detecção de intrusão. Thapa e Mailewa (34) apresentam uma revisão abrangente sobre a história e os conceitos dos sistemas de prevenção (IPS) e detecção de intrusão (IDS), como suas funções e componentes, além de elencarem as ferramentas mais utilizadas. Os sistemas de detecção de intrusão (IDS) têm evoluído significativamente nos últimos anos, inclusive, sendo integrados a soluções de inteligência artificial.

Bandeira et al. (35) propõe um modelo para identificar dispositivos IoT espúrios conectados fisicamente à rede, utilizando fingerprints de sistemas operacionais como principal mecanismo de detecção. A pesquisa demonstra que a combinação de técnicas passivas e ativas permite reconhecer equipamentos não autorizados em ambientes sem NAC, validando a abordagem por meio de experimentos em laboratório e análises de cenários reais.

Khraisat et al. (36) forneceram uma revisão abrangente das abordagens contemporâneas de detecção de intrusão, destacando técnicas de evasão utilizadas por atacantes. Em relação a segurança de redes internas, o protocolo IEEE 802.1x desempenha papel fundamental, em que ele é utilizado para realizar controle de acesso à rede, provendo um mecanismo de autenticação para permitir ou negar a conexão de dispositivos legítimos a rede corporativa (37). Apesar de largamente utilizado em sua versão mais básica, o protocolo 802.1x é altamente vulnerável a formas de contorno, conforme Vishnu e Praveen (38).

Kang et al. (39) destacam que, no contexto de Zero Trust, a ameaça interna envolve indivíduos com acesso privilegiado que podem, de forma intencional ou acidental, causar mau uso desses privilégios, resultando em alterações observáveis nos sistemas; assim, a detecção deve considerar três dimensões: o próprio insider, seus comportamentos operacionais e os efeitos gerados no sistema.

Jahangeer et al. (40) apontam que, em redes IoT, é comum o uso de sistemas de detecção distribuídos, em que cada nó monitora vizinhos para identificar atividades suspeitas. De forma análoga, em redes locais vulneráveis à inserção de dispositivos compactos, pode-se aplicar agentes leves de monitoramento, como o Zabbix Agent, para coletar métricas de tráfego e recursos, permitindo identificar sinais precoces de comprometimento.

Parte desta pesquisa trata deste protocolo e suas atualizações, conforme o trabalho de Ryan (41). Esses trabalhos fornecem uma visão abrangente sobre alguns controles fundamentais para o problema em questão. Contudo, para alcançar a qualidade apropriada para o modelo proposto, este trabalho também revisita outras obras, para propor controles fundamentais e otimizados.

O trabalho de La (42) trata da importância em priorizar controles de segurança, considerando a impossibilidade de implementar todos eles, utilizando como critério a probabilidade de ocorrência e as técnicas utilizadas num ataque. Neste sentido, este trabalho aborda diversos conceitos e controles de segurança, com vistas a propor um modelo baseado em defesa em profundidade para o problema apresentado. Apesar de encontrar diversos trabalhos sobre tecnologias, conceitos ou controles de segurança específicos e até sobre a importância de priorização de controles de segurança, esta pesquisa se diferencia de outras correlatas, pois, visa desenvolver um modelo de controles prioritários para um problema específico, cujos impactos afetam organizações de todas as naturezas e portes ao redor do mundo.

Hevner (43) contribui para o entendimento da metodologia Design Science Research, ao estabelecer diretrizes claras para a criação e avaliação de artefatos destinados a resolver problemas reais de forma

inovadora. Na dissertação, a DSR é utilizada como base metodológica para estruturar todo o processo de investigação sobre intrusões físicas com dispositivos compactos, guiando as etapas de identificação do problema, construção do modelo de defesa em profundidade, demonstração dos controles e avaliação de sua eficácia. Diferenciando-se da ciência comportamental por seu foco na utilidade prática, a DSR permite ciclos iterativos de refinamento em que compreensão e solução evoluem simultaneamente. O trabalho destaca ainda que a abordagem é especialmente adequada para desafios complexos e pouco estruturados, como os ataques que utilizam dispositivos compactos para intrusão, para os quais não existem soluções diretas e consolidadas. Assim, as diretrizes de Hevner garantem rigor, relevância e inovação na priorização dos controles propostos.

O trabalho de David Hunt (44) apresenta um guia prático para a construção de uma "attack box" descartável utilizando um Raspberry Pi, descrevendo desde a configuração do hardware e da imagem de sistema até a implantação de ferramentas de intrusão de redes corporativas. Com foco em cenários realistas de infiltração física, o autor demonstra como dispositivos compactos podem ser usados para ponte, clonagem de endereços MAC, interceptação de tráfego e estabelecimento de persistência.

O framework MITRE ATT&CK destaca-se como uma base de conhecimento amplamente utilizada para compreender o comportamento de adversários cibernéticos, estruturando de forma sistemática as táticas, técnicas e procedimentos (TTPs) empregados em diferentes fases de um ataque. Entre seus pontos-chave estão a categorização detalhada de vetores de ataque, o mapeamento de técnicas a grupos de ameaças persistentes avançadas (APTs) e a possibilidade de relacionar controles de segurança às ações adversárias que buscam mitigar. Dessa forma, o ATT&CK não apenas facilita o entendimento sobre como ameaças reais se manifestam, mas também apoia a análise de lacunas defensivas, a priorização de controles e o fortalecimento de estratégias de defesa em profundidade, tornando-se uma ferramenta essencial para o entendimento de cenários de ameaças em segurança cibernética (45).

Adicionalmente, o CIS Controls V8 se destaca pela objetividade e clareza, oferecendo controles em linguagem simples, acompanhados de exemplos práticos de implementação, o que o torna especialmente útil para equipes que não possuem maturidade avançada em cibersegurança. Uma de suas características únicas é a divisão em três grupos de implementação (IG1, IG2 e IG3), que permitem adaptar os controles ao nível de complexidade e recursos disponíveis da organização. No contexto deste trabalho, o CIS Controls foi consultado como opção para controles que formassem esta proposta, contudo, não serviu de base para controles, uma vez que a ameaça estudada é específica e demanda controles mais ajustados ao cenário identificado. O CIS Controls é composto de contramedidas como, por exemplo, inventário de ativos, controle de acesso e monitoramento contínuo, que são pontos críticos para mitigar ataques físicos e lógicos realizados por equipamentos pequenos e de fácil inserção em redes locais. (13).

Abaixo, seguem os principais pontos destes trabalhos, de forma consolidada em uma tabela, para melhor entendimento. Na última linha da tabela, seguem informações sobre a proposta deste trabalho, para fins de comparação.

Trabalhos Correlatos - Tabela Comparativa			
Autor/Ano	**Proposta**	**Limitações**	**Relevância**
Alsaqour et al. (2021)	Revisão de Defesa em profundidade e conceitos relacionados	Trabalho com foco no conceito formal, não abrange casos materiais	Base de conhecimento sobre conceitos fundamentais acerca do tema
Thapa & Mailewa (2020)	Revisão de conceitos IDS/IPS	Revisão de literatura sobre IDS/IPS em redes tradicionais	Demonstrar o funcionamento de IDS/IPS e seus componentes
Bandeira et al. (2024)	Detectar dispositivos IoT espúrios em redes sem NAC usando fingerprints de sistemas operacionais.	O modelo depende da precisão das fingerprints e pode falhar contra dispositivos mais sofisticados.	Oferece uma solução prática para identificar intrusões físicas em redes legadas.
Khraisat et al. (2019)	Revisão de técnicas e datasets existentes de IDS	Sem validação prática em cenários reais ou emergentes	Evidenciar que IDS tradicionais podem falhar em detectar ataques com dispositivos compactos.
Ryan (2018)	Estudar vulnerabilidades do protocolo MACsec em redes locais	Foco em métodos específicos fracos (EAP-MD5)	Evidenciar que mesmo MACsec pode ser explorado por dispositivos compactos em redes locais.
Vishnu & Praveen (2020)	Demonstrar ataques para burlar o 802.1X/NAC usando Raspberry Pi e scripts modificados	Restringe-se a explorar vulnerabilidades do 802.1X em redes cabeadas com acesso físico a dispositivo legítimo	Mostra como dispositivos compactos podem efetivamente burlar controles de rede, reforçando a importância de controles adicionais e defesa em profundidade
Kang et al. (2023)	Revisar teoria e aplicações do Zero Trust	Baseado em literatura, pouca validação prática	Fundamenta princípios de Zero Trust que servem para validar a presença de dispositivos compactos na rede
Jahangeer et al. (2023)	Revisar segurança da camada de rede em IoT, com foco em ataques ao Protocolo de roteamento RPL	Restringe-se a ataques internos no RPL e análise de técnicas, sobretudo com machine learning	Mostra fragilidades exploráveis por dispositivos compactos e sugere ML como reforço de controles
La (2023)	Priorizar controles usando NIST 800-53 com mapeamento no MITRE ATT&CK	Foco em domínio Enterprise, com mapeamentos binários, sem medir graus complexos	Apoia escolha de controles mais eficazes para dispositivos compactos
Proposta deste trabalho (2025)	Priorizar controles utilizando NIST 800-53 como base de controles	Foco em priorizar controles de segurança para prevenção, detecção, mitigação e resposta a ataques que utilizam dispositivos compactos	Preencher lacuna de conhecimento, através da criação de artefato, para resolução de problema de segurança com alto grau de impacto

Tabela 2.1: Trabalhos Correlatos Avaliados

2.10 LACUNA CIENTÍFÍCA

Apesar das contribuições significativas dos trabalhos analisados — como o detalhamento de técnicas adversárias pelo MITRE ATT&CK, o conjunto de controles pelo CIS Controls v8, os estudos de vulnerabilidades em 802.1X/NAC, priorização de controles de segurança e as propostas de mitigação em IoT e camadas de rede, por exemplo —, observa-se uma lacuna científica relevante: nenhum deles se dedica especificamente à compreensão e definição de um conjunto estruturado de controles voltados para ataques realizados por dispositivos compactos em redes cabeadas. Esse tipo de ameaça, recorrente e de alto impacto, permanece subexplorado no meio acadêmico, ainda que represente um vetor prático e viável de intrusão em ambientes corporativos. Portanto, percebe-se a necessidade de pesquisas que sistematizem controles direcionados a esse cenário, permitindo não apenas o fortalecimento da defesa em profundidade,

mas também a criação de diretrizes aplicáveis a diferentes contextos organizacionais.

3 METODOLOGIA

Este trabalho utiliza como metodologia principal a Design Science Research (DSR), que é amplamente utilizada em pesquisas de sistemas de informação e engenharias e tem o objetivo de criar e avaliar iterativamente artefatos que resolvam problemas práticos enquanto contribuem para o conhecimento científico (43). Além da aderência às diretrizes que norteiam a DSR, este trabalho é desenvolvido com base no ciclo regulador de Wieringa (46), que é uma forma iterativa de estruturar as fases da pesquisa pautada nesse método, conforme a figura 3.1.

Figura 3.1: Ciclo Regulador de Wieringa (Adaptado)

Fonte: do Autor

Wieringa define o ciclo regulador para criação e avaliação de artefatos como um processo cíclico e contínuo, em que as fases se repetem até que uma solução satisfatória seja desenvolvida e validada. O ciclo adotado neste trabalho é uma versão adaptada desse modelo, estruturada em três fases principais:

1. Investigação do Problema: O ciclo começa com a definição e descrição clara do problema prático a ser enfrentado. Nessa fase, é fundamental que haja um entendimento profundo do problema enfrentado, pois, a qualidade dessa investigação reflete na estratégia desenvolvida para o tratamento das fragilidades. Essa etapa busca compreender, com profundidade, o contexto e os fatores que originam a necessidade de intervenção. Nesta etapa, para investigação e entendimento do cenário, o ataque é graficamente representado por uma Attack-tree, utilizando técnicas de modelagem de ameaça. Além disso, o ataque é discutido em detalhes, conforme a literatura disponível sobre o assunto.

2. Projeto da Solução: Com os requisitos definidos, o próximo passo é projetar o desenho da solução ou artefato. Essa fase envolve a construção de um artefato que resolva o problema identificado. Neste estudo, com base nas diretrizes da NIST SP 800-53, foram revisados e selecionados, de forma cíclica e reiterada, os controles de segurança capazes de mitigar, detectar ou prevenir diretamente o problema identificado.

3. Implementação e Avaliação: Nesta fase do ciclo são apresentadas as Provas de Conceito (PoC) produzidas em laboratório e analisados os resultados obtidos a partir da implementação dos controles em um cenário real. Para isso, utilizou-se o método prático para implementação dos controles em ambiente de laboratório. A fase de implementação em cenário real e simulado e avaliação de resultados foi destacada para os capítulos 4 e 5, em que foram construídas provas de conceito de alguns controles em laboratório e, em seguida, foram expostos e discutidos outros controles implementados em um cenário real.

3.0.1 Diretrizes do Design Science Research

No contexto da DSR, artefatos podem ser construtos, modelos ou métodos. Esses artefatos têm o principal objetivo de resolver problemas específicos sem soluções até então. Segundo Hevner(43), a pesquisa baseada em DSR deve seguir sete diretrizes ou pilares para ser considerada efetiva. A tabela 3.1 resume as sete diretrizes da DSR:

Diretrizes de Pesquisa em Design Science	
Diretriz	**Descrição da Diretriz**
Diretriz 1: Design como um Artefato	A pesquisa em design science deve produzir um artefato viável na forma de um construto, um modelo, um método ou uma instanciação.
Diretriz 2: Relevância do Problema	O objetivo da pesquisa em design science é desenvolver soluções baseadas em tecnologia para importantes e relevantes problemas de negócios.
Diretriz 3: Avaliação de Design	A utilidade, qualidade e eficácia de um artefato de design devem ser rigorosamente demonstradas através de uma avaliação bem executada.
Diretriz 4: Contribuições de Pesquisa	A pesquisa eficaz em design science deve fornecer informações claras e contribuições verificáveis nas áreas do artefato de design, fundamentos de design e/ou metodologias de design.
Diretriz 5: Rigor da Pesquisa	A pesquisa em design science depende da aplicação de métodos rigorosos tanto na construção quanto na avaliação do artefato de design.
Diretriz 6: Design como um processo de pesquisa	A busca por um artefato eficaz requer a utilização de recursos disponíveis para alcançar os fins desejados e, ao mesmo tempo, satisfazer as leis do ambiente problemático.
Diretriz 7: Comunicação de Pesquisa	A pesquisa em design science deve ser apresentada de forma eficaz tanto orientada para a tecnologia quanto como orientada para a audiência.

Tabela 3.1: Diretrizes para Design Science

Nesse sentido, as fases de (1) investigação problema, (2) projeto da solução e (3) implementação e avaliação são desenvolvidas com aderência às diretrizes da DSR.

3.1 INVESTIGAÇÃO DO PROBLEMA - MODELAGEM DA AMEAÇA COM ATTACK-TREE

Bruce Schneier(47) deu origem ao modelo Attack-Tree (Árvore de Ataque) partindo do pressuposto de que uma violação de segurança nada mais é do que uma sequência de eventos que, de forma combinada, levam ao objetivo principal, o ataque. Attack-Tree é um diagrama com múltiplos níveis que consistem em uma raiz (objetivo principal) e folhas (ataques). Uma árvore de ataque representa os ataques que precisam ocorrer para que o principal objetivo seja atingido (47) e seu objetivo principal é mapear as possíveis causas raízes do risco considerado. Ainda segundo Schneier, na figura 3.2 temos a estrutura básica de uma Attack-Tree:

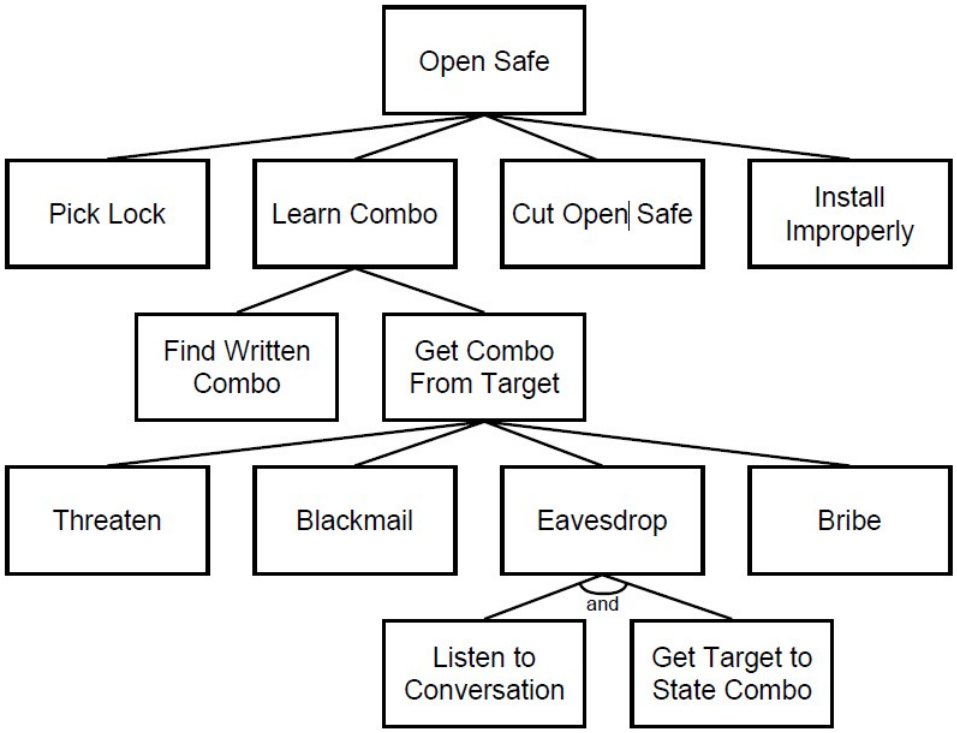

Figura 3.2: Estrutura Básica de uma Attack-Tree (Schneier).

Fonte: do Autor

Existem muitas notações diferentes para árvores de ataque. De forma geral, essas notações podem expressar operadores lógicos “E” e “OU”. Com o auxílio de legendas, é possível representar ataques como possíveis ou impossíveis, fáceis ou não, caros ou não, intrusivos ou não, legais ou ilegais e se precisam de equipamentos especiais ou não, por exemplo (47). Em suma, utilizando essa metodologia para modelagem de ameaças é possível descrever, com riqueza de detalhes, os mais variados tipos de ataques. A utilização de árvores de ataque auxilia na identificação e no entendimento de ameaças, pois representam cenários

complexos através de diagramas gráficos mais simples, conforme Schneier. Portanto, ameaças descritas como árvores de ataque fornecem uma abordagem mais rigorosa e análise do problema com foco em engenharia (48). Após entender o modo de atuação dos atacantes, a técnica será modelada, conforme a metodologia árvore de ataque.

3.1.1 Como o Ataque Ocorre

O principal objetivo dos atacantes é conectar e ocultar um dispositivo compacto na rede interna da organização-alvo, criando uma ponte para que o atacante possa acessar remotamente a infraestrutura interna. O dispositivo pode ser um roteador compacto, como o Mikrotik HAP Mini 3.4 ou um minicomputador como o Raspberry Pi 3.3, que é ainda mais versátil e barato.

Figura 3.3: Raspberry Pi 4

Fonte: Cytron (49)

Figura 3.4: Mikrotik HAP Mini

Fonte: Mikrotik (50)

A conexão do atacante com o dispositivo pode ser realizada de formas variadas como conexão reversa ou acesso direto por 3G/4G/5G, configurado no dispositivo espúrio. Scott Eggimann, demonstra como

preparar o dispositivo, por exemplo, instalando ferramentas e realizando a configuração da conexão reversa (reverse shell), que utiliza SSH (Secure Shell), um protocolo de acesso remoto criptografado, nativo de sistemas Unix/Linux (51). O autor do artigo traz reflexões sobre a grande quantidade de pontos de rede expostos a atacantes. Já David Hunt, demonstra a possibilidade de utilização de servidores de comando e controle (C2) para controle remoto do dispositivo, além da utilização de outras ferramentas utilizadas para exploração de máquinas da rede do alvo, como Nmap, Metasploit e BurpSuite (44).

Em pesquisa na matriz de informações do MITRE ATT&CK, foi possível identificar a ocorrência de um grupo chamado "Dark Vishnya", número de identificação G0105, classificado como APT (Advanced Persistent Threat)(52). Segundo o NIST SP 800-30, APT ou Ameaça Persistente Avançada são adversários com níveis sofisticados de conhecimento e recursos significativos, geralmente patrocinados por governos (53). O grupo em questão é descrito pelo MITRE como um ator de ameaça com motivação monetária que visa instituições financeiras na Europa Oriental. Segundo a Kaspersky, em 2017 e 2018 o grupo atacou pelo menos 8 bancos naquela região da Europa. Entre as técnicas utilizadas pelo grupo, a mais notável é a inserção de dispositivos como Raspberry Pi, Bash Bunny, netbooks ou outros tipos de laptops baratos (1). O Bash Bunny é um dispositivo USB que simula um equipamento USB legítimo, mas que na verdade executa scripts maliciosos nos computadores alvo do ataque cibernético.

Ainda segundo a Kaspersky, os ataques se iniciavam com o (1) criminoso acessando o ambiente físico dos alvos, se fazendo passar por um visitante ou prestador de serviço; em seguida, (2) o dispositivo era inserido e ocultado em algum ponto da rede corporativa (Os pontos de rede, quase sempre, estão expostos em vários lugares dos escritórios corporativos como corredores e salas de reunião, onde visitantes, clientes e parceiros são permitidos); após a inserção do dispositivo, (3) O atacante realizava acesso remoto à rede corporativa por meio de uma conexão celular 3G/4G/5G, previamente configurada no dispositivo espúrio. Utilizando o dispositivo conectado à rede como estação de salto, o atacante realizava movimentação lateral em direção a hosts legítimos e para conseguir escalar privilégios e persistir o acesso em outros pontos da rede. Os objetivos desses ataques eram, principalmente, espionagem, roubo de credenciais e execução de outros ataques e fraudes. No Brasil, alguns ataques registrados repetiram essas formas de atuação e tinham objetivos similares (35). Neste trabalho, o estudo do ataque tem como foco aquelas ações realizadas com dispositivos Raspberry Pi e que utilizam conexões reversas ou conexões diretas via 3G/4G/5G como forma de comunicação com o atacante.

A figura 3.5 de um caso real, identificado em uma instituição financeira brasileira, confirmam que a forma de atuação do grupo Dark Vishnya foi replicada para outros locais do mundo e que a utilização de dispositivos compactos ainda é realizada e a estratégia de ocultação também se repete. No caso da imagem, um dispositivo Mikrotik HAP Mini foi conectado à rede interna do alvo e ocultado abaixo do piso elevado.

Figura 3.5: Dispositivo encontrado abaixo do piso elevado

Fonte: do Autor

No trabalho desenvolvido e apresentado por Daniel Ryan(41), na DEF CON 26, em 2018, foram demonstrados alguns cenários capazes de contornar o protocolo IEEE 802.1AE (MACsec), quando utilizando métodos criptográficos “fracos”, como EAP-MD5. Basicamente, o MACsec atua em conjunto com o protocolo IEEE 802.1x e criptografa o tráfego em nível de camada de enlace de dados (37). Além disso, Daniel apresenta um histórico da evolução desse tipo de ataque, em que, por exemplo, Steve Riley demonstrou, em 2005, que era possível explorar o controle de acesso à rede (802.1x- 2004), apenas colocando um Hub entre um dispositivo autorizado e o switch. Em seguida, Daniel traz a informação de que um pesquisador chamado “Abb” publicou uma ferramenta denominada Marvin, que era capaz de fazer a mesma exploração, mas ligando o dispositivo como bridge, ou seja, diretamente entre o switch e o dispositivo autorizado, mas sem a necessidade de um Hub(41). Sem a presença de um Controle de Acesso à Rede (NAC – Network Access Control), é possível realizar a ligação do dispositivo diretamente a rede interna. Abaixo, a figura 3.6 ilustra de que formas esses dispositivos podem ser inseridos na rede do alvo:

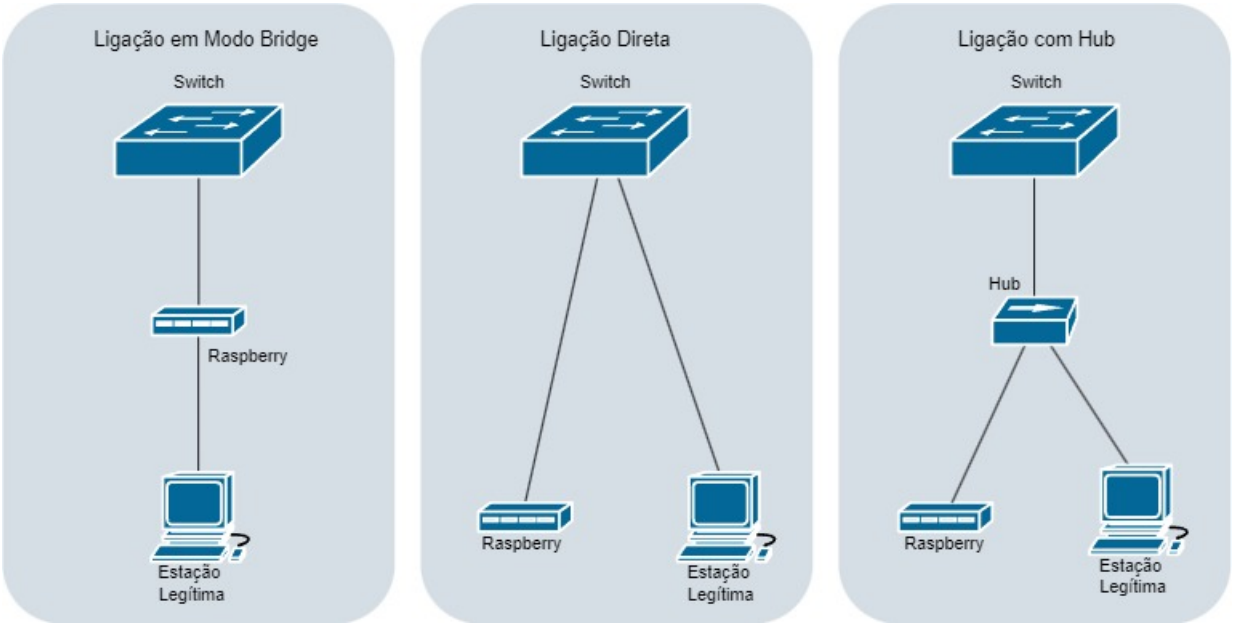

Figura 3.6: Formas de inserção do dispositivo

Fonte: do Autor

1. Na ligação em modo bridge, o dispositivo invasor possui duas interfaces de rede, uma conectada a uma estação legítima da rede interna e outra conectada ao ponto de rede, dessa forma, todo o tráfego passa pelo equipamento e pode ser coletado e, teoricamente, lido.

2. Em ligação direta, vale ressaltar que para esse cenário não costuma haver qualquer solução de controle de acesso à rede (NAC), pois qualquer NAC poderia identificar o dispositivo e bloquear o ponto de acesso.

3. No último caso, em ligação com o Hub, o ataque é mais sofisticado, pois a estação legítima faz a autenticação ante o NAC e, em seguida, o dispositivo utiliza o ponto já autorizado a funcionar para realizar comunicação com a rede do alvo. Nesse caso, o ataque ainda pode ser mais difícil de detectar, caso o Raspberry realize clonagem de endereço físico (MAC Address) e e IP da estação legítima, pois, do ponto de vista do switch e ferramentas de monitoração, só um host pode ser identificado naquele segmento.

Neste trabalho, o dispositivo invasor foi generalizado como sendo o Raspberry Pi, por ser compacto e versátil, permitindo a instalação de uma distribuição Linux completa e a utilização de diversas ferramentas para exploração. Na figura 3.7, temos a visão geral do ataque e como a conexão remota é realizada, utilizando uma conexão reversa pela própria rede do alvo ou via 3G/4G/5G, passando pela Internet.

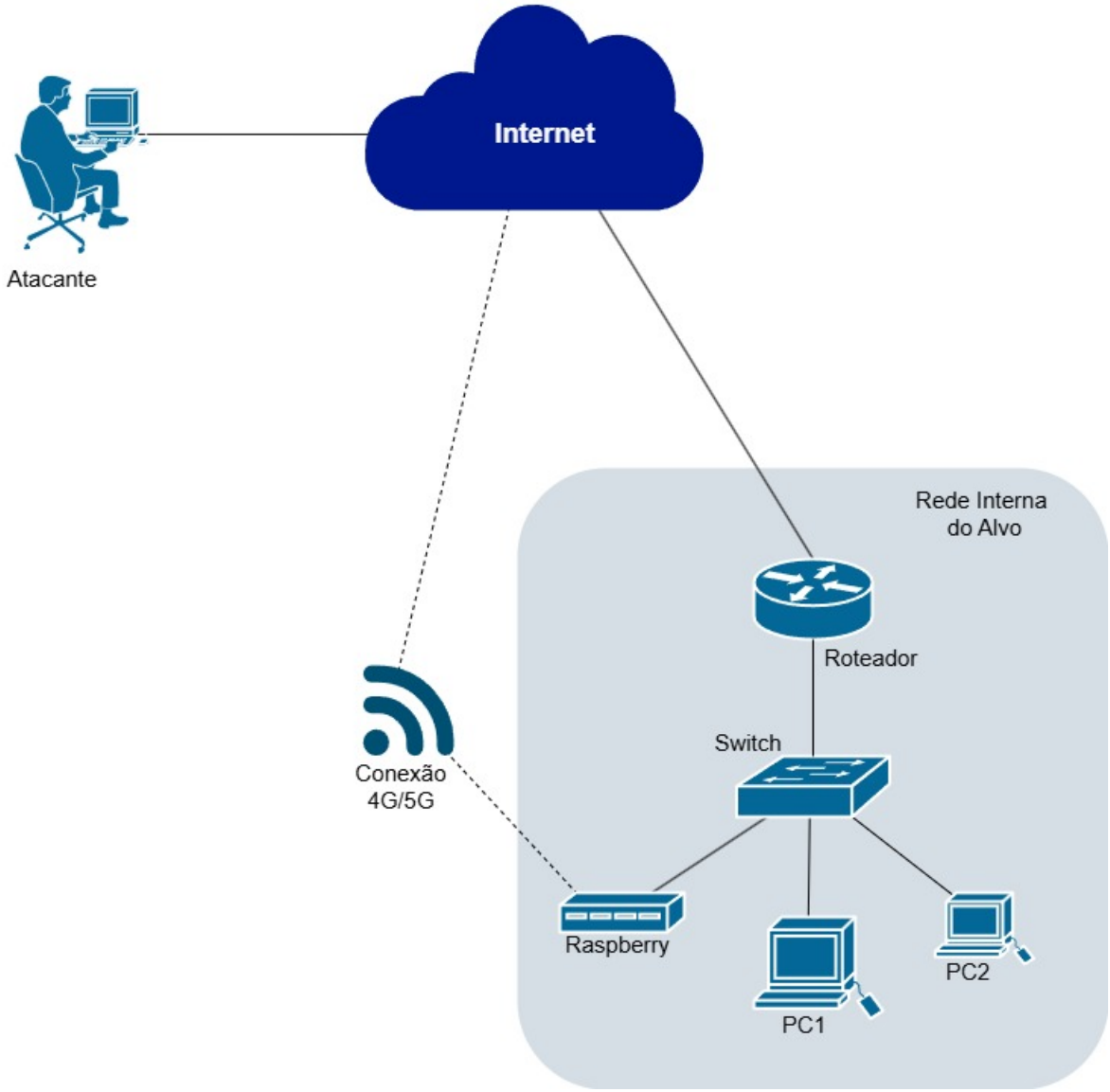

Figura 3.7: Visão Geral do Ataque

Fonte: do Autor

Assim, após reunir as informações disponíveis sobre as variações dessa técnica, foi possível criar uma árvore de ataque com condições-chave para que um ataque dessa natureza ocorra, conforme a figura 3.8.

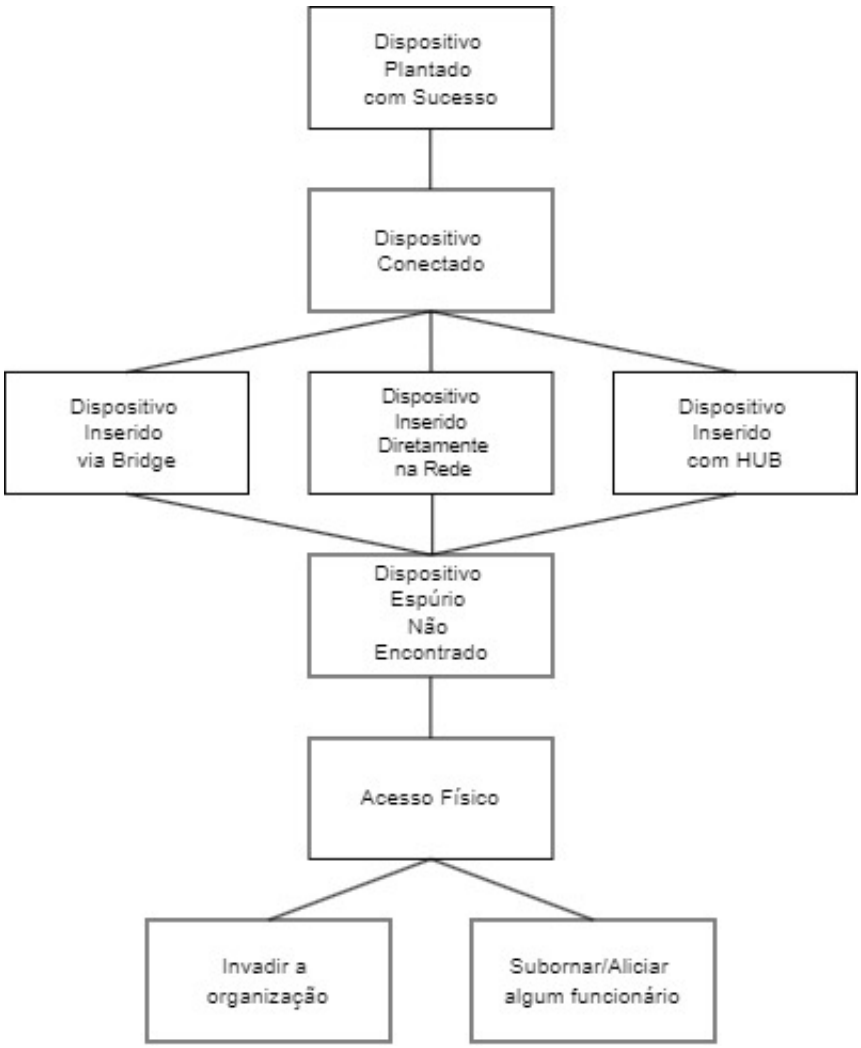

Figura 3.8: Árvore do Ataque

Fonte: do Autor

3.2 PROJETO DA SOLUÇÃO - SELEÇÃO PRELIMINAR DE CONTROLES

Para o desenvolvimento da proposta, inicialmente, foram definidos quais frameworks de controles de segurança poderiam ser utilizados como base de conhecimento. Assim, foram consultados e avaliados os modelos CYBOK 1.1.0, definido como um conjunto abrangente de conhecimentos para informar e apoiar a educação e a formação profissional para o setor da segurança cibernética (12) e; CIS Controls V8, que é um conjunto priorizado de salvaguardas para mitigar os ataques cibernéticos mais prevalentes contra sistemas e redes (13). Como opção, também foi avaliada a publicação especial NIST SP 800-53, revisão 5 que, para o objetivo deste trabalho, se mostrou superior, no sentido de abranger os controles anteriormente levantados no CIS Controls e CYBOK, além de oferecer controles adicionais. Em termos comparativos, os CIS Controls v8 reúnem 153 salvaguardas, organizadas em 18 grupos (CIS, 2021), enquanto a NIST SP 800-53 apresenta mais de 1.000 salvaguardas, abrangendo uma gama muito mais ampla de domínios. Sendo assim, o NIST SP 800-53 foi a escolha primária de fonte de controles para compor esta proposta.

A seguir, todo o framework foi avaliado, em busca de controles que pudessem detectar, prevenir ou mitigar diretamente quaisquer das ações descritas no ataque, na seção 3.1.1, “Como o Ataque Ocorre”. Assim, esses controles foram avaliados, conforme a própria explicação do modelo, presente na seção “Discussão” de cada medida da SP 800-53, conforme aquele documento. O tópico de discussão na SP 800-53 traz reflexões sobre como, onde e quando os controles se aplicam, além de discutir sobre o objetivo de cada controle. Adicionalmente, foram consultadas fontes diversas sobre a implementação de cada medida, com objetivo de obter pleno entendimento de cada uma delas.

No sentido de conferir variedade na natureza dos controles, foram relacionados não só controles puramente técnicos, mas também de tipos administrativo e operacional. A necessidade de variedade de tipos de controles, se deve ao objetivo desta proposta em definir um modelo de controles prioritários para o problema específico, baseado no conceito de segurança em camadas ou defesa em profundidade. Dessa maneira, os controles devem compor uma abordagem multicamada e serem distintos entre si, focando em proteção de dados, aplicações, dispositivos, rede e perímetro (33). Assim, se chegou à relação de controles da fase seguinte do trabalho.

3.2.1 Definição dos Controles

Com base nos critérios discutidos na fase de projeto, foram selecionados 47 controles ou aprimoramentos. O foco para a escolha desses controles foi a capacidade de detectar, prevenir ou mitigar diretamente alguma das técnicas empregadas para consecução do ataque. Esses controles foram organizados, conforme a tabela 3.2:

ID NIST SP 800-53	**Descrição do Controle**
AC-2 (g)	Monitorar o uso das contas.
AC-17 [1]	Empregar mecanismos automatizados para monitorar e controlar métodos de acesso remoto.
AT-2 (b)	Empregue técnicas para aumentar a conscientização sobre segurança e privacidade dos usuários.
AT-2 (d)	Incorporar em treinamentos as lições aprendidas com incidentes ou violações de segurança internas ou externas.
AT-2 [2]	Fornecer formação sobre como reconhecer e reportar potenciais indicadores de ameaça interna.
AT-2 [5]	Fornecer formação sobre a ameaça persistente avançada.
CA-7 (e)	Correlação e análise de informações geradas por avaliações de controle e monitoramento.
CA-8 [1]	Empregar um agente ou equipe de teste de penetração independente para realizar testes de penetração no ambiente.
CA-8 [2]	Empregar exercícios de redteam para simular tentativas de adversários de comprometer os sistemas e ambientes organizacionais.
CA-8 [3]	Empregar um processo de teste de penetração que inclua tentativas de contornar os controles associados aos pontos de acesso físico à instalação.

ID NIST SP 800-53	Descrição do Controle
CA-9 (a)	Autorizar conexões internas ao ambiente apenas de componentes definidos pela organização.
CM-7 (b)	Proibir ou restringir/desabilitar o uso de funções, portas, protocolos, software e/ou serviços restritos.
CM-7 [9] (b)	Proibir o uso ou conexão de componentes de hardware não autorizados.
CM-8 (a)	Desenvolver e documentar um inventário de componentes do sistema que reflita com precisão o ambiente.
IA-2 [1]	Implementar autenticação multifator para acesso a contas privilegiadas.
IA-2 [2]	Implementar autenticação multifator para acesso a contas não privilegiadas.
IA-3	Identificar e autenticar dispositivos definidos pela organização antes de estabelecer uma conexão de rede.
IA-3 [1]	Identificar e autenticar dispositivos | Autenticação de rede Bidirecional.
IA-5 [1] (b)	Verificar, quando os usuários criam ou atualizam senhas, se as senhas não são encontradas na lista de senhas comumente usadas, esperadas ou comprometidas em bases de senhas vazadas.
IA-5 [1] (c)	Transmitir senhas somente através de canais protegidos com criptografia.
IA-5 [1] (d)	Armazenar senhas usando uma função aprovada de derivação de chave com sal, de preferência usando um hash codificado.
IR-2 [3]	Fornecer treinamento de resposta a incidentes sobre como identificar e responder a uma violação, incluindo o processo da organização para relatar uma violação.
IR-4 (a)	Implementar capacidade de tratamento de incidentes que seja consistente com o plano de resposta a incidentes e inclua preparação, detecção e análise, contenção, erradicação e recuperação.
IR-4 [5]	Implemente um recurso para desabilitar automaticamente um recurso caso violações de segurança sejam detectadas.
IR-6 (a)	Requisitar que o pessoal relate suspeitas de incidentes à resposta organizacional a incidentes.
IR-9 (d)	Isolar o sistema ou componente do sistema comprometido.
MA-5 (a)	Estabelecer um processo para autorização do pessoal de manutenção e manter uma lista de organizações ou pessoal de manutenção autorizado.
MA-5 (b)	Verifique se o pessoal não escoltado que realiza manutenção no sistema possui as autorizações de acesso necessárias.
MA-5 (c)	Designar pessoal organizacional com autorizações de acesso exigidas e competência técnica para supervisionar as atividades de manutenção de pessoal que não possua as autorizações de acesso exigidas.
PE-2 (a)	Desenvolver, aprovar e manter uma lista de indivíduos com acesso autorizado às instalações onde o sistema reside.
PE-2 (b)	Emitir credenciais de autorização para acesso às instalações.

ID NIST SP 800-53	Descrição do Controle
PE-3 (d)	Acompanhar visitantes e controlar suas atividades que exigem escolta e controle.
PE-3 [3]	Empregar guardas para controlar os pontos de acesso físico às instalações onde o sistema reside, 24 horas por dia, 7 dias por semana.
PE-3 [8]	Utilize vestíbulos de controle de acesso em locais dentro das instalações.
PE-6 (a)	Monitorar o acesso físico ao ambiente para detectar e responder a incidentes de segurança física.
PE-6 [1]	Utilizar alarmes de intrusão e equipamentos de vigilância.
RA-10 (a)	Estabelecer e manter um programa de threat hunting para procurar indicadores de comprometimento (IoC) nos sistemas organizacionais e Detectar, rastrear e interromper ameaças que escapam aos controles existentes.
SA-8 [18]	Implementar o princípio de segurança por design em canais de comunicação confiáveis do ambiente organizacional.
SC-7 [20]	Fornecer a capacidade de isolar dinamicamente o ambiente de outros componentes do sistema.
SC-8 [1]	Implementar mecanismos criptográficos para impedir a divulgação não autorizada de informações.
SC-26	Incluir componentes nos sistemas organizacionais projetados especificamente para serem alvo de ataques maliciosos para detectar, desviar e analisar tais ataques.
SI-4 (a) [1]	Monitore o sistema para detectar ataques e indicadores de ataques potenciais de acordo com os seguintes objetivos de monitoramento.
SI-4 (a) [2]	Monitore o sistema para detectar conexões locais e remotas não autorizadas.
SI-4 [1]	Conecte e configure ferramentas de detecção de intrusão
SI-4 [13] (a)	Analisar o tráfego de comunicações e os padrões de eventos do sistema.
SI-4 [13] (b)	Desenvolver perfis que representem padrões comuns de tráfego e eventos.
SI-4 [13] (c)	Usar os perfis de tráfego e eventos no ajuste dos dispositivos de monitoramento do sistema.

Tabela 3.2: Proposta de Controles de Segurança

3.2.2 Critérios de Priorização de Controles para Cada Cenário

A seguir, são elencados os critérios que devem ser levados em consideração para adoção dos controles desta proposta em cada cenário. Organizações diversas encontram-se em diferentes situações e possuem variados níveis de maturidade de segurança cibernética. Dessa forma, sugere-se que a adoção de controles dentro do rol proposto deve ser adequada para cada situação, considerando critérios como:

1. Tamanho e complexidade da infraestrutura organizacional: Empresas maiores, geralmente possuem infraestruturas mais complexas e que demandam controles mais robustos;

2. Exposição e tolerância a riscos cibernéticos: A exposição a riscos específicos é um fator a ser considerado para escolha de controles;

3. Soluções já implementadas: As soluções adotadas devem ser focadas em problemas específicos. Ferramentas redundantes podem conferir risco residual excessivo ao ambiente que se quer proteger;

4. Custo/Orçamento disponível: Deve-se equilibrar custos e eficácia, priorizando controles de menor custo e maior impacto;

5. Quantidade de usuários: Organizações com mais usuários, podem precisar de controles escaláveis, ou seja, que podem se adaptar a demandas maiores;

6. Sensibilidade de dados: Organizações que lidam com dados sensíveis devem priorizar controles de criptografia, prevenção de perda de dados e proteção de endpoints;

7. Capacidade Operacional: A disponibilidade e expertise dos times internos é fator fundamental para escolha de controles a serem adotados;

8. Histórico de incidentes: Análise dos tipos e da frequência de incidentes já ocorridos, pode ser um norteador importante para priorização dos controles de segurança;

9. Tipo de tecnologias adotadas: Organizações que utilizam tecnologias específicas como Internet of Things (IoT), computação em nuvem ou Inteligência artificial (IA) podem precisar de controles especializados;

10. Parcerias e cadeia de suprimento: Controles que avaliem a segurança de fornecedores ou parceiros devem ser considerados.

11. Criticidade dos ativos expostos: A importância relativa dos ativos acessíveis pela rede deve nortear a priorização dos controles, considerando o impacto potencial de sua indisponibilidade, comprometimento ou vazamento.

12. Eficácia comprovada dos controles: A priorização deve considerar controles já validados por meio de testes práticos, auditorias, benchmarks de mercado ou frameworks consolidados, garantindo que a eficácia do controle seja evidenciada em cenários reais ou simulados.

Adicionalmente, deve-se considerar a adoção de outros controles para complementação do modelo de segurança de rede interna. Na seção 4, em que foi realizada prova de conceito da solução em laboratório, apenas uma parte dos controles desta proposta foram implementados para demonstração da eficácia da proposta.

Nas próximas seções, parte desses controles serão demonstrados em ambientes de testes e, posteriormente, sua eficácia será discutida em um caso real, em que parte dos controles foram implementados, considerando-se análise de riscos da empresa, histórico de incidentes e capacidade operacional da organização.

4 PROVA DE CONCEITO (POC) PARCIAL DA SOLUÇÃO

Após a definição dos controles identificados como prioritários para mitigação, prevenção ou detecção dos ataques estudados, foram construídos laboratórios específicos para implementação de alguns controles técnicos, especificamente, aqueles cuja adoção poderia gerar algum impacto operacional num cenário real. Para isso, o objetivo dessa implementação parcial é realizar prova de conceito para demonstração da eficácia de alguns desses controles face às características dos ataques estudados. A seguir, são detalhados os cenários de cada teste, os controles, as ferramentas utilizadas e os resultados obtidos com cada medida. Além disso, com as provas de conceito a seguir, buscou-se responder às hipóteses de pesquisa abaixo:

H1 (AC-2 – Monitorar o uso das contas) O monitoramento contínuo do uso de contas de usuário permite identificar padrões anômalos que indicam comprometimento de credenciais decorrentes da inserção de dispositivos não autorizados?

H2 (AC-17 – Controlar métodos de acesso remoto) O emprego de mecanismos automatizados para monitorar e restringir acessos remotos reduz a probabilidade de que dispositivos compactos se tornem vetores de entrada externa para a rede interna?

H3 (CM-7 – Proibir hardware não autorizado) A aplicação de políticas que bloqueiem conexões de hardware não autorizado é eficaz na prevenção do uso de dispositivos espúrios como pontos de acesso clandestinos?

H4 (CM-8 – Inventário de componentes) A criação e a atualização contínua de inventários de ativos permitem diferenciar rapidamente dispositivos não cadastrados inseridos no ambiente corporativo?

H5 (IA-3 – Autenticação bidirecional de dispositivos) O uso de autenticação bidirecional em nível de enlace, como o MACsec, impede que dispositivos não autorizados se conectem à rede e garante integridade e confidencialidade na comunicação?

H6 (IR-4 – Desabilitação automática) A implementação de mecanismos que desativam automaticamente serviços ou portas quando violações de segurança são detectadas reduz significativamente o tempo de resposta frente a ataques baseados em dispositivos compactos?

H7 (SI-4 – Integração com IDS/IPS) A integração de ferramentas de detecção de intrusão ao ambiente monitorado aumenta a capacidade de detectar tráfego anômalo gerado por dispositivos maliciosos e possibilita ações de resposta em tempo quase real?

4.1 CONTROLES IMPLEMENTADOS EM LABORATÓRIO

Para as provas de conceito a seguir, foram escolhidos alguns controles técnicos presentes nesta proposta, para implementação em ambiente de testes, com o objetivo de demonstrar sua eficácia, complexidade e formas de funcionamento, em relação ao problema identificado e suas particularidades. Essas provas de conceito foram implementadas em laboratórios, utilizando VirtualBox, VMWare Workstation e

GNS3, como soluções de virtualização. Além disso, foram utilizadas imagens diversas de soluções, como switches, SIEM, Firewall, Zabbix, dentre outros. A descrição exata de cada caso é mostrada nas respectivas subseções a seguir.

4.1.1 AC-2 (g) Monitorar o Uso das Contas

Conforme o NIST 800-53, a atividade de monitorar contas de usuários é composta de diversos controles como monitorar o uso de contas, autorizar determinados usuários para cada tipo de recurso, designar contas privilegiadas com base em políticas pré-definidas pela organização, dentre outros. Para casos em que outros controles falhem em prevenir, detectar ou mitigar intrusões em redes internas, a monitoria de contas de usuário pode ser um indicativo eficaz de que alguma conta de usuário foi comprometida e está sendo utilizada de forma indevida. Por exemplo, após uma intrusão bem-sucedida, é altamente provável que ocorra a captura de credenciais de rede, nesse caso, o atacante ao tentar utilizar essas credenciais, pode fornecer pistas sobre a utilização indevida desses dados, como, por exemplo, utilização fora do ambiente de uso comum (outro escritório, VLAN ou estação de trabalho), logins em horários diversos do esperado para determinado usuário, casos de viagem impossível (impossible travel).

A simples monitoria de eventos suspeitos pode fortalecer a capacidade de detecção de uma organização, enquanto a utilização de múltiplo fator de autenticação (MFA) pode incrementar a capacidade de mitigação no uso indevido de credenciais. Nesse sentido, para avaliar a efetividade desse tipo de controle, foi implementado em laboratório (simulado no GNS3 e virtualizado no VirtualBox) um cenário simples de gerenciamento de contas de usuário. Esse laboratório foi construído utilizando um controlador de domínio Windows Server 2022, com Active Directory habilitado, e duas estações de trabalho vinculadas ao domínio, ambas com Windows 10. A seguir, foram criados dois usuários de teste para geração de eventos de segurança. A arquitetura dessa prova de conceito é demonstrada na figura 4.1:

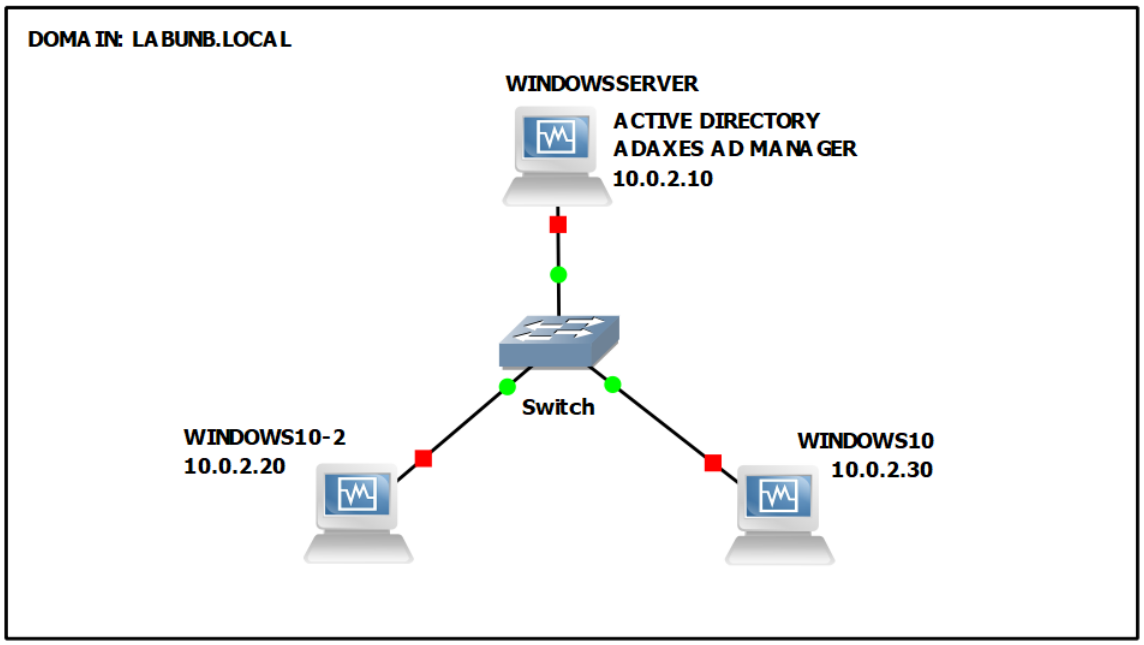

Figura 4.1: Arquitetura do laboratório para Monitoria de Contas de Usuários.

Fonte: do Autor

Após pesquisa por ferramentas que auxiliassem na administração do Active Directory (AD), surgiram opções como Softerra Adaxes ou ManageEngine ADManager. Como o objetivo dessa prova de conceito é demonstrar a eficácia de alguns controles, de forma independente de tecnologias específicas, optou-se pelo uso do Softerra Adaxes, pois a ferramenta oferece uma versão de testes. Assim, após instalação da ferramenta no próprio servidor Windows Server 2022, foi feita a integração da ferramenta com o AD. Dessa forma, foi possível obter dados sobre os dois hosts Windows 10 e os dois usuários de teste, além de seus respectivos dados de eventos relacionados. Na figura 4.2, é possível visualizar a interface da ferramenta Adaxes com a árvore de instâncias e funções do AD, bem como gráficos que facilitam a identificação de métricas anômalas, como contas desabilitadas ou trocas de passwords, por exemplo.

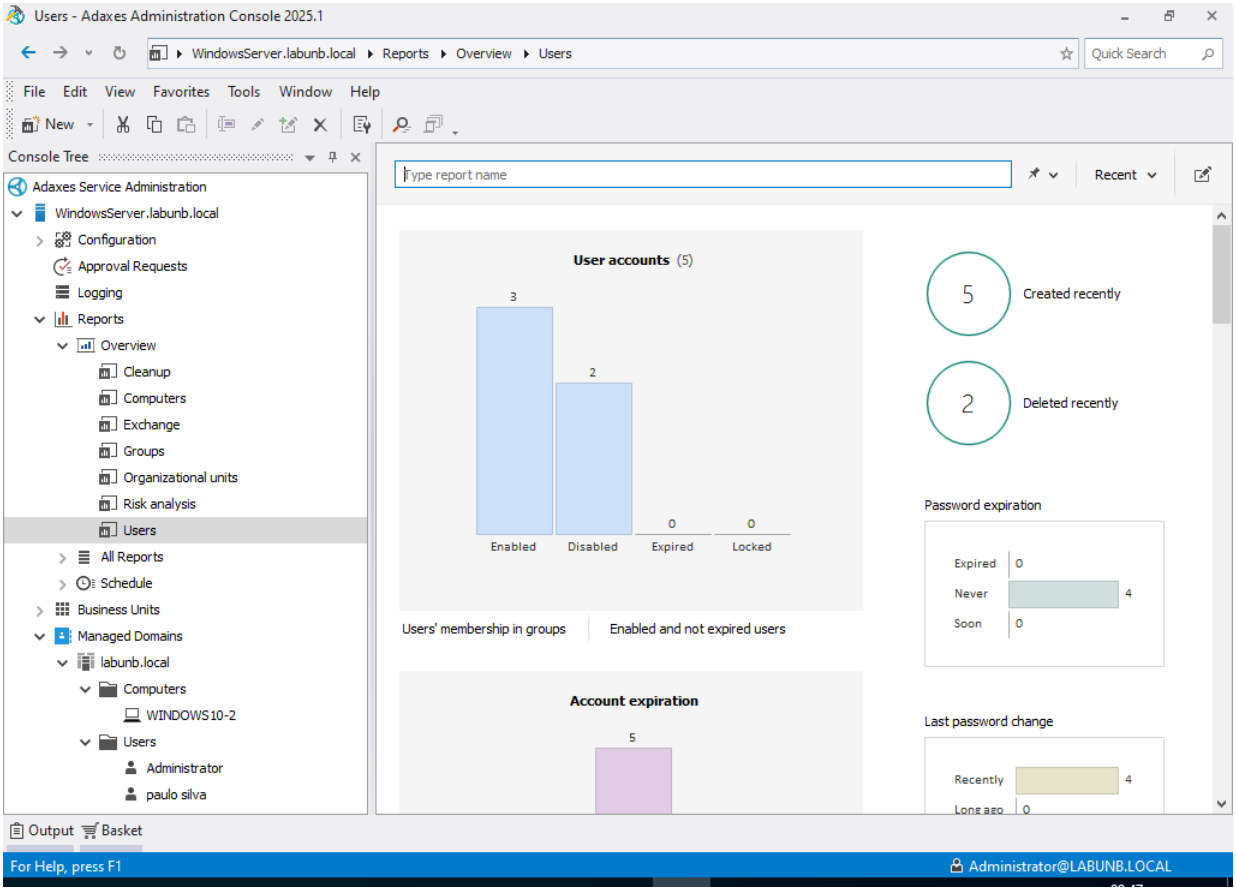

Figura 4.2: Interface Adaxes.

Fonte: do Autor

Ao se aprofundar em algum métrica fornecida pelo AD e gerenciada pelo Adaxes, é possível obter mais destaque e detalhes de cada indicador, conforme figura 4.3:

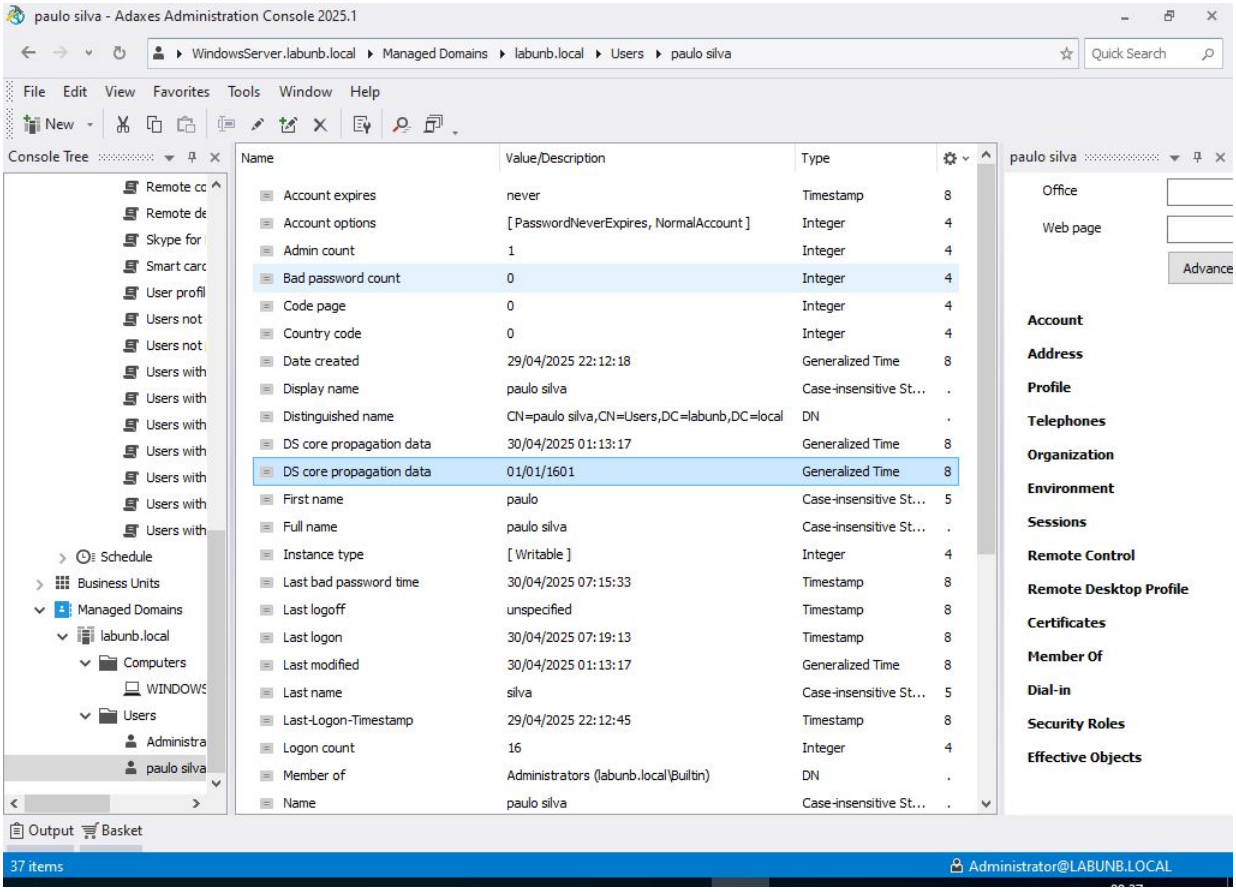

Figura 4.3: Adaxes - Último Logon de Usuário

Fonte: do Autor

O uso deste tipo de ferramenta facilita a monitoria dos diversos aspectos do gerenciamento de identidade. Além disso, a integração delas a um Centro de Operações de Segurança (SOC - Security Operations Center) reduz drasticamente o tempo de detecção e resposta no uso indevido de contas e identidades. Além de respostas automatizadas, um SOC provê respostas com base em ações humanas, nesse caso, informações gráficas são mais facilmente percebidas do que a leitura de logs, por exemplo, essa característica faz com que a monitoração em SOCs utilizando dashboards gráficos seja amplamente realizado.

4.1.2 AC-17 [1] Empregar Mecanismos Automatizados para Monitorar e Controlar Métodos de Acesso Remoto

O controle AC-17 (Access Control 17) da norma SP 800-53, prevê e discute algumas questões importantes sobre controle de acesso remoto como monitorar, gerenciamento de pontos de controle de acesso, comandos e acessos privilegiados, dentre outros. Contudo, a norma não faz recomendações específicas sobre uma técnica amplamente abordada em ataques como os estudados neste trabalho. Considerando as variações do ataque apresentado, em que o ator malicioso realiza comunicação com seu dispositivo via 3G/4G/5G, conexão reversa ou comando e controle (C2), é necessário elencar medidas para mitigar essa comunicação, quando ela utiliza, particularmente, a infraestrutura da própria organização, Nesse caso, em

consonância ao controle AC-17 item de melhoria 1, onde se recomenda monitorar e controlar os mecanismos de controle de acesso, é recomendável aplicar uma medida de controle de tráfego com base em conexões de rede.

Para isso, nesta prova de conceito, foi implementada uma medida de controle de acesso em um firewall, para os casos de conexão reversa, ou seja, conexões que partem da rede interna para o host do atacante. Assim, nos casos em que o atacante realiza conexões reversas utilizando a própria infraestrutura da organização, por exemplo, é possível criar uma ou mais regras no firewall para bloquear esse tipo de tráfego. Para esse laboratório foi criada uma simulação no GNS3 com duas redes, separadas por um firewall PfSense. Em uma das redes, considerada externa a organização, foi criado um servidor Debian para receber uma conexão SSH. Na outra rede, considerada interna, foi simulada uma situação em que um dispositivo Raspberry Pi executou uma técnica de clonagem de uma estação de trabalho legítima (Workstation), conforme a figura 4.4:

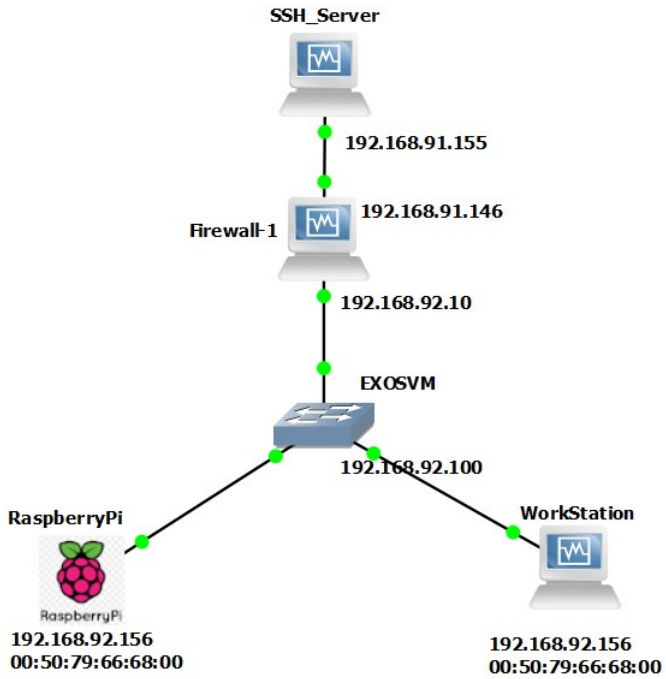

Figura 4.4: Arquitetura do laboratório para Teste de Bloqueio de Tráfego

Fonte: do Autor

Sem um definição de que o acesso via SSH para recursos externos seja implementado, é possível para qualquer host realizar uma conexão desse tipo. Sem uma conexão 3G/4G/5G, um atacante pode automatizar script de conexão para um host externo sob seu controle. Dentre as formas mapeadas para ataques desse tipo, a utilização de comando e controle ou SSH são consideradas comuns, conforme registros de casos similares. Na figura 4.5, é possível notar que, sem um controle do tráfego de saída, o dispositivo Raspberry Pi realiza conexão SSH com sucesso para a rede externa, evidenciando a falta de regra para impedir esse tipo de ação.

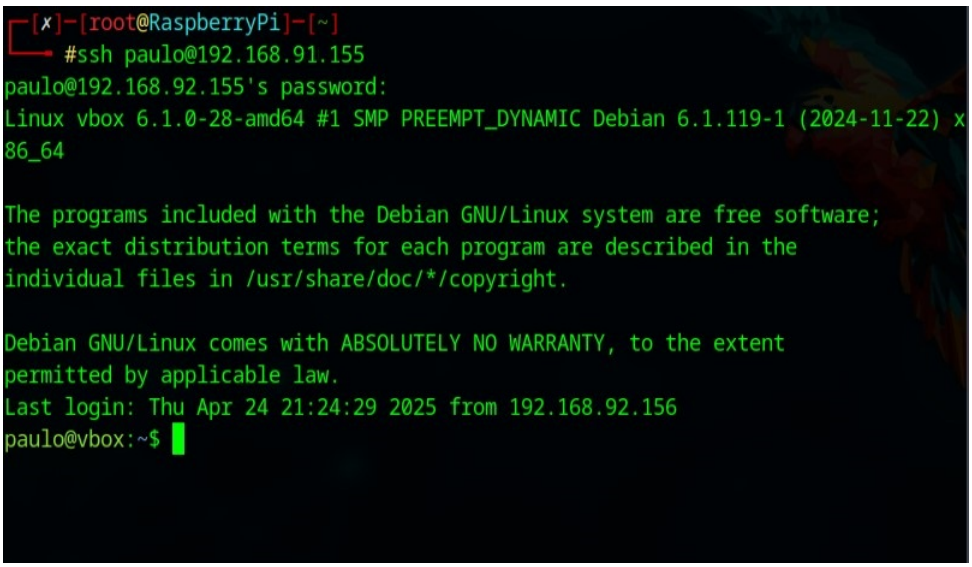

Figura 4.5: Teste de Conexão SSH Bem-sucedida

Fonte: do Autor

Contudo, há que se considerar as devidas políticas e cenários organizacionais que, por exemplo, deem suporte a protocolos dessa natureza, seja SSH, RDP ou portas TCP aleatórias, comumente usadas em comunicações C2, por exemplo. Para demonstração prática, na figura 4.6, foi criada uma única regra capaz de impedir que alguma conexão oriunda da rede interna faça comunicação com recursos externos utilizando SSH.

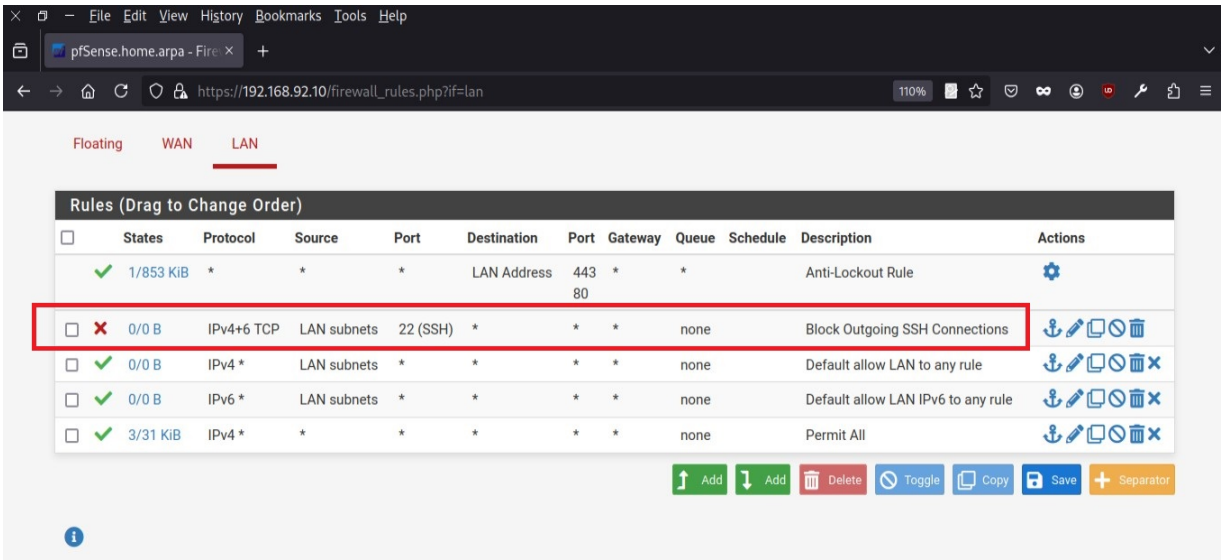

Figura 4.6: Regra de Firewall para Bloqueio de Conexões Indevidas

Fonte: do Autor

Na figura 4.7, após aplicação da regra de bloqueio do protocolo SSH, ao tentar realizar nova tentativa de conexão, o dispositivo não obtém resposta, o que evidencia o funcionamento da contramedida para controle do tráfego de saída.

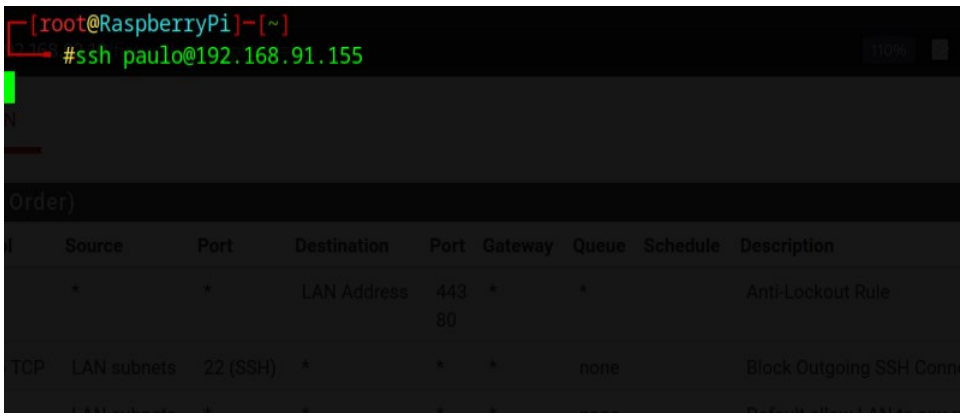

Figura 4.7: Teste de Conexão SSH Mal-sucedida

Fonte: do Autor

Vale ressaltar que, para tecnologias e técnicas diferentes, o gerenciamento de controle de acesso para mitigação desse tipo de ataque pode ser mais complexo e medidas diversas podem ser aplicadas. Para o caso específico apresentado, a medida apresentada nessa prova de conceito é capaz de bloquear a comunicação e pode ser considerada eficaz.

4.1.3 CM-7 (9) (b) Proibir o Uso ou Conexão de Componentes de Hardware não Autorizados

De acordo com a disciplina gerenciamento de configuração (Configuration Management - CM), o controle CM-7 que trata da funcionalidade mínima para uso de hardware, a melhoria 9 desse controle é taxativa ao recomendar que o uso de hardware não autorizado deve ser bloqueado. É comum encontrar políticas de segurança que fazem referência explícita a dispositivos de armazenamento, como discos rígidos externos e pendrives ou dispositivos de rede. Para demonstração da eficácia na adoção desse controle, optou-se por exemplificar o cenário em que um atacante tenta realizar um ataque com o uso de um pendrive ou similar.

Vale ressaltar que, dentre as formas de ataques mapeados sobre o grupo Dark Vishnya, o uso de "Bash Bunny"é reconhecido como um dos métodos preferidos pelo grupo (52). Bash Bunny é um dispositivo similar a um pendrive, com capacidades de execução de scripts e outras ações maliciosas automáticas. O Bash Bunny tem capacidades similares a um Rubber Ducky, ambos são dispositivos para ataques baseados em inserção dispositivos USB, a diferença entre eles é que, enquanto o Rubber Ducky utiliza uma interface lógica HID (Human Interface Device), o Bash Bunny cria dois dispositivos lógicos (54). Ataques que utilizam esse tipo de dispositivo são conhecidos como "USB Drop", em que o atacante deixa um desses dispositivos a mostra em algum ponto dentro ou próximo à organização alvo, assim, um empregado desavisado, motivado por curiosidade, encontra o dispositivo e tenta inserí-lo em um computador para verificar seu conteúdo. Nesse momento, os scripts maliciosos são automaticamente executados no alvo, comprometendo arquivos, criando persistência de acesso e conexões reversas para um servidor do atacante. Os casos de contaminação por ransomware também são comuns de ser iniciados dessa forma.

Sobre o laboratório para produção da prova de conceito do controle CM-7, nesse caso, foi criada uma única máquina virtual, executada sobre o Virtualbox, com sistema operacional Linux (Kali Linux). Para de-

monstração de um exemplo de contramedida de segurança,, optou-se por utilizar a ferramenta USBGuard, que é Open Source. O USBGuard oferece mecanismos de whitelist e blacklist, ou seja, é capaz de permitir determinados dispositivos ou bloquear aqueles definidos pelo administrador da ferramenta. A instalação é realizada no Linux e pode ser feita via gerenciador de pacotes (apt, yum, dnf, por exemplo). Após a instalação, deve-se definir políticas de bloqueio ou permissionamento, essas regras podem ser inseridas via linha de comando, que não persistem após reinício do computador. Para persistência do comportamento, deve-se criar as regras via arquivo de configuração. No exemplo da figura 4.8, é possível visualizar a saída do comando "lsusb"em que são listados todos os dispositivos conectados ao barramento USB da máquina.

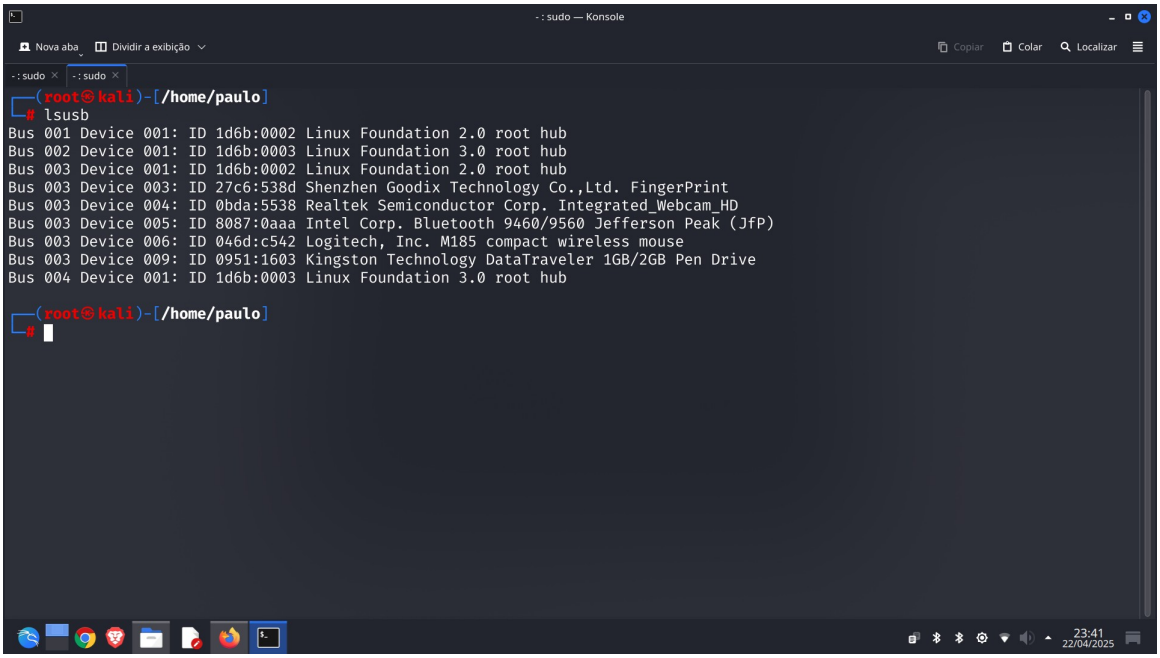

Figura 4.8: Dispositivos Listados por lsusb.

Fonte: do Autor

Cabe ressaltar que o parâmetro ID da saída do comando lsusb é utilizado para referenciar determinados dispositivos. Esse valor é representado por identificador do fabricante (vendor id) e do produto (product id). Por exemplo, o valor do dispositivo 0951:1603 diz respeito ao fabricante "Kingston Technology Company"e ao produto "DataTraveler 1GB/2GB Pen Drive". Essas informações são importantes para definição de políticas no USBGuard. O USBGuard é composto de alguns subcomandos, como "watch"que, conforme tradução do inglês, "assiste"a novos eventos relativos a conexões, desconexões, bloqueio, dentre outros. A figura 4.9 exemplifica eventos de conexão e desconexão do dispositivo 0951:1603.

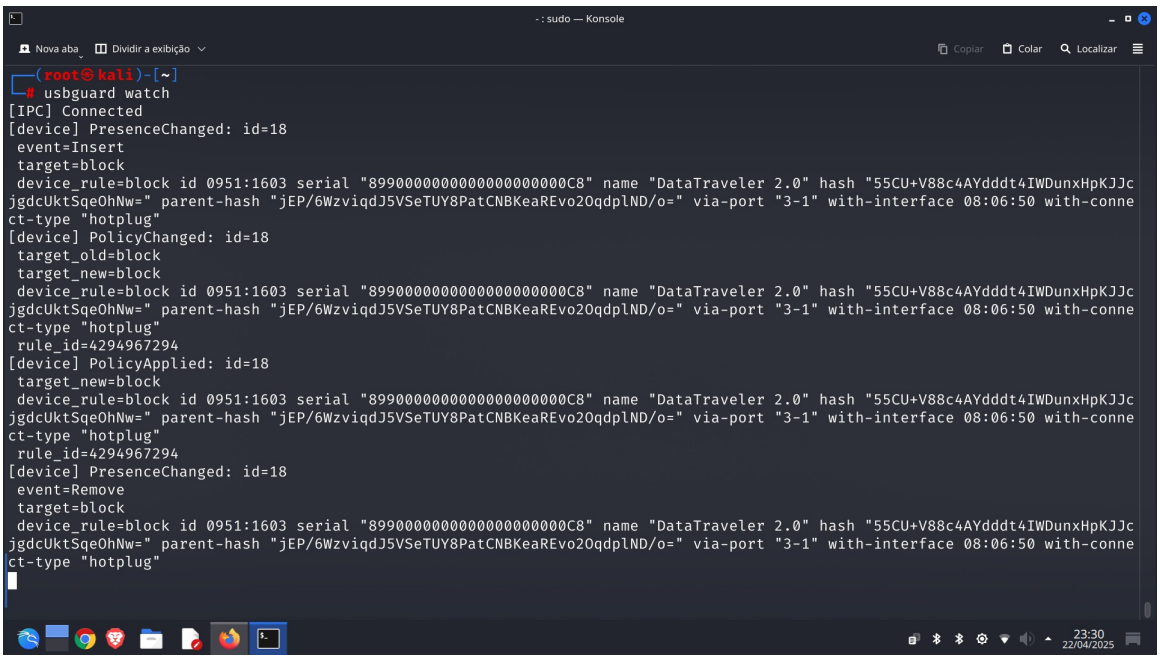

Figura 4.9: Eventos Relativos ao Dispositivo de Teste.

Fonte: do Autor

Outro exemplo pode ser visto na figura 4.10, em que o subcomando list-devices mostra dispositivos, e o parâmetro -b especifica se tratar daqueles bloqueados por alguma política.

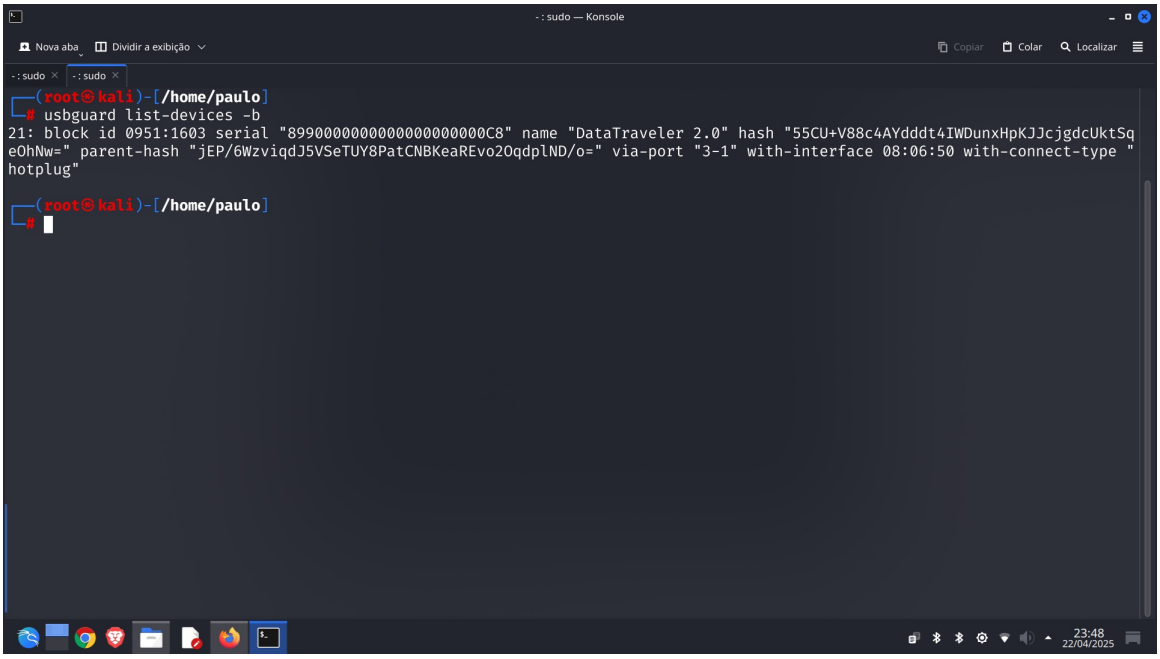

Figura 4.10: Monitorando Dispositivos Bloqueados.

Fonte: do Autor

Por fim, a figura 4.11 mostra a definição de uma política de bloqueio com o comando "usbguard block-device -p 0951:1603". Na parte de baixo da mesma figura, o comando usbguard watch mostra

eventos relativos a USB mostrando, inclusive, a conexão e o posterior bloqueio do mesmo dispositivo.

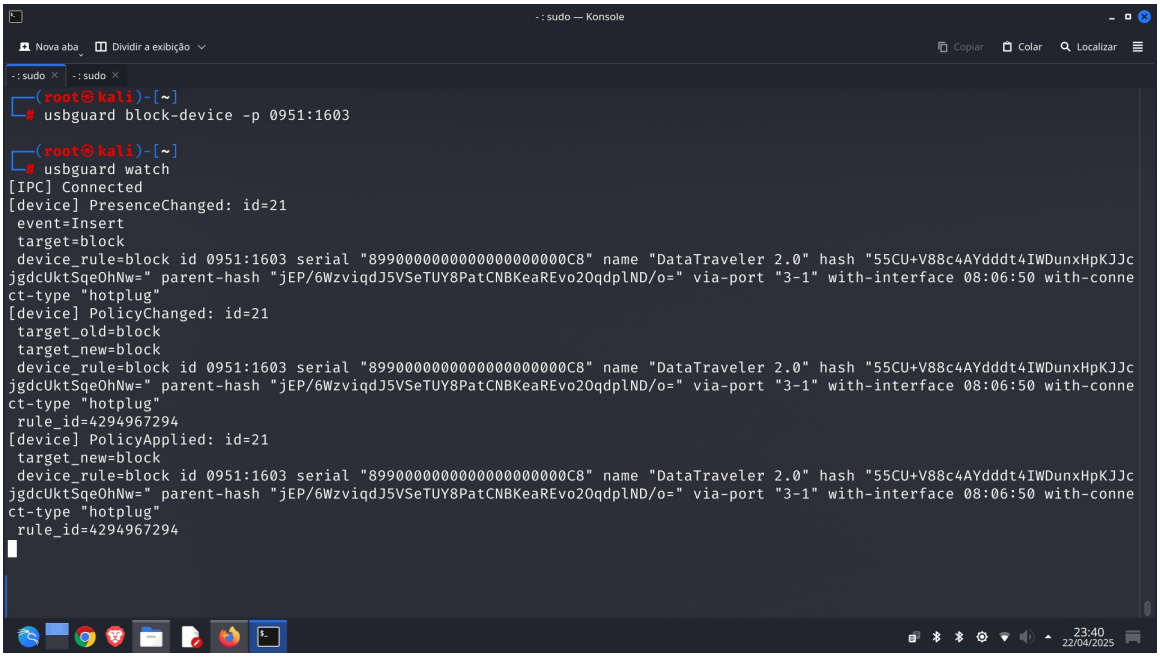

Figura 4.11: Definição e Aplicação de Política por Linha de Comando.

Fonte: do Autor

Por fim, cabe mencionar que o USBGuard é capaz de políticas mais complexas, bloqueando dispositivos conectados em modo HID, basicamente mouses, teclados e outros dispositivos, enquanto o modo storage se refere a dispositivos de armazenamento, como pendrives. O USBGuard foi escolhido para exemplificação desse controle pela facilidade de utilização e por ser uma ferramenta open source, de fácil implementação. Contudo, ferramentas como Free USB Guard ou USB Disk Security podem ser opções para sistemas como Windows. Em relação a sistemas Windows, é muito comum que ambientes corporativos implementem as mesmas políticas via Active Directory, utilizando GPO (Group Policy Objects). Portanto, esta prova conceito demonstrou que a aplicação do controle CM-7, ao bloquear a conexão de hardware não autorizado, efetivamente impediu a inserção de dispositivos espúrios na rede, confirmando a hipótese de que essa medida é capaz de prevenir o uso de pontos de acesso clandestinos.

4.1.4 CM-8 (a) Desenvolver e Documentar um Inventário de Componentes do Sistema que Reflita com Precisão o Ambiente

A publicação especial NIST SP 800-53 tem um grupo de controles voltados a gerenciamento de configuração e, mais especificamente, um dos controles constantes nesta proposta, que pode impactar diretamente o cenário de ataque com dispositivos compactos, é o controle CM-8 item (a). A descrição desta medida é específica em tratar de inventário de componentes do sistema e o item (a) fornece diretrizes sobre desenvolver e documentar um inventário que reflita com precisão o ambiente organizacional. Nesse sentido, essa prova de conceito foi dividida em duas partes, sendo a primeira focada em utilizar uma ferramenta acessível e capaz de realizar a tarefa de manter esse inventário; e a segunda parte com foco identificar

dispositivos clonados, capazes de contornar a visibilidade precisa do inventário. Para esse laboratório, foi criada uma estrutura virtualizada, conforme a figura 4.12:

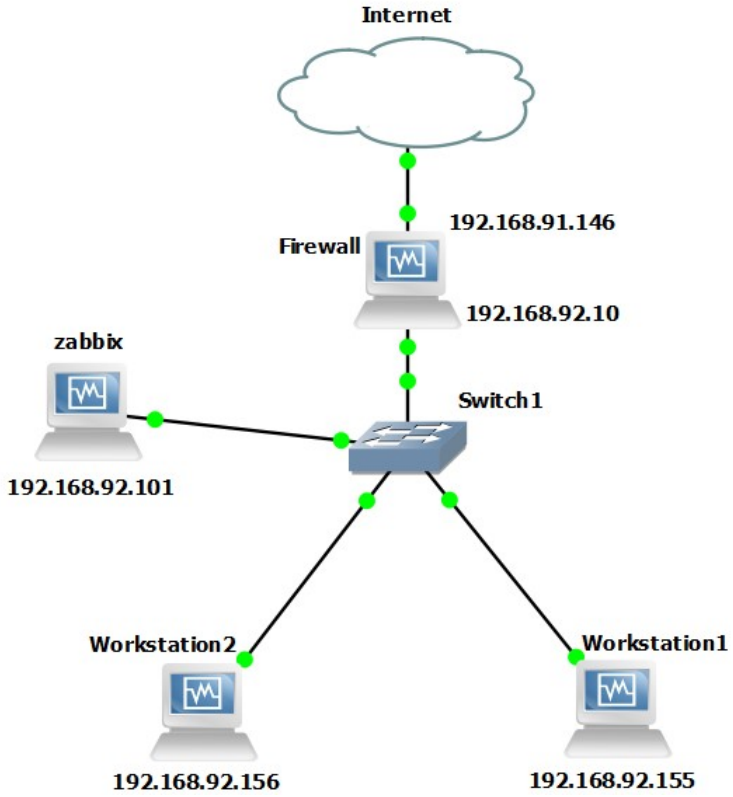

Figura 4.12: Arquitetura do Laboratório Utilizada para Testes de Inventário.

Fonte: do Autor

Nessa arquitetura, foi criado um servidor de monitoração e inventário, que utiliza a ferramenta open source Zabbix. Na mesma rede desse servidor, foram conectados dois hosts legítimos a serem monitorados e inventariados, Workstation1 e Workstation2 (ambos Linux), um Switch e a conexão internet com Firewall. Para a primeira parte do laboratório, em que se cria um inventário dos dispositivos da rede, pode-se (1) usar o protocolo SNMP, utilizado para monitoração de ativos computacionais e de rede ou (2) realizar a instalação de agentes do Zabbix, nos hosts que dão suporte a instalação do agente. Neste laboratório, foram utilizados agentes nos hosts Workstation1, Workstation2 e Firewall, no Switch foi habilitado o suporte ao SNMP versão 2. Para configuração dos agentes Zabbix nos hosts Workstation1 e Workstation2 e Firewall, basta (1) instalar o software do agente através do comando sudo apt install zabbix-agent; (2) atualizar o arquivo principal de configuração /etc/zabbix/zabbix_agentd.conf, modificando as variáveis Server, ServerActive e Hostname com dados relativos ao servidor Zabbix, conforme figura 4.13, por fim, deve-se reiniciar a execução do agente com o comando sudo systemctl restart zabbix-agent.

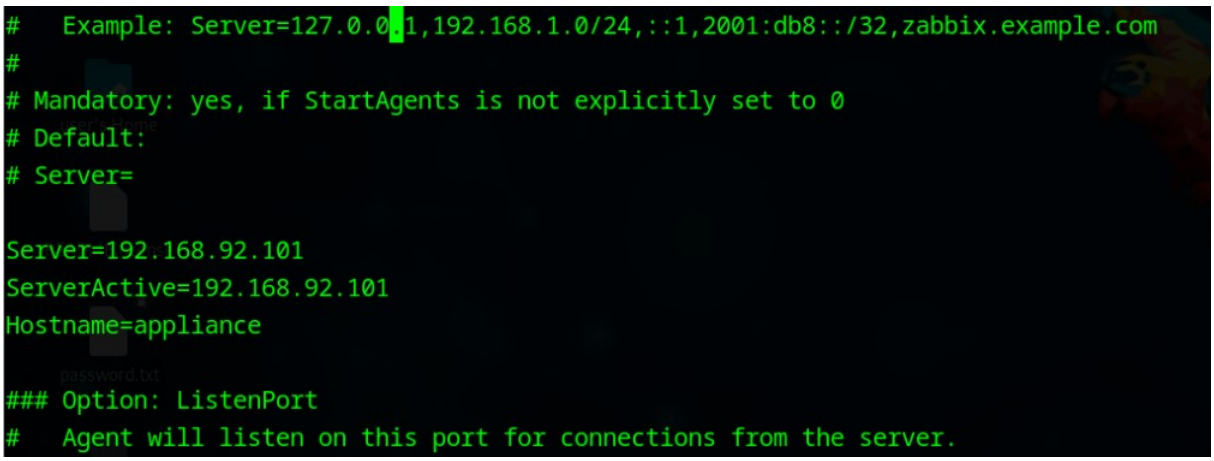

Figura 4.13: Configuração do Arquivo do Agente Zabbix.

Fonte: do Autor

A configuração do monitoramento no Switch deve ser feita utilizando SNMP, já que o sistema operacional do dispositivo não permite a instalação do agente. Assim, foram utilizados os comandos mostrados na figura 4.14, sendo executados os comandos do topo para baixo.

```
configure snmpv3 add community "public" name "public" user "v1v2c_rw"
enable snmp access
enable snmp access snmp-v1v2c
disable snmp access snmpv3
```

Figura 4.14: Comandos para Ativação do SNMPv2 no Switch EXOS.

Fonte: do Autor

Após a configuração nos hosts a serem monitorados, deve-se proceder com a configuração no servidor. Para isso, deve-se acessar a aba Configuration e, a seguir, a opção Hosts, clicar em Create Host no canto superior direito, conforme figura 4.15.

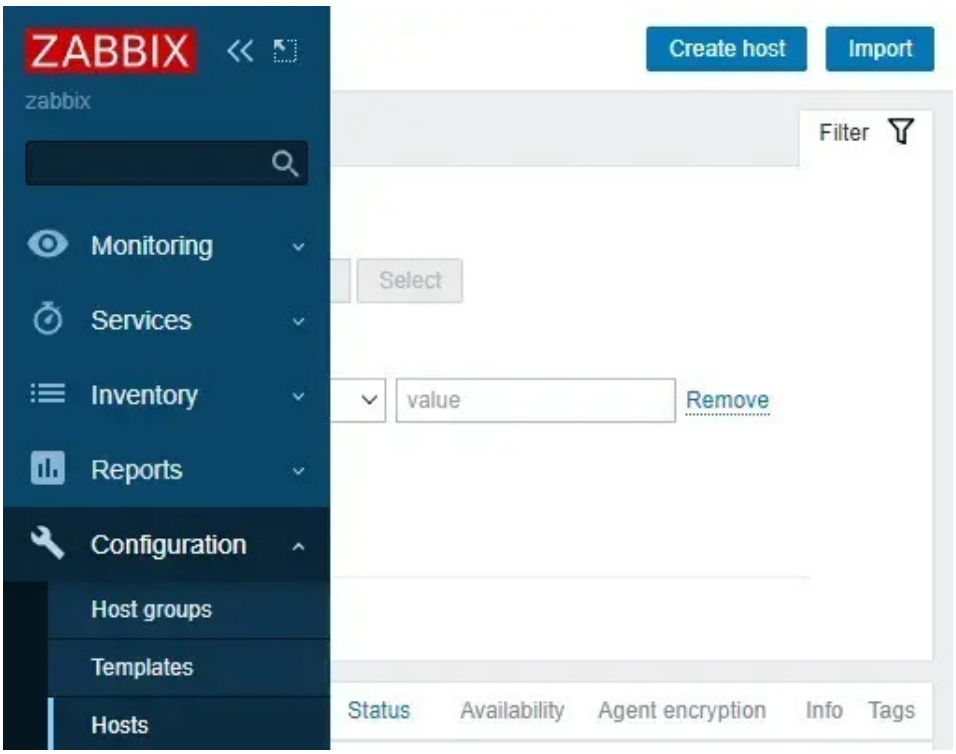

Figura 4.15: Caminho para Criação de Instâncias de Host a Serem Monitorados.

Fonte: do Autor

Na janela que se abre, deve-se preencher minimamente (1) o Host name, (2) escolher o template a ser utilizado (que reflita o tipo do host a ser monitorado), (3) endereço IP e porta (por padrão, 10050 para agente e 161 para agente SNMP) do agente ou cliente SNMP (Nesta opção, informar dados de autenticação do SNMP), por fim, deve-se clicar em add, conforme figura 4.16.

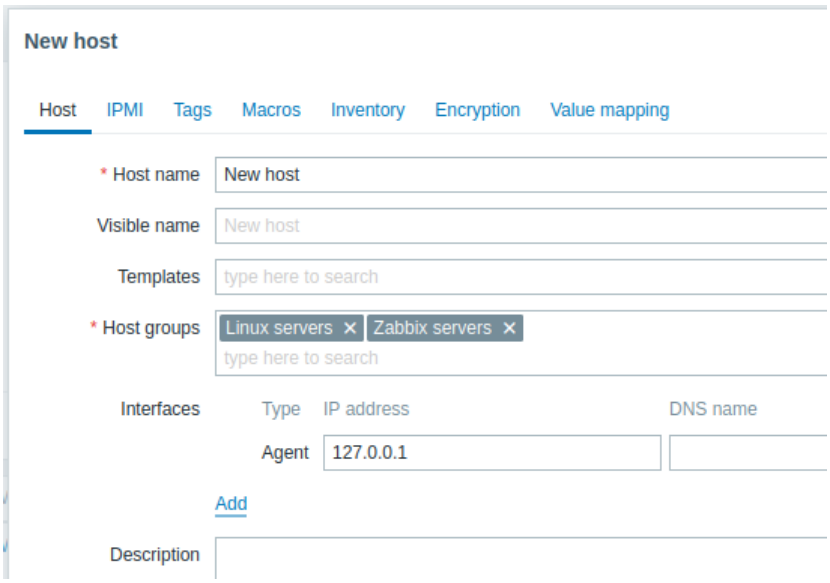

Figura 4.16: Janela para Criação de Hosts para Monitoração.

Fonte: do Autor

No Zabbix, é possível gerar um mapa gráfico do inventário cadastrado, conforme figura 4.17.

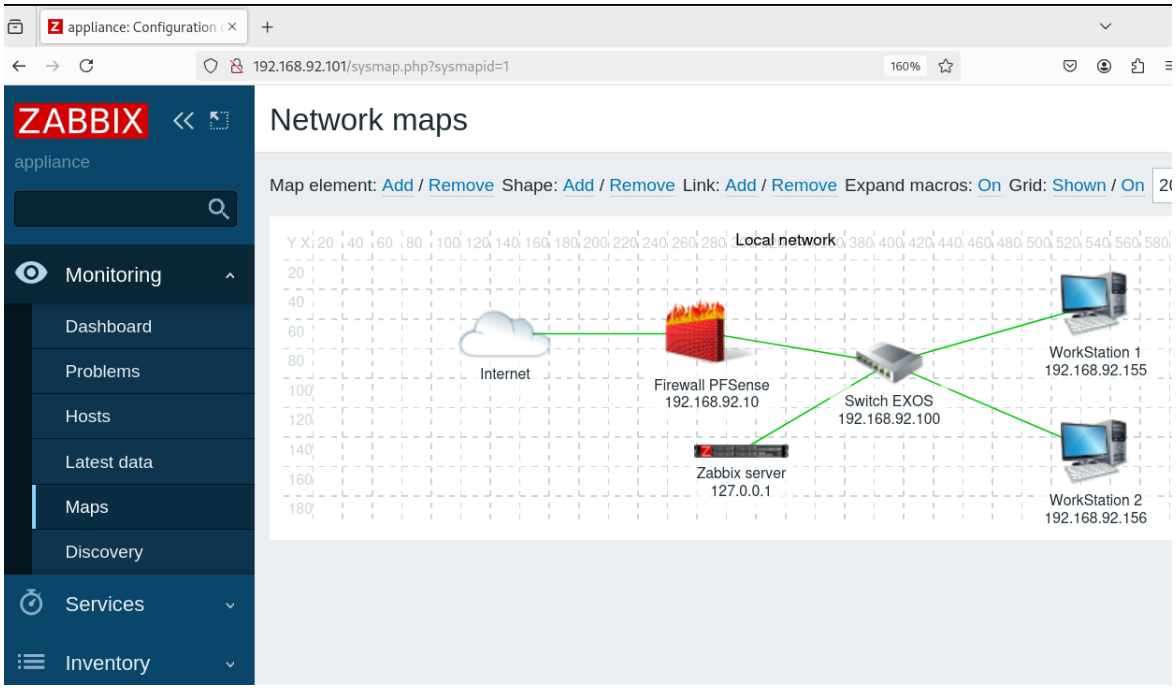

Figura 4.17: Mapa do Inventário Monitorado Gerado no Zabbix.

Fonte: do Autor

Para replicação da técnica de bypass no contorno da monitoração dos hosts conhecidos, foi inserido um Hub no meio da conexão, entre o estação Workstation2 e o Switch. Em seguida, foi criado um clone do host Workstation2, um dispositivo com Linux que simule a presença de um Raspberry Pi na rede. O clone foi configurado de forma que seu endereço físico, IP e hostname fossem iguais aos da estação Workstation2. Assim, o clone Raspberry Pi deve, do ponto de vista do Switch e das ferramentas de monitoração e inventário, ser identificado como um único dispositivo, juntamente com a estação Workstation2 clonada, conforme figura 4.18 que retrata de forma mais detalhada a estrutura. Esse arranjo impede que um dispositivo espúrio seja devidamente identificado, pois o Switch e as ferramentas de monitoração e inventário, continuam visualizando apenas um dispositivo, pois só há registro de um único endereço IP, endereço físico e Hostname.

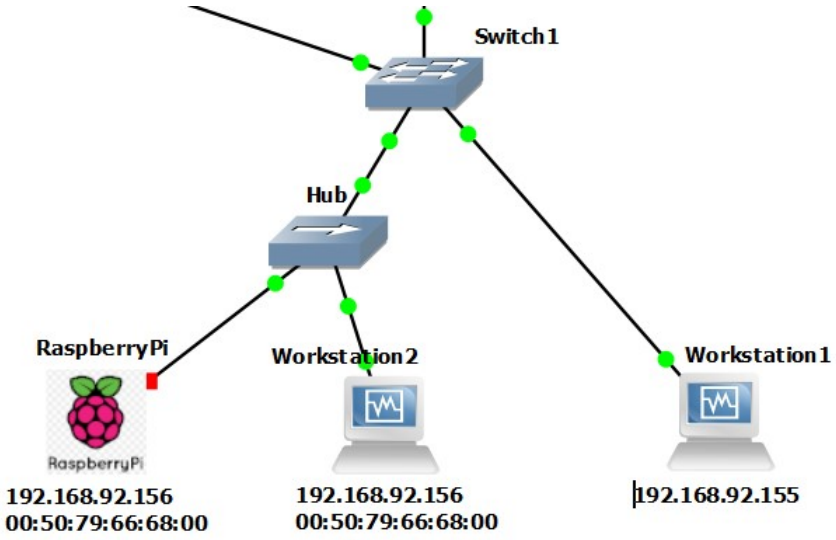

Figura 4.18: Inserção do Hub e Dispositivo Espúrio como Clone de Host Legítimo.

Fonte: do Autor

Para identificação do dispositivo espúrio na rede, é possível utilizar um script para varredura de hosts por avaliação de respostas ARP (Address Resolution Protocol), o ARP-Scan. O ARP-Scan pode ser utilizado em sistemas Linux e Windows e, uma vez instalado em um host da rede, é possível automatizar sua execução para um determinado segmento de rede. O ARP-Scan funciona enviando requisições ARP (ARP Request) para os hosts da rede e, em caso de duplicação, ele recebe uma resposta com alerta de duplicação de endereço físico, conforme figura 4.19.

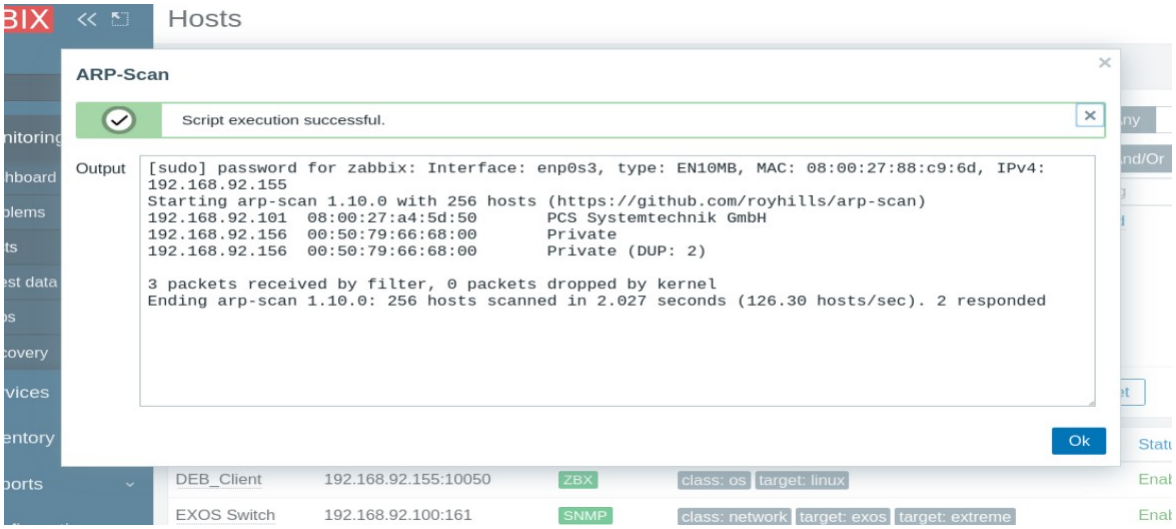

Figura 4.19: Resultado do Script ARP-Scan para percepção de Host Clonado.

Fonte: do Autor

A automação pode ser realizada com o próprio agente do Zabbix, através da função de Scripts, presente no caminho Administração > Scripts da console Web do Zabbix, conforme figura 4.20. Outra forma comum é utilizar alguma ferramenta de agendamento do próprio sistema operacional, como o cron, no

caso do Linux.

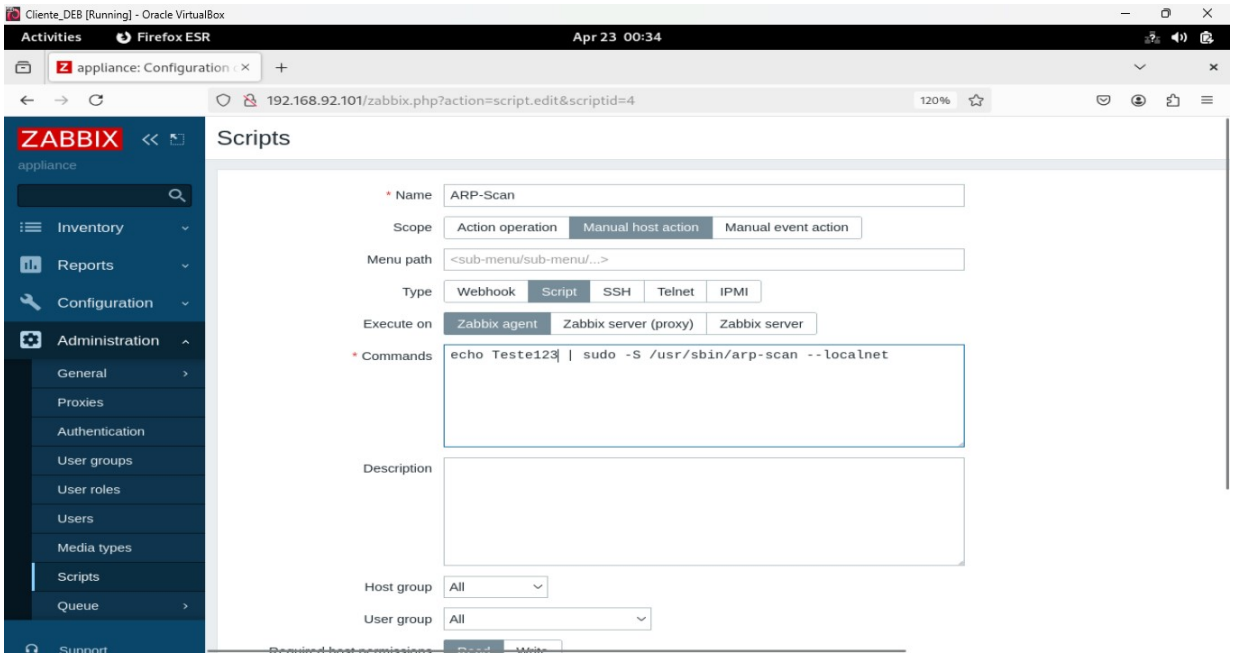

Figura 4.20: Definição do Comando para Execução de Script no Host.

Fonte: do Autor

Após a definição do script a ser executado no host monitorado, a rotina aparecerá como opção do host na lista de dispositivos do inventário Zabbix, conforme demonstrado na figura 4.21.

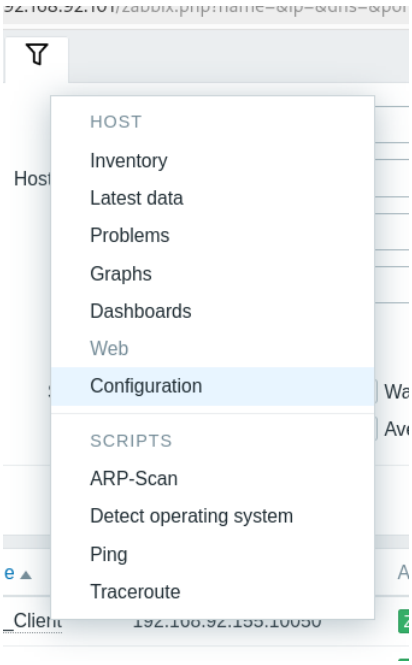

Figura 4.21: Seleção de Script a ser Executado no Host.

Fonte: do Autor

Portanto, esta prova de conceito evidenciou que a criação e manutenção de um inventário preciso de ativos, aliado ao uso de uma ferramenta centralizada, não apenas permite validar hosts legítimos, mas também possibilita identificar rapidamente dispositivos não cadastrados ou clones espúrios conectados à rede. Isso confirma a hipótese H4, ao demonstrar que um inventário atualizado e confiável é fundamental para detectar e mitigar a presença de dispositivos não autorizados em ambientes corporativos.

4.1.5 IA-3 [1] Identificar e Autenticar Dispositivos | Autenticação de Rede Bidirecional

Segundo a definição do NIST, o controle IA-3 se refere a identificação e autenticação, de forma ampla. Mas especificamente, a melhoria 1, ou seja, IA-3 [1], trata sobre autenticação e identificação de dispositivos, utilizando criptografia, de forma bidirecional. Nesse caso, a identificação e autenticação ocorrem de forma simultânea e nos dois sentidos, antes que uma conexão possa ser realizada, por exemplo, no caso em que um cliente identifica um servidor e vice-versa. Nesse caso específico, optou-se por utilizar a tecnologia MACsec, padrão IEEE 802.1ae, para prova de conceito sobre como esse controle pode ser implementado e quais resultados podem ser obtidos a partir da adoção de medidas como essa. O MACsec é um protocolo de segurança ponto a ponto, utilizado em links Ethernet (Camada 2 do modelo OSI, conforme a figura 4.22), que pode ser implementado em conjunto com outros protocolos para conferir autenticidade, confidencialidade e integridade (22).

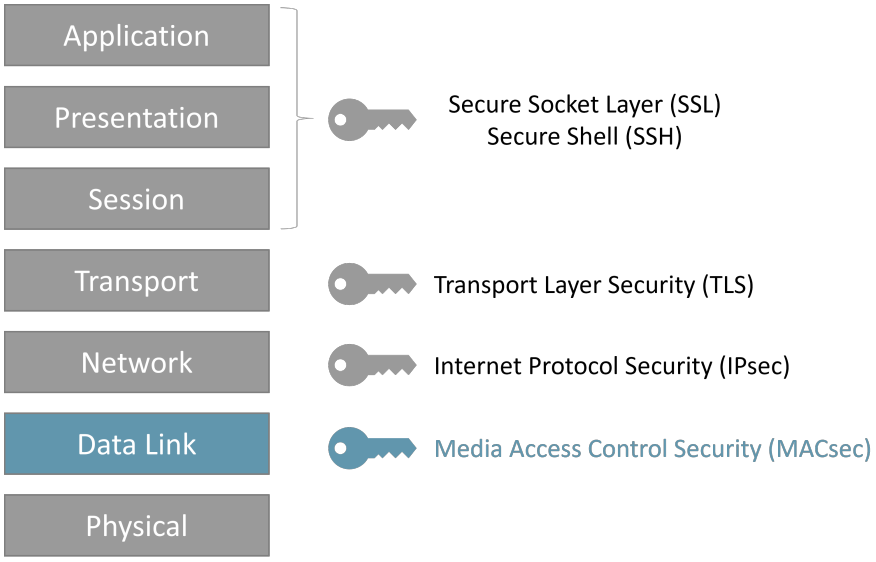

Figura 4.22: MACsec atua na Camada 2 do Modelo OSI.

Fonte: https://www.comcores.com/what-is-macsec/

O MACsec é capaz de prevenir uma série de ataques comuns em redes locais como negação de serviço (DoS - Denial of Service), Homem no Meio (Man in the Middle), ataques de reprodução (Replay Attack), dentre outros (55). O funcionamento do MACsec deve ser habilitado em dois nós diretamente conectados, podendo ser realizado entre dois hosts, um host e um switch/roteador ou entre dois switches/roteadores. Utilizando MACsec, hosts Ethernet só realizam o envio de frames em uma rede local (LAN), primeiramente, estando autenticados. A autenticação de hosts com MACsec na mesma LAN ocorre por Associação

de conectividade (CA - Connectivity Association), isso significa que hosts MACsec estão conectados e são autorizados a se comunicar entre eles, desde que os membros do mesmo CA se reconheçam e possuem chaves de associação de conectividade (CAK - Connectivity Association Key) e nome de chave de associação de conectividade (CKN - Connectivity Association Key Name) correspondentes. Ocorrido o processo de autenticação, o protocolo MACsec permite a criptografia de cargas de dados (payloads) utilizando algoritmo simétrico, AES-GCM de 128 (padrão), 192 ou 256 bits. Como o estudo do protocolo MACsec está além do escopo deste trabalho, o assunto não pôde ser exaurido. Para o laboratório desta prova de conceito, foram criadas duas máquinas virtuais (VMs), executando sistema operacional Linux (Debian e Parrot Linux), conectadas diretamente entre si. Conforme figura 4.23, foram executados os respectivos comandos nas duas máquina, na ordem em que aparecem.

DEBIAN

```
ip link set enp0s3 down
modprobe macsec
ip link add link enp0s3 macsec0 type macsec encrypt on
ip macsec add macsec0 tx sa 0 pn 1 on key AAAA 01234567012345670123456701234567
ip macsec add macsec0 rx address 08:00:27:e1:04:25 port 1
ip macsec add macsec0 rx address 08:00:27:e1:04:25 port 1 sa 0 pn 1 on key BBBB 89ABCDEF89ABCDEF89ABCDEF89ABCDEF
ip addr add 192.0.2.1/30 dev macsec0
ip -6 addr add 2001:db8::a/127 dev macsec0
ip link set enp0s3 up
ip link set macsec0 up
```

PARROT

```
ip link set enp0s3 down
modprobe macsec
ip link add link enp0s3 macsec0 type macsec encrypt on
ip macsec add macsec0 tx sa 0 pn 1 on key BBBB 89ABCDEF89ABCDEF89ABCDEF89ABCDEF
ip macsec add macsec0 rx address 08:00:27:10:62:18 port 1
ip macsec add macsec0 rx address 08:00:27:10:62:18 port 1 sa 0 pn 1 on key AAAA 01234567012345670123456701234567
ip addr add 192.0.2.2/30 dev macsec0
ip -6 addr add 2001:db8::b/127 dev macsec0
ip link set enp0s3 up
ip link set macsec0 up
```

Figura 4.23: Comandos para Ativação e Configuração do MACsec no Linux.

Fonte: do Autor

Após as devidas definições de chaves e configuração do protocolo, é possível verificar o estado de funcionamento da implementação em cada host, com o comando ip macsec show, conforme figura 4.24 E figura 4.25:

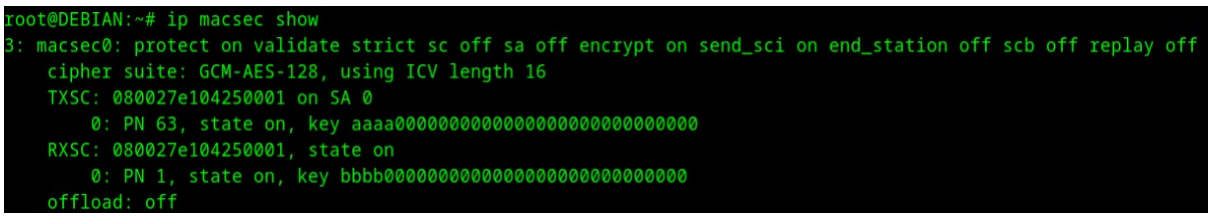

Figura 4.24: Verificação do estado do MACsec no Debian.

Fonte: do Autor

Figura 4.25: Verificação do estado do MACsec no Parrot.

Fonte: do Autor

Adicionalmente, pode-se verificar as estatísticas de envio e recepção de dados em cada um dos hosts relacionados na mesma associação de conectividade, utilizando o comando ip -s macsec show, conforme figura 4.26 e figura 4.27:

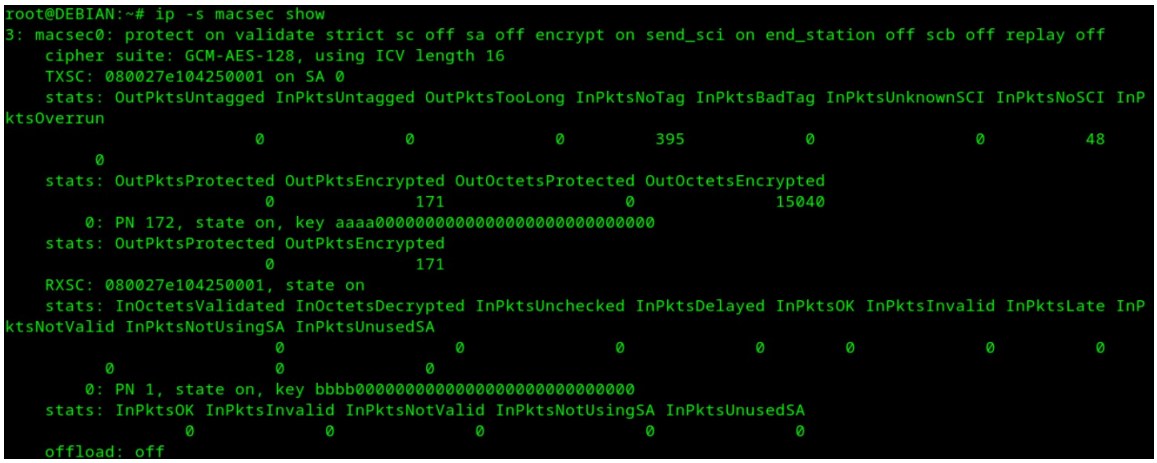

Figura 4.26: Verificação do estatísticas do MACsec no Debian.

Fonte: do Autor

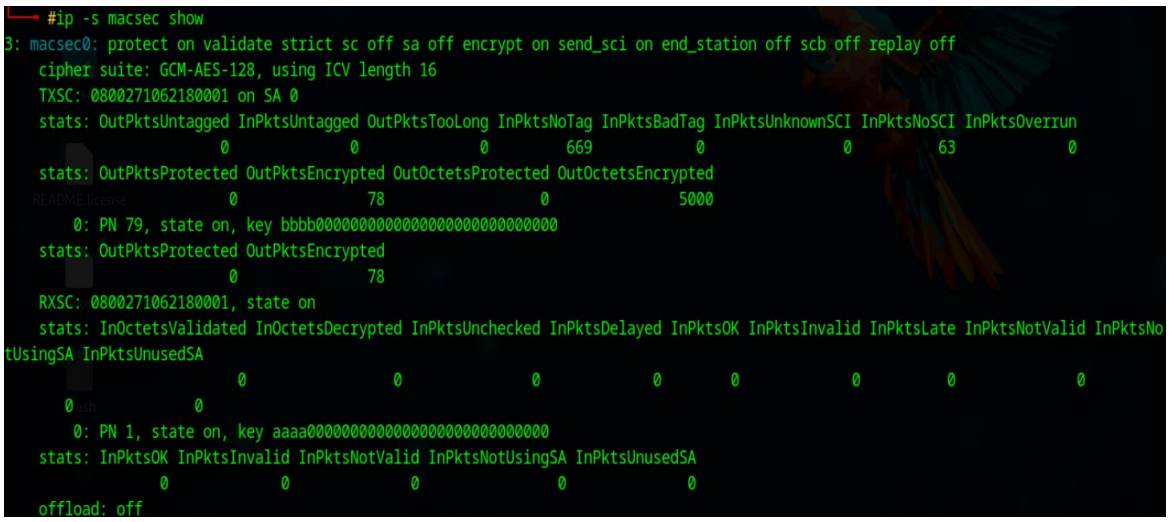

Figura 4.27: Verificação do estatísticas do MACsec no Parrot.

Fonte: do Autor

Realizando captura de tráfego, com Wireshark, entre os hosts Debian e Parrot, é possível constatar e analisar o funcionamento do MACsec, conforme figura 4.27. Na imagem, é possível observar o uso do MACsec na coluna Protocol (1). Na seção detalhes do pacote (2) é possível ver mais informações sobre o pacote selecionado, como protocolo, encapsulamento, dentre outros. A seção bytes do pacote (3) possibilita a leitura dos dados do pacote em formato hexadecimal e ASCII. A seção 3 mostra uma informação importante pois, de fato, os dados mostrados em ASCII estão criptografados.

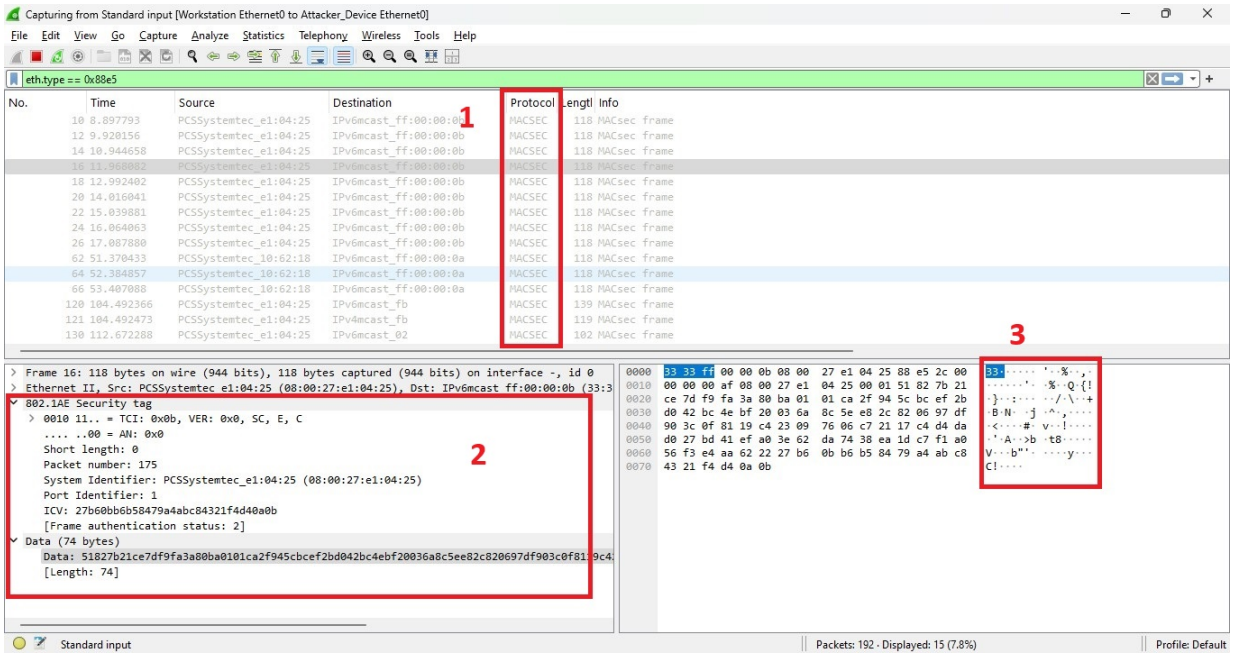

Figura 4.28: Captura de Tráfego MACsec entre os Hosts.

Fonte: do Autor

Apesar de sua robustez, a segurança do MACsec depende diretamente da força dos algoritmos crip-

tográficos e dos protocolos de autenticação utilizados em conjunto com ele. Um exemplo crítico, sobre o assunto, é a vulnerabilidade CVE-2018-15372, que expôs falhas na implementação do protocolo EAP-TLS (Extensible Authentication Protocol - Transport Layer Security) para MACsec. Essa falha permitia que um invasor, explorando algoritmos criptográficos fracos ou mal configurados, burlasse a autenticação mútua e estabelecesse conexões não autorizadas (56).

A vulnerabilidade destacou a importância de evitar o uso de algoritmos considerados obsoletos ou inseguros, como RC4, MD5 e versões antigas do TLS (como TLS 1.0 e 1.1), que ainda podem ser suportadas por implementações mal configuradas. Em ambientes que utilizam MACsec, é essencial garantir que apenas algoritmos modernos e seguros estejam habilitados, como AES-GCM com chaves de 128 ou 256 bits, e que o protocolo de negociação de chaves (como o MKA – MACsec Key Agreement) esteja corretamente configurado para rejeitar conexões com parâmetros criptográficos fracos.

O suporte ao MACsec em sistemas operacionais varia conforme a plataforma. No Linux, o suporte ao MACsec é nativo, permitindo a configuração direta por meio de ferramentas como ip (do pacote iproute2) e wpa_supplicant para negociação de chaves com 802.1X/MKA (57). Já no Windows, o suporte nativo ao MACsec é limitado, especialmente em versões voltadas ao usuário final. No entanto, é possível utilizar o MACsec em ambientes Windows por meio de soluções de terceiros, como o Cisco AnyConnect Secure Mobility Client, que oferece suporte à autenticação 802.1X e à criptografia MACsec quando integrado a uma infraestrutura compatível, como switches Cisco e servidores de autenticação (58). Essa abordagem permite que dispositivos Windows participem de redes seguras com MACsec, mesmo sem suporte direto do sistema operacional.

Assim, a implementação de autenticação criptográfica bidirecional demonstrou ser eficaz para impedir que dispositivos não autorizados estabeleçam comunicação plena na rede, mesmo em cenários de acesso físico. Essa medida não apenas dificulta a captura de dados em trânsito por atacantes, como também reforça a integridade e a confidencialidade das conexões entre os nós legítimos. Dessa forma, confirma-se a hipótese H5, ao evidenciar que a autenticação bidirecional com protocolos como o MACsec é capaz de prevenir a conexão e o uso indevido de dispositivos espúrios, reforçando a proteção contra ataques de interceptação e injeção de tráfego em redes locais.

4.1.6 IR-4 (5) Implementar um Recurso para Desabilitar Automaticamente um Recurso Caso Violações de Segurança sejam Detectadas

O controle IR-4 se refere a tratamento de incidentes, mais especificamente, a melhoria 5 diz respeito ao desligamento automático de sistemas afetados. Nesse contexto, o NIST SP 800-53 recomenda, de forma neutra sobre tecnologia, que sejam implementados controles que deem capacidade de desabilitar recursos, caso violações definidas sejam detectadas (10). Em ataques de intrusão em redes internas, é comum a utilização de Hubs para aumento da quantidade de portas em switches, o que pode favorecer cenários de man-in-the-middle, por exemplo. Considerando esse cenário, foi criado um ambiente simulado para replicação de ataques desse tipo e posterior aplicação de contra-medida para o problema. O laboratório, controlado e simulado pelo GNS3 e virtualizado por VirtualBox, é composto de um Switch Extreme (EXOS), um host legítimo (Workstation) e o host do atacante. Foi utilizado também um Hub para construção do caso em questão. A arquitetura pode ser vista na figura 4.29:

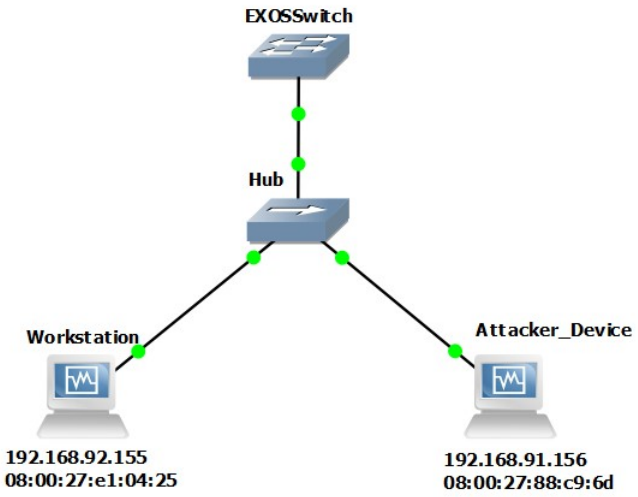

Figura 4.29: Arquitetura do Laboratório para Teste de Bloqueio de Porta.

Fonte: do Autor

Simulando uma conexão comum, o host legítimo é conectado a porta do switch, e ao verificar estado das portas do switch, é percebido estado de "Enabled"(E), na porta 1, na coluna "Port State", conforme figura 4.30:

```
EXOS-VM.15 # show ports 1
Port Summary Monitor                    Tue Jan  7 18:20:04 2025
Port     Display             VLAN Name          Port  Link  Speed  Duplex
#        String              (or # VLANs)       State State Actual Actual
================================================================================
1                            Default            E     A      100    FULL









================================================================================
   Port State: D-Disabled, E-Enabled, F-Disabled by link-flap detection,
               L-Disabled due to licensing
   Link State: A-Active, R-Ready, NP-Port Not Present, L-Loopback,
               D-ELSM enabled but not up,
               d-Ethernet OAM enabled but not up,
               B-MACsec enabled but blocked awaiting authentication
```

Figura 4.30: Estado da Porta Habilitado.

Fonte: do Autor

Verificando informações sobre endereços físicos conhecidos pelo switch, executando o comando "show fdb", é mostrado o endereço físico de apenas um dispositivo, conforme pode ser visto na figura 4.31:

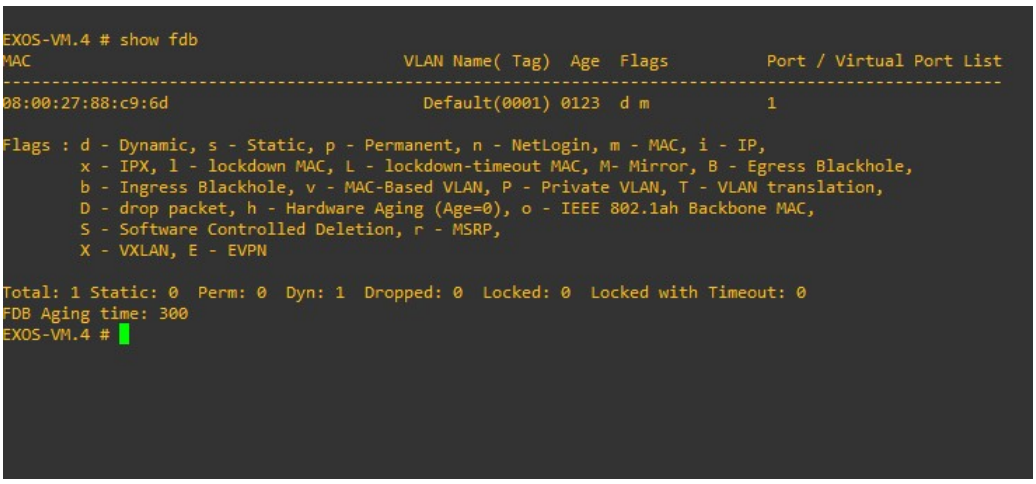

Figura 4.31: Dispositivo Legítimo Identificado.

Fonte: do Autor

O comportamento acima é considerado comum numa conexão de dispositivo legítimo em uma rede interna. Contudo, para simular a ação de um atacante, foi conectado um Hub entre o switch e o host legítimo (figura 4.29) e, com exceção da diferença na inserção desse dispositivo, toda conexão e aprendizagem de endereço físico ocorre da mesma maneira. O próximo passo do ataque é inserir o dispositivo invasor em outra porta do Hub e tentar utilizar a porta de switch já em funcionamento normal. Desse modo, um atacante pode se utilizar de um mesmo ponto para realizar inserção do seu dispositivo espúrio na rede alvo. Sem nenhuma proteção no nível do switch, a inserção do segundo dispositivo no segmento de rede não gera nenhum alarme ou bloqueio de porta, conforme figura 4.32:

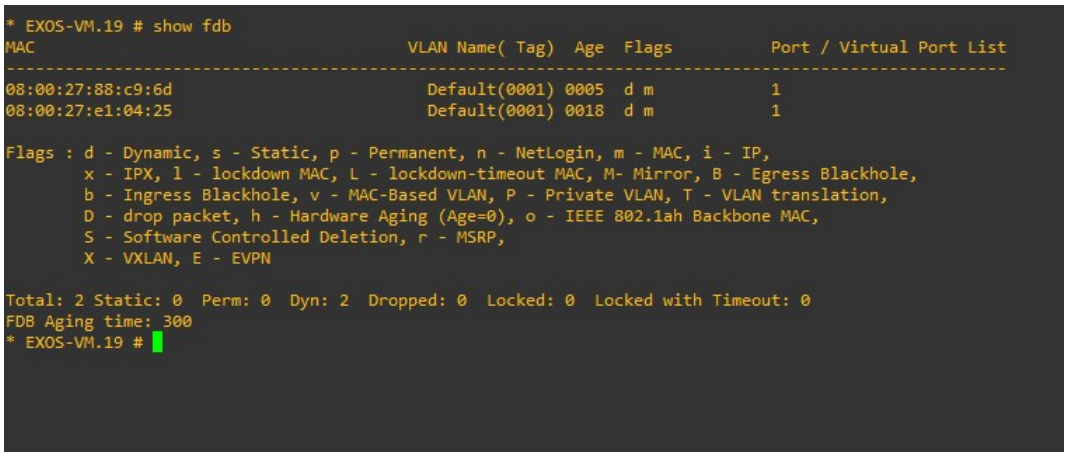

Figura 4.32: Identificação do Dispositivo do Atacante.

Fonte: do Autor

Assim, o atacante tem acesso livre ao tráfego do host legítimo, podendo capturá-lo e analisar o conteúdo em busca de informações sensíveis, como credenciais de acesso. Sem um controle de segurança, esse tipo de técnica pode ser utilizada para conexão indevida de dispositivos espúrios em redes corporativas. Contudo, existem controles capazes de limitar a quantidade de endereços físicos permitidos por porta, bem

como limitar quais endereços MAC podem se conectar. Popularmente, essa funcionalidade é conhecida como port security, mas fabricantes diversos, geralmente, adotam nomes próprios, como é o caso do switch Extreme utilizado nesse laboratório. Nesse caso, a funcionalidade se chama MAC Locking (do inglês, travamento de MAC). Após consulta em documentação oficial do fabricante, foi realizada a ativação e configuração dessa função, limitando que cada porta pudesse ter apenas um endereço físico vinculado a ela. Nesse caso, não foi feita limitação de quais MACs podem se conectar, havendo apenas crítica quanto a quantidade figura 4.33.

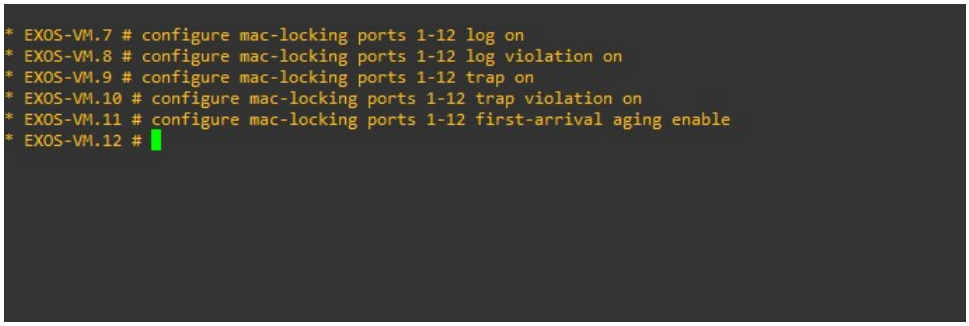

Figura 4.33: Comandos Para Ativação do MAC-Locking.

Fonte: do Autor

Após a configuração da funcionalidade, repetiu-se a conexão do segundo dispositivo no Hub e, ao contrário da primeira tentativa, houve desativação da porta, conforme coluna "Port State", com valor D - Disable, da figura 4.34:

Figura 4.34: Bloqueio de Porta Utilizada para o Ataque.

Fonte: do Autor

Esse controle faz com que essa técnica amplamente utilizada não tenha efeito para ingresso na rede alvo. Isso obriga o atacante a tentar conexão direta no switch, forçando-o a lidar com controles mais robustos como NAC. Além disso, para ter acesso a tráfego de outros dispositivos, o atacante precisaria realizar ARP ou MAC Spoofing, para alcançar o tráfego de outras portas do switch, o que produz tráfego

excessivo e aumenta as chances de detecção do ataque. Outras técnicas possíveis como double tagging, limitam a capacidade de ação do atacante, pois essa técnica pressupõe falta de resposta do alvo. Na prova de conceito para demonstração do controle CM-8, um cenário similar, mas mais complexo, é apresentado.

O controle IR-4 comprovou a hipótese H6, ao mostrar que a desabilitação automática diante de violações reduz o tempo de resposta e mitiga rapidamente ataques com dispositivos espúrios.

4.1.7 SI-4 (1) Conectar e Configurar Ferramentas de Detecção de Intrusão em um Sistema de Detecção de Intrusão para Todo o Sistema

Conforme definido pelo NIST, na publicação especial SP 800-53, o controle SI-4 trata de monitoração de sistemas e a melhoria 1 desse controle é específica em apresentar diretrizes e ressaltar a importância em implementar ferramentas de detecção de intrusos para toda a organização. Esse controle não apresenta nenhuma inovação, contudo, fornece informações básicas sobre o ambiente e os sistemas organizacionais, sobre as quais se baseiam os sistemas mais complexos. Partindo da atividade de monitorar e detectar anomalias é que medidas mais robustas podem ser implementadas, como resposta e detecção em endpoints (EDR - Endpoint Detection and Response) e Orquestação, Automação e Resposta de Segurança (SOAR - Security Orchestration, Automation and Response). O exemplo mais comum de uma dessas soluções, alimentada também por informações de sistemas IDS, talvez seja o Gerenciamento de Informações e Eventos de Segurança (SIEM - Security Information and Event Management).

Sobre o controle em questão, segundo o NIST(10), integrar ferramentas de detecção de intrusões em um sistema abrangente melhora a cobertura e a eficácia da detecção, tornando o sistema mais robusto através do compartilhamento de informações entre instâncias diversas de detecção de intrusos ou com sistemas de correlacionamento de dados e resposta a violações. Para a produção de uma prova de conceito deste controle, foi criado um laboratório, segundo a arquitetura mostrada na figura 4.35, em que os hosts foram virtualizados por Virtualbox e controlados pelo GNS3.

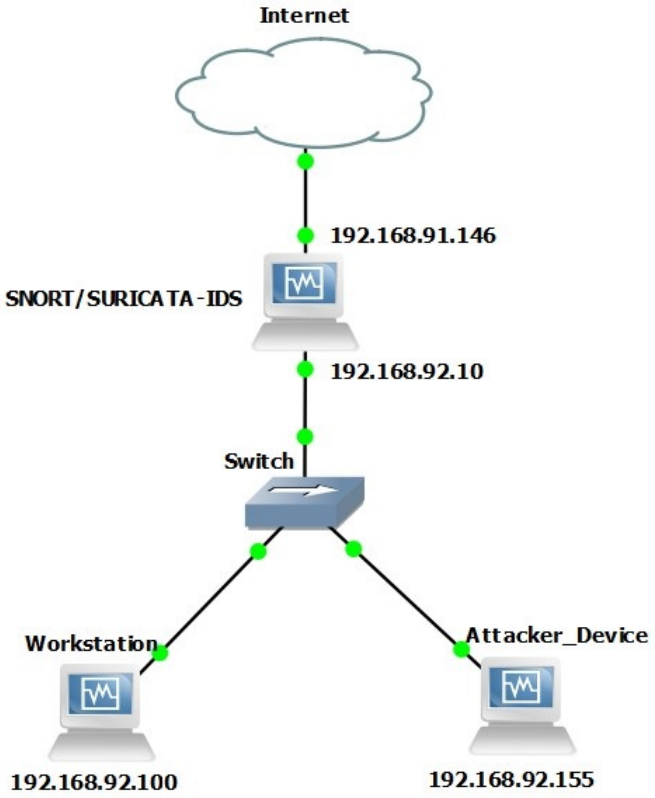

Figura 4.35: Arquitetura do Laboratório para Teste com IDS.

Fonte: do Autor

Ainda conforme a arquitetura apresentada, o host SNORT/SURICATA - IDS executa um sistema Pfsense (firewall). Nesse sistema foram instaladas duas ferramentas para detecção de intrusos, ambas open source, Snort e Suricata. O Snort é um sistema de detecção de intrusão (IDS) de código aberto e sistema de prevenção de intrusão(IPS) que realiza análise de tráfego de rede em tempo real e registro de pacotes de dados. O Snort utiliza uma linguagem baseada em regras que combina métodos de inspeção de anomalias, protocolos e assinaturas para deteccção de atividades potencialmente maliciosas. O Snort depende da presença de regras para identificar comportamentos típicos de intrusos, essas regras consistem em duas seções principais: (1) O cabeçalho da regra define a ação a ser tomada sobre qualquer tráfego correspondente, bem como os protocolos, endereços de rede, números de porta e direção do tráfego ao qual a regra deve aplicar. (2) A seção do corpo de regras define a mensagem associada a uma determinada regra e, mais importante, os critérios de carga útil (payload) e não-carga útil que precisam ser atendidos para que uma regra corresponda (59). Embora as opções de regras não sejam necessárias, elas são essenciais para garantir que uma dada regra tenha eficácia em identificar determinado tráfego. Abaixo, na figura 4.36, é demonstrado um exemplo de regra Snort:

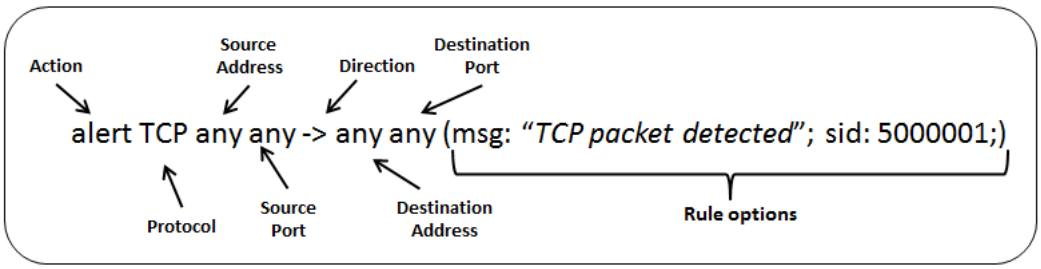

Figura 4.36: Formato de Regra do Snort.

Fonte: Internet(59)

Da esquerda para a direita, é possível verificar os valores de (1) ação a ser tomada (Action), (2) protocolo utilizado (Prococol), (3) endereço de origem (Source Address), (4) porta de origem (Source Port), (5) direção do tráfego analisado (Direction), (6) endereço de destino (Destination Address), (7) porta de destino (Destination Port) e (8) Opções da Regra (Rule Options).

Para demonstração da ferramenta, foram importados pacotes de regras padrão, oferecidos no repositório do Snort. Em seguida, deve-se escolher a interface de rede que se quer monitorar. Neste caso, foi definida a interface de rede local (LAN), para monitoração e identificação de ataques internos. A partir disso, utilizando o host Workstation, com sistema operacional Linux, foram conduzidos ataques de força bruta contra a própria aplicação WEB para gerência do Firewall PfSense. Esse ataque foi realizado utilizando a ferramenta gobuster para descoberta de diretórios ocultos na console WEB do firewall, utilizando um dicionário com palavras-chave típicas de nomes de diretórios. O objetivo desse ataque é apenas gerar um alto número de requisições HTTP contra o alvo. O tipo de ataque a ser realizado nesse caso, não é relevante, de forma que o objetivo é apenas gerar comportamento similar a outros tipos de escanemanento de rede. Ataques internos podem ou não gerar alto ruído na rede, nesse sentido, a qualidade da regra para cada cenário determina a capacidade de identificar ou não o ataque. Após a simulação de ataque contra o Firewall, ao verificar os alertas do Snort, conforme figura 4.37, é possível ver os metadados sobre cada requisição identificada e a descrição do motivo do alerta (Campo Description).

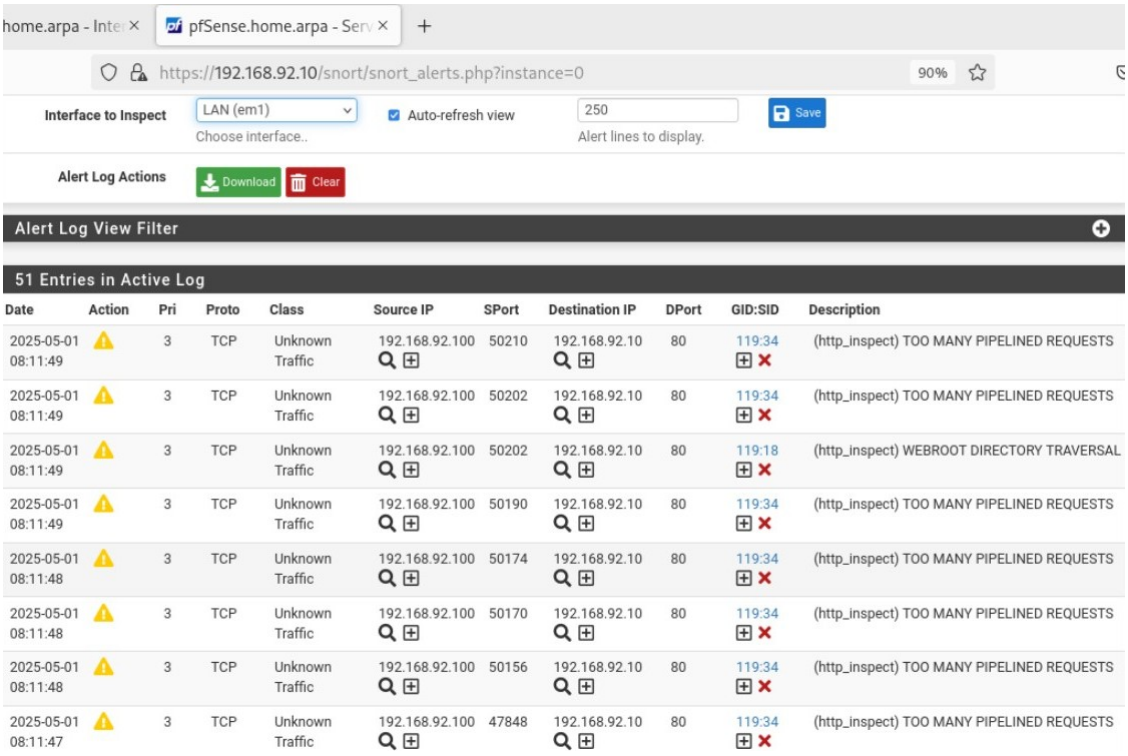

Figura 4.37: Tela de Alertas do Snort com Evidências de Anomalias.

Fonte: do Autor

De forma similar, foi instalada a ferramenta Suricata no host SNORT/SURICATA - IDS. Apesar de ser construído com arquitetura diferente, o Suricata se comporta de forma similar ao Snort e pode utilizar as mesmas assinaturas para identificação de tráfego malicioso. Nesse caso, foi conduzido um ataque diferente para geração de um alerta diverso. A partir do host AttackerDevice, foi realizado ataque de força bruta contra um serviço de Transferência de Arquivos (FTP) no host Workstation. Para o ataque, foi utilizada a ferramenta Hydra, que é capaz de realizar força bruta para descoberta de credenciais de acesso. Na figura 4.38 pode ser visto o alerta na ferramenta Suricata.

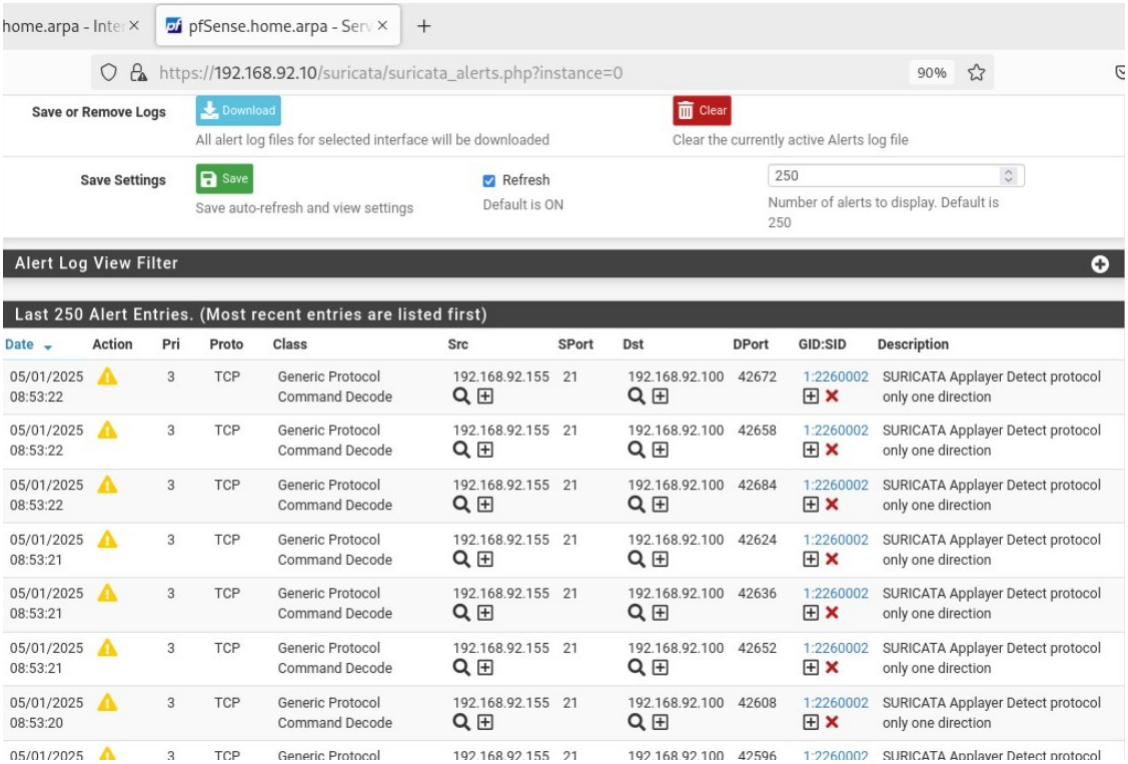

Figura 4.38: Tela de Alertas do Suricata com Evidências de Anomalias.

Fonte: do Autor

Assim, fica demonstrado que ferramentas de detecção de intrusos são capazes de gerar alertas valiosos para monitoração simples ou para alimentação de ferramentas mais robustas, como SIEM. Nesse caso, os alertas de ambas as ferramentas podem ser coletados para geração de painéis mais complexos ou insumos para ferramentas de resposta ativa. Dessa forma, confirma-se a hipótese H7, uma vez que a integração dessas soluções aumentou a capacidade de identificar tráfego anômalo gerado por dispositivos espúrios e possibilitou respostas em tempo quase real às tentativas de ataque.

4.2 SÍNTESE DOS AMBIENTES E RECURSOS UTILIZADOS NAS PROVAS DE CONCEITO

Com o objetivo de consolidar os dados apresentados ao longo das subseções anteriores, foi elaborada uma tabela-resumo contendo os principais softwares, tecnologias e comandos empregados na execução das provas de conceito. Essa síntese permite visualizar de forma estruturada os elementos técnicos que compuseram o ambiente laboratorial, bem como os controles avaliados segundo a taxonomia do NIST SP 800-53. A organização dessas informações possibilita correlacionar, de maneira direta, cada controle com as ferramentas e configurações utilizadas em sua validação prática.

Além de facilitar a rastreabilidade metodológica, a tabela proporciona uma visão integrada das camadas de defesa contempladas — desde a autenticação e inventário de dispositivos até a detecção e resposta automatizada a incidentes. Tal consolidação reforça a natureza experimental e aplicada deste trabalho,

demonstrando a coerência entre os objetivos definidos, as implementações realizadas em laboratório e os resultados posteriormente analisados no capítulo seguinte.

Tabela-Resumo dos Ambientes Criados em Laboratório			
Prova de Conceito / Controle	**Código NIST**	**Softwares e Tecnologias Utilizadas**	**Comandos/Funcionalidades Executados**
Monitorar o uso das contas	AC-2 (g)	Adaxes Directory Management, Windows Server 2022, Windows 10, Active Directory	Integração do Adaxes com AD; Geração de relatórios no Adaxes
Monitorar e controlar métodos de acesso remoto	AC-17 [1]	Firewall Pfsense 2.7.2, Debian 12, Extreme Switch	SSH paulo@192.168.91.55; bloqueios seletivos de IP no Pfsense
Proibir conexão de hardware não autorizado	CM-7 (9)(b)	Kali Linux, lsusb, USBGuard	lsusb; usbguard watch; usbguard list-devices -b; usbguard block-device -p 0951:1603
Inventário de componentes de sistema	CM-8 (a)	Zabbix Server e Agent 7.0, Switch Extreme (SNMPv2), Debian	install zabbix-agent; Comandos Figura 4.14; Criação de Hosts no Zabbix Figura 4.15/4.16; arp-scan –localnet
Autenticação de dispositivos (MACsec)	IA-3 [1]	Debian Linux 12, Parrot OS, ip macsec, Wireshark	Comandos da figura 4.23
Desabilitar recursos em caso de violação (MAC Locking)	IR-4 (5)	Switch Extreme, Debian Linux 12	Comandos das figuras 4.31, 4.32, 4.33 e 4.34
Detecção de intrusão (IDS)	SI-4 (1)	Snort, Suricata, PfSense 2.7.2, Linux Debian 12	Utilização de regras pré-definidas para Snort e Suricata, conforme Figuras 4.37 e 4.38

Tabela 4.1: Informações consolidadas dos laboratórios implementados.

4.3 LIMITAÇÕES PRÁTICAS DAS PROVAS DE CONCEITO

As provas de conceito executadas em laboratório demonstraram, de forma controlada, a viabilidade técnica dos controles propostos no contexto de mitigação de ataques como os estudados neste trabalho. No entanto, sua aplicação em ambientes corporativos de grande porte apresenta desafios relacionados a custos, complexidade de integração e escalabilidade operacional. Cada controle implementado — embora eficaz em seu escopo — impõe requisitos técnicos e organizacionais que precisam ser considerados de forma criteriosa antes da adoção em escala produtiva.

No caso do AC-2 (Monitorar o uso das contas), a limitação principal decorre da dependência de infraestrutura de diretórios atualizada, servidores redundantes e ferramentas corporativas de auditoria (como o Adaxes ou módulos avançados do Active Directory). Em ambientes de centenas de milhares de contas, a coleta e correlação de logs de logon podem gerar sobrecarga no controlador de domínio e exigir soluções complementares de SIEM. Os custos operacionais incluem licenciamento por usuário e armazenamento de registros de longa retenção, o que torna essencial a definição de janelas de retenção otimizadas e filtros de auditoria seletivos para evitar desperdício de recursos computacionais e de armazenamento.

Para o AC-17 [1] (Monitorar e controlar métodos de acesso remoto), a limitação mais evidente está na necessidade de políticas de firewall e VPN unificadas, capazes de diferenciar acessos legítimos e suspeitos. A implementação de mecanismos automatizados de bloqueio e registro, embora tecnicamente viável, exige integração com sistemas de autenticação federada, servidores RADIUS e módulos de resposta orquestrada (SOAR). Essa interdependência aumenta o custo de integração e a complexidade de manutenção, pois

qualquer ajuste na infraestrutura de rede pode demandar revalidação de políticas e regras. Em termos de escalabilidade, a inspeção constante de sessões remotas pode gerar latência perceptível em ambientes com alto volume de conexões simultâneas.

O controle CM-7 (9)(b) (Proibir conexão de hardware não autorizado), demonstrado com ferramentas nativas do Linux (como lsusb e usbguard), depende de uma infraestrutura de endpoint management madura para ser efetivo em larga escala. A detecção de dispositivos exige monitoração contínua de portas USB e interfaces físicas, o que pode se tornar impraticável em milhares de estações de trabalho heterogêneas. Além disso, políticas muito restritivas podem gerar incidentes de indisponibilidade e aumento de chamados de suporte técnico. O custo de implementação desse controle reside mais na gestão de políticas e na compatibilidade entre sistemas operacionais do que em investimentos diretos em software.

O CM-8 (Inventário de componentes de sistema), implementado com Zabbix e SNMPv2, apresentou bom desempenho em ambiente controlado, mas enfrenta limitações de escalabilidade em redes extensas, sobretudo quanto à saturação de tráfego SNMP e à necessidade de manutenção contínua dos agentes de monitoração. Em redes com milhares de dispositivos, é comum ocorrer perda parcial de dados ou atrasos na atualização dos inventários. Além disso, a precisão do inventário depende da consistência da convenção de nomes e do controle de endereçamento, exigindo governança de ativos bem estruturada e integração com bancos de dados de configuração (CMDBs corporativos). O custo de infraestrutura aumenta proporcionalmente ao número de dispositivos monitorados e ao tamanho do banco de dados de histórico de métricas.

O IA-3 [1] (Autenticação de dispositivos por MACsec), apesar de tecnicamente robusto, apresenta o conjunto mais evidente de limitações práticas. A implementação do IEEE 802.1AE requer switches e NICs compatíveis, suporte a MKA (MACsec Key Agreement) e, em muitos casos, licenciamento adicional de firmware. Em redes legadas, a substituição de equipamentos pode representar investimento substancial. Além disso, a administração de chaves e certificados entre milhares de dispositivos traz elevada complexidade operacional. A sincronização com mecanismos 802.1X e servidores RADIUS aumenta a carga administrativa e pode impactar o desempenho das portas de acesso. A escalabilidade plena do MACsec, portanto, depende de planejamento progressivo e de infraestrutura moderna com suporte nativo ao padrão.

O controle IR-4 (5) (Desabilitar automaticamente recursos em caso de violação), demonstrado por meio do MAC-Locking em switches EXOS, também possui limitações significativas em ambientes produtivos. O bloqueio automático de portas com base em violações de endereço MAC é uma estratégia eficaz em laboratório, mas em redes reais pode causar indisponibilidades indesejadas caso políticas de exceção não estejam bem definidas. A operação desse tipo de automação requer calibração cuidadosa e integração com sistemas de tickets e SIEM, para evitar falsos positivos que resultem em paralisações de usuários legítimos. O custo de adoção é relativamente baixo em hardware compatível, mas o custo operacional de monitoramento e ajuste fino é elevado, especialmente em redes distribuídas geograficamente (WAN).

Por fim, o SI-4 (1) (Ferramentas de detecção de intrusão integradas ao sistema) demonstrou alta eficácia técnica, mas traz desafios de custo e escalabilidade significativos. Soluções baseadas em Snort e Suricata demandam poder computacional proporcional ao volume de tráfego analisado, exigindo servidores dedicados, segmentação de sensores e armazenamento volumoso de logs. A manutenção de assinaturas e o treinamento de analistas para ajustar regras reduzem a taxa de falsos positivos, mas aumentam o custo hu-

mano e a complexidade operacional. Além disso, em redes de grande porte, a necessidade de correlacionar alertas entre múltiplos sensores requer integração robusta com SIEM e orquestradores de resposta.

Em resumo, todos os controles validados em laboratório mostraram-se eficazes para os objetivos de mitigação do problema estudado; contudo, sua implementação em larga escala demanda planejamento gradual, padronização de infraestrutura, treinamento contínuo e mecanismos de automação que reduzam o impacto operacional. A proposta de priorização de controles, portanto, deve ser interpretada não apenas sob o prisma técnico, mas também sob a ótica de viabilidade econômica e sustentabilidade administrativa, garantindo que o modelo de segurança em profundidade se mantenha eficiente e exequível no longo prazo.

4.4 PORQUE IMPLEMENTAR CONTROLES DE SEGURANÇA EM AMBIENTE DE TESTES

Testar medidas de segurança em laboratório antes de sua implementação em ambientes reais é vital para testar a eficácia e a confiabilidade das soluções adotadas. Em um ambiente controlado, é possível simular diferentes cenários de ataque, falhas de sistema e comportamentos inesperados sem colocar em risco dados sensíveis ou a continuidade das operações. Isso permite que sejam identificadas vulnerabilidades, configurações sejam ajustadas e a performance das ferramentas de proteção seja testada com maior precisão e segurança.

Além disso, o ambiente de testes oferece um espaço para experimentação e aprendizado, onde novas tecnologias e estratégias podem ser avaliadas e comparadas fora de um ambiente de produção. Essa abordagem reduz significativamente os riscos de incidentes cibernéticos, evita prejuízos financeiros e protege a reputação da organização. Portanto, executar testes de soluções complexas em ambiente segregado, antes da implementação real, é uma boa prática de segurança.

5 ANÁLISE DE RESULTADOS

A estratégia de validação dos resultados foi concebida de forma bifásica, contemplando tanto a avaliação em laboratório quanto a análise em ambiente real. No primeiro momento, os controles foram implementados em um ambiente laboratorial controlado, possibilitando a observação direta de sua eficácia técnica frente a cenários de ataque simulados com dispositivos compactos. Essa etapa forneceu dados objetivos e empiricamente mensuráveis sobre a capacidade de cada controle em prevenir, detectar, mitigar e responder a ameaças específicas. Em um segundo momento, buscou-se projetar e analisar como esses mesmos controles se comportariam em cenários reais de produção, considerando variáveis adicionais como escala de usuários, diversidade de ativos, custos operacionais e integração com sistemas legados. Dessa forma, a validação combinada permitiu não apenas verificar a viabilidade prática das soluções propostas em condições experimentais, mas também discutir sua aplicabilidade e relevância em contextos corporativos reais, equilibrando rigor científico e utilidade prática.

Este capítulo apresenta e analisa os resultados obtidos com a implementação prática de parte dos controles propostos (Conforme Tabela 3.2) em um ambiente corporativo real. Novamente, ressalta-se que para cada caso exige-se adaptação e estudos comparativos para a escolha mais assertiva dos controles a serem implementados e quais tecnologias deve-se utilizar. Nesse sentido, com o objetivo de avaliar a aplicabilidade e a eficácia da proposta em um contexto real, foram selecionados e implementados 20 controles extraídos da proposta apresentada neste trabalho. A aplicação prática ocorreu em uma empresa pública brasileira do setor financeiro, que tem sido alvo recorrente de ataques com dispositivos compactos. Para isso, foram adotados controles específicos (utilizando tecnologias disponíveis na instituição) selecionados com base em análise de riscos da empresa, histórico de incidentes e capacidade operacional da organização, conforme apresentado na Tabela 3.2:

1. Monitorar o uso das contas de usuário: Monitoramento de horários, locais e dispositivos utilizados para login, realizado com Active Directory e Azure Entra.

2. Empregar mecanismos automatizados para monitorar e controlar métodos de acesso remoto: Utilização de Firewalls para monitorar conexões não autorizadas de entrada de saída de protocolos de acesso remoto, como SSH e RDP.

3. Correlacionar e analisar informações geradas por avaliações de controle e monitoramento: Criação de regras SIEM para identificação de padrões de ataques, como varreduras de rede.

4. Empregar um agente ou equipe de teste de penetração independente para realizar testes de penetração no ambiente: Para identificação proativa de vulnerabilidades que possam ser exploradas no futuro.

5. Empregar exercícios de redteam para simular tentativas de adversários de comprometer os sistemas e ambientes organizacionais: Foi realizado exercício de intrusão física e cibernética, para simular o ataque com Raspberry Pi, em departamento aleatório da organização, para entender o comportamento dos colaboradores e a capacidade de resposta das contramedidas de segurança.

6. Autorizar conexões internas ao ambiente apenas de componentes predefinidos: Autenticação via padrão IEEE 802.1x, apenas de dispositivos legítimos.

7. Proibir o uso ou conexão de componentes de hardware não autorizados: Portas de Switch em modo de bloqueio, em caso de não autenticação e bloqueio de dispositivos USB, por padrão.

8. Desenvolver e documentar um inventário de componentes do sistema que reflita com precisão o ambiente: Criação e gerenciamento do inventário por ferramentas como Zabbix e Active Directory SCCM. Essa medida possibilita melhor observabilidade dos ativos legítimos em relação aos dispositivos espúrios.

9. Identificar e autenticar dispositivos definidos pela organização antes de estabelecer uma conexão de rede: Reforço de configuração do Controle de Admissão à Rede (NAC) para pré-admissão, baseada em certificados digitais.

10. Identificar e autenticar dispositivos | Autenticação de rede Bidirecional: Autenticação 802.1x com EAP-TLS, utilizando certificados digitais e PEAP. Essa medida é importante para coibir spoofing de endereços físicos.

11. Fornecer treinamento de resposta a incidentes sobre como identificar e responder a uma violação, incluindo o processo da organização para relatar uma violação: Treinamentos rotineiros para times diversos, com reforço sobre as formas de reporte em caso de alarme.

12. Implementação de rotina para desabilitar automaticamente um recurso caso violações de segurança sejam detectadas: Port Violation habilitado em caso de mais de um endereço físico ser identificado em uma mesma porta de switch.

13. Estabelecer um processo para autorização do pessoal de manutenção e manter uma lista de entidades ou pessoal de manutenção autorizado: Reforço nas políticas de acesso físico.

14. Desenvolver, aprovar e manter uma lista de usuários com acesso às instalações onde o sistema reside: Acesso físico mais rigoroso com redefinição de políticas.

15. Acompanhar visitantes e controlar suas atividades que exigem escolta e controle: Acesso físico mais rigoroso com redefinição de políticas.

16. Empregar guardas para controlar os pontos de acesso físico às instalações onde o sistema reside, 24 horas por dia, 7 dias por semana: Acesso físico mais rigoroso, em ambientes críticos (como datacenter), com redefinição de políticas.

17. Fornecer a capacidade de isolar dinamicamente o ambiente de outros componentes do sistema: Criação de listas de controle de acesso dinâmicas (dACL) para isolamento, microsegmentação e contenção de dispositivos, em caso de violação de regras de segurança.

18. Monitorar o sistema para detectar conexões locais e remotas não autorizadas: Monitoramento via CISCO ISE + SIEM para monitoramento de limite de MACs conectados em conexões locais e conexões extranet.

19. Conectar e configurar ferramentas de detecção de intrusão em um IDS para todo o ambiente: Uso de IDS para identificação de indicadores de comprometimento (IoC) e monitoramento de volumetria do tráfego da rede.

20. Analisar o tráfego de comunicações e os padrões de eventos do sistema: Uso de IDS para identificação de indicadores de comprometimento (IoC) pelo tráfego da rede.

Considerando os números identificadores atribuídos a cada controle na lista acima, o gráfico 5.1 a seguir ilustra o grau de complexidade de implementação dos controles de segurança no ambiente real, tomando como referência o caso concreto analisado. O grau de complexidade (azul) foi classificado de zero (menor complexidade) a dez (maior complexidade). A avaliação empírica foi conduzida considerando não apenas os aspectos técnicos de cada solução, mas também os custos efetivos identificados incluindo aquisição, operação e necessidade de infraestrutura adicional, o nível de complexidade operacional enfrentado durante os testes e a própria implementação, como dependências entre sistemas, requisitos de integração e possíveis impactos no tráfego de rede; a necessidade de pessoal especializado para sua manutenção, envolvendo capacitação contínua, tuning de regras e monitoramento ativo; e a extensão do parque tecnológico envolvido, que afeta diretamente a escalabilidade, a distribuição geográfica dos equipamentos, a heterogeneidade dos dispositivos e o esforço necessário para aplicar o controle de forma uniforme em toda a rede.

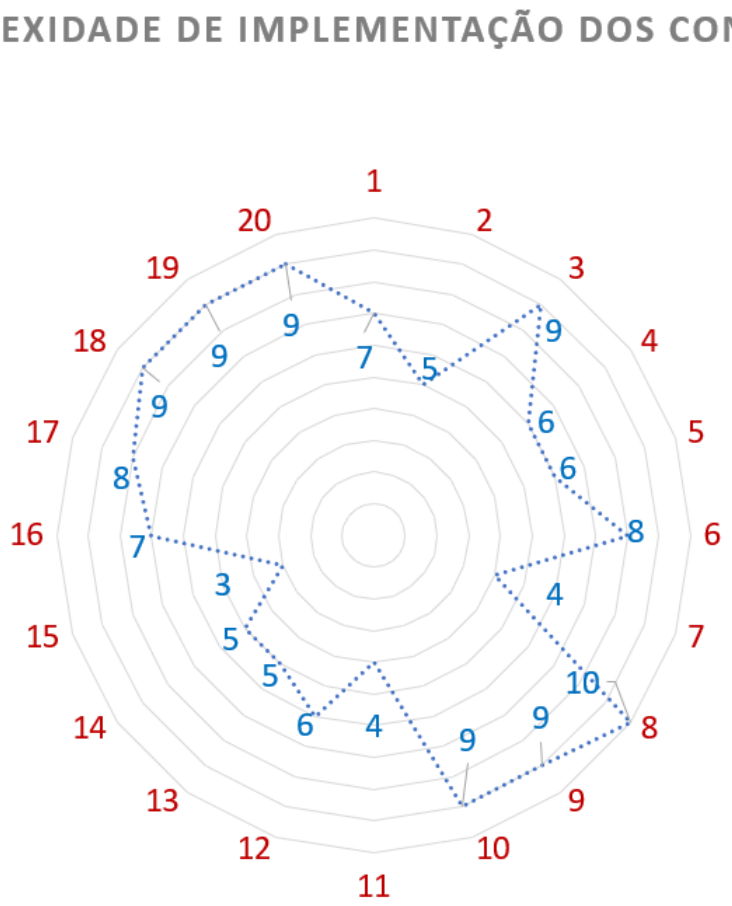

Figura 5.1: Grau de complexidade de implementação cada controle

Fonte: do Autor

Após a realização de testes em ambiente controlado (laboratório), as medidas selecionadas foram implementadas em ambiente real entre agosto de 2023 e setembro de 2024. Durante o ano de 2023, foram identificados e recolhidos 30 dispositivos Mikrotik e Raspberry Pi, todos conectados, de alguma forma, à rede corporativa da organização. Esses incidentes ocorreram antes da implementação efetiva das medidas de controle propostas neste trabalho. Já em 2024, com os controles parcialmente implementados e operacionais, foi possível detectar 28 dispositivos similares, que não chegaram a estabelecer conexões efetivas com os ativos da organização, conforme ilustrado na Figura 5.2. Assim, embora não tenha havido redução significativa da quantidade de tentativas de intrusão, houve mitigação quase completa dos impactos dessas tentativas, de 30 para apenas 1 caso, ou 96,67%. Nesses casos, os dispositivos geraram apenas alertas nos sistemas de monitoramento, permitindo ações preventivas e respostas rápidas por parte da equipe de segurança. Houve apenas um caso de conexão bem-sucedida, no qual ocorreu roubo de credenciais e acesso não autorizado a sistemas internos. Apesar da gravidade do incidente isolado, os resultados indicam redução significativa da superfície de ataque e aumento da capacidade de detecção precoce, refletindo a eficácia dos controles adotados.

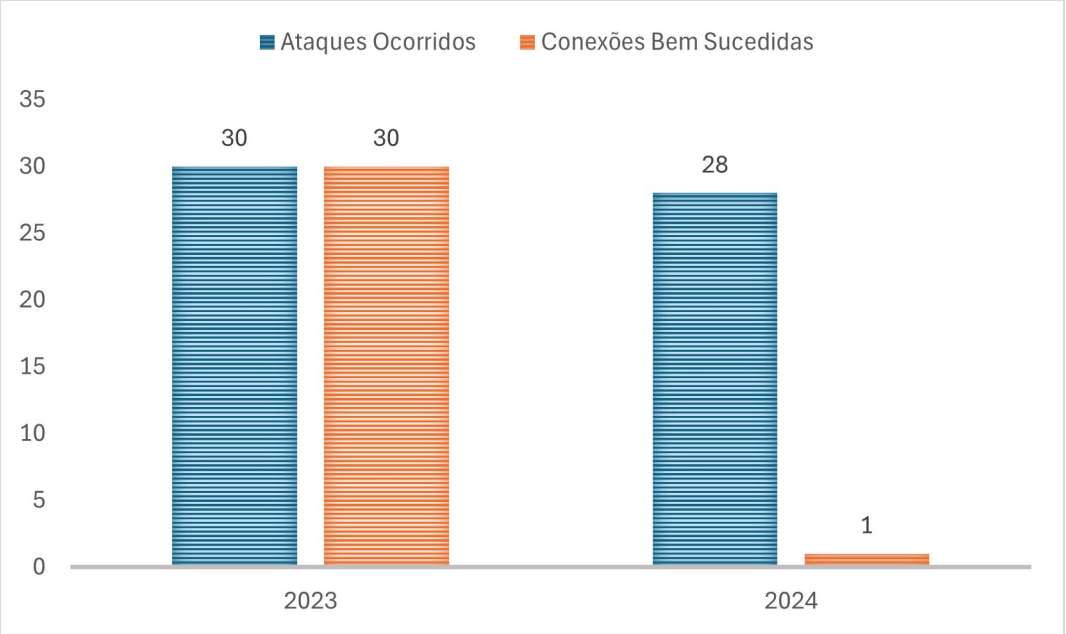

Figura 5.2: Comparação de Ataques Ocorridos e Bem-sucedidos, Antes e Após Implementação de Controles em um Cenário Real

Fonte: do Autor

Durante os incidentes registrados em 2024, observou-se que diversos controles implementados no ambiente de testes não atuaram de forma isolada, mas sim em complementaridade, reforçando a eficácia do modelo de defesa em profundidade. É importante destacar que a sobreposição de números observada na análise reflete justamente essa atuação conjunta, em que múltiplos controles reagiram ao mesmo incidente, ampliando a capacidade de identificar, mitigar e responder de forma mais eficaz às ameaças enfrentadas. No gráfico 5.3 evidencia como foi a distribuição da atuação dos controles implementados face aos incidentes registrados.

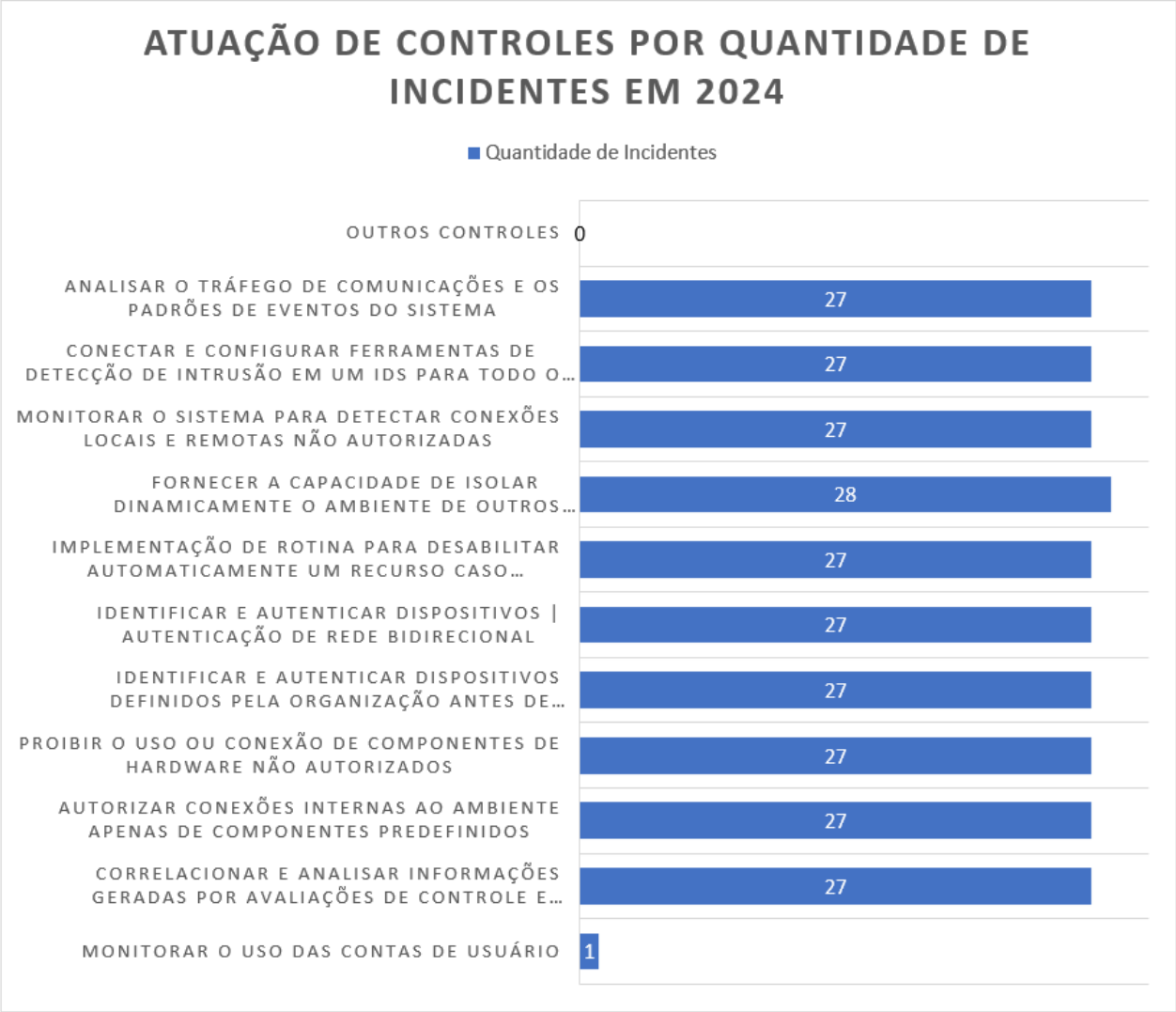

Figura 5.3: Distribuição de atuação de controles em relação aos incidentes registrados em 2024

Fonte: do Autor

Os resultados obtidos com a implementação real desses controles indicaram também impacto direto em indicadores como MTTR - Mean Time to Respond (Tempo Médio de Resposta) e MTTD - Mean Time to Detection (Tempo Médio de Detecção) que foi reduzido para milisegundos (Anteriormente, não haviam dados quanto a essas métricas, pois a identificação era quase sempre acidental e feita por inspeção visual), especialmente devido à maior automação e visibilidade introduzidas nos ambientes monitorados. Com a implementação dessas medidas em ambiente real, os incidentes deixaram de ser identificados, na maioria dos casos, após dias ou até semanas — quando a detecção dependia exclusivamente da identificação visual desses dispositivos espúrios conectados à rede — para serem detectados em tempo quase real. Essa evolução foi viabilizada, principalmente, (1) pela adoção de ferramentas automatizadas de detecção de dispositivos não autorizados e bloqueio de portas de rede e (2) pela integração com uma plataforma SIEM. Esses avanços demonstram que mesmo medidas de baixo custo, quando bem estruturadas, podem elevar a capacidade de resposta a ameaças em redes locais.

5.1 AVANÇOS ALCANÇADOS EM RELAÇÃO AOS TRABALHOS CORRELATOS

Os estudos correlatos revisados discutem componentes importantes — p.ex., IDS/IPS, 802.1X/NAC e a necessidade de priorizar controles — mas, em geral, tratam-nos de forma isolada ou genérica, sem focar o vetor específico de inserção física de dispositivos compactos (Raspberry Pi/Mikrotik) em redes cabeadas e sem ofertar um portfólio priorizado de contramedidas direcionadas a esse problema. Esta dissertação avança esse estado da arte ao (i) modelar o ataque com base em attack-tree (Schneier) para explicitar caminhos e condições do comprometimento, e (ii) selecionar e organizar controles a partir do NIST SP 800-53 de modo cíclico e justificado, mirando mitigação direta das etapas do ataque — em vez de uma adoção genérica de boas práticas.

Além do recorte teórico, há avanço empírico: as provas de conceito e a aplicação parcial em cenário real mostram que, após a adoção de medidas automatizadas (inventário/descoberta de dispositivos não autorizados, bloqueio de portas) integradas a SIEM, a detecção de dispositivos espúrios passou de dias/semanas (dependente de identificação visual) para quase tempo real, evidenciando ganho prático relevante que os trabalhos correlatos não quantificam. Este trabalho também explicita métricas e diretrizes de avaliação, o que torna possível conectar resultados a indicadores de desempenho organizacionais.

Metodologicamente, o trabalho consolida um artefato (portfólio priorizado) construído e avaliado sob Design Science Research e Ciclo Regulador de Wieringa — aportando estrutura e rastreabilidade entre problema, solução e avaliação, algo pouco presente nos correlatos analisados. Em síntese, o avanço reside em: (1) foco no vetor físico-compacto com modelagem explícita do ataque; (2) priorização justificada de controles do NIST com variedade (técnicos, administrativos, operacionais) e cobertura das fases prevenir-detectar-mitigar-responder; e (3) evidência empírica de eficácia em laboratório e sinais de efetividade em ambiente real, reduzindo sensivelmente o tempo de detecção e resposta — uma ponte concreta entre teoria e prática que eleva o patamar frente ao estado da arte.

6 CONCLUSÕES E TRABALHOS FUTUROS

Considerando o cenário alarmante e o crescente número de ataques que exploram dispositivos compactos e furtivos, esta pesquisa desenvolveu uma proposta de controles de segurança prioritários, especificamente voltados ao tratamento desse vetor de ameaça. A principal contribuição metodológica está no uso da Design Science Research (DSR), fundamentada em Hevner e Wieringa, para construir e avaliar um artefato — um portfólio priorizado de controles — capaz de endereçar um problema real e recorrente em ambientes corporativos. Do ponto de vista prático, foram priorizados controles com base no NIST SP 800-53 e validados em provas de conceito (PoCs) envolvendo tecnologias como SIEM/IDS, MACsec, NAC, inventário/descoberta e bloqueios automáticos, com evidências obtidas em cenários reais. No campo científico, o estudo avança ao preencher uma lacuna pouco explorada, pois poucos trabalhos abordam explicitamente ataques com dispositivos compactos físicos em redes internas com validação prática em múltiplas camadas de defesa. Além disso, a pesquisa oferece valor reutilizável ao propor critérios de priorização e roteiros de PoC que podem ser aplicados em diferentes contextos corporativos. Por fim, constatou-se que, ao reduzir o conjunto de controles a ser considerado com base em critérios técnicos e operacionais, o processo de tratamento de vulnerabilidades torna-se mais assertivo, eficiente e alinhado à realidade dos ambientes analisados.

Conclui-se, portanto, que é imprescindível um aprofundamento contínuo sobre ameaças específicas, não apenas devido ao surgimento constante de novas metodologias e variações de ataque, mas também pela necessidade de compreender em profundidade as técnicas de intrusão para fortalecer as bases de recomendações mais eficazes de contramedidas. Com isso, constata-se que a resposta a essas ameaças requer medidas específicas de identificação, mitigação e detecção, que devem ser atualizadas e ajustadas conforme cada cenário. As limitações e os objetivos específicos deste trabalho concentraram-se na análise de ataques cibernéticos que, apesar de causarem alto impacto em diferentes tipos de organizações, ainda carecem de visibilidade e não são amplamente discutidos na literatura. Além do estudo aprofundado desses ataques, buscou-se também reunir e sistematizar contramedidas eficazes com base em um framework amplamente utilizado e recomendado, contribuindo assim para o fortalecimento das práticas de segurança da informação.

Ressalta-se que a pesquisa possui limitações, como a restrição parcial das provas de conceito (POCs) a ambientes laboratoriais controlados, o que pode não refletir integralmente a complexidade de redes corporativas reais. Também não foram realizados estudos aprofundados de custos para implementação ou manutenção dos controles sugeridos, e não houve testes em larga escala e em diferentes segmentos corporativos e industriais, o que limita a abrangência e a generalização dos resultados. Apesar dessas limitações, a pesquisa contribui ao aplicar a Design Science Research (DSR) na criação de um portfólio priorizado de controles e, de forma prática, ao propor um modelo baseado no NIST SP 800-53, que orienta organizações na mitigação de ataques com dispositivos compactos em redes cabeadas.

Como trabalhos futuros, sugere-se incrementar a proposta, testando e implementando outros possíveis controles como: Uso de mapas de calor para identificação de conexões 3G/4G/5G para acesso remoto aos dispositivos maliciosos; Criação de inventário de dispositivos com base em outras técnicas, como

fingerprint de dispositivos utilizando SNMP ou outro protocolo, por exemplo; Implementação de novas tecnologias como ZTNA (Zero Trust Network Access) para controle do acesso mais granular e preciso aos recursos de rede. Também se aponta como promissor o uso de técnicas de Inteligência Artificial associadas aos controles sugeridos, potencializando a eficácia e eficiência por meio de mecanismos autônomos de detecção e resposta. Outra vertente relevante é a simulação de cenários mais complexos, que permitam validar a resiliência das propostas em contextos adversos e dinâmicos.

A proposta mostra-se especialmente útil em redes IoT e 6G, onde a alta densidade de dispositivos, o acesso facilitado a endpoints e, em alguns casos, o isolamento geográfico ampliam significativamente a superfície de ataque. Controles como inventário contínuo, fingerprinting de dispositivos, autenticação forte e monitoramento em tempo real tornam-se essenciais para identificar equipamentos espúrios ou comprometidos em ambientes de comunicação massiva e baixa latência. Nesse sentido, um trabalho futuro promissor consiste em adaptar e estender o modelo de defesa em profundidade para cenários IoT/6G, avaliando sua eficácia em arquiteturas distribuídas, dispositivos de baixa capacidade computacional e redes avançadas de borda, de modo a desenvolver um framework abrangente e escalável para proteção contra inserção física de dispositivos compactos nesses ecossistemas emergentes.

Por fim, destaca-se a necessidade de maior foco em segurança da cadeia de suprimentos, incluindo a verificação da integridade de firmwares de ativos de rede, que possa avaliar os possíveis riscos de backdoors de acesso às redes corporativas. Como desdobramento futuro, também recomenda-se transformar o conjunto de controles priorizados e o modelo de defesa em profundidade aqui proposto em um framework estruturado, capaz de orientar de forma padronizada a prevenção, detecção e resposta a intrusões físicas com dispositivos compactos em redes locais.

REFERÊNCIAS BIBLIOGRÁFICAS

1 PANKOV, N. *DarkVishnya attacks from inside*. Kaspersky, 2018. Acessado em: 2018-20-09. Disponível em: <https://www.kaspersky.com/blog/dark-vishnya-attack/24867/>.

2 NOGUEIRA, LUIZ. *Laboratório da NASA é hackeado com ajuda de um Raspberry Pi*. Olhar Digital, 2019. Acessado em: 2024-21-09. Disponível em: <https://dev.olhardigital.com.br/ciencia-e-espaco/laboratorio-da-nasa-tem-sistema-invadido-por-meio-de-um-raspberry-pi/>.

3 LEITÃO, LESLIE. *Operação mira quadrilha que hackeava agências bancárias no RJ*. G1, 2024. Acessado em: 20124-21-09. Disponível em: <https://g1.globo.com/rj/rio-de-janeiro/noticia/2024/07/08/operacao-mira-quadrilha-que-hackeava-agencias-bancarias.ghtml>.

4 PINHEIRO, MIRELLE e CARONE, CARLOS. *Hackers invadem sistema do INSS e geram prejuízo de R$ 1 bilhao*. Metrópoles, 2023. Acessado em: 2024-21-09. Disponível em: <https://www.metropoles.com/distrito-federal/na-mira/hackers-invadem-sistema-do-inss-e-geram-prejuizo-de-r-1-bilhao>.

5 BRASIL, P. da República Federativa do. *LEI GERAL DE PROTEÇÃO DE DADOS (Lei nº 13.709, de 14 de agosto de 2018)*. 2018. Brasília, Brasil. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>.

6 UNION, E. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. 2016. Official Journal of the European Union, L 119. Disponível em: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.

7 UNION, E. *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*. Official Journal of the European Union, L 333, 27 December 2022, 2022. Replaces Directive (EU) 2016/1148 (NIS Directive). Disponível em: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>.

8 CONGRESS, U. S. *FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014*. 2014. Public Law 113-283, 113th Congress. Amends the Federal Information Security Management Act of 2002. Disponível em: <https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf>.

9 BRASIL, P. da República Federativa do. *PLANO NACIONAL DE CIBERSEGURANÇA (PNCIBER)*. 2024. Decreto nº 11.856, de 31 de dezembro de 2023. Institui o PNCiber no Brasil. Disponível em: <https://www.in.gov.br/en/web/dou/-/decreto-n-11.856-de-31-de-dezembro-de-2023-524469461>.

10 STANDARDS, N. I. O.; TECHNOLOGY. *Security and Privacy Controls for Information Systems and Organizations*. Washington, D.C.: Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, 2020.

11 ISO. *Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação*. Rio de Janeiro, 2018.

12 CYBOK. *CYBOK – The Cyber Security Body of Knowledge*. 2024. Acessado em: 2024-05-11. Disponível em: <https://www.cybok.org/>.

13 CENTER FOR INTERNET SECURITY. *CIS Controls v8*. 2021. Acessado em: 2025-09-12. Disponível em: <https://www.cisecurity.org/controls/v8>.

14 TANENBAUM A. S; WETHERALL, D. F. N. *Redes de Computadores – 6ª*. [S.l.]: Ed. Pearson, 2021.

15 LABORATÓRIO DE ELETRÔNICA. *Figura de circuito eletrônico*. 2014. Acessado em: 21 maio 2025. Disponível em: <https://labdeeletronica.com.br/wp-content/uploads/2014/03/figura1.jpg>.

16 FORTINET. *Network Access Control: o que é controle de acesso à rede?* 2024. Acessado em: 2024-10-11. Disponível em: <https://www.fortinet.com/br/resources/cyberglossary/what-is-network-access-control/>.

17 CLOUDRADIUS. *The components of 802.1X*. 2023. Acessado em: 2025-09-08. Disponível em: <https://cloudradius.com/wp-content/uploads/2023/03/Graphic-4-1.jpg>.

18 IBM. *O que é gerenciamento de eventos e informações de segurança (SIEM)?* 2024. Acessado em: 2024-12-11. Disponível em: <https://www.ibm.com/br-pt/topics/siem/>.

19 RESEARCHGATE. *Improving SIEM capabilities through an enhanced probe for encrypted Skype traffic detection — Scientific Figure*. 2017. Acessado em: 2025-09-09. Disponível em: <https://www.researchgate.net/figure/A-classical-architecture-of-a-SIEM-system_fig1_320821171>.

20 JUNIPER NETWORKS. *O que é o IDS e o IPS?* 2024. Acessado em: 2024-12-11. Disponível em: <https://www.juniper.net/br/pt/research-topics/what-is-ids-ips.html/>.

21 TOPS HONG KONG. *Intrusion Detection System versus Intrusion Prevention System*. n.d. Acessado em: 2025-09-08. Disponível em: <https://www.tops.hk/images/ips-and-ids-in-network-security.png>.

22 IEEE. *IEEE Standard for Local and metropolitan area networks–Media Access Control (MAC) Security*. Nova Iorque, NY, 2018.

23 KEYSIGHT TECHNOLOGIES. *MACsec Hardware Testing Diagram*. 2020. Acessado em: 2025-09-08. Disponível em: <https://www.keysight.com/blogs/en/tech/traf-gen/2020/08/03/media_1b5226b6d18c931e43a6bd2e96207f6fceeab0f35.png>.

24 VMware, Inc. *VMware vSphere Documentation*. 2024. Acesso em: 2025. Disponível em: <https://www.vmware.com/>.

25 Oracle Corporation. *Oracle VM VirtualBox User Manual*. 2024. Acesso em: 2025. Disponível em: <https://www.virtualbox.org/>.

26 GNS3 Technologies. *GNS3 – Graphical Network Simulator*. 2024. Acesso em: 2025. Disponível em: <https://www.gns3.com/>.

27 Zabbix LLC. *Zabbix Monitoring Solution Documentation*. 2024. Acesso em: 2025. Disponível em: <https://www.zabbix.com/>.

28 Microsoft Corporation. *Active Directory Documentation*. 2024. Acesso em: 2025. Disponível em: <https://learn.microsoft.com/en-us/troubleshoot/windows-server/active-directory/active-directory-overview>.

29 Netgate. *pfSense Documentation*. 2024. Acesso em: 2025. Disponível em: <https://www.pfsense.org/>.

30 Cisco Secure. *Snort Open Source IDS/IPS*. 2024. Acesso em: 2025. Disponível em: <https://www.snort.org/>.

31 Open Information Security Foundation. *Suricata IDS/IPS/NSM*. 2024. Acesso em: 2025. Disponível em: <https://suricata.io/>.

32 Wireshark Foundation. *Wireshark Network Protocol Analyzer*. 2024. Acesso em: 2025. Disponível em: <https://www.wireshark.org/>.

33 ALSAQOUR R.; MAJRASHI, A. A. M. A. K. A. M. Defense in depth: Multilayer of security. *International Journal of Communication Networks and Information Security*, v. 13, n. 2, p. 242–248, 2021.

34 THAPA S.; MAILEWA, A. The role of intrusion detection/prevention systems in modern computer networks: A review. In: *Midwest Instruction and Computing Symposium*. Winsconsin, WI: EasyChair Preprint, 2020. v. 53.

35 BANDEIRA A. B.; NEUMANN, C. S. D. A. N. G. D. A. S. A. L. M. M. F. L. L. Modelo para utilização de fingerprints de sistemas operacionais (so) para identificar e responder a conexões não autorizadas de dispositivos iot na ausência de controle de admissão à rede (nac). *Conferências IADIS Ibero-Americanas Computação Aplicada e WWW/Internet*, Único, p. 27–34, 2023.

36 KHRAISAT A.; GONDAL, I. V. P. K. J. Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity*, v. 2, n. 20, p. 1–22, 2019.

37 IEEE. *IEEE Standard for Local and Metropolitan Area Networks—Port-Based Network Access Control*. Nova Iorque, NY, 2020.

38 VISHNU V.; PRAVEEN, K. Bypassing wired port security. *International Journal of Recent Technology and Engineering (IJRTE)*, v. 8, n. 6, p. 3293–3297, 2020.

39 KANG, H.; LIU, G.; WANG, Q.; MENG, L.; LIU, J. Theory and application of zero trust security: A brief survey. *Entropy*, v. 25, n. 12, 2023. Disponível em: <https://www.mdpi.com/1099-4300/25/12/1595>.

40 JAHANGEER, A.; BAZAI, S. U.; ASLAM, S.; MARJAN, S.; ANAS, M.; HASHEMI, S. H. A review on the security of iot networks: From network layer's perspective. *IEEE Access*, v. 11, p. 71073–71087, 2023.

41 RYAN, G. *Bypassing Port Security in 2018: Defeating MACsec and 802.1x-2010. DEF CON 26*. Digital Silence, 2018. Acessado em: 2024-15-10. Disponível em: <https://digitalsilence.com/wp-content/uploads/2022/01/DEF-CON-26-Gabriel-Ryan-Whitepaper-Bypassing-Port-Security-In-2018-Defeating-MacSEC-and-802.1x-2010.pdf>.

42 LA, S. *Prioritizing Cybersecurity Controls Based on the Coverage of Attack Techniques and Attack Probabilities*. Dissertação (Mestrado) — ETH Zurich, Zurich, CH, 2023.

43 HEVNER A. R.; MARCH, S. T. P. J. R. S. Design science in information systems research. *MIS Quarterly*, v. 28, n. 1, p. 75–105, 2004.

44 HUNT, D. *Catch me if you can: How to build a disposable attack box using a Raspberry Pi*. 2021. Archived in the Wayback Machine, Acessado em: 2024-15-10. Disponível em: <https://web.archive.org/web/20241004211326/https://feed.prelude.org/p/catch-me-if-you-can>.

45 MITRE CORPORATION. *MITRE ATT&CK Framework*. 2024. Acessado em: 2025-09-12. Disponível em: <https://attack.mitre.org/>.

46 WIERINGA, R. J. *Design Science Methodology for Information Systems and Software Engineering*. Netherlands: Springer Berlin, 2014.

47 SCHNEIER, B. Attack-trees: Modeling security threats. *Dr. Dobb's Journal*, v. 24, n. 12, p. 21–29, 1999.

48 INGOLDSBY, J. *Attack-Tree-based Threat Risk Analysis*. Amenaza Technologies Limited, 2021. Acessado em: 2024-10-09. Disponível em: <https://www.amenaza.com/downloads/docs/Attack-Tree-Threat-Risk-Analysis.pdf>.

49 CYTRON. *Raspberry Pi case — modelo 5BG (Cytron) — imagem do produto*. 2025. Acessado em: 2025-09-13. Disponível em: <https://static.cytron.io/image/cache/catalog/products/RPI-CASE-5BG/rpi-case-5bg-b-800x800.jpg>.

50 MIKROTIK. *MikroTik RB-series device (RB 1284) — high resolution image*. 2025. Acessado em: 2025-09-12. Disponível em: <https://cdn.mikrotik.com/web-assets/rb_images/1284_hi_res.png>.

51 EGGIMANN, S. *Rogue Raspberry Pi Exploit*. Medium, 2018. Acessado em: 2024-15-10. Disponível em: <https://medium.com/@wicked_picker/rogue-raspberry-pi-exploit-a5f769b784d1>.

52 MITRE CORPORATION. *DarkVishnya, Group G0105 - MITRE ATT&CK*. 2025. Acessado em: 2025-22-05. Disponível em: <https://attack.mitre.org/groups/G0105/>.

53 STANDARDS, N. I. O.; TECHNOLOGY. *Guide for Conducting Risk Assessments. NIST Special Publication 800-30, Revision 1*. Gaithersburg, MD: Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, 2012.

54 THOMAS, T.; PISCITELLI, M.; NAHAR, B. A.; BAGGILI, I. Duck hunt: Memory forensics of usb attack platforms. *Forensic Science International: Digital Investigation*, v. 37, p. 301190, 2021. ISSN 2666-2817. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2666281721000986>.

55 JUNIPER NETWORKS. *Understanding Media Access Control Security (MACsec)*. 2025. Acessado em: 2025-05-22. Disponível em: <https://www.juniper.net/documentation/br/pt/software/junos/security-services/topics/topic-map/understanding_media_access_control_security_qfx_ex.html>.

56 TENABLE, INC. *Cisco IOS XE Software MACsec MKA Using EAP-TLS Authentication Bypass (CVE-2018-15372)*. 2018. Acessado em: 2025-22-05. Disponível em: <https://www.tenable.com/plugins/nessus/132104>.

57 RED HAT, INC. *Using MACsec to encrypt layer-2 traffic in the same physical network*. 2024. Acessado em: 2025-22-05. Disponível em: <https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/8/html/configuring_and_managing_networking/assembly_using-macsec-to-encrypt-layer-2-traffic-in-the-same-physical-network_configuring-and-managing-networking>.

58 CISCO SYSTEMS. *MACsec Switch-host Encryption with Cisco AnyConnect and ISE Configuration Example*. 2014. Acessado em: 2025-22-05. Disponível em: <https://www.cisco.com/c/en/us/support/docs/lan-switching/8021x/117277-config-anyconnect-00.html>.

59 TRABELSI, Z.; ALKETBI, L. *Using Network Packet Generators and Snort Rules for Teaching Denial of Service Attacks*. 2015.