Universidade Federal de Goiás (UFG)
Escola de Engenharia Elétrica, Mecânica e de Computação (EMC)

Luan Weba Soares

Adaptação e implementação da framework NIST em Redes Domésticas

Goiânia
2024

UNIVERSIDADE FEDERAL DE GOIÁS
ESCOLA DE ENGENHARIA ELÉTRICA, MECÂNICA E DE COMPUTAÇÃO

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO PARA DISPONIBILIZAR VERSÕES ELETRÔNICAS DE TRABALHO DE CONCLUSÃO DE CURSO DE GRADUAÇÃO NO REPOSITÓRIO INSTITUCIONAL DA UFG

Na qualidade de titular dos direitos de autor, autorizo a Universidade Federal de Goiás (UFG) a disponibilizar, gratuitamente, por meio do Repositório Institucional (RI/UFG), regulamentado pela Resolução CEPEC no 1240/2014, sem ressarcimento dos direitos autorais, de acordo com a Lei no 9.610/98, o documento conforme permissões assinaladas abaixo, para fins de leitura, impressão e/ou download, a título de divulgação da produção científica brasileira, a partir desta data.

O conteúdo dos Trabalhos de Conclusão dos Cursos de Graduação disponibilizado no RI/UFG é de responsabilidade exclusiva dos autores. Ao encaminhar(em) o produto final, o(s) autor(a)(es)(as) e o(a) orientador(a) firmam o compromisso de que o trabalho não contém nenhuma violação de quaisquer direitos autorais ou outro direito de terceiros.

1. Identificação do Trabalho de Conclusão de Curso de Graduação (TCCG)

Nome(s) completo(s) do(a)(s) autor(a)(es)(as): Luan Weba Soares

Título do trabalho: Adaptação e implementação da framework NIST em Redes Domésticas

2. Informações de acesso ao documento (este campo deve ser preenchido pelo orientador) Concorda com a liberação total do documento [X] SIM [ ] NÃO[1]

[1] Neste caso o documento será embargado por até um ano a partir da data de defesa. Após esse período, a possível disponibilização ocorrerá apenas mediante: a) consulta ao(à)(s) autor(a)(es)(as) e ao(à) orientador(a); b) novo Termo de Ciência e de Autorização (TECA) assinado e inserido no arquivo do TCCG. O documento não será disponibilizado durante o período de embargo.

Casos de embargo:

- Solicitação de registro de patente;

- Submissão de artigo em revista científica;

- Publicação como capítulo de livro.

Obs.: Este termo deve ser assinado no SEI pelo orientador e pelo autor.

Documento assinado eletronicamente por **Carlos Galvao Pinheiro Junior**, **Professor do Magistério Superior**, em 31/01/2024, às 19:45, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

Documento assinado eletronicamente por **Luan Weba Soares**, **Discente**, em 05/02/2024, às 13:15, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Luan Weba Soares

Adaptação e implementação da framework NIST em Redes Domésticas

Trabalho de Conclusão de Curso apresentado ao curso de Engenharia da Computação, da Universidade Federal de Goiás (UFG), como requisito para obtenção do título de bacharel em Engenharia da Computação. Orientador: Carlos Galvão Pinheiro Júnior

Goiânia
2024

Ficha de identificação da obra elaborada pelo autor, através do
Programa de Geração Automática do Sistema de Bibliotecas da UFG.

Soares, Luan Weba
Adaptação e implementação da framework NIST em redes domésticas [manuscrito] / Luan Weba Soares. - 2024.
xxiv, 24 f.

Orientador: Prof. Dr. Carlos Galvão Pinheiro Júnior.
Trabalho de Conclusão de Curso (Graduação) - Universidade Federal de Goiás, Escola de Engenharia Elétrica, Mecânica e de Computação (EMC), Engenharia da Computação, Goiânia, 2024.

Inclui gráfico, tabelas.

1. NIST CSF. 2. Cibersegurança. 3. SIEM. 4. EDR. I. Júnior, Carlos Galvão Pinheiro , orient. II. Título.

CDU 004

UNIVERSIDADE FEDERAL DE GOIÁS
ESCOLA DE ENGENHARIA ELÉTRICA, MECÂNICA E DE COMPUTAÇÃO

ATA DE DEFESA DE TRABALHO DE CONCLUSÃO DE CURSO

Ao(s) 31 dia(s) do mês de janeiro do ano de 2024 iniciou-se a sessão pública de defesa do Projeto de Final de Curso 2 intitulado **"Adaptação e implementação da framework NIST em Redes Domésticas"**, de autoria de **Luan Weba Soares** , do curso de Engenharia de Computação, do Escola de Engenharia Elétrica Mecânica e de Computação da UFG. Os trabalhos foram instalados pelo Dr. Carlos Galvão Pinheiro Júnior com a participação dos demais membros da Banca Examinadora: **Marco Antonio Assfalk de Oliveira** e **João Miguel Estevão Alves** . Após a apresentação, a banca examinadora realizou a arguição do estudante. Posteriormente, de forma reservada, a Banca Examinadora atribuiu a nota final de 9,4 , tendo sido o PFC 2 considerado **APROVADO**.

Proclamados os resultados, os trabalhos foram encerrados e, para constar, lavrou-se a presente ata que segue assinada pelos Membros da Banca Examinadora.

Documento assinado eletronicamente por **Carlos Galvao Pinheiro Junior**, **Professor do Magistério Superior**, em 31/01/2024, às 19:41, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

Documento assinado eletronicamente por **Marco Antonio Assfalk De Oliveira** , **Professor do Magistério Superior**, em 01/02/2024, às 19:42, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

Documento assinado eletronicamente por **João Miguel Estevao Alves** , **Usuário Externo**, em 05/02/2024, às 13:14, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

A autenticidade deste documento pode ser conferida no site https://sei.ufg.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **4321768** e o código CRC **7CF16BF2**.

Referência: Processo nº 23070.058411/2023-61 SEI nº 4321768

Adaptação e implementação da framework NIST em Redes Domésticas

Luan Weba Soares, Graduando em Engenharia de Computação
EMC/UFG, luanweba@discente.ufg.br

Resumo **- Este estudo aborda a adaptação e implementação do *National Institute of Standards and Technology Cybersecurity Framework* (NIST CSF) em redes domésticas. Exploramos os desafios trazidos pelo aumento do trabalho remoto em ambientes residenciais, contribuindo para uma paisagem de Segurança mais complexa. Utilizando o *Raspberry Pi* equipado com ferramentas de segurança como SIEM (*Security Information and Event Management*) e EDR (*Endpoint Detection and Response*), e técnicas de varredura de vulnerabilidade, o estudo propõe um conjunto abrangente de práticas de segurança baseadas no NIST CSF. Ele visa oferecer um modelo claro e de baixo custo para a implementação efetiva de medidas de cibersegurança, protegendo a integridade e privacidade dos dados em redes domésticas. Por fim chegamos no resultado que a framework é adaptável, porém requer muita intervenção de especialistas, a ponto de ser mais adequado a sustentação por estes ao invés do usuário final.**

Palavras Chaves - NIST CSF, SIEM, EDR, Cibersegurança

Abstract **- This study addresses the implementation and feasibility of the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). We explore the challenges brought by the rise of remote work in residential environments, both of which contribute to a more complex security landscape. Using the Raspberry Pi equipped with security tools such as SIEM and EDR, and vulnerability scanning techniques, the study proposes a comprehensive set of security practices based on the NIST CSF. It aims to provide a clear, low-cost roadmap for effectively modeling cybersecurity measures, protecting data integrity and privacy on home networks. Finally, we arrived at the result that the framework is adaptable, but requires a lot of intervention from specialists, to the point that support by them rather than the end user is more appropriate.**

Index Terms - NIST CSF, SIEM, EDR, Cybersecurity

1. INTRODUÇÃO

A cibersegurança desempenha um papel crucial em nossa sociedade moderna. Com a crescente dependência de sistemas digitais em praticamente todos os momentos de nossas vidas, desde transações bancárias e comunicações pessoais até a infraestrutura crítica, é fundamental garantir a proteção dessas informações contra ameaças cibernéticas. Ataques cibernéticos podem resultar em perdas financeiras, roubo de dados sensíveis, interrupção de serviços essenciais e até mesmo impactos sociais e políticos significativos. Portanto, a implementação de medidas robustas de cibersegurança é essencial para garantir a integridade, a confidencialidade e a disponibilidade das informações de um mundo cada vez mais digital.

Um dos novos problemas enfrentados é a ascensãodo trabalho remoto. ela trouxe consigo uma série de desafios quando se trata de cibersegurança. Com mais pessoas trabalhando fora dos ambientes tradicionais de escritório,os dados corporativos agora são acessados a partir de redes domésticas, muitas vezes menos seguras do que as redes corporativas. Isso aumenta a exposição a ameaças cibernéticas, como *malware*, *phishing* e ataques de engenharia social. Além disso, a utilização de dispositivos pessoais para fins profissionais e a necessidade de compartilhamento de arquivos e informações sensíveis via internet adicionam camadas adicionais de vulnerabilidade. É fundamental adotar práticas adequadas para garantir a proteção dos dados da corporação e a continuidade dos negócios no ambiente de trabalho remoto.

O artigo [1] explora a preparação das organizações e funcionários para o aumento repentino do trabalho remoto e as ameaças cibernéticas associadas, especialmente durante o surto inicial da COVID-19, nele explica que apenas 15% dos funcionários do Reino Unido estavam trabalhando remotamente, mas esse número mais que dobrou no mês seguinte, atingindo 38%, sugerindo um adicional de aproximadamente 6,8 milhões de funcionários trabalhando em casa no pico do lockdown. Apenas 12% das empresas implementaram todas as 10 etapas recomendadas pelo Centro Nacional de Segurança Cibernética do Reino Unido para proteção contra-ataques e violações. A conformidade aumenta com o tamanho da empresa, mas há uma queda notável em aspectos mais orientados para políticas empresariais e pessoas, com apenas um quarto a um terço das empresas abordando questões como trabalho remoto e conscientização do usuário. Cerca de 75% das empresas não têm regras escritas e explícitas de segurança cibernética para trabalho remoto, apenas 11% das empresas forneceram treinamento de segurança cibernética a funcionários não especializados no ano anterior. Isso resultou em quase um quarto das organizações experimentando um aumento nos incidentes cibernéticos após a mudança para o trabalho remoto, com alguns relatando que o volume dobrou. Os ataques aumentaram particularmente em torno de golpes relacionados à COVID-19, com o *National Cyber Security Centre* (NCSC) derrubando mais de 2.000 golpes online relacionados ao vírus durante março de 2020.

Diante dos desafios apresentados pela cibersegurança nas situações explicadas, este projeto de conclusão de curso propõe desenvolver um conjunto de práticas de segurança utilizando o NIST CSF como base. O objetivo é fornecer um roteiro claro e abrangente para a implementação de medidas de cibersegurança em redes domésticas.

Em paralelo com a *framework*, foi proposto a utilização de um *Raspberry Pi*, equipado com ferramentas e programas de segurança, a pretensão é oferecer uma solução de baixo custo e eficaz para garantir a integridade e privacidade dos dados transmitidos em redes domésticas.

Na próxima seção, serão apresentados os principais conceitos do *NIST Cybersecurity Framework*, tecnologias usadas e casos de ataques reais que podem ocorrer em uma rede doméstica. Na seção 3 (Metodologia) será explicado a criação de um perfil para a rede doméstica e os seus motivos, a implementação das ferramentas e aonde cada ferramenta se encaixa. Na seção 4 discutiremos problemas encontrados durante o projeto, comparação de tecnologias que fazem funções similares e casos de ataque na qual ocorreu. Por fim na seção 5, concluímos os resultados do projeto.

2. FUNDAMENTAÇÃO TEORICA

Nesta seção, abordamos os conceitos fundamentais da *NIST Cybersecurity Framework* e as práticas de segurança recomendadas para proteger redes domésticas. Também explicamos as principais tecnologias que instalamos e configuramos para atender aos desafios delineados no framework. Implementando essas práticas, se espera fornecer um guia claro e eficaz para fortalecer a segurança da informação em ambientes residenciais.

2.1 Framework NIST CSF

O NIST CSF é um conjunto de diretrizes, melhores práticas e padrões de segurança cibernética desenvolvido pelo *National Institute of Standards and Technology* (NIST), que é uma agência do Departamento de Comércio dos Estados Unidos, responsável por desenvolver e promover padrões e tecnologias para melhorar a competitividade e inovação das empresas norte-americanas em escala global. O CSF foi criado para ajudar organizações de diversos setores a fortalecerem suas práticas de segurança e a gerenciarem melhor os riscos.

Ela foi desenvolvida devido a uma ordem executiva assinada pelo então presidente dos Estados Unidos, Barack Obama, em fevereiro de 2013. A ordem executiva 13636[2], intitulada “Melhorando a Segurança Cibernética da Infraestrutura Crítica” destacou a necessidade de desenvolver um conjunto de padrões voluntários e melhores práticas para melhorar a cibersegurança das infraestruturas críticas nos Estados Unidos.

A partir dessa ordem executiva, o NIST foi encarregado de criar um *framework* que fornecesse orientações claras e concisas para as organizações fortalecerem sua postura de segurança.

O motivo desse *framework* era fornece uma estrutura flexível, repetível e de custo eficaz queas organizações pudessem adotar para melhorar sua segurança da informação. As ameaças estão em constante evolução, e as organizações precisam encontrar maneiras eficazes e adaptáveis para lidar com essas ameaças.

Além disso, o *framework* foi projetado para ser voluntário e não prescritivo, o que significa que as organizações não são obrigadas por lei a implementá-lo. Em vez disso, a CSF fornece um conjunto de princípios e práticas que podem ser adaptados às necessidades específicas e ao contexto de cada organização, devido a essa flexibilidade ela foi escolhida para ser usada como referência no projeto.

Diante disso, ela é bem-conceituada em seu uso em empresas privadas de todo o mundo. Possui a versão 1.0, desenvolvida em 2014 e a versão 1.1, desenvolvida em 2018[3], atualmente estão desenvolvendo a versão 2.0[4].A *framework* é dividida em três partes principais: o *Core* (Núcleo) do *framework*, *Tiers* (Níveis) e os *Profiles* (Perfis). O *core* da *framework* consiste em atividades de segurança, resultados esperados e referências que são aplicáveis a todos os setores de infraestrutura. E com ele pode ser usado para fornecer orientações detalhadas para criar perfis organizacionais personalizados. Ao usar esses perfis, o *framework* auxilia as organizações a alinhar e priorizar suas estratégias de segurança de acordo com as necessidades de seus negócios, missão, tolerâncias ao risco e recursos disponíveis. Além disso, os *tiers* oferecem um método para as organizações entenderem melhor as características de sua abordagem no gerenciamento de riscos, o que facilita a priorização e o alcance de metas específicas.

Vale ressaltar que a *framework* não substitui programas de cibersegurança existente na empresa ou residência, mas pode ser usado para criar um caso não tenha, logo usar a framework é válido em situações que precisam ser criados do zero, nas subseções 2.2, 2.3 e 2.4 serão explicadas as 3 categorias da NIST: *Core*, *Tiers* e *Profiles*

2.2 CORE

O *core* do *framework* apresenta padrões da indústria, diretrizes e práticas de modo a facilitar a comunicação das atividades e dos resultados no quesito de cibersegurança em toda a organização, desde os níveis executivos até as operações de implementação. Ele é composto por cinco categorias simultâneas e contínuas: Identificar, Proteger, Detectar, Responder e Recuperar, como mostrado na figura 1.

Quando consideradas em conjunto, essas funções oferecem uma visão abrangente da gestão de riscos em

segurança da informação de uma organização. O *core* da estrutura também identifica categorias e subcategorias-chave, que representam resultados específicos para cada função, e as relaciona com exemplos de referências para se aprofundar no seu uso, como normas existentes, diretrizes e práticas para cada subcategoria.

Fig 1. NIST CSF CORE [5]

Identificar estabelece uma compreensão organizacional para a administração dos riscos da infraestrutura relacionados a sistemas, indivíduos, recursos, informações e capacidades. Essa compreensão é a base para a aplicação efetiva do *framework*. Ao entender o contexto da infraestrutura, os recursos fundamentais para funções críticas e os riscos inerentes, uma organização pode direcionar e priorizar seus esforços de forma coerente.

Proteger implementa os meios apropriados para garantir os três pilares da segurança da informação (integridade, disponibilidade e confidencialidade) da infraestrutura. A função de proteção tem como objetivo limitar ou conter o impacto de um evento de cibersegurança possível. Exemplos de categorias de resultados nessa função incluem: Gerenciamento de identidade e controle de acesso; conscientização e treinamento; segurança de dados; processos e procedimentos de proteção de informações; manutenção; e tecnologia de proteção (como antivírus e firewalls).

Detectar envolve o desenvolvimento e a implementação das atividades necessárias para identificar a ocorrência de um evento de cibersegurança. O objetivo dessa função é permitir uma detecção oportuna de incidentes. O que compõe essa função é monitoramento contínuo, detecção de anomalias e criar alertas de segurança

Responder desenvolve e implementa atividades apropriadas para tomar medidas em relação a um incidente de cibersegurança detectado. A função de resposta apoia capacidade de conter o impacto de um possível incidente. Exemplos de categorias de resultados dentro desta função incluem: Planejamento de resposta; comunicações; análise; mitigação; e melhorias.

Recuperar desenvolve e implementa atividades apropriadas para manter planos de resiliência e restaurar quaisquer capacidades ou serviços que foram prejudicados devido a um incidente de cibersegurança. A função de recuperação permite a restauração oportuna das operações normais para reduzir o impacto de um incidente de cibersegurança. Exemplos de categorias de resultados dentro desta função incluem: planejamento de recuperação; melhorias; e comunicações.

A tabela 1 mostra todas as categorias, subcategorias de todas as funções, com ela podemos abranger o vasto nível de detalhes que a *framework* aborda para proteger uma organização.

2.1 TIERS

Os níveis fornecem um contexto sobre como a empresa encara a sua gestão de risco, variando do nível 1 ao nível 4. No nível 1, a empresa tem uma compreensão limitada da gestão de risco, enquanto no nível 4 a empresa possui plena consciência sobre a sua gestão. Empresas do nível 1 têm práticas informais de gestão de risco e lidam com ela de forma reativa. A gestão de risco é feita de maneira irregular, caso a caso, sem compreender plenamente a sua função no ecossistema. Essas empresas não compartilham nem recebem informações sobre ameaças e não reconhecem os riscos relacionados à *supply chain*.

Empresas do nível 2 têm uma gestão de risco aprovada pela gestão, mas ainda pode não estar estabelecida de forma geral. A informação de cibersegurança é compartilhada informalmente, e o compartilhamento de informações sobre ameaças ocorre, mas não de forma regular.

No caso de empresas de nível 3, as práticas de gestão de riscos da organização são oficialmente aprovadas e expressas como política. Existe uma abordagem generalizada na organização para lidar com o risco de segurança cibernética. A organização reconhece sua posição, dependências e interdependências dentro de um ecossistema maior, e pode contribuir para um entendimento mais abrangente dos riscos da comunidade.

Por outro lado, empresas de nível 4 são organizações que adaptam suas práticas de segurança com base em atividades passadas e atuais, aprendendo com lições e indicadores preditivos. Existe uma abordagem generalizada na organização para gerenciar o risco de segurança. São usadas políticas, processos e procedimentos que levam em a consideração os riscos possíveis. A organização compreende sua posição, dependênciase interdependências em um ecossistema mais amplo, contribuindo para um entendimento mais abrangente dos riscos da comunidade.

Tabela 1: NIST COMPLETA

Função	Categoria	Subcategoria
Identificar (ID)	**Gerenciamento de Ativos (ID.AM):** Os dados, pessoais, dispositivos, sistemas e instalações que permitem à organização atingir os objetivos de negócio são identificados e geridos de forma consistente com a sua importância relativa para os objetivos de negócio e para a estratégia de risco da organização.	**ID.AM-1:** Dispositivos físicos e sistemas dentro da organização são inventariados
		ID.AM-2: Plataformas de software e aplicativos dentro da organização são inventariados
		ID.AM-3: A comunicação organizacional e os fluxos de dados são mapeados
		ID.AM-4: Os sistemas de informação externos são catalogados
		ID.AM-5: Os recursos (por exemplo, hardware, dispositivos, dados e software) são priorizados com base em sua classificação, criticidade e valor comercial
		ID.AM-6: As funções e responsabilidades de segurança cibernética para toda a força de trabalho e terceiros interessados (por exemplo, fornecedores, clientes, parceiros) são estabelecidas
	Ambiente de Negócios (ID.BE): A missão, os objetivos, as partes interessadas e as atividades da organização são compreendidas e priorizadas; essas informações são usadas para informar funções, responsabilidades e decisões de gerenciamento de riscos de segurança cibernética.	**ID.BE-1:** O papel da organização na *supply chain* é identificado e comunicado
		ID.BE-2: O lugar da organização na infraestrutura crítica e no seu setor industrial é identificado e comunicado
		ID.BE-3: Prioridades para missão, objetivos e atividades organizacionais são estabelecidas e comunicadas
		ID.BE-4: Dependências e funções críticas para entrega de serviços críticos são estabelecidas
		ID.BE-5: Requisitos de resiliência para apoiar a prestação de serviços críticos são estabelecidos
	Governança (ID.GV): As políticas, procedimentos e processos para gerenciar e monitorar os requisitos regulatórios, legais, de risco, ambientais e operacionais da organização são compreendidos e informam o gerenciamento do risco de segurança cibernética.	**ID.GV-1:** Política organizacional de segurança da informação é estabelecida
		ID.GV-2: As funções e responsabilidades de segurança da informação são coordenadas e alinhadas com as funções internas e parceiros externos
		ID. GV-3: Os requisitos legais e regulamentares relativos à segurança cibernética, incluindo obrigações de privacidade e liberdades civis, são compreendidos e gerenciados
	Avaliação de risco (ID.RA): A organização compreende o risco de segurança cibernética para as operações organizacionais (incluindo missão, funções, imagem ou reputação), ativos organizacionais e individuais.	**ID.RA-1:** As vulnerabilidades de ativos são identificadas e documentadas
		ID.RA-2: Informações sobre ameaças e vulnerabilidades são recebidas de fóruns e fontes de compartilhamento de informações
		ID.RA-3: Ameaças, tanto internas quanto externas, são identificadas e documentadas
		ID.RA-4: Potenciais impactos e probabilidades de negócios são identificados
		ID.RA-5: Ameaças, vulnerabilidades, probabilidades e impactos são usados para determinar o risco
		ID.RA-6: As respostas aos riscos são identificadas e priorizadas
	Estratégia de Gestão de Risco (ID.RM): As prioridades, restrições, tolerâncias ao risco e suposições da organização são estabelecidas e usadas para apoiar decisões de risco operacional.	**ID.RM-1:** Os processos de gestão de riscos são estabelecidos, gerenciados e acordados pelas partes interessadas organizacionais
		ID.RM-2: A tolerância ao risco organizacional é determinada e claramente expressa
		ID.RM-3: A determinação da tolerância ao risco da organização é informada pelo seu papel na infraestrutura crítica e na análise de risco específica do setor
Proteger (PR)	**Controle de Acesso (PR.AC):** O acesso a ativos e instalações associadas é limitado a usuários, processos ou dispositivos autorizados e a atividades e transações autorizadas.	**PR.AC-1:** Identidades e credenciais são gerenciadas para dispositivos e usuários autorizados
		PR.AC-2: O acesso físico aos ativos é gerenciado e protegido
		PR.AC-3: O acesso remoto é gerenciado
		PR.AC-4: As permissões de acesso são gerenciadas, incorporando os princípios de menor privilégio e separação de funções

		PR.AC-5: A integridade da rede é protegida, incorporando segregação de rede quando apropriado
	Conscientização e treinamento (PR.AT): O pessoal e os parceiros da organização recebem educação de conscientização sobre segurança cibernética e são adequadamente treinados para desempenhar suas funções e responsabilidades relacionadas à segurança da informação, de acordo com as políticas, procedimentos e acordos relacionados.	**PR.AT-1:** Todos os usuários são informados e treinados
		PR.AT-2: Usuários privilegiados entendem funções e responsabilidades
		PR.AT-3: Terceiros interessados (por exemplo, fornecedores, clientes, parceiros) entendem funções e responsabilidades
		PR.AT-4: Executivos seniores entendem funções e responsabilidades
		PR.AT-5: O pessoal de segurança física e da informação entende as funções e responsabilidades
	Segurança de Dados (PR.DS): As informações e registros (dados) são gerenciados de forma consistente com a estratégia de risco da organização para proteger a confidencialidade, integridade e disponibilidade das informações.	**PR.DS-1:** Os dados em repouso estão protegidos
		PR.DS-2: Data-em-trânsito é protegido
		PR.DS-3: Os ativos são gerenciados formalmente durante a remoção, transferência e disposição
		PR.DS-4: Capacidade adequada para garantir que a disponibilidade seja mantida
		PR.DS-5: Implementadas proteções contra vazamentos de dados
		PR.DS-6: Mecanismos de verificação de integridade são usados para verificar software, firmware e integridade de informações
		PR.DS-7: O(s) ambiente(s) de desenvolvimento e teste são separados do ambiente de produção
	Processos e Procedimentos de Proteção da Informação (PR.IP): Políticas de segurança (que abordam propósito, escopo, funções, responsabilidades, compromisso de gerenciamento e coordenação entre entidades organizacionais), processos e procedimentos são mantidos e usados para gerenciar a proteção de sistemas e ativos de informação.	**PR.IP-1:** Uma configuração básica de sistemas de tecnologia da informação/controle industrial é criada e mantida
		PR.IP-2: Um ciclo de vida de desenvolvimento de sistema para gerenciar sistemas é implementado
		PR.IP-3: Os processos de controle de alterações de configuração estão em vigor
		PR.IP-4: Backups de informações são conduzidos, mantidos e testados periodicamente
		PR.IP-5: Políticas e regulamentos relativos ao ambiente operacional físico para ativos organizacionais são atendidos
		PR.IP-6: Os dados são destruídos de acordo com a política
		PR.IP-7: Os processos de proteção são continuamente melhorados
		PR.IP-8: A eficácia das tecnologias de proteção é compartilhada com as partes apropriadas
		PR.IP-9: Planos de resposta (Resposta a Incidentes e Continuidade de Negócios) e planos de recuperação (Recuperação de Incidentes e Recuperação de Desastres) estão em vigor e gerenciados.
		PR.IP-10: Planos de resposta e recuperação são testados
		PR.IP-11: A segurança cibernética está incluída nas práticas de recursos humanos (por exemplo, desprovisionamento, triagem de pessoal)
		PR.IP-12: Um plano de gerenciamento de vulnerabilidades é desenvolvido e implementado
	Manutenção (PR.MA): A manutenção e reparos de componentes de controle industrial e sistemas de informação são realizados de acordo com políticas e procedimentos.	**PR.MA-1:** A manutenção e o reparo dos ativos organizacionais são realizados e registrados em tempo hábil, com ferramentas aprovadas e controladas
		PR.MA-2: A manutenção remota de ativos organizacionais é aprovada, registrada e executada de maneira a impedir o acesso não autorizado
	Tecnologia de Proteção (PR.PT): As soluções técnicas de segurança são geridas para garantir a segurança e resiliência dos sistemas e ativos, consistentes com as políticas, procedimentos e acordos relacionados.	**PR.PT-1:** Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política
		PR.PT-2: A mídia removível é protegida e seu uso é restrito de acordo com a política
		PR.PT-3: O acesso aos sistemas e ativos é controlado, incorporando o princípio da menor

		funcionalidade
		PR.PT-4: Redes de comunicações e controlo estão protegidas
Detectar (DE)	**Anomalias e Eventos (DE.AE):** A atividade anômala é detectada em tempo hábil e o impacto potencial dos eventos é compreendido.	**DE.AE-1:** Uma base das operações de rede e dos fluxos de dados esperados para usuários e sistemas é estabelecida e gerenciada.
		DE.AE-2: Os eventos detectados são analisados para entender os alvos e métodos de ataque
		DE.AE-3: Os dados de eventos são agregados e correlacionados de diversas fontes e sensores
		DE.AE-4: Impacto do evento é determinado
		DE.AE-5: São estabelecidos os limites de alerta para incidentes.
	Monitoramento Contínuo de Segurança (DE.CM): Os sistema e ativos são monitorados em intervalos discretos para identificar eventos de segurança cibernética e verificar a eficácia das medidas de proteção.	**DE.CM-1:** A rede é monitorada para detectar possíveis eventos de segurança cibernética
		DE.CM-2: O ambiente físico é monitorado para detectar possíveis eventos de segurança cibernética
		DE.CM-3: A atividade do pessoal é monitorada para detectar possíveis eventos de segurança cibernética
		DE.CM-4: Código Malicioso é detectado
		DE.CM-5: Código móvel não autorizado é detectado
		DE.CM-6: A atividade do provedor de serviços externo é monitorada para detectar possíveis eventos de segurança cibernética
		DE.CM-7: O monitoramento de pessoal, conexões, dispositivos e software não autorizados é realizado
		DE.CM-8: *Scans* de vulnerabilidade são realizados
	Processos de detecção (DE.DP): Os processos e procedimentos de detecção são mantidos e testados para garantir a conscientização oportuna e adequada de eventos anômalos.	**DE.DP-1:** As funções e responsabilidades pela detecção estão bem definidas para garantir a responsabilização
		DE.DP-2: As atividades de detecção cumprem todos os requisitos aplicáveis
		DE.DP-3: Processos de detecção são testados
		DE.DP-4: As informações de detecção de eventos são comunicadas às partes apropriadas.
		DE.DP-5: Os processos de detecção são continuamente melhorados
RESPONDER (RS)	**Planejamento de Resposta (RS.RP):** Os processos e procedimentos de resposta são executados e mantidos, para garantir uma resposta oportuna aos eventos de segurança cibernética detectados.	**RS.RP-1:** O plano de resposta é executado durante ou após um evento.
	Comunicações (RS.CO): As atividades de resposta são coordenadas com as partes interessadas internas e externas, conforme apropriado, para incluir o apoio externo das agências de aplicação da lei.	**RS.CO-1:** O pessoal conhece suas funções e a ordem das operações quando uma resposta é necessária
		RS.CO-2: Os eventos são relatados de acordo com os critérios estabelecidos
		RS.CO-3: As informações são compartilhadas de acordo com os planos de resposta
		RS.CO-4: A coordenação com as partes interessadas ocorre de forma consistente com os planos de resposta
		RS.CO-5: O compartilhamento voluntário de informações ocorre com partes interessadas externas para alcançar uma consciência situacional mais ampla de segurança cibernética
	Análise (RS.AN): A análise é conduzida para garantir uma resposta adequada e apoiar atividades de recuperação.	**RS.AN-1:** As notificações dos sistemas de detecção são investigadas.
		RS.AN-2: O impacto do incidente é compreendido
		RS.AN-3: A perícia é realizada
		RS.AN-4: Os incidentes são categorizados de acordo com os planos de resposta
	Mitigação (RS.MI): Atividades são realizadas para prevenir a expansão de um evento, mitigar seus efeitos e erradicar o incidente.	**RS.MI-1:** Incidentes são contidos
		RS.MI-2: Incidentes são mitigados
		RS.MI-3: Vulnerabilidades recentemente identificadas são mitigadas ou documentadas como riscos aceitos
	Melhorias (RS.IM): As atividades de resposta organizacional são	**RS.IM-1:** Os planos de resposta incorporam lições

	melhoradas através da incorporação de lições aprendidas com atividades de detecção/resposta atuais e anteriores.	aprendidas
		RS.IM-2: Estratégias de resposta são atualizadas
RECUPERAR (RC)	**Planejamento de Recuperação (RS.RP):** Os processos e procedimentos de recuperação são executados e mantidos para garantir a restauração oportuna de sistemas ou ativos afetados por eventos de segurança cibernética.	**RC.RP-1:** O plano de recuperação é executado durante ou após um evento.
	Melhorias (RC.IM): O planejamento e os processos de recuperação são melhorados através da incorporação de lições aprendidas em atividades futuras.	**RC.IM-1:** Planos de recuperação incorporam lições aprendidas
		RC.IM-2: Estratégias de recuperação são atualizadas
	Comunicações (RC.CO): As atividades de restauração são coordenadas com partes internas e externas, como centros de coordenação, provedores de serviços de Internet, proprietários de sistemas de ataque, vítimas, outros fornecedores.	**RC.CO-1:** As relações públicas são gerenciadas
		RC.CO-2: Reputação após um evento ser reparado
		RC.CO-3: As atividades de recuperação são comunicadas às partes interessadas internas e às equipes executivas e de gestão

2.4. PROFILES

Profile são usados para definir metas em cada tema ou tecnologia que deseja melhorar a segurança. Para cada *profile* que deseja melhorar são criados perfis usando o *core* e *tiers* do framework. A ideia do *profile* é ser um *benchmark* para melhoria de segurança. Ao chegar em uma empresa sua infraestrutura terá um *profile* seguindo algumas das características da NIST, mas para melhorar ainda mais é criado um novo *profile* com mais características, com isso temos um plano bem definido e escrito mostrando onde queremos chegar em um ponto da infraestrutura de uma empresa.

2.5. TECNOLOGIAS USADAS

Para atender as demandas do framework, foram utilizadas diversas tecnologias conhecidas no mundo da segurança da informação para apoiar nas funções do framework, como SIEM, EDR, *scanner* de vulnerabilidade. Essas tecnologias trabalham entre si para permitir uma rede mais segura.

SIEM é uma solução tecnológica abrangente na área de segurança da informação. Seu principal objetivo é proporcionar uma visão holística da segurança de uma organização através da coleta, análise e correlação de dados de eventos de segurança gerados por diversos dispositivos e aplicações. SIEM em geral coletam registros e dados de eventos de uma variedade de fontes, como firewalls, sistemas de prevenção de intrusão (IPS), antivírus, servidores e aplicativos. Estes dados podem incluir registros de acesso, atividades de usuários, alertas de segurança e muito mais. Os dados são coletados frequentemente com vários formatos diferentes. SIEMs normalizam esses dados para um formato consistente, facilitando a análise. Uma de suas principais funções é a correlação de eventos. Ele analisa os dados coletados, buscando padrões e relações que podem indicar atividades suspeitas ou anômalas. Isso é feito através de algoritmos e regras definidas, que podem identificar comportamentos que desviam do normal ou que correspondem a assinaturas de ameaças conhecidas. Quando uma atividade suspeita é identificada, o SIEM gera alertas. Além disso, ele oferece *dashboards* para visualização em tempo real das informações de segurança, auxiliando na tomada de decisões. Os dados são armazenados para análises retrospectivas e de longo prazo, que podem ser usados para investigações de incidentes e para aprimoramento das políticas de segurança. Ele é essencial para função de detecção e identificação encontrado no *framework*.

Outra tecnologia utilizada no projeto foi o que chamamos de **EDR** é uma solução tecnológica focada na segurança de dispositivos de *endpoint*, como computadores, laptops e servidores móveis. O objetivo do EDR é detectar, investigar e responder a atividades maliciosas e questões de segurança em *endpoints*. Diferente das soluções tradicionais de antivírus, que são mais focadas na prevenção de ameaças conhecidas, o EDR oferece uma abordagem mais dinâmica e analítica para identificar e responder a ameaças. O EDR monitora continuamente os *endpoints* para detectar atividades suspeitas ou anomalias. Como mudanças em arquivos, processos em execução, uso da rede e registros do sistema. Ele também utiliza análise comportamental e heurística para identificar padrões de atividades que possam indicar uma ameaça, como *malware*, *ransomware*, ou ataques de dia zero. Isso é feito através da comparação de comportamentos observados com padrões conhecidos de atividades maliciosas. Quando atividades suspeitas são detectadas, o sistema gera alertas. Além disso, EDRs muitas vezes utilizam inteligência de ameaças em tempo real para identificar e classificar ameaças emergentes.

Além disso, oferecem ferramentas para análise forense e investigação detalhada, permitindo aos analistas entendero escopo, a origem e o impacto de um incidente de segurança. EDR é essencial para abranger a categoria de proteção em uma rede doméstica, pois é com ele que podemos impedir execução de atividades suspeitas no *endpoint*.

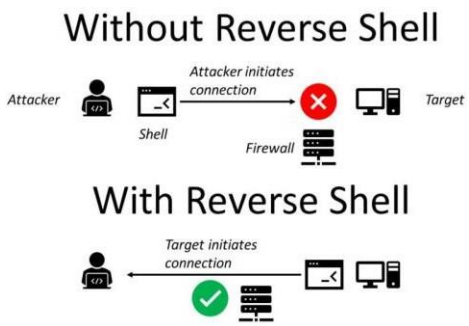
Também foi usado um ***scan* de vulnerabilidades** ele é permite identificar, classificar e priorizar vulnerabilidades em sistemas, redes e aplicações. É uma ferramenta fundamental para prevenir invasões e ataques, ajudando as organizações a entender e mitigar pontos fracos em sua infraestrutura e inventariar máquinas presentes na rede. Primeiramente, o sistema de *scan* de vulnerabilidade identifica todos os ativos de

rede relevantes, como servidores, dispositivos de rede, aplicações e *endpoints*. O sistema então realiza uma varredura (*scan*) desses ativos, procurando por falhasde segurança conhecidas. Isso pode incluir a verificação de configurações incorretas, software desatualizado, falta de patches de segurança, vulnerabilidades conhecidas,portas abertas e serviços inseguros. Após a varredura, o sistema analisa os dados coletados para identificar vulnerabilidades. Esta análise pode ser feita com base em bancos de dados de vulnerabilidades conhecidas, como o *Common Vulnerabilities and Exposures* (CVE), muito usado para inventariar vulnerabilidades. Os resultados são então compilados em um relatório, que detalha as vulnerabilidades encontradas, classificando-as com base em sua gravidade e potencial impacto. O relatório também inclui recomendações para a remediação das vulnerabilidades identificadas, como a aplicação de *patches*, mudanças de configuração ou atualizações de software

2.6. TIPOS DE ATAQUES

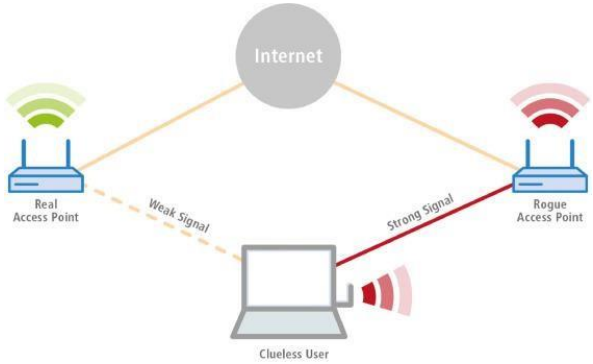
O primeiro ataque testado é o conhecido *reverse shell*, esse tipo de ataque inverte o modelo típico de conexão entre um cliente e um servidor, permitindo que um servidor (neste caso, o sistema alvo) se conecte de volta a um cliente (o computador do atacante). Isso é feito geralmente para evitar medidas de segurança, como firewalls, que podem bloquear conexões de entrada, mas permitem conexões de saída. Primeiro, o atacante precisa de algum meio para executar comandos no sistema alvo. Isso pode ser feito através de vulnerabilidades de segurança, como injeção de SQL, falhas em aplicativos web, *phishing* por email, ou qualquer outro método que permita a execução de código. Uma vez que o atacante pode executar comandos, ele configura e executa um *script* ou comando que inicia uma conexão de volta para um computador ou servidor que ele controla. Este *script* geralmente é escrito em linguagens como *bash* (para sistemas Unix/Linux) ou *powershell* (para Windows). O sistema alvo, ao executar o *script*, abre uma conexão com o servidor do atacante. Esta conexão geralmente é feita em portas comumente abertas, como HTTP (80) ou HTTPS (443), para evitar detecção. Uma vez estabelecida a conexão, o atacante tem um *shell* (interface de linha de comando) no sistema alvo. Isso permite que o atacante execute comandos como se estivesse localmente presente no sistema alvo.

Fig. 2. Ilustração Reverse Shell [6]



O segundo ataque testado é conhecido como *rogue AP* ele é uma técnica na qual um atacante configura um ponto de acesso Wi-Fi não autorizado em uma rede. Este ponto de acesso parece legítimo, mas é controlado pelo atacante. O objetivo é enganar usuários para que se conectem a ele, possibilitando ao atacante interceptar dados, realizar ataque conhecido como "*man-in-the-middle*" (homem no meio), ou ganhar acesso à rede da vítima. O atacante configura um ponto de acesso Wi-Fi, muitas vezes com um nome de rede (SSID) semelhante ao de uma rede legítima na área, como o Wi-Fi de uma empresa ou de um local público. O Rogue AP transmite um sinal Wi-Fi, se tornando visível para dispositivos próximos. Usuários desavisados podem se conectar a este ponto de acesso, pensando que é uma rede legítima. Uma vez que um usuário se conecta ao Rogue AP, o atacante pode monitorar e interceptar todo o tráfego de dados enviado e recebido pelo usuário, incluindo informações sensíveis, como senhas e dados financeiros. Além da interceptação de dados, o atacante pode realizar outros tipos de ataques, como *phishing*, injeção de *malware*, ou ataques de *man-in-the-middle*, alterando o conteúdo das comunicações ou redirecionando os usuários para sites maliciosos.

Fig. 3. Ilustração Rogue AP [7]



3. METODOLOGIA

Nesta seção, será apresentada a metodologia empregada para realizar os experimentos. Inicialmente, será apresentado o *profile* criado baseado no framework, seguida da topologia onde foi feito o experimento, após isso serão apresentadas as análises feitas nos diferentes dispositivos testados como servidor NIST, por fim serão

mostradas as diferentes ferramentas utilizadas que cobrem as exigências necessárias do *profile* criado para o experimento.

3.1 Profile da infraestrutura

Com base na tabela da NIST, foi criado um *profile* para redes domésticas, como mostra a tabela 2. Na fase de identificação, procederemos com a gestão de ativos, abordando a identificação de todos os dispositivos físicos presentes na residência (ID.AM-1), bem como dos softwares que serão objeto de monitoramento (ID.AM- 2). Adicionalmente, será empreendido o mapeamento do fluxo de dados na residência (ID.AM-3), constituindo uma abordagem para compreender os dispositivos e comunicações rotineiros no ambiente doméstico.

A Governança, por sua vez, desempenhará um papel em fornecer a orientação necessária no âmbito jurídico, especialmente no que tange aos direitos e deveres relacionados à segurança residencial (ID. GV-3). Este componente permite uma abordagem legal apropriada para a manutenção da segurança no ambiente doméstico.

Adicionalmente, a avaliação de risco será empregada como categoria para analisar os riscos cibernéticos inerentes à organização da residência. Dentro dessa abordagem, serão identificadas as vulnerabilidades dos ativos, devidamente documentadas (ID.RA-1), e será realizada uma análise das ameaças tanto internas quanto externas à rede domiciliar (ID.RA-3) como dispositivos comprometidos dentro da rede doméstica.

A priorização dos riscos será executada com base em critérios estabelecidos (ID.RA-6), sendo que a identificação de que a presença de um dispositivo desconhecido na rede demanda priorização superior em relação a uma instância de *adware* encontrada em um computador, destacando, assim, a necessidade de tratamento imediato do primeiro cenário.

Na função de proteção, é analisado implementar treinamentos destinados aos membros responsáveis pela administração do ambiente, visando garantir uma compreensão apropriada de suas respectivas responsabilidades sendo usuários e gestores das ferramentas empregadas (PR.AT-2). Este enfoque busca promover a conscientização e a competência necessárias para a eficaz gestão da segurança da rede doméstica.

No âmbito da segurança de dados, os dispositivos da rede devem concentrar em proteger as informações durante sua transmissão, com vistas a mitigar potenciais ataques, tais como *man-in-the-middle*, interceptação, *sniffing* e vazamento de informações. Esse foco, delineado pela prática PR.DS-2, é particularmente relevante, especialmente no que diz respeito à comunicação entre o roteador residencial e o provedor de serviços de internet. A prevenção destas ameaças assume papel importante na proteção da integridade e confidencialidade dosdados em trânsito.

Adicionalmente, é recomendável a elaboração e documentação de um plano de resposta (PR.IP-9) para contingências, a fim de preparar os membros da família para agirem de forma apropriada diante de eventuais incidentes de segurança cibernética. Tal plano é essencial para assegurar uma resposta rápida e eficaz após a ocorrência de um ataque, contribuindo para a pronta recuperação do ambiente.

Na função de detecção, a ênfase recai sobre os dispositivos, concentrando na identificação de tráfegos anômalos (DE.AE-1), um exemplo seria detecção de tráfego originado ou direcionado à servidores provenientes da China ou Rússia, países com histórico em atuação no cibercrime. Simultaneamente, durante esse processo, também é avaliado o impacto do evento e é estabelecido limites de alerta para incidentes, configurando, por exemplo, alertas após a ocorrência de uma determinada comunicação anormal ocorrida três vezes seguidas (DE.AE-5).

A etapa subsequente envolve o monitoramento contínuo para identificação de potenciais eventos, incorporando a detecção de código malicioso (DE.CM-4) e o escaneamento de vulnerabilidades (DE.CM-8). Este conjunto de práticas visa aprimorar a capacidade de identificação proativa de ameaças e vulnerabilidades na rede doméstica. Por último, os processos de detecção são submetidos a testes, e alertas são gerados de forma a notificar as partes pertinentes (DE.DP-4). Esta abordagem busca garantir a eficácia dos processos de detecção implementados, assegurando uma resposta ágil diante de eventos de cibersegurança, com alertas direcionados às pessoas designadas para lidar com tais situações.

No âmbito da resposta a incidentes, a execução do plano de resposta (RS.RP-1) é iniciada, tipicamente conduzindo à investigação e à coleta de dados relacionados a um incidente específico. Esta investigação é preferencialmente realizada por um especialista em segurança cibernética, considerando que usuários comuns possuem limitações no conhecimento necessário para investigar ataques cibernéticos de forma eficaz. Um dos procedimentos iniciais para a implementação do plano consiste na análise de alertas identificados na fase de detecção (RS.AN-1). Estes alertas são investigados para assegurar maior efetividade nas respostas ao incidente.

Na fase de Recuperação, a implementação de um plano (RS.RP) é essencial. Esse tipo de plano frequentemente inclui a elaboração e execução de procedimentos de backup e restauração, com ênfase em sistemas e máquinas críticas ou sensíveis ao ambiente. A gestão e execução dessas rotinas requerem a intervenção de um especialista em segurança da informação e recuperação de dados. O papel do especialista é garantir a manutenção da integridade, confiabilidade e disponibilidade dos dados durante todo o processo de recuperação. Este processoé necessário para restaurar as operações normais do sistema e minimizar o impacto do incidente na continuidade dos negócios.

Tabela 2: Tabela NIST para perfil de Rede doméstica

Função	Categoria	Subcategoria
Identificar (ID)	Gerenciamento de Ativos (ID.AM)	**ID.AM-1:** Dispositivos físicos e sistemas dentro da organização são inventariados
		ID.AM-2: Plataformas de software e aplicativos dentro da organização são inventariados
		ID.AM-3: A comunicação organizacional e os fluxos de dados são mapeados
	Governança (ID.GV)	**ID. GV-3:** Os requisitos legais e regulamentares relativos à segurança cibernética, incluindo obrigações de privacidade e liberdades civis, são compreendidos e gerenciados
	Avaliação de risco (ID.RA)	**ID.RA-1:** As vulnerabilidades de ativos são identificadas e documentadas
		ID.RA-3: Ameaças, tanto internas quanto externas, são identificadas e documentadas
		ID.RA-6: As respostas aos riscos são identificadas e priorizadas
Proteger (PR)	Conscientização e treinamento (PR.AT)	**PR.AT-2:** Usuários privilegiados entendem funções e responsabilidades
	Segurança de Dados (PR.DS)	**PR.DS-2:** Data-em-trânsito é protegido
	Processos e Procedimentos de Proteção da Informação (PR.IP)	**PR.IP-9:** Planos de resposta (Resposta a Incidentes e Continuidade de Negócios) e planos de recuperação (Recuperação de Incidentes e Recuperação de Desastres) estão em vigor e gerenciados.
Detectar (DE)	Anomalia de Eventos (DE.AE)	**DE.AE-1:** Uma base das operações de rede e dos fluxos de dados esperados para usuários e sistemas é estabelecida e gerenciada.
		DE.AE-4: Impacto do evento é determinado
		DE.AE-5: São estabelecidos os limites de alerta para incidentes.
	Monitoramento Contínuo de Segurança (DE.CM)	**DE.CM-1:** A rede é monitorada para detectar potenciais eventos de cibersegurança.
		DE.CM-4: Código Malicioso é detectado
		DE.CM-8: Scans de vulnerabilidade são realizados
	Processo de Detecção (DE.DP)	**DE.DP-3:** Processos de detecção são testados
		DE.DP-4: As informações de detecção de eventos são comunicadas às partes apropriadas.
RESPONDER (RS)	Planejamento de Resposta (RS.RP)	**RS.RP-1:** O plano de resposta é executado durante ou após um evento.
	Análise (RS.AN)	**RS.AN-1:** As notificações dos sistemas de detecção são investigadas.
RECUPERAR (RC)	Planejamento de Recuperação (RS.RP)	**RC.RP-1:** O plano de recuperação é executado durante ou após um evento.

Embora o *profile* aborde diversas ações para a segurança da rede que operam de maneira reativa, ou seja, em que o usuário recebe informações e decide como agir, em muitos momentos, será necessário contar com assistência especializada para alcançar os objetivos delineados no *profile*. Inicialmente, é preciso contar com um profissional capacitado para instalar o dispositivo e configurar as máquinas, para assegurar o funcionamento adequado. Após a instalação, entra em cena a fase de sustentação, na qual cada função específica é desempenhada. Na identificação, o usuário recebe informações relevantes sobre as vulnerabilidades nos dispositivos, mas a correção dessas falhas demandará a intervenção de um especialista, dada a complexidade que muitos usuários enfrentam.

Na proteção, é preciso treinar o usuário para interpretar os alertas e compreender o significado por trás deles. Em relação à resposta e recuperação, o usuário raramente conseguirá interagir diretamente, devido à complexidade das ferramentas empregadas nessas categorias de funções. Assim, ao receber alertas graves, será necessário recorrer a assistência mais especializada para lidar com a resposta e a recuperação eficazes

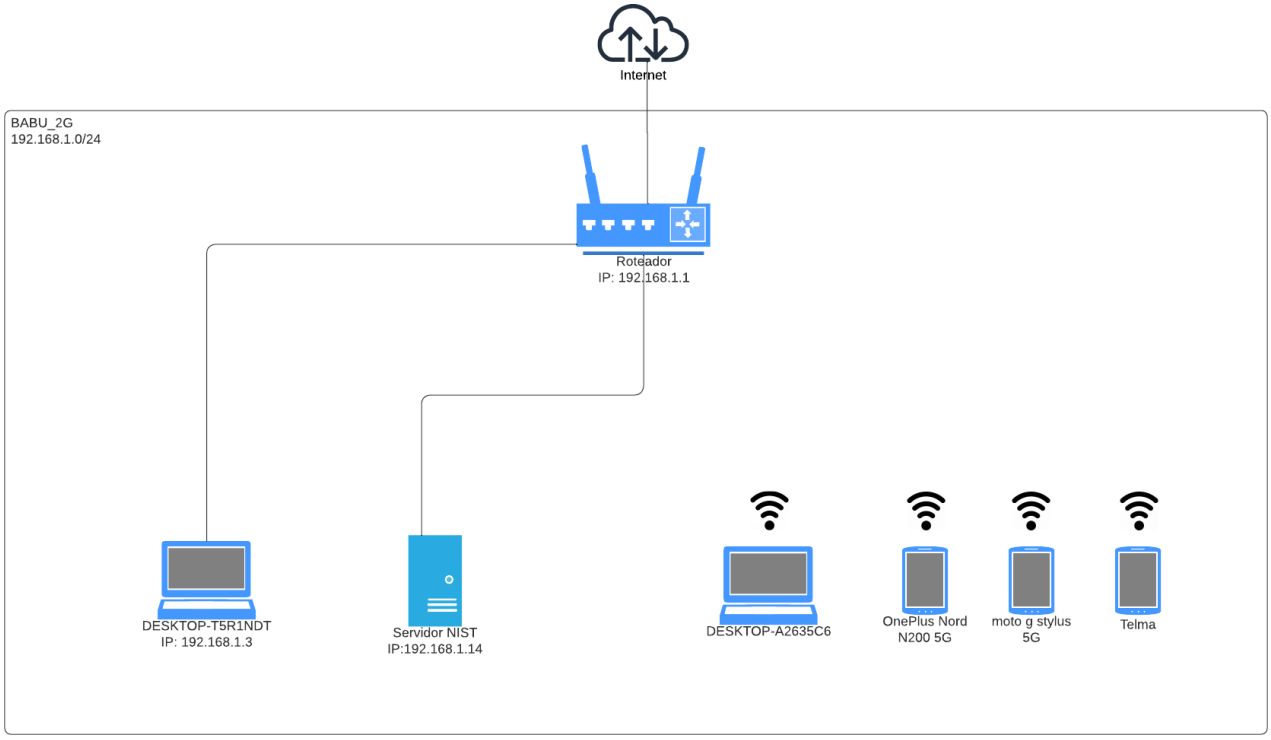
3.2 Topologia da rede

A fase prática do projeto teve início com a consideração da topologia da rede, conforme ilustrado na figura 4. Nessa configuração, o servidor NIST estabelece comunicação com os dispositivos presentes na mesma rede. Dada a natureza de uma rede doméstica, os dispositivos envolvidos incluíram computadores e

celulares. Inicialmente, foi contemplado a utilização do *Raspberry Pi*, porém, devido a desafios relacionados ao desempenho do microprocessador, conforme detalhado na seção 3.3, essa opção foi reconsiderada.

A topologia proposta compreende um servidor equipado com as ferramentas identificadas na pesquisa, alinhadas à *framework* do NIST, interagindo com dois computadores e dois dispositivos móveis.

Fig. 4. Topologia da Rede Inicial



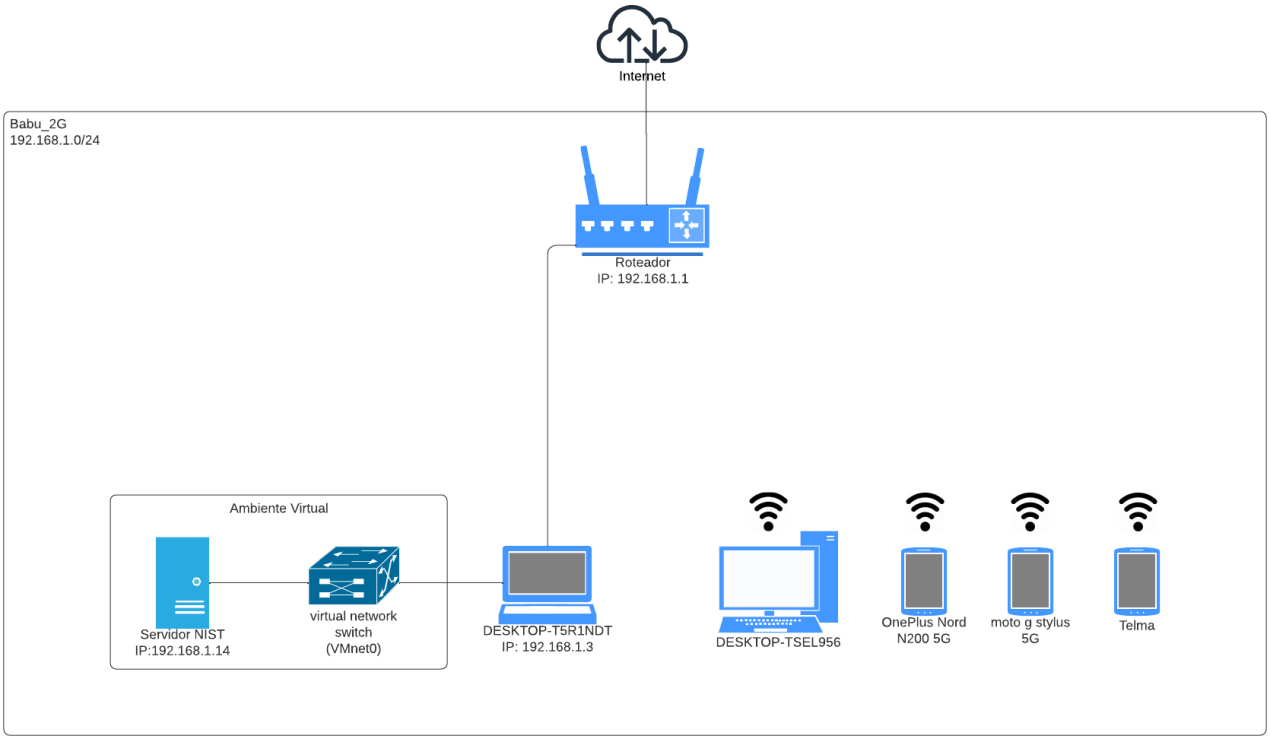
3.3 Servidor NIST, sistema operacional e performance

Inicialmente, a implementação do projeto foi conduzida utilizando um *Raspberry Pi* 3 Modelo B V1.2, equipado com o sistema operacional Kali Linux, o qual foi conectado diretamente no roteador com um cabo ethernet. A escolha desse dispositivo visava aproveitar suas características de tamanho compacto e facilidade de manuseio, proporcionando uma presença discreta na residência durante a execução das atividades de cibersegurança.

O sistema operacional (SO) selecionado, Kali Linux, foi determinado em virtude da extensa variedade de ferramentas disponíveis para tarefas relacionadas à cibersegurança. A escolha do Kali Linux foi ainda influenciada pela existência de uma versão específica para arquitetura arm64, necessária para a instalação no *Raspberry Pi*, além de ser uma opção gratuita. Dentre suas características fundamentais, é destacado a desativação por padrão dos serviços de rede e uma seleção mínima de repositórios confiáveis, conforme mencionado por [8], visando manter a integridade do sistema. Além disso, muitos dos serviços utilizados no projeto possui suporte a distribuição do Kali, isso aumenta a variedade de ferramentas disponíveis para a conclusão do trabalho. Contudo, em decorrência de diversos contratempos relacionados ao desempenho do microprocessador, evidenciados por questões como lentidão e travamentos, notadamente durante a instalação do primeiro software empregado no projeto, a continuidade do uso do *Raspberry Pi v.3* foi considerada inviável. Diante dessa situação, foi optado por adotar uma abordagem alternativa, utilizando uma Máquina Virtual (VM).

Nesse novo ambiente, a conexão foi feita em modo *bridge*, nele a placa de rede da VM se conecta a placa de rede física do dispositivo por meio de um *switch* virtual, permitido que ele compartilhe a rede na mesma residência, como é demonstrado na figura 5. Na máquina virtual foi instalada uma versão mais específica e recente do sistema operacional Kali, denominada Kali *Purple*. Diferentemente do Kali Linux, cujo foco central é em testes de penetração, o Kali *Purple* foi concebido com ênfase na segurança defensiva. Lançado em março de 2023, em comemoração ao décimo aniversário do Kali Linux, o Kali *Purple* visa criar um Centro de Operações de Segurança (SOC) por meio de uma arquitetura conhecida como "soc-*in-a-box*", proporcionando uma plataforma exclusivamente dedicada à segurança defensiva, conforme descrito por [9].

Fig. 5. Topologia de Rede atualizada



Essa mudança foi orientada pela necessidade de alinhar o sistema operacional às metas específicas do projeto, e direcionando para uma abordagem mais alinhada com os princípios de segurança defensiva propostos. As especificações técnicas de cada dispositivo estão detalhadas na Tabela 3.

Tabela 3: Especificações dos dispositivos na rede

Dispositivo	CPU	Memória (GB)	Disco (GB)
DESKTOP-T5R1NDT	4 x 2.5 GHz	16	256 SSD
			930 HD
Servidor NIST (VM)	4 x 2.5 GHz	13.4	512 GB
DESKTOP-A2635C6	4 x 2.5 GHz	16	256 SSD
			930 HD
OnePlus Nord N200 5G	2x 2.0 GHz +6x 1.8 GHz	6	64
Moto g stylus 5G	2x 2.0 GHz + 6x 1.8 GHz	4	128
Telma	2x 2.0 GHz + 6x 1.8 GHz	6	64

3.1 Identificar

Para abordar a categoria "Identificar", foi concebida a utilização de um software com a finalidade de detecção de vulnerabilidades e dispositivos na rede. Um servidor para a detecção de vulnerabilidades demonstra ser útil ao realizar varreduras na rede, possibilitando a identificação de todos os dispositivos conectados. Além disso, esse servidor oferece funcionalidades como a elaboração de inventário das especificações dos sistemas, identificação de vulnerabilidades em aplicações e a capacidade de gerar alertas e relatórios periódicos, elementos cruciais para a descoberta de novos dispositivos. Para essa finalidade, foi escolhido o Greenbone OpenVAS. O procedimento em instalar e configurar o software requer a execução dos comandos mostrados na figura 6.

Fig. 6. Comandos para instalação no Greenbone

```
# Faz update e upgrade dos pacotes
sudo apt-get update
sudo apt-get upgrade
#Instala o gvm
sudo apt-get install gvm
# Faz download do banco de dados
sudo gvm-setup
# Força sincronização com banco de dados
sudo gvm-feed-update
# Script que checa se a instalação foi bem sucedida
sudo gvm-check-setup
# Script que inicia o gvm
sudo gvm-start
# Comando nmap para criar um arquivo com todos IPs de uma rede doméstica e salvar em um arquivo
nmap -sP 192.168.1.0/24 | awk '/is up/ {print up}; {gsub(/\(|\)/,""); up = $NF}' > network
```

Nas mais recentes versões do Kali Linux, o PostgreSQL Cluster é predefinido nas edições 15 e 16. O OpenVAS, por sua vez, faz uso do PostgreSQL na versão 16 como seu banco de dados primário. Portanto, é necessário remover a versão 15. Este procedimento envolve a eliminação da versão 16, a atualização da 15 para a 16 e, subsequentemente, a desinstalação completa da versão 15 do sistema.

Após habilitar a comunicação com o banco de dados, o OpenVAS requer o download do banco de vulnerabilidades mantido pela comunidade. Em ambientes domésticos, é comum a ausência de firewalls protegendo a rede; no entanto, caso estejam presentes, é necessário liberar a porta 873 para permitir o acesso ao *feed.community.greenbone.net*.

Quando o comando *gvm-setup* finalizar, será exibida a senha de administrador. Essa senha é importante para acessar o servidor por meio da interface web. Caso a instalação transcorra sem problemas, é possível acessar o site utilizando o IP do dispositivo com a URL https://192.168.1.14:9392. Neste ponto, é possível inserir o nome de usuário e senha para acessar o painel de controle do Greenbone.

A partir dessa interface, é possível configurar varreduras periódicas na rede, permitindo a identificação de dispositivos conectados e a detecção de vulnerabilidades nesses dispositivos. Além disso, ao configurar um serviço de e-mail no sistema, o servidor de vulnerabilidades se torna capaz de enviar relatórios por e-mail ao usuário. Esses relatórios contêm informações detalhadas sobre os resultados da varredura, dispositivos identificados, portas abertas e vulnerabilidades encontradas. Essa funcionalidade aprimora a capacidade do sistema em fornecer feedback eficiente e notificações importantes. Exemplo de relatório está na figura 7, nele é possível analisar todos os dispositivos encontrados na rede no momento do scan, portas abertas e vulnerabilidades encontradas.

Fig. 7. Relatório Greenbone

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.1.1 myrouter	2	9	3	0	0
192.168.1.3 galaxy-a7-2018-de-silvio	0	1	0	0	0
192.168.1.10	0	0	1	0	0
192.168.1.11	0	0	3	0	0
192.168.1.6 telma	0	0	1	0	0
192.168.1.7	0	0	1	0	0
Total: 6	2	10	9	0	0

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 21 results selected by the filtering described above. Before filtering there were 158 results.

2 Results per Host

2.1 192.168.1.1

Host scan start Sun Oct 22 22:42:08 2023 UTC
Host scan end Mon Oct 23 01:16:55 2023 UTC

Service (Port)	Threat Level
443/tcp	High
4343/tcp	High
443/tcp	Medium
53/udp	Medium
4343/tcp	Medium
443/tcp	Low
general/icmp	Low
4343/tcp	Low

Para iniciar a varredura, o Greenborne necessita primeiramente identificar a rede a ser escaneada. Para isso, é necessário obter um mapeamento dos endereços IP de toda a rede. Dado que, em grande parte das redes domésticas, o intervalo de IP é 192.168.1.0/24, você pode adquirir essa lista por meio do comando *nmap* referenciado na figura 6 e, posteriormente, importar esse arquivo para o serviço Greenborne, como mostra a figura 8.

Fig. 8. Greenborne configuração *range* da rede

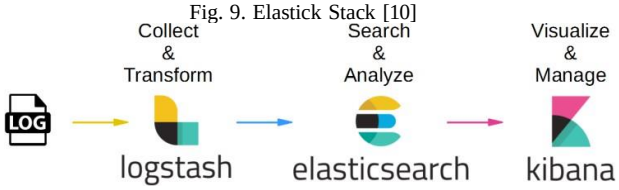
Name ▲	Hosts	IPs	Port List	Credentials
Rede Local	192.168.1.0, 192.168.1.1, 192.168.1.2, 192.168.1.3, 192.168.1.4, 192.168.1.5, 192.168.1.6, 192.168.1.7, 192.168.1.8, 192.168.1.9, 192.168.1.10, 192.168.1.11, 192.168.1.12, 192.168.1.13, 192.168.1.14, 192.168.1.15, 192.168.1.16, 192.168.1.17, 192.168.1.18, 192.168.1.19, 192.168.1.20, 192.168.1.21, 192.168.1.22, 192.168.1.23, 192.168.1.24, 192.168.1.25, 192.168.1.26, 192.168.1.27, 192.168.1.28, 192.168.1.29, 192.168.1.30, 192.168.1.31, 192.168.1.32, 192.168.1.33, 192.168.1.34, 192.168.1.35, 192.16...	256	All IANA assigned TCP and UDP	

(Applied filter: sort=name first=1 rows=10)

3.4 Proteger e Detectar

Esta seção é unificada, pois será empregada uma ferramenta única que desempenha as funções mencionadas, a Elastic Stack (ELK). ELK é uma denominação comum para referir a três serviços *opensource* distintos: Elasticsearch, Logstash e Kibana. Esses serviços colaboram entre si para centralizar diversas soluções de cibersegurança em um único dispositivo, uma abordagem alinhada com os requisitos da documentação da NIST. O ELK oferece funcionalidades de agregação de *logs*, análise e visualizações para o monitoramento de segurança e eventos de sistemas.

Fig. 9. Elastick Stack [10]



O primeiro componente da pilha é o Kibana, cuja principal função é fornecer uma ferramenta de visualização e exploração de dados para análise de *logs* e eventos. Por meio do Kibana, é possível construir painéis, gráficos e filtros em uma interface *web* que capacita o monitoramento de eventos

No segundo nível da pilha, se encontra o Elasticsearch, projetado como um mecanismo de busca baseado em arquivos JSON para requisições e análises em tempo real. Todos os campos do JSON são identificados e indexados, permitindo a busca eficaz de dados na ferramenta.

O terceiro nível dos serviços engloba o Logstash e o Beats. O Logstash é opcional e pode ser utilizado para processar e enriquecer os dados coletados. Por outro lado, o Beats desempenha o papel de encaminhador de dados, direcionando-os para o Logstash, caso seja necessária a etapa de enriquecimento, ou para o Elasticsearch, visando a centralização direta.

Elastic Stack foi escolhido em questão de proteção em redes domésticas por possuir funcionalidade de *Endpoint Security and response* (EDR) e *Security Information and Event Management* (SIEM) integrado em uma única ferramenta. Portanto com ele diminui a complexidade de gerenciar múltiplos servidores e principalmente, é *open-source*, que permite diminuir o preço do servidor.

Para a implementação do Elasticsearch, inicialmente, é necessário adicionar os pacotes correspondentes, juntamente com a versão desejada, à biblioteca do sistema operacional. Esse procedimento preliminar estabelece a base para a subsequente instalação do Elasticsearch, que pode ser efetuada através de um comando simplificado. Ao término do processo de instalação, são fornecidas as credenciais do usuário administrativo, incluindo o nome de usuário e a senha.

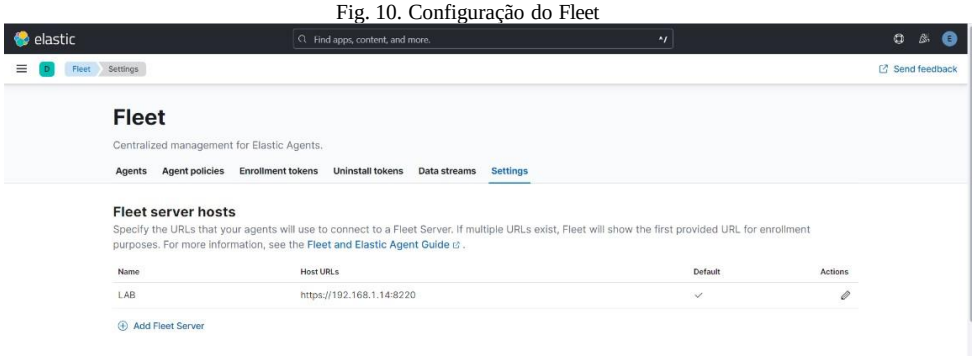
Posteriormente, devemos proceder à configuração do arquivo de parâmetros do sistema do Elasticsearch para delinear as restrições de rede. Esse ajuste visa restringir o acesso às funções de requisição do Elasticsearch exclusivamente ao Fleet e ao Kibana. A validação da instalação e configuração correta é verificada mediante uma requisição ao servidor do Elasticsearch. Uma resposta afirmativa do servidor, caracterizada pela *tagline* "*You Know, for Search*", indica uma comunicação bem-sucedida e a operacionalidade do sistema.

Após a configuração apropriada do Elasticsearch, a próxima etapa envolve a implementação do Kibana, um aplicativo que estabelece comunicação direta com o Elasticsearch. Para uma autenticação do servidor Kibana pelo Elasticsearch, é mandatório configurar o servidor com um token específico, gerado pelo próprio Elasticsearch. A integração desse token autoriza a comunicação entre o Kibana e o Elasticsearch, resultando consequentemente na criação do servidor *web*.

O acesso ao servidor *web* é viabilizado mediante a utilização da senha estabelecida durante o processo de instalação do Elasticsearch. Uma vez concedido o acesso, é possível proceder à instalação do Fleet, um sistema centralizado de gerenciamento de agentes. O Fleet facilita a administração de vários agentes através de comandos simplificados. Para otimização de recursos e simplificação da infraestrutura, é recomendado a instalação do Fleet no próprio servidor do Elasticsearch. A figura 10 ilustra o parâmetro resultante após a conclusão do procedimento.

Essa abordagem não só promove uma integração entre o Kibana, o Elasticsearch e o Fleet, mas também assegura um gerenciamento centralizado dos agentes.

Fig. 10. Configuração do Fleet



Com a conclusão da instalação do *Fleet*, é possível proceder à implementação dos agentes nas estações de trabalho. A instalação de cada agente é efetuada por meio de um comando específico, previamente gerado pelo Elasticsearch, que contém as configurações necessárias para estabelecer uma comunicação eficiente com o Fleet. Esse processo é ilustrado na figura 11.

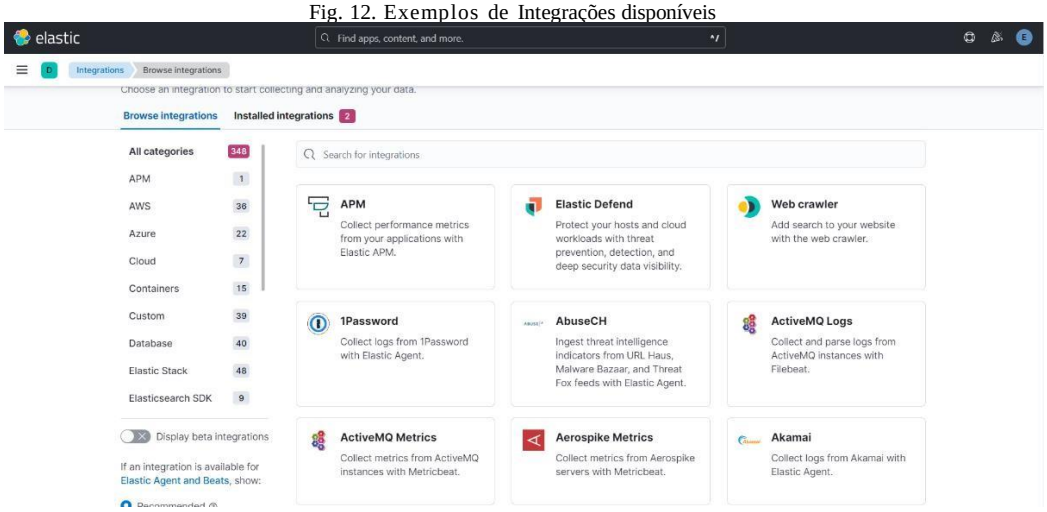
Fig. 11. Comandos para instalação do Agent

Este método permite que os agentes estejam corretamente configurados e sincronizados com o servidor central do Fleet, possibilitando um gerenciamento facilitado, assim como uma coleta de dados consistente e padronizado das estações de trabalho. A abordagem simplifica o processo de instalação dos agentes em ambientes diversificados, isso promove uma arquitetura de monitoramento e gestão de sistemas mais eficiente.

Na eventualidade de se optar pelo uso de um *hostname* em vez de um endereço IP durante a instalação do Fleet, é necessário publicar tal *hostname* no seu roteador para o restante da rede identificar o IP pelo *hostname*, ou realizar ajustes no arquivo de configuração das máquinas. Subsequentemente à instalação do agente, é necessário proceder à configuração das políticas. Estas constituem um conjunto de integrações desenhadas para coletar variados tipos de registros (logs) e ampliar a funcionalidade do sistema. O Elasticsearch oferece mais de 300 integrações possíveis, que podem ser empregadas para monitorar aplicativos e sistemas operacionais. A disponibilidade dessas integrações pode ser visualizadas no servidor web, conforme ilustrado na figura 12.

Essa estrutura de políticas e integrações permite a customização e extensão significativas das capacidades de monitoramento e análise do Elasticsearch, possibilitando adaptações às necessidades específicas de cada ambiente.

Fig. 12. Exemplos de Integrações disponíveis



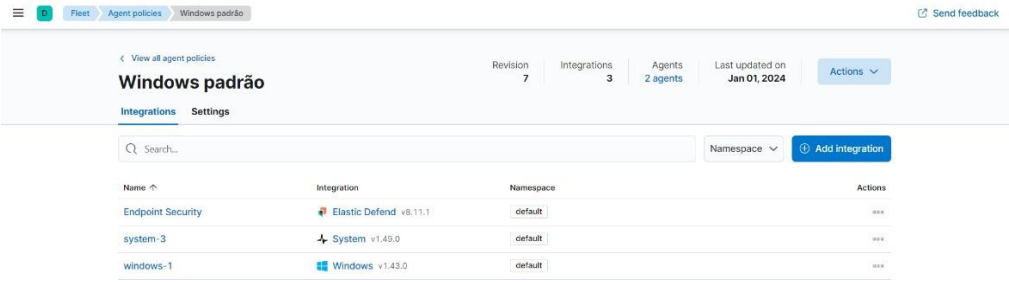
A política configurada para uma estação de trabalho padrão incorpora três integrações disponíveis no elastic: *System*, Windows e *Elastic Defend*, conforme demonstrado na figura 13.

System: Esse serviço é um componente do Metricbeat, uma ferramenta leve projetada para o envio de métricas ao Elasticsearch. O Metricbeat faz parte da arquitetura ELK ("Beats"). Com essa integração, é possível realizar o monitoramento de variados parâmetros do sistema, incluindo CPU, memória, disco, rede, processos, sistema de arquivos e tempo de atividade.

Windows: Também pertencente ao Metricbeat, este serviço é especializada no monitoramento e na transmissão de eventos específicos do sistema operacional Windows. Ela coleta e envia dados relacionados a eventos de segurança, aplicativos e sistema, proporcionando visão das operações e potenciais questões de segurança no ambiente Windows.

Elastic Defend: Parte do Elastic Security, o Elastic Defend é uma solução focada na proteção contra ameaças de segurança em tempo real. Projetado para integrar harmoniosamente ao ecossistema do Elastic Stack (Elasticsearch, Logstash, Kibana), ele emprega vária técnicas, incluindo *machine learning* e detecção de anomalias, para identificar e reagir a ameaças de maneira eficaz. Este serviço oferece a capacidade de prevenir e alertar sobre possíveis ataques, reforçando assim a segurança da infraestrutura.

Fig. 13. Política padrão com os Serviços



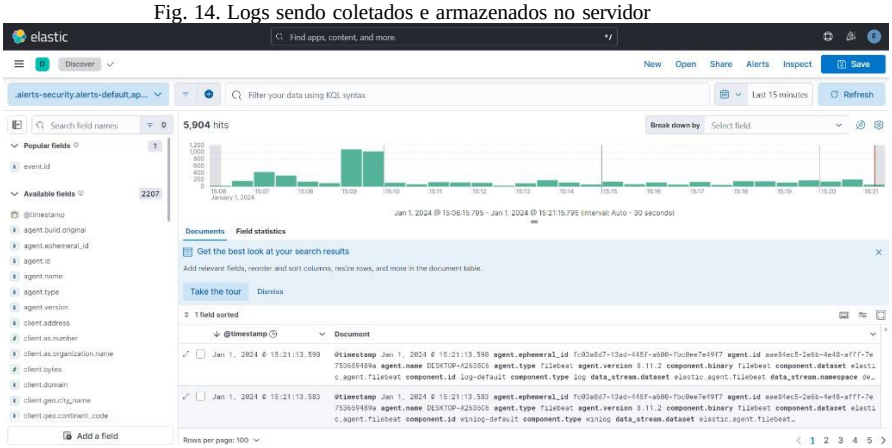
Com as políticas e integrações devidamente configuradas, é possível proceder à validação da coleta de registros (logs) por meio da sessão de *Analytics* do Elasticsearch. Esta análise é ilustrada na figura 14, onde os dados coletados são apresentados e podem ser examinados detalhadamente. A verificação do status operacional dos agentes é igualmente crucial e pode ser realizada na sessão de *Management*.

A sessão de *Analytics* oferece uma interface interativa para a inspeção e interpretação dos dados coletados, permitindo uma compreensão das operações e possíveis anomalias. Por outro lado, a sessão de *Management* fornece uma visão do estado dos agentes, possibilitando monitorar a saúde e desempenho dos dispositivos.

Subsequentemente à instalação do agente, devemos proceder à configuração dos sistemas de alerta. O Elasticsearch oferece um conjunto predefinido de alertas que podem ser importados para facilitar a iniciação das análises de segurança. Através da importação e ativação desses alertas, é possível notificar o pessoal relevante acerca de quaisquer anomalias ou comportamentos suspeitos detectados nos sistemas.

Com as políticas devidamente estabelecidas e o agente instalado na estação de trabalho, a fase de monitoramento por ameaças e anomalias no sistema inicia.

Fig. 14. Logs sendo coletados e armazenados no servidor

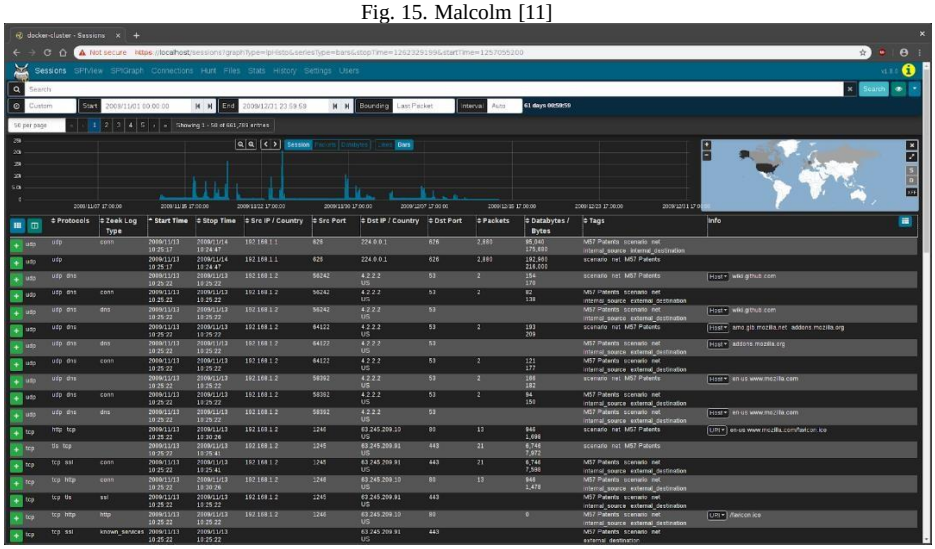


Esse processo envolve a monitoramento contínuo e a análise de dados para identificar padrões atípicos ou atividades maliciosas potenciais. A implementação eficaz desses mecanismos de alerta e monitoramento é necessária para garantir a integridade e segurança do ambiente, como documentado no perfil da NIST.

3.5 Responder e Recuperar

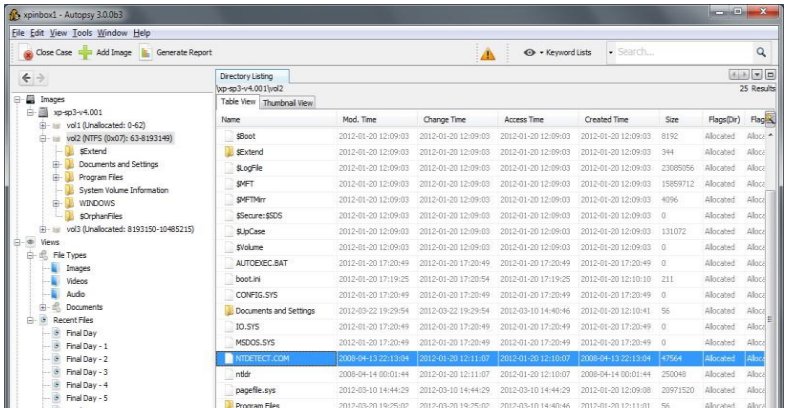
Conforme discutido na seção 3.1, as funções de resposta e recuperação são de pouca aplicabilidade direta para o usuário final, dado que a participação deste nas referidas etapas é limitada. Assim, é mais apropriado que esses serviços sejam gerenciados por especialistas e, consequentemente, a instalação destes em locais distintos, operando via conexão VPN para a comunicação com dispositivos do usuário final, é uma estratégia mais eficaz. Neste contexto, para a função de resposta, os serviços de Malcolm e Autopsy foram concebidos. Malcolm éuma solução de análise de tráfego de rede e segurança, projetada para processar, analisar e visualizar de maneira eficiente e automatizada grandes volumes de dados de tráfego de rede. Este software é capaz de interpretar dados de tráfego de rede, como arquivos PCAP (*Packet Capture*), identificando padrões, atividades suspeitas ou ameaças potenciais. A sua aplicação se estende na detecção de malware, ataques de rede e outras ameaças de segurança, auxiliando na rápida resposta das equipes de segurança. Como ele é *open-source*, Malcolm representa uma solução custo-eficiente em termos de manutenção

Fig. 15. Malcolm [11]



Por outro lado, o Autopsy é uma plataforma de análise *forense* digital, instrumental em investigações. Como aplicativo *open-source*, oferece uma variedade de módulos para a recuperação e análise de dados em sistemas computacionais, mostrando particularmente útil em investigações criminais, violações de segurança e na recuperação de dados pós-incidentes. O Autopsy é capaz de processar imagens de disco completo e dados de dispositivos móveis, além de permitir a visualização de eventos em uma linha do tempo e a geração de relatórios detalhados para documentação em procedimentos legais.

Fig. 16. Autopsy [12]



Portanto, com a implementação destes softwares em um servidor externo, que mantém comunicação com a rede doméstica, especialistas podem responder a incidentes que ocorram na residência, tanto em cenários de rede, utilizando Malcolm, quanto em cenários envolvendo dispositivos, com o uso do Autopsy.

Na fase de recuperação de dados, a implementação do software *open source* duplicati é uma opção como escolha. Este software é compatível com sistemas operacionais Windows, macOS e Linux, e se adequa a ambientes domésticos com diversidade tecnológica. O Duplicati permite a execução de backups em uma variedade de destinos, incluindodiscos locais, servidores NAS (*Network Attached Storage*) e plataformas de armazenamento em nuvem, como Google Drive, OneDrive e Dropbox.

Uma característica do Duplicati é a incorporação de criptografia, isso garante a segurança dos dados durante o armazenamento. Adicionalmente, o software facilita a configuração de rotinas de backup automáticas, e isso promove a regularidade na execução dos backups sem necessidade de intervenção manual contínua. A

interface do usuário do Duplicati é projetada para ser intuitiva, permitindo ser acessível até mesmo para indivíduos com conhecimento técnico limitado.

Duplicati suporta backups incrementais e diferenciais, e isso otimiza o uso de tempo e espaço de armazenamento ao copiar exclusivamente os arquivos que sofreram alterações desde o último backup realizado [13].

3. Resultados e Discussão

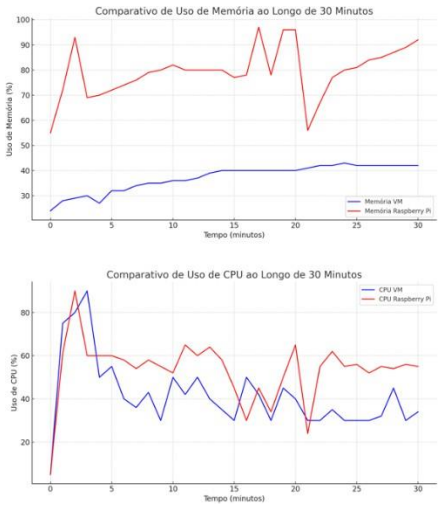
Nesta seção serão discutidos todos os passos seguidos pela metodologia, mostrando resultados encontrados e discussões para possíveis melhorias, ela é dividida em três momentos, Desempenho, Tecnologias e Casos de Uso;

4.1 Desempenho

Como dito na metodologia, a ideia do projeto seria criar um sistema SOC integrado em um único dispositivo, de preferência pequeno e portátil, para proteger uma residência usando como base a *framework* NIST. Entretando, devido a perdas de performance, foi considerado inviável continuar o projeto com o microprocessador, A figura 17 apresenta uma comparação entre as especificações da VM e do *Raspberry Pi*, incluindo a porcentagem de utilização da CPU e da memória após 30 minutos da instalação do primeiro serviço (Greenbone), durante o uso padrão deste.

Na análise comparativa entre o *Raspberry Pi* e a Máquina Virtual (VM) em relação ao desempenho dos recursos computacionais, observa-se que o *Raspberry Pi* apresentou uma utilização mais intensa e generalizada da Unidade de Processamento Central (CPU). Esse fenômeno é caracterizado por variações significativas no uso ao longo do período observado. Adicionalmente, considerando apenas a instalação do primeiro serviço, registrou-se uma tendência crescente no consumo de memória no *Raspberry Pi*, aproximando-se do limite máximo de capacidade, o que indica uma possível iminência de esgotamento de recursos.

Fig. 17. Comparativo uso de Recurso VM e *Raspberry PI* com apenas o greenbone instalado



Tal comportamento sugere que o *Raspberry Pi*, apesar de ser uma solução de baixo custo e eficiência energética, pode enfrentar desafios de desempenho quando submetido a cargas de trabalho crescentes ou intensivas. A análise do comportamento da memória, em particular, destaca a necessidade de monitoramento contínuo e possíveis estratégias de otimização para prevenir a degradação do desempenho em cenários de uso prolongado ou intensificado.

Essa mudança para uma VM foi motivada pela necessidade de superar as limitações de desempenho encontradas no *Raspberry Pi*, permitindo uma execução mais eficientedas atividades de cibersegurança propostas no projeto. A comparação das especificações e do desempenho entre as duas abordagens destaca a escolha pela VM como uma solução mais adequada às exigências do projeto.

Diante das adversidades enfrentadas, principalmente em relação à falta de memória, torna evidente a inviabilidade da continuidade da utilização do *Raspberry Pi* no prosseguimento do projeto, dadas as limitações de desempenho padrão e a insustentabilidade de seu uso contínuo.

A tabela 4 mostra comparação de *hardware* para diferentes modelos *Raspberry Pi*, com ela podemos observar que o servidor NIST seria mais viável caso fosse usado *Raspberry Pi* com especificações mais semelhantes a VM, principalmente no âmbito de memória, o *Raspberry Pi* 4 com 8GB de memória estaria mais próximo da realidade do trabalho pensando também no custo-benefício (869 R$ no fornecedor oficial), porém se estiver mais disposição no investimento um *Raspberry Pi 5(*1000 R$ no fornecedor oficial) permitiria mais poder de processamento

Relativo à performance do *Elastic Agent* em um dispositivo, a demanda por recursos é intrinsecamente dependente do número de serviços atribuídas ao agente. Conforme especificado na documentação oficial, para um monitoramento considerado básico, isto é, utilizando exclusivamente a integração *System* é recomendado que a máquina possua, no mínimo, 2 vCPUs, 1,7 gigabytes de espaço em disco e 1 gigabyte de memória [14].

Essa especificação de recursos serve como uma linha de base para assegurar o funcionamento do *Elastic Agent* sob uma configuração mínima. Contudo, é importante reconhecer que, à medida que integrações adicionais são empregadas, os requisitos de recursos podem aumentar proporcionalmente. Portanto, uma avaliação cuidadosa e ajustes correspondentes são essenciais para otimizar o desempenho do agente e garantir a coleta e análise eficazes de dados dentro do ambiente monitorado.

Tabela 4: Modelos *Raspberry PI*

Modelo	Ano de Lançamento	Processador	Memória RAM	Portas USB	Conectividade de Rede
Raspberry Pi 3 Modelo B+	**2018**	**1.4 GHz quad-core ARM Cortex-A53**	**1 GB**	**4x USB 2.0**	**Ethernet (300 Mbps), Wi-Fi, Bluetooth**
Raspberry Pi 3 Modelo A+	2018	1.4 GHz quad-core ARM Cortex-A53	512 MB	1x USB 2.0	Wi-Fi, Bluetooth
Raspberry Pi 4 Modelo B	2019	1.5 GHz quad-core ARM Cortex-A72	1/2/4/8 GB	2x USB 3.0, 2x USB 2.0	Ethernet (Gigabit), Wi-Fi, Bluetooth
Raspberry Pi 400	2020	1.8 GHz quad-core ARM Cortex-A72	4 GB	3x USB 2.0, 1x USB 3.0	Ethernet (Gigabit), Wi-Fi, Bluetooth
Raspberry Pi Zero 2 W	2021	1 GHz quad-core ARM Cortex-A53	512 MB	1x Micro USB	Wi-Fi, Bluetooth
Raspberry Pi 5	2023	2.4 GHz quad-core Arm Cortex-A76	4/8 GB	2x USB 3.0, 2x USB 2.0	Ethernet (Gigabit), Wi-Fi, Bluetooth

4.2 Tecnologias

O OpenVAS foi selecionado como a ferramenta primária para atender às demandas de identificação de dispositivos e vulnerabilidades em redes. Embora apresente certas restrições em sua base de dados de vulnerabilidades, o OpenVAS demonstra competência na identificação de vulnerabilidades em suítes de cifra SSL/TLS em portais de roteadores. Além disso, é capaz de detectar a ativação de protocolos como Telnet e/ou SSH na rede, uma funcionalidade crucial para a identificação de possíveis vulnerabilidades na infraestrutura. Na literatura [15] foi feito uma comparação sugerindo a inclusão de outras ferramentas de varredura de vulnerabilidades, conforme detalhado na tabela 5

Tabela 5: Comparação de *Scans* de Vulnerabilidade [8]

	Nessus (versão 10.0.2)	OpenVAS (Versão 7.0.3)	Nexpose (versão 6.6.120)	GFI *LanGuard* (versão 12.5)
Banco de CVEs	67K CVEs	<27K CVEs	<42K CVEs	60K
Sistema Operacional	Windows, Linux	Linux	Windows, Linux	Windows, Linux, MacOS
Facilidade na instalação	Fácil	Complexo	Fácil	Fácil
Templates de conformidades e configurações	+700 (DISA, STIG, HIPAA…)	Poucos *templates* oferecidos	Número limitado, pagando licença é liberado mais *templates*	PCI DSS, HIPAA, SOX, GLB/GLBA, ou PSN CoCo
Templates de Vulnerabilidades Pré-Configurado	*Templates* de vulnerabilidades importantes *(WannaCry, Spectre e Meltdown)*	Sem *templates* pré-configurado para *WannaCry, Spectre e Meltdown*	Sem *templates* pré-configurado para *WannaCry*, *Spectre* e *Meltdown*	Sem *templates* pré-configurado para *WannaCry*, *Spectre* e *Meltdown*
Custo	Inscrição para Nessus: $3000/ano para IPs ilimitado	Gratuito	$10000/ano para licença de 500 IPs, valor aumenta à medida que IPs	Preço começa com 26$/ano e varia dependendo das funcionalidades

	Nessus (versão 10.0.2)	OpenVAS (Versão 7.0.3)	Nexpose (versão 6.6.120)	GFI *LanGuard* (versão 12.5)
			aumentam	selecionadas
Relatório	Suporta formatos PDF, HTML, XML, CSV, Nessus DB	Suporta formatos PDF, HTML, XML, texto	Suporta formatos PDF, HTML, XML, CSV e RTF/texto	Suporta formatos PDF, HTML, XLS, XLSX,RTF e CSV
Scan de vulnerabilidades WLAN	Capaz de detectar um dispositivo agindo como um AP e encontrar Vulnerabilidades	Capaz de detectar vulnerabilidades em um APs	Capaz de detectar vulnerabilidades em um APs	Capaz de detectar vulnerabilidades em um APs e proativamente desativar
Detecção de Pontos de Acesso Rogue	Possível através de plugins	Sem plugins ou opções para detectar	Sem plugins ou opções para detectar	Possível detectar

Nessus Possui um banco de 67K CVEs, suporte a múltiplos sistemas operacionais, facilidade de instalação e um vasto conjunto de *templates* de conformidade, o Nessus se destaca como uma opção de qualidade elevada. No entanto, o custo anual de 3000 dólares para IPs ilimitados reduz sua atratividade para o cenário do projeto.

OpenVAS é uma solução gratuita e capaz de identificar vulnerabilidades em APs, devido a isso, o OpenVAS é uma escolha atraente e a que foi testada, a complexidade na instalação, configuração e da limitação de menos de 27K CVEs, assim como ausência de *plugins* são pontos negativos.

Nexpose Oferece uma quantidade significativa de CVEs e suporte a múltiplos sistemas operacionais. Ele é flexível nos custos conforme aumento os IPs, e isso torna o *scan* adaptável a diferentes escalas de redes.

GFI *LanGuard* é compatível com uma ampla gama de sistemas operacionais e um custo variável que começa em 26 dólares/ano, é uma opção acessível para redes domésticas. A capacidade de detectar e desativar proativamente vulnerabilidades em APs também é uma vantagem significativa.

Levando em consideração essas informações, implementar um servidor de vulnerabilidade, deve considerar a relação custo-benefício, a complexidade de instalação, manutenção e a abrangência do banco de CVEs. Dependendo da rede e da pessoa, uma característica possui mais peso na escolha do software que outra. O OpenVAS, apesar de suas limitações, oferece um ponto de partida adequado devido ser gratuito e capacidade de identificar de vulnerabilidades comuns. No entanto, para uma cobertura mais abrangente e recursos avançados, ferramentas como o Nessus e o GFI *LanGuard* podem ser consideradas, levando em conta o orçamento e as necessidades específicas da rede. A escolha final deve equilibrar a necessidade de segurança com a viabilidade e praticidade dentro do contexto doméstico.

A solução SIEM, em que cobre a função de detectar na NIST CSF, [16] fizeram uma pesquisa com vários softwares SIEM de código aberto, a tabela 6 nos mostra o resultado dessa pesquisa, com ele podemos deduzir pontos positivos e negativos para cada tecnologia de código aberto, lembrando que todas as soluções pesquisadas possuem formato pago.

Tabela 6: Comparação SIEM [16]

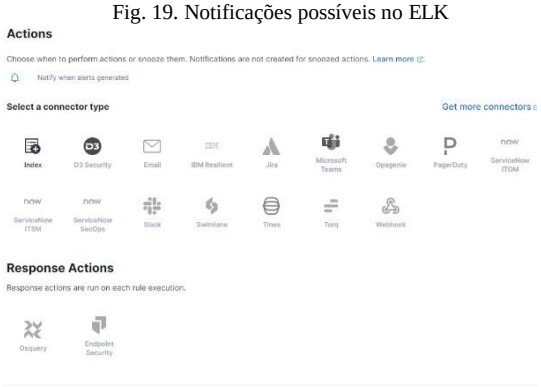
Funcionalidade	OSSIM	ELK	Splunk *Free*	*Graylog*
Licença	Código Aberto	Código Aberto	Código Aberto	Código Aberto
Identificação de vulnerabilidades	Sim	Não	Não	Não
Correlação de Eventos SIEM	Sim	Não	Não	Não
Gestão de logs	Não	Sim	Sim	Sim
Relatórios	Sim	Não	Sim	Não
Escalabilidade	Não	Sim	Sim	Sim
Pesquisa	Estruturada	Abrangente	Abrangente	Abrangente

Alertas via email	Possui	Versão Paga	Versão Paga	Possui
Instalação dos Agentes	Médio/Difícil	Médio/Difícil	Fácil	Médio/Difícil

OSSIM (*Alien Vault*) É a única solução que oferece identificação de vulnerabilidades e correlação de eventos SIEM, tornando-a uma escolha adequada para uma proteção abrangente, ele também oferece relatórios e autenticação, componentes importantes para monitoramento e segurança. Porém a falta de gestão de logs pode limitar aumenta sua complexidade. A instalação dos agentes foi considerada média/difícil na pesquisa, o que pode ser um desafio para usuários menos experientes.

ELK foi o software usado no projeto, a pesquisa abrangente facilita a análise de dados. Porém ele não oferece relatórios nem autenticação, o que pode limitar a visão geral e a segurança. Além disso, envio de alertas é extremamente limitado na versão gratuita, caso utilizar a versão paga é possível enviar alertas para vários serviços de alerta, inclusive email, como mostra a figura 18, o tom preto significa disponível no gratuito, tom cinza significa somente disponível na versão paga.

Fig. 19. Notificações possíveis no ELK



Splunk Free Possui gestão de logs, e a facilidade na instalação de agentes é o fator mais atrativo, o que é ideal para usuários residenciais. Porém, ele não permite criação de alertas, e somente permite ingestão de 500 MegaBytes por dia, e assim como o ELK, não oferece identificação de vulnerabilidades nem correlação de eventos SIEM.

Graylog Foi o melhor SIEM pensando em redes residenciais, ele pode enviar alertas via email de maneira gratuita, método de pesquisa de logs abrangente, possui gestão de logs. Porém, apesar de ter mais benefícios como SIEM, ele não tem funcionalidades de EDR como o Elastic, deixando então o ambiente mais complexo e uso de mais recurso se fosse usado.

4.3 Casos de Uso

Para avaliar a eficácia das ferramentas de proteção em uma rede doméstica, foram conduzidos dois tipos distintos de ataques onde seus métodos de detecção são diferentes, *reverse shell* e *rogue AP*.

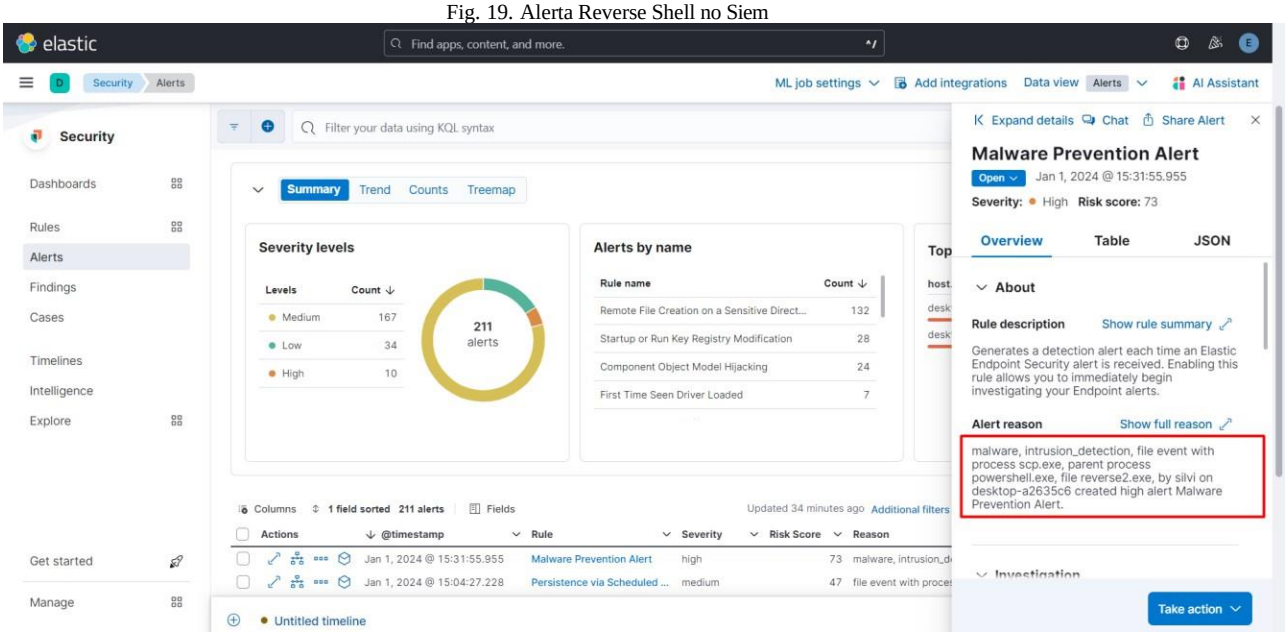
O primeiro ataque empregou malware destinado a estabelecer um *reverse shell* na máquina alvo. O método consistiu na criação de um malware que estabelece uma conexão reversa. Neste cenário, a máquina do atacante, simulada pelo servidor NIST, transmitiu o malware para o usuário de destino, identificado pelo IP 192.168.1.2. Assim que o usuário clicou no executável, a conexão foi estabelecida, permitindo o controle remoto da máquina. Este processo é ilustrado na figura 2.

A transferência do executável poderia ser efetuada por diversos meios, incluindo e-mail, *WhatsApp* ou links em sites. No entanto, para simplificação, optou-se por um comando de transferência de arquivo remoto na estação de trabalho. Durante a tentativa de transferência, o EDR do Elastic bloqueou a ação, como demonstrado na Figura 18.

Fig. 18. Tentativa de ataque *reverse shell* e seu bloqueio

Consequentemente, um alerta foi enviado para o SIEM, conforme ilustrado na Figura 19. Embora seja possível configurar o envio de alertas via e-mail para a vítima ou para o responsável pela rede, essa funcionalidade é um serviço pago no *ELK Stack* e, portanto, não foi implementada neste estudo

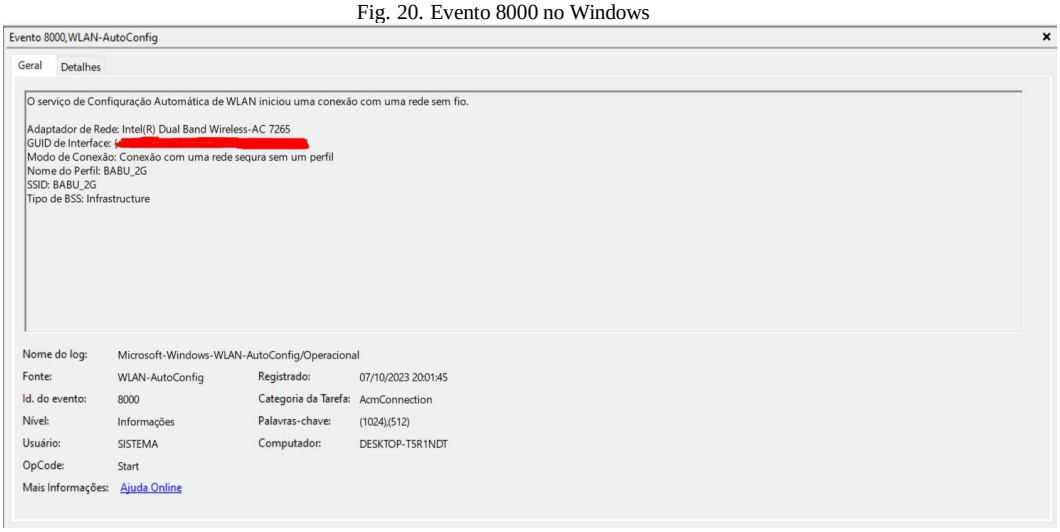
Fig. 19. Alerta Reverse Shell no Siem



A implementação do ataque *rogue AP* demandou a criação de um alerta personalizado e a instalação de uma ferramenta específica do *ELK Stack* no host. Notavelmente, os eventos do Windows relacionados à conexão Wi-Fi são registrados em um local diferente do usual, denominado *WLAN AutoConfig*. Esses registros podem ser encontrados em Logs de Aplicativos e Serviços > Microsoft > Windows > *WLAN-AutoConfig* > Operacional. Consequentemente, para realizar o monitoramento, foi necessário a instalação do Winlogbeat no dispositivo alvo. O *Winlogbeat* oferece a vantagem de ser configurável para ler qualquer canal de log de eventos do Windows, proporcionando assim uma maior capacidade de personalização no monitoramento.

Após a instalação e configuração do Winlogbeat, a próxima etapa é a identificação do log específico para a detecção da anomalia. O *log* de interesse possui o ID 8000, gerado quando um dispositivo estabelece conexão bem-sucedida com uma rede sem fio. Diversos parâmetros são registrados nesse *log*, conforme ilustrado na figura 20, sendo o nome da rede, ou SSID, o dado de maior relevância para esta análise. Conforme discutido anteriormente na Seção 2.6, um ataque *rogue AP* ocorre quando um usuário se conecta inadvertidamente a uma rede Wi-Fi não autorizada e desprotegida, frequentemente devido à similaridade nos nomes das redes. Portanto, para identificar tal anomalia, é preciso estabelecer um alerta que notifique quando um usuário se conectar a uma rede cujo nome difere da rede pré-estabelecida.

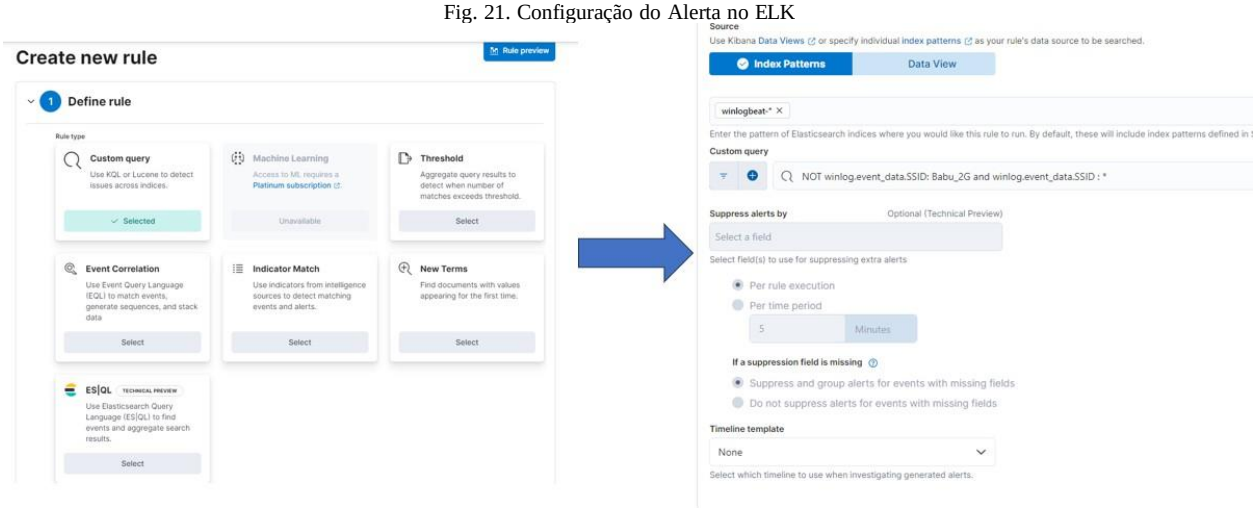
Fig. 20. Evento 8000 no Windows



Para implementar as condições necessárias no Kibana, é preciso criar comandos utilizando a *Kibana Query Language* (KQL). O KQL é uma linguagem de consulta desenvolvida pela Elastic, especificamente para uso com o Elastic Stack. Essa linguagem é projetada para simplificar a exploração e análise de grandes volumes de dados, permitindo aos usuários formular consultas complexas de maneira mais acessível. A figura 21 ilustra a aplicação do KQL para o caso em questão. Primeiramente, é especificado a regra que será baseada em uma consulta personalizada. Em seguida, é filtrado a origem dos *logs* a serem analisados, neste caso, o

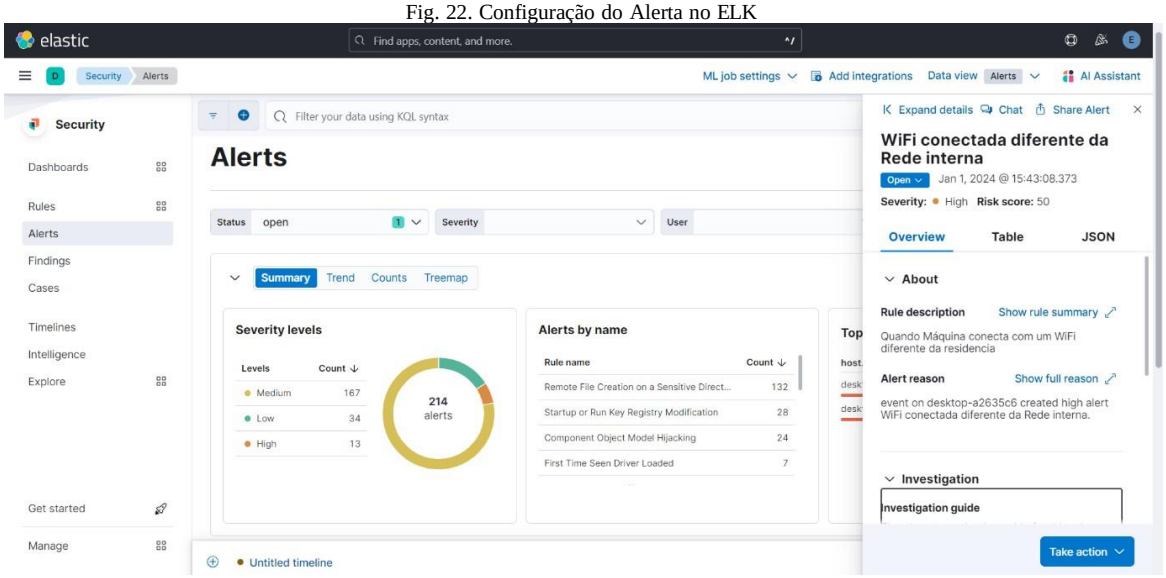
Winlogbeat. Essa filtragem é crucial para evitar consultas extensas e desnecessárias no banco de dados do Elastic. Por último, definimos as condições: o alerta será acionado quando o evento do SSID for diferente do nome da rede residencial especificada (Babu2G) e o campo correspondente ao SSID não estiver vazio.

Fig. 21. Configuração do Alerta no ELK



A figura 22 mostra o alerta aparecendo ao conectarem uma rede diferente. Repare que o corpo do alerta já mostra o nome da máquina e sua severidade, para uma rápida resposta do usuário.

Fig. 22. Configuração do Alerta no ELK



4. Conclusão

O estudo demonstrou que é possível adaptar a *framework* para identificar falhas de segurança em redes residenciais. Através da implementação de práticas recomendadas e da utilização de tecnologias como SIEM, EDR e varredura de vulnerabilidades, sendo capaz de manter uma rede segura, identificando vulnerabilidades e dispositivos, prevenindo ataques e alertando quando ocorrem, com o custo dependendo das demandas do usuário, envolvendo inicialmente somente o custo do *hardware* e aumentando à medida que o usuário requisitar mais funcionalidades ou softwares mais robustos para melhorar a segurança da residência.

Porém, em muitos momentos seria necessário suporte técnico especializado, principalmente quando se trata da instalação do dispositivo, e das funções de responder e recuperar. Também seria necessário o treinamento dos usuários para interpretação dos alertas e relatórios recebidos e deixar claro o que devem fazer caso sofram um ataque.

Portanto, podemos concluir que um sistema de segurança completo está fora do alcance de um usuário com pouco conhecimento na área de segurança da informação, sendo necessário mesmo depois da instalação de todos os dispositivos e ferramentas, a necessidade de suporte para implementação, sustentação e acompanhamento.

Com o uso em massa de *cloud*, talvez seja mais interessante a implementação da ferramenta não como um servidor NIST local, mas sim com um *proxy* para enviar os *logs* do dispositivo de maneira

segura para servidores na *cloud*, onde estes seriam sustentados por especialistas, enquanto estes mesmos analisam eventuais problemas levando em consideração a *framework*, dessa forma seria possível criar um produto com escalabilidade, onde todas as informações seriam presentes em uma central de segurança, como ocorre em grandes corporações atualmente. Porém, levando em consideração este raciocínio, o próximo desafio seria delimitar a linha entre segurança e privacidade, duas faces da mesma moeda e alvo de longas horas de discussão tanto em grandes conferências internacionais quanto na sua mesa de bar mais próxima.

Outra forma mais direta de implementar a *framework* é retirar totalmente a responsabilidade do usuário e colocar na mão de especialistas que trabalham para as grandes empresas. Onde estes conseguiriam detectar e monitorar os dispositivos pertencentes a empresa que está em posse do trabalhador remoto, isso permitiria toda o suporte e implementação da *framework*, além de fornecer um nível maior de segurança para empresas que possuem trabalhadores remotos.

No final, com a crescente ascensão da Inteligência Artificial, fica cada vez mais fácil criar software malicioso e comprometer uma residência, e da mesma maneira, devemos cada vez mais simplificar a compreensão e melhorar a defesa para o usuário comum, este que incorpora todos os dias mais produtos digitais em seu dia-a-dia, e consequentemente, no ambiente que muitas vezes se sente mais seguro, seu lar.

AGRADECIMENTOS

Gostaria de agradecer minha família, que compartilharam todos os momentos bons e ruins que permitiu chegar até esse momento. Meu pai e minha mãe pelos conselhos, amor, afeto e apoio, meu irmão pela inspiração que me traz todos os dias.

Meus amigos que percorreram todo o curso junto comigo, Ronan, Heinrych, Vinicius e Artur e pelos aprendizados que veio junto.

Meu Orientador, Carlos Galvão, pelos conselhos, ideias e conhecimentos que permitiu eu chegar até aqui.

E acima de tudo a Deus, por ter me dado a oportunidade de crescer nessa instituição de ensino e conhecer todas as pessoas maravilhosas que fizeram parte dessa jornada comigo.

REFERÊNCIAS

[1] S. Furnell, “Home working and cyber security-an outbreakof unpreparedness?” 2020.

[2] White House (2013), Ordem Executiva 13636: Disponivel em: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[3] NIST. (2018) Framework documents. [Online]. Disponivel em: https://www.nist.gov/cyberframework/framework

[4] (2022) Updating the nist cybersecurity framework journey to csf 2.0.[Online].Disponivel em: https://www.nist.gov/cyberframework/updating-nist cybersecurity-framework-journey-csf-20

[5] (2014) History and creation of the framework. [Online]. Disponivel em: https://www.nist.gov/cyberframework/ online-learning/history-and-creation-framework

[6] Chris. Python one line reverse shell. [Online]. Disponivel em: https://blog.finxter.com/python-one-line-reverse-shell/

[7] J. O. Agyemang, J. J. Kponyo, G. S. Klogo, and J. O. Boateng, “Lightweight rogue access point detection algorithm for wifi-enabled internet of things(iot) devices,” *Internet of Things*, vol. 11, p. 100200, 2020. [Online]. Disponível em:https://www.sciencedirect.com/science/article/pii/S2542660518301501

[8] B. Wilson. Should i use kali linux? [Online]. Disponivel em: https://www.kali.org/docs/introduction/should- i-use-kali-linux/

[9] K. Team. Kali linux 2023.1 release. [Online]. Disponivel em: https://www.kali.org/blog/kali-linux-2023-1-release/

[10] devanshu. What is elastic stack? [Online]. Disponivel em: https://www.geeksforgeeks.org/what-is-elastic-stack-and-elasticsearch/

[11] ZION3R. (2019) Malcolm - a powerful, easily deployable network traffic analysis tool suite for full packet capture artifacts (pcap files) and zeek logs. [Online]. Disponivel em: https://www.kitploit.com/2019/08/ malcolm-powerful-easily-deployable.html

[12] B.Carrier.Autopsy.[Online].Disponivel em:https://www.sleuthkit.org/autopsy/

[13] Duplicati 2.0 [Online]. Disponivel em: https://www.duplicati.com

[14] E. Team. (2023) Install elastic agents. [Online]. Disponivel em: https://www.elastic.co/guide/en/fleet/current/ elastic-agent-installation.html

[15] A. Kejiou and G. Bekaroo, “A review and comparative analysis of vulnerability scanning tools for wireless lans,” in 2022 3rd International Conference on Next Generation Computing Applications (NextComp), 2022, pp. 1–6.

[16] A. Vazão, L. Santos, M. B. Piedade, and C. Rabadão, “Siem open source solutions: A comparative study,” in 2019 14th Iberian Conference on Information Systems and Technologies (CISTI), 2019, pp. 1–5.

Luan Weba Soares, é estudante de Engenharia de Computação na Universidade Federal de Goiás, possui certificações CompTia Security+, Cisco CCNA e Fortinet NSE4 e tem atuado no setor de Redes e Segurança a 8 meses. Utiliza principalmente ferramentas como *Firewalls*, *EDR* e *VPN* em seu trabalho. Possui forte interesse em cibersegurança, mais especificamente em SOC e resposta a incidentes.