CENTRO UNIVERSITÁRIO UNIFECAF
GESTÃO TECNOLOGIA DA INFORMAÇÃO

Dannyelly Dayane Queiroz

Fortalecimento da Segurança Digital: Análise de Malware, Monitoramento de Tráfego de Rede e Varredura de Vulnerabilidades

Taboão da Serra,
SP 2024

DANNYELLY DAYANE QUEIROZ

DESAFIO DE SEGURANÇA CIBERNÉTICA: AUMENTANDO A CONSCIENTIZAÇÃO E A PROTEÇÃO DIGITAL EM AMBIENTES CORPORATIVOS

Trabalho apresentado como requisito parcial de avaliação da disciplina **Cyber Security** do Curso de Graduação em **Gestão Tecnologia da Informação** do Centro Universitário UniFECAF.

Tutor(a): **Fernando Leonid**

Taboão da Serra,

SP

LISTA DE FIGURAS

SUMÁRIO

1. INTRODUÇÃO

O avanço das tecnologias e a crescente interconexão de redes tornam o ambiente digital mais complexo e vulnerável a ameaças cibernéticas. Ataques como phishing, ransomware, vazamento de dados e explorações de vulnerabilidades são apenas alguns dos riscos que podem comprometer a operação e a reputação de instituições como o TSTI.

A segurança digital é uma necessidade estratégica para organizações que dependem da tecnologia para suas operações diárias. O Taboão da Serra Tech Institute (TSTI), como uma instituição educacional voltada para a inovação e o aprendizado, enfrenta desafios significativos para proteger sua infraestrutura tecnológica e os dados sensíveis de alunos, professores e funcionários.

Diante desse cenário, é essencial desenvolver um plano de segurança digital que identifique riscos, monitore a rede para comportamentos suspeitos e implemente soluções práticas para mitigar vulnerabilidades. Este projeto se propõe a estruturar um conjunto de ações e estratégias baseadas em ferramentas como VirusTotal, Wireshark e Nmap, alinhando a proteção cibernética à missão do TSTI de proporcionar um ambiente seguro para o aprendizado e a inovação.

Além disso, o plano reforça a importância de criar uma cultura de segurança digital na instituição, envolvendo a capacitação de colaboradores e a conscientização de toda a comunidade acadêmica. A segurança digital, portanto, não é apenas uma responsabilidade técnica, mas uma prioridade estratégica para garantir a continuidade, a confiabilidade e o crescimento sustentável do TSTI.

2. OBJETIVO

O objetivo principal deste plano é fortalecer a segurança digital do TSTI por meio da identificação de vulnerabilidades, monitoramento contínuo de redes e implementação de ferramentas avançadas de análise, como VirusTotal, Wireshark e Nmap. Este projeto também busca:

- Mitigar riscos e prevenir incidentes cibernéticos.
- Implementar práticas de segurança robustas e alinhadas às regulamentações.

- Conscientizar colaboradores e alunos sobre a importância da segurança digital.
- Estabelecer um plano contínuo de evolução e resposta a incidentes.

3. PESSOAS AFETADAS

A falta de conscientização em segurança cibernética pode afetar diversos setores e níveis de uma empresa, prejudicando não apenas os funcionários, mas também outros stakeholders, como gestores, clientes, fornecedores e investidores. Essa falta de preparação torna a empresa vulnerável a uma série de ataques cibernéticos que podem ter consequências graves e de longo prazo. A seguir vamos detalhar cada um:

a) Funcionários

Os funcionários são o grupo mais diretamente afetado pela falta de conscientização em segurança cibernética. Isso ocorre principalmente porque eles representam o elo mais fraco na cadeia de segurança da informação. Muitos ataques cibernéticos, como o phishing, dependem de enganar o funcionário para que ele forneça dados sensíveis ou clique em links maliciosos. A falta de treinamento adequado e a falta de conhecimento sobre práticas seguras deixam os colaboradores vulneráveis a cometer erros.

b) Clientes

Os clientes são impactados diretamente pela falta de segurança cibernética principalmente quando seus dados pessoais e financeiros são comprometidos pela empresa.

c) Setor de TI

O setor está diretamente afetado pela falta de conscientização em segurança cibernética, pois são os responsáveis pela proteção e manutenção da infraestrutura tecnológica da empresa. E quando os funcionários não estão preparados ou informados sobre as melhores práticas de segurança, as medidas implementadas pela equipe de TI podem ser comprometidas, tornando-se ineficazes.

4. IMPORTÂNCIA DA SEGURANÇA DIGITAL

A crescente relevância da Cibersegurança tem sido amplamente demonstrada pelas frequentes notícias sobre grandes ciberataques e ameaças cibernéticas que afetam organizações em todo o mundo. De acordo com a Kaspersky, cibersegurança é a prática que protege computadores e servidores, dispositivos móveis, sistemas eletrônicos, redes e dados contra ataques maliciosos. Também é chamada de segurança da tecnologia da informação ou segurança de informações eletrônicas. O termo é aplicável a uma variedade de contextos, desde negócios até computação móvel, e pode ser dividido em algumas categorias comuns.

No contexto da economia digital, a cibersegurança não pode ser vista como uma preocupação isolada, mas deve ser priorizada em todos os setores da sociedade e da economia. Silva enfatiza que, no ambiente digital, a informação é um ativo crucial para as empresas, permitindo o desenvolvimento de novas oportunidades de negócios. Ao utilizar dados dos clientes, as organizações podem otimizar seus processos e criar estratégias mais eficazes.

Contudo, a cibersegurança vai além da simples implementação de tecnologias avançadas. Como destacado pelo Silva, “a proteção digital deve ser vista como um conjunto integrado que envolve tecnologia, pessoas e processos.” Não adianta uma empresa adquirir os equipamentos de segurança mais modernos ou adotar softwares conceituados se ela não contar com profissionais capacitados em segurança cibernética. Além disso, a cultura organizacional e a conscientização dos colaboradores são fundamentais, uma vez que práticas como a engenharia social podem ser exploradas por cibercriminosos.

Os ataques cibernéticos têm um impacto enorme e crescente nas empresas e na economia. Segundo estimativas da IBM, o crime cibernético custará à economia mundial US$ 10,5 trilhões por ano até 2025. Esse impacto financeiro sublinha a urgência da implementação de estratégias eficazes de cibersegurança para proteger os ativos digitais das organizações e garantir sua continuidade operacional.

Sendo assim, a cibersegurança é uma questão estratégica que deve ser abordada de maneira abrangente e contínua, combinando investimentos em tecnologia com treinamento de pessoal e uma forte governança de processos. Só assim será possível mitigar as ameaças cibernéticas e garantir que o potencial da

economia digital seja verdadeiramente desbloqueado, sem comprometer a integridade e a privacidade das informações.

5. PRINCÍPIOS DA CIBERSEGURANÇA

As informações são ativos valiosos para as empresas, sendo assim, indispensável que as informações sejam seguras. Segundo Silva, para que isso ocorra as informações devem satisfazer três princípios fundamentais, conhecidos como a tríade CIA sendo eles:

a) Confidencialidade

"propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados" (ABNT, 2006);

b) Integridade

"propriedade de salvaguarda da exatidão e completeza de ativos" (ABNT, 2006)

c) Disponibilidade

"propriedade de que (um sistema de) informação esteja acessível e utilizável sob demanda por uma entidade autorizada" (ABNT, 2006);

6. DESAFIOS DA CIBERSEGURANÇA

A cibersegurança é um campo complexo e dinâmico, e os desafios enfrentados pelas organizações se tornam cada vez mais conectados à medida que as tecnologias evoluem e as ameaças cibernéticas se tornam mais sofisticadas. Um dos principais desafios é o aumento da sofisticação dos ataques. Os cibercriminosos aprimoram constantemente suas técnicas, utilizando malwares avançados, ransomwares, ataques de phishing mais elaborados e até técnicas como botnets e ataques de dia zero, que exploram falhas desconhecidas nos sistemas. Com isso, as organizações precisam estar constantemente atualizadas e preparadas para identificar e mitigar esses ataques antes que causem danos significativos.

As ameaças internas também se apresentam como um desafio crucial. Embora os ataques externos sejam frequentemente a principal preocupação, as ameaças internas podem ser igualmente prejudiciais. Funcionários ou ex-funcionários com más intenções ou negligência podem comprometer sistemas, expor dados sensíveis ou até facilitar o acesso de atacantes. Para lidar com isso, é necessária uma gestão

cuidadosa de acessos e uma vigilância constante sobre as atividades dos usuários dentro da organização.

Outro desafio relevante é a falta de conscientização e de uma cultura de segurança consolidada. Muitas vezes, as organizações falham em comunicar a importância da cibersegurança para seus funcionários. A ausência de treinamento adequado pode resultar em comportamentos de risco, como o uso de senhas fracas, o clique em links fraudulentos e o compartilhamento imprudente de informações sensíveis. Para mitigar esse risco, é necessário promover uma cultura de segurança, com treinamentos regulares e uma comunicação eficaz sobre os riscos cibernéticos.

A resposta a incidentes e recuperação de desastres também é um grande desafio. Embora as organizações possam adotar medidas preventivas para reduzir o risco de ataques, é inevitável que incidentes de segurança aconteçam. Ter um plano de resposta eficaz é crucial para minimizar os danos e restaurar rapidamente as operações. Muitas empresas, no entanto, não possuem processos bem definidos ou equipes treinadas para responder a incidentes de segurança de maneira eficiente.

No caso do TSTI, a segurança digital enfrenta desafios semelhantes aos enfrentados por outras organizações, mas com características próprias. A instituição lida com dados altamente sensíveis de pesquisas e inovações tecnológicas, que são alvos para ataques. Além disso, a crescente complexidade tecnológica da instituição, com sistemas conectados a diversas áreas operacionais, cria múltiplos pontos de entrada para ataques. A evolução constante das ameaças cibernéticas e o uso crescente de malwares sofisticados tornam ainda mais difícil a proteção total.

A falta de uma cultura de segurança consolidada dentro do TSTI é outro desafio importante. A crescente falta de recursos humanos especializados em segurança digital é um fator que contribui para a vulnerabilidade da instituição. A medida que o TSTI expande suas operações e sistemas, a implementação de uma estratégia robusta de segurança cibernética, com treinamento contínuo para todos os colaboradores e alunos com ferramentas adequadas de monitoramento e mitigação de riscos, torna-se crucial para garantir a proteção de seus dados e a continuidade de suas operações.

7. RISCO

Segundo Hertzberger, "um risco é a probabilidade de um agente ameaçador tirar vantagem de uma vulnerabilidade e o correspondente impacto nos negócios. Se um firewall tem diversas portas abertas, há uma maior probabilidade de um invasor usar uma delas para acessar a rede de forma não autorizada.”

No contexto do TSTI, os riscos incluem a possibilidade de invasões na rede devido a portas expostas, acesso indevido a informações sigilosas e a interrupção de serviços essenciais devido a ataques cibernéticos.

6.1. Gestão de riscos

A gestão de riscos é um processo essencial para a segurança da informação e para a proteção das operações e ativos de uma organização. A ISO/IEC 27005 fornece orientações detalhadas para a gestão dos riscos de segurança da informação, alinhando-se às melhores práticas e normas internacionais, como a ISO/IEC 27001 e a ISO 31000.

As normas visam minimizar os efeitos adversos de possíveis ameaças e maximizar as oportunidades, e é composta por 5 etapas: identificar, avaliar, tratar e monitorar os riscos à segurança da informação.

A gestão de riscos começa com a compreensão do contexto da organização, incluindo fatores externos e internos que podem afetar os objetivos e operações da empresa. Esse contexto envolve variáveis sociais, políticas, econômicas, tecnológicas e até mesmo culturais.

8. IDENTIFICAÇÃO

7.1. Ameaças Internas e Externas identificadas:

a) Malware

O TSTI já sofreu detecção de malware, que pode comprometer sistemas críticos.

b) Comportamento anômalo no tráfego de rede

Indicando a possibilidade de um ataque de rede em andamento, como DDoS ou tentativas de intrusão.

c) Portas vulneráveis

A exposição de portas vulneráveis na infraestrutura da organização, que pode ser explorada por atacantes para obter acesso não autorizado.

7.2. Vulnerabilidades identificadas:

a) Sistemas desatualizados e com patches de segurança pendentes.

b) Falhas em controles de tráfego de rede e no monitoramento de atividades suspeitas.

c) Insuficiência de políticas de segurança ou implementação inadequada de ferramentas de proteção.

7.3. Avaliação

Após os riscos identificados, é preciso avaliar a probabilidade de ocorrência e o impacto de cada risco. Para o TSTI, a avaliação pode ser feita com base em uma matriz de riscos, onde foi atribuída a de probabilidade (baixa, média, alta) e impacto (baixo, médio, alto) a cada risco identificado, conforme tabela a seguir:

Figura 1- Riscos e Probabilidades

Risco	Probabilidade	Impacto	Classificação do Risco
Malware	Alta	Alto	Crítico
Comportamento anômalo no tráfego de rede	Média	Alto	Alto
Exposição de portas vulneráveis	Alta	Médio	Alto
Falta de controles de segurança	Média	Médio	Médio

Fonte- Criação Própria

9. AMEAÇA

De acordo com Hertzberger, “uma ameaça é uma potencial causa de um incidente não desejado, o que pode resultar em prejuízo ao sistema ou à organização. A entidade que tirar vantagem de uma vulnerabilidade é referida como agente ameaçador.

8.1. Tipos de ameaças

O TSTI enfrenta ameaças como malware, ataques de phishing, exploração de

vulnerabilidades em software e tentativas de acesso não autorizado por agentes mal-intencionados. Nesse topicos, vamos entender o que são cada um e como vamos evita-los na TSTI.

a) Vírus

Um vírus, conforme explicado pela McAfee, é um tipo de malware que geralmente vem como um anexo em um e-mail ou como parte de um arquivo que executa uma ação maliciosa assim que é aberto pelo usuário. Após a vítima abrir o arquivo, o dispositivo é infectado, permitindo que o vírus se espalhe ou cause danos aos dados armazenados (McAfee, 2025).

b) Ransomware

Este tipo de malware criptografa os arquivos da vítima e exige um resgate (geralmente pago em Bitcoin) para devolver o acesso aos dados. O ransomware tem sido um dos ataques mais rentáveis para os cibercriminosos, devido à pressão que exerce sobre as vítimas para pagar o resgate rapidamente (McAfee, 2025).

c) Scareware

Os cibercriminosos utilizam o scareware para enganar os usuários, fazendo-os acreditar que seus sistemas estão infectados com malware. Um exemplo típico é a exibição de mensagens pop-up alarmantes, como "Aviso: seu computador está infectado!" com o objetivo de convencer a vítima a comprar um software falso de segurança (McAfee, 2025).

d) Worms

Os worms são malwares autossuficientes, ou seja, eles têm a capacidade de se copiar e se propagar automaticamente de uma máquina para outra, muitas vezes explorando falhas de segurança em sistemas operacionais ou softwares. O mais preocupante dos worms é que eles não exigem interação do usuário para se espalharem (McAfee, 2025).

e) Spyware

O spyware é um software que é instalado no computador da vítima, geralmente sem o seu conhecimento, para capturar e transmitir informações pessoais ou detalhes de navegação na Internet. Frequentemente usado para monitoramento de comunicações, o spyware pode ser empregado para coletar dados como senhas, números de cartão de crédito e hábitos de navegação (McAfee, 2025).

f) Cavalos de Troia (Trojan Horse)

Este tipo de malware disfarça-se como um programa aparentemente legítimo,

mas uma vez executado, ele pode roubar dados, danificar arquivos, espionar o usuário ou até mesmo abrir uma "porta dos fundos" para que outros ataques ocorram (McAfee, 2025).

g) Adware

O adware é um tipo de malware que exibe anúncios indesejados aos usuários, como janelas pop-up ou banners intrusivos. Normalmente, ele é instalado quando o usuário aceita baixar um software gratuito ou compartilha um arquivo de origem duvidosa (McAfee, 2025).

h) Malware Sem Arquivo

Este tipo de malware é mais sofisticado, pois não deixa arquivos ou rastros de sua atividade no sistema. Ele utiliza programas legítimos para infectar o computador e pode ser extremamente difícil de detectar e remover, uma vez que não deixa vestígios (McAfee, 2025).

8.2. Análise do malware

A análise de malware é um processo crucial para identificar, entender e neutralizar ameaças cibernéticas. Existem dois tipos principais de análise de malware: estática e dinâmica. Ambas têm suas vantagens e são frequentemente usadas em conjunto para obter uma visão completa do comportamento e dos impactos de um malware.

Para o TSTI vamos usar a análise estática, onde o arquivo ou URL é examinado sem ser executado. Com a ferramenta VirusTotal, que analisa o código, as assinaturas de malware, a estrutura do arquivo e outras características estáticas. Ele busca por "assinaturas" que indicam que aquele arquivo ou URL é malicioso com base em um banco de dados de malware conhecido. Porém, tem como desvantagem, a depependencia de assinaturas de antivírus e de motores de análise conhecidos para identificar ameaças. Isso significa que ele pode não detectar novas ameaças

Diferente da analise estática, a analise dinâmica, executa o arquivo ou URL e observa como age quando em execução, identificando comportamentos maliciosos como a criação de arquivos, tentativas de conexão a servidores externos, ou modificação de sistemas. Entretanto, esse tipo de análise é realizado em ambientes controlados, como sandboxes ou máquinas virtuais.

10. VIRUS TOTAL

> O VirusTotal inspeciona itens com mais de 70 scanners antivírus e serviços de lista de bloqueio de URL/domínio, além de uma infinidade de ferramentas para extrair sinais do conteúdo estudado. Qualquer usuário pode selecionar um arquivo de seu computador usando seu navegador e enviá-lo para o VirusTotal. O VirusTotal oferece vários métodos de envio de arquivos, incluindo a interface pública da Web primária, uploaders de desktop, extensões de navegador e uma API programática. (VirusTotal, 2025)

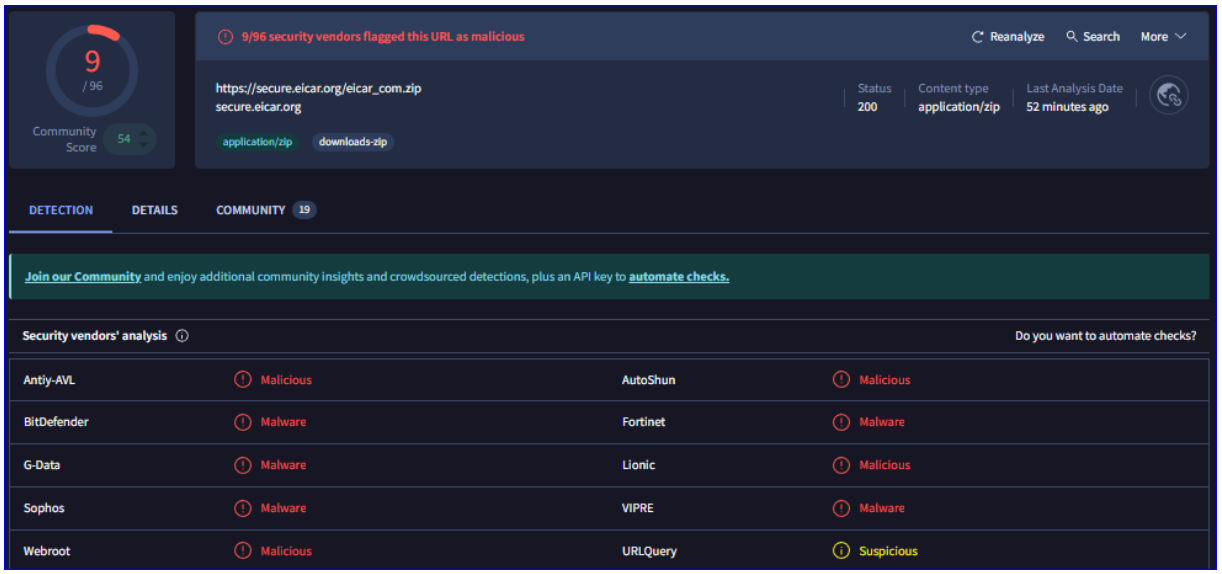
O VirusTotal é bastante eficiente para detecção de ameaças conhecidas, fornecendo uma verificação abrangente através de múltiplos antivírus, o que aumenta a precisão da identificação de malwares.

No entanto, também tem limitações. Uma delas é a restrição de tamanho para arquivos na versão gratuita (25 MB), o que pode ser um problema quando se precisa analisar arquivos grandes. Além disso, o VirusTotal realiza uma análise estática, o que significa que ele não consegue detectar comportamentos dinâmicos do malware, como a exfiltraçã.o de dados ou a comunicação com servidores de comando e controle em tempo real. Isso limita a capacidade de identificar ameaças mais sofisticadas que podem se esconder durante a execução.

9.1. Detalhamento dos resultados no Virus Total

Na imagem a seguir, observamos o site VirusTotal em ação. Após inserção da URL para análise, o sistema realizou a inspeção com mais de 96 scanners antivírus que sinalizou a URL como malware A detecção de malware em arquivos e URLs tem implicações significativas para a segurança digital pois podem comprometer a confidencialidade com vazamento de informações críticas, como dados administrativos ou acadêmicos, integridade, modificando ou corrompendo registros importantes e a disponibilidade interrompendo serviços essenciais, como sistemas de gestão ou comunicação interna.

Figura 2- Captura do site Virus Total



Fonte- Criação Própria

9.2. Mitigação após análise

Após a análise da URL através do VirusTotal, e embora não tenha sido fornecida informação detalhada sobre o tipo específico de malware, é fundamental adotar uma série de ações para mitigar riscos e fortalecer a segurança digital da organização.

E uma medida importante é o monitoramento contínuo da atividade de rede dessa URL. Utilizando o Wireshark, é possível capturar pacotes de rede e verificar se há tentativas de comunicação com a URL maliciosa ou domínios relacionados. Isso ajuda a identificar qualquer atividade anômala ou tentativa de comunicação com servidores de comando e controle que podem estar relacionados ao malware.

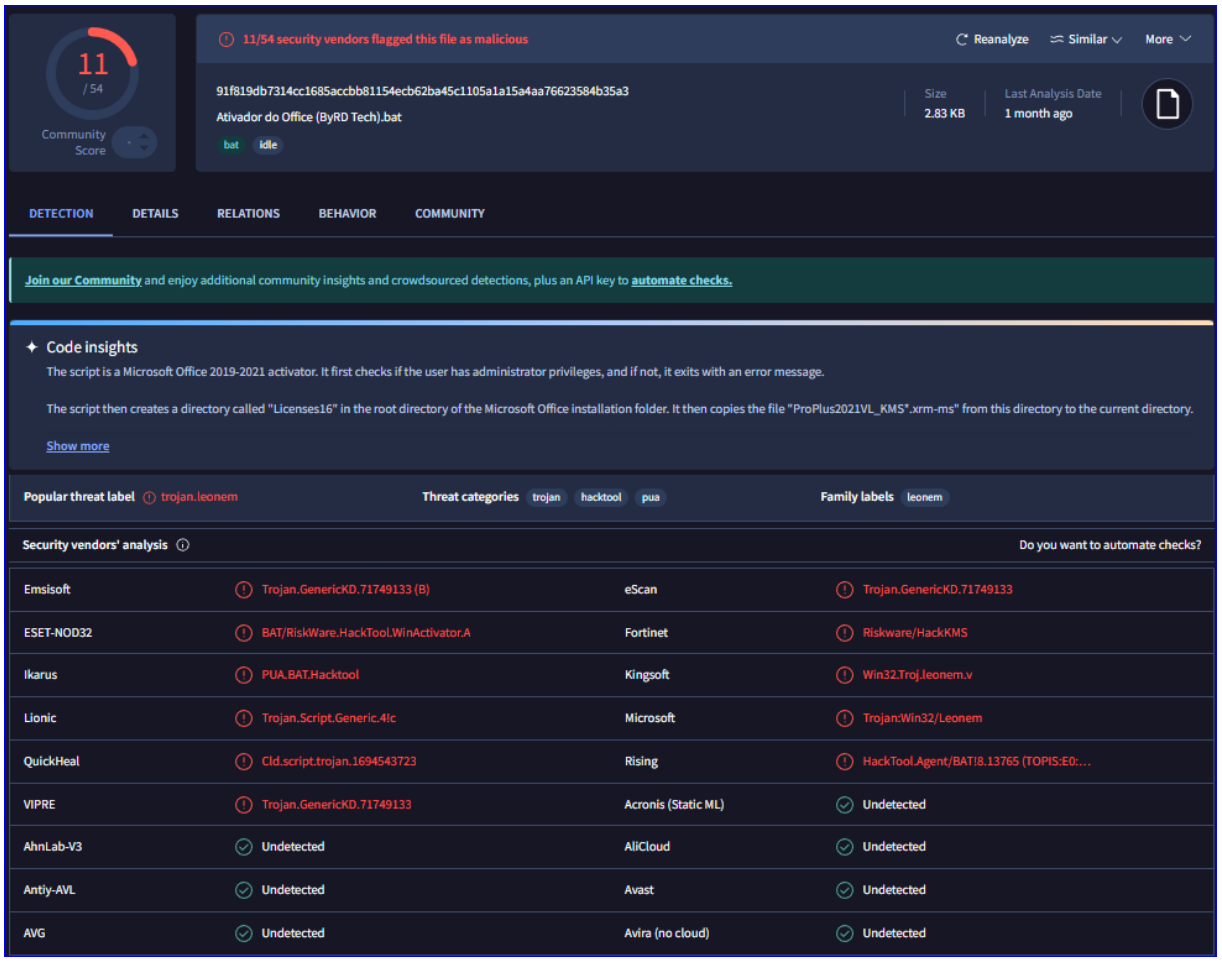
Após mitigação da URL, é importante a conscientização e treinamento dos usuários para evitar que URLs maliciosas sejam acessadas acidentalmente. Informar os usuários sobre os riscos de acessar sites suspeitos, reforçar a importância de verificar os links antes de clicar e incentivar a adesão a boas práticas de segurança cibernética são passos essenciais para reduzir a probabilidade de exposição a riscos futuros.

Na imagem a seguir, (figura 2) a análise refere-se a um arquivo que foi detectado como malware por diversos scanners de antivírus, cada um utilizando

diferentes classificações para descrever a natureza da ameaça.

O arquivo foi identificado como um trojan, especificamente classificado por ferramentas como Emsisoft, eScan, ESET-NOD32, Fortinet, Microsoft e outros, com diversas variantes do mesmo tipo de ameaça. Esses tipos de malwares, são conhecidos por sua capacidade de permitir acesso remoto não autorizado, comprometem a segurança do sistema e podem ser usados para roubo de dados, execução de comandos maliciosos ou manipulação de recursos do sistema.

Figura 3- Captura do site Virus Total



Fonte- Criação Própria

Dado o risco representado por esse arquivo malicioso, será realizada ações imediatas para evitar a propagação da ameaça e minimizar os danos. O primeiro passo é o bloqueio imediato e o isolamento do arquivo infectado. E caso já tenha sido executado, o dispositivo deve ser desconectado da rede para impedir que a ameaça se espalhe. Para garantir que o arquivo seja completamente erradicado, é importante utilizar antivírus confiáveis, que serão capazes de identificar e eliminar o malware,

além de quaisquer outras ameaças associadas.

A próxima etapa envolve uma análise dinâmica do malware, para verificar seu comportamento em um ambiente controlado, como uma máquina virtual ou sandbox. Isso permitirá identificar as ações do malware, como criação de arquivos, modificações no sistema ou tentativas de comunicação com servidores externos.

Após essa análise, o Wireshark pode ser utilizado para capturar o tráfego de rede gerado pelo Trojan. Ao monitorar pacotes HTTP e DNS, é possível observar se o malware tenta se conectar a servidores de comando e controle ou se está realizando atividades de exfiltração de dados. Para complementar a investigação, o Nmap pode ser usado para realizar uma varredura de portas e serviços no sistema ou rede infectada, a fim de identificar se o Trojan utilizou algum serviço vulnerável para estabelecer um ponto de acesso ou backdoor.

Em seguida, é importante verificar e revisar os logs de acesso para identificar atividades suspeitas ou anômalas relacionadas ao arquivo malicioso, como tentativas de uso indevido de credenciais administrativas ou acesso remoto não autorizado.

Além disso, será necessária uma atualização completa de sistema e software para corrigir quaisquer vulnerabilidades que o Trojan tenha explorado. A aplicação de patches de segurança em softwares, sistemas operacionais e servidores ajuda a prevenir novas infecções e fortalece a segurança da rede.

Será realizado o bloqueio a acesso de sites desconhecidos ou não confiáveis que possam hospedar malware, além de restringir permissões de usuários para downloads e instalações de softwares, permitindo apenas ações autorizadas pela equipe de TI

Por fim, é fundamental realizar um trabalho de treinamento e conscientização com os usuários da rede, alertando-os sobre os perigos de executar arquivos desconhecidos e reforçando a importância de utilizar apenas ferramentas e programas licenciados.

10. VULNERABILIDADE

Segundo autora Hertzberger, “uma vulnerabilidade é uma fraqueza de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças. Uma

vulnerabilidade caracteriza a ausência ou a fraqueza de uma proteção que pode ser explorada. “

> “Na cibersegurança, uma vulnerabilidade é uma fraqueza que pode ser explorada por cibercriminosos para obter acesso não autorizado a um sistema. Depois de explorar uma vulnerabilidade, um ciberataque pode executar código malicioso, instalar malware e até roubar dados confidenciais. (WatchGuard, 2022)

Os ataques que exploram vulnerabilidades podem ser classificados em diversas categorias, dependendo do objetivo e da metodologia utilizada pelos agentes maliciosos. Alguns dos principais tipos são:

10.1. Ataques de Negação de Serviço (DoS)

Esses ataques visam sobrecarregar sistemas, servidores ou redes, tornando-os indisponíveis para os usuários legítimos.

10.2. Ataques Negação de Serviço Distribuída (DDoS)

Um ataque de DDoS é uma evolução do ataque de Negação de Serviço (DoS). Ele utiliza um grande número de dispositivos (chamados de zumbis) que foram previamente comprometidos e estão sob o controle de um computador(master) ou servidor de comando e controle (C&C). O objetivo é sobrecarregar a máquina-alvo com um volume massivo de requisições simultâneas, tornando-a incapaz de atender a usuários legítimos.

10.3. Mitigar as vulnerabilidades

Na TSTI as vulnerabilidades identificadas, como a exposição de portas, aumentam o risco de ataques de Negação de Serviço (DoS) e Negação de Serviço Distribuída (DDoS).

Um ataque desse tipo pode interromper o acesso a sistemas essenciais, como o ambiente virtual de aprendizagem, portais administrativos ou até mesmo os recursos de rede da própria instituição, comprometendo suas operações e impactando negativamente sua reputação.

Para mitigar essas vulnerabilidades, o TSTI adotará medidas preventivas e reativas, sendo elas:

- Identificação e correção de portas vulneráveis por meio do uso de ferramentas como Nmap;
- Monitoramento constante do tráfego de rede para identificar anomalias, utilizando ferramentas como Wireshark;
- Implementação de sistemas de mitigação DDoS, como firewalls avançados.

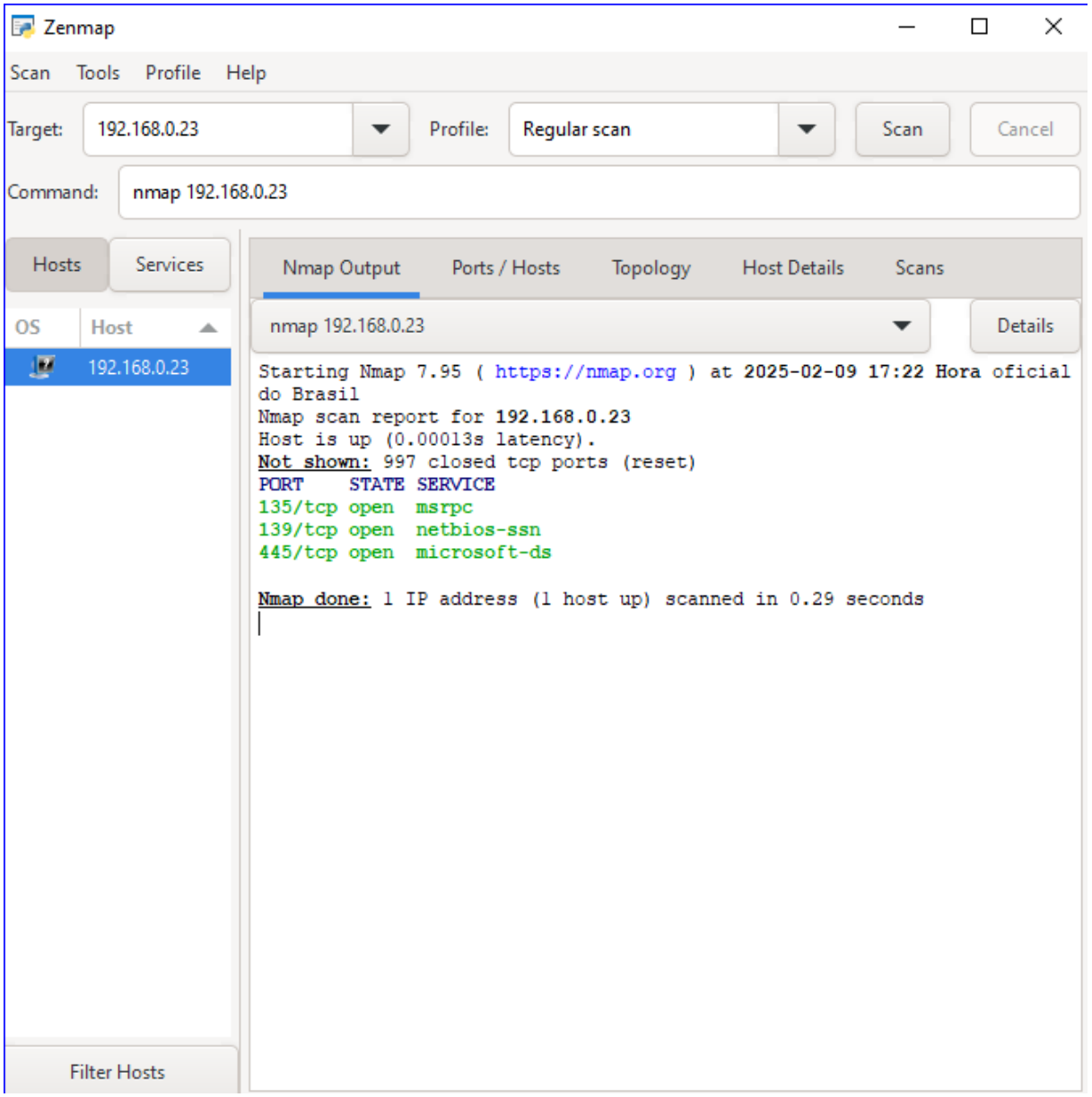
11. NMAP

> O Nmap ("Network Mapper") é uma ferramenta gratuita e de código aberto utilizada para descoberta de redes e auditoria de segurança. Muitos administradores de sistemas e redes também o utilizam para tarefas como inventário de rede, gerenciamento de cronogramas de atualização de serviços e monitoramento de disponibilidade de hosts ou serviços [...]
>
> O Nmap utiliza pacotes IP brutos de formas inovadoras para determinar quais hosts estão disponíveis na rede, quais serviços (nome e versão das aplicações) esses hosts oferecem, quais sistemas operacionais (e suas versões) estão sendo executados, que tipos de filtros de pacotes/firewalls estão em uso, entre outras dezenas de características. Ele foi projetado para escanear rapidamente redes de grande porte, mas também funciona bem para hosts individuais. (Nmap, 2025)

No entanto, o Nmap também possui limitações. Ele pode não conseguir detectar dispositivos ou serviços que estão protegidos por firewalls, o que restringe sua visibilidade em redes com segurança robusta. Além disso, o uso avançado da ferramenta exige um bom entendimento técnico sobre redes e segurança, já que algumas opções de varredura são complexas para iniciantes. Outra limitação é que o Nmap pode gerar falsos positivos, identificando erroneamente algo como vulnerável, ou falsos negativos, deixando de identificar uma vulnerabilidade real

No nmap foi realizada uma varredura de portas para identificar serviços abertos e potenciais vulnerabilidades na rede do TSTI. A seguir, apresentamos os resultados da varredura, incluindo recomendações específicas de mitigação para cada serviço ou porta identificada como vulnuravel.

Figura 4- Captura de tela do Nmap



Fonte- Criação Própria

11.1. Porta 135/tcp

Segundo o site CBTNuggets, “a porta 135 é dedicada ao Serviço deMapeamento de Chamada de Procedimento Remoto (RPC) do Windows.” O RPC é utilizado para permitir que processos executados em diferentes máquinas se comuniquem, especialmente em sistemas Windows. O serviço permite que diferentes programas em uma rede possam solicitar e executar funções de outros programas em máquinas remotas. Quando exposta à rede pública, a porta 135 pode

ser alvo de ataques, como exploração de vulnerabilidades, o que pode comprometer a segurança e a integridade dos sistemas.

11.2. Porta 139/tcp - NetBIOS Session Service

Segundo o CBTNugget, “A porta 139 é uma porta dedicada para fornecer serviços de sessão para o protocolo Server Message Block (SMB) sobre NetBIOS, sendo utilizada principalmente para compartilhamento de arquivos e impressoras em redes baseadas no Windows.” O NetBIOS facilita a comunicação entre sistemas Windows em uma rede local, permitindo que recursos como arquivos e impressoras sejam compartilhados. Quando exposta à rede pública, a porta 139 pode permitir que um atacante acesse arquivos compartilhados ou impressoras, explorando falhas de segurança. Além disso, a exposição do NetBIOS pode resultar em ataques, como o Denial of Service (DoS) ou vazamento de dados.

11.3. Porta 445/tcp - open microsoft-ds

Segundo o CBT, “A porta 445 é dedicada ao protocolo Server Message Block (SMB), que permite compartilhar recursos, como arquivos e impressoras, dentro de uma rede usando TCP.” A porta 445 é usada para comunicação SMB em redes Windows, permitindo que arquivos e impressoras sejam acessados remotamente dentro de uma rede. Quando exposta à rede pública, a porta 445 pode ser explorada por atacantes para acessar recursos compartilhados ou comprometer a segurança dos sistemas, especialmente se vulnerabilidades no protocolo SMB não forem corrigidas.

11.4. Mitigação das portas abertas

Após a verificação das portas abertas é essencial tomar ações imediatas para garantir a segurança da infraestrutura e prevenir possíveis ataques cibernéticos.

Porém, antes de tomar medidas drásticas, é importante avaliar o contexto de cada porta aberta. A empresa deve determinar se as portas são necessárias para o funcionamento de serviços essenciais ou se podem ser fechadas ou restritas.

Com base nos resultados da verificação, devem ser implementadas as

seguintes ações de segurança:

11.5. Controle de Acesso

Fechar as portas nas configurações de firewall para impedir o acesso externo, bloqueando tráfego de qualquer IP que não seja confiável. Se for necessário permitir o tráfego interno, configure o firewall para permitir o acesso apenas dentro da rede privada e de dispositivos confiáveis.

11.5.1. Desativação de Serviços Desnecessários

Se RPC, NetBIOS ou SMB não forem essenciais para as operações da empresa, desative-os nas configurações do sistema. Desabilitar o SMBv1 e, se possível, remover qualquer dependência de SMB em favor de soluções de compartilhamento de arquivos mais seguras.

11.5.2. Implementação de Patches de Segurança

Instalar patches de segurança mais recentes relacionados a RPC, NetBIOS e SMB para corrigir vulnerabilidades conhecidas. Manter um cronograma de atualizações regulares de segurança, garantindo que os sistemas e servidores estejam sempre protegidos contra ameaças.

11.5.3. Monitoramento Contínuo

Configuração de ferramentas de monitoramento para detectar tentativas de exploração das portas abertas. Implementar Sistemas de Detecção de Intrusão (IDS) e Sistemas de Prevenção de Intrusão (IPS) para identificar atividades suspeitas em tempo real. Certificar-se de que os controles de acesso, como firewalls e ACLs, estão configurados corretamente e limitam o tráfego apenas a usuários e dispositivos autorizados. Analisar os registros de atividades de rede para identificar acessos indevidos ou tentativas de exploração.

12. WIRESHARK

O Wireshark é uma ferramenta poderosa para a captura e análise de pacotes

de rede, permitindo examinar o tráfego de dados e identificar potenciais atividades maliciosas. Seu principal ponto forte é a capacidade de fornecer informações detalhadas sobre o tráfego de rede, identificando padrões anômalos ou tentativas de comunicação com servidores de comando e controle. Ele permite realizar uma análise em tempo real e oferece suporte a uma ampla gama de protocolos de rede.

> Wireshark é uma ferramenta de análise de protocolos de rede que captura e exibe pacotes de dados que trafegam por uma rede em tempo real. É uma solução gratuita e de código aberto, amplamente utilizada por analistas de segurança, administradores de redes e pesquisadores para entender o comportamento de redes e solucionar problemas de conectividade. Com o Wireshark, é possível capturar todos os pacotes que passam por uma interface de rede e visualizar detalhes, como IPs de origem e destino, portas utilizadas, protocolos aplicados e muito mais. (Wireshark, 2025)

No entanto, suas limitações são notáveis. Ele pode ser complexo para iniciantes, exigindo conhecimento técnico em redes para interpretar corretamente os pacotes capturados. O processo de análise também pode ser demorado, especialmente em redes com tráfego intenso, já que o Wireshark pode gerar uma grande quantidade de dados. Esse volume de informações pode tornar a análise mais desafiadora, especialmente sem filtros ou parâmetros bem definidos. Além disso, por ser uma ferramenta de monitoramento em tempo real, seu uso indevido ou sem a devida configuração pode impactar o desempenho da rede.

No wireshark foi realizado uma captura para exibir os pacotes que trafegam na rede da TSTI em tempo real.

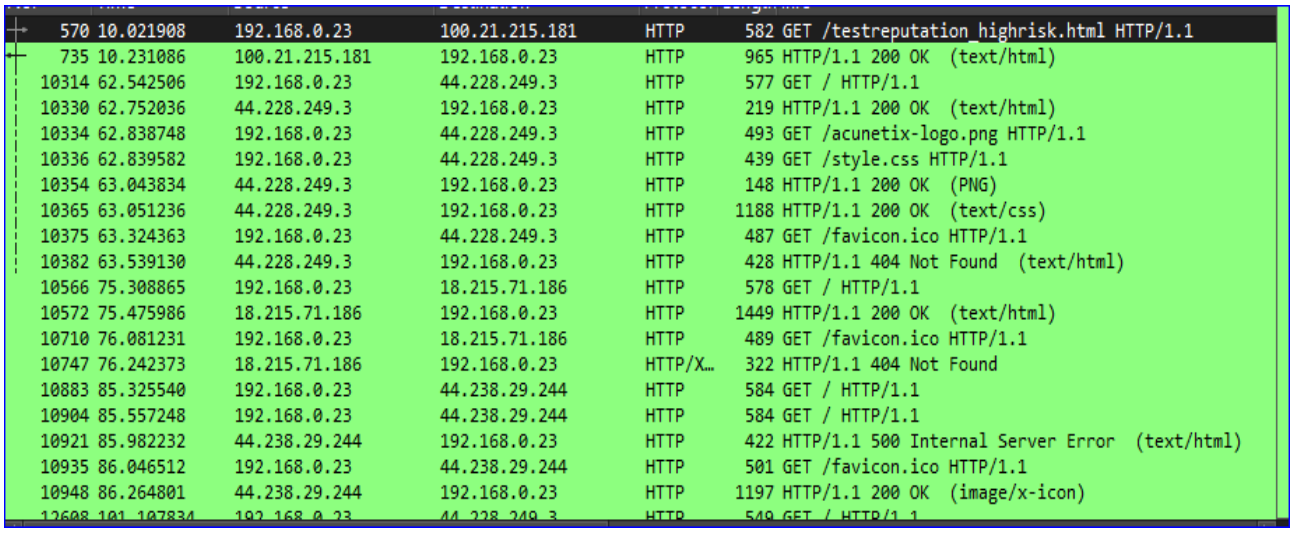
12.1. Detalhamento do resultado WireShark

O Wireshark permite filtrar pacotes para facilitar a análise. Para analisar tráfego relevante, vou utilizar os seguintes filtros:

12.1.2. HTTP

Conforme a imagem a seguir, com o filtro HTTP no Wireshark analisamos o tráfego de dados da camada de aplicação (Camada 7) da rede. Ele se refere ao protocolo HTTP (HyperText Transfer Protocol), que é amplamente usado para transferência de dados na web.

Figura 5- Captura de Tela Wireshark com filtro HTTP



570	10.021908	192.168.0.23	100.21.215.181	HTTP	582	GET /testreputation_highrisk.html HTTP/1.1
735	10.231086	100.21.215.181	192.168.0.23	HTTP	965	HTTP/1.1 200 OK (text/html)
10314	62.542506	192.168.0.23	44.228.249.3	HTTP	577	GET / HTTP/1.1
10330	62.752036	44.228.249.3	192.168.0.23	HTTP	219	HTTP/1.1 200 OK (text/html)
10334	62.838748	192.168.0.23	44.228.249.3	HTTP	493	GET /acunetix-logo.png HTTP/1.1
10336	62.839582	192.168.0.23	44.228.249.3	HTTP	439	GET /style.css HTTP/1.1
10354	63.043834	44.228.249.3	192.168.0.23	HTTP	148	HTTP/1.1 200 OK (PNG)
10365	63.051236	44.228.249.3	192.168.0.23	HTTP	1188	HTTP/1.1 200 OK (text/css)
10375	63.324363	192.168.0.23	44.228.249.3	HTTP	487	GET /favicon.ico HTTP/1.1
10382	63.539130	44.228.249.3	192.168.0.23	HTTP	428	HTTP/1.1 404 Not Found (text/html)
10566	75.308865	192.168.0.23	18.215.71.186	HTTP	578	GET / HTTP/1.1
10572	75.475986	18.215.71.186	192.168.0.23	HTTP	1449	HTTP/1.1 200 OK (text/html)
10710	76.081231	192.168.0.23	18.215.71.186	HTTP	489	GET /favicon.ico HTTP/1.1
10747	76.242373	18.215.71.186	192.168.0.23	HTTP/X…	322	HTTP/1.1 404 Not Found
10883	85.325540	192.168.0.23	44.238.29.244	HTTP	584	GET / HTTP/1.1
10904	85.557248	192.168.0.23	44.238.29.244	HTTP	584	GET / HTTP/1.1
10921	85.982232	44.238.29.244	192.168.0.23	HTTP	422	HTTP/1.1 500 Internal Server Error (text/html)
10935	86.046512	192.168.0.23	44.238.29.244	HTTP	501	GET /favicon.ico HTTP/1.1
10948	86.264801	44.238.29.244	192.168.0.23	HTTP	1197	HTTP/1.1 200 OK (image/x-icon)
12608	101.107834	192.168.0.23	44.228.249.3	HTTP	549	GET / HTTP/1.1

Fonte- Criação Própria

O tráfego consiste principalmente em requisições GET do IP 192.168.0.23(TSTI), que é um tipo comum de requisição HTTP utilizado para solicitar recursos de um servidor web. Vários pacotes indicam comunicação entre o dispositivo local e endereços IP externos, retornando respostas como 200 OK, 404 Not Found e 500 Internal Server Error, que são respostas típicas em requisições HTTP.

A requisição para o arquivo /testreputation_highrisk.html pode levantar uma suspeita, pois o nome do arquivo sugere que está relacionado a uma avaliação de risco de reputação. Arquivos com esse tipo de nome podem estar associados a testes de segurança ou tentativas de exploração de vulnerabilidades.

O tráfego envolvendo múltiplas requisições GET, como acessos a arquivos estáticos como imagens (acunetix-logo.png), ícones (favicon.ico), e folhas de estilo (style.css), pode indicar uma varredura por parte de um atacante tentando coletar informações sobre o servidor. O arquivo "acunetix-logo.png" é particularmente interessante, pois o Acunetix é uma ferramenta de análise de vulnerabilidades, e a presença desse arquivo pode indicar uma tentativa de explorar o servidor.

A presença de respostas 500 Internal Server Error pode ser uma indicação de que o servidor está sofrendo falhas internas. Embora nem sempre seja indicativo de ataque, esse erro é comum quando há tentativas de exploração.

Respostas 404 Not Found indicam que o atacante está tentando acessar recursos que não existem, uma técnica comum em scanners que tentam identificar

quais caminhos e recursos estão disponíveis no servidor.

Os dados no Wireshark, revela comportamentos normais, mas também aponta para algumas possíveis anomalias, como a requisição de arquivos de alto risco (/testreputation_highrisk.html) e interações com servidores que resultam em erros internos e falhas de página. Tais padrões podem ser indicadores de tentativas de exploração ou varredura.

- Investigar qualquer solicitação incomum de arquivos ou URLs.
- Monitorar erros do servidor (404 e 500) e implementar medidas de segurança para prevenir exploração.
- Implementar controles de tráfego, bloqueando IPs suspeitos e utilizando ferramentas de segurança como firewalls e IDS.
- Auditar serviços e sistemas expostos para garantir que não há pontos vulneráveis acessíveis externamente.

Após a confirmação de um ataque HTTP, o TSTI tomará as seguintes medidas para mitigar o impacto e fortalecer a segurança da rede e dos sistemas:

Caso algum servidor ou serviço tenha sido comprometido, ele será isolado da rede para evitar a propagação do ataque. Além disso, a equipe de TI desativará temporariamente serviços que possam estar vulneráveis ou sendo explorados durante o ataque, evitando que outras partes da infraestrutura sejam afetadas.

Todos os sistemas e servidores estarão atualizados com os patches de segurança mais recentes, especialmente em servidores web e outras infraestruturas críticas. As APIs expostas serão configuradas com autenticação forte, para garantir que apenas usuários e sistemas autorizados possam acessar informações sensíveis.

A comunicação entre os servidores e unidades remotas será protegida por VPNs seguras, garantindo que somente tráfego criptografado e autenticado possa transitar.

Regras de firewall serão ajustadas para bloquear tráfego de fontes externas e regiões geográficas suspeitas, minimizando o risco de ataques. A rede será segmentada para isolar sistemas críticos, como servidores de dados e ERP, limitando o impacto de um eventual ataque a áreas específicas.

Será realizada uma análise do impacto nas operações, priorizando a recuperação dos serviços críticos, como o ERP e sistemas internos. A partir dos backups mais recentes, os dados afetados serão restaurados, garantindo que não haja comprometimento de informações e que os sistemas estejam livres de malware.

Para aprimorar a resposta a incidentes, serão realizados treinamentos focados em identificar padrões de ataques HTTP, adotar boas práticas de segurança e promover campanhas de conscientização sobre phishing e outras ameaças relacionadas.

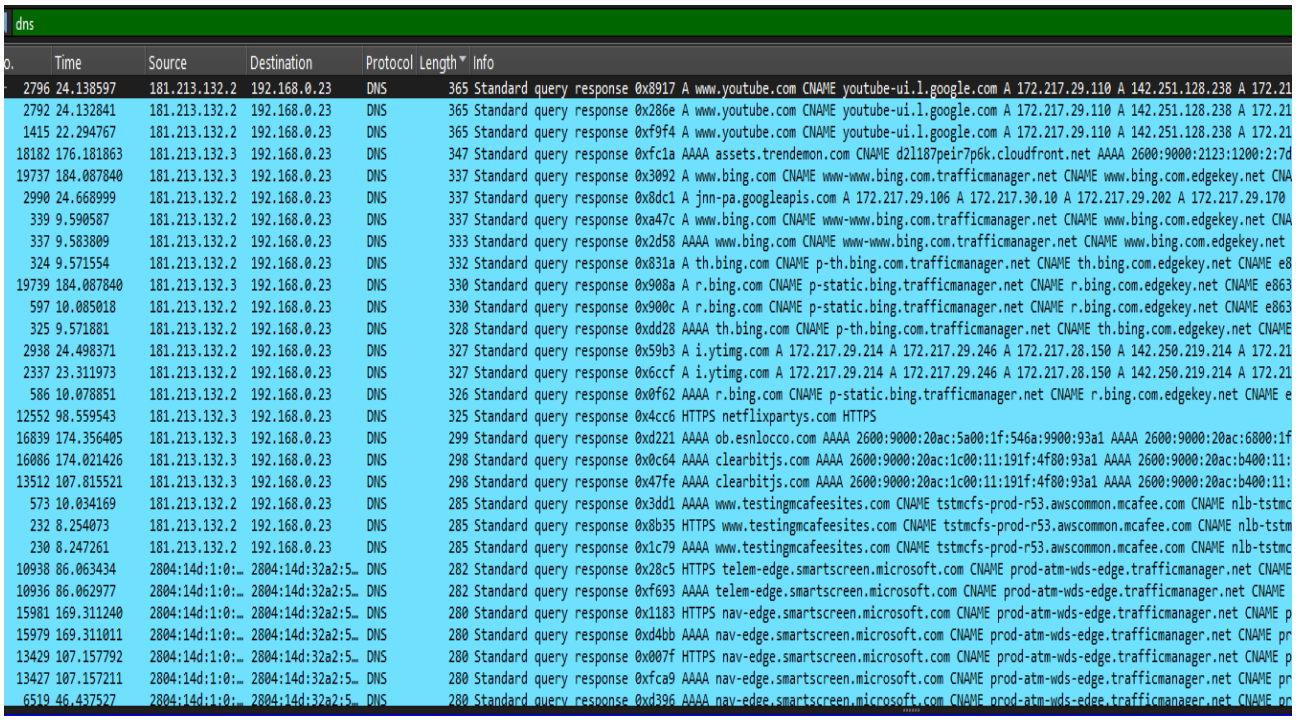
Após a mitigação do ataque, a equipe de TI implementará um monitoramento contínuo do tráfego de rede para detectar qualquer atividade suspeita remanescente e garantir que a infraestrutura do TSTI continue segura.

12.1.3. DNS

O DNS (Domain Name System) é um sistema que traduz nomes de domínio em endereços IP, funcionando de maneira semelhante a uma agenda telefônica. Em vez de procurar o número de telefone de uma pessoa pelo nome, você busca o nome de um site pela sua "identificação numérica", ou seja, o endereço IP.

Ao utilizar o filtro do Wireshark para monitorar o tráfego DNS, podemos identificar quais IPs estão fazendo as requisições e verificar se eles são esperados na rede. A imagem a seguir mostra o filtro aplicado no Wireshark, onde podemos visualizar quais IPs estão gerando o tráfego DNS.

Figura 6 - Captura de tela com filtro DNS



dns

No.	Time	Source	Destination	Protocol	Length	Info
2796	24.138597	181.213.132.2	192.168.0.23	DNS	365	Standard query response 0x8917 A www.youtube.com CNAME youtube-ui.l.google.com A 172.217.29.110 A 142.251.128.238 A 172.21
2792	24.132841	181.213.132.2	192.168.0.23	DNS	365	Standard query response 0x286e A www.youtube.com CNAME youtube-ui.l.google.com A 172.217.29.110 A 142.251.128.238 A 172.21
1415	22.294767	181.213.132.2	192.168.0.23	DNS	365	Standard query response 0xf9f4 A www.youtube.com CNAME youtube-ui.l.google.com A 172.217.29.110 A 142.251.128.238 A 172.21
18182	176.181863	181.213.132.3	192.168.0.23	DNS	347	Standard query response 0xfc1a AAAA assets.trendemon.com CNAME d2l187peir7p6k.cloudfront.net AAAA 2600:9000:2123:1200:2:7d
19737	184.087840	181.213.132.3	192.168.0.23	DNS	337	Standard query response 0x3092 A www.bing.com CNAME www-www.bing.com.trafficmanager.net CNAME www.bing.com.edgekey.net CNA
2990	24.668999	181.213.132.2	192.168.0.23	DNS	337	Standard query response 0x8dc1 A jnn-pa.googleapis.com A 172.217.29.106 A 172.217.30.10 A 172.217.29.202 A 172.217.29.170
339	9.590587	181.213.132.2	192.168.0.23	DNS	337	Standard query response 0xa47c A www.bing.com CNAME www-www.bing.com.trafficmanager.net CNAME www.bing.com.edgekey.net CNA
337	9.583809	181.213.132.2	192.168.0.23	DNS	333	Standard query response 0x2d58 AAAA www.bing.com CNAME www-www.bing.com.trafficmanager.net CNAME www.bing.com.edgekey.net
324	9.571554	181.213.132.2	192.168.0.23	DNS	332	Standard query response 0x831a A th.bing.com CNAME p-th.bing.com.trafficmanager.net CNAME th.bing.com.edgekey.net CNAME e8
19739	184.087840	181.213.132.3	192.168.0.23	DNS	330	Standard query response 0x908a A r.bing.com CNAME p-static.bing.trafficmanager.net CNAME r.bing.com.edgekey.net CNAME e863
597	10.085018	181.213.132.2	192.168.0.23	DNS	330	Standard query response 0x900c A r.bing.com CNAME p-static.bing.trafficmanager.net CNAME r.bing.com.edgekey.net CNAME e863
325	9.571881	181.213.132.2	192.168.0.23	DNS	328	Standard query response 0xdd28 AAAA th.bing.com CNAME p-th.bing.com.trafficmanager.net CNAME th.bing.com.edgekey.net CNAME
2938	24.498371	181.213.132.2	192.168.0.23	DNS	327	Standard query response 0x59b3 A i.ytimg.com A 172.217.29.214 A 172.217.29.246 A 172.217.28.150 A 142.250.219.214 A 172.21
2337	23.311973	181.213.132.2	192.168.0.23	DNS	327	Standard query response 0x6ccf A i.ytimg.com A 172.217.29.214 A 172.217.29.246 A 172.217.28.150 A 142.250.219.214 A 172.21
586	10.078851	181.213.132.2	192.168.0.23	DNS	326	Standard query response 0x0f62 AAAA r.bing.com CNAME p-static.bing.trafficmanager.net CNAME r.bing.com.edgekey.net CNAME e
12552	98.559543	181.213.132.3	192.168.0.23	DNS	325	Standard query response 0x4cc6 HTTPS netflixpartys.com HTTPS
16839	174.356405	181.213.132.3	192.168.0.23	DNS	299	Standard query response 0xd221 AAAA ob.esnlocco.com AAAA 2600:9000:20ac:5a00:1f:546a:9900:93a1 AAAA 2600:9000:20ac:6800:1f
16086	174.021426	181.213.132.3	192.168.0.23	DNS	298	Standard query response 0x0c64 AAAA clearbitjs.com AAAA 2600:9000:20ac:1c00:11:191f:4f80:93a1 AAAA 2600:9000:20ac:b400:11:
13512	107.815521	181.213.132.3	192.168.0.23	DNS	298	Standard query response 0x47fe AAAA clearbitjs.com AAAA 2600:9000:20ac:1c00:11:191f:4f80:93a1 AAAA 2600:9000:20ac:b400:11:
573	10.034169	181.213.132.2	192.168.0.23	DNS	285	Standard query response 0x3dd1 AAAA www.testingmcafeesites.com CNAME tstmcfs-prod-r53.awscommon.mcafee.com CNAME nlb-tstmc
232	8.254073	181.213.132.2	192.168.0.23	DNS	285	Standard query response 0x8b35 HTTPS www.testingmcafeesites.com CNAME tstmcfs-prod-r53.awscommon.mcafee.com CNAME nlb-tstm
230	8.247261	181.213.132.2	192.168.0.23	DNS	285	Standard query response 0x1c79 AAAA www.testingmcafeesites.com CNAME tstmcfs-prod-r53.awscommon.mcafee.com CNAME nlb-tstmc
10938	86.063434	2804:14d:1:0:…	2804:14d:32a2:5…	DNS	282	Standard query response 0x28c5 HTTPS telem-edge.smartscreen.microsoft.com CNAME prod-atm-wds-edge.trafficmanager.net CNAME
10936	86.062977	2804:14d:1:0:…	2804:14d:32a2:5…	DNS	282	Standard query response 0xf693 AAAA telem-edge.smartscreen.microsoft.com CNAME prod-atm-wds-edge.trafficmanager.net CNAME
15981	169.311240	2804:14d:1:0:…	2804:14d:32a2:5…	DNS	280	Standard query response 0x1183 HTTPS nav-edge.smartscreen.microsoft.com CNAME prod-atm-wds-edge.trafficmanager.net CNAME p
15979	169.311011	2804:14d:1:0:…	2804:14d:32a2:5…	DNS	280	Standard query response 0xd4bb AAAA nav-edge.smartscreen.microsoft.com CNAME prod-atm-wds-edge.trafficmanager.net CNAME pr
13429	107.157792	2804:14d:1:0:…	2804:14d:32a2:5…	DNS	280	Standard query response 0x007f HTTPS nav-edge.smartscreen.microsoft.com CNAME prod-atm-wds-edge.trafficmanager.net CNAME p
13427	107.157211	2804:14d:1:0:…	2804:14d:32a2:5…	DNS	280	Standard query response 0xfca9 AAAA nav-edge.smartscreen.microsoft.com CNAME prod-atm-wds-edge.trafficmanager.net CNAME pr
6519	46.437527	2804:14d:1:0:…	2804:14d:32a2:5…	DNS	280	Standard query response 0xd396 AAAA nav-edge.smartscreen.microsoft.com CNAME prod-atm-wds-edge.trafficmanager.net CNAME pr

Fonte- Criação Própria

Ao analisar os dados, verifica-se a quantidade excessiva de pacotes DNS pois pode ser um sinal de ataque, e pacotes com tamanho anormalmente grande também podem indicar algo fora do comum. Além disso, é importante verificar o volume de consultas para um determinado domínio ou IP, identificando registros DNS incomuns. Um pico anormal no número de consultas pode ser indicativo de um ataque DNS.

Monitorar o número de consultas para cada domínio, em um intervalo de tempo, ajuda a identificar anomalias na rede, principalmente se um domínio apresentar um número de consultas muito maior do que o normal. Também é importante analisar o tempo de resposta DNS, que pode variar, mas valores extremos podem indicar congestionamento, problemas no servidor DNS ou ataques.

Consultas de tipos incomuns, como "ANY" ou outros tipos desconhecidos, também podem ser uma maneira eficaz de identificar anomalias.

Após a confirmação de um ataque DNS, a equipe de TI do TSTI tomará as seguintes medidas para mitigar o impacto:

- Utilizar firewalls ou sistemas de prevenção de intrusões (IPS) para bloquear o

tráfego DNS proveniente de IPs maliciosos ou falsificados.

- Implementar a limitação da taxa de consultas DNS por IP, para evitar que um único endereço sobrecarregue o servidor.
- Configurar o servidor DNS para não responder a consultas do tipo "ANY", que são frequentemente usadas em ataques de amplificação.
- Caso o tráfego seja excessivo, pode-se redirecionar o tráfego DNS para servidores de mitigação específicos.

E caso seja confirmado que realmente é um ataque, durante o incidente, a comunicação entre a equipe de TI e a administração do TSTI será essencial. A equipe de TI deve ser notificada imediatamente para que as ações corretivas sejam tomadas rapidamente. A comunicação interna deve incluir:

- Notificação imediata sobre o ataque e os primeiros sinais detectados.
- Atualizações contínuas sobre as ações de mitigação.
- Relatório pós-incidente detalhado, explicando o ataque

12. FIREWALL

> Os firewalls podem ser vistos como barreiras ou gateways que gerenciam o percurso de atividades da Web permitidas e proibidas em uma rede privada. O termo vem do conceito de paredes físicas como barreiras para retardar a propagação do fogo até que os serviços de emergência possam extingui-lo. Em comparação, os firewalls de segurança de rede são usados para gerenciamento de tráfego da Web. Normalmente, são destinados a retardar a propagação de ameaças da Web. (Karspersky,2025)

Os firewalls têm evoluído ao longo do tempo, incorporando novas tecnologias e metodologias para suprir as lacunas das gerações anteriores. A abordagem de filtragem de um firewall pode variar dependendo de sua implementação, e existem diferentes tipos de firewalls, cada um com suas características e vantagens. Abaixo, explico as principais diferenças entre os tipos de firewalls com base em três abordagens principais: rastreamento de conexão, regras de filtragem e registros de auditoria.

12.1. Firewall de filtragem estática de pacotes

> Os firewalls de filtragem estática de pacotes, também conhecidos como firewalls de inspeção sem estado, operam na camada de rede OSI (camada 3). Oferecem filtragem básica verificando todos os pacotes de dados individuais enviados por uma rede, com base na origem deles e para onde estão tentando ir. Particularmente, as conexões aceitas anteriormente não são rastreadas. Isso significa que cada conexão deve ser aprovada novamente com cada pacote de dados enviado. (Kaspersky,2025)

De acordo com Kaspersky os firewalls de filtragem estática de pacotes realizam uma verificação simples e independente de cada pacote de dados, sem manter o estado das conexões anteriores. Eles tomam decisões de filtragem baseadas em critérios como o endereço IP de origem e destino, portas e protocolos, mas não sabem se o pacote faz parte de uma comunicação contínua ou se foi enviado previamente. Isso torna esses firewalls relativamente simples e rápidos, mas com uma capacidade limitada de detectar ameaças complexas ou comportamentos maliciosos mais sofisticados.

12.2. Firewall de Gateway em Nível de Circuito

> Os gateways de nível de circuito operam no nível de sessão (camada 5). Esses firewalls verificam pacotes funcionais em uma tentativa de conexão e, se funcionarem bem, permitirão uma conexão aberta persistente entre as duas redes. O firewall para de supervisionar a conexão depois que isso ocorre.(Kaspersky,2025)

O firewall de gateway em nível de circuito verifica a tentativa de conexão entre dois sistemas ou redes, validando que a comunicação está funcionando corretamente. Uma vez estabelecida a conexão, ele permite que os dados fluam livremente entre os dois sistemas sem a necessidade de mais verificações. Esse tipo de firewall oferece um controle mais flexível, mas também pode ser menos seguro, pois ele não monitora continuamente a comunicação depois de permitir a conexão, o que pode ser explorado por um atacante após a inicialização da sessão.

12.3. Firewall de inspeção com estado

> Os firewalls de inspeção com estado, também chamados de firewalls de filtragem dinâmica de pacotes, se diferenciam da filtragem estática por sua

> capacidade de monitorar conexões em andamento e se lembrar das anteriores. Anteriormente, operavam na camada de transporte (camada 4), mas, hoje em dia, esses firewalls podem monitorar muitas camadas, inclusive a de aplicativo (camada 7).(Kaspersky,2025)

Os firewalls de inspeção com estado são mais avançados e inteligentes do que os firewalls de filtragem estática, pois podem monitorar e lembrar o estado das conexões ao longo do tempo, proporcionando maior controle e segurança. Além disso, esses firewalls não se limitam mais à camada de transporte, mas podem monitorar e filtrar tráfego em várias camadas, até mesmo na camada de aplicação, permitindo uma inspeção mais profunda do tráfego de rede. Isso torna os firewalls de inspeção com estado uma das opções mais robustas e eficazes para proteger redes contra ameaças.

No entanto, esses firewalls apresentam algumas desvantagens. O consumo elevado de recursos, como poder de processamento e memória, pode impactar a escalabilidade em redes grandes. Além disso, são vulneráveis a ataques de flooding, que podem sobrecarregar o sistema. A latência também pode ser aumentada, uma vez que o firewall precisa processar pacotes e atualizar as tabelas de estado, o que pode gerar atrasos no tráfego. Além disso, eles têm limitações na detecção de ameaças internas e podem não ser tão eficazes contra ataques originados da rede interna.

12.4. Firewall de proxy

> Os firewalls de proxy, também conhecidos como firewalls de nível de aplicativo (camada 7), são únicos no que se refere à leitura e à filtragem de protocolos de aplicativos. Eles combinam inspeção em nível de aplicativo, ou "inspeção profunda de pacotes (DPI)" e inspeção com estado. ... A filtragem se baseia em dados de nível de aplicativo, em vez de apenas endereços IP, portas e protocolos básicos de pacotes (UDP, ICMP), como ocorre em firewalls baseados em pacotes. A leitura e a compreensão de FTP, HTTP, DNS e outros protocolos permitem a investigação mais aprofundada e a filtragem cruzada de muitas características de dados diferentes.(Kaspersky,2025)

Essa abordagem permite que os firewalls de proxy analisem e compreendam de forma mais detalhada o tráfego da rede, o que proporciona uma filtragem mais precisa e eficaz. Em vez de simplesmente permitir ou bloquear pacotes com base em parâmetros simples como endereços IP, portas ou protocolos, os firewalls de proxy

podem investigar de forma mais detalhada o comportamento das comunicações e bloquear tráfego malicioso antes que ele alcance a rede interna.

No entanto, apesar de suas vantagens, esses firewalls também apresentam algumas desvantagens. A inspeção profunda de pacotes pode aumentar a latência do tráfego, já que cada pacote precisa ser analisado com mais detalhes. Isso pode resultar em uma redução no desempenho da rede, especialmente em ambientes com alto volume de tráfego. Além disso, o processamento detalhado do tráfego exige mais recursos computacionais, o que pode aumentar o custo de implementação e manutenção do firewall. A complexidade para configurar e gerenciar esse tipo de firewall também é maior, pois é necessário ajustar e monitorar regras detalhadas para garantir que não haja interferências indesejadas nas aplicações legítimas, o que pode gerar falsos positivos ou até bloquear serviços necessários.

12.5. Firewall de última geração (NGFW)

> As ameaças em evolução continuam a exigir soluções mais intensas, e os firewalls de última geração estão preparados para essa questão, combinando os recursos de um firewall tradicional com sistemas de prevenção de invasões de rede.
>
> Os firewalls de última geração específicos para determinadas ameaças foram projetados para examinar e identificar ameaças específicas, como malware avançado, em um nível mais granular. Mais usados por empresas e redes sofisticadas, eles fornecem uma solução holística para filtrar ameaças. .(Kaspersky,2025)

Os firewalls de última geração (NGFW) são projetados para lidar com as ameaças em evolução que estão se tornando cada vez mais complexas. Diferente dos firewalls tradicionais, que oferecem filtragem básica de pacotes com base em regras predefinidas, os NGFW combinam as funcionalidades de um firewall convencional com sistemas mais avançados de prevenção de invasões de rede (IPS). Isso significa que eles são capazes de monitorar o tráfego de rede de forma contínua e ativa, não apenas filtrando pacotes, mas também detectando e respondendo a ataques em tempo real.

Esses firewalls vão além da simples análise de tráfego, sendo capazes de identificar ameaças específicas, como malware avançado e ataques direcionados, em um nível mais detalhado. Eles também podem aplicar técnicas como inspeção

profunda de pacotes (DPI) e análise comportamental, o que os torna mais eficazes na identificação de ameaças desconhecidas, como zero-day attacks (ataques que exploram vulnerabilidades ainda não conhecidas).

Além disso, os firewalls NGFW são altamente escaláveis e integrados, permitindo a filtragem holística de ameaças, o que significa que eles não só bloqueiam o tráfego malicioso, mas também integram funções de autenticação, controle de aplicativos, VPN e inspeção de tráfego criptografado.

Apesar de sua sofisticação, o uso de NGFWs também apresenta desafios. O alto custo de implementação e manutenção pode ser uma limitação para organizações menores ou com orçamento restrito. Esses firewalls exigem recursos computacionais elevados, o que pode impactar o desempenho da rede, especialmente se não forem adequadamente dimensionados. Além disso, como essas soluções são mais complexas, demandam maior capacidade de gerenciamento e monitoramento constante, o que pode exigir uma equipe de TI mais qualificada para operar de maneira eficiente.

12.6. Firewall híbrido

De acordo com Kaspersky os firewalls híbridos usam dois ou mais tipos de firewall em uma única rede privada. Ele pode combinar firewalls de filtragem de pacotes com inspeção profunda de pacotes (DPI) ou firewalls de proxy, a fim de tirar proveito das vantagens de cada tipo de firewall, proporcionando um nível mais flexível de proteção. Esse tipo de firewall é utilizado em redes onde diferentes camadas de segurança são necessárias para diferentes serviços ou ambientes, sendo uma opção interessante para organizações que têm necessidades de segurança diversificadas.

Dada a complexidade dos riscos de segurança que o TSTI enfrenta, um firewall híbrido irá fornecer a proteção abrangente e flexível necessária para garantir a segurança da infraestrutura digital da instituição. Além disso, ele pode se integrar bem com outras ferramentas de segurança, como sistemas de prevenção de intrusões (IPS) e analisadores de tráfego de rede como o Wireshark.

CONCLUSÃO

A análise e o desenvolvimento do plano de segurança digital para o Taboão da Serra Tech Institute (TSTI) foram fundamentais para identificar e mitigar os riscos de segurança que a instituição enfrenta, em virtude de incidentes recentes e vulnerabilidades no tráfego de rede. A utilização de ferramentas como VirusTotal, Wireshark e Nmap, associada à implementação de controles de segurança adequados, contribui de maneira significativa para a proteção dos ativos críticos e da infraestrutura tecnológica da instituição.

A implementação dessas recomendações, com foco em controles preventivos e de monitoramento, permitirá não apenas a redução de riscos, mas também a criação de uma cultura de segurança cibernética que sustente o crescimento da instituição, minimizando os impactos de possíveis ataques e garantindo a confiança nas operações.

REFERÊNCIAS

CBT Nuggets. What is Port 135? CBT Nuggets, 2025. Disponível em: https://www.cbtnuggets.com/common-ports/what-is-port-135. Acesso em: 28 jan. 2025.

CBT Nuggets. What is Port 139? CBT Nuggets, 2025. Disponível em: https://www.cbtnuggets.com/common-ports/what-is-port-139. Acesso em: 28 jan. 2025.

CBT Nuggets. What is Port 445? CBT Nuggets, 2025. Disponível em: https://www.cbtnuggets.com/common-ports/what-is-port-445. Acesso em: 28 jan. 2025.

GALVÃO, Michele da Costa (org.). Fundamentos em segurança da informação. São Paulo: Pearson, 2015.

IBM. Cibersegurança. *IBM*. Disponível em: https://www.ibm.com/br-pt/topics/cybersecurity#:~:text=Segundo%20estimativas%2C%20o%20crime%20cibern%C3%A9tico,trilh%C3%B5es%20por%20ano%20at%C3%A9%202025.&text=O%20custo%20dos%20ataques%20cibern%C3%A9ticos,cibercriminosos%20se%20tornam%20mais%20avan%C3%A7ados. Acesso em: 20 jan. 2025.

MICROSOFT. Detectar, habilitar e desabilitar SMBv1, v2 e v3 no Windows Server. Microsoft Learn. Disponível em: https://learn.microsoft.com/pt-br/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3?tabs=server. Acesso em: 29 jan. 2025.

MCAfee. Malware: O que é e como se proteger? McAfee, 2025. Disponível em: https://www.mcafee.com/pt-br/antivirus/malware.html#:~:text=Malware%20%C3%A9%20um%20termo%20gen%C3%A9rico,v%C3%ADtimas%20para%20obter%20ganhos%20financeiros. Acesso em: 9 jan. 2025.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Cybersecurity Framework Version 1.1 [Special Publication 800-161]. 2024. Disponível em: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.ipd.pdf. Acesso em: 19 dez. 2024.

NMAP. Nmap - Network exploration tool and security scanner. *Nmap*. Disponível em: https://nmap.org/. Acesso em: 18 jan. 2025.

SÊMOLA, M. Gestão da segurança da informação: visão executiva da

segurança da informação. Rio de Janeiro: Elsevier, 2003.

SILVA, Michel Bernardo Fernandes da. Cibersegurança: uma visão panorâmica sobre a segurança da informação na internet. Rio de Janeiro: Freitas Bastos, 2023.

STALLINGS, William. Criptografia e segurança de redes: princípios e práticas. 6. ed. São Paulo: Pearson, 2014.

TALAGALA, Nishata. Data as the new oil is not enough: Four principles for avoiding data fires. Forbes, 2 mar. 2022. Disponível em: https://www.forbes.com/sites/nishatalagala/2022/03/02/data-as-the-new-oil-is-not-enough-four-principles-for-avoiding-data-fires/#:~:text=Generally%20credited%20to%20mathematician%20Clive,it%20cannot%20really%20be%20used. Acesso em: 10 dez. 2024.

WATCHGUARD. O que é uma vulnerabilidade na cibersegurança. WatchGuard. Disponível em: https://www.watchguard.com/br/wgrd-news/blog/o-que-e-uma-vulnerabilidade-na-ciberseguranca#:~:text=Na%20ciberseguran%C3%A7a%2C%20uma%20vulnerabilidade%20%C3%A9,n%C3%A3o%20autorizado%20a%20um%20sistema. Acesso em: 17 jan 2025.

WIRESHARK. About Wireshark. *Wireshark*. Disponível em: https://www.wireshark.org/about.html. Acesso em: 17 jan. 2025.

VIRUSTOTAL. About VirusTotal. Disponível em: https://www.virustotal.com. Acesso em: 27 jan. 2025.

ANEXOS

Anexo A – Video_Portfolio_DannyellyQueiroz_GTIEAD

O vídeo a seguir apresenta um resumo do projeto detalhando os principais conceitos e justificativas técnicas empregados no desafio.

Link do vídeo: [Clique aqui]

Anexo B – Apresentacao_Portfolio_DannyellyQueiroz_GTIEAD

A apresentação em PowerPoint complementa o vídeo e detalha visualmente os aspectos do projeto.

Link da apresentação: [Clique aqui]