RELATÓRIO TÉCNICO

Nome do Autor: Beatriz Santos
Instituição : VNW
Curso: Cybersec
Versão: 1.0
Data: Julho de 2025

Sumário Executivo

Este documento apresenta um resumo conciso da análise de segurança realizada em uma rede simulada, segmentada para replicar um ambiente corporativo real. A rede foi dividida em três segmentos principais: corp_net (rede corporativa), guest_net (rede de convidados) e infra_net (infraestrutura e serviços de rede). Para identificar dispositivos, serviços expostos e potenciais riscos, foram utilizadas ferramentas como Nmap, Curl e Ping.

Objetivo

Analisar uma rede simulada com foco na identificação de exposições, segmentações e riscos operacionais existentes. Para isso, serão utilizadas ferramentas de coleta ativa de dados. Através dessas ferramentas, será mapeado o dispositivo conectados, onde será identificado as portas e serviços ativos, além de possíveis vulnerabilidades, contribuindo para uma avaliação mais precisa da segurança da rede.

Escopo

Este trabalho tem como foco realizar uma simulação de rede, visando identificar possíveis exposições, falhas de segmentação e riscos operacionais que comprometam a segurança do ambiente. A metodologia aplicada baseia-se na

coleta ativa de dados, utilizando ferramentas específicas de varredura e mapeamento, tais como:

- **Nmap** – para detecção de hosts, portas abertas e serviços em execução;
- **Rustscan** – para varredura rápida e identificação de serviços ativos;
- **Ping** – para teste de conectividade e resposta dos nós.

A coleta ativa permite interagir diretamente com os dispositivos da rede, simulando ações reais, com o intuito de levantar informações relevantes para a análise de segurança. Com os dados obtidos, será possível compreender a estrutura da rede simulada, avaliar a eficácia da segmentação implementada e identificar pontos de exposição que possam representar vulnerabilidades exploráveis.

Metodologia

Identificação das Interfaces de Rede (ip a)

A primeira etapa da análise consistiu na identificação das interfaces de rede disponíveis no sistema. Para isso, foi utilizado o comando:

ip a

Esse comando lista todas as interfaces de rede da máquina (como eth0, wlan0, lo, etc.), exibindo informações como:

- Endereço IP atribuído (inet)
- Endereço MAC (link/ether)
- Estado da interface (UP/DOWN)
- Máscara de sub-rede

Exemplo de saída parcial:

: **eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500**

inet 10.10.10.5/24 brd 10.10.10.255 scope global eth0

link/ether 00:1a:2b:3c:4d:5e brd ff:ff:ff:ff:ff:ff

A partir dessas informações, foi possível:

- Determinar o(s) IP(s) da máquina analisadora.
- Entender em qual faixa de rede local a máquina estava inserida.
- Preparar o escopo da varredura com ferramentas como **nmap** e **netdiscover**.

Para filtrar apenas os endereços IPv4 de forma direta, também foi utilizado:

ip a | grep inet

Esse comando auxilia na rápida visualização dos IPs atribuídos às interfaces, excluindo outras informações menos relevantes na etapa inicial.

Teste de Conectividade com as Redes (ping)

Após identificar as interfaces e os endereços IP locais, foi realizado um teste de conectividade com os gateways de cada segmento de rede. O comando utilizado foi:

ping -c 3 10.10.10.1 # corp_net
ping -c 3 10.10.30.1 # guest_net
ping -c 3 10.10.50.1 # infra_net

Objetivo:

- Verificar se o host de análise consegue alcançar os gateways das três redes segmentadas.
- Confirmar que há conectividade básica (camada 3 – IP) com cada rede-alvo.
- Validar o escopo antes de realizar varreduras mais profundas.

Parâmetros utilizados:

- **-c 3**: define o envio de apenas três pacotes ICMP por teste, para evitar tráfego excessivo.

Saída esperada (exemplo):

sql

PING 10.10.10.1 (10.10.10.1) 56(84) bytes of data.
64 bytes from 10.10.10.1: icmp_seq=1 ttl=64 time=0.510 ms
64 bytes from 10.10.10.1: icmp_seq=2 ttl=64 time=0.300 ms
64 bytes from 10.10.10.1: icmp_seq=3 ttl=64 time=0.250 ms

--- 10.10.10.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms

Se todos os pacotes forem recebidos sem perda, confirma-se que a rede está acessível e pronta para análise.

Descoberta de Hosts com Nmap

Para identificar os dispositivos ativos na rede, foi utilizado o **Nmap** com o tipo de varredura **ping scan** (**-sn**), que envia pacotes ICMP, TCP SYN e ARP (quando aplicável) para verificar quais hosts estão "ativos" ou "respondendo".

Os comandos utilizados foram:

nmap -sn -T4 10.10.10.0/24 -oG - | grep "Up"

Realiza a varredura na faixa de IPs **10.10.10.0/24**, utilizando a opção **-T4** (velocidade agressiva porém segura), e filtra os dispositivos que estão ativos (com status "Up").

nmap -sn -T4 10.10.10.0/24 -oG - | awk '/Up$/{print $2}' | tee corp_net_ips.txt

Lista apenas os endereços IP dos hosts ativos, salvando-os no arquivo

corp_net_ips.txt.

nmap -sn -T4 10.10.10.0/24 -oG - | awk '/Up$/{print $2, $3}' | tee corp_net_ips_hosts.txt

Lista os endereços IP e possíveis nomes de host dos dispositivos ativos, salvando os dados em **corp_net_ips_hosts.txt**.

Esses comandos foram fundamentais para iniciar a coleta ativa de dados da rede e formar uma base de endereços a serem analisados nas etapas seguintes da investigação.

Varredura de Portas com Rustscan

Após identificar os hosts ativos em cada rede, foi utilizado o **Rustscan** para realizar uma varredura rápida nas máquinas detectadas. O objetivo foi identificar portas abertas de forma ágil, otimizando o tempo de análise.

O **Rustscan** é conhecido por sua velocidade superior ao Nmap na detecção de portas, sendo ideal para grandes volumes de IPs. A seguir, os comandos utilizados por rede:

Rede Corporativa

rustscan -a 'corp_net_ips.txt' | grep Open > corp_net_ips_ports.txt

Varre todos os IPs listados no arquivo **corp_net_ips.txt**, filtra somente as portas abertas e salva em **corp_net_ips_ports.txt**.

Rede de Infraestrutura:

rustscan -a 'infra_net_ips.txt' | grep Open > infra_net_ips_ports.txt

Realiza o mesmo processo para os hosts da rede de infraestrutura, salvando os resultados em **infra_net_ips_ports.txt**.

Rede de Convidados:

rustscan -a 'guest_net_ips.txt' | grep Open > guest_net_ips_ports.txt

Aplica a varredura nos IPs da rede de convidados, com os resultados registrados em **guest_net_ips_ports.txt**.

Essa etapa foi essencial para identificar serviços possivelmente expostos em cada rede, permitindo uma análise mais aprofundada dos riscos operacionais associados a essas portas abertas.

Análise de Serviços Específicos – FTP

Após a identificação de portas abertas com Rustscan, foi iniciada a análise manual dos serviços expostos em cada host. Um dos serviços identificados na rede de

infraestrutura foi o **FTP (porta 21)**, o que motivou a investigação sobre permissões de acesso anônimo, uma vulnerabilidade comum e crítica em redes corporativas.

Comando utilizado:

nmap -p 21 --script ftp-anon 10.10.30.10

Realiza uma análise específica na porta 21 do host 10.10.30.10, utilizando o script **ftp-anon** do Nmap para verificar se o servidor FTP permite login anônimo.

Registro da análise:

nmap -p 21 --script ftp-anon 10.10.30.10 > infra_net_servico_ftp-anon.txt

Os resultados foram salvos no arquivo **infra_net_servico_ftp-anon.txt** para posterior consulta e documentação.

Essa etapa permitiu verificar se o servidor FTP está configurado corretamente ou se apresenta riscos relacionados a permissões indevidas de acesso, o que pode expor arquivos sensíveis da rede de infraestrutura.

Análise de Serviços Específicos – MySQL

Foi identificado que o host **10.10.30.11** na rede de infraestrutura estava com a porta **3306** (MySQL) aberta. Para coletar informações detalhadas sobre o serviço, foi utilizado o script **mysql-info** do Nmap, que permite extrair dados como versão, protocolo e configurações básicas do servidor MySQL.

Comando utilizado:

nmap -p 3306 --script mysql-info 10.10.30.11

Executa a varredura na porta 3306 do host 10.10.30.11, aplicando o script **mysql-info** para descobrir informações sobre o serviço MySQL em execução.

Registro da análise:

nmap -p 3306 --script mysql-info 10.10.30.11 > infra_net_servico_mysql-info.txt

Os dados obtidos foram armazenados no arquivo **infra_net_servico_mysql-info.txt** para consulta e documentação.

Essa análise é importante para identificar versões desatualizadas, configurações frágeis e possíveis exposições que possam ser exploradas em ataques direcionados ao banco de dados.

Análise de Serviços Específicos – LDAP

O host **10.10.30.17**, localizado na rede de infraestrutura, apresentou a porta **389** aberta, correspondente ao protocolo **LDAP (Lightweight Directory Access Protocol)**, comumente utilizado para autenticação e diretórios corporativos. Para obter informações iniciais sobre a estrutura do serviço, foi utilizado o script **ldap-rootdse** do Nmap.

Comando utilizado:

nmap -p 389 --script ldap-rootdse 10.10.30.17

Executa a análise na porta 389 do host **10.10.30.17**, utilizando o script **ldap-rootdse**, que retorna informações do *Root DSE* (Directory Server Entry), como nome do servidor, base DN e outros atributos públicos.

Registro da análise:

nmap -p 389 --script ldap-rootdse 10.10.30.17 > infra_net_servico_ldap-rootdse.txt

Os dados obtidos foram salvos em **infra_net_servico_ldap-rootdse.txt** para futura consulta e documentação.

Essa verificação é fundamental para entender a estrutura de diretório exposta e avaliar se há risco de vazamento de metadados ou configurações sensíveis através de consultas públicas.

Análise de Serviços Específicos – SMB

No host **10.10.30.15**, foi detectada a porta **445** aberta, utilizada pelo protocolo **SMB (Server Message Block)**, responsável por compartilhamento de arquivos, impressoras e outros recursos em redes Windows. A investigação teve como foco identificar o sistema operacional remoto e descobrir compartilhamentos acessíveis.

Comando utilizado:

nmap -p 445 --script smb-os-discovery,smb-enum-shares 10.10.30.15

Executa scripts do Nmap para:

- **smb-os-discovery**: identificar o sistema operacional e informações da máquina remota.
- **smb-enum-shares**: enumerar compartilhamentos SMB disponíveis e seus níveis de acesso.

Registro da análise:

nmap -p 445 --script smb-os-discovery,smb-enum-shares 10.10.30.15 > infra_net_servico_smb.txt

Os resultados foram armazenados no arquivo infra_net_servico_smb.txt.

Essa análise é essencial para verificar possíveis exposições de compartilhamentos indevidos, permissões de leitura/escritas não autorizadas e identificar sistemas vulneráveis a exploits SMB conhecidos (como EternalBlue).

Análise de Serviços Específicos – HTTP (Web)

O host **10.10.30.117** apresentou a porta **80** (HTTP) aberta, indicando a presença de um servidor web ativo. Para coletar informações sobre o serviço, como cabeçalhos HTTP, banners e conteúdo da página, foi utilizada a ferramenta **curl**, amplamente empregada para comunicação via protocolo HTTP.

Comandos utilizados:

curl -I http://10.10.30.117

Exibe apenas os **cabeçalhos HTTP** da resposta, permitindo identificar o tipo de servidor, data, status da requisição e outros metadados importantes.

curl -I http://10.10.30.117 > infra_net_servico_webserver.txt

Salva os cabeçalhos obtidos no arquivo

infra_net_servico_webserver.txt para documentação.

curl http://10.10.30.117

Realiza uma requisição completa ao servidor web e retorna o **conteúdo HTML da página inicial**.

curl http://10.10.30.117 > infra_net_servico_zabbix.txt

Armazena o conteúdo da página no arquivo **infra_net_servico_zabbix.txt**. A análise do código-fonte da resposta revelou a presença de uma interface do sistema de monitoramento Zabbix, o que pode indicar exposição indevida do painel de gerenciamento.

Essa verificação foi essencial para identificar possíveis aplicações web expostas, analisar vulnerabilidades visíveis (como interfaces administrativas acessíveis publicamente) e entender melhor o papel do host na infraestrutura da rede.

corp_net (Corporate Network – Rede Corporativa)

É a rede principal usada por funcionários e sistemas internos da empresa.
Ela costuma conter:

- Computadores dos funcionários
- Servidores internos (arquivos, banco de dados, aplicações empresariais)
- Impressoras e dispositivos utilizados no ambiente de trabalho
- **10.10.10.1** – Gateway/roteador
- **10.10.10.10, 10.10.10.101, 10.10.10.127, 10.10.10.222 – Hosts ativos**
- **Alta prioridade de segurança**, pois armazena dados sensíveis e recursos críticos para o funcionamento da organização.

guest_net (Guest Network – Rede de Convidados)

Rede separada criada para visitantes ou dispositivos não confiáveis.
Costuma ser usada por:

- Visitantes em reuniões

- Dispositivos pessoais dos funcionários (BYOD – Bring Your Own Device)
- **10.10.30.1** – Gateway/roteador

- **10.10.30.10, 10.10.30.11, 10.10.30.15, 10.10.30.17, 10.10.30.117, 10.10.30.227, 10.10.30.2** – Hosts ativos

Isolada da rede principal (corp_net) para evitar acesso acidental ou malicioso aos dados internos da empresa.

infra_net (Infrastructure Network – Rede de Infraestrutura)

Essa rede conecta equipamentos e serviços que sustentam o funcionamento da rede como um todo. Pode incluir:

- Servidores DNS, DHCP, Zabbix (monitoramento)

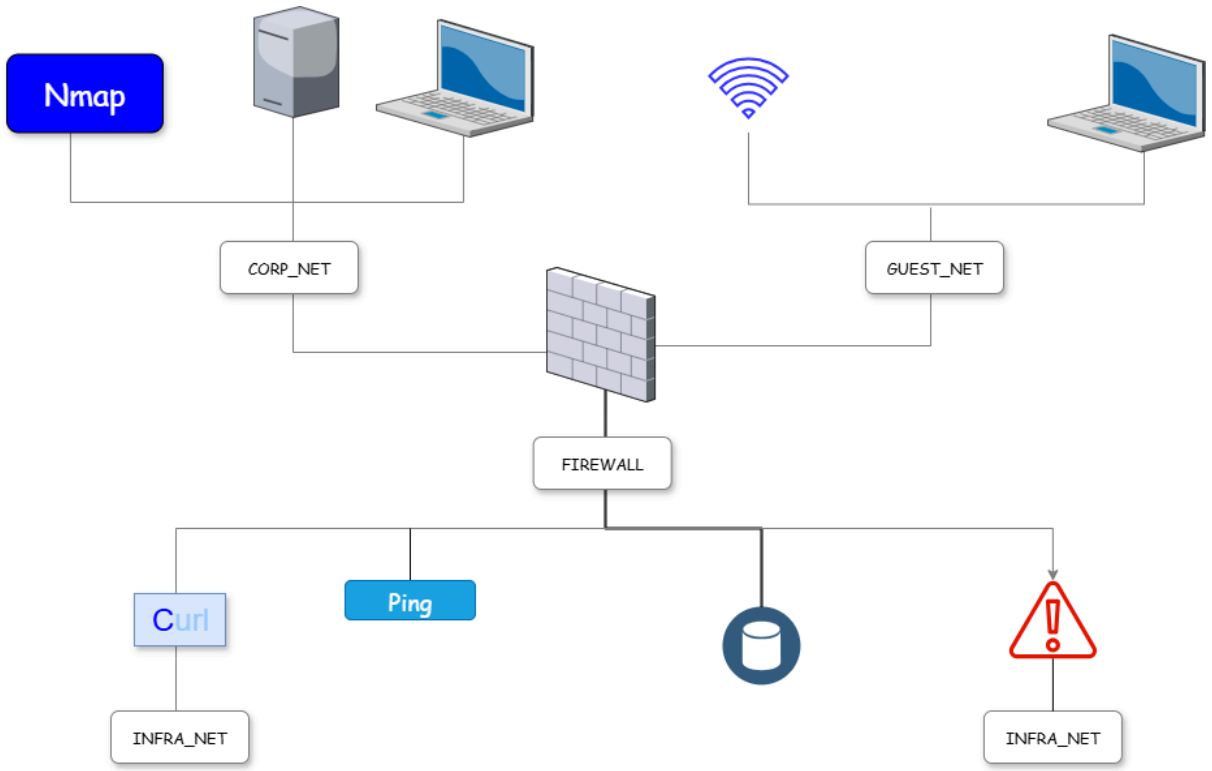
- Switches gerenciáveis e roteadores

- Dispositivos de gerenciamento e automação de rede.
- **10.10.50.1** – Gateway ou servidor de infraestrutura

Foco em estabilidade e controle, já que é a base para todas as outras redes funcionarem corretamente.

Diagrama de Rede

Este documento apresenta o diagrama de rede com três segmentos principais identificados: corp_net (rede corporativa), guest_net (rede de convidados) e infra_net (infraestrutura e serviços de rede). A identificação de dispositivos, serviços expostos e potenciais riscos foi realizada por meio das ferramentas Nmap, Curl e Ping.



Diagnóstico (Achados)

A análise revelou diversas configurações que representam riscos à segurança da rede. Os achados mais críticos incluem:

Portas e Serviços Expostos:

- **FTP com Acesso Anônimo (Host: 10.10.30.10):** O serviço FTP está configurado para permitir acesso anônimo, o que facilita a entrada de arquivos maliciosos e o acesso não autorizado a dados.
- **Serviço MySQL Ativo com Banner Visível (Host: 10.10.30.11):** A presença de um serviço MySQL com seu *banner* visível expõe informações sobre a versão do software, o que pode ser explorado por atacantes.
- **Servidor LDAP Acessível (Host: 10.10.30.17):** Um servidor LDAP está acessível, indicando uma possível falta de controle de acesso adequado, o que pode levar à enumeração de diretórios e informações de usuários.
- **Serviço SMB com Enumeração de Compartilhamentos (Host: 10.10.30.15):** O serviço SMB permite a enumeração de compartilhamentos, expondo a estrutura de arquivos e diretórios internos da rede.
- **Interface Web do Zabbix Exposta (Host: 10.10.30.117):** A interface de monitoramento Zabbix está acessível externamente, representando um risco significativo para a integridade e disponibilidade do sistema de monitoramento.

Riscos Identificados:

- **Infiltração de Malware:** O acesso anônimo via FTP é um vetor direto para a inserção de *malware* ou a exfiltração de dados.
- **Exposição de Recursos Internos:** A enumeração via SMB pode revelar informações sensíveis sobre a estrutura da rede e os recursos disponíveis.

- **Aumento da Superfície de Ataque:** Serviços com *banners* abertos ou sem autenticação visível fornecem informações valiosas a atacantes, facilitando a identificação de vulnerabilidades.

Recomendações

Para mitigar os riscos identificados e fortalecer a postura de segurança da rede, as seguintes recomendações são essenciais:

- **Restrição de Acesso FTP:** Desabilitar ou configurar restrições rigorosas para o acesso anônimo em serviços FTP.
  O acesso FTP anônimo, quando mal configurado, permite que qualquer pessoa sem credenciais acesse, visualize e, em alguns casos, modifique ou faça upload de arquivos para o servidor. Isso representa um risco significativo de exposição de dados confidenciais, distribuição de malware ou uso indevido dos recursos do servidor. Restringir ou desabilitar o acesso anônimo garante que apenas usuários autenticados e autorizados possam interagir com o servidor FTP, reduzindo a superfície de ataque e prevenindo acessos não autorizados.

- **Isolamento de Infraestrutura Crítica:** Implementar o isolamento de dispositivos de infraestrutura, como servidores de monitoramento (Zabbix) e impressoras, em segmentos de rede dedicados e com políticas de acesso restritas.
  Servidores de monitoramento e impressoras, embora pareçam inofensivos, podem ser pontos de entrada para ataques se não forem devidamente protegidos. Ao isolá-los em segmentos de rede dedicados (VLANs ou sub-redes separadas) com firewalls e políticas de acesso rigorosas, você impede que um comprometimento nesses dispositivos se propague para a rede principal. Isso limita o "movimento lateral" de um atacante, contendo qualquer violação a um segmento específico e protegendo ativos mais críticos da rede.

- **Desativação de Serviços Desnecessários:** Desativar todos os serviços que não são estritamente necessários ou aplicar regras de *firewall* para limitar o acesso por endereço IP a apenas fontes autorizadas.

  Cada serviço ativo em um sistema representa uma porta potencialmente aberta para vulnerabilidades. Serviços desnecessários consomem recursos e, mais importante, aumentam a superfície de ataque da rede. Ao desativá-los, você remove potenciais vetores de ataque que poderiam ser explorados por atacantes. Para serviços que precisam permanecer ativos, mas têm uso limitado, a aplicação de regras de firewall baseadas em IP garante que apenas as fontes legítimas e autorizadas possam acessá-los, minimizando o risco de acesso indevido por atacantes externos ou internos.

- **Monitoramento e Auditoria:** Estabelecer um sistema robusto de monitoramento e registro de acessos para serviços críticos como MySQL, SMB e LDAP, permitindo a detecção precoce de atividades suspeitas.
  O monitoramento e a auditoria contínuos são cruciais para a detecção de ameaças e a resposta a incidentes. Serviços como MySQL (bancos de dados), SMB (compartilhamento de arquivos) e LDAP (autenticação e diretório) são alvos comuns de atacantes devido à sensibilidade dos dados que eles gerenciam. Registrar e analisar logs de acesso para esses serviços permite identificar tentativas de acesso não autorizadas, atividades incomuns (como acessos em horários estranhos ou de IPs desconhecidos) e o uso indevido de credenciais. Isso permite uma resposta rápida a incidentes de segurança, minimizando o dano potencial.

- **Revisão de Permissões:** Realizar uma revisão completa das configurações de compartilhamento e permissões em todos os serviços expostos para garantir o princípio do menor privilégio.
  O princípio do menor privilégio é um conceito fundamental em segurança da informação, que estabelece que cada usuário, programa ou processo deve ter apenas o nível de acesso e as permissões mínimas necessárias para executar suas funções. Permissões excessivas (por exemplo, acesso de escrita onde apenas leitura é necessária, ou acesso a dados confidenciais por usuários que não precisam deles) criam uma porta aberta para abusos e vazamentos de dados em caso de comprometimento. Uma revisão detalhada garante que os usuários e sistemas tenham apenas o acesso estritamente necessário, reduzindo o risco de movimentação lateral, escalonamento de privilégios e exfiltração de dados.

Plano de Ação (80/20)

Ação	Impacto	Facilidade	Prioridade	Justificativa
Isolar a impressora da rede principal	Alto	Média	Alta	Impressoras com serviços SMB abertos são alvos comuns de ataques como ransomware e exploração de compartilhamentos indevidos.
Desativar serviço FTP (porta 21)	Médio	Alta	Alta	FTP é um protocolo inseguro (dados em texto claro). Desativar ou migrar para SFTP reduz

				riscos de interceptação.
Restringir acesso ao serviço MySQL (porta 3306)	Alto	Média	Alta	O banco de dados deve ser acessível apenas a IPs autorizados; aberto na rede pode expor dados sensíveis.
Reforçar autenticação no serviço LDAP	Médio	Baixa	Média	LDAP pode expor informações de diretório se não estiver adequadamente configurado e protegido.
Revisar e restringir compartilhamentos SMB	Alto	Média	Alta	Compartilhamentos mal configurados podem permitir acesso não autorizado a arquivos críticos.
Monitorar o servidor web Zabbix (porta 80)	Médio	Alta	Média	Aplicações web com painéis expostos (Zabbix) devem ter autenticação forte e atualizações em dia.

Conclusão

A análise da rede mostrou que existem algumas "portas abertas" e serviços que não estão configurados de forma segura em várias partes da rede, como na rede corporativa, na rede de convidados e na rede de infraestrutura. Encontramos serviços como **FTP** e **SMB**, que podem ser facilmente explorados por pessoas mal-intencionadas se não forem corrigidos.

Usamos algumas ferramentas para identificar os computadores conectados e os serviços que estavam rodando. Com base no que encontramos, criamos um plano de ação focado nas melhorias mais importantes e fáceis de implementar para aumentar a segurança.

Próximos Passos Recomendados:

- **Ação Imediata:** Colocar em prática as medidas de segurança mais urgentes do nosso plano.
- **Melhorar a Separação da Rede:** Organizar a rede para que diferentes partes (como a rede de convidados e a rede corporativa) fiquem mais isoladas, limitando o acesso.
- **Monitoramento Constante:** Começar a monitorar continuamente os serviços da rede e fazer verificações regulares para garantir que tudo continue seguro.
- **Treinamento da Equipe:** Treinar as pessoas para saberem como prevenir problemas e como agir rapidamente caso aconteça um incidente de segurança.

Essas ações são muito importantes para diminuir os riscos e deixar a rede mais forte contra ataques cibernéticos.

Anexos

- Saída dos scans

https://github.com/BeatrizSanto/formacao-cybersec-Projeto1/tree/main/modulo1-fundamentos/projeto_final_opcao_1/Sa%C3%ADda%20dos%20scans