

P.PORTO

ESCOLA
SUPERIOR
DE TECNOLOGIA
E GESTÃO

LICENCIATURA EM
SEGURANÇA INFORMÁTICA EM REDES DE COMPUTADORES

AUDITORIA INFORMÁTICA

Trabalho Prático 1



David Santos – 8220651

ESTG, abril de 2025

ÍNDICE

1	Sumário Executivo.....	2
2	Arquitetura da Rede (Topologia e Ativos Identificados)	3
2.1	Ambiente da Auditoria	3
2.2	Máquinas Identificadas e Endereçamento IP	3
3	Metodologia	4
3.1	Abordagem Geral	4
3.2	Mapeamento da Rede e Serviços	4
3.3	Ferramentas de Análise e Identificação de Vulnerabilidades Automatizadas	8
3.4	Análise de Tráfego de Rede	20
3.5	Validações Manuais.....	24
4	Identificação das Vulnerabilidades.....	30
4.1	Nessus	30
4.2	OpenVAS.....	39
5	Análise de Impacto e Probabilidade.....	43
5.1	Metodologia de Avaliação	43
5.2	Agrupamento de Vulnerabilidades.....	43
5.3	Análise por Host	44
5.4	Resumo Geral	47
6	Propostas de Mitigação	48
6.1	Mitigações a nível da Rede.....	48
6.2	Mitigações para Sistemas Operativos Desatualizados	49
6.3	Mitigações para Serviços Inseguros	49
6.4	Mitigações para Software Desatualizado	50
6.5	Mitigações para Configurações Inseguras.....	51
6.6	Medidas Gerais de Segurança	52
6.7	Priorização das Mitigações.....	52
6.8	Resumo das Mitigações.....	53
7	Respostas às Questões	54
7.1	Questão 1 - Uso de Múltiplas Plataformas de Armazenamento na Cloud	54
7.2	Questão 2 - Uso de Dispositivos Pessoais	55
7.3	Questão 3 - Uso de Aplicações de Mensagens Não Autorizadas	56
7.4	Questão 4 - Sistemas Legados (WinServer 2016 e Windows 7)	57
7.5	Questão 5 - Permissões Excessivas e Falta de MFA.....	58
8	Conclusões.....	60

1 SUMÁRIO EXECUTIVO

A auditoria à infraestrutura de TI da SECURETECH revelou vulnerabilidades críticas que colocam em risco a confidencialidade, integridade e disponibilidade dos dados e serviços corporativos. Realizada num ambiente simulado (rede 10.0.10.0/24), a análise identificou quatro máquinas, com destaque para o Windows Server 2016 (10.0.10.10) e o Ubuntu 18.04 Server (10.0.10.12), ambos com falhas graves, como a vulnerabilidade EternalBlue (MS17-010) e uma backdoor na porta 5555, respectivamente. Estas, combinadas com a ausência de segmentação de rede, permitem a propagação rápida de ataques, como ransomware ou roubo de dados.

Foram identificadas práticas inadequadas que amplificam os riscos: uso de plataformas de cloud não autorizadas, dispositivos pessoais sem controlo, aplicações de mensagens inseguras, sistemas legados (Windows 7) e permissões excessivas sem autenticação multifator (MFA). Estas questões expõem a SECURETECH a violações de conformidade e possíveis perdas.

As recomendações prioritárias incluem:

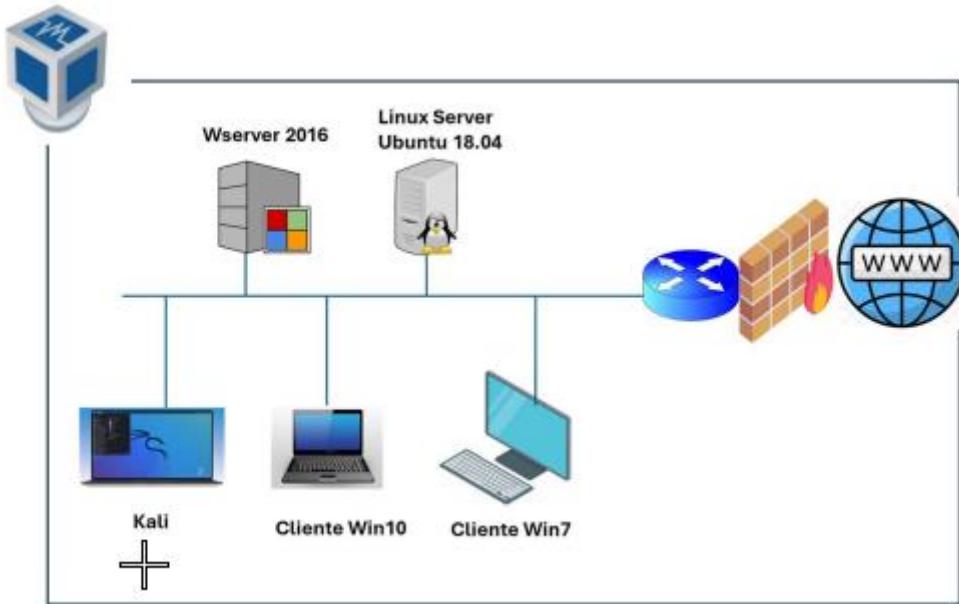
- Fechar imediatamente a backdoor na porta 5555 e aplicar o patch no Windows.
- Segmentar a rede com VLANs e firewalls para limitar ataques laterais.
- Migrar sistemas legados (Ubuntu 18.04 para 22.04, Windows 7 para 11).
- Implementar MFA e RBAC para proteger acessos sensíveis.
- Adotar plataformas oficiais (OneDrive, Microsoft Teams) com DLP e monitoramento.

A implementação destas medidas reduzirá drasticamente o risco de incidentes, garantindo conformidade e continuidade operacional. Propõe-se um plano faseado, com ações críticas imediatas, seguido de auditorias trimestrais para validar a eficácia. A SECURETECH deve agir rapidamente para proteger os seus ativos e reputação.

2 ARQUITETURA DA REDE (TOPOLOGIA E ATIVOS IDENTIFICADOS)

2.1 Ambiente da Auditoria

A auditoria foi conduzida num ambiente controlado e simulado, recorrendo à ferramenta VirtualBox, num cenário montado especificamente para representar a infraestrutura da empresa SECURETECH. Todas as máquinas virtuais foram configuradas para operarem na rede interna 10.0.10.0/24, sem qualquer tipo de segmentação lógica ou física da mesma.



A nível de rede, trata-se de um cenário que simula uma infraestrutura empresarial em que máquinas e utilizadores operam sem distinção de áreas ou funções, permitindo comunicação direta entre todos os nós, independentemente de suas funções ou serviços, o que aumenta o risco de propagação de ataques em caso de comprometimento de um dos sistemas.

2.2 Máquinas Identificadas e Endereçamento IP

Foram identificadas cinco máquinas activas na rede, incluindo a máquina utilizada para a auditoria (Kali Linux) e quatro máquinas-alvo. A tabela abaixo sumariza os endereços IP, sistemas operacionais e funções principais, com base no mapeamento inicial e no cenário fornecido:

Endereço IP	Sistema Operativo	Descrição / Função
10.0.10.5	Kali Linux	Máquina de auditoria utilizada para testes. Ferramentas de ataque e análise.
10.0.10.10	Windows Server 2016	Servidor com aplicações críticas e serviços corporativos.
10.0.10.11	Windows 10	Posto de trabalho de utilizador comum. Aplicações corporativas.
10.0.10.12	Ubuntu 18.04 Server	Servidor de armazenamento e serviços de rede.
10.0.10.13	Windows 7	Posto de trabalho de utilizador comum. Aplicações corporativas.

3 METODOLOGIA

3.1 Abordagem Geral

A auditoria foi conduzida de forma estruturada, com o objectivo de mapear os activos da rede, identificar serviços activos, detectar vulnerabilidades e analisar a segurança das comunicações na infraestrutura da SECURETECH. O processo envolveu várias fases: reconhecimento e mapeamento inicial da rede, análise automatizada de vulnerabilidades, captura de tráfego e validação manual de resultados. Todas as actividades foram realizadas a partir da máquina Kali Linux (10.0.10.5).

Nota: A preparação do ambiente Kali Linux, incluindo a instalação das ferramentas utilizadas, não será abordada, uma vez que está fora do âmbito deste trabalho, que se centra na execução e análise dos testes de segurança.

3.2 Mapeamento da Rede e Serviços

Esta fase teve como objectivo identificar as máquinas activas, os sistemas operativos em execução e os serviços disponíveis na rede 10.0.10.0/24. Foram utilizadas duas ferramentas complementares: Nmap e Wafw00f.

3.2.1 Nmap

O Nmap (Network Mapper) é uma ferramenta de open-source para mapeamento de redes e enumeração de serviços. Permite descobrir dispositivos activos, identificar portas abertas, detectar sistemas operativos e recolher informações detalhadas sobre serviços, incluindo versões de software e configurações.

Na auditoria, o Nmap foi executado primeiramente para ter uma visão geral sobre a rede.

```
(kali㉿kali)-[~]
$ nmap 10.0.10.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-23 20:11 WET
Nmap scan report for 10.0.10.10
Host is up (0.00069s latency).
Not shown: 987 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
7070/tcp  open  realserver
MAC Address: 08:00:27:09:B7:1C (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.10.11
Host is up (0.00039s latency).
All 1000 scanned ports on 10.0.10.11 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:31:24:99 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.10.12
Host is up (0.00053s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
5555/tcp  open  freeciv
MAC Address: 08:00:27:D3:77:54 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.10.13
Host is up (0.00057s latency).
All 1000 scanned ports on 10.0.10.13 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:42:5A:95 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.10.5
Host is up (0.0000030s latency).
All 1000 scanned ports on 10.0.10.5 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (5 hosts up) scanned in 22.14 seconds
```

A partir disto já pude detalhar o scope do nmap com o seguinte comando para analisar apenas os endereços 10.0.10.10 a 10.0.10.13:

```
nmap -sV -A -Pn -p- -oN services_nmap.txt 10.0.10.10-13
```

Parâmetros:

```
-sV: Identifica versões dos serviços activos.  
-A: Activa opções agressivas, incluindo detecção de sistema operativo, scripts de enumeração e traceroute.  
-Pn: Ignora a descoberta de hosts, assumindo que todos os alvos estão activos.  
-p-: Analisa todas as 65.535 portas TCP.  
-oN: Guarda o resultado no ficheiro services_nmap.txt (anexado).
```

O Nmap identificou quatro máquinas activas, com as seguintes informações extraídas:

3.2.1.1 10.0.10.10

- **Sistema Operativo:** Windows Server 2016 Standard Evaluation.
- **Portas e Serviços:**
 - 53/tcp: DNS (Simple DNS Plus).
 - 80/tcp: HTTP (Microsoft IIS 10.0).
 - 88/tcp: Kerberos (Microsoft Windows Kerberos).
 - 135/tcp: MSRPC (Microsoft Windows RPC).
 - 139/tcp: NetBIOS-SSN (Microsoft Windows NetBIOS).
 - 389/tcp: LDAP (Microsoft Windows Active Directory LDAP, domínio securetech.local).
 - 445/tcp: Microsoft-DS (SMB, grupo de trabalho SECURETECH).
 - 464/tcp: kpasswd5 (serviço relacionado com Kerberos).
 - 593/tcp: ncacn_http (Microsoft Windows RPC over HTTP 1.0).
 - 636/tcp: tcpwrapped (LDAP seguro, possivelmente filtrado).
 - 3268/tcp: LDAP (Microsoft Windows Active Directory LDAP, domínio securetech.local).
 - 3269/tcp: tcpwrapped (LDAP seguro, possivelmente filtrado).
 - 5985/tcp: HTTP (Microsoft HTTPAPI 2.0, usado por SSDP/UPnP).
 - 7070/tcp: SSL/realserver (identificado como AnyDesk Client, com certificado).
 - 9389/tcp: .NET Message Framing.
 - 49666/tcp, 49667/tcp, 49670/tcp, 49672/tcp, 49685/tcp, 49706/tcp: Serviços desconhecidos.
- **Informações Adicionais:** Nome do host WIN-JJ98QQ44QVU, domínio securetech.local, MAC Address 08:00:27:09:B7:1C (VirtualBox). Scripts

SMB confirmaram assinatura obrigatória (smb2-security-mode) e autenticação ao nível de utilizador (smb-security-mode).

3.2.1.2 10.0.10.11:

- **Sistema Operativo:** Windows (identificação incerta, sugerido como XP SP3 ou Server 2019, com baixa fiabilidade devido a uma única porta aberta).
- **Portas e Serviços:**
 - 7680/tcp: Serviço desconhecido (identificado como pando-pub, possivelmente alguma porta P2P).
- **Informações Adicionais:** MAC Address 08:00:27:31:24:99 (VirtualBox). Resultados limitados devido à falta de portas adicionais.

3.2.1.3 10.0.10.12:

- **Sistema Operativo:** Linux (provavelmente Ubuntu 18.04, com base nos serviços e versão do kernel sugerida).
- **Portas e Serviços:**
 - 21/tcp: FTP (vsftpd 3.0.3).
 - 22/tcp: SSH (OpenSSH 7.6p1 Ubuntu 4ubuntu0.7, protocolo 2.0, com chaves RSA, ECDSA e ED25519).
 - 80/tcp: HTTP (Apache httpd 2.4.29, Ubuntu).
 - 5555/tcp: Serviço desconhecido (identificado como freeciv, possivelmente um falso positivo).
- **Informações Adicionais:** MAC Address 08:00:27:D3:77:54 (VirtualBox). Scripts SSH confirmaram detalhes das chaves de host.

3.2.1.4 10.0.10.13:

- **Sistema Operativo:** Não identificado devido à ausência de portas abertas.
- **Portas e Serviços:** Nenhuma porta detectada (todas filtradas ou fechadas).
- **Informações Adicionais:** MAC Address 08:00:27:42:5A:95 (VirtualBox). Provavelmente filtrado pelo windows firewall activo na máquina.

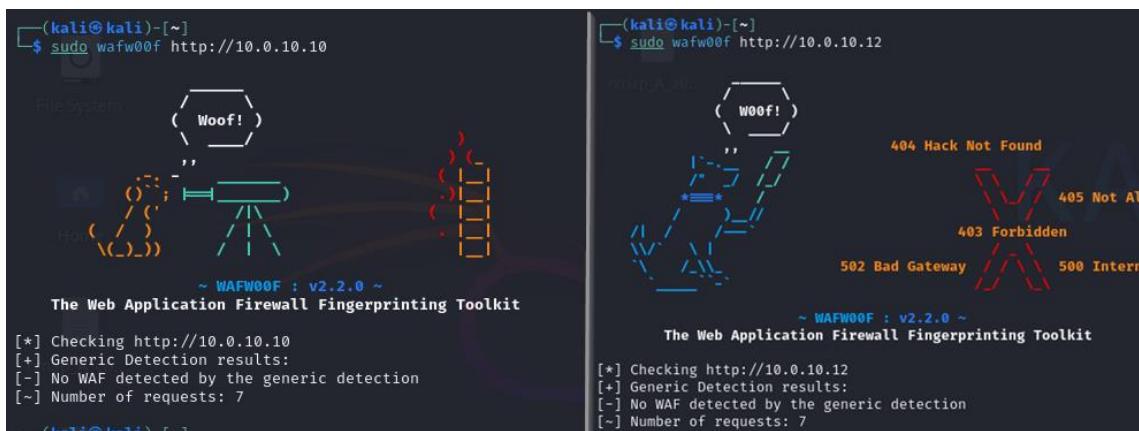
Toda a informação dada pelo Nmap foi guardada no ficheiro de nome **services_nmap.txt** enviado em anexo.

3.2.2 Wafw00f

O Wafw00f (Web Application Firewall Fingerprint) é uma ferramenta destinada a detectar a presença de firewalls de aplicações web (WAFs) à frente de servidores HTTP. Ajuda a identificar protecções que possam influenciar os resultados de scans, evitando falsos positivos em testes de vulnerabilidades web.

Foi executado os seguintes comandos para verificar os servidores HTTP identificados pelo Nmap (10.0.10.10 e 10.0.10.12):

```
wafw00f http://10.0.10.10  
wafw00f http://10.0.10.12
```



```
(kali㉿kali)-[~] $ sudo wafw00f http://10.0.10.10  
File System  
Woof!  
Host  
~ WAFW00F : v2.2.0 ~  
The Web Application Firewall Fingerprinting Toolkit  
[*] Checking http://10.0.10.10  
[+] Generic Detection results:  
[-] No WAF detected by the generic detection  
[~] Number of requests: 7  
(kali㉿kali)-[~] $ sudo wafw00f http://10.0.10.12  
File System  
Woof!  
404 Hack Not Found  
405 Not Allowed  
403 Forbidden  
502 Bad Gateway  
500 Internal Server Error  
~ WAFW00F : v2.2.0 ~  
The Web Application Firewall Fingerprinting Toolkit  
[*] Checking http://10.0.10.12  
[+] Generic Detection results:  
[-] No WAF detected by the generic detection  
[~] Number of requests: 7
```

O Wafw00f confirmou que nenhum WAF estava presente à frente dos serviços HTTP em 10.0.10.10 (IIS 10.0) e 10.0.10.12 (Apache 2.4.29). Esta ausência elimina a possibilidade de falsos positivos causados por filtragem de WAFs, garantindo maior fiabilidade nos testes subsequentes.

3.3 Ferramentas de Análise e Identificação de Vulnerabilidades Automatizadas

Nesta fase da auditoria foram utilizadas ferramentas automatizadas de vulnerability scanning com o objetivo de identificar falhas nos sistemas de SECURETECH, tanto a partir de uma perspectiva externa (sem credenciais) como interna (com credenciais). Para isso, recorreu-se ao **Nuclei**, **Nessus** e **OpenVAS**, sendo cada uma delas configuradas para maximizar a detecção de falhas, com processos documentados através de printscreens que ilustram a criação e execução dos scans. Os resultados obtidos serão analisados em detalhe na seção seguinte.

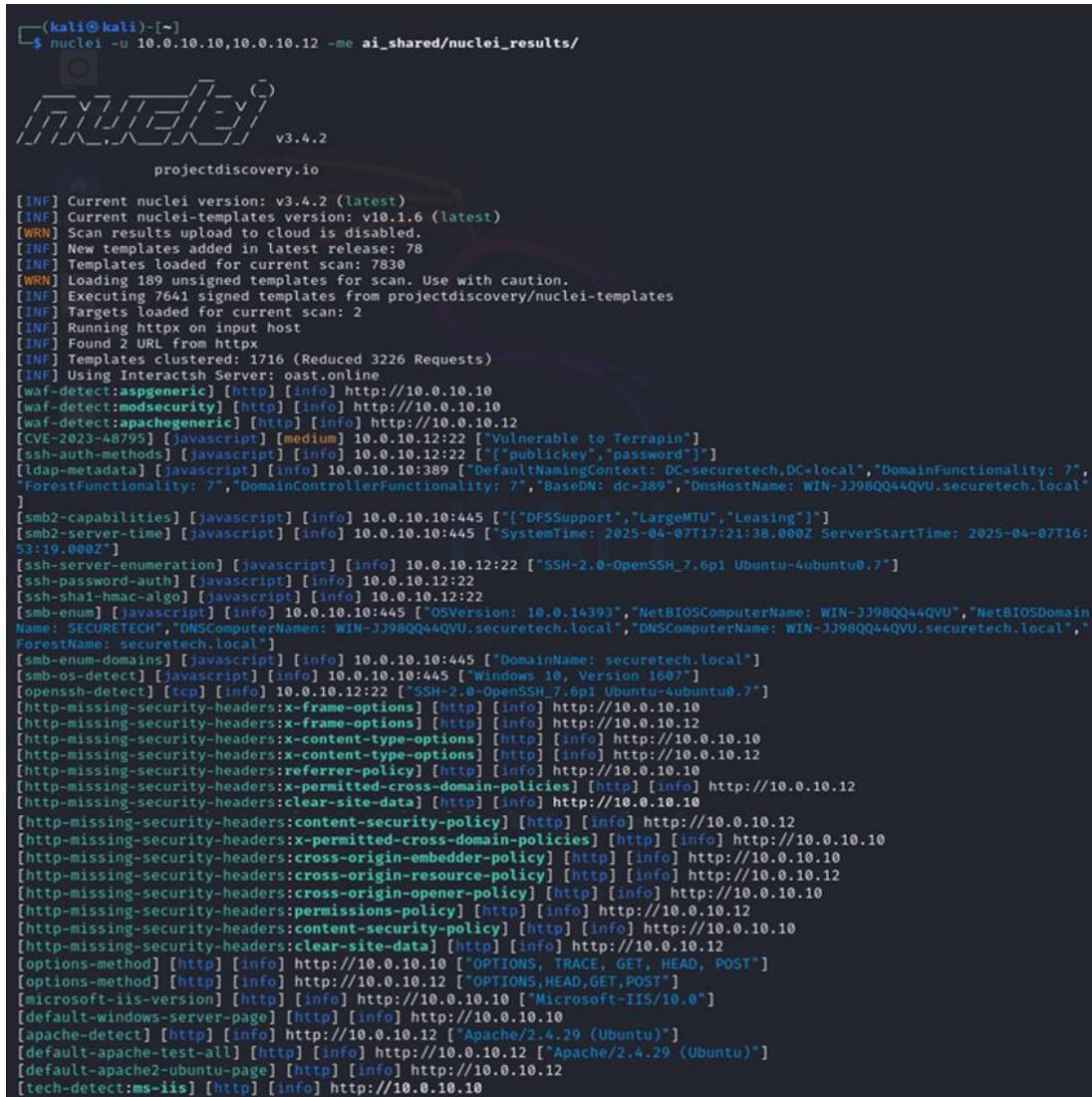
3.3.1 Nuclei

O Nuclei é uma ferramenta de detecção de vulnerabilidades que opera com base em modelos (templates), permitindo a identificação rápida de falhas comuns em serviços web, configurações inseguras, vulnerabilidades conhecidas e exposições em serviços de rede. Foi utilizado para examinar os serviços activos nas máquinas 10.0.10.10 (Windows Server 2016) e 10.0.10.12 (Ubuntu 18.04), com foco particular nos serviços HTTP, SMB e SSH. O comando executado foi o seguinte:

```
nuclei -u 10.0.10.10,10.0.10.12 -me ai_shared/nuclei_results/
```

Parâmetros:

- u: Especifica os alvos (10.0.10.10 e 10.0.10.12).
- me: Define o directório para exportação de resultados em markdown.



```
(kali㉿kali)-[~]
$ nuclei -u 10.0.10.10,10.0.10.12 -me ai_shared/nuclei_results/
```

projectdiscovery.io

```
[INF] Current nuclei version: v3.4.2 (latest)
[INF] Current nuclei-templates version: v10.1.6 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 78
[INF] Templates loaded for current scan: 7830
[WRN] Loading 189 unsigned templates for scan. Use with caution.
[INF] Executing 7641 signed templates from projectdiscovery/nuclei-templates
[INF] Targets loaded for current scan: 2
[INF] Running httpx on input host
[INF] Found 2 URL from httpx
[INF] Templates clustered: 1716 (Reduced 3226 Requests)
[INF] Using Interactsh Server: oast.online
[waf-detect:aspgeneric] [http] [info] http://10.0.10.10
[waf-detect:modsecurity] [http] [info] http://10.0.10.10
[waf-detect:apachegeneric] [http] [info] http://10.0.10.12
[CVE-2023-48795] [javascript] [medium] 10.0.10.12:22 ["Vulnerable to Terrapin"]
[ssh-auth-methods] [javascript] [info] 10.0.10.12:22 [{"publickey","password"}]
[ldap-metadata] [javascript] [info] 10.0.10.10:389 ["DefaultNamingContext: DC=securetech,DC=local","DomainFunctionality: 7","ForestFunctionality: 7","DomainControllerFunctionality: 7","BaseDN: dc=389","OuName: WIN-JJ98QQ44QVU.securetech.local"]
[smb2-capabilities] [javascript] [info] 10.0.10.10:445 [{"DFSSupport","LargeMTU","Leasing"}]
[smb2-server-time] [javascript] [info] 10.0.10.10:445 ["SystemTime: 2025-04-07T17:21:38.000Z ServerStartTime: 2025-04-07T16:54:19.000Z"]
[ssh-server-enumeration] [javascript] [info] 10.0.10.12:22 ["SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.7"]
[ssh-password-auth] [javascript] [info] 10.0.10.12:22
[ssh-sha1-hmac-algo] [javascript] [info] 10.0.10.12:22
[smb-enum] [javascript] [info] 10.0.10.10:445 ["OSVersion: 10.0.14393","NetBIOSComputerName: WIN-JJ98QQ44QVU","NetBIOSDomainName: SECURETECH","DNSComputerName: WIN-JJ98QQ44QVU.securetech.local","DNSComputerName: WIN-JJ98QQ44QVU.securetech.local","ForestName: securetech.local"]
[smb-enum-domains] [javascript] [info] 10.0.10.10:445 ["DomainName: securetech.local"]
[smb-os-detect] [javascript] [info] 10.0.10.10:445 ["Windows 10, Version 1607"]
[openssh-detect] [tcp] [info] 10.0.10.12:22 ["SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.7"]
[http-missing-security-headers:x-frame-options] [http] [info] http://10.0.10.10
[http-missing-security-headers:x-frame-options] [http] [info] http://10.0.10.12
[http-missing-security-headers:x-content-type-options] [http] [info] http://10.0.10.10
[http-missing-security-headers:x-content-type-options] [http] [info] http://10.0.10.12
[http-missing-security-headers:referrer-policy] [http] [info] http://10.0.10.10
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://10.0.10.12
[http-missing-security-headers:clear-site-data] [http] [info] http://10.0.10.10
[http-missing-security-headers:content-security-policy] [http] [info] http://10.0.10.12
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://10.0.10.10
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://10.0.10.10
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://10.0.10.12
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://10.0.10.10
[http-missing-security-headers:permissions-policy] [http] [info] http://10.0.10.12
[http-missing-security-headers:content-security-policy] [http] [info] http://10.0.10.10
[http-missing-security-headers:clear-site-data] [http] [info] http://10.0.10.12
[options-method] [http] [info] http://10.0.10.10 ["OPTIONS, TRACE, GET, HEAD, POST"]
[options-method] [http] [info] http://10.0.10.12 ["OPTIONS, HEAD, GET, POST"]
[microsoft-iis-version] [http] [info] http://10.0.10.10 ["Microsoft-IIS/10.0"]
[default-windows-server-page] [http] [info] http://10.0.10.10
[apache-detect] [http] [info] http://10.0.10.12 ["Apache/2.4.29 (Ubuntu)"]
[default-apache-test-all] [http] [info] http://10.0.10.12 ["Apache/2.4.29 (Ubuntu)"]
[default-apache2-ubuntu-page] [http] [info] http://10.0.10.12
[tech-detect:ms-iis] [http] [info] http://10.0.10.10
```

O Nuclei recolheu algumas informações sobre os serviços analisados, e aqui estão alguns dos resultados organizados por alvo:

- **10.0.10.10 (Windows Server 2016):**
 - **HTTP (porta 80):** Identificado servidor Microsoft IIS 10.0 com página padrão do Windows Server. Detectados métodos HTTP disponíveis (OPTIONS, TRACE, GET, HEAD, POST) e ausência de cabeçalhos de segurança, como X-Frame-Options e Content-Security-Policy. Sugestão de presença de WAF mas confirmado falso positivo visto que já tínhamos essa informação da ferramenta wafw00f.
 - **LDAP (porta 389):** Expostas informações do Active Directory, incluindo BaseDN (DC=securetech,DC=local), DnsHostName (WIN-JJ98QQ44QVU.securetech.local) e nível de funcionalidade de domínio/floresta (7, compatível com Windows Server 2016).
 - **SMB (porta 445):** Confirmado domínio securetech.local, nome do computador (WIN-JJ98QQ44QVU), versão do sistema operativo (Windows Server 2016, build 10.0.14393) e capacidades como suporte a DFS, Large MTU e Leasing.
- **10.0.10.12 (Ubuntu 18.04):**
 - **HTTP (porta 80):** Identificado servidor Apache 2.4.29 (Ubuntu) com página padrão ("It works"). Detectados métodos HTTP disponíveis (GET, POST, OPTIONS, HEAD) e ausência de cabeçalhos de segurança, como Strict-Transport-Security e X-Content-Type-Options. Sugestão de WAF mas confirmado falso positivo visto que já tínhamos essa informação da ferramenta wafw00f.
 - **SSH (porta 22):** Confirmado OpenSSH 7.6p1 Ubuntu-4ubuntu0.7, com autenticação por password e chave pública habilitadas. Identificado uso de algoritmos SHA-1 em HMAC e uma potencial vulnerabilidade no protocolo SSH (nível médio), a analisar posteriormente.

Os resultados foram guardados no directório **nuclei_results** tanto em **Md** como em **txt**, disponibilizados em anexo.

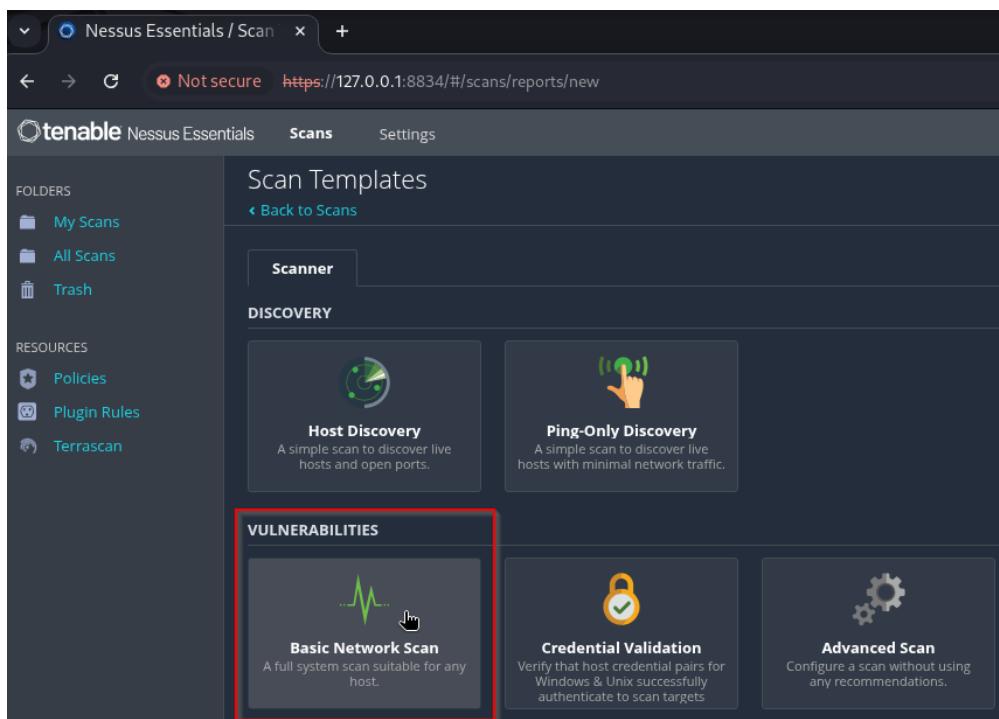
3.3.2 Nessus

O Nessus, acessível via <https://10.0.10.5:8834> (localhost no Kali Linux), é uma das ferramentas comerciais mais utilizadas para análise e avaliação de vulnerabilidades, sendo reconhecida pela sua capacidade de identificar falhas em sistemas, redes e aplicações. Foram configurados dois scans do tipo **Basic Network Scan**, abrangendo todas as portas TCP nos alvos 10.0.10.10 até 10.0.10.13:

- **AI_Basic_Scan (sem credenciais):** Configurado para simular a perspectiva de um atacante externo, sem acesso privilegiado, identificando serviços acessíveis e vulnerabilidades (remotas) associadas.
- **AI_Internal_Scan (com credenciais):** Configurado para realizar uma análise mais profunda com base nas credenciais fornecidas para os sistemas alvo, permitindo inspecção de configurações locais, software instalado e falhas que requerem autenticação para serem visíveis.

3.3.2.1 Processo de configuração

No interface web do Nessus, os scans foram criados seleccionando o modelo Basic Network Scan. Os alvos foram definidos como 10.0.10.10-13, com scanning de todas as portas activado. O processo foi documentado com capturas de ecrã que mostram a criação e configuração dos scans.



New Scan / Basic Network Scan

[Back to Scan Templates](#)

Settings [Credentials](#) [Plugins](#)

BASIC

- General
- Schedule
- Notifications

DISCOVERY >

ASSESSMENT >

REPORT >

ADVANCED >

Name: AI_basic_scan

Description: Scan básico sem uso de credenciais

Folder: My Scans

Targets: 10.0.10.10-10.0.10.13

Upload Targets Add File

Save | **Cancel**

New Scan / Basic Network Scan

[Back to Scan Templates](#)

Settings [Credentials](#) [Plugins](#)

BASIC

- General
- Schedule
- Notifications

DISCOVERY >

ASSESSMENT >

REPORT >

ADVANCED >

Name: AI_Internal_scan

Description: Scan básico usando credenciais

Folder: My Scans

Targets: 10.0.10.10-10.0.10.13

Upload Targets Add File

Save | **Cancel**

Settings

[Credentials](#) [Plugins](#)

BASIC >

DISCOVERY >

ASSESSMENT >

REPORT >

ADVANCED >

Scan Type: Port scan (all ports)

General Settings:
Always test the local Nessus host
Use fast network discovery

Port Scanner Settings:
Scan all ports (1-65535)
Use netstat if credentials are provided
Use SYN scanner if necessary

Ping hosts using:
TCP
ARP
ICMP (2 retries)

The screenshot shows the configuration interface for an internal scan. Under the 'Credentials' tab, there are four entries:

- SSH: User: openapp, Auth method: password
- Windows: User: administrator, Auth method: Password
- Windows: User: Win10User, Auth method: Password
- Windows: User: win7user, Auth method: Password

3.3.2.2 Resultados dos Scans

Os scans forneceram dados sobre sistemas, serviços e potenciais vulnerabilidades, que serão analisados na seção seguinte, complementando os resultados das ferramentas já usadas.

The screenshot shows the results of a basic network scan. It displays 4 hosts with their respective vulnerability counts:

Host	Vulnerabilities
10.0.10.10	76
10.0.10.12	33
10.0.10.11	9
10.0.10.13	4

Scan Details

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 4:48 PM
- End: Today at 5:02 PM
- Elapsed: 14 minutes

Vulnerabilities

The screenshot shows the detailed list of 41 vulnerabilities found during the scan. The table includes columns for Severity, CVSS, VPR, EPSS, Name, Family, and Count.

Sev	CVSS	VPR	EPSS	Name	Family	Count
MIXED	Microsoft...	Windows	3
MIXED	Openbsd ...	Misc.	5
LOW	2.1 *	2.9	0.0037	ICMP Timesta...	General	1
INFO	HTTP (Mu...)	Web Servers	8
INFO	SMB (Mul...)	Windows	7
INFO	SSH (Mult...)	Misc.	2
INFO	SSH (Mult...)	Service detection	2
INFO				Nessus SYN sc...	Port scanners	27
INFO				DCE Services E...	Windows	11
INFO				Service Detect...	Service detection	6
INFO				Ethernet Card ...	Misc.	4

Scan Details

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 4:48 PM
- End: Today at 5:02 PM
- Elapsed: 14 minutes

Vulnerabilities

AI_Internal_Scan

[Configure](#) [Audit Trail](#) [Launch](#) [Report](#) [Export](#)

Hosts 4 Vulnerabilities 97 Remediations 182 History 5

Filter Search Hosts 4 Hosts

Host	Vulnerabilities
10.0.10.10	58 Critical, 91 High, 15 Medium, 236 Low, 4 Info
10.0.10.12	23 Critical, 104 High, 68 Medium, 94 Low
10.0.10.11	9 Critical, 104 High, 68 Medium, 94 Low
10.0.10.13	4 Critical, 104 High, 68 Medium, 94 Low

Scan Details

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 2:49 PM
- End: Today at 3:12 PM
- Elapsed: 23 minutes

Vulnerabilities

Critical
High
Medium
Low
Info

AI_Internal_Scan

[Configure](#) [Audit Trail](#) [Launch](#) [Report](#) [Export](#)

Hosts 4 Vulnerabilities 97 Remediations 182 History 5

Filter Search Vulnerabilities 97 Vulnerabilities

Sev	CVSS	VPR	EPSS	Na...	Family	Count
Critical	10.0	C...	General	1
Mixed	Ubuntu	Local Security Checks	203
Mixed	Windows		97
Mixed	Windows	: Microsoft Bulletins	54
Mixed	Windows	: Microsoft Bulletins	33
Mixed	Windows	: Microsoft Bulletins	31
Mixed	Windows	: Microsoft Bulletins	17
Mixed	Windows		8
Critical	Misc.		2
High	7.5	8.9	0.4059	K...	Windows : Microsoft Bulletins	1
Mixed	Windows		13
Mixed	Windows		2
Medium	4.3	1.4	0.1818	M...	Windows : Microsoft Bulletins	1
Mixed	Misc.		5

Scan Details

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: March 31 at 2:49 PM
- End: March 31 at 3:12 PM
- Elapsed: 23 minutes

Vulnerabilities

Critical
High
Medium
Low
Info

Os relatórios foram exportados em formato PDF e estão disponíveis na pasta **Nessus** enviada em anexo.

3.3.3 OpenVAS

O OpenVAS (Open Vulnerability Assessment Scanner), acessível via <https://10.0.10.5:9392> (localhost do Kali), é uma plataforma open-source de identificação e análise de vulnerabilidades, baseada numa base de dados pública de CVEs. Tal como no Nessus, foram executados dois scans:

- **AI_Basic_Scan (sem credenciais):** Configurado para simular a perspectiva de um atacante externo, sem acesso privilegiado, identificando serviços acessíveis e vulnerabilidades (remotas) associadas.
- **AI_Scan (com credenciais):** Configurado para realizar uma análise mais profunda com base nas credenciais fornecidas para os sistemas alvo, permitindo inspecção de configurações locais, software instalado e falhas que requerem autenticação para serem visíveis.

3.3.3.1 Processo de Configuração:

No interface do Greenbone Security Assistant, os scans foram criados com a opção Full and Fast. Os alvos foram definidos como 10.0.10.10-13, com scannig de todas as portas TCP. Capturas de ecrã documentam a criação e execução dos scans.

The screenshot shows the 'New Target' configuration dialog. The fields are as follows:

- Name:** internal no credentials
- Comment:** (empty)
- Hosts:** Manual input field contains "10.0.10.10-13".
From file input field has "Choose File" and "No file chosen".
- Exclude Hosts:** Manual input field is empty.
From file input field has "Choose File" and "No file chosen".
- Allow simultaneous scanning via multiple IPs:** Yes (radio button selected).
- Port List:** All IANA assigned TCP (dropdown menu).
Buttons: [] [] []
- Alive Test:** Consider Alive (dropdown menu).
Buttons: [] []
- Credentials for authenticated checks:**
 - SSH:** -- (dropdown menu) on port 22 (dropdown menu).
Buttons: [] []
 - SMB:** -- (dropdown menu).
Buttons: [] []

At the bottom right are the **Cancel** and **Save** buttons.

New Task

Name AI_basic_scan

Comment Sem credenciais

Scan Targets internal no credentials

Alerts

Schedule -- Once

Add results to Assets Yes No

Apply Overrides Yes No

Min QoD 70

Alterable Task Yes No

Auto Delete Reports Do not automatically delete reports
 Automatically delete oldest reports but always keep newest reports

Scanner OpenVAS Default

Scan Config Full and fast

Cancel **Save**

New Target

Name internal network

Comment rede das máquinas de AI

Hosts Manual 10.0.10.10-13
 From file Choose File No file chosen

Exclude Hosts Manual
 From file Choose File No file chosen

Allow simultaneous scanning via multiple IPs Yes No

Port List All TCP and Nmap top 10

Alive Test Consider Alive

Credentials for authenticated checks

SSH ssh linux server on port 22

i Elevate privileges --

SMB smb winServer

ESXi --

SNMP --

Reverse Lookup Only Yes No

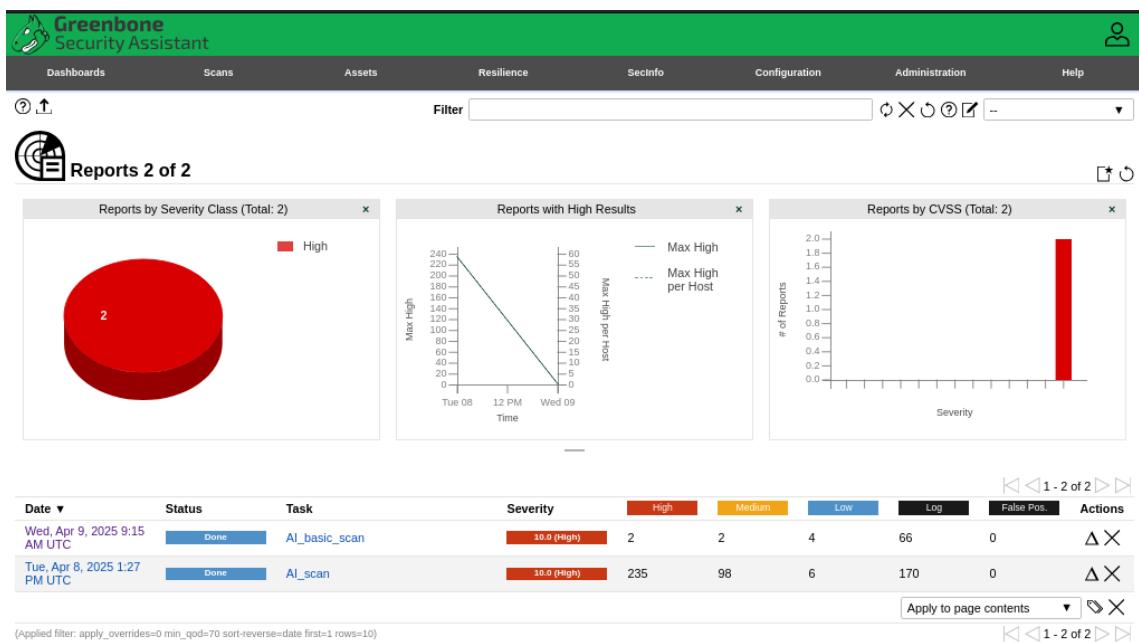
Cancel **Save**

New Task

Name	AI_scan
Comment	
Scan Targets	internal network <input type="button" value="..."/>
Alerts	<input type="button" value="..."/>
Schedule	-- <input type="checkbox"/> Once <input type="button" value="..."/>
Add results to Assets	<input checked="" type="radio"/> Yes <input type="radio"/> No
Apply Overrides	<input checked="" type="radio"/> Yes <input type="radio"/> No
Min QoD	70 <input type="button" value="..."/> %
Alterable Task	<input type="radio"/> Yes <input checked="" type="radio"/> No
Auto Delete Reports	<input checked="" type="radio"/> Do not automatically delete reports <input type="radio"/> Automatically delete oldest reports but always keep newest <input type="text" value="5"/> reports
Scanner	OpenVAS Default <input type="button" value="..."/>
Scan Config	<input type="button" value="..."/>
Order for target hosts	Sequential <input type="button" value="..."/>
Maximum concurrently executed NVTs per host	4 <input type="button" value="..."/>
Maximum concurrently scanned hosts	20 <input type="button" value="..."/>
<input type="button" value="Cancel"/> <input type="button" value="Save"/>	

3.3.3.2 Resultados dos Scans

Os scans identificaram informações sobre potenciais vulnerabilidades, que serão detalhadas na seção seguinte, em conjunto com os resultados das demais ferramentas.



AI_Basic_Scan:

Greenbone Security Assistant

Scans

Report Wed, Apr 9, 2025 9:15 AM UTC

Done

ID: bead550f-e64d-4406-8429-c16e52ac270b

Created: Wed, Apr 9, 2025 9:15 AM UTC Modified: Wed, Apr 9, 2025 9:45 AM UTC Owner: admin

Information	Results (8 of 120)	Hosts (2 of 4)	Ports (5 of 15)	Applications (6 of 6)	Operating Systems (2 of 2)	CVEs (2 of 2)	Closed CVEs (20 of 20)	TLS Certificates (1 of 1)	Error Messages (0 of 0)	User Tags (0)
Task Name	AI_basic_scan									
Comment	Sem credenciais									
Scan Time	Wed, Apr 9, 2025 9:15 AM UTC - Wed, Apr 9, 2025 9:45 AM UTC									
Scan Duration	0:29 h									
Scan Status	Done									
Hosts scanned	4									
Filter	apply_overrides=0 levels=html min_qod=70									
Timezone	Coordinated Universal Time (UTC)									

Greenbone Security Assistant

Scans

Report Wed, Apr 9, 2025 9:15 AM UTC

Done

ID: bead550f-e64d-4406-8429-c16e52ac270b

Created: Wed, Apr 9, 2025 9:15 AM UTC Modified: Wed, Apr 9, 2025 9:45 AM UTC Owner: admin

Information	Results (8 of 120)	Hosts (2 of 4)	Ports (5 of 15)	Applications (6 of 6)	Operating Systems (2 of 2)	CVEs (2 of 2)	Closed CVEs (20 of 20)	TLS Certificates (1 of 1)	Error Messages (0 of 0)	User Tags (0)					
IP Address	Hostname	OS	Ports	Apps	Distance	Auth	Start	End	High	Medium	Low	Log	False Positive	Total	Severity ▾
10.0.10.12		Windows	3	4			Wed, Apr 9, 2025 9:16 AM UTC	Wed, Apr 9, 2025 9:36 AM UTC	1	1	3	0	0	5	10.0 (High)
10.0.10.10		Windows	2	2			Wed, Apr 9, 2025 9:16 AM UTC	Wed, Apr 9, 2025 9:44 AM UTC	1	1	1	0	0	3	8.8 (High)

(Applied filter: apply_overrides=0 levels=html rows=100 min_qod=70 first=1 sort-reverse=severity)

Greenbone Security Assistant

Scans

Report Wed, Apr 9, 2025 9:15 AM UTC

Done

ID: bead550f-e64d-4406-8429-c16e52ac270b

Created: Wed, Apr 9, 2025 9:15 AM UTC Modified: Wed, Apr 9, 2025 9:45 AM UTC Owner: admin

Information	Results (8 of 120)	Hosts (2 of 4)	Ports (5 of 15)	Applications (6 of 6)	Operating Systems (2 of 2)	CVEs (2 of 2)	Closed CVEs (20 of 20)	TLS Certificates (1 of 1)	Error Messages (0 of 0)	User Tags (0)
Vulnerability		Severity ▾	QoD	Host IP	Name	Location	Created			
Possible Backdoor: Ingreslock	Medium	99 %	10.0.10.12			5555/tcp	Wed, Apr 9, 2025 9:25 AM UTC			
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	High	95 %	10.0.10.10			445/tcp	Wed, Apr 9, 2025 9:39 AM UTC			
DCE/RPC and MSRPC Services Enumeration Reporting	Medium	80 %	10.0.10.10			135/tcp	Wed, Apr 9, 2025 9:31 AM UTC			
FTP Unencrypted Cleartext Login	Medium	70 %	10.0.10.12			21/tcp	Wed, Apr 9, 2025 9:19 AM UTC			
TCP Timestamps Information Disclosure	Low	80 %	10.0.10.12			general/tcp	Wed, Apr 9, 2025 9:20 AM UTC			
Weak MAC Algorithm(s) Supported (SSH)	Low	80 %	10.0.10.12			22/tcp	Wed, Apr 9, 2025 9:21 AM UTC			
TCP Timestamps Information Disclosure	Low	80 %	10.0.10.10			general/tcp	Wed, Apr 9, 2025 9:26 AM UTC			
ICMP Timestamp Reply Information Disclosure	Low	80 %	10.0.10.12			general/icmp	Wed, Apr 9, 2025 9:19 AM UTC			

(Applied filter: apply_overrides=0 levels=html rows=100 min_qod=70 first=1 sort-reverse=severity)

AI_Scan:

Greenbone Security Assistant

Repo Tue, Apr 8, 2025
rt: 1:27 PM UTC

Information	Results (339 of 1135)	Hosts (2 of 4)	Ports (6 of 31)	Applications (51 of 51)	Operating Systems (2 of 2)	CVEs (328 of 328)	Closed CVEs (152 of 152)	TLS Certificates (1 of 1)	Error Messages (1 of 1)	User Tags (0)
Task Name	AI_scan									
Scan Time	Tue, Apr 8, 2025 1:28 PM UTC - Tue, Apr 8, 2025 2:33 PM UTC									
Scan Duration	1:05 h									
Scan Status	Done									
Hosts scanned	4									
Filter	apply_overrides=0 levels=hml min_qod=70									
Timezone	Coordinated Universal Time (UTC)									

Greenbone Security Assistant

Report Tue, Apr 8, 2025 1:27 PM UTC

Information	Results (339 of 1135)	Hosts (2 of 4)	Ports (6 of 31)	Applications (51 of 51)	Operating Systems (2 of 2)	CVEs (328 of 328)	Closed CVEs (152 of 152)	TLS Certificates (1 of 1)	Error Messages (1 of 1)	User Tags (0)					
IP Address	Hostname	OS	Ports	Apps	Distance	Auth	Start	End	High	Medium	Low	Log	False Positive	Total	Severity ▾
10.0.10.10	se06srv05.priv.fccn.pt	Windows	2	10		SSL	Tue, Apr 8, 2025 1:29 PM UTC	Tue, Apr 8, 2025 2:33 PM UTC	120	16	1	0	0	137	10.0 (High)
10.0.10.12	se06srv07.priv.fccn.pt	Windows	4	42		SSL	Tue, Apr 8, 2025 1:29 PM UTC	Tue, Apr 8, 2025 2:00 PM UTC	115	82	5	0	0	202	10.0 (High)

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

Greenbone Security Assistant

Information	Results (339 of 1135)	Hosts (2 of 4)	Ports (6 of 31)	Applications (51 of 51)	Operating Systems (2 of 2)	CVEs (328 of 328)	Closed CVEs (152 of 152)	TLS Certificates (1 of 1)	Error Messages (1 of 1)	User Tags (0)
Vulnerability	Severity ▾	QoD	Host IP	Name	Location	Created				
Possible Backdoor: Ingrislock	10.0 (High)	99 %	10.0.10.12	se06srv07.priv.fccn.pt	5555/tcp	Tue, Apr 8, 2025 1:49 PM UTC				
Microsoft Windows Multiple Vulnerabilities (KB4571694)	10.0 (High)	80 %	10.0.10.10	se06srv05.priv.fccn.pt	general/tcp	Tue, Apr 8, 2025 2:12 PM UTC				
Microsoft Windows Multiple Vulnerabilities (KB4565511)	10.0 (High)	80 %	10.0.10.10	se06srv05.priv.fccn.pt	general/tcp	Tue, Apr 8, 2025 2:12 PM UTC				
Microsoft Windows Multiple Vulnerabilities (KB4519998)	9.9 (High)	80 %	10.0.10.10	se06srv05.priv.fccn.pt	general/tcp	Tue, Apr 8, 2025 2:11 PM UTC				
Microsoft Windows Multiple Vulnerabilities (KB4525236)	9.9 (High)	80 %	10.0.10.10	se06srv05.priv.fccn.pt	general/tcp	Tue, Apr 8, 2025 2:11 PM UTC				
Microsoft Windows Multiple Vulnerabilities (KB5004238)	9.9 (High)	80 %	10.0.10.10	se06srv05.priv.fccn.pt	general/tcp	Tue, Apr 8, 2025 2:12 PM UTC				
Microsoft Windows Multiple Vulnerabilities (KB4494440)	9.9 (High)	80 %	10.0.10.10	se06srv05.priv.fccn.pt	general/tcp	Tue, Apr 8, 2025 2:11 PM UTC				
Microsoft Windows Multiple Vulnerabilities (KB5003197)	9.9 (High)	80 %	10.0.10.10	se06srv05.priv.fccn.pt	general/tcp	Tue, Apr 8, 2025 2:12 PM UTC				
Microsoft Windows Multiple Vulnerabilities (KB5005043)	9.9 (High)	80 %	10.0.10.10	se06srv05.priv.fccn.pt	general/tcp	Tue, Apr 8, 2025 2:12 PM UTC				
Microsoft Windows Multiple Vulnerabilities (KB4556813)	9.9 (High)	80 %	10.0.10.10	se06srv05.priv.fccn.pt	general/tcp	Tue, Apr 8, 2025 2:12 PM UTC				
Ubuntu: Security Advisory (USN-6522-2)	9.8 (High)	97 %	10.0.10.12	se06srv07.priv.fccn.pt	package	Tue, Apr 8, 2025 1:31 PM UTC				
Microsoft Windows Multiple Vulnerabilities (KB5008207)	9.8 (High)	80 %	10.0.10.10	se06srv05.priv.fccn.pt	general/tcp	Tue, Apr 8, 2025 2:12 PM UTC				

Os relatórios foram exportados em formato PDF e estão disponíveis na pasta OpenVAS enviada em anexo.

3.4 Análise de Tráfego de Rede

Esta fase tem como objectivo identificar comunicações inseguras na rede da SECURETECH, validar configurações observadas pelas ferramentas utilizadas anteriormente e detectar possíveis exposições de dados sensíveis. O Wireshark foi a ferramenta principal para captura de pacotes, com tráfego gerado através de interacções com ferramentas como netcat, curl, smbclient, ldapsearch, ftp e ssh. O processo e a análise dos pacotes capturados foram documentados com capturas de ecrã, incluídas em anexo, que ilustram a configuração, os filtros aplicados, os comandos executados e os pacotes analisados. Os resultados desta análise serão complementados na seção seguinte.

3.4.1 Wireshark

O Wireshark é uma ferramenta open-source para captura e análise de pacotes de rede, permitindo a inspecção detalhada de comunicações em tempo real ou a partir de ficheiros de captura gravados.

Na auditoria, o Wireshark foi executada a partir do Kali Linux (10.0.10.5) para capturar tráfego na interface eth0 correspondente ao ambiente VirtualBox da rede 10.0.10.0/24. Foram monitorizadas comunicações dos serviços identificados pelo Nmap, incluindo HTTP (10.0.10.10:80, 10.0.10.12:80), SMB (10.0.10.10:445), LDAP (10.0.10.10:389), FTP (10.0.10.12:21), SSH (10.0.10.12:22) e a porta suspeita 5555 (10.0.10.12). Para isso, foi gerado tráfego desses serviços e, para isolar comunicações relevantes, foram aplicados filtros de visualização no wireshark.

3.4.1.1 HTTP (10.0.10.10:80 e 10.0.10.12:80)

O filtro utilizado no wireshark foi **http** e o tráfego foi gerado com:

```
curl -X GET http://10.0.10.10
curl -X GET http://10.0.10.12
```

```
(kali㉿kali)-[~]
└─$ curl -X GET http://10.0.10.10
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<style type="text/css">
<!--
body {
    color:#000000;
    background-color:#0072C6;
    margin:0;
}
-->
<!--
#container {
    margin-left:auto;
    margin-right:auto;
    text-align:center;
}
-->
a img { A.com
    border:none;
}
-->
</style>
</head>
<body> A.all
<div id="container">
<a href="http://go.microsoft.com/fwlink/.png" alt="IIS" width="960" height=1></a>
</div>
</body>
</html>
```

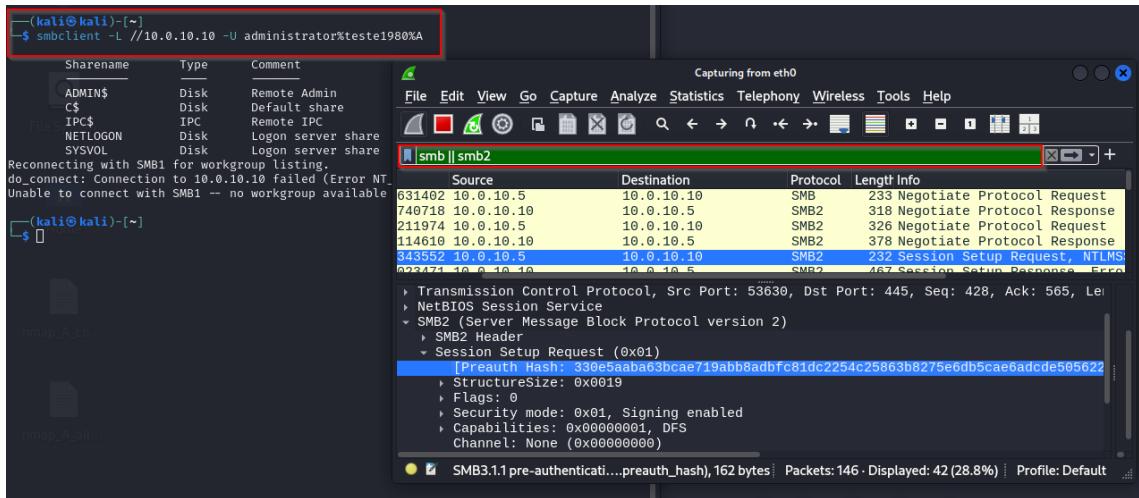
```
(kali㉿kali)-[~]
└─$ curl -X GET http://10.0.10.12
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<!--
Modified from the Debian original
Last updated: 2016-11-16
See: https://launchpad.net/bugs/1
-->
<head>
<meta http-equiv="Content-Type" c
<title>Apache2 Ubuntu Default Page</title>
<style type="text/css" media="scr
* {
    margin: 0px 0px 0px 0px;
    padding: 0px 0px 0px 0px;
}
body, html {
    padding: 3px 3px 3px 3px;
    background-color: #D8DBE2;
    font-family: Verdana, sans-serif;
    font-size: 11pt;
    text-align: center;
}
map {
    display: none;
}
div.main_page {
    position: relative;
    display: table;
    width: 800px;
    margin-bottom: 3px;
    margin-left: auto;
    margin-right: auto;
}
```

Os pacotes capturados mostram pedidos HTTP GET e respostas das páginas padrão do IIS ("IIS Windows Server") e do Apache ("It works"). O tráfego foi transmitido em texto plano, sem criptografia (HTTP em vez de HTTPS), permitindo a visualização de cabeçalhos e conteúdos das respostas.

3.4.1.2 SMB (10.0.10.10:445)

O filtro utilizado no wireshark foi **smb || smb2** e o tráfego foi gerado com:

```
smbclient -L //10.0.10.10 -U administrator%teste1980%
```

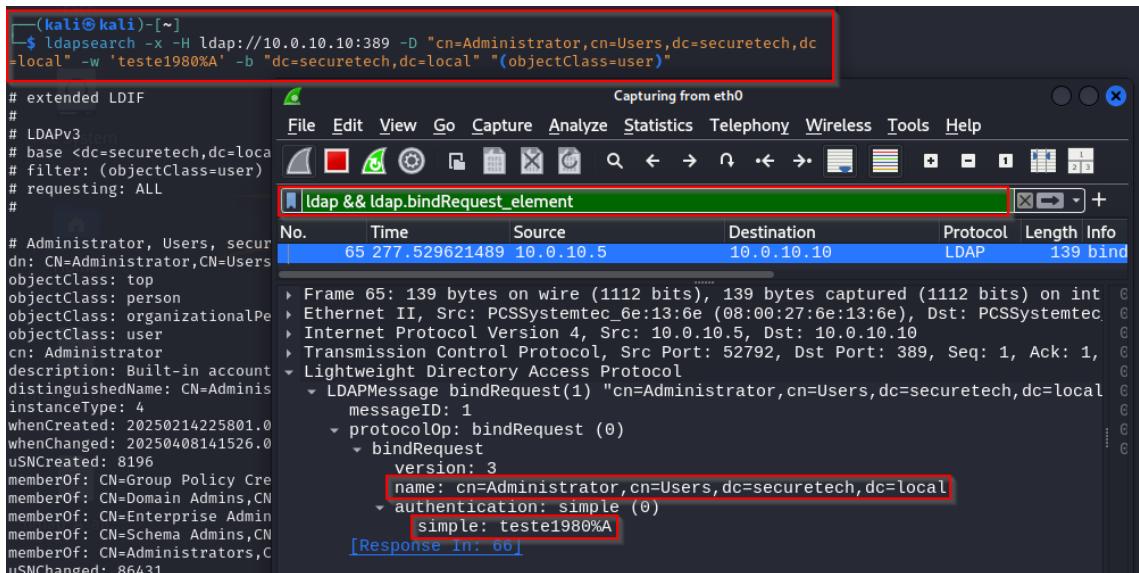


Os pacotes capturados incluem mensagens de "Negotiate Protocol" e "Session Request NTLM". A autenticação utilizou hashes NTLM, sem exposição de credenciais em texto plano mas permitindo rastrear ações como a listagem de partilhas (Shares), embora sem exposição direta da password. No entanto, alguns pacotes indicam o uso do protocolo SMBv1, que é obsoleto.

3.4.1.3 LDAP (10.0.10.10:389)

O filtro utilizado no wireshark foi **ldap** e o tráfego foi gerado com:

```
ldapsearch -x -H ldap://10.0.10.10 -D "administrator@securetech.local" -w teste1980%A -b "DC=securetech,DC=local"
```



Os pacotes capturados mostram uma autenticação simples, com a password administrativa transmitida diretamente no pacote de autenticação em texto plano.

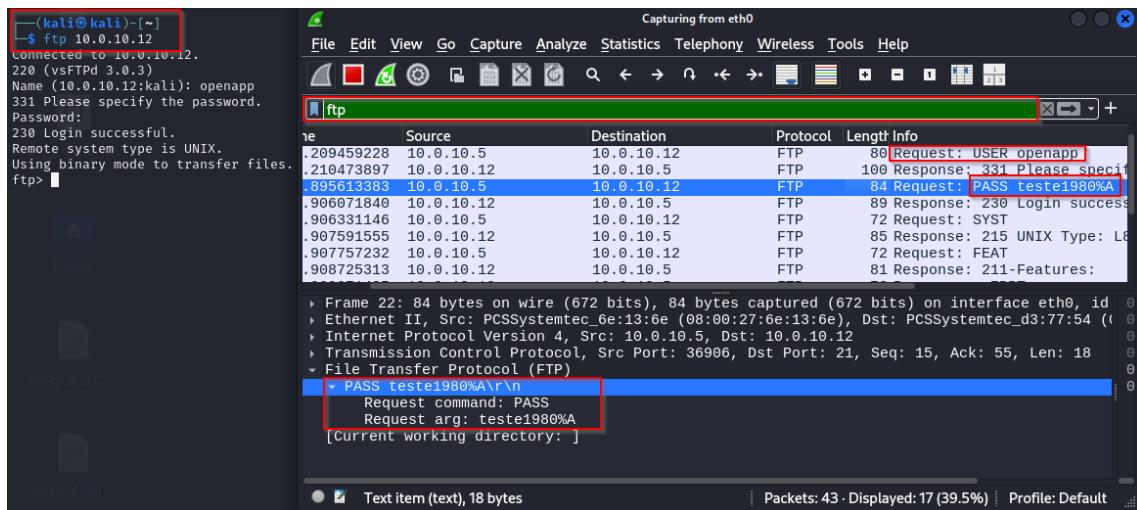
O servidor LDAP aceita autenticação sem criptografia pela porta 389, expondo

as credenciais e dados do Active Directory, como nomes de utilizadores e grupos.

3.4.1.4 FTP (10.0.10.12:21)

O filtro utilizado no wireshark foi **ftp** e o tráfego foi gerado com:

```
ftp 10.0.10.12
```

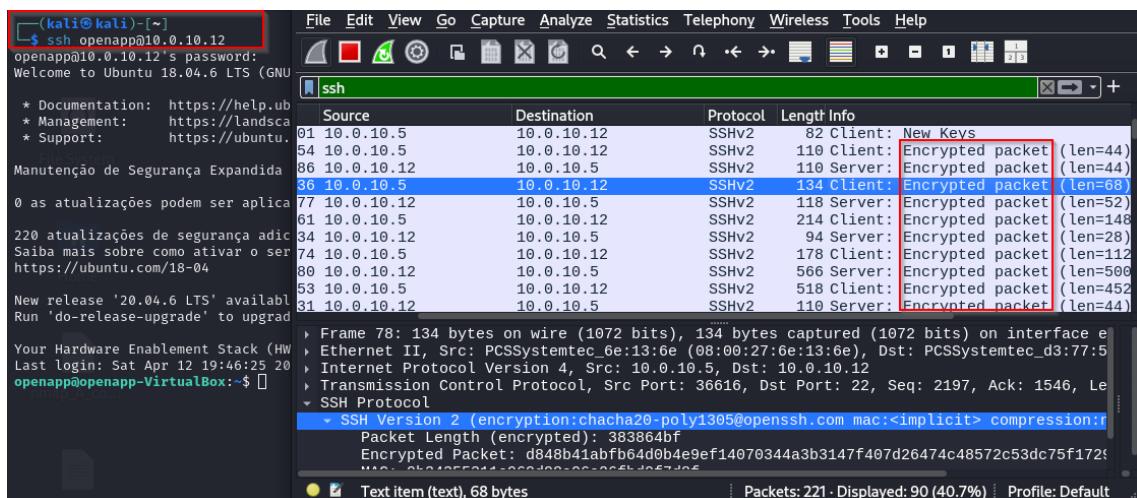


Os pacotes capturados revelam credenciais e transferências de ficheiros em texto plano. Dados de autenticação e conteúdos transferidos são visíveis sem criptografia, permitindo a interceptação completa das comunicações.

3.4.1.5 SSH (10.0.10.12:22)

O filtro utilizado no wireshark foi **ssh** e o tráfego foi gerado com:

```
ssh openapp@10.0.10.12
```

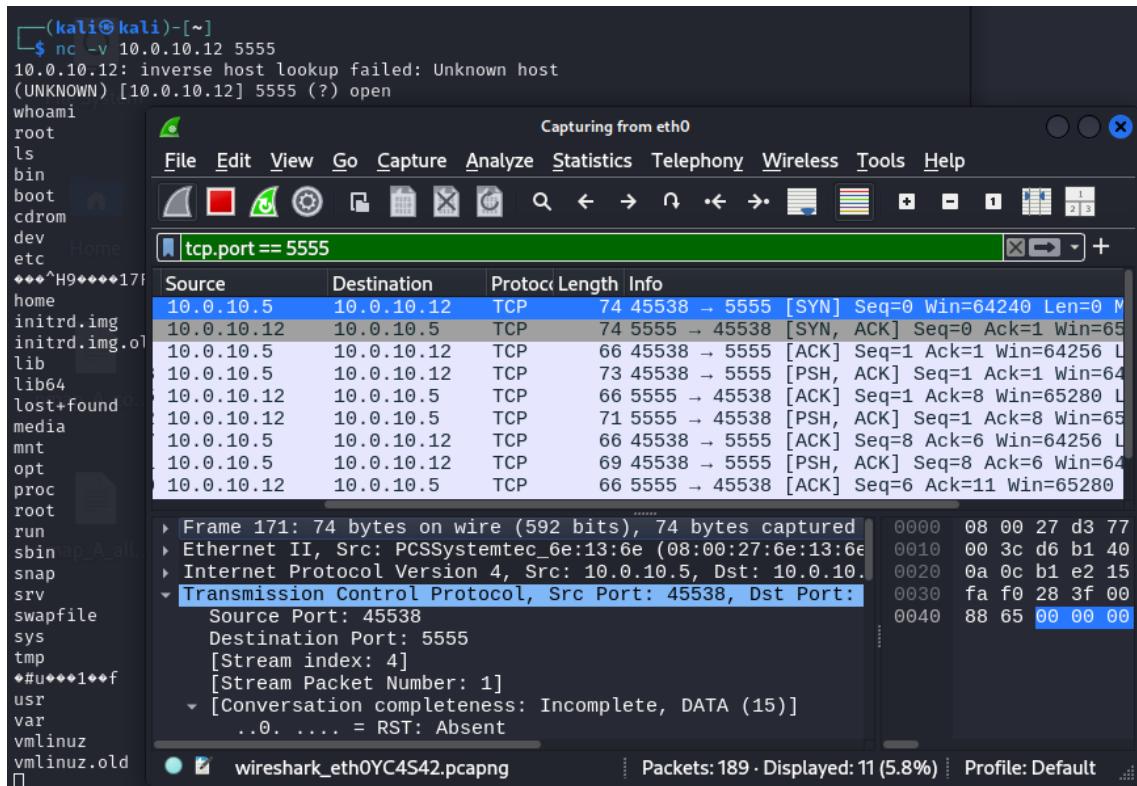


O tráfego capturado está totalmente criptografado, sem exposição de credenciais ou dados. Não foram observados conteúdos em texto plano, indicando que a comunicação SSH é segura em termos de confidencialidade.

3.4.1.6 Porta 5555 (10.0.10.12)

O filtro utilizado no wireshark foi **tcp.port == 5555** e o tráfego foi gerado com:

```
nc -v 10.0.10.12 5555
```



Os pacotes capturados mostram comandos enviados e respostas recebidas em texto plano, sem criptografia. A porta 5555 funciona como uma backdoor, permitindo a execução remota de comandos no servidor Ubuntu, com todas as interacções visíveis no tráfego.

3.5 Validações Manuais

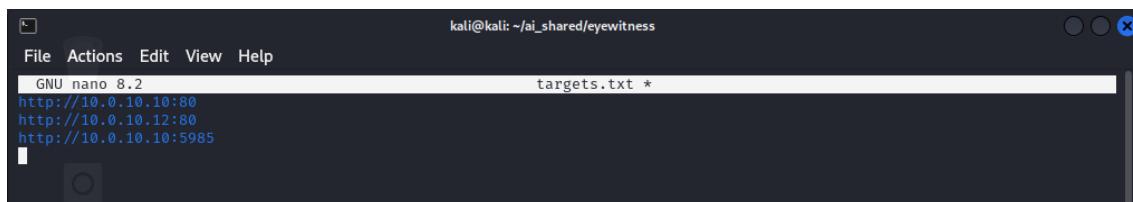
Esta fase tem como objectivo validar manualmente os serviços e configurações identificados nas fases anteriores, bem como detectar exposições adicionais que complementem as análises automatizadas. Foram utilizadas ferramentas como EyeWitness, curl e scripts do Nmap para inspecionar serviços HTTP/HTTPS, métodos HTTP e configurações SMB. O processo e os resultados foram

documentados com capturas de ecrã, incluídas no anexo, para evidenciar as verificações realizadas.

3.5.1 EyeWitness

O EyeWitness é uma ferramenta open-source que captura screenshots de serviços web (HTTP/HTTPS), permitindo a análise visual automatizada de páginas e interfaces expostas.

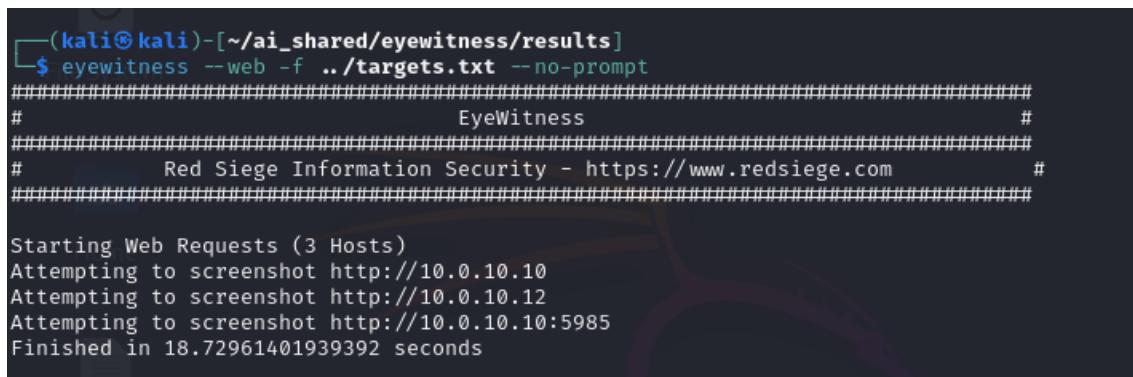
Na auditoria, o EyeWitness foi executado a partir do Kali Linux (10.0.10.5) para capturar screenshots dos serviços HTTP/HTTPS identificados pelo Nmap. Foi criado um ficheiro **targets.txt** com os alvos:



```
kali@kali: ~/ai_shared/eyewitness
File Actions Edit View Help
GNU nano 8.2                                         targets.txt *
http://10.0.10.10:80
http://10.0.10.12:80
http://10.0.10.10:5985
```

O comando utilizado foi:

```
eyewitness --web -f targets.txt --no-prompt
```



```
(kali㉿kali)-[~/ai_shared/eyewitness/results]
$ eyewitness --web -f ..//targets.txt --no-prompt
#####
#                               EyeWitness                         #
#####
#           Red Siege Information Security - https://www.redsiege.com      #
#####

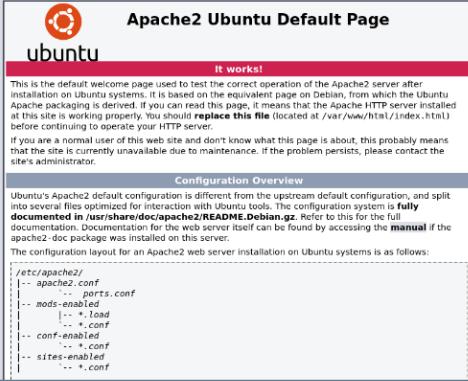
Starting Web Requests (3 Hosts)
Attempting to screenshot http://10.0.10.10
Attempting to screenshot http://10.0.10.12
Attempting to screenshot http://10.0.10.10:5985
Finished in 18.72961401939392 seconds
```

Parâmetros:

```
--web: Modo para captura de serviços web.
-f: Ficheiro com a lista de alvos (targets.txt).
--no-prompt: Executa sem interacção manual.
```

O EyeWitness processou os três alvos, capturando screenshots das interfaces web. Os resultados foram consolidados num relatório HTML, com capturas de ecrã que mostram as páginas padrão do IIS (10.0.10.10:80), Apache (10.0.10.12:80) e a interface WS-Management (10.0.10.10:5985).

Splash Pages

Web Request Info	Web Screenshot
<p>http://10.0.10.12</p> <p>Page Title: Apache2 Ubuntu Default Page: It works Date: Wed, 09 Apr 2025 11:15:46 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Sat, 15 Feb 2025 00:05:21 GMT ETag: "2aa6-62e230c0efb53" Accept-Ranges: bytes Content-Length: 10918 Vary: Accept-Encoding Connection: close Content-Type: text/html Response Code: 200</p> <p>Source Code</p>	
<p>http://10.0.10.10</p> <p>Page Title: IIS Windows Server Content-Type: text/html Last-Modified: Fri, 14 Feb 2025 22:18:48 GMT Accept-Ranges: bytes ETag: "dbc71f6b2e7fdb1:0" Server: Microsoft-IIS/10.0 X-Powered-By: ASP.NET Date: Wed, 09 Apr 2025 11:14:39 GMT Connection: close Content-Length: 703 Response Code: 200</p> <p>Source Code</p>	

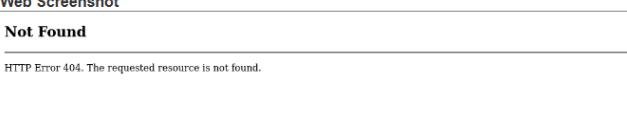
[Page 1](#) [Page 2](#)

Page 2

[Previous Page](#)

[Page 1](#) [Page 2](#)

404 Not Found

Web Request Info	Web Screenshot
<p>http://10.0.10.10:5985</p> <p>Page Title: Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Wed, 09 Apr 2025 11:14:36 GMT Connection: close Content-Length: 315 Response Code: 404</p> <p>Source Code</p>	

[Page 1](#) [Page 2](#)

O relatório e os screenshots associados foram guardados na pasta **eyewitness** enviada em anexo.

3.5.2 Validação de Métodos HTTP (TRACE)

O método HTTP TRACE foi testado manualmente para verificar configurações potencialmente inseguras nos serviços web, já que pode ser explorado em ataques como Cross-Site Tracing (XST).

O teste foi realizado no servidor 10.0.10.10:80 (IIS 10.0) com o comando:

```
curl -X TRACE http://10.0.10.10
```

Parâmetros:

```
-X TRACE: Especifica o método HTTP TRACE.
```

```
(kali㉿kali)-[~]
└─$ curl -X TRACE http://10.0.10.10
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>501 - Header values specify a method that is not implemented.</title>
<style type="text/css">
!--
body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}
fieldset{padding:0 15px 10px 15px;}
h1{font-size:2.4em;margin:0;color:#FFF;}
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.2em;margin:0 0 0;color:#000000;}
#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;
background-color:#555555;}
#content{margin:0 0 2%;position:relative;}
.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}
→
</style>
</head>
<body>
<div id="header"><h1>Server Error</h1></div>
<div id="content">
<div class="content-container"><fieldset>
<h2>501 - Header values specify a method that is not implemented.</h2>
<h3>The page you are looking for cannot be displayed because a header value in the request does not match certain configuration settings on the Web server. For example, a request header might specify a POST to a static file that cannot be posted to, or specify a Transfer-Encoding value that cannot make use of compression.</h3>
</fieldset></div>
</div>
</body>
</html>
```

O servidor retornou um erro 501 ("Not Implemented"), indicando que o método TRACE não é totalmente suportado ou foi bloqueado por configuração parcial. A resposta inclui a mensagem "The server you are requesting for cannot make use of a header", sugerindo que o IIS não processa o método TRACE adequadamente, mas a sua presença (mesmo com erro) confirma que o método está habilitado.

3.5.3 Enumeração SMB (Nmap)

O Nmap foi utilizado com scripts específicos para enumerar utilizadores e partilhas SMB no servidor Windows (10.0.10.10:445), validando configurações e permissões.

O comando executado foi:

```
sudo nmap --script smb-enum-users,smb-enum-shares -p 445 --script-args
smbuser=administrator,smbpass=teste1980%A 10.0.10.10
```

Parâmetros:

```
--script: Executa os scripts smb-enum-users (enumeração de utilizadores) e smb-enum-shares (enumeração de partilhas).
-p 445: Porta SMB.
--script-args: Credenciais para autenticação (smbuser=administrator, smbpass=teste1980%A).
```

```
(kali㉿kali)-[~]
$ sudo nmap --script smb-enum-users,smb-enum-shares -p 445 --script-args smbuser=administrator,smbpass=teste1980%A 10.0.10.10

Starting Nmap 7.94SVN ( https://nmap.org )
Nmap scan report for 10.0.10.10
Host is up (0.00041s latency).

PORT      STATE SERVICE
445/tcp    open  microsoft-ds
MAC Address: 08:00:27:09:B7:1C (Oracle VirtualBox virtual NIC)
```

3.5.3.1 Utilizadores Enumerados (smb-enum-users)

```
Host script results:
| smb-enum-users:
|_ SECURETECH\Administrator (RID: 500)
|   Description: Built-in account for administering the computer/domain
|   Flags:     Password does not expire, Normal user account
|_ SECURETECH\DefaultAccount (RID: 503)
|   Description: A user account managed by the system.
|   Flags:     Account disabled, Password not required, Password does not expire, Normal user account
|_ SECURETECH\Guest (RID: 501)
|   Description: Built-in account for guest access to the computer/domain
|   Flags:     Account disabled, Password not required, Password does not expire, Normal user account
|_ SECURETECH\krbtgt (RID: 502)
|   Description: Key Distribution Center Service Account
|   Flags:     Account disabled, Password Expired, Normal user account
|_ SECURETECH\testuser (RID: 1103)
|   Flags:     Account disabled, Password Expired, Normal user account
```

- SECURETECH\Administrator (RID: 500): Conta administrativa, sem expiração de senha.
- SECURETECH\DefaultAccount (RID: 503): Conta gerida pelo sistema, desativada.
- SECURETECH\Guest (RID: 501): Conta de convidado, desativada.
- SECURETECH\krbtgt (RID: 502): Conta de serviço Kerberos, desativada.
- SECURETECH\testuser (RID: 1103): Conta de utilizador, desativada, senha expirada.

3.5.3.2 Partilhas Enumeradas (smb-enum-shares):

- \\10.0.10.10\ADMIN\$: Partilha administrativa oculta, caminho C:\Windows, acesso READ/WRITE para o utilizador administrator, sem acesso anónimo.
- \\10.0.10.10\C\$: Partilha padrão oculta, caminho C:\, acesso READ/WRITE para o utilizador administrator, sem acesso anónimo.
- \\10.0.10.10\IPC\$: Partilha IPC oculta, acesso READ/WRITE para o utilizador administrator, acesso READ para anónimos.

- \\10.0.10.10\NETLOGON: Partilha do servidor de logon, caminho C:\Windows\SYSVOL\sysvol\securetech.local\SCRIPTS, acesso READ/WRITE para o utilizador administrator, sem acesso anónimo.
- \\10.0.10.10\SYSVOL: Partilha do servidor de logon, caminho C:\Windows\SYSVOL\sysvol, acesso READ para o utilizador administrator, sem acesso anónimo.

```

|- smb-enum-shares:
|   account_used: administrator
|   \\10.0.10.10\ADMIN$:
|     Type: STYPE_DISKTREE_HIDDEN
|     Comment: Remote Admin
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\Windows
|     Anonymous access: <none>
|     Current user access: READ/WRITE
|   \\10.0.10.10\C$:
|     Type: STYPE_DISKTREE_HIDDEN
|     Comment: Default share
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\
|     Anonymous access: <none>
|     Current user access: READ/WRITE
|   \\10.0.10.10\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: Remote IPC
|     Users: 1
|     Max Users: <unlimited>
|     Path:
|     Anonymous access: READ
|     Current user access: READ/WRITE
|   \\10.0.10.10\NETLOGON:
|     Type: STYPE_DISKTREE
|     Comment: Logon server share
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\Windows\SYSVOL\sysvol\securetech.local\SCRIPTS
|     Anonymous access: <none>
|     Current user access: READ/WRITE
|   \\10.0.10.10\SYSVOL:
|     Type: STYPE_DISKTREE
|     Comment: Logon server share
|     Users: 2
|     Max Users: <unlimited>
|     Path: C:\Windows\SYSVOL\sysvol
|     Anonymous access: <none>
|     Current user access: READ
|_

```

A enumeração de utilizadores confirma a existência de contas padrão (Administrator, Guest) e de um utilizador adicional (testuser), mas todas as contas não administrativas estão desativadas, reduzindo a superfície de ataque. A autenticação bem-sucedida com credenciais conhecidas valida os achados do Wireshark (autenticação NTLM). As partilhas ADMIN\$ e C\$ fornecem acesso total (READ/WRITE) ao utilizador administrator, enquanto IPC\$ permite leitura anónima, e SYSVOL e NETLOGON expõem caminhos críticos do Active Directory, mas apenas com acesso autenticado (excepto SYSVOL, limitado a leitura).

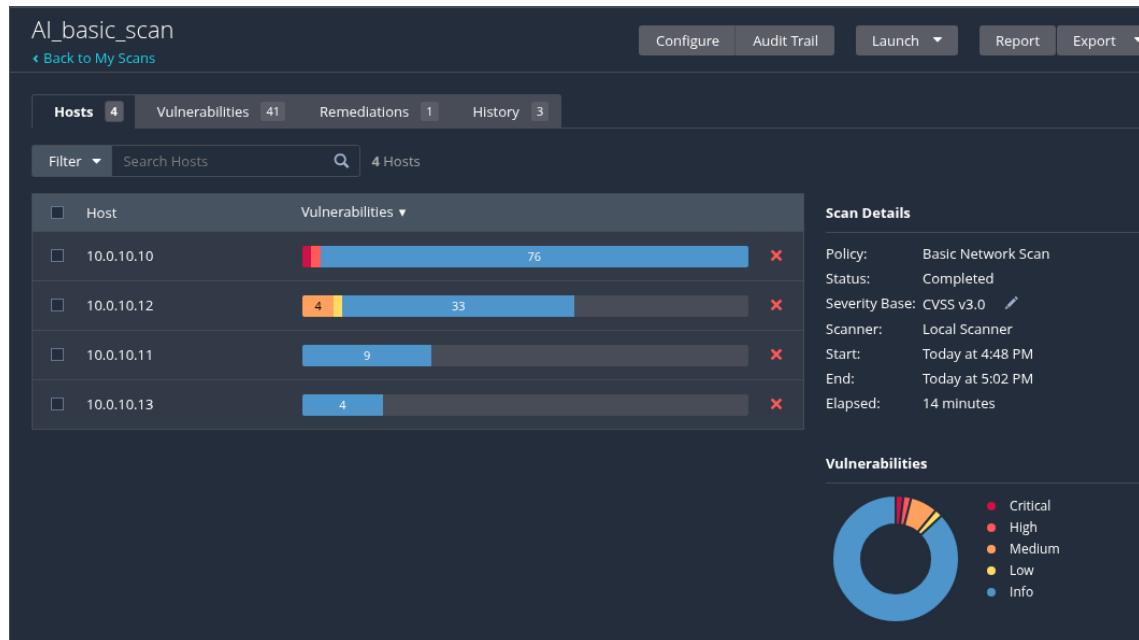
4 IDENTIFICAÇÃO DAS VULNERABILIDADES

Esta seção consolida os resultados dos vulnerability scans realizados nos hosts da rede, utilizando as ferramentas Nessus e OpenVAS, complementados por findings manuais (Nmap, Nuclei, Wireshark).

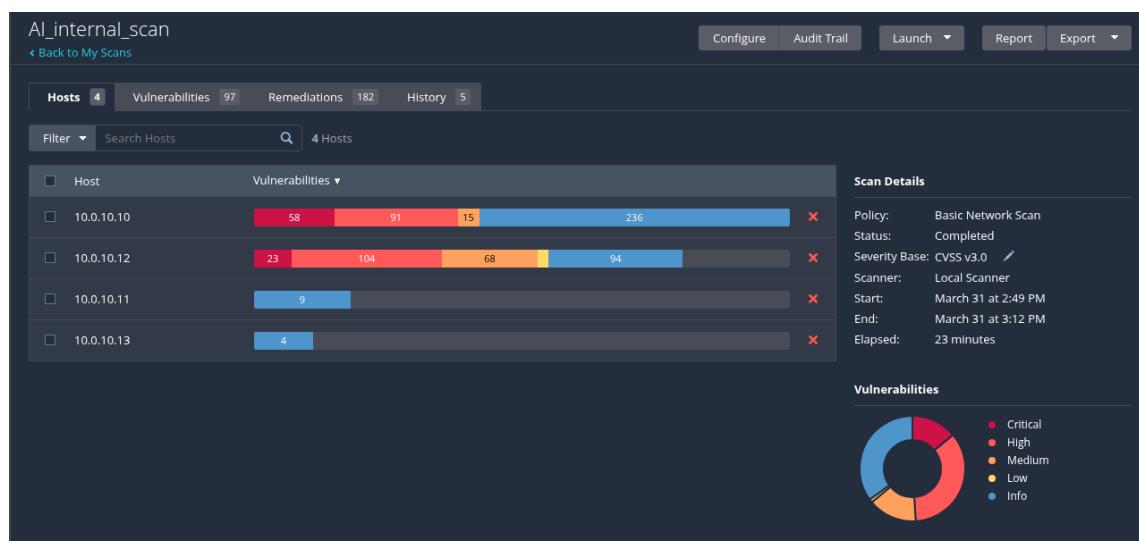
4.1 Nessus

Aqui, listam-se as vulnerabilidades de severidade Critical, High e Medium identificadas pelo Nessus, organizadas por host e, dentro de cada host, por serviço. Lembrando que são resultados dos dois scans:

- **AI_Basic_Scan (14 minutos)**



- **AI_Internal_Scan (23 minutos)**



4.1.1 10.0.10.10 (Windows Server 2016)

Total Vulnerabilidades: 307

10.0.10.10



SMB (Server Message Block)

Sev ▾	CVSS ▾	VPR ▾	EPSS ▾	Name ▾	Family ▾	Count ▾	⚙️
CRITICAL	9.8	6.7	0.2724	Microsoft Windows SMBv1 Multiple Vulnerabilities	Windows	1	∅ ✓
HIGH	8.6	4.7	0.1426	Microsoft Windows SMB Server (2017-10) Multiple Vulnerabilities (unprivileged check)	Windows	1	∅ ✓
HIGH	8.1	9.8	0.9443	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETE...	Windows	1	∅ ✓

- **Microsoft Windows SMBv1 Multiple Vulnerabilities**
 - **Nível de Ameaça:** Critical (CVSS: 9.8, VPR: 6.7, EPSS: 0.2724, AI_basic_scan)
 - **Descrição:** O servidor SMBv1 apresenta múltiplas vulnerabilidades que permitem execução remota de código e divulgação de informações.
 - **Impacto:** Atacantes podem explorar essas falhas para executar código arbitrário ou acessar informações sensíveis.
 - **Solução:** Desabilitar o SMBv1 e aplicar as atualizações recomendadas pela Microsoft.
- **MS17-010: Security Update for Microsoft Windows SMB Server (ETERNALBLUE, WannaCry, etc.)**
 - **Nível de Ameaça:** High (CVSS: 8.1, VPR: 9.8, EPSS: 0.9443, AI_internal_scan e AI_basic_scan)
 - **Descrição:** Falta a atualização MS17-010, que corrige vulnerabilidades críticas no SMB Server, incluindo exploits como ETERNALBLUE e WannaCry.
 - **Impacto:** Permite execução remota de código e propagação de ransomware.
 - **Solução:** Aplicar o patch MS17-010.

- **Microsoft Windows SMB Server (2017-10) Multiple Vulnerabilities (uncredentialed check)**
 - **Nível de Ameaça:** High (CVSS: 8.6, VPR: 4.7, EPSS: 0.1426, AI_internal_scan)
 - **Descrição:** O servidor SMB apresenta vulnerabilidades adicionais identificadas em outubro de 2017, que podem permitir ataques remotos.
 - **Impacto:** Risco de exploração remota, incluindo negação de serviço ou acesso não autorizado.

Sistema Operativo (Windows)

Sev ▾	CVSS ▾	VPR ▾	EPSS ▾	Name ▾	Family ▾	Count ▾	⋮
□ CRITICAL	10.0	10.0	0.9358	Windows DNS Server RCE (CVE-2020-1350)	Windows : Microsoft Bulletins	1	ⓘ ⚙
□ CRITICAL	9.9	9.6	0.8314	KB4525236: Windows 10 Version 1607 and Windows Server 2016 November 2019 Security Up...	Windows : Microsoft Bulletins	1	ⓘ ⚙
□ CRITICAL	9.9	9.6	0.8039	KB4556813: Windows 10 Version 1607 and Windows Server 2016 May 2020 Security Update	Windows : Microsoft Bulletins	1	ⓘ ⚙
□ CRITICAL	9.9	8.9	0.589	KB4519998: Windows 10 Version 1607 and Windows Server 2016 October 2019 Security Update	Windows : Microsoft Bulletins	1	ⓘ ⚙
□ CRITICAL	9.8	9.8	0.922	KB5000803: Windows Security Update (March 2021)	Windows : Microsoft Bulletins	1	ⓘ ⚙
□ CRITICAL	9.8	9.6	0.9062	KB4471321: Windows 10 Version 1607 and Windows Server 2016 December 2018 Security Up...	Windows : Microsoft Bulletins	1	ⓘ ⚙
□ CRITICAL	9.8	9.6	0.8254	KB4457131: Windows 10 Version 1607 and Windows Server 2016 September 2018 Security U...	Windows : Microsoft Bulletins	1	ⓘ ⚙
□ CRITICAL	9.8	9.6	0.6405	KB4540670: Windows 10 Version 1607 and Windows Server 2016 March 2020 Security Update	Windows : Microsoft Bulletins	1	ⓘ ⚙
□ CRITICAL	9.8	9.2	0.6489	KB4494440: Windows 10 Version 1607 and Windows Server 2016 May 2019 Security Update (...)	Windows : Microsoft Bulletins	1	ⓘ ⚙
□ CRITICAL	9.8	9.0	0.9364	KB4022715: Windows 10 Version 1607 and Windows Server 2016 June 2017 Cumulative Update	Windows : Microsoft Bulletins	1	ⓘ ⚙
□ CRITICAL	9.8	8.9	0.837	KB4034658: Windows 10 Version 1607 and Windows Server 2016 August 2017 Cumulative Up...	Windows : Microsoft Bulletins	1	ⓘ ⚙

- **KB4519998: Windows 10 Version 1607 and Windows Server 2016 October 2019 Security Update**
 - **Nível de Ameaça:** Critical (CVSS: 9.9, VPR: 8.9, EPSS: 0.589, AI_internal_scan)
 - **Descrição:** Falta a atualização de segurança de outubro de 2019, que corrige vulnerabilidades críticas no Windows 10 Versão 1607 e Server 2016.
 - **Impacto:** Permite execução remota de código, escalonamento de privilégios e negação de serviço.
 - **Solução:** Aplicar o patch KB4519998.
- **KB4525236: Windows 10 Version 1607 and Windows Server 2016 November 2019 Security Update**
 - **Nível de Ameaça:** Critical (CVSS: 9.9, VPR: 9.6, EPSS: 0.8314, AI_internal_scan)

- **Descrição:** Falta a atualização de novembro de 2019, que corrige falhas críticas no Windows.
 - **Impacto:** Risco de exploração remota e comprometimento total do sistema.
 - **Solução:** Aplicar o patch KB4525236.
- **Windows DNS Server RCE (CVE-2020-1350)**
 - **Nível de Ameaça:** Critical (CVSS: 10.0, VPR: 10.0, EPSS: 0.9358, AI_internal_scan)
 - **Descrição:** Vulnerabilidade crítica no Windows DNS Server permite execução remota de código (CVE-2020-1350).
 - **Impacto:** Atacantes podem assumir o controle total do sistema.
 - **Solução:** Aplicar o patch correspondente.
- **KB4056890: Windows 10 Version 1607 and Windows Server 2016 January 2018 Security Update (Meltdown)(Spectre)**
 - **Nível de Ameaça:** High (CVSS: 8.8, VPR: 9.0, EPSS: 0.9417, AI_internal_scan)
 - **Descrição:** Falta a atualização de janeiro de 2018, que mitiga vulnerabilidades Meltdown e Spectre.
 - **Impacto:** Permite acesso a dados sensíveis via ataques de execução especulativa.
 - **Solução:** Aplicar o patch KB4056890.
- **Windows Speculative Execution Configuration Check**
 - **Nível de Ameaça:** Medium (CVSS: 6.5, VPR: 8.5, EPSS: 0.9417, AI_internal_scan)
 - **Descrição:** Configurações inadequadas para mitigar vulnerabilidades de execução especulativa (Spectre, Meltdown).
 - **Impacto:** Risco de vazamento de informações sensíveis.
 - **Solução:** Revisar e ajustar as configurações de mitigação no sistema.

<input type="checkbox"/>	MEDIUM	6.5	4.4	0.2763	Windows 10 / Windows Server 2016 September 2017 Information Disclosure Vulnerability (CVE-2017-8529)	Windows : Microsoft Bulletins	1	<input type="radio"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	MEDIUM	6.4	6.7	0.4674	Security Updates for Windows 10 / Windows Server 2016 (August 2018) (Spectre) (Meltdown) (Foreshadow)	Windows : Microsoft Bulletins	1	<input type="radio"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	MEDIUM	5.6	7.6	0.9066	Security Updates for Windows 10 / Windows Server 2016 (January 2019) (Spectre)	Windows : Microsoft Bulletins	1	<input type="radio"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	MEDIUM	5.6	7.6	0.9066	Security Updates for Windows 10 / Windows Server 2016 (September 2018) (Spectre)	Windows : Microsoft Bulletins	1	<input type="radio"/>	<input checked="" type="checkbox"/>

Browser (Google Chrome)

Sev	CVSS	VPR	EPSS	Name	Family	Count	Actions
Critical	9.8	7.4	0.0046	Google Chrome < 134.0.6998.117 Vulnerability	Windows	1	
Critical	9.8	7.4	0.0046	Google Chrome < 134.0.6998.118 Vulnerability	Windows	1	
Critical	9.8	7.4	0.0046	Google Chrome < 134.0.6998.89 Vulnerability	Windows	1	
Critical	9.8	6.7	0.0007	Google Chrome < 134.0.6998.35 Multiple Vulnerabilities	Windows	1	
High	8.8	9.2	0.0021	Google Chrome < 134.0.6998.88 Multiple Vulnerabilities	Windows	1	
High	8.3	10.0		Google Chrome < 134.0.6998.177 Vulnerability	Windows	1	

- **Google Chrome < 134.0.6998.117 Vulnerability**

- **Nível de Ameaça:** Critical (CVSS: 9.8, VPR: 7.4, EPSS: 0.0046, AI_internal_scan)
- **Descrição:** Vulnerabilidade crítica no Google Chrome anterior à versão 134.0.6998.117.
- **Impacto:** Permite execução remota de código.
- **Solução:** Atualizar o Google Chrome para a versão 134.0.6998.117 ou superior.

- **Google Chrome < 134.0.6998.88 Multiple Vulnerabilities**

- **Nível de Ameaça:** High (CVSS: 8.8, VPR: 9.2, EPSS: 0.0021, AI_internal_scan)
- **Descrição:** Múltiplas vulnerabilidades no Google Chrome anterior à versão 134.0.6998.88.
- **Impacto:** Risco de execução de código e negação de serviço.
- **Solução:** Atualizar o Google Chrome para a versão 134.0.6998.88 ou superior.

-

Outros (Wireshark)

Sev	CVSS	VPR	EPSS	Name	Family	Count	Actions
Critical	10.0			Wireshark / Ethereal Unsupported Version Detection	Misc.	1	
Critical	10.0			Wireshark S/EOL (2.0.x)	Misc.	1	
High	7.5	4.4	0.0643	Wireshark 2.0.x < 2.0.13 / 2.2.x < 2.2.7 Multiple DoS	Windows	1	
High	7.5	4.4	0.0281	Wireshark 2.0.x < 2.0.5 Multiple DoS	Windows	1	
High	7.5	4.4	0.0092	Wireshark 2.0.x < 2.0.4 Multiple DoS	Windows	1	
High	7.5	4.4	0.0022	Wireshark 2.0.x < 2.0.3 Multiple DoS	Windows	1	
High	7.5	2.6	0.0204	Wireshark 2.0.x < 2.0.12 / 2.2.x < 2.2.6 Multiple DoS	Misc/Windows	1	

- **Wireshark / Ethereal Unsupported Version Detection**

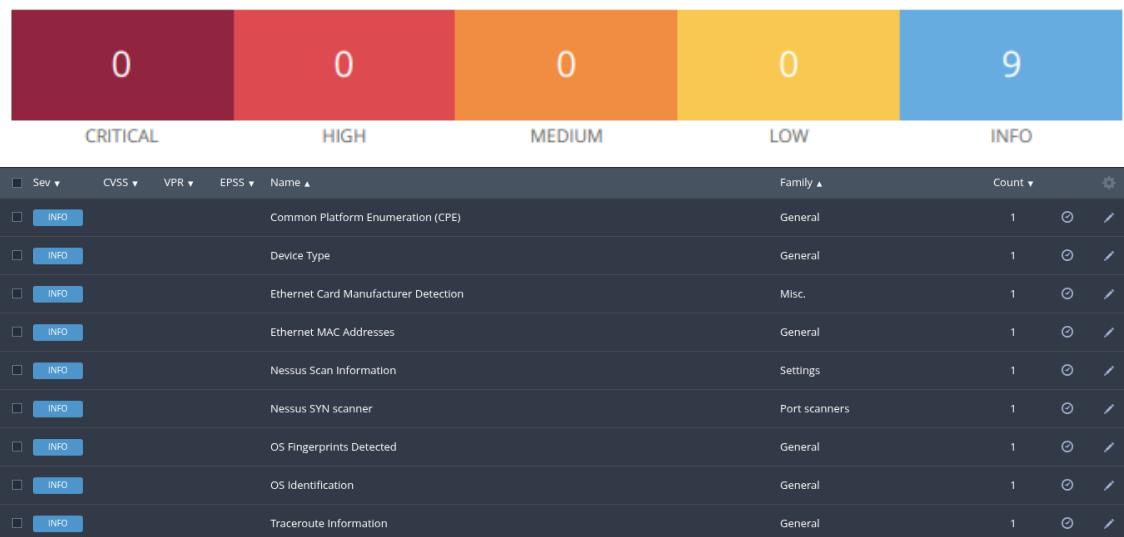
- **Nível de Ameaça:** Critical (CVSS: 10.0, AI_internal_scan)
- **Descrição:** Versão do Wireshark instalada não é mais suportada, contendo vulnerabilidades conhecidas.

- **Impacto:** Risco de exploração remota devido a falhas não corrigidas.
- **Solução:** Atualizar o Wireshark para uma versão suportada.
- **Wireshark 2.0.x<2.0.10/2.2.x<2.2.4 Multiple DoS**
 - **Nível de Ameaça:** High (CVSS: 7.5, VPR: 3.6, EPSS: 0.0074, AI_internal_scan)
 - **Descrição:** Versões do Wireshark 2.0.x anteriores a 2.0.10 e 2.2.x anteriores a 2.2.4 são vulneráveis a ataques de negação de serviço (DoS).
 - **Impacto:** Pode causar interrupção do serviço.
 - **Solução:** Atualizar o Wireshark para uma versão mais recente.

4.1.2 10.0.10.11 (Windows 10)

Não foram identificadas vulnerabilidades de severidade Critical, High ou Medium neste host. Apenas vulnerabilidades de severidade Info foram detectadas.

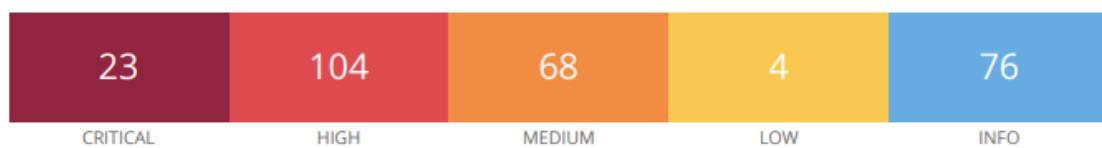
10.0.10.11



4.1.3 10.0.10.12 (Ubuntu Server)

Total Vulnerabilidades: 275

10.0.10.12



Sistema Operativo (Ubuntu)

Sev	CVSS	VPR	EPSS	Name	Family	Count	Actions	
Critical	10.0			Canonical Ubuntu Linux SEoL (18.04.x)	General	1		
Critical	9.8	9.0	0.2233	Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : rsync vulnerabilities (USN-6305-2)	Ubuntu Local Security Checks	1		
Critical	9.8	7.4	0.9274	Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : kilbC vulnerabilities (USN-6522-2)	Ubuntu Local Security Checks	1		
Critical	9.8	7.4	0.6071	Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : PHP vulnerabilities (USN-6305-2)	Ubuntu Local Security Checks	1		
Critical	9.8	7.4	0.0503	Ubuntu 18.04 ESM : FreeRDP vulnerabilities (USN-6522-2)	Ubuntu Local Security Checks	1		
Critical	9.8	7.4	0.0027	Ubuntu 18.04 LTS : Linux kernel vulnerabilities (USN-7003-2)	Ubuntu Local Security Checks	1		
Critical	9.8	7.2	0.935	Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : GNU C Library vulnerabilities (USN-6762-1)	Ubuntu Local Security Checks	1		
Critical	9.8	7.1	0.0631	Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : Python vulnerabilities (USN-6885-3)	Ubuntu Local Security Checks	1		
Critical	9.8	6.7	0.8139	Ubuntu 16.04 LTS / 18.04 LTS : Apache HTTP Server vulnerabilities (USN-6885-3)	Ubuntu Local Security Checks	1		

- **Canonical Ubuntu Linux SEoL (18.04.x)**
 - **Nível de Ameaça:** Critical (CVSS: 10.0, AI_internal_scan)
 - **Descrição:** O Ubuntu 18.04 LTS atingiu o fim de suporte (SEoL), não recebendo mais atualizações de segurança.
 - **Impacto:** Sistema exposto a vulnerabilidades conhecidas sem patches disponíveis.
 - **Solução:** Atualizar para uma versão suportada do Ubuntu (ex:Ubuntu 22.04 LTS).
- **Ubuntu 16.04 LTS / 18.04 LTS: Apache HTTP Server vulnerabilities (USN-6885-3)**
 - **Nível de Ameaça:** Critical (CVSS: 9.8, VPR: 6.7, EPSS: 0.8139, AI_internal_scan)
 - **Descrição:** Vulnerabilidades críticas no Apache HTTP Server em versões do Ubuntu 16.04 e 18.04 LTS.
 - **Impacto:** Permite execução remota de código ou negação de serviço.
 - **Solução:** Aplicar as atualizações de segurança (USN-6885-3).
- **Ubuntu 16.04 LTS / 18.04 LTS: PHP vulnerability (USN-7153-1)**
 - **Nível de Ameaça:** Critical (CVSS: 9.8, VPR: 6.7, EPSS: 0.0013, AI_internal_scan)
 - **Descrição:** Uma vulnerabilidade crítica no PHP pode permitir ataques remotos.
 - **Impacto:** Risco de execução remota de código.
 - **Solução:** Aplicar o patch USN-7153-1.

- **Ubuntu 18.04 LTS / 20.04 LTS: Linux kernel vulnerabilities (USN-7088-1)**

- **Nível de Ameaça:** High (CVSS: 8.8, VPR: 7.4, EPSS: 0.0237, AI_internal_scan)
- **Descrição:** Múltiplas vulnerabilidades no kernel Linux afetam o Ubuntu 18.04 e 20.04 LTS.
- **Impacto:** Pode permitir escalonamento de privilégios ou negação de serviço.
- **Solução:** Aplicar o patch USN-7088-1.

SSH (Secure Shell)

Sev ▾	CVSS ▾	VPR ▾	EPSS ▾	Name ▾	Family ▾	Count ▾	⚙
□ MEDIUM	6.8	6.1	0.5669	OpenSSH < 8.0	Misc.	1	ⓘ ⚡
□ MEDIUM	6.5	6.1	0.7957	OpenSSH < 9.6 Multiple Vulnerabilities	Misc.	1	ⓘ ⚡
□ MEDIUM	5.9	6.1	0.7957	SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)	Misc.	1	ⓘ ⚡
□ MEDIUM	5.3	4.9	0.9053	OpenSSH < 7.8	Misc.	1	ⓘ ⚡
□ INFO				OpenSSH Detection	Misc.	1	ⓘ ⚡

- **OpenSSH < 8.0**

- **Nível de Ameaça:** Medium (CVSS: 6.8, VPR: 6.1, EPSS: 0.5669, AI_basic_scan)
- **Descrição:** A versão do OpenSSH instalada é anterior à 8.0, contendo vulnerabilidades conhecidas.
- **Impacto:** Risco de exploração remota, como escalonamento de privilégios ou acesso não autorizado.
- **Solução:** Atualizar o OpenSSH para a versão 8.0 ou superior.

- **OpenSSH < 9.6 Multiple Vulnerabilities**

- **Nível de Ameaça:** Medium (CVSS: 6.5, VPR: 6.1, EPSS: 0.7957, AI_basic_scan)
- **Descrição:** Versões do OpenSSH anteriores à 9.6 apresentam múltiplas vulnerabilidades, incluindo falhas de segurança conhecidas.
- **Impacto:** Pode permitir ataques remotos ou comprometimento da integridade da conexão.
- **Solução:** Atualizar o OpenSSH para a versão 9.6 ou superior.

- **SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)**
 - **Nível de Ameaça:** Medium (CVSS: 5.9, VPR: 6.1, EPSS: 0.7957, AI_basic_scan)
 - **Descrição:** O servidor SSH é vulnerável ao ataque Terrapin, que explora falhas na implementação do protocolo SSH, permitindo manipulação de pacotes.
 - **Impacto:** Atacantes podem comprometer a integridade da conexão SSH, potencialmente downgradeando a segurança.
 - **Solução:** Atualizar o OpenSSH para uma versão que mitigue o ataque Terrapin (ex.: OpenSSH 9.6 ou superior).

Outros

<input type="checkbox"/>	LOW	2.1 *	2.9	0.0037	ICMP Timestamp Request Remote Date Disclosure	General	1	<input type="radio"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	INFO	SSH (Multiple Issues)	General	8	<input type="radio"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	INFO	SSH (Multiple Issues)	Misc.	4	<input type="radio"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	INFO	Apache HTTP Server (Multiple Issues)	Web Servers	3	<input type="radio"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	INFO	HTTP (Multiple Issues)	Web Servers	3	<input type="radio"/>	<input checked="" type="checkbox"/>

4.1.4 10.0.10.13 (Windows 7)

Não foram identificadas vulnerabilidades de severidade Critical, High ou Medium neste host. Apenas vulnerabilidades de severidade Info foram detectadas.

10.0.10.13



Sev ▾	CVSS ▾	VPR ▾	EPSS ▾	Name ▾	Family ▾	Count ▾	⚙	
<input type="checkbox"/>	INFO			Ethernet Card Manufacturer Detection	Misc.	1	<input type="radio"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	INFO			Ethernet MAC Addresses	General	1	<input type="radio"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	INFO			Nessus Scan Information	Settings	1	<input type="radio"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	INFO			Traceroute Information	General	1	<input type="radio"/>	<input checked="" type="checkbox"/>

4.2 OpenVAS

Aqui, listam-se as vulnerabilidades de severidade High e Medium identificadas pelo OpenVAS, organizadas por host e, dentro de cada host, por serviço. Lembrando que são resultados dos dois scans:

- **AI_Basic_Scan (29 minutos)**
- **AI_Internal_Scan (65 minutos)**

Task	Severity	High	Medium	Low	Log	False Pos.
AI_basic_scan	10.0 (High)	2	2	4	66	0
AI_scan	10.0 (High)	235	98	6	170	0

Host	High	Medium	Low	Log	False Positive
10.0.10.10 se06srv05.priv.fccn.pt	120	16	1	0	0
10.0.10.12 se06srv07.priv.fccn.pt	115	82	5	0	0
Total: 2	235	98	6	0	0

4.2.1 10.0.10.10 (Windows Server 2016)

Service (Port)	Threat Level
general/tcp	High
445/tcp	High
general/tcp	Medium
135/tcp	Medium
general/tcp	Low

SMB e Windows (Porta 445/tcp e general/tcp)

Microsoft Windows SMB Server Multiple Vulnerabilities (4013389)	8.8 (High)	80 %	10.0.10.10	se06srv05.priv.fccn.pt	general/tcp
Vulnerability					
Microsoft Windows Multiple Vulnerabilities (KB4487026)	9.8 (High)	80 %	10.0.10.10	se06srv05.priv.fccn.pt	general/tcp
Microsoft Windows Multiple Vulnerabilities (KB5010359)	7.8 (High)	80 %	10.0.10.10	se06srv05.priv.fccn.pt	general/tcp
Microsoft Defender Antimalware Platform Elevation of Privilege Vulnerability (Apr 2020)	7.8 (High)	80 %	10.0.10.10	se06srv05.priv.fccn.pt	general/tcp
Microsoft Windows Multiple Vulnerabilities (KB4480961)	8.8 (High)	80 %	10.0.10.10	se06srv05.priv.fccn.pt	general/tcp
Microsoft Windows Multiple Vulnerabilities (KB4577015)	8.8 (High)	80 %	10.0.10.10	se06srv05.priv.fccn.pt	general/tcp
Microsoft Windows Multiple Vulnerabilities (KB5009546)	9.8 (High)	80 %	10.0.10.10	se06srv05.priv.fccn.pt	general/tcp
Wireshark Multiple Denial of Service Vulnerabilities (May 2016) - Windows	5.5 (Medium)	97 %	10.0.10.10	se06srv05.priv.fccn.pt	general/tcp
Wireshark 'non-NUL DACL' Access Control Vulnerability - Windows	7.5 (High)	97 %	10.0.10.10	se06srv05.priv.fccn.pt	general/tcp
Microsoft Windows Multiple Vulnerabilities (KB4038712)	9.8 (High)	80 %	10.0.10.10	se06srv05.priv.fccn.pt	general/tcp
Microsoft Windows Multiple Vulnerabilities (KB4471321)	9.8 (High)	80 %	10.0.10.10	se06srv05.priv.fccn.pt	general/tcp
Microsoft Windows Multiple Vulnerabilities (KB4534271)	9.8 (High)	80 %	10.0.10.10	se06srv05.priv.fccn.pt	general/tcp
Microsoft Windows Multiple Vulnerabilities (KB4571694)	10.0 (High)	80 %	10.0.10.10	se06srv05.priv.fccn.pt	general/tcp
Microsoft Windows Multiple Vulnerabilities (KB5003197)	9.9 (High)	80 %	10.0.10.10	se06srv05.priv.fccn.pt	general/tcp

Wireshark e Chrome (general/tcp)

Wireshark CORBA IDL Dissector Denial of Service Vulnerability - Windows			97 %	10.0.10.10	se06srv05.priv.fccn.pt	general/tcp
Wireshark 'File_read_line' Function Denial of Service Vulnerability - Windows			97 %	10.0.10.10	se06srv05.priv.fccn.pt	general/tcp
Wireshark Multiple Denial of Service Vulnerabilities-02 (Aug 2016) - Windows			97 %	10.0.10.10	se06srv05.priv.fccn.pt	general/tcp
Wireshark Multiple Denial of Service Vulnerabilities-04 (Aug 2016) - Windows			97 %	10.0.10.10	se06srv05.priv.fccn.pt	general/tcp
Wireshark Multiple DoS Vulnerabilities-02 (Apr 2017) - Windows			97 %	10.0.10.10	se06srv05.priv.fccn.pt	general/tcp
Wireshark Security Updates (wnpa-sec-2017-44) - Windows			97 %	10.0.10.10	se06srv05.priv.fccn.pt	general/tcp
Google Chrome Security Update (stable-channel-update-for-desktop_19-2025-03) - Windows			97 %	10.0.10.10	se06srv05.priv.fccn.pt	general/tcp
TCP Timestamps Information Disclosure			80 %	10.0.10.10	se06srv05.priv.fccn.pt	general/tcp

Wireshark ASTERIX And DHCPv6 Dissector Multiple DoS Vulnerabilities - Windows			97 %	10.0.10.10	se06srv05.priv.fccn.pt	general/tcp
Wireshark Denial of Service Vulnerability - Windows			97 %	10.0.10.10	se06srv05.priv.fccn.pt	general/tcp
Wireshark Multiple Denial of Service Vulnerabilities-01 (Aug 2016) - Windows			97 %	10.0.10.10	se06srv05.priv.fccn.pt	general/tcp
Wireshark 'IrCOMM' And 'MSDP' Dissectors DoS Vulnerabilities - Windows			97 %	10.0.10.10	se06srv05.priv.fccn.pt	general/tcp
Wireshark Multiple Denial-of-Service Vulnerabilities-01 (Jun 2017) - Windows			97 %	10.0.10.10	se06srv05.priv.fccn.pt	general/tcp
Wireshark Multiple Denial of Service Vulnerabilities -02 (May 2016) - Windows			97 %	10.0.10.10	se06srv05.priv.fccn.pt	general/tcp
Wireshark Multiple Denial-of-Service Vulnerabilities-03 (Jun 2017) - Windows			97 %	10.0.10.10	se06srv05.priv.fccn.pt	general/tcp
Wireshark Multiple Denial of Service Vulnerabilities (Nov 2016) - Windows			97 %	10.0.10.10	se06srv05.priv.fccn.pt	general/tcp
Wireshark Multiple Denial of Service Vulnerabilities (Sep 2016) - Windows			97 %	10.0.10.10	se06srv05.priv.fccn.pt	general/tcp
Wireshark Multiple DoS Vulnerabilities (Jul 2017) - Windows			97 %	10.0.10.10	se06srv05.priv.fccn.pt	general/tcp
Wireshark Multiple DoS Vulnerabilities (Mar 2017) - Windows			97 %	10.0.10.10	se06srv05.priv.fccn.pt	general/tcp
Google Chrome Security Update (stable-channel-update-for-desktop_25-2025-03) - Windows			97 %	10.0.10.10	se06srv05.priv.fccn.pt	general/tcp
Google Chrome Security Update (stable-channel-update-for-desktop_10-2025-03) - Windows			97 %	10.0.10.10	se06srv05.priv.fccn.pt	general/tcp
Google Chrome Security Update (stable-channel-update-for-desktop-2025-03) - Windows			97 %	10.0.10.10	se06srv05.priv.fccn.pt	general/tcp
Google Chrome Security Update (stable-channel-update-for-desktop-2025-04) - Windows			97 %	10.0.10.10	se06srv05.priv.fccn.pt	general/tcp

4.2.2 10.0.10.12 (Ubuntu Server)

Service (Port)	Threat Level
package	High
5555/tcp	High
package	Medium
21/tcp	Medium
general/tcp	Medium
general/icmp	Low
package	Low
22/tcp	Low
general/tcp	Low

Ingreslock (Porta 5555/tcp)

Vulnerability	Severity	QoD ▾	Host IP	Name	Location	
Possible Backdoor: Ingreslock			99 %	10.0.10.12	se06srv07.priv.fccn.pt	5555/tcp

- **Possible Backdoor: Ingreslock:** Possível backdoor na porta 5555/tcp, indicando risco de acesso não autorizado (não detectado pelo Nessus).

Sistema Operativo (Pacotes)

Ubuntu: Security Advisory (USN-7153-1)		9.8 (High)	97 %	10.0.10.12	se06srv07.priv.fccn.pt	package
Ubuntu: Security Advisory (USN-7038-1)		5.5 (Medium)	97 %	10.0.10.12	se06srv07.priv.fccn.pt	package
Ubuntu: Security Advisory (USN-7070-1)		9.8 (High)	97 %	10.0.10.12	se06srv07.priv.fccn.pt	package
Ubuntu: Security Advisory (USN-6421-1)		7.5 (High)	97 %	10.0.10.12	se06srv07.priv.fccn.pt	package
Ubuntu: Security Advisory (USN-6164-2)		7.5 (High)	97 %	10.0.10.12	se06srv07.priv.fccn.pt	package
Ubuntu: Security Advisory (USN-6676-1)		5.5 (Medium)	97 %	10.0.10.12	se06srv07.priv.fccn.pt	package
Ubuntu: Security Advisory (USN-6541-1)		7.5 (High)	97 %	10.0.10.12	se06srv07.priv.fccn.pt	package
Ubuntu: Security Advisory (USN-6762-1)		9.8 (High)	97 %	10.0.10.12	se06srv07.priv.fccn.pt	package
Ubuntu: Security Advisory (USN-7259-1)		5.5 (Medium)	97 %	10.0.10.12	se06srv07.priv.fccn.pt	package
Ubuntu: Security Advisory (USN-7126-1)		5.5 (Medium)	97 %	10.0.10.12	se06srv07.priv.fccn.pt	package
Ubuntu: Security Advisory (USN-6958-1)		7.1 (High)	97 %	10.0.10.12	se06srv07.priv.fccn.pt	package
Ubuntu: Security Advisory (USN-6237-3)		5.5 (Medium)	97 %	10.0.10.12	se06srv07.priv.fccn.pt	package
Ubuntu: Security Advisory (USN-6429-2)		3.7 (Low)	97 %	10.0.10.12	se06srv07.priv.fccn.pt	package
Ubuntu: Security Advisory (USN-6641-1)		6.5 (Medium)	97 %	10.0.10.12	se06srv07.priv.fccn.pt	package
Ubuntu: Security Advisory (USN-6718-2)		5.0 (Medium)	97 %	10.0.10.12	se06srv07.priv.fccn.pt	package
Ubuntu: Security Advisory (USN-6944-2)		6.5 (Medium)	97 %	10.0.10.12	se06srv07.priv.fccn.pt	package
Ubuntu: Security Advisory (USN-6322-1)		6.5 (Medium)	97 %	10.0.10.12	se06srv07.priv.fccn.pt	package
Ubuntu: Security Advisory (USN-7000-1)		9.8 (High)	97 %	10.0.10.12	se06srv07.priv.fccn.pt	package
Ubuntu: Security Advisory (USN-7145-1)		5.0 (Medium)	97 %	10.0.10.12	se06srv07.priv.fccn.pt	package
Ubuntu: Security Advisory (USN-6360-2)		7.8 (High)	97 %	10.0.10.12	se06srv07.priv.fccn.pt	package
Ubuntu: Security Advisory (USN-6401-1)		9.8 (High)	97 %	10.0.10.12	se06srv07.priv.fccn.pt	package

Copyright © 2009-2

- **Ubuntu 18.04 LTS: End of Life (SEoL):** Sistema operacional sem suporte, não recebe mais atualizações de segurança.
- **Ubuntu: Security Advisory (USN-6522-2):** Vulnerabilidades em pacotes do Ubuntu, suscetíveis a ataques remotos.
- **Ubuntu: Security Advisory (USN-7206-1):** Falhas críticas em pacotes do sistema, permitindo exploração remota.
- **Ubuntu: Security Advisory (USN-6401-1):** Problemas de segurança em pacotes, comprometendo o sistema.
- **Ubuntu: Security Advisory (USN-6242-2):** Vulnerabilidades em pacotes, permitindo elevação de privilégios.

Outros

- **jQuery < 1.6.3 XSS Vulnerability:** Versão vulnerável do jQuery, suscetível a ataques de cross-site scripting (XSS).

jQuery < 1.6.3 XSS Vulnerability  4.3 (Medium) 80 % 10.0.10.12 se06srv07.priv.fccn.pt general/tcp

- **FTP Unencrypted Cleartext Login:** Login FTP sem criptografia, permitindo captura de credenciais (já detetado nas validações manuais feitas na seção anterior).

FTP Unencrypted Cleartext Login  4.8 (Medium) 70 % 10.0.10.12 se06srv07.priv.fccn.pt 21/tcp

- **Weak MAC Algorithms Supported (SSH):** Algoritmos MAC fracos no SSH, comprometendo a segurança da conexão.

Weak MAC Algorithm(s) Supported (SSH)  2.8 (Low) 80 % 10.0.10.12 se06srv07.priv.fccn.pt 22/tcp

- **Wireshark < 4.2.0 DoS Vulnerabilities:** Versão do Wireshark com falhas que permitem ataques de negação de serviço (DoS).

Wireshark < 4.2.0 DoS Vulnerabilities  6.8 (Medium) 97 % 10.0.10.12 se06srv07.priv.fccn.pt general/tcp

5 ANÁLISE DE IMPACTO E PROBABILIDADE

Esta seção avalia os riscos associados às vulnerabilidades identificadas na infraestrutura da SECURETECH, com base no impacto potencial e na probabilidade de exploração. O risco foi calculado combinando o **impacto** (gravidade do dano em caso de exploração, com base em CVSS e contexto) e a **probabilidade** (likelihood de exploração, considerando EPSS, VPR, exposição dos serviços e falta de segmentação de rede). A classificação de risco segue a escala: **Baixo, Médio, Alto e Crítico**.

5.1 Metodologia de Avaliação

A análise utiliza uma abordagem qualitativa, onde o risco é determinado por:

- **Impacto:** Avaliado com base na pontuação CVSS, criticidade do serviço afetado (ex: serviços críticos no Windows Server 2016) e potencial para perda de confidencialidade, integridade ou disponibilidade.
- **Probabilidade:** Estimada com base no EPSS (probabilidade de exploração nos próximos 30 dias), VPR (prioridade de vulnerabilidade), facilidade de exploração (ex: exploits públicos como EternalBlue) e exposição dos serviços (ex: portas abertas sem WAF).
- **Fatores Contextuais:** A ausência de segmentação de rede (rede 10.0.10.0/24 plana) e a falta de monitorização aumentam a probabilidade de propagação de ataques.

A tabela abaixo define os níveis de risco:

Impacto	Probabilidade	Risco
Alto	Alta	Crítico
Alto	Média	Alto
Médio	Alta	Alto
Médio	Média	Médio
Baixo	Baixa	Baixo

5.2 Agrupamento de Vulnerabilidades

Para simplificar a análise, as vulnerabilidades foram agrupadas em quatro categorias:

- Sistemas Operativos Desatualizados:** Inclui Ubuntu 18.04 (EoL), configurações vulneráveis a Meltdown/Spectre no Windows Server 2016 e potencial uso de Windows 7 (10.0.10.13).
- Serviços Inseguros:** Abrange FTP sem criptografia, SSH com algoritmos fracos, SMB vulnerável (MS17-010), Apache e PHP com falhas críticas, e uma backdoor super crítica na porta 5555.
- Software Desatualizado:** Inclui Google Chrome, Wireshark e jQuery com vulnerabilidades conhecidas.
- Configurações Inseguras:** Ausência de cabeçalhos de segurança HTTP, LDAP exposto e falta de WAF.

5.3 Análise por Host

5.3.1 10.0.10.10 (Windows Server 2016)

Categoría	Vulnerabilidades Principais	Impacto	Probabilidade	Risco
Sistemas Operativos	MS17-010 (EternalBlue), Meltdown/Spectre	Alto	Alta (EPSS: 0.97)	Crítico
Serviços Inseguros	SMB (MS17-010), LDAP exposto	Alto	Alta	Crítico
Software Desatualizado	Chrome (<134.0.6998.117), Wireshark (<4.2.0)	Alto	Média	Alto
Configurações Inseguras	Ausência de cabeçalhos HTTP, página IIS padrão	Médio	Alta	Alto

5.3.1.1 Justificativas

- MS17-010 (EternalBlue):** Vulnerabilidade crítica com exploits públicos amplamente usados. O impacto é alto devido ao potencial de controlo total do servidor, que hospeda serviços críticos. A probabilidade é alta (EPSS: 0.97) devido à exposição do SMB e à facilidade de exploração.

- **Meltdown/Spectre:** Permite acesso a dados sensíveis, comprometendo a confidencialidade. A probabilidade é alta devido à falta de patches.
- **Chrome/Wireshark:** Versões desatualizadas podem ser exploradas para execução de código remoto, mas a probabilidade é média, pois requer interação do utilizador (autenticado) ou tráfego malicioso.
- **Configurações Inseguras:** A exposição do LDAP e a página padrão do IIS aumentam o risco de ataques de enumeração e exploração web, especialmente numa rede sem segmentação.

Risco Global: Crítico, devido à combinação de vulnerabilidades de alto impacto e alta probabilidade, agravadas pela criticidade do servidor.

5.3.2 10.0.10.12 (Ubuntu 18.04 Server)

Categoría	Vulnerabilidades Principais	Impacto	Probabilidad	Risco
Backdoor	Backdoor porta 5555	Alto	Alta	Crítico
Sistemas Operativos	Ubuntu 18.04 EoL, kernel vulnerável (USN-7088-1)	Alto	Alta (EPSS: 0.81)	Crítico
Serviços Inseguros	Apache (USN-6885-3), PHP (USN-7153-1), FTP	Alto	Alta	Crítico
Software Desatualizado	jQuery (<1.6.3), Wireshark	Médio	Média	Médio
Configurações Inseguras	SSH (Terrapin, algoritmos fracos), sem cabeçalhos HTTP	Médio	Alta	Alto

5.3.2.1 Justificativas

- **Backdoor Porta 5555:** Esta vulnerabilidade super crítica permite acesso total ao sistema sem autenticação, possibilitando execução remota de código, roubo de dados ou instalação de malware. A probabilidade é alta

devido à exposição completa da porta 5555, frequentemente associada a backdoors conhecidas, e à facilidade de exploração com ferramentas públicas.

- **Ubuntu 18.04 EoL:** A falta de suporte deixa o sistema exposto a novas vulnerabilidades sem patches, com impacto alto devido ao armazenamento de dados sensíveis. A probabilidade é alta (EPSS: 0.81 para falhas conhecidas).
- **Apache/PHP/FTP:** Vulnerabilidades críticas permitem execução remota de código ou captura de credenciais. A probabilidade é alta devido à exposição pública dos serviços e exploits disponíveis.
- **jQuery/Wireshark:** Riscos de XSS e DoS, mas com impacto e probabilidade médios, pois dependem de cenários específicos (ex.: acesso a páginas web maliciosas).
- **SSH e Configurações:** O ataque Terrapin e algoritmos fracos no SSH aumentam o risco de comprometimento da integridade, com probabilidade alta devido à exposição do serviço.

Risco Global: Crítico, devido às vulnerabilidades críticas no sistema operativo e serviços, especialmente a backdoor na porta 5555, agravadas pela falta de segmentação.

5.3.3 10.0.10.11 (Windows 10) e 10.0.10.13 (Windows 7)

Categoria	Vulnerabilidades Principais	Impacto	Probabilidade	Risco
Sistemas Operativos	Nenhuma crítica identificada	Baixo	Baixa	Baixo
Serviços Inseguros	Nenhuma crítica identificada	Baixo	Baixa	Baixo
Software Desatualizado	Nenhuma crítica identificada	Baixo	Baixa	Baixo
Configurações Inseguras	Possível firewall ativo	Baixo	Baixa	Baixo

5.3.3.1 Justificativas

- Não foram identificadas vulnerabilidades críticas, altas ou médias, provavelmente devido a firewalls que bloqueiam portas ou à ausência de serviços expostos.
- No caso do **Windows 7 (10.0.10.13)**, o sistema operativo está desatualizado (EoL), mas a falta de portas abertas reduz a probabilidade de exploração remota.
- O **Windows 10 (10.0.10.11)** apresentou apenas uma porta aberta (7680/tcp, serviço desconhecido), com impacto e probabilidade baixos.

Risco Global: **Baixo**, mas com ressalva de que, pelos sistemas operativos, principalmente Windows 7, existem diversos riscos associados que conforme a exposição de portas podem revelar riscos críticos.

5.4 Resumo Geral

Os hosts **10.0.10.10 (Windows Server 2016)** e **10.0.10.12 (Ubuntu 18.04)** apresentam riscos **críticos** devido a vulnerabilidades de alto impacto e alta probabilidade, como MS17-010, Ubuntu EoL, falhas em serviços expostos (Apache, FTP) e, especialmente, a backdoor super crítica na porta 5555 do Ubuntu, que permite acesso total ao sistema. A ausência de segmentação de rede amplifica o risco, permitindo que um comprometimento inicial se propague rapidamente. Os hosts **10.0.10.11** e **10.0.10.13** apresentam risco **baixo** devido a falta de dados detalhados e exposição dessas máquinas.

6 PROPÓSTAS DE MITIGAÇÃO

Esta seção apresenta recomendações para mitigar os riscos identificados na infraestrutura da SECURETECH, abordando as vulnerabilidades críticas e altas nos hosts **10.0.10.10 (Windows Server 2016)** e **10.0.10.12 (Ubuntu 18.04)**, bem como potenciais riscos nos hosts **10.0.10.11** e **10.0.10.13**. As propostas estão organizadas por categorias (rede, sistemas operativos, serviços, software e configurações) para garantir uma abordagem abrangente e alinhada com as melhores práticas de cibersegurança e de tratamento de riscos.

6.1 Mitigações a nível da Rede

A ausência de segmentação na rede (10.0.10.0/24) amplifica o impacto de qualquer comprometimento. As seguintes medidas são recomendadas:

- **Segmentação de Rede:**
 - Implementar VLANs ou subnets para isolar servidores (Windows Server e Ubuntu Server) de estações de trabalho (clientes Windows 7 e 10), reduzindo o risco de propagação lateral de eventuais ataques.
 - Configurar regras de firewall para permitir apenas tráfego essencial entre segmentos.
- **Controlo de Acesso à Rede:**
 - Configurar firewalls nos hosts e no perímetro para bloquear portas desnecessárias.
 - Restringir o acesso remoto a serviços críticos (ex: RDP) a endereços IP autorizados via VPN.
- **Monitorização:**
 - Implementar um sistema de deteção e prevenção de intrusões (IDS/IPS) junto da firewall para identificar tentativas de exploração ou enumerações (para reconhecimento) do ambiente.
 - Configurar logging centralizado para monitorizar eventos de segurança em tempo real.

6.2 Mitigações para Sistemas Operativos Desatualizados

Os sistemas operativos desatualizados representam riscos críticos, especialmente no Ubuntu 18.04 e no Windows Server 2016. Recomenda-se:

- **10.0.10.10 (Windows Server 2016):**
 - Aplicar imediatamente o patch para **MS17-010 (EternalBlue)**, disponível no boletim de segurança KB4012212, para prevenir execução remota de código.
 - Instalar todas as atualizações de segurança propostas pelo suporte da Windows.
 - Verificar a conformidade com atualizações mensais da Microsoft para evitar novas vulnerabilidades e automatizar processo de atualização caso possível.
- **10.0.10.12 (Ubuntu 18.04):**
 - Migrar para uma versão suportada, como **Ubuntu 22.04 LTS**, para garantir atualizações de segurança contínuas.
 - Aplicar patches de kernel pendentes antes da migração, se necessário, para mitigar vulnerabilidades conhecidas.
- **10.0.10.13 (Windows 7):**
 - Substituir por um sistema operativo windows recente (Windows 11) devido ao fim de suporte em 2020.
 - Se a substituição não for imediata, isolar o host em uma VLAN restrita e garantir que são limitados os serviços expostos.

6.3 Mitigações para Serviços Inseguros

Os serviços vulneráveis, incluindo SMB, Apache, PHP, FTP e a backdoor na porta 5555, são alvos prioritários para atacantes. As medidas incluem:

- **10.0.10.10 (Windows Server 2016):**
 - **SMB (MS17-010):** Desativar o protocolo SMBv1 e garantir que apenas versões seguras (SMBv2/SMBv3) estão ativas. Configurar autenticação forte para acessos SMB.

- **LDAP:** Restringir o acesso ao serviço LDAP (porta 389) a clientes autorizados, implementar TLS para criptografia e desativar autenticação anónima.
- **10.0.10.12 (Ubuntu 18.04):**
 - **Apache e PHP:** Atualizar para as versões mais recentes (ex: Apache 2.4.62, PHP 8.2) para corrigir falhas críticas. Configurar o Apache com módulos de segurança (mod_security).
 - **FTP:** Substituir o FTP por **SFTP** (integrado ao OpenSSH) para garantir criptografia de dados e credenciais. Desativar o serviço FTP atual.
 - **Backdoor Porta 5555:** Fechar imediatamente a porta 5555 via firewall (ex: ufw deny 5555) e investigar o sistema para detetar malware ou rootkits. Reinstalar o sistema, se necessário, para garantir integridade.
 - **OpenSSH:** Atualizar para a versão mais recente (ex: OpenSSH 9.8) e desativar algoritmos fracos (sha1) no ficheiro de configuração. Configurar autenticação baseada em chaves com MFA.

6.4 Mitigações para Software Desatualizado

O software desatualizado aumenta o risco de exploração local e remota em alguns casos. Recomenda-se:

- **Google Chrome:**
 - Atualizar para a versão mais recente para corrigir vulnerabilidades.
 - Configurar atualizações automáticas para evitar atrasos.
- **Wireshark:**
 - Atualizar para a versão mais recente para mitigar falhas de parsing de pacotes.
 - Restringir o uso do Wireshark a contas administrativas com permissões mínimas.
- **jQuery (10.0.10.12):**
 - Atualizar para uma versão segura nas aplicações web hospedadas no Apache.

- Validar scripts de terceiros para evitar vulnerabilidades XSS adicionais.
- **Política de Atualizações:**
 - Implementar uma solução de gestão de patches para automatizar atualizações de software.

6.5 Mitigações para Configurações Inseguras

As configurações inadequadas expõem os sistemas a ataques evitáveis. As medidas incluem:

- **Cabeçalhos de Segurança HTTP:**
 - No **10.0.10.12 (Apache)**, configurar cabeçalhos como **HSTS**, **Content-Security-Policy (CSP)** e **X-Frame-Options** para mitigar XSS e clickjacking.
 - No **10.0.10.10 (IIS)**, implementar configurações equivalentes via ficheiro web.config.
- **LDAP (10.0.10.10):**
 - Configurar **LDAPS** (LDAP sobre TLS) e desativar ligações não criptografadas na porta 389.
 - Limitar consultas LDAP a utilizadores autenticados com permissões mínimas.
- **SSH (10.0.10.12):**
 - Mitigar o ataque **Terrapin** atualizando o OpenSSH e desativando algoritmos vulneráveis.
 - Configurar um banner de aviso e limitar logins SSH a chaves públicas.
- **Web Application Firewall (WAF):**
 - Implementar um WAF para proteger serviços web em ambos os servidores contra ataques como injeção SQL e XSS.
- **Página Padrão IIS (10.0.10.10):**
 - Substituir a página padrão do IIS por uma página personalizada ou desativar o site padrão para evitar enumeração.

6.6 Medidas Gerais de Segurança

Para reforçar a postura de segurança global da SECURETECH, recomenda-se:

- **Autenticação Multifator (MFA):**
 - Implementar MFA para serviços críticos, como SSH, RDP e aplicações web.
- **Auditorias Regulares:**
 - Realizar análises trimestrais com ferramentas como **Nessus**, **OpenVAS**, **Nuclei** e **OWASP ZAP** para identificar novas vulnerabilidades.
 - Executar testes de penetração anuais para validar a eficácia das mitigações.
- **Backup e Recuperação:**
 - Implementar backups regulares para os servidores com armazenamento offline.
 - Testar planos de recuperação de desastres para garantir continuidade em caso de comprometimento.

6.7 Priorização das Mitigações

As seguintes medidas devem ser implementadas com **prioridade imediata** devido ao risco crítico:

1. Fechar a **backdoor na porta 5555** (10.0.10.12) e investigar possíveis comprometimentos.
2. Aplicar o patch para **MS17-010** (10.0.10.10) para prevenir exploração do EternalBlue.
3. Migrar o **Ubuntu 18.04** (10.0.10.12) para uma versão suportada.
4. Desativar **SMBv1** e **FTP**, substituindo por protocolos seguros (SMBv3, SFTP).
5. Configurar **firewalls** para bloquear portas desnecessárias.

As demais recomendações podem ser implementadas em fases, dependendo dos recursos disponíveis.

6.8 Resumo das Mitigações

A tabela abaixo resume as principais ações por categoria:

Categoria	Ações Principais	Prioridade
Rede	Segmentação, firewall, IDS/IPS	Alta
Sistemas Operativos	Atualizar Ubuntu, patch MS17-010, substituir Win7	Crítica
Serviços Inseguros	Desativar SMBv1/FTP, fechar backdoor 5555, atualizar Apache/PHP/SSH	Crítica
Software Desatualizado	Atualizar Chrome, Wireshark, jQuery	Média
Configurações Inseguras	Cabeçalhos HTTP, LDAPS, WAF, SSH seguro	Alta
Geral	MFA, auditorias, backups	Média/Alta

7 RESPOSTAS ÀS QUESTÕES

Esta seção responde às cinco questões específicas levantadas no contexto da auditoria à infraestrutura da SECURETECH. As perguntas abordam práticas inadequadas que amplificam os riscos, propondo soluções práticas e alinhadas com as melhores práticas de cibersegurança.

7.1 Questão 1 - Uso de Múltiplas Plataformas de Armazenamento na Cloud

Durante a auditoria, foi identificado que os utilizadores utilizavam diferentes plataformas de armazenamento na cloud, como Dropbox, Google Drive e Mega, para partilhar ficheiros de trabalho, apesar de a política da empresa definir o OneDrive como a única solução oficial.

7.1.1 *Porque esta situação pode representar um risco de segurança para a empresa?*

- **Falta de Controlo:** O uso de serviços como Dropbox, Google Drive e Mega, fora da política oficial (OneDrive), impede que a empresa monitore ou proteja os dados adequadamente.
- **Riscos de Segurança:** Esses serviços podem não ter criptografia adequada ou podem ser alvos de ataques (phishing, data breach de credenciais).
- **Exfiltração de Dados:** Funcionários podem, intencionalmente ou não, compartilhar informações sensíveis em plataformas não seguras.

7.1.2 *Principais riscos de conformidade e proteção de dados*

- **Conformidade:** Violações de regulamentações como GDPR (UE), que exigem controlo rigoroso sobre armazenamento e processamento de dados.
- **Vazamento de dados:** Sem visibilidade, a SECURETECH não pode rastrear incidentes nem garantir a proteção de dados sensíveis, como informações de clientes.

7.1.3 Como limitar ou monitorizar sem prejudicar a produtividade?

- **Políticas claras:** Reforçar o uso exclusivo do OneDrive através de uma política formal, comunicada em sessões de formação trimestrais.
- **DLP (Data Loss Prevention):** Implementar ferramentas como Microsoft Defender for Cloud Apps para detetar e bloquear uploads para serviços não autorizados, preservando o acesso ao OneDrive.
- **Monitoramento:** Usar um proxy ou firewall para rastrear tráfego para serviços de cloud e alertar sobre violações.

7.2 Questão 2 - Uso de Dispositivos Pessoais

A auditoria revelou que os funcionários utilizavam dispositivos pessoais (portáteis e smartphones) para aceder ao email corporativo e a sistemas internos. Além disso, verificou-se que não havia qualquer política de segurança para esses dispositivos, e alguns armazenavam dados sensíveis localmente.

7.2.1 Riscos associados

- **Falta de Segurança:** Dispositivos pessoais podem não ter antivírus atualizado, atualizações ou criptografia, aumentando o risco de malware na rede e exposição de dados corporativos.
- **Perda ou Roubo:** Dados corporativos armazenados localmente podem ser comprometidos.
- **Malware:** Dispositivos infetados podem propagar ameaças, como ransomware, para outros hosts, aproveitando a ausência de segmentação.

7.2.2 Como permitir essa prática de forma segura?

- **Política BYOD:** Definir regras claras, exigindo sistemas atualizados, antivírus e criptografia.
- **Contêineres:** Usar aplicações com sandbox (ex: **Microsoft Outlook, Teams**) para separar dados corporativos de pessoais, protegendo informações sensíveis.

- **Acesso Restrito:** Limitar dispositivos pessoais a redes isoladas (ex: VLAN específica) e proibir acesso direto a servidores críticos (10.0.10.10, 10.0.10.12).

7.2.3 Soluções tecnológicas

- **VPN:** Exigir acesso via VPN com autenticação forte para garantir segurança fora da rede corporativa.
- **MFA (Autenticação Multifator):** Implementar MFA em todos os acessos com dispositivos pessoais, usando soluções como **Microsoft Authenticator**.
- **Criptografia:** Forçar criptografia de dados em trânsito (via TLS) e em repouso (via BitLocker por exemplo), mesmo em dispositivos pessoais.

7.3 Questão 3 - Uso de Aplicações de Mensagens Não Autorizadas

Durante a análise do tráfego de rede, verificou-se que funcionários estavam a utilizar aplicações de mensagens como WhatsApp, Telegram e Discord para partilhar informações internas da empresa. Algumas dessas aplicações não tinham controlo nem monitorização por parte da equipa de segurança da informação.

7.3.1 Por que é um risco?

- **Falta de Controlo:** Aplicações como WhatsApp ou Discord não são geridas pela TI, permitindo partilhas não monitorizadas que podem expor dados sensíveis.
- **Criptografia Limitada:** Mensagens podem ser interceptadas em redes comprometidas.
- **Uso Indevido:** Funcionários podem partilhar credenciais ou informações confidenciais sem intenção, facilitando ataques de engenharia social.

7.3.2 Medidas para comunicação segura

- **Plataforma Oficial:** Adotar **Microsoft Teams** ou **Slack**, com criptografia ponta-a-ponta, integração com MFA e logging para auditoria.

- **Bloqueio:** Configurar firewalls para restringir apps não autorizados na rede corporativa, permitindo exceções apenas com aprovação da TI.
- **Formação:** Realizar workshops semestrais para educar sobre riscos de apps pessoais e promover o uso de canais corporativos.

7.3.3 Equilíbrio entre controlo e flexibilidade

- Permitir o uso de apps como Telegram em emergências, mediante registo prévio no MDM e monitorização via DLP, garantindo flexibilidade sem comprometer a segurança.

7.4 Questão 4 - Sistemas Legados (WinServer 2016 e Windows 7)

Foi identificado que a empresa ainda possui servidores Windows Server 2016 e Windows 7 em produção. Esses sistemas operativos já não recebem atualizações de segurança e foram identificadas vulnerabilidades conhecidas nas máquinas.

7.4.1 Por que é um risco?

- **Vulnerabilidades Conhecidas:** O Windows Server 2016 (10.0.10.10) tem falhas críticas como **MS17-010 (EternalBlue)**, e o Windows 7 (10.0.10.13) está sem suporte (EoL), sendo alvos fáceis para exploits.
- **Falta de Suporte:** Ausência de patches para novas ameaças aumenta a exposição.
- **Impacto em Cadeia:** Um sistema comprometido pode servir de ponto de entrada para ataques laterais numa rede plana, afetando servidores críticos.

7.4.2 Estratégias de mitigação

- **Atualização:** Migrar o Windows Server 2016 para **Windows Server 2022** e o Windows 7 para **Windows 11**, garantindo suporte e patches regulares.
- **Isolamento:** Colocar sistemas legados numa VLAN restrita com acesso limitado usando firewalls para bloquear tráfego não essencial.

- **Controles Compensatórios:** Implementar IDS/IPS (ex: **Snort**) e monitorização com SIEM para detetar tentativas de exploração.

7.4.3 Quando é aceitável mantê-los?

- Apenas quando a migração é inviável a curto prazo causado por dependências de software legado incompatível. Nesse caso, reforçar com WAF, backups diários e honeypots para desviar atacantes, minimizando riscos até à substituição.

7.5 Questão 5 - Permissões Excessivas e Falta de MFA

A auditoria revelou que funcionários tinham permissões excessivas para aceder a sistemas internos, e que não havia um registo adequado de acessos. Além disso, identificou-se que nenhuma ação administrativa era autenticada com múltiplos fatores.

7.5.1 Riscos técnicos e humanos

- **Técnico:** Permissões excessivas permitem que contas comprometidas acedam a sistemas críticos.
- **Humano:** Colaboradores mal-intencionados ou descuidados podem abusar de privilégios para roubar dados ou causar danos, sem deteção imediata.
- **Sem MFA:** A ausência de autenticação multifator facilita acessos não autorizados, especialmente em serviços como SSH ou RDP.

7.5.2 Proteção contra ameaças internas

- **Princípio do Menor Privilégio:** Configurar contas com permissões mínimas (ex: remover utilizadores do grupo “Administradores” no Windows Server, limitar root no Ubuntu).
- **MFA:** Implementar autenticação multifator em todos os acessos administrativos, usando **Microsoft Authenticator** por exemplo.

- **Controlo de Acesso Baseado em Funções (RBAC):** Estruturar permissões por função no LDAP e Active Directory, garantindo que apenas utilizadores autorizados acedem a recursos sensíveis.

7.5.3 *Medidas de monitoramento*

- **Logs Centralizados:** Configurar logging detalhado (ex: **Syslog** no Ubuntu, **Event Viewer** no Windows) num SIEM para rastrear ações privilegiadas.
- **Auditorias Regulares:** Rever permissões trimestralmente com ferramentas como **PowerShell** ou **auditd**, desativando contas obsoletas.
- **Alertas em Tempo Real:** Usar SIEM para notificar acessos anómalos, como logins administrativos fora do horário.
- **Registo de Ações Administrativas:** Implementar soluções de PAM (Privileged Access Management, ex: **BeyondTrust**) para gravar sessões administrativas, facilitando investigações em caso de incidentes.

8 CONCLUSÕES

A auditoria à infraestrutura da SECURETECH expôs uma postura de segurança frágil, marcada por vulnerabilidades críticas nos hosts 10.0.10.10 (Windows Server 2016) e 10.0.10.12 (Ubuntu 18.04), como a exploração EternalBlue (MS17-010) e uma backdoor na porta 5555. Estas falhas, agravadas pela rede plana (10.0.10.0/24) e práticas inadequadas — como uso de múltiplas plataformas de armazenamento na cloud, uso descontrolado de dispositivos pessoais, mensagens inseguras, sistemas legados e permissões excessivas —, criam um ambiente propenso a ataques devastadores, como roubo de dados ou interrupção de serviços.

As recomendações propostas, incluindo segmentação de rede, atualização de sistemas, implementação de MFA, RBAC, DLP e plataformas corporativas (como OneDrive, Teams), oferecem um caminho robusto para mitigar esses riscos. A priorização de ações críticas, como fechar a backdoor 5555 e corrigir o MS17-010, é essencial para proteção imediata, enquanto medidas a médio prazo, como auditorias regulares e formação contínua, fortalecerão a resiliência a longo prazo.

A principal lição é a necessidade de uma abordagem proativa à cibersegurança, com políticas claras, tecnologias modernas e sensibilização dos colaboradores. A SECURETECH deve investir em monitorização contínua e testes periódicos para evitar a recorrência de falhas. A adoção destas práticas não só protegerá os ativos da empresa, mas também assegurará conformidade com regulamentos como o RGPD, preservando a confiança dos clientes e a reputação no mercado.

REFERÊNCIAS BIBLIOGRAFICAS

- [1] Tenable, “Nessus: Vulnerability Scanner,” Tenable Network Security. [Online]. Disponível em: <https://www.tenable.com/products/nessus> .
- [2] Greenbone, “OpenVAS: Open Vulnerability Assessment Scanner,” Greenbone Networks. [Online]. Disponível em: <https://www.openvas.org> .
- [3] ProjectDiscovery, “Nuclei: Fast and Customizable Vulnerability Scanner,” ProjectDiscovery. [Online]. Disponível em: <https://nuclei.projectdiscovery.io> .
- [4] Wireshark, “Wireshark: Network Protocol Analyzer,” Wireshark Foundation. [Online]. Disponível em: <https://www.wireshark.org> .
- [5] EnableSecurity, “Wafw00f: Web Application Firewall Fingerprinting Tool,” EnableSecurity. [Online]. Disponível em <https://github.com/EnableSecurity/wafw00f> :
- [6] Netcat, “Ncat: Network Connectivity Tool,” Nmap Project. [Online]. Disponível em: <https://nmap.org/ncat> .