



Universidade do Minho
Escola de Engenharia

Universidade do Minho
Escola de Engenharia
Mestrado em Engenharia Informática

Unidade Curricular de Tecnologias de Segurança

Ano Letivo de 2024/2025

Trabalho Prático 2 - Grupo 6

Martim Redondo
PG55929

João Rodrigues
PG57879

Benjamim Rodrigues
PG57511

Março, 2025

Índice

1. Parte A	1
1.1. Introdução e Metodologia	1
1.2. NOS (Grande Corporação)	1
1.3. A Padaria Portuguesa (Negócio Local)	2
1.4. Comparação e Análise Crítica	4
1.5. Riscos e Propostas	4
1.5.1. NOS (Grande corporação)	4
1.5.2. A Padaria Portuguesa (Negócio local)	5
1.6. Conclusão	5
1.7. Capturas de Ecrã Relativas ao Processo	6
2. Parte B	10
2.1. B1	10
2.2. B2	10
2.2.1. B2.1	11
2.2.2. B2.2	13
2.3. B3	15
2.4. B4	16
2.5. B5	18
2.6. B6	19
2.7. B7	21
2.7.1. B7.1	21
2.7.2. B7.2	21

Lista de Figuras

Figura 1 Ferramentas de Desenvolvimento (F12 no browser)	6
Figura 2 Censys	7
Figura 3 Censys	7
Figura 4 Censys	8
Figura 5 SecurityHeaders	8
Figura 6 Netcraft	8
Figura 7 Netcraft	9
Figura 8 Captura do tráfego gerado pelo protocolo Telnet	10
Figura 9 Output nmap -sV	11
Figura 10 Output nmap -sV -p 80	12
Figura 11 Output nmap -sV --script vulners	12
Figura 12 Output nmap -A	13
Figura 13 Notificações do NIDS relativamente a nmap -sV	14
Figura 14 Notificações do NIDS relativamente a nmap -sV -p 80	14

Figura 15	Notificações do NIDS relativamente a nmap -sV -script vulners .	
14		
Figura 16	Notificações do NIDS relativamente a nmap -A	14
Figura 17	Output nmap -sV após configuração das iptables	16
Figura 18	Output nmap -sV -p 80 após configuração das iptables	16
Figura 19	Output nmap -sV –script vulners após configuração das iptables	17
Figura 20	Output nmap -A após configuração das iptables	17
Figura 21	Output nmap -Pn -sA	18
Figura 22	Output nmap -Pn -sF	18
Figura 23	Output nmap -Pn -sN	19
Figura 24	Output nmap -Pn -sX	19
Figura 25	Output nmap -Pn -sU -p 513,6000	19
Figura 26	Resultados do Nikto	20
Figura 27	Tráfego causado pela varredura	20

Lista de Tabelas

Tabela 1	Comparação entre NOS e A Padaria Portuguesa	4
-----------------	---	---

1. Parte A

Selecione duas empresas que realizam suas operações comerciais por meio de serviços online - uma grande corporação e um negócio local — e aplique técnicas de coleta passiva (i.e., de domínio público) de informações para descobrir detalhes sobre seus sistemas e infraestrutura. Relate as estratégias utilizadas, os resultados encontrados e as possíveis diferenças na forma como os administradores desses domínios gerenciam sua segurança e exposição. Por fim, apresente uma análise crítica sobre os riscos relacionados às práticas observadas.

1.1. Introdução e Metodologia

Foram analisadas duas empresas com perfis distintos: a **NOS** (grande corporação do setor das telecomunicações) e **A Padaria Portuguesa** (negócio local com presença digital). O objetivo foi avaliar a sua exposição e postura de segurança online através de técnicas de recolha passiva, utilizando apenas fontes públicas, respeitando sempre os limites éticos e legais.

Foram utilizadas várias ferramentas para esta análise:

- **Ferramentas do navegador (F12)**: para inspecionar cabeçalhos HTTP, cookies, redirecionamentos e comportamentos visíveis do lado do cliente.
- **Shodan e Censys**: para identificar serviços expostos à internet, certificados, portas abertas e detalhes da infraestrutura.
- **SecurityHeaders**: para avaliar a presença e configuração de cabeçalhos de segurança nos websites.
- **Netcraft**: para recolher informações sobre tecnologias utilizadas, alojamento, sistemas operativos e serviços externos.
- **Pesquisa web**: para confirmar dados técnicos ou obter contexto adicional sobre a infraestrutura de cada empresa.

A abordagem foi exclusivamente passiva e não intrusiva, simulando o que seria acessível a qualquer utilizador comum ou potencial atacante, sem interferir com os sistemas analisados.

1.2. NOS (Grande Corporação)

A NOS, enquanto uma das maiores operadoras de telecomunicações em Portugal, apresenta uma infraestrutura digital robusta e bem protegida. Através da análise passiva de fontes públicas (Shodan, Censys, SecurityHeaders, Netcraft), foi possível identificar várias boas práticas de segurança implementadas no seu domínio principal.

- **Infraestrutura protegida por Cloudflare (CDN)**, ocultando o servidor de origem e oferecendo proteção contra DDoS e outras ameaças. Esta escolha também melhora a performance global do website.

- **Redirecionamento forçado de HTTP para HTTPS**, com uso de certificados válidos e atualizados (SHA-256), emitidos por entidades confiáveis como a Google Trust Services.
- **Presença do cabeçalho HSTS** (Strict-Transport-Security), que obriga os navegadores a manterem comunicações seguras, mitigando riscos de downgrade attacks e man-in-the-middle.
- **Implementação de múltiplos cabeçalhos de segurança**, incluindo Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy e outros, reduzindo exposição a ataques como XSS, clickjacking e MIME sniffing.
- **Utilização de Web Application Firewall (WAF)**, presumivelmente integrado via Cloudflare, como defesa adicional contra exploração de vulnerabilidades em aplicações web.
- **Cookies analisados apresentam algumas flags ausentes** (Secure, HttpOnly), o que pode representar um risco em cenários específicos, nomeadamente se combinados com outras falhas de segurança.
- **Tecnologias utilizadas** não são totalmente visíveis, mas confirma-se o uso da Cloudflare e a ausência de dados sobre o servidor web e frameworks back-end, possivelmente ocultados por design.
- **Registros Whois** parcialmente ofuscados, o que é comum em grandes empresas, mas reduz a transparência para auditorias externas.
- **Sem confirmação pública de participação em programas de bug bounty**, como HackerOne ou Bugcrowd, o que poderia melhorar a colaboração com a comunidade de cibersegurança.

Em suma, a NOS revela uma postura proativa e estratégica em termos de segurança digital, com várias camadas de proteção bem implementadas. No entanto, há espaço para melhorias em aspectos como a transparência dos registos e o fortalecimento da política de cookies.

1.3. A Padaria Portuguesa (Negócio Local)

Apesar de se tratar de uma PME não tecnológica, A Padaria Portuguesa revela algumas preocupações com a segurança da sua presença online, nomeadamente no seu website oficial. A análise passiva, feita com ferramentas como Shodan, Censys, Neteck e SecurityHeaders, permitiu obter uma visão geral da sua infraestrutura e postura digital.

- **Alojamento nacional**: O domínio principal (www.apadariaportuguesa.pt) está alojado em servidores da empresa portuguesa PTisp (AlmourolTec), geridos pela team.blue. Este alojamento, de pequena escala, é compatível com o perfil da empresa e assegura proximidade geográfica e legal.
- **Proteção de DNS via Cloudflare**: Embora o site não esteja diretamente atrás da CDN da Cloudflare a nível de tráfego HTTP, utiliza os serviços DNS da mesma, o que garante alguma resiliência contra ataques como DDoS e aproveita funcionalidades de performance e segurança como o DNSSEC, que está ativo.

- **Certificado SSL/TLS válido:** O site utiliza um certificado emitido pela GlobalSign, garantindo comunicações cifradas quando acedido por HTTPS. No entanto, não força redirecionamento de HTTP para HTTPS, o que pode deixar os utilizadores expostos em acessos manuais ou através de links inseguros.
- **Implementação de cabeçalhos de segurança:** Foram detetados headers como Content-Security-Policy, X-Frame-Options e X-Content-Type-Options. A presença destes cabeçalhos revela uma adoção mínima de boas práticas de segurança, suficientes para prevenir ataques como clickjacking, MIME sniffing e alguns vetores de XSS.
- **Tecnologias utilizadas:** No backend, a aplicação recorre a PHP. No frontend, usa tecnologias comuns como jQuery, Google Tag Manager e JavaScript, adequadas a uma estrutura simples e funcional. Não foi identificada qualquer framework ou CMS específico (como WordPress), embora não se possa excluir a sua utilização sem análise interna.
- **Gestão externa da infraestrutura:** A empresa delega a infraestrutura técnica a prestadores especializados, prática comum entre empresas não tecnológicas. A gestão do DNS pela Cloudflare e o alojamento pela PTisp indicam uma estratégia consciente de dependência de soluções externas fiáveis.
- **Privacidade e registos de domínio:** O WHOIS do domínio não revela informação pessoal identificável sobre o proprietário, o que reduz o risco de ataques de engenharia social por essa via, mas também limita a transparência do ponto de vista de auditoria.
- **Ausência de políticas públicas de segurança:** Não foram encontradas informações sobre gestão de incidentes, políticas de privacidade visíveis ou programas de bug bounty. Esta falta de documentação ou comunicação pública de práticas de segurança é comum em negócios locais, mas representa uma oportunidade de melhoria.
- **Mecanismos de defesa não visíveis:** Não há evidências claras da utilização de firewalls de aplicação web (WAF) ou mecanismos anti-bot ativos. No entanto, algumas proteções básicas poderão estar disponíveis via Cloudflare, ainda que não tenham sido observáveis diretamente.

Em suma, A Padaria Portuguesa demonstra um nível básico, mas funcional, de segurança digital. Embora não disponha de medidas avançadas nem de transparência nas suas políticas, recorre a fornecedores sólidos e implementa práticas adequadas ao seu contexto.

1.4. Comparação e Análise Crítica

Critério	NOS (grande corporação)	Padaria Portuguesa (negócio local)
Exposição Digital	Elevada: múltiplos domínios, APIs e serviços empresariais complexos	Moderada: website com funcionalidades básicas
Controlo de Infraestrutura	Interno: equipas técnicas próprias, integração com CDN e WAF	Subcontratado: alojamento e DNS geridos por fornecedores externos
Tecnologias Expostas	Soluções empresariais modernas, segmentadas e protegidas por CDN (Cloudflare)	Backend simples em PHP, frontend com jQuery e Google Tag Manager
Certificados e Encriptação	Certificados atualizados, encriptação forte (SHA-256), HTTPS forçado com HSTS	Certificado SSL válido, mas sem redirecionamento automático para HTTPS
Cabeçalhos de Segurança	Implementação completa e atualizada (CSP, HSTS, XFO, etc.)	Implementação básica, mas com presença de CSP, XFO e X-Content-Type-Options
Políticas Públicas de Segurança	Parcialmente acessíveis, mas sem transparência total (e.g., não há bug bounty conhecido)	Inexistentes ou não divulgadas publicamente
Gestão de Vulnerabilidades	Proativa: boas práticas evidenciadas, mas sem confirmação de programas formais de bug bounty	Reativa: ausência de medidas visíveis ou políticas formais

Tabela 1: Comparação entre NOS e A Padaria Portuguesa

1.5. Riscos e Propostas

A seguir apresenta-se uma análise crítica dos principais riscos de segurança observados para cada entidade avaliada, bem como propostas específicas de mitigação adaptadas à sua realidade.

1.5.1. NOS (Grande corporação)

Principais riscos:

- Alvo atrativo para campanhas de cibercrime avançadas (e.g., APTs, ransomware, exploração de APIs críticas).
- Complexidade elevada da infraestrutura pode originar pontos cegos difíceis de monitorizar.
- Falta de visibilidade sobre práticas colaborativas com a comunidade de segurança (ex: bug bounty).

Fragilidades observadas:

- Cookies identificados sem a flag **Secure**, o que pode representar um risco em contextos não cifrados.
- Ausência de políticas públicas detalhadas sobre resposta a vulnerabilidades.

Propostas de mitigação:

- **Aumentar a transparéncia:** Publicação de políticas claras de disclosure de vulnerabilidades, mesmo sem programa de recompensa.
- **Implementar threat hunting:** Monitorização proativa de comportamentos suspeitos, com integração de ferramentas SIEM.
- **Reforçar segmentação:** Adoção de estratégias de micro-segmentação para limitar movimentos laterais em caso de intrusão.
- **Auditorias regulares:** Reforçar ciclos de auditoria técnica (interna e externa), incluindo análise de headers, cookies e configurações HTTPS.
- **Formação contínua:** Investir em campanhas regulares de sensibilização para todos os colaboradores, incluindo áreas não técnicas.

1.5.2. A Padaria Portuguesa (Negócio local)

Principais riscos:

- Vulnerabilidade a ataques automatizados e scan genérico da internet.
- Exploração potencial de falhas em CMS ou headers de segurança mal configurados.
- Phishing e engenharia social facilitados por ausência de políticas visíveis e boas práticas digitais.

Fragilidades observadas:

- Falta de redirecionamento forçado de HTTP para HTTPS, o que pode comprometer a confidencialidade inicial da ligação.
- Gestão técnica entregue a terceiros, sem garantias públicas de segurança ou de atualizações regulares.
- Inexistência de políticas de privacidade ou segurança publicadas no site.

Propostas de mitigação:

- **Redirecionamento HTTPS obrigatório:** Configurar o servidor (ou Cloudflare) para forçar ligação cifrada com HSTS.
- **Aproveitar ferramentas acessíveis:** Configurar regras de proteção (WAF básico) via Cloudflare gratuito.
- **Atualizações regulares:** Verificar e manter atualizados todos os componentes (ex: CMS, plugins, bibliotecas JS).
- **Documentar práticas mínimas:** Publicar uma política simples de privacidade e segurança, alinhada com as obrigações do RGPD.
- **Capacitação interna:** Formação básica em cibersegurança para quem gera o site e canais digitais.

1.6. Conclusão

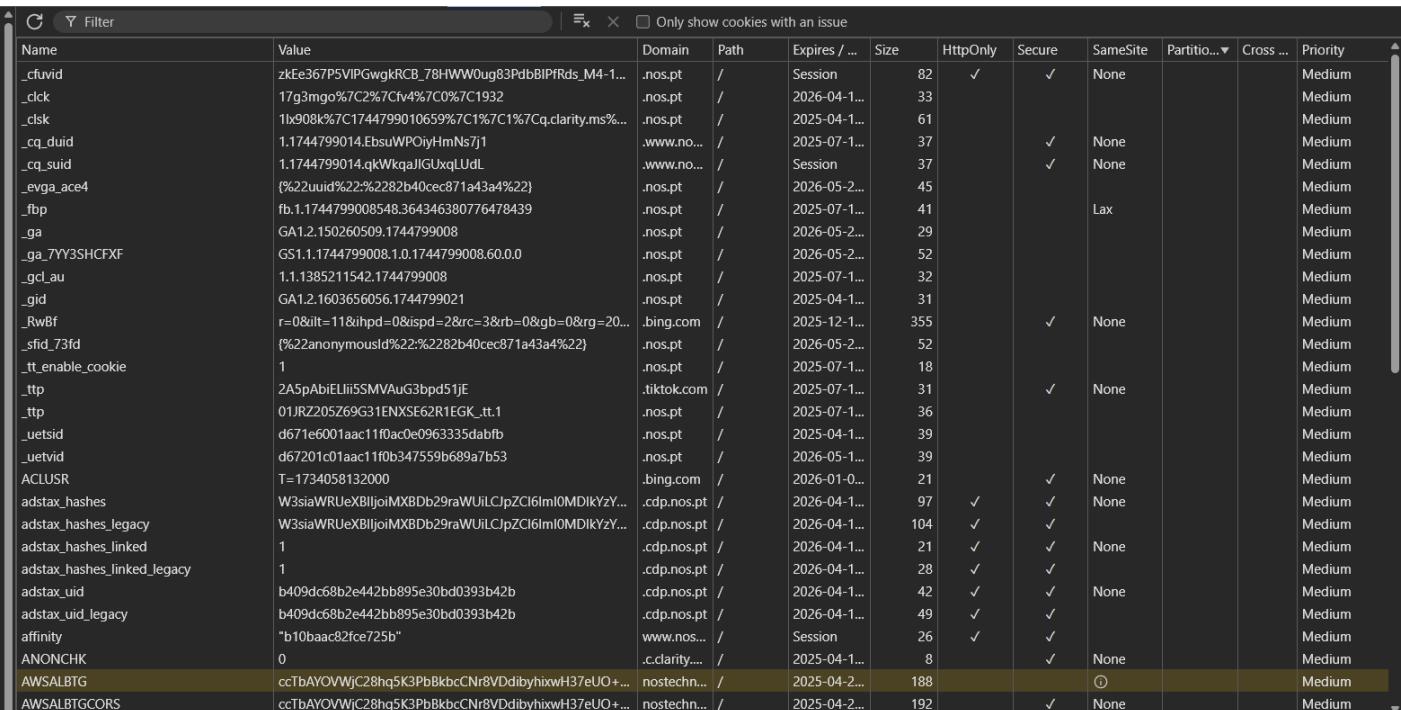
A análise realizada revela que, na cibersegurança, o fator determinante não é exclusivamente o tamanho da organização, mas sim a maturidade e a abordagem proativa adotada para mitigar riscos. A NOS, com a sua infraestrutura robusta e recursos técnicos

avançados, demonstra uma base sólida em segurança, mas ainda apresenta oportunidades de melhoria, principalmente na transparência e no maior envolvimento com a comunidade de segurança.

Por outro lado, a Padaria Portuguesa, embora com menos recursos, tem um grande potencial para reforçar a sua postura de segurança com medidas simples e de baixo custo, bastando para isso cultivar uma cultura de segurança digital que permeie toda a gestão e operação. Adotar práticas mínimas, como a implementação de HTTPS forçado, já traria benefícios significativos, revelando que, na cibersegurança, a conscientização e a proatividade podem superar limitações de recursos.

1.7. Capturas de Ecrã Relativas ao Processo

Por uma questão de brevidade, serão apresentadas apenas as evidências correspondentes ao processo seguido para a grande corporação (NOS). No entanto, é importante destacar que o processo foi semelhante para o negócio local.



The screenshot shows the developer tools interface with several tabs open. On the left, the 'Application' tab is selected, displaying a tree view of storage types: Manifest, Service workers, Storage, Local storage, Session storage, Extension storage, IndexedDB, and Cookies. Under Cookies, there are entries for various domains including nos.pt, bing.com, tiktok.com, and www.nos.pt. Each entry shows details like name, value, domain, path, expiration date, size, and security settings. A 'Priority' column on the right indicates the risk level for each cookie. Other tabs visible include Network, Timeline, Elements, and Sources.

Application	Name	Value	Domain	Path	Expires / ...	Size	HttpOnly	Secure	SameSite	Partition	Cross ...	Priority
Manifest	_ctivid	zkEe367P5VlPGwgkRCB_78HWW0ug83PdbBIPfRds.M4-1...	.nos.pt	/	Session	82	✓	✓	None			Medium
Service workers	_clk	17g3mgo%7C2%7Cf4%7C0%7C1932	.nos.pt	/	2026-04-1...	33						Medium
Storage	_clsk	1b908lk67C1744799010659%7C1%7C1%7Cq.clarity.ms%...	.nos.pt	/	2025-04-1...	61						Medium
Local storage	_cq_duid	1.1744799014.EbsuWPOiyHmNs7j1	www.no...	/	2025-07-1...	37	✓	✓	None			Medium
Session storage	_cq_suid	1.1744799014.qkWkqajGLlxqlUdl	www.no...	/	Session	37	✓	✓	None			Medium
Extension storage	_evga_ace4	(%22uuiid%22%2282b40cec871a43a4%22)	.nos.pt	/	2026-05-2...	45						Medium
IndexedDB	_fbp	fb.1.1744799008548.364346380776478439	.nos.pt	/	2025-07-1...	41				Lax		Medium
Cookies	_ga	GA1.2.150260509.1744799008	.nos.pt	/	2026-05-2...	29						Medium
	_ga_7YY3SHCFXF	GS1.1.1744799008.1.0.1744799008.60.0.0	.nos.pt	/	2026-05-2...	52						Medium
	_gcl_au	1.1.1385211542.1744799008	.nos.pt	/	2025-07-1...	32						Medium
	_gid	GA1.2.1603656056.1744799021	.nos.pt	/	2025-04-1...	31						Medium
	_RwBf	r=0&ilt=11&ihp=0&ispd=2&rcc=3&rb=0&gb=0&rg=20...	bing.com	/	2025-12-1...	355	✓	✓	None			Medium
	_sfid_73fd	(%22anonymousId%22%2282b40cec871a43a4%22)	.nos.pt	/	2026-05-2...	52						Medium
	_tt_enable_cookie	1	.nos.pt	/	2025-07-1...	18						Medium
	_ttip	2A5pAbiELii5SMVAuG3bpdi51je	tiktok.com	/	2025-07-1...	31	✓	✓	None			Medium
	utpp	01JRZ205269G31ENXS662R1EGK.tt1	.nos.pt	/	2025-07-1...	36						Medium
	_utsid	d671e6001aac11f0ac0e0963335dabfb	.nos.pt	/	2025-04-1...	39						Medium
	_uetvid	d67201c01aac11fb347559b689a7b53	.nos.pt	/	2026-05-1...	39						Medium
	ACLUSR	T=1734058132000	.bing.com	/	2026-01-0...	21		✓	None			Medium
	adstax_hashes	W3siaWRUeXBljoiMXDb29raWUiLCJpZCI6ImI0MDIKY2...	.cdp.nos.pt	/	2026-04-1...	97	✓	✓	None			Medium
	adstax_hashes_legacy	W3siaWRUeXBljoiMXDb29raWUiLCJpZCI6ImI0MDIKY2...	.cdp.nos.pt	/	2026-04-1...	104	✓	✓				Medium
	adstax_hashes_linked	1	.cdp.nos.pt	/	2026-04-1...	21	✓	✓	None			Medium
	adstax_hashes_linked_legacy	1	.cdp.nos.pt	/	2026-04-1...	28	✓	✓				Medium
	adstax_uid	b409dc68b2e442bb895e30bd0393b42b	.cdp.nos.pt	/	2026-04-1...	42	✓	✓	✓			Medium
	adstax_uid_legacy	b409dc68b2e442bb895e30bd0393b42b	.cdp.nos.pt	/	2026-04-1...	49	✓	✓				Medium
	affinity	"b10baac82fce725b"	www.nos...	/	Session	26	✓	✓				Medium
	ANONCHK	0	.clarity...	/	2025-04-1...	8	✓	✓	None			Medium
	AWSLBTG	ccTbAYOVWjC28hq5K3PbBkbCNr8VDDibyhxwH37eUO+...	nostechn...	/	2025-04-2...	188				ⓘ		Medium
	AWSALBTG CORS	ccTbAYOVWjC28hq5K3PbBkbCNr8VDDibyhxwH37eUO+...	nostechn...	/	2025-04-2...	192	✓	✓	None			Medium

Figura 1: Ferramentas de Desenvolvimento (F12 no browser)

Figura 2: Censys

Figura 3: Censys

```

SSL Certificate

Certificate:
Data:
    Version: 3 (0x2)
    Serial Number:
        83:e1:8c:2a:fa:bf:e6:bc
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=US, ST=Arizona, L=Scottsdale, O=GoDaddy.com, Inc., OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2
    Validity
        Not Before: Apr 1 16:06:46 2025 GMT
        Not After : Apr 1 16:06:46 2026 GMT
    Subject: CN=*.nos.pt
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
        Public-Key: (2048 bit)

```

Figura 4: Censys

Security Report Summary	
Site:	https://www.nos.pt/
IP Address:	104.18.18.73
Report Time:	15 Apr 2025 16:34:36 UTC
Headers:	<input checked="" type="checkbox"/> Content-Security-Policy <input checked="" type="checkbox"/> Referrer-Policy <input checked="" type="checkbox"/> Strict-Transport-Security <input checked="" type="checkbox"/> X-Frame-Options <input checked="" type="checkbox"/> X-Content-Type-Options <input type="checkbox"/> Permissions-Policy
Advanced:	Great grade! Perform a deeper security analysis of your website and APIs. Try Now

Figura 5: SecurityHeaders

Background

Site title	https://www.nos.pt	Date first seen	July 2014
Site rank	73738	Primary language	Portuguese
Description	Liga-te à rede 5G com os nossos tarifários móveis ou pacotes de internet e televisão. Internet fixa e móvel, loja online com smartphones e muito mais.		

Network

Site	https://www.nos.pt	Domain	nos.pt
Netblock Owner	Cloudflare, Inc.	Nameserver	ns5.nos.pt
Hosting company	Cloudflare	Domain registrar	Unknown
Hosting country	US	Nameserver organisation	Unknown
IPv4 address	104.18.18.73 (VirusTotal)	Organisation	Unknown
IPv4 autonomous systems	AS13335	DNS admin	dns@cloudflare.com
IPv6 address	2606:4700:0:0:0:6812:1249	Top Level Domain	Portugal (.pt)
IPv6 autonomous systems	AS13335	DNS Security Extensions	Enabled
Reverse DNS	Unknown		

IP delegation

IPv4 address (104.18.18.73)

IP range	Country	Name	Description
::ffff:0.0.0.0/96	United States	IANA-IPv4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
104.0.0.0-104.255.255	United States	NET104	American Registry for Internet Numbers
104.16.0.0-104.31.255.255	United States	CLOUDFLARENET	Cloudflare, Inc.
104.18.18.73	United States	CLOUDFLARENET	Cloudflare, Inc.

IPv6 address (2606:4700:0:0:0:6812:1249)

IP range	Country	Name	Description
::/0	N/A	ROOT	Root inetnum object
2600::/12	United States	NET6-2600	American Registry for Internet Numbers
2606:4700::/32	United States	CLOUDFLARENET	Cloudflare, Inc.
2606:4700:0:0:0:6812:1249	United States	CLOUDFLARENET	Cloudflare, Inc.

Figura 6: Neteckraft

SSL/TLS

Assurance	Domain validation	Perfect Forward Secrecy	Yes
Common name	nos.pt	Supported TLS Extensions	RFC8446 key share, RFC8446 supported versions, RFC4366 server name, RFC7301 application-layer protocol negotiation, RFC4366 status request, RFC8446 early data
Organisation	Not Present	Application-Layer Protocol Negotiation	h2
State	Not Present	Next Protocol Negotiation	Not Present
Country	Not Present	Issuing organisation	Google Trust Services
Organisational unit	Not Present	Issuer common name	WE1
Subject Alternative Name	nos.pt, www.nos.pt	Issuer unit	Not Present
Validity period	From Mar 13 2025 to Jun 11 2025 (2 months, 4 weeks, 1 day)	Issuer location	Not Present
Matches hostname	Yes	Issuer country	US
Server	cloudflare	Issuer state	Not Present
Public key algorithm	id-ecPublicKey	Certificate Revocation Lists	http://c.pki.goog/we1/BwYkd5XkYBc.crl
Protocol version	TLSv1.3	Certificate Hash	wcmiuCl4/Z2PYO1yFDV+XxjPLU
Public key length	256	Public Key Hash	d9cb932f6942fa60bea3f8ffbf4b2d8f9511632099c852dddea3da54bcd69e
Certificate check	ok	OCSP servers	http://o.pki.goog/s/we1/rre
Signature algorithm	ecdsa-with-SHA256	OCSP stapling response	Certificate valid
Serial number	0xaeb113bd61d416170edcbe98806ef3a3	OCSP data generated	Apr 12 07:54:04 2025 GMT
Cipher	TLS_AES_256_GCM_SHA384	OCSP data expires	Apr 19 06:54:03 2025 GMT
Version number	0x02		

Certificate Transparency

Signed Certificate Timestamps (SCTs)

Source	Log	Timestamp	Signature Verification
Certificate	Unknown zxFlw7tuufK/zh1v2a58b6Rpx28quF+ysAdJbd87M0wg=	2025-03-13 03:52:34	Unknown
Certificate	DigiCert Yeti2025 Log FvkxEuF4KnscYwd8xv3481dcFKB01265Ay/2Dowuebg=	2025-03-13 03:52:34	Success

SSLv3/POODLE

This site does not support the SSL version 3 protocol.

[More information about SSL version 3 and the POODLE vulnerability.](#)

Heartbleed

The site did not offer the Heartbeat TLS extension prior to the Heartbleed disclosure, and so was not exploitable.

This test does not exploit the Heartbleed vulnerability but uses information from conventional HTTPS requests. [More information about Heartbleed detection.](#)

Figura 7: Netcraft

2. Parte B

2.1. B1

B1: Conecte-se ao sistema alvo usando o protocolo de rede telnet. Analise o tráfego capturado e discuta os potenciais problemas de segurança identificados. Qual seria a solução para os problemas identificados?

O tráfego capturado com o **Wireshark**, utilizando um filtro específico para o protocolo **Telnet**, revelou uma comunicação entre o cliente (172.25.6.20) e o servidor (172.25.6.10), onde se observaram várias mensagens de negociação típicas do **Telnet**, seguidas por pacotes com apenas 1 byte de dados, característicos da introdução de comandos ou palavras-passe. Esta análise evidencia um problema grave de segurança: o **Telnet** transmite toda a informação em texto claro, incluindo credenciais e comandos, o que permite a qualquer atacante com acesso à rede capturar facilmente dados sensíveis. Como solução, recomenda-se a substituição do **Telnet** por SSH, que oferece comunicação segura e encriptada, além de autenticação robusta. Adicionalmente, deve-se desativar o serviço **Telnet** nos sistemas, aplicar filtros de *firewall* para restringir acessos remotos e monitorizar a rede com ferramentas NIDS para detetar usos indevidos de protocolos inseguros.

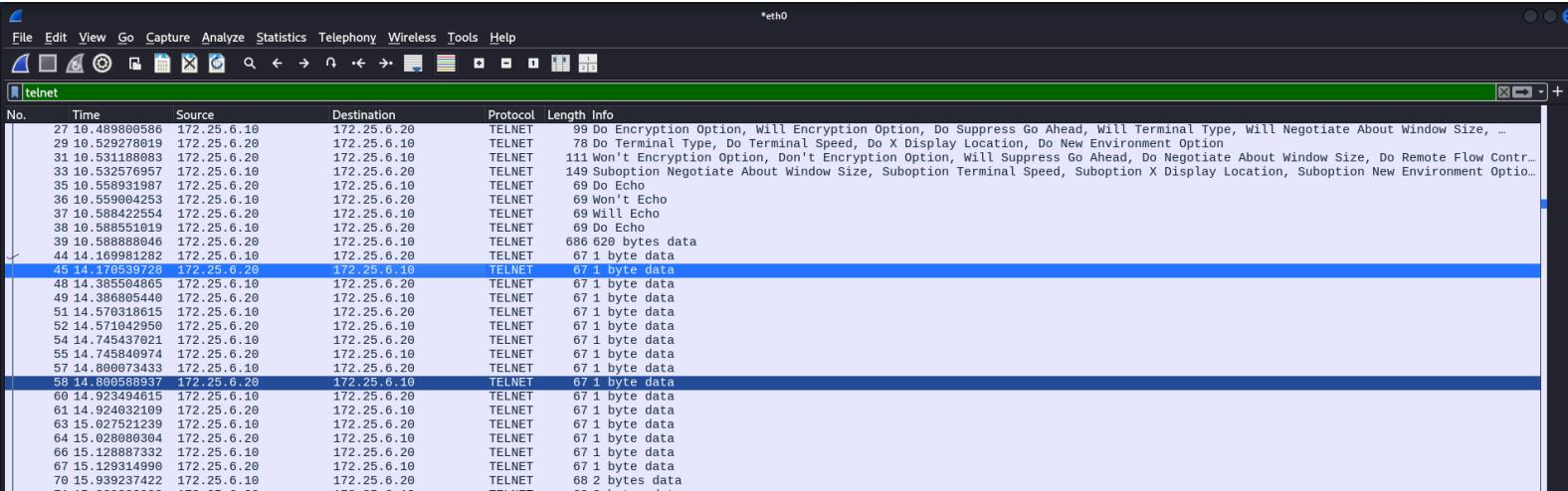


Figura 8: Captura do tráfego gerado pelo protocolo Telnet

2.2. B2

B2: Use a ferramenta Network Mapper (Nmap) para executar quatro varreduras distintas:

1. nmap -sV IP_alvo
2. nmap -sV -p 80 IP_alvo
3. nmap -sV --script vulners IP_alvo
4. nmap -A IP_alvo

2.2.1. B2.1

B2.1: Compare e discuta os resultados de cada varredura (i.e., output do Nmap)

As quatro varreduras **Nmap** realizadas sobre o sistema alvo (IP 172.25.6.20) permitiram recolher diferentes níveis de informação, desde uma visão geral até uma análise detalhada de segurança.

A primeira varredura (**nmap -sV**) revelou diversas portas abertas com serviços como FTP, SSH, Telnet, HTTP, SMB, MySQL e VNC, incluindo as versões dos mesmos. Esta varredura é essencial numa fase inicial de reconhecimento, pois fornece uma visão abrangente dos serviços disponíveis no sistema.

A segunda varredura (**nmap -sV -p 80**) concentrou-se unicamente na porta 80, confirmado que se trata de um servidor Apache httpd 2.2.8. Esta abordagem mais rápida e específica é útil quando se pretende analisar em detalhe apenas um serviço.

A terceira varredura (**nmap -sV --script vulners**) foi orientada para a identificação de vulnerabilidades conhecidas. Ao cruzar as versões dos serviços com uma base de dados de CVEs, foi possível detetar múltiplas vulnerabilidades associadas. Esta técnica é extremamente útil para avaliação de risco e planeamento de exploração.

Por fim, a varredura avançada (**nmap -A**) ofereceu uma análise muito mais detalhada, incluindo detalhes de segurança do SMB, chaves SSH do host, informações de certificados SSL, configurações detalhadas de serviços como MySQL, traceroute ao alvo e detecção precisa do sistema operacional — informações que indicam fortemente de que se trata de uma máquina Metasploitable configurada para testes. Esta varredura é mais demorada e invasiva, mas fornece um perfil completo do alvo e das suas potenciais falhas de segurança.

Em resumo, cada varredura tem uma finalidade distinta: desde o reconhecimento geral de serviços até à deteção de vulnerabilidades e análise avançada do sistema. A combinação destas técnicas permite construir uma visão sólida da postura de segurança do alvo.

```
[kali㉿kali]:~]$ nmap -sV 172.25.6.20
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-14 11:38 EDT
Nmap scan report for 172.25.6.20
Host is up (0.00018s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
23/tcp    open  telnet   Linux telnetd
25/tcp    open  smtp     Postfix smtpd
53/tcp    open  domain   ISC BIND 9.4.2
80/tcp    open  http     Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind  2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec     netkit-rsh rexd
513/tcp   open  login    OpenBSD or Solaris rlogind
514/tcp   open  shell    NetKit rshd
1099/tcp  open  java-rmi  GNU Classpath grmiregistry
1524/tcp  open  bindshell Metasploitable root shell
2049/tcp  open  nfs     2-4 (RPC #100003)
2121/tcp  open  ftp     ProFTPD 1.3.1
3306/tcp  open  mysql   MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc     VNC (protocol 3.3)
6000/tcp  open  X11    (access denied)
6667/tcp  open  irc     UnrealIRCd
8009/tcp  open  ajp13   Apache Jserv (Protocol v1.3)
8180/tcp  open  http    Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:DC:51:EA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSS: Unix, Linux; CPE:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.77 seconds
```

Figura 9: Output nmap -sV

```
(kali㉿kali)-[~]
└─$ nmap -sV -p 80 172.25.6.20
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-14 11:41 EDT
Nmap scan report for 172.25.6.20
Host is up (0.00040s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.2.8 ((Ubuntu) DAV/2)
MAC Address: 08:00:27:DC:51:EA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.57 seconds

(kali㉿kali)-[~]
└─$ █
```

Figura 10: Output nmap -sV -p 80

```
└─$ nmap -sV --script vulners 172.25.6.20
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-14 12:02 EDT
nmap_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 172.25.6.20
Host is up (0.00046s latency).

Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp        vsftpd 2.3.4
22/tcp    open  ssh        OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet     Linux telnetd
25/tcp    open  smtp       Postfix smtpd  few Help
53/tcp    open  domain    ISC BIND 9.4.2
80/tcp    open  http       Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 ((Ubuntu) DAV/2
111/tcp   open  rpcbind   2 (RPC #100000)
| rpcinfo:
|   program version port/proto service
|   100000  2          111/tcp  rpcbind [Priority: 1] (TCP) 172.25.6.10:44200 → 172.25.6.20:8100
|   100000  2          111/udp  rpcbind [Priority: 1] (TCP) 172.25.6.10:44200 → 172.25.6.20:80
|   100003  2,3,4     2049/tcp nfs      [Priority: 1] (TCP) 172.25.6.10:44200 → 172.25.6.20:80
|   100003  2,3,4     2049/udp nfs     [Priority: 1] (TCP) 172.25.6.10:44200 → 172.25.6.20:80
|   100005  1,2,3     44458/tcp mountd   [Priority: 1] (TCP) 172.25.6.10:44200 → 172.25.6.20:80
|   100005  1,2,3     50742/udp mountd   [Priority: 1] (TCP) 172.25.6.10:44200 → 172.25.6.20:80
|   100021  1,3,4     36794/tcp nlockmgr [Priority: 1] (TCP) 172.25.6.10:44200 → 172.25.6.20:80
|   100021  1,3,4     58730/udp nlockmgr [Priority: 1] (TCP) 172.25.6.10:44200 → 172.25.6.20:80
|   100024  1          37705/tcp status    [Priority: 1] (TCP) 172.25.6.10:44200 → 172.25.6.20:80
|   100024  1          44644/udp status    [Priority: 1] (TCP) 172.25.6.10:44200 → 172.25.6.20:80
|_139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
|_445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
|_512/tcp   open  exec      netkit-rsh reexec
|_513/tcp   open  login     OpenBSD or Solaris rlogin
|_514/tcp   open  shell     Netkit rshd
1099/tcp  open  java-rmi  GNU Classpath grmiregistry
1524/tcp  open  bindshell  Metasploitable root shell
2049/tcp  open  nfs      2-4 (RPC #100003)
2121/tcp  open  ftp      ProFTPD 1.3.1
3306/tcp  open  mysql    MySQL 5.0.51a-Ubuntu5
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7.
5900/tcp  open  vnc      VNC (protocol 3.3)
5000/tcp  open  X11      (access denied)
5667/tcp  open  irc      UnrealIRCd
8009/tcp  open  ajp13   Apache Jserv (Protocol v1.3)
8180/tcp  open  http     Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
MAC Address: 08:00:27:DC:51:EA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.17 seconds
```

Figura 11: Output nmap -sV --script vulners

```

└→ nmap -A 172.25.6.20
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-14 12:07 EDT
Nmap scan report for 172.25.6.20
Host is up (0.00056s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|_ STAT: 
FTP server status:
| Connected to 172.25.6.10
| Logged in as ftp
| TYPE: ASCII
| No session bandwidth limit
| Session timeout in seconds is 300
| Control connection is plain text
| Data connections will be plain text
|_VSFTPD 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntui (protocol 2.0)
| ssh-hostkey:
|_ 1024 60:8f:cfe1:0:5f:6a:74:d6:90:24:fa:c4:d5:6c:c0 (DSA)
|_ 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet        Linux telnetd
25/tcp    open  smtp         Postfix smtpd
| ssl-cert: Subject: commonName=ubuntu04-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
|_Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
| sslv2:
|_ SSLv2 supported
| ciphers:
|_ SSL2_RC2_128_CBC_WITH_MD5
|_ SSL2_RC4_128_WITH_MD5
|_ SSL2_RC4_128_EXPORT40_WITH_MD5
|_ SSL2_DES_64_CBC_WITH_MD5
|_ SSL2_RC2_128_EXPORT40_WITH_MD5
|_ SSL2_DES_192_EDE3_CBC_WITH_MD5
|_ _metaCommands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-date: 2025-04-14T16:06:50+00:00; -40s from scanner time.
53/tcp    open  domain       ISC BIND 9.4.2
| dns-nsid:
|_ bind.version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)  OpenSSL/1.0.2-fips  PHP/7.0.33-fpm
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2 PHP/7.0.33-fpm OpenSSL/1.0.2-fips PHP/7.0.33-fpm
|_http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind     2 (RPC #100000)
| rpcinfo:
|_ program version port/proto service
| 100000  2        111/tcp  rpcbind
| 100000  2        111/udp  rpcbind
| 100003  2,3,4   2049/tcp nfss

```

Figura 12: Output nmap -A

2.2.2. B2.2

B2.2: Analise o tráfego capturado e discuta o impacto (detectabilidade) de cada um do ponto de vista de um NIDS.

Os comandos **Nmap** variam em detectabilidade conforme o tráfego que geram.

O **nmap -sV** é facilmente detectável pelo volume de pacotes SYN e conexões sequenciais em múltiplas portas. O **nmap -sV -p 80** é mais discreto por se focar apenas numa porta, mas ainda detectável pelos padrões anómalos de interação após conexão. O **nmap -sV --script vulners** é claramente intrusivo, gerando tráfego distintivo com *payloads* incomuns e tentativas de exploração que acionam facilmente alarmes. O **nmap -A** é o mais detectável de todos, combinando múltiplas técnicas que geram tráfego diversificado com *flags* TCP incomuns e tentativas de conexão em várias portas, sendo imediatamente identificável como uma varredura agressiva.

B2.3: Analise o relatório do NIDS e discuta os resultados considerando a sua resposta ao item B2.2.

Os resultados dos relatórios do **NIDS (Suricata)** demonstram uma eficácia consistente na detecção de todas as variantes de comandos **Nmap** testados, corroborando a análise prévia sobre a detectabilidade destas ferramentas de reconhecimento. Os *logs* mostram que, independentemente do nível de agressividade do comando, o **NIDS** identificou consistentemente a atividade como “ET SCAN Possible Nmap User-Agent Observed” com classificação de “Web Application Attack”. Os resultados práticos indicam que mesmo o comando mais básico é facilmente detectado através de assinaturas como o User-

-Agent característico do Nmap. Observa-se também que o comando **-A** produz uma maior variedade de alertas (incluindo “TLS Invalid record type” e “Applayer Mismatch protocol”).

Esta evidência sugere que os **NIDS** modernos estão bem equipados para identificar ferramentas de reconhecimento padronizadas, independentemente das técnicas de evasão básicas como limitação de portas-alvo, demonstrando como os sistemas de detecção modernos evoluíram para reconhecer comportamentos específicos nas interações de rede, indo além da simples análise do volume ou da variedade de tráfego gerado pelos diferentes comandos do **Nmap**.

```
04/14/2025-11:38:38.476917 [**] [1:2260002:1] SURICATA Applayer Detect protocol only one direction [**]
[Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 172.25.6.10:37634 → 172.25.6.2
04/14/2025-11:38:43.531139 [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent Observed [**] [Classification: Web Application Attack] [Priority: 1] {TCP} 172.25.6.10:48342 → 17.25.6.20:80
04/14/2025-11:38:43.531423 [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent Observed [**] [Classification: Web Application Attack] [Priority: 1] {TCP} 172.25.6.10:48346 → 17.25.6.20:80
04/14/2025-11:38:43.550941 [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent Observed [**] [Classification: Web Application Attack] [Priority: 1] {TCP} 172.25.6.10:34782 → 17.25.6.20:8180
04/14/2025-11:38:43.553607 [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent Observed [**] [Classification: Web Application Attack] [Priority: 1] {TCP} 172.25.6.10:34796 → 17.25.6.20:8180
04/14/2025-11:38:43.560107 [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent Observed [**] [Classification: Web Application Attack] [Priority: 1] {TCP} 172.25.6.10:48372 → 17.25.6.20:80
04/14/2025-11:38:43.563624 [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent Observed [**] [Classification: Web Application Attack] [Priority: 1] {TCP} 172.25.6.10:34820 → 17.25.6.20:8180
04/14/2025-11:38:43.564242 [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent Observed [**] [Classification: Web Application Attack] [Priority: 1] {TCP} 172.25.6.10:48378 → 17.25.6.20:80
04/14/2025-11:38:43.568323 [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent Observed [**] [Classification: Web Application Attack] [Priority: 1] {TCP} 172.25.6.10:34828 → 17.25.6.20:8180
```

Figura 13: Notificações do NIDS relativamente a nmap -sV

```
04/14/2025-11:24:09.181316 [**] [TCP/0243645] ET SAN Possible Nmap User-Agent Observed [**] [Classification: Web Application Attack] [Priority: 1] [TCP] 172.25.6.10:44266 -> 172.25.6.20:80  
04/14/2025-11:24:09.181884 [**] [TCP/0243645] ET SAN Possible Nmap User-Agent Observed [**] [Classification: Web Application Attack] [Priority: 1] [TCP] 172.25.6.10:44280 -> 172.25.6.20:80  
04/14/2025-11:24:09.196039 [**] [TCP/0243645] ET SAN Possible Nmap User-Agent Observed [**] [Classification: Web Application Attack] [Priority: 1] [TCP] 172.25.6.10:44294 -> 172.25.6.20:80  
04/14/2025-11:24:09.198079 [**] [TCP/0243645] ET SAN Possible Nmap User-Agent Observed [**] [Classification: Web Application Attack] [Priority: 1] [TCP] 172.25.6.10:44300 -> 172.25.6.20:80
```

Figura 14: Notificações do NIDS relativamente a nmap -sV -p 80

```
04/14/2025-12:05:08.605186 [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent Observed [*] [Classification: Web Application Attack] [Priority: 1] {TCP[172.25.6.10:50954 -> 172.25.6.20:80]}

04/14/2025-12:05:08.605015 [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent Observed [*] [Classification: Web Application Attack] [Priority: 1] {TCP[172.25.6.10:50954 -> 172.25.6.20:80]}

04/14/2025-12:05:08.605094 [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent Observed [*] [Classification: Web Application Attack] [Priority: 1] {TCP[172.25.6.10:55178 -> 172.25.6.20:8188]

04/14/2025-12:05:08.605094 [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent Observed [*] [Classification: Web Application Attack] [Priority: 1] {TCP[172.25.6.10:55178 -> 172.25.6.20:8188]

04/14/2025-12:05:08.612051 [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent Observed [*] [Classification: Web Application Attack] [Priority: 1] {TCP[172.25.6.10:55178 -> 172.25.6.20:8188]

04/14/2025-12:05:08.612193 [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent Observed [*] [Classification: Web Application Attack] [Priority: 1] {TCP[172.25.6.10:55178 -> 172.25.6.20:8188]

04/14/2025-12:05:08.612235 [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent Observed [*] [Classification: Web Application Attack] [Priority: 1] {TCP[172.25.6.10:55178 -> 172.25.6.20:8188]

04/14/2025-12:05:08.632735 [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent Observed [*] [Classification: Web Application Attack] [Priority: 1] {TCP[172.25.6.10:50980 -> 172.25.6.20:80]

04/14/2025-12:05:08.632868 [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent Observed [*] [Classification: Web Application Attack] [Priority: 1] {TCP[172.25.6.10:50984 -> 172.25.6.20:80]

04/14/2025-12:05:08.636907 [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent Observed [*] [Classification: Web Application Attack] [Priority: 1] {TCP[172.25.6.10:55194 -> 172.25.6.20:8188]
```

Figura 15: Notificações do NIDS relativamente a nmap -sV -script vulners

```
[kali㉿kali ~]
File Actions Edit View Help
eneric Protocol Command Decode] [Priority: 3] [TCP] 172.25.6.10:44042 → 172.25.6.20:445
04/14/2025-12:07:30.258464 [**] [i:2002023:18] ET CHAT IRC USER command [**] [Classification: Misc activity]
[Priority: 3] [TCP] 172.25.6.10:56106 → 172.25.6.20:6667
04/14/2025-12:07:30.258464 [**] [i:2002024:21] ET CHAT IRC NICK command [**] [Classification: Misc activity]
[Priority: 3] [TCP] 172.25.6.10:56106 → 172.25.6.20:6667
04/14/2025-12:07:30.698857 [**] [i:2260002:1] SURICATA Applayer Detect protocol only one direction [**] [Classification: Generic Protocol Command Decode] [Priority: 3] [TCP] 172.25.6.20:205 → 172.25.6.10:48676
04/14/2025-12:07:30.698857 [**] [i:2260002:1] SURICATA Applayer Detect protocol only one direction [**] [Classification: Generic Protocol Command Decode] [Priority: 3] [TCP] 172.25.6.20:205 → 172.25.6.10:48686
04/14/2025-12:07:30.772213 [**] [i:2230002:1] SURICATA TLS invalid record type [**] [Classification: Generic Protocol Command Decode] [Priority: 3] [TCP] 172.25.6.10:36538 → 172.25.6.20:21
04/14/2025-12:07:30.772213 [**] [i:2260001:1] SURICATA Applayer Mismatch protocol both directions [**] [Classification: Generic Protocol Command Decode] [Priority: 3] [TCP] 172.25.6.10:36538 → 172.25.6.20:21
04/14/2025-12:07:30.772466 [**] [i:2230002:1] SURICATA TLS invalid record type [**] [Classification: Generic Protocol Command Decode] [Priority: 3] [TCP] 172.25.6.20:29 → 172.25.6.10:36538
04/14/2025-12:07:30.775574 [**] [i:2260001:1] SURICATA Applayer Mismatch protocol both directions [**] [Classification: Generic Protocol Command Decode] [Priority: 3] [TCP] 172.25.6.20:29 → 172.25.6.10:36540
04/14/2025-12:07:30.790147 [**] [i:2260001:1] SURICATA Applayer Mismatch protocol both directions [**] [Classification: Generic Protocol Command Decode] [Priority: 3] [TCP] 172.25.6.20:50900 → 172.25.6.10:58236
04/14/2025-12:07:30.794296 [**] [i:2260001:1] SURICATA Applayer Mismatch protocol both directions [**] [Classification: Generic Protocol Command Decode] [Priority: 3] [TCP] 172.25.6.20:50900 → 172.25.6.10:58250
04/14/2025-12:07:30.795746 [**] [i:2260002:1] SURICATA Applayer Detect protocol only one direction [**] [Classification: Generic Protocol Command Decode] [Priority: 3] [TCP] 172.25.6.20:201 → 172.25.6.10:48702
04/14/2025-12:07:30.801610 [**] [i:2260002:1] SURICATA Applayer Detect protocol only one direction [**] [Classification: Generic Protocol Command Decode] [Priority: 3] [TCP] 172.25.6.20:201 → 172.25.6.10:48708
04/14/2025-12:07:30.817643 [**] [i:2230002:1] SURICATA TLS invalid record type [**] [Classification: Generic Protocol Command Decode] [Priority: 3] [TCP] 172.25.6.10:40314 → 172.25.6.20:2121
04/14/2025-12:07:30.817643 [**] [i:2260002:1] SURICATA Applayer Detect protocol only one direction [**] [Classification: Generic Protocol Command Decode] [Priority: 3] [TCP] 172.25.6.10:40314 → 172.25.6.20:2121
04/14/2025-12:07:30.817949 [**] [i:2230002:1] SURICATA TLS invalid record type [**] [Classification: Generic Protocol Command Decode] [Priority: 3] [TCP] 172.25.6.20:2121 → 172.25.6.10:40314
04/14/2025-12:07:30.832656 [**] [i:2230002:1] SURICATA TLS invalid record type [**] [Classification: Generic Protocol Command Decode] [Priority: 3] [TCP] 172.25.6.20:3306 → 172.25.6.10:34004
04/14/2025-12:07:30.832656 [**] [i:2260002:1] SURICATA Applayer Detect protocol only one direction [**] [Classification: Generic Protocol Command Decode] [Priority: 3] [TCP] 172.25.6.20:3306 → 172.25.6.10:34004
04/14/2025-12:07:30.832676 [**] [i:2230002:1] SURICATA TLS invalid record type [**] [Classification: Generic Protocol Command Decode] [Priority: 3] [TCP] 172.25.6.20:3306 → 172.25.6.10:34004
```

Figura 16: Notificações do NIDS relativamente a nmap -A

2.3. B3

B3: Discuta como os levantamentos efetuados na Parte A do trabalho podem otimizar a varredura de sistemas alvo, em particular, reduzindo a sua detectabilidade.

A análise efetuada na Parte A do trabalho, através de técnicas de recolha passiva de informações sobre os sistemas da NOS e da A Padaria Portuguesa, permite compreender como este tipo de levantamento prévio pode otimizar fases posteriores de varredura ativa, nomeadamente ao nível da redução da sua detectabilidade. Ao identificar antecipadamente elementos da infraestrutura como domínios associados, IPs expostos, certificados SSL, tecnologias utilizadas e cabeçalhos de segurança implementados, é possível planear ataques ou auditorias técnicas de forma mais dirigida e discreta.

Por exemplo, o conhecimento de que a NOS utiliza Cloudflare para proteção da sua infraestrutura permite a um analista evitar interações desnecessárias com o sistema de defesa da CDN, optando por outras abordagens mais silenciosas, como o fingerprinting de subdomínios ou o uso de técnicas de correlação de certificados para tentar identificar servidores de origem. Da mesma forma, saber que a empresa força redirecionamento HTTPS e utiliza cabeçalhos como HSTS e CSP ajuda a evitar vetores de ataque ineficazes, como injecções simples em HTTP ou manipulação de scripts sem controlo de origem. Isto reduz o número de tentativas visíveis feitas ao sistema, diminuindo a probabilidade de deteção.

No caso da A Padaria Portuguesa, as informações recolhidas indicam uma estrutura mais simples, com serviços alojados externamente e segurança mais básica. Neste contexto, a recolha passiva ajuda a revelar potenciais fragilidades (como a ausência de redirecionamento automático para HTTPS ou a configuração parcial de cabeçalhos de segurança), permitindo selecionar vetores de varredura mais prováveis de sucesso sem acionar alarmes, como a análise de diretórios vulneráveis, versões de PHP expostas ou exploração de endpoints mal protegidos. Ao evitar técnicas invasivas desde o início e focar a varredura apenas em pontos potencialmente frágeis, reduz-se a superfície de deteção e o ruído gerado por scanners automatizados.

Em resumo, os levantamentos passivos realizados são fundamentais para uma abordagem estratégica à fase de varrimento de sistemas. Ao fornecerem uma base sólida de conhecimento sobre o alvo, permitem orientar as ações seguintes com maior precisão, minimizar interações desnecessárias e, sobretudo, reduzir significativamente a probabilidade de deteção por mecanismos de defesa e monitorização. Esta preparação é essencial tanto para atividades ofensivas (em contexto de teste de intrusão) como para avaliações defensivas eficazes.

2.4. B4

B4: O sistema alvo possui uma firewall instalada, i.e., iptables. Adicione regras para bloquear tráfego externo TCP para os portos 513 e 6000. Volte a executar as varreduras da questão B2, compare e discuta os resultados do Nmap.

Após a configuração da *firewall* com **iptables** para bloquear tráfego externo TCP nas portas 513 e 6000, os resultados das varreduras realizadas com os comandos do **Nmap** (conforme na questão B2) mostram que essas portas agora aparecem como *filtered*. Isso indica que o **Nmap** não conseguiu determinar se essas portas estão abertas ou fechadas, pois não houve resposta do *host*, o que é típico de uma política de *firewall* que descarta silenciosamente os pacotes.

No caso do comando **nmap -sV -p 80**, o impacto da *firewall* é inexistente, pois o comando está restrito à análise da porta 80, que não foi afetada pelas regras de bloqueio. Assim, os resultados antes e depois da aplicação da *firewall* são equivalentes.

Esta diferença nos resultados evidencia como regras simples de *firewall* podem modificar de forma significativa a percepção externa da segurança de um sistema. As portas filtradas impedem qualquer resposta, ocultando totalmente a existência de serviços ativos. Esta estratégia introduz uma camada adicional de obscuridade, dificultando a identificação precisa de serviços vulneráveis por parte de possíveis atacantes.

```
(kali㉿kali)-[~]
└─$ nmap -sV 172.25.6.20
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-14 14:34 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 172.25.6.20
Host is up (0.00035s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE     SERVICE VERSION
21/tcp    open      ftp      vsftpd 2.3.4
22/tcp    open      ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open      telnet   Linux telnetd
25/tcp    open      smtp     Postfix smtpd
53/tcp    open      domain   ISC BIND 9.4.2
80/tcp    open      http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open      rpcbind 2 (RPC #100000)
139/tcp   open      netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open      netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open      exec    netkit-rsh rexecd
513/tcp   filtered login   Netkit rshd
514/tcp   open      shell    Netkit rshd
1099/tcp  open      java-rmi GNU Classpath grmiregistry
1524/tcp  open      bindshell Metasploitable root shell
2049/tcp  open      nfs     2-4 (RPC #100003)
2121/tcp  open      ftp     ProFTPD 1.3.1
3306/tcp  open      mysql   MySQL 5.0.51a-3ubuntu5
5432/tcp  open      postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open      vnc     VNC (protocol 3.3)
6000/tcp  filtered X11
6667/tcp  open      irc     UnrealIRCd
8009/tcp  open      ajp13   Apache Jserv (Protocol v1.3)
8180/tcp  open      http    Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:DC:51:EA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.64 seconds
```

Figura 17: Output nmap -sV após configuração das iptables

```
(kali㉿kali)-[~]
└─$ nmap -sV -p 80 172.25.6.20
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-14 14:41 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 172.25.6.20
Host is up (0.00050s latency).

PORT      STATE     SERVICE VERSION
80/tcp    open      http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
MAC Address: 08:00:27:DC:51:EA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.58 seconds
```

Figura 18: Output nmap -sV -p 80 após configuração das iptables

```

└$ nmap -sV --script vulners 172.25.6.20
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-14 14:42 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 172.25.6.20
Host is up (0.00022s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE    SERVICE      VERSION
21/tcp    open     ftp          vsftpd 2.3.4
22/tcp    open     ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open     telnet       Linux telnetd
25/tcp    open     smtp         Postfix smtpd
53/tcp    open     domain      ISC BIND 9.4.2
80/tcp    open     http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp   open     rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version  port/proto  service
|   100000  2          111/tcp    rpcbind
|   100000  2          111/udp   rpcbind
|   100003  2,3,4     2049/tcp   nfs
|   100003  2,3,4     2049/udp  nfs
|   100005  1,2,3     33620/tcp  mountd
|   100005  1,2,3     60697/udp  mountd
|   100021  1,3,4     47075/tcp  nlockmgr
|   100021  1,3,4     59641/tcp  nlockmgr
|   100024  1          34717/tcp  status
|_ 100024  1          38031/udp  status
139/tcp   open     netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open     netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open     exec        netkit-rsh rexecd
513/tcp   filtered login
514/tcp   open     shell        Netkit rshd
1099/tcp  open     java-rmi   GNU Classpath grmiregistry
1524/tcp  open     bindshell   Metasploitable root shell
2049/tcp  open     nfs         2-4 (RPC #100003)
2121/tcp  open     ftp         ProFTPD 1.3.1
3306/tcp  open     mysql      MySQL 5.0.51a-Subuntu5
5432/tcp  open     postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open     vnc        VNC (protocol 3.3)
6000/tcp  filtered X11
6667/tcp  open     irc        UnrealIRCd
8009/tcp  open     ajp13     Apache Jserv (Protocol v1.3)
8180/tcp  open     http       Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
MAC Address: 08:00:27:DC:51:EA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.90 seconds

```

Figura 19: Output nmap -sV –script vulners após configuração das iptables

```

| rpcinfo:
|   program version  port/proto  service
|   100000  2          111/tcp    rpcbind
|   100000  2          111/udp   rpcbind
|   100003  2,3,4     2049/tcp   nfs
|   100003  2,3,4     2049/udp  nfs
|   100005  1,2,3     33620/tcp  mountd
|   100005  1,2,3     60697/udp  mountd
|   100021  1,3,4     47075/tcp  nlockmgr
|   100021  1,3,4     59641/tcp  nlockmgr
|   100024  1          34717/tcp  status
|_ 100024  1          38031/udp  status
139/tcp   open     netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open     netbios-ssn  Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp   open     exec        netkit-rsh rexecd
513/tcp   filtered login
514/tcp   open     shell        Netkit rshd
1099/tcp  open     java-rmi   GNU Classpath grmiregistry
1524/tcp  open     bindshell   Metasploitable root shell
2049/tcp  open     nfs         2-4 (RPC #100003)
2121/tcp  open     ftp         ProFTPD 1.3.1
3306/tcp  open     mysql      MySQL 5.0.51a-Subuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-Subuntu5
|   Thread ID: 10
|   Capabilities flags: 43564
|   Some Capabilities: Supports4Auth, SwitchToSSLAfterHandshake, ConnectWithDatabase, SupportsCompression, SupportsTransactions, LongColumnFlag, Speaks41ProtocolNew
|   Status: Autocommit
|_ Salt: ;BwSy'RK'ydia-XX!Ws
5432/tcp  open     postgresql PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2025-04-14T18:44:44+00:00; -is from scanner time.
|_ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after: 2010-04-16T14:07:45
5900/tcp  open     vnc        VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_  VNC Authentication (2)
6000/tcp  filtered X11
6667/tcp  open     irc        UnrealIRCd
8009/tcp  open     ajp13     Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp  open     http       Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat/5.5
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
MAC Address: 08:00:27:DC:51:EA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33

```

Figura 20: Output nmap -A após configuração das iptables

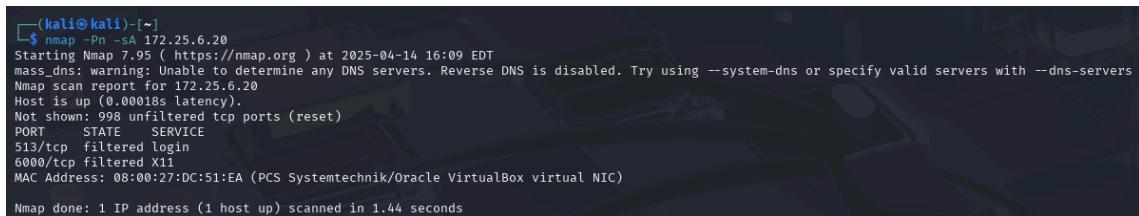
2.5. B5

B5: Ainda com os portos 513 e 6000 bloqueados para tráfego TCP de entrada, execute as varreduras abaixo, analise, compare e discuta os resultados.

1. nmap -Pn -sA IP_alvo
2. nmap -Pn -sF IP_alvo
3. nmap -Pn -sN IP_alvo
4. nmap -Pn -sX IP_alvo
5. nmap -Pn -sU -p 513,6000 IP_alvo

Os resultados dos cinco comandos **Nmap** revelam como diferentes técnicas de varredura interagem com o *firewall* configurado para bloquear as portas TCP 513 e 6000. O scan ACK (nmap -Pn -sA) identificou apenas estas duas portas como filtradas, confirmando a eficácia das regras de *firewall* implementadas. Os scans FIN, NULL e XMAS (-sF, -sN, -sX) produziram resultados semelhantes entre si, classificando múltiplas portas como “open|filtered”, demonstrando como estas técnicas podem contornar *firewalls* simples que se focam apenas em pacotes SYN, por exemplo. Particularmente interessante foi o scan UDP (-sU -p 513,6000), que revelou que as mesmas *ports* que estavam filtradas em TCP apareceram como “closed” em UDP, indicando que as regras implementadas bloqueiam especificamente o tráfego TCP, mas não UDP para essas *ports*.

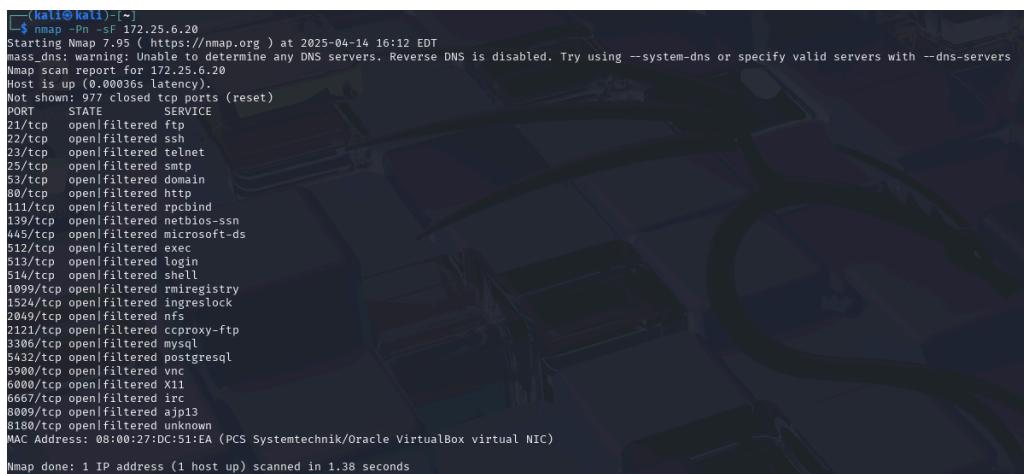
Esta comparação demonstra a importância de utilizar múltiplas técnicas de varredura durante avaliações de segurança, já que cada método interage diferentemente com mecanismos de proteção. Também evidencia que *firewalls* básicos podem ser insuficientes contra técnicas de reconhecimento avançadas, reforçando a necessidade de configurações de segurança mais abrangentes que considerem diferentes vetores de exploração.



```
(kali㉿kali)-[~]
$ nmap -Pn -sA 172.25.6.20
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-14 16:09 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 172.25.6.20
Host is up (0.00018s latency).
Not shown: 998 unfiltered tcp ports (reset)
PORT      STATE     SERVICE
513/tcp    filtered  login
6000/tcp   filtered  X11
MAC Address: 08:00:27:DC:51:EA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.44 seconds
```

Figura 21: Output nmap -Pn -sA



```
(kali㉿kali)-[~]
$ nmap -Pn -sF 172.25.6.20
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-14 16:12 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 172.25.6.20
Host is up (0.00036s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE     SERVICE
21/tcp    open|filtered  ftp
22/tcp    open|filtered  ssh
23/tcp    open|filtered  telnet
25/tcp    open|filtered  smtp
53/tcp    open|filtered  domain
80/tcp    open|filtered  http
111/tcp   open|filtered  rpcbind
139/tcp   open|filtered  netbios-ssn
445/tcp   open|filtered  microsoft-ds
512/tcp   open|filtered  exec
513/tcp   open|filtered  login
514/tcp   open|filtered  shell
1099/tcp  open|filtered  rmiregistry
1524/tcp  open|filtered  ingreslock
2049/tcp  open|filtered  nfs
2121/tcp  open|filtered  cproxxy-ftp
3306/tcp  open|filtered  mysql
5432/tcp  open|filtered  postgresql
5900/tcp  open|filtered  vnc
6000/tcp  open|filtered  X11
6667/tcp  open|filtered  irc
8009/tcp  open|filtered  ajp13
8180/tcp  open|filtered  unknown
MAC Address: 08:00:27:DC:51:EA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.38 seconds
```

Figura 22: Output nmap -Pn -sF

```
(kali㉿kali)-[~]
└─$ nmap -Pn -sN 172.25.6.20
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-14 16:12 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 172.25.6.20
Host is up (0.00027s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE     SERVICE
21/tcp    open|filtered  ftp
22/tcp    open|filtered  ssh
23/tcp    open|filtered  telnet
25/tcp    open|filtered  smtp
53/tcp    open|filtered  domain
80/tcp    open|filtered  http
111/tcp   open|filtered  rpcbind
139/tcp   open|filtered  netbios-ssn
445/tcp   open|filtered  microsoft-ds
512/tcp   open|filtered  exec
513/tcp   open|filtered  login
514/tcp   open|filtered  shell
1099/tcp  open|filtered  rmiregistry
1524/tcp  open|filtered  ingreslock
2049/tcp  open|filtered  nfs
2121/tcp  open|filtered  cproxy-ftp
3306/tcp  open|filtered  mysql
5432/tcp  open|filtered  postgresql
5900/tcp  open|filtered  vnc
6000/tcp  open|filtered  X11
6667/tcp  open|filtered  irc
8009/tcp  open|filtered  ajp13
8180/tcp  open|filtered  unknown
MAC Address: 08:00:27:DC:51:EA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.49 seconds
```

Figura 23: Output nmap -Pn -sN

```
(kali㉿kali)-[~]
└─$ nmap -Pn -sX 172.25.6.20
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-14 16:13 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 172.25.6.20
Host is up (0.0010s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE     SERVICE
21/tcp    open|filtered  ftp
22/tcp    open|filtered  ssh
23/tcp    open|filtered  telnet
25/tcp    open|filtered  smtp
53/tcp    open|filtered  domain
80/tcp    open|filtered  http
111/tcp   open|filtered  rpcbind
139/tcp   open|filtered  netbios-ssn
445/tcp   open|filtered  microsoft-ds
512/tcp   open|filtered  exec
513/tcp   open|filtered  login
514/tcp   open|filtered  shell
1099/tcp  open|filtered  rmiregistry
1524/tcp  open|filtered  ingreslock
2049/tcp  open|filtered  nfs
2121/tcp  open|filtered  cproxy-ftp
3306/tcp  open|filtered  mysql
5432/tcp  open|filtered  postgresql
5900/tcp  open|filtered  vnc
6000/tcp  open|filtered  X11
6667/tcp  open|filtered  irc
8009/tcp  open|filtered  ajp13
8180/tcp  open|filtered  unknown
MAC Address: 08:00:27:DC:51:EA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.52 seconds
```

Figura 24: Output nmap -Pn -sX

```
(kali㉿kali)-[~]
└─$ nmap -Pn -sU -p 513,6000 172.25.6.20
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-14 16:14 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 172.25.6.20
Host is up (0.00065s latency).

PORT      STATE     SERVICE
513/udp  closed  who
6000/udp closed  X11
MAC Address: 08:00:27:DC:51:EA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
```

Figura 25: Output nmap -Pn -sU -p 513,6000

2.6. B6

B6: Use o scanner de vulnerabilidades Nikto para varrer os serviços web a correr no sistema alvo. Compare os resultados da varredura e do tráfego capturado com aqueles observados nos comandos 3 e 4 da questão B2.

A varredura realizada com a ferramenta **Nikto** identificou diversas vulnerabilidades específicas no serviço web do sistema alvo, incluindo diretorias potencialmente sensíveis

como /phpMyAdmin e /test, além de ficheiros acessíveis que representam riscos de segurança. A análise do tráfego capturado confirmou estes resultados, mostrando múltiplas requisições HTTP GET e HEAD, com várias recebendo respostas “200 OK”, evidenciando a abordagem sistemática do **Nikto** em testar caminhos comuns e padrões conhecidos de vulnerabilidades web.

O **Nmap** com script vulners concentra-se principalmente na identificação de versões de serviços e vulnerabilidades conhecidas associadas a essas versões. Esta ferramenta gera uma quantidade limitada de tráfego HTTP, geralmente do tipo HEAD e GET, oferecendo uma visão mais superficial da segurança. O **Nmap** em modo agressivo (-A) realiza uma varredura mais abrangente, incluindo detecção do sistema operativo, trace route e execução de scripts NSE, gerando mais tráfego e variedade de pacotes. No entanto, mesmo assim, não oferece uma análise detalhada do serviço HTTP, limitando-se a testar configurações e cabeçalhos padrão.

Conclui-se que o **Nikto** proporciona uma análise significativamente mais detalhada e especializada sobre o serviço web, com requisições que vão além das simples consultas de versão, permitindo detetar problemas concretos exploráveis por atacantes. O **Nmap** produz resultados mais genéricos, úteis para um primeiro mapeamento da superfície de ataque, mas insuficientes para uma análise de segurança web completa.

Figura 26: Resultados do Nikto

Figura 27: Tráfego causado pela varredura

2.7. B7

B7: Use o openVAS (ou Nessus) para uma nova varredura de vulnerabilidades do sistema alvo.

Para este exercício decidimos usar a ferramenta **Nessus**.

2.7.1. B7.1

B7.1: Compare os resultados desta ferramenta com os obtidos nas questões **B5** e **B2**.

A diferença entre os resultados obtidos pelo **Nessus** e pelo **Nmap** evidencia as funções distintas de cada ferramenta no contexto da análise de segurança.

O **Nessus** fornece uma avaliação detalhada de vulnerabilidades com classificação por gravidade (CVSS), identificando problemas críticos de segurança como vulnerabilidades em Node.js, certificados SSL não confiáveis e serviços desatualizados. No caso analisado, o **Nessus** encontrou 70 vulnerabilidades no *host* 172.25.6.10 (com 1 crítica, 3 altas e 1 média) e 116 no *host* 172.25.6.20 (com 7 críticas, 5 altas e 18 médias), além de fornecer descrições completas e recomendações para correção de cada problema.

Por outro lado, o **Nmap** concentra-se principalmente na descoberta e identificação de portas e serviços abertos, com informações básicas sobre versões.

Além disso, o **Nessus** analisou o *host* auditor e o *host* alvo, enquanto os resultados do **Nmap** mostravam apenas o segundo.

2.7.2. B7.2

B7.2: Observe que algumas notificações do NIDS não possuem vulnerabilidades correspondentes no relatório do scanner de vulnerabilidades. Discuta as possíveis razões para tais diferenças.

Algumas notificações do **NIDS** não possuem vulnerabilidades correspondentes no relatório do scanner de vulnerabilidades por diversas razões relacionadas às diferentes naturezas destas ferramentas.

Primeiramente, os **NIDSs** como o **Suricata** analisam o tráfego de rede em tempo real, detetando comportamentos anómalos e padrões suspeitos que podem não estar associados a vulnerabilidades específicas. Muitos alertas **NIDS** são gerados pela própria atividade de *scanning* quando o **Nessus** tenta estabelecer diferentes tipos de conexões para testar serviços, o que o **NIDS** interpreta como potencialmente malicioso. Também são comuns

falsos positivos no **NIDS** quando tráfego legítimo mas incomum é interpretado como suspeito.

Adicionalmente, o **NIDS** pode detetar ataques direcionados a vulnerabilidades que já foram corrigidas nos sistemas alvo, resultando em alertas sem vulnerabilidades correspondentes. A utilização inadequada de protocolos pode gerar alertas no **NIDS** sem que existam vulnerabilidades exploráveis que o *scanner* reportaria.