

Tecnologias de Segurança

Trabalho Prático 2

Eduardo Cunha PG55939

João Magalhães PG55956

Rodrigo Gomes PG56004

Abril, 2025

Indice

1. Introdução	3
2. Parte A	4
2.1. Sintanet	4
2.1.1. WhoIs	4
2.1.2. HTTP	5
2.1.3. Utilizador do GitHub	7
2.1.4. 404	7
2.1.5. IP	8
2.1.6. BuiltWith	8
2.1.7. Robots	9
2.1.8. Openssl	11
2.1.9. Conclusões relativas à Sintanet	11
2.2. Nike	12
2.2.1. WhoIs	12
2.2.2. Vagas de Trabalho	14
2.2.3. Página Web	16
2.2.4. 404	18
2.2.5. IP	18
2.2.6. Openssl	20
2.2.7. Exposição de Informação	21
2.2.8. Data Breaches	22
2.2.9. Wappalyzer	22
2.2.10. Inferência Node.js	22
2.2.11. Conclusões	23
2.3. Conclusão Global da Parte A	23
3. Parte B	24
3.1. B1	24
3.2. B2	25
3.2.1. B2.1	26
3.2.2. B2.2	29
3.2.3. B2.3	30
3.3. B3	32
3.4. B4	32
3.5. B5	34
3.6. B6	38
3.7. B7	42
3.7.1. B7.1	42
3.7.2. B7.2	43
4. Conclusão	44

1. Introdução

Num cenário cada vez mais digital, a segurança da informação assume um papel crucial na proteção das infraestruturas tecnológicas que sustentam as operações de organizações de todas as dimensões. O presente trabalho prático tem como principal objetivo a exploração de técnicas de footprinting, um processo essencial na fase inicial dos testes de penetração, que permite mapear a superfície de exposição dos sistemas e identificar potenciais riscos associados. Numa fase subsequente, o foco incide na análise de vulnerabilidades, através de um contacto direto com o sistema alvo.

Através da análise de serviços conectados, pretende-se compreender de que forma distintas abordagens de recolha de informação, tanto passivas como ativas, podem revelar vulnerabilidades e fragilidades nas infraestruturas tecnológicas. Este trabalho encontra-se organizado em duas partes complementares. A primeira parte (Parte A) incide na recolha passiva de informação relativa a duas entidades com presença online, nomeadamente uma grande corporação e uma empresa de âmbito local, permitindo observar e comparar as respetivas práticas de gestão da segurança. A segunda parte (Parte B) foca-se na realização de varrimentos e na enumeração de vulnerabilidades num ambiente de testes controlado, com o objetivo de avaliar o potencial impacto das falhas identificadas, bem como a eficácia de diferentes técnicas de análise.

Com este exercício, pretende-se não só aplicar conhecimentos técnicos, mas também desenvolver uma visão crítica sobre os riscos e desafios associados à exposição digital, contribuindo para a construção de estratégias de defesa mais robustas e informadas.

2. Parte A

Nesta primeira parte do trabalho, foi realizada a análise passiva de duas entidades com presença online: uma empresa local e uma grande corporação. O objetivo passou por aplicar técnicas de recolha de informação disponíveis em fontes de domínio público, visando obter dados relevantes sobre os sistemas, infraestruturas e práticas de segurança associadas a cada uma. Este exercício permitiu não só identificar elementos técnicos expostos, como também refletir sobre as diferenças na gestão da segurança digital entre organizações de diferentes dimensões e contextos operacionais.

2.1. Sintanet

Como pequena corporação decidimos escolher a empresa Sintanet, especializada na venda de telemóveis, acessórios e serviços de reparação de dispositivos móveis.

Pesquisando pela empresa na internet facilmente obtemos informações sobre a sua localização.

The screenshot shows a search result for 'SINTANET'. At the top, it displays a rating of 4,5 stars from 247 reviews. Below the rating, the text 'Loja de telemóveis na Caldelas' is shown. There are several buttons for actions like 'Website', 'Direções' (Directions), 'Críticas' (Reviews), 'Guardar' (Save), 'Partilhar' (Share), and 'Ligar' (Call). Underneath these buttons, there is a section titled 'Opções de serviço:' which lists services such as repair, same-day delivery, and battery recycling. The location is listed as 'Localizado em: Centro Comercial Passerelle'. The address is 'Centro Comercial Passerelle, Praça Dr. João Antunes Guimarães Loja 62-63, 4805-121 Guimarães'. The phone number is '253 097 000'. The opening hours are listed as 'Aberto · Fecha às 13:00 · Volta a abrir às 15:00 ▾'. At the bottom, there is a link to 'Sugerir edição · É o proprietário desta empresa?'.

Figure 1: Localização Sintanet

2.1.1. WhoIs

A primeira tentativa de recolha de dados foi através do **WHOIS**, onde obtivemos as seguintes informações:

```
# whois.dns.pt

Domain: sintanet.pt
Domain Status: Registered
Creation Date: 18/10/2011 01:27:39
Expiration Date: 18/10/2026 23:59:39
Owner Name:
Owner Address:
Owner Locality:
Owner ZipCode:
Owner Locality ZipCode:
Owner Country Code:
Owner Email:
Admin Name:
Admin Address:
Admin Locality:
Admin ZipCode:
Admin Locality ZipCode:
Admin Country Code:
Admin Email:
Name Server: ns2.bsous.pt | IPv4: 185.15.23.147 and IPv6:
Name Server: ns1.bsous.pt | IPv4: 130.185.86.152 and IPv6:
```

Figure 2: WHOIS da sintanet.pt

Através desta informação concluimos que a Sintanet possui o domínio “*sintanet.pt*” registado desde 2011 e com validade até 2026, sem informações públicas do proprietário, e utiliza servidores com os nomes geridos pela bsous.pt. A Bsous atua como um facilitador para que as empresas possam criar e gerir os seus negócios digitais de forma eficiente e escalável, garantindo também um bom desempenho nas operações online.

Através do serviço WHOIS, foi ainda possível obter informações adicionais sobre a infraestrutura do site. Constatou-se que este utiliza o servidor web NGINX, uma escolha popular devido à sua elevada eficiência no processamento de grandes volumes de tráfego e à sua flexibilidade para servir conteúdos dinâmicos e estáticos.

Registrar Info		Site Status	
Name		Status	Active
Referral URL		Server Type	nginx
Status			

Figure 3: WHOIS da sintanet.pt (2)

2.1.2. HTTP

Ao aceder ao site da Sintanet, salta imediatamente à vista a utilização do protocolo HTTP em detrimento do HTTPS, o que abre espaço para diversas vulnerabilidades de segurança. Quando um site utiliza HTTP, os dados transmitidos entre o servidor e o navegador não são criptografados, o que os torna suscetíveis a interceptações e manipulações por atacantes. Isso inclui informações sensíveis, como credenciais de login, dados pessoais e até dados bancários.

Seguem as vulnerabilidades mais críticas causadas por não usar HTTPS:

- **Interceptação de Dados (Ataque Man-in-the-Middle):** Os dados enviados por HTTP podem ser interceptados por atacantes em redes públicas ou vulneráveis, permitindo que roubem informações sensíveis, como senhas e informações pessoais.
- **Integridade dos Dados Comprometida:** Como os dados não são criptografados, eles podem ser alterados durante o trajeto, permitindo que atacantes injetem scripts maliciosos ou modifiquem o conteúdo da comunicação.
- **Falta de Autenticidade do Servidor:** Sem HTTPS, não há garantia de que o site acessado seja realmente o sintanet.pt. Isso pode abrir portas para ataques de phishing, onde os utilizadores podem ser redirecionados para sites fraudulentos que se tentem passar por legítimos.

Recorrendo ao comando ***curl -i*** (sendo a *flag -i* utilizada para incluir os cabeçalhos da resposta HTTP), foi possível confirmar a utilização do protocolo HTTP no site da Sintanet, bem como identificar a versão do PHP em uso.

```
[(base) jony@NULL Desktop % curl -I http://www.sintanet.pt
HTTP/1.1 303 See other
Server: nginx
Date: Thu, 03 Apr 2025 14:02:25 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
X-Powered-By: PHP/5.2.17
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: 34f89a0939fa77f620be6ec5f4ea84c1=b4495b678bbd3291377ffecd9d76c418; path=/
Location: http://www.sintanet.pt/pt/
Vary: User-Agent
X-Scale: YXBvY2FzQGdpdGh1Yg==
```

Figure 4: curl -I “http://www.sintanet.pt”^o

A versão de PHP detetada é consideravelmente desatualizada, o que torna o sistema vulnerável a diversas falhas de segurança, conforme ilustrado na imagem seguinte:

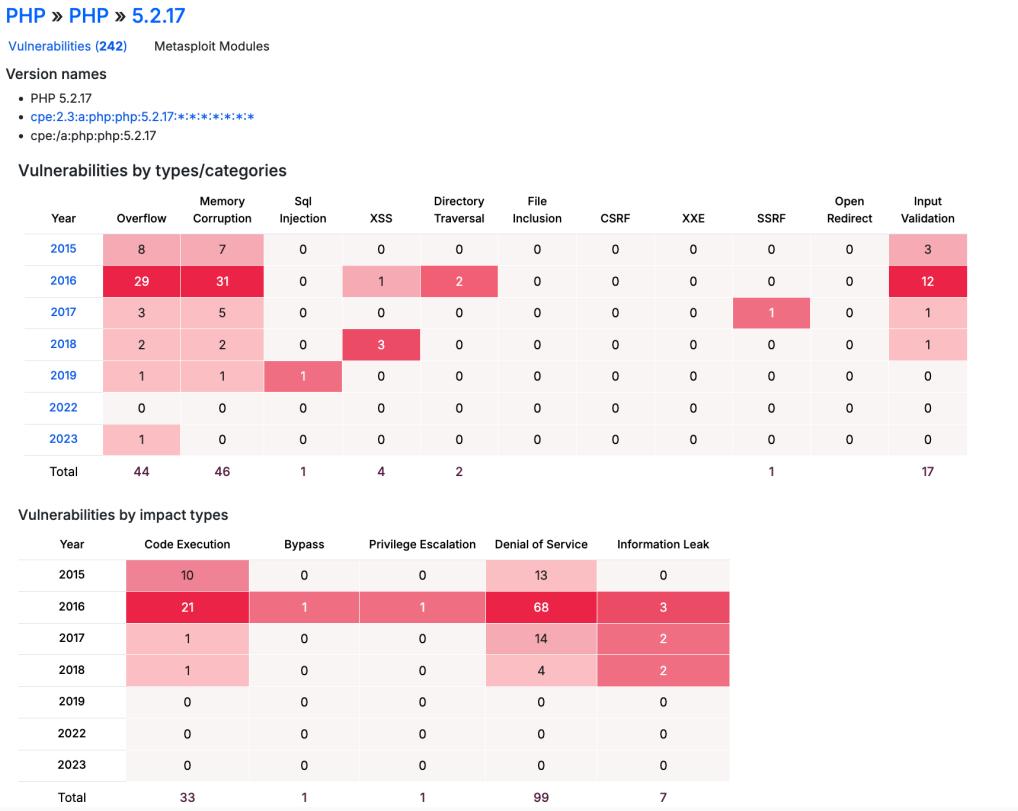


Figure 5: Vulnerabilidades PHP 5.2.17 (CVEdetails.com)

2.1.3. Utilizador do GitHub

Durante a análise do site sintanet.pt, foi possível obter informações adicionais através da descodificação de um campo específico no código HTML, o X-Scale. Este campo contém uma string codificada em Base64, que ao ser descodificada revelou o nome apocas@github . Essa informação parece ser uma pista, possivelmente vinculada a um utilizador do GitHub, mas não encontramos relações diretas entre este nome e o site sintanet.pt durante a restante pesquisa.

```
eduardo@eduardo-HP-Pavilion:~$ curl -I https://www.sintanet.pt
HTTP/2 301
server: nginx
date: Wed, 23 Apr 2025 13:30:39 GMT
content-type: text/html; charset=iso-8859-1
location: http://www.sintanet.pt/
cache-control: max-age=0
expires: Wed, 23 Apr 2025 13:30:39 GMT
x-scale: YXBvY2FzQGdpdGh1Yg==
```

Figure 6: String X-Scale em Base64

2.1.4. 404

De seguida, procedeu-se à verificação do tratamento da página de erro 404 Not Found. A ausência de um tratamento adequado poderia expor informações sensíveis sobre a tecnologia ou a versão do servidor em utilização. Verificou-se, no entanto, que a página de erro 404 está devidamente tratada: ao tentar aceder a URLs inexistentes, o site “www.sintanet.pt” redireciona automaticamente essas ligações para a página principal da loja, em vez de apresentar a típica mensagem de erro 404.

2.1.5. IP

Após a realização de um teste de ping, foi possível identificar o endereço IP associado ao servidor. Utilizando ferramentas de pesquisa online, como o IP Lookup, verificou-se que o servidor encontra-se alojado em Tomar, Santarém.

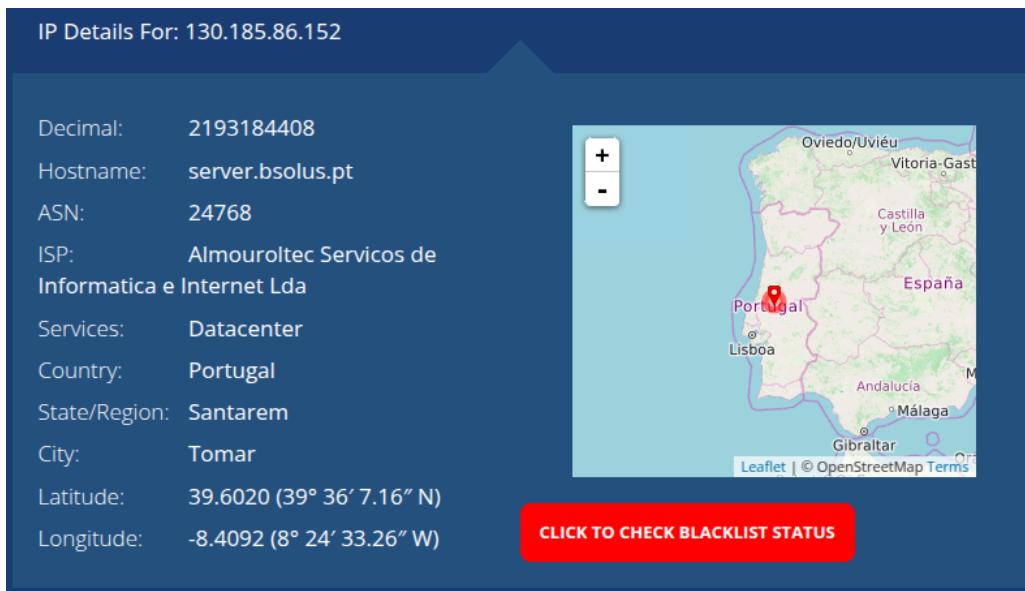


Figure 7: Localização do IP da Sintanet

2.1.6. BuiltWith

O BuiltWith é uma ferramenta extremamente útil para identificar as tecnologias utilizadas por websites, incluindo frameworks, sistemas de gestão de conteúdos (CMS), servidores e bibliotecas. Através de uma análise realizada nesta plataforma, foi possível verificar que o site da Sintanet utiliza a biblioteca jQuery, especificamente a versão 1.8.3.

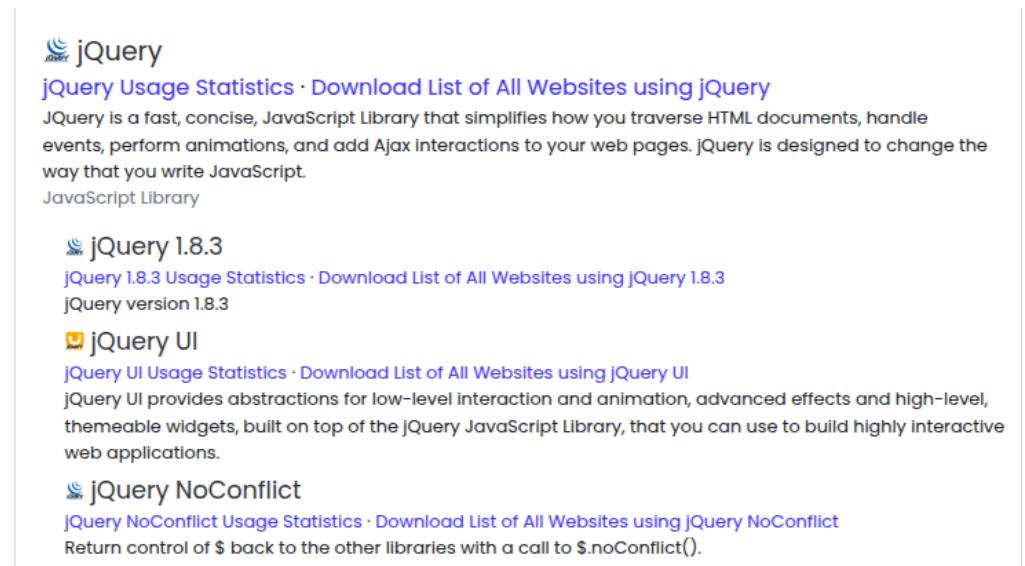


Figure 8: BuiltWith Sintanet.pt

Com base nesta informação, foi possível pesquisar e analisar as vulnerabilidades conhecidas associadas à versão 1.8.3 do jQuery. Sendo uma versão desatualizada e sem atualizações de segurança, ela contém várias falhas documentadas, algumas das quais podem ser exploradas por agentes maliciosos.

CVE-2012-6708

jQuery before 1.9.0 is vulnerable to Cross-site Scripting (XSS) attacks. The `jQuery(strlput)` function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '`<`' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '`<`' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Source: MITRE

Figure 9: Vulnerabilidade 1 associada ao jQuery 1.8.3 (CVEdetails.com)

CVE-2015-9251

jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the `dataType` option, causing text/javascript responses to be executed.

Source: MITRE

Figure 10: Vulnerabilidade 2 associada ao jQuery 1.8.3 (CVEdetails.com)

Prototype Pollution

Affecting [jquery](#) package, versions `<3.4.0`

INTRODUCED: 26 MAR 2019 [CVE-2019-11358](#) ⓘ [CWE-1321](#) ⓘ

How to fix?

Upgrade `jquery` to version 3.4.0 or higher.

Overview

[jquery](#) is a package that makes things like HTML document traversal and manipulation, event handling, animation, and Ajax much simpler with an easy-to-use API that works across a multitude of browsers.

Affected versions of this package are vulnerable to Prototype Pollution. The `extend` function can be tricked into modifying the prototype of `Object` when the attacker controls part of the structure passed to this function. This can let an attacker add or modify an existing property that will then exist on all objects.

Note: CVE-2019-5428 is a duplicate of CVE-2019-11358

Figure 11: Vulnerabilidade 3 associada ao jQuery 1.8.3 (CVEdetails.com)

2.1.7. Robots

A diretoria ‘robots’ refere-se ao arquivo `robots.txt`, utilizado pelos websites para informar os motores de busca (como o Google, por exemplo) sobre quais páginas ou diretórias do site devem ser acessados ou ignorados durante o processo de indexação. Ao procurar por este arquivo, obtemos as seguintes diretórias:

```

eduardo@eduardo-HP-Pavilion:~$ curl -X GET "http://www.sintanet.pt/robots.txt"
## Pastas Bloqueadas
User-agent: *
Disallow: /administrator/
Disallow: /assinaturas/
Disallow: /BsolusCach/
Disallow: /cgi-bin/
Disallow: /cli/
Disallow: /components/
Disallow: /imagens/
Disallow: /images/sampledata
Disallow: /includes/
Disallow: /installation/
Disallow: /language/
Disallow: /libraries/
Disallow: /logs/
Disallow: /loja5_form/
Disallow: /media/
Disallow: /modules/
Disallow: /PIIDs/
Disallow: /catalogo/
Disallow: /plugins/
Disallow: /templates/
Disallow: /tmp/
Disallow: /ipay/
Disallow: /n/

## NOVAS REGRAS GOOGLE ALGORITMO
Allow: /modules/mod_reslider/assets/
Allow: /templates/bsoluslayout/css/
Allow: /templates/bsoluslayout/images/
Allow: /templates/bsoluslayout/js/
Allow: /templates/loja5responsivo/images/
Allow: /cache/sitemap/

## SiteMap
Sitemap: http://www.sintanet.pt/sitemap.xml

```

Figure 12: GET robots.txt

Ao fazer o comando `get` na diretoria administrador apresentada no ficheiro “*robots.txt*”, encontramos uma página web que não conseguimos aceder no browser

```

eduardo@eduardo-HP-Pavilion:~$ curl -X GET "http://www.sintanet.pt/administrator/"
<!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" xml:lang="pt-pt" lang="pt-pt" dir="ltr">
<head>
    <meta http-equiv="content-type" content="text/html; charset=utf-8" />
    <meta name="robots" content="index, follow" />
    <meta name="keywords" content="Venda de telemóveis,Acessórios, Acessórios de Smartphones, Reparação de Smartphones, Smart
sórios Telemóveis, Apple, Nokia, Sony Ericsson, Motorola, Samsung, LG, Tm, Vodafone, Optimus, Capas, Baterias, Flex, Touch
Huawei, Componentes, ZTE, ZTE, Playstation, Xbox, PSP, Consolas, Reparação Consolas, Revenda Telemóveis, Informatica, Pelic
aptador, aeg, alcatel, antenas, apple, asus, audio, auriculares, baku, bateria, blackberry, bolsas, book, cabos, canon, cap
splays, dooge, dual, externos, ferramentas, gps, headphones, htc, huawei, ics, internet, ipad, iphone, iphone/ipad, ipod, i
pen, placas, portatil, psp, redes, samsung, sony, stylus/canetas, tablets, teclados, toshiba, touchscreen, touchscreens, vo
Reparar Samsung" />
    <meta name="description" content="A Sintanet.pt é uma loja online destinada ao comércio de produtos na área das telecomun
rios e componentes.

Venda de telemóveis,Acessórios, Acessórios de Smartphones, Reparação de Smartphones, Smartphones, Loja, Sintanet, Loja Tele
Sony Ericsson, Motorola, Samsung, LG, Tm, Vodafone, Optimus, Capas, Baterias, Flex, Touchscreens, Cabo Dados, Displays, Ca
aystation, Xbox, PSP, Consolas, Reparação Consolas, Revenda Telemóveis, Informatica, Peliculas, Bolsas Silicone, Capas Sili
<meta name="generator" content="DEVELOPED BY BSOLUS.PT" />
<title> Sintanet.pt - Venda de telemóveis, Acessórios e Reparação de Smartphones - Administração</title>
<link href="/administrator/templates/bsolus/favicon.ico" rel="shortcut icon" type="image/vnd.microsoft.icon" />
<link rel="stylesheet" href="templates/system/css/system.css" type="text/css" />
<link rel="stylesheet" href="templates/bsolus/css/template.css" type="text/css" />
<style type="text/css">
```

Figure 13: GET /administrador/

Prometemos solenemente que não tentámos fazer login, nem muito menos contornar o processo.

Ao tentar aceder ao diretório ‘tmp’ através de um pedido GET, é retornado um erro 403, indicando que o acesso está restrito. O mesmo ocorre ao tentar aceder às diretórias de logs, onde o servidor impede o acesso a essas informações. Este comportamento é um mecanismo de segurança que visa proteger dados sensíveis e evitar acessos não autorizados a áreas críticas do sistema.

```
eduardo@eduardo-HP-Pavilion:~$ curl -X GET "http://www.sintanet.pt/tmp/"<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>403 Forbidden</title></head><body><h1>Forbidden</h1><p>You don't have permission to access this resource.</p><p>Additionally, a 403 Forbidden error was encountered while trying to use an ErrorDocument to handle the request.</p></body></html>eduardo@eduardo-HP-Pavilion:~$
```

Figure 14: GET /tmp/

2.1.8. Openssl

Foi utilizado o comando `openssl s_client -connect sintanet.pt:443` com o objetivo de verificar a presença e a configuração de uma ligação segura (HTTPS) no servidor sintanet.pt. A ligação foi estabelecida com sucesso, demonstrando que o servidor escuta na porta 443 e suporta conexões TLS.

Durante esta análise, verificou-se que o servidor apresenta um certificado digital válido, emitido pela autoridade certificadora Let's Encrypt, associado ao domínio *.sintanet.pt. O certificado utiliza uma cifra considerada segura (ECDHE-RSA-AES256-GCM-SHA384) e uma chave pública RSA de 2048 bits, o que garante um bom nível de segurança criptográfica.

Contudo, apesar de o servidor possuir uma configuração HTTPS funcional, foi observado, através de comandos como `curl -I https://sintanet.pt`, que o site redireciona automaticamente as ligações HTTPS para HTTP (nomeadamente para `http://www.sintanet.pt`), utilizando um redirecionamento permanente (código 301).

Esta prática é fortemente desaconselhada, pois força o utilizador a abandonar uma ligação segura (HTTPS) em favor de uma ligação não segura (HTTP), deixando a comunicação vulnerável a ataques como man-in-the-middle, interceptação de dados e alteração do conteúdo transmitido.

O comportamento ideal seria o oposto: todas as ligações HTTP deveriam ser redirecionadas para HTTPS, garantindo que toda a interação com o site ocorra através de um canal encriptado e confiável.

2.1.9. Conclusões relativas à Sintanet

Em síntese, a análise passiva de Sintanet evidenciou que, embora o domínio esteja ativo desde 2011 e utilize servidores NGINX bem dimensionados, há diversas lacunas de segurança decorrentes da falta de adoção consistente de HTTPS e de componentes desatualizados. O site força o downgrade de HTTPS para HTTP, expondo tráfego a interceptações, e opera com PHP 5.2.17 e jQuery 1.8.3, ambos com vulnerabilidades conhecidas.

Recomenda-se, portanto, a ativação e imposição de HTTPS (preferencialmente com TLS 1.3), atualização imediata do PHP e das bibliotecas JavaScript, bem como revisão das regras de acesso a diretórios críticos, de modo a mitigar riscos de interceptação, execução de código malicioso e divulgação de informações sensíveis

2.2. Nike

Como grande corporação que realiza as suas operações comerciais através de serviços online, escolhemos a Nike.

2.2.1. WhoIs

A primeira abordagem consistiu em pesquisar o domínio **nike.com** no serviço **WHOIS**.

Registrar Info

Name	MarkMonitor Inc.
Whois Server	whois.markmonitor.com
Referral URL	http://www.markmonitor.com
Status	clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited clientTransferProhibited https://icann.org/epp#clientTransferProhibited clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited serverTransferProhibited https://icann.org/epp#serverTransferProhibited serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited

Important Dates

Expires On	2026-03-05
Registered On	1995-03-04
Updated On	2024-02-02

Figure 15: WHOIS de nike.com

```

Registrant Contact Information:
Name: Internet Domain Administrator
Organization: Nike, Inc.
Address Line 1: One Bowerman Drive, DF/4
Address Line 2:
City: Beaverton
State/Province: OR
Postal Code: 97005
Country: US
Phone: +1.5036716453
Fax:
Email: internet.domain.administrator@nike.com
Full Address: One Bowerman Drive, DF/4, Beaverton, OR, 97005, US

Administrative Contact Information:
Name: Internet Domain Administrator
Organization: Nike, Inc.
Address Line 1: One Bowerman Drive, DF/4
Address Line 2:
City: Beaverton
State/Province: OR
Postal Code: 97005
Country: US
Phone: +1.5036716453
Fax:
Email: internet.domain.administrator@nike.com
Full Address: One Bowerman Drive, DF/4, Beaverton, OR, 97005, US

Tech Contact Information:
Name: Internet Domain Administrator
Organization: Nike, Inc.
Address Line 1: One Bowerman Drive, DF/4
Address Line 2:
City: Beaverton
State/Province: OR
Postal Code: 97005
Country: US
Phone: +1.5036716453
Fax:
Email: internet.domain.administrator@nike.com
Full Address: One Bowerman Drive, DF/4, Beaverton, OR, 97005, US

Information Updated: 2025-03-26 12:15:30.538952+00

```

Figure 16: WHOIS de nike.com (detalhes)

É fácil perceber que os nomes de domínio não estão diretamente associados ao verdadeiro proprietário, mas sim à MarkMonitor, uma empresa especializada em software para a proteção de marcas corporativas contra falsificação, fraude, pirataria, entre outros riscos.

Outras informações, como a localização, o número de telefone e o email, referem-se à sede principal da Nike nos Estados Unidos, não expondo, assim, quaisquer dados pessoais no seu registo de domínio.



Figure 17: Sede principal da Nike

2.2.2. Vagas de Trabalho

Outra abordagem consistiu em pesquisar vagas de trabalho na área de informática para verificar se havia informações sensíveis expostas, como as tecnologias utilizadas e as respetivas versões.

Através de Google Dorks simples, como “nike” & “IT” & “job” ou “nike” & “Software” & “job”, foi possível encontrar várias oportunidades de emprego para funções na área de software no site oficial da Nike.

Exemplo de vaga de emprego:

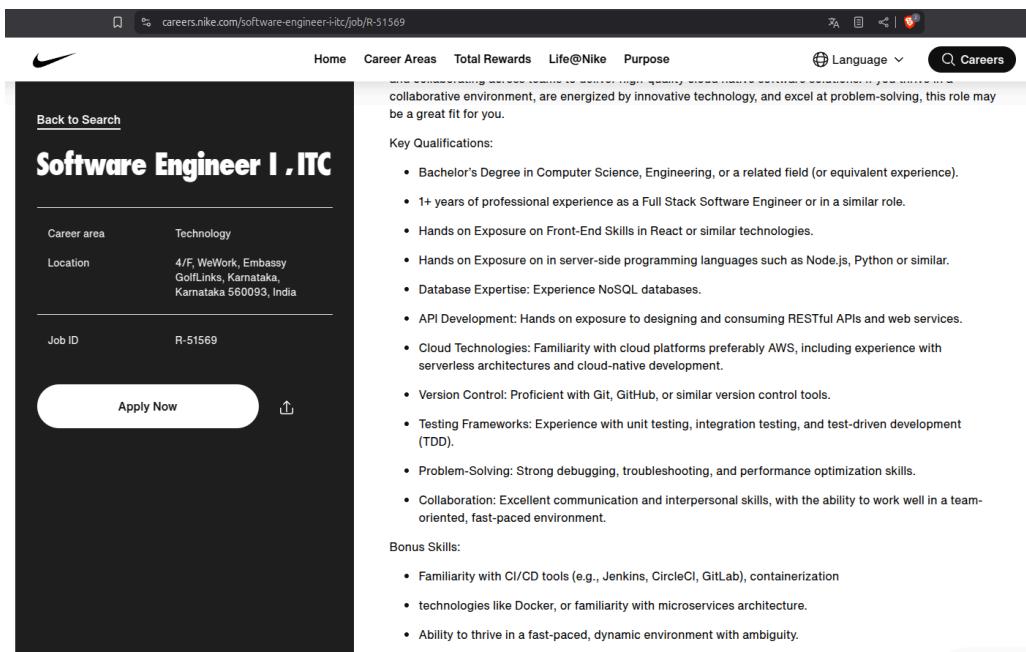


Figure 18: Vaga de Emprego Nike

As a Software Engineer I, you will:

- Design & Develop: Build, test, and maintain scalable web applications and services. Work on both front-end and back-end development to deliver end-to-end functionality.
- Collaborate: Work closely with product managers, designers, and other engineers to define requirements, technical specifications, and deliver quality software.
- Front-End Development: Implement dynamic, responsive, and user-friendly web interfaces using modern JavaScript frameworks (React).
- Back-End Development: Design and implement RESTful APIs, microservices, and backend services using technologies like Node.js, Python or similar.
- Database Management: Develop NoSQL databases, ensuring efficient data storage and retrieval.
- Testing & Quality Assurance: Write unit tests, integration tests, and maintain high code quality standards using tools such as Jest, Mocha, or similar.
- Performance Optimization: Identify and fix performance bottlenecks across the full stack,
- ensuring high availability and responsiveness. CI/CD Integration: Integrate with and maintain continuous integration/continuous deployment (CI/CD) pipelines for seamless software delivery.
- Agile Methodologies: Participate in Agile processes, including sprint planning, daily stand-ups, code reviews, and retrospectives.

Figure 19: Vaga de Emprego Nike (Detalhes)

Nesta vaga, é possível observar que são requisitadas diversas tecnologias, como Python, Node.js, bases de dados NoSQL, bem como informações sobre a arquitetura utilizada, por exemplo: “*Technologies like Docker, or familiarity with microservices architecture.*”

Isto sugere que a Nike assenta a sua infraestrutura numa arquitetura de microserviços, utilizando Docker para a gestão dos seus containers.

Outros detalhes encontrados incluem:

- **Front-End Development:** Implementação de interfaces web dinâmicas e responsivas com frameworks modernos de JavaScript, como React.

- **Back-End Development:** Desenvolvimento de APIs RESTful, microserviços e serviços backend com tecnologias como Node.js e Python.
- **Database Management:** Utilização de bases de dados NoSQL para armazenamento e recuperação eficiente de dados.
- **Testing & Quality Assurance:** Escrita de testes unitários e de integração, garantindo elevados padrões de qualidade de código com ferramentas como Jest e Mocha.

Além desta, foram encontradas outras ofertas de emprego. Com base nestas vagas, acreditamos que a Nike utiliza hospedagem AWS e frameworks como Next.js. Algumas descrições mencionam tanto React como Next.js, o que pode ser uma estratégia da Nike para confundir curiosos como nós. No entanto, mais adiante procuraremos determinar se a empresa utiliza efetivamente Next.js ou React.

Foi também encontrada uma oportunidade de emprego na área de redes:

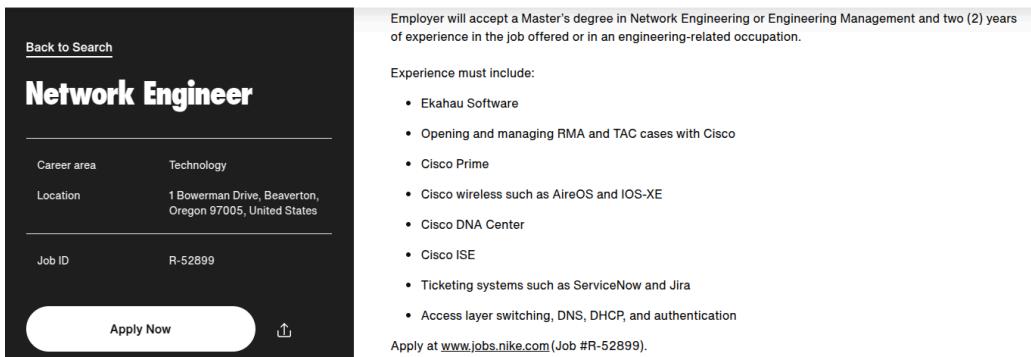


Figure 20: Vaga de Emprego Nike na Área de Redes

Esta vaga menciona tecnologias como Cisco ISE e DNA Center, ferramentas avançadas para gestão e automação de redes, bem como controlo de identidade e acesso. Isto sugere que a Nike investe fortemente em políticas rigorosas de controlo de acessos, reduzindo o risco de invasões.

2.2.3. Página Web

Saltámos então para o site da Nike e analisámos o código da página web. Felizmente (ou infelizmente, dependendo do ponto de vista), nada no código disponibilizado na web indicava explicitamente o uso de uma framework específica. O site apresentava HTML simples com alguns scripts de monitorização.

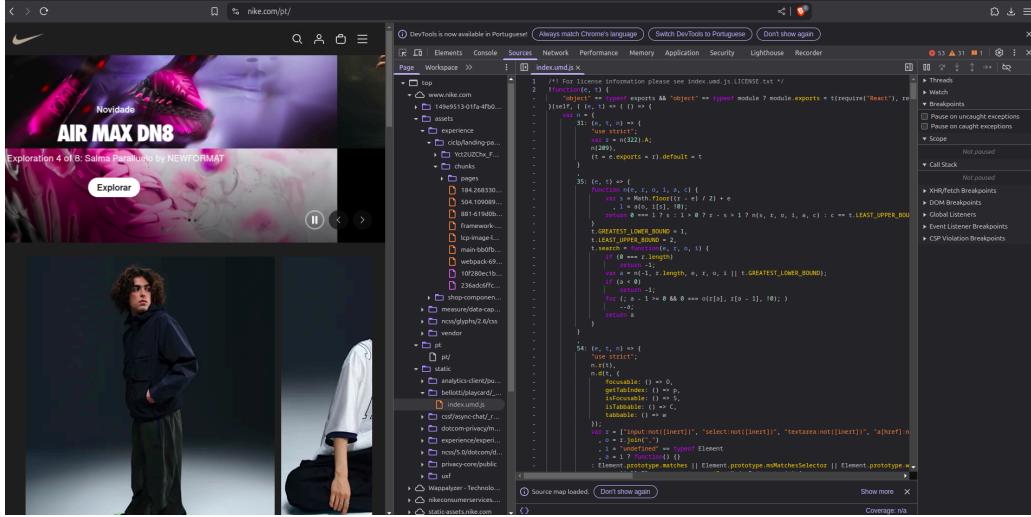


Figure 21: Inspeção do Site da Nike (Aba Sources)

Ao analisar mais detalhadamente a aba Network, foi possível verificar que o servidor está, de facto, hospedado em Amazon S3. Além disso, identificámos que a encriptação no lado do servidor (Server-Side Encryption) utiliza o algoritmo AES-256.

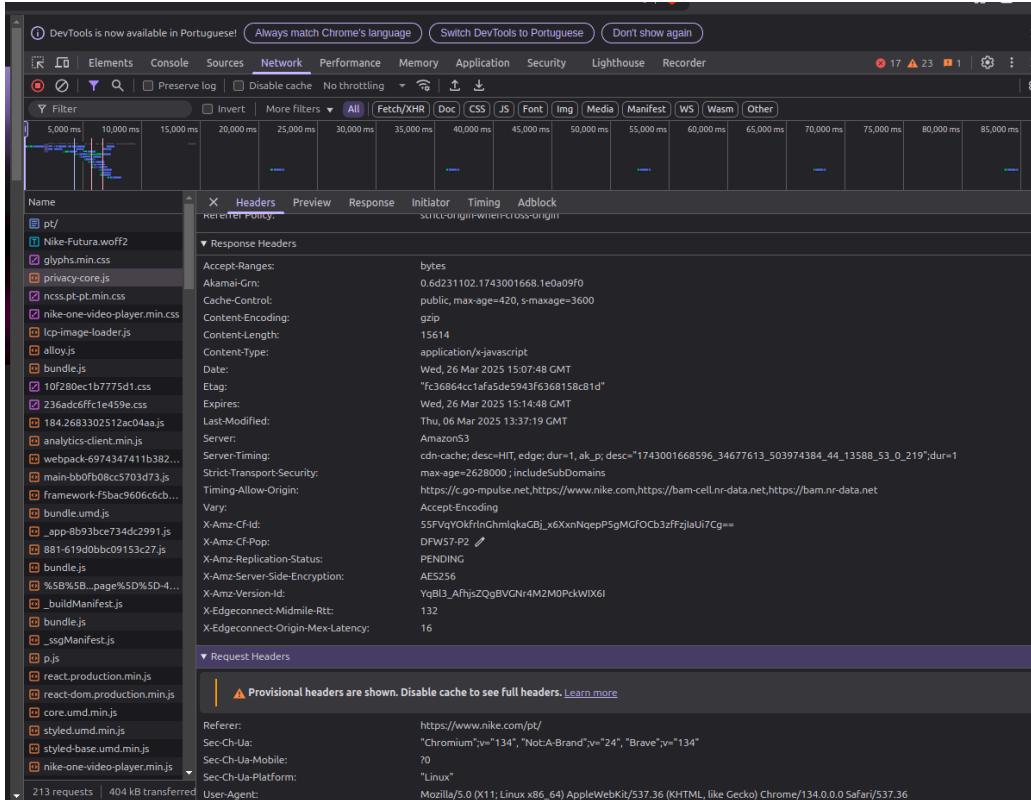


Figure 22: Inspeção do Site da Nike (Aba Network)

Na aba Security, além de confirmarmos o uso de AES-256, também verificámos que a comunicação é protegida com TLS 1.3, e que o site utiliza certificados SHA-2 emitidos pela DigiCert.

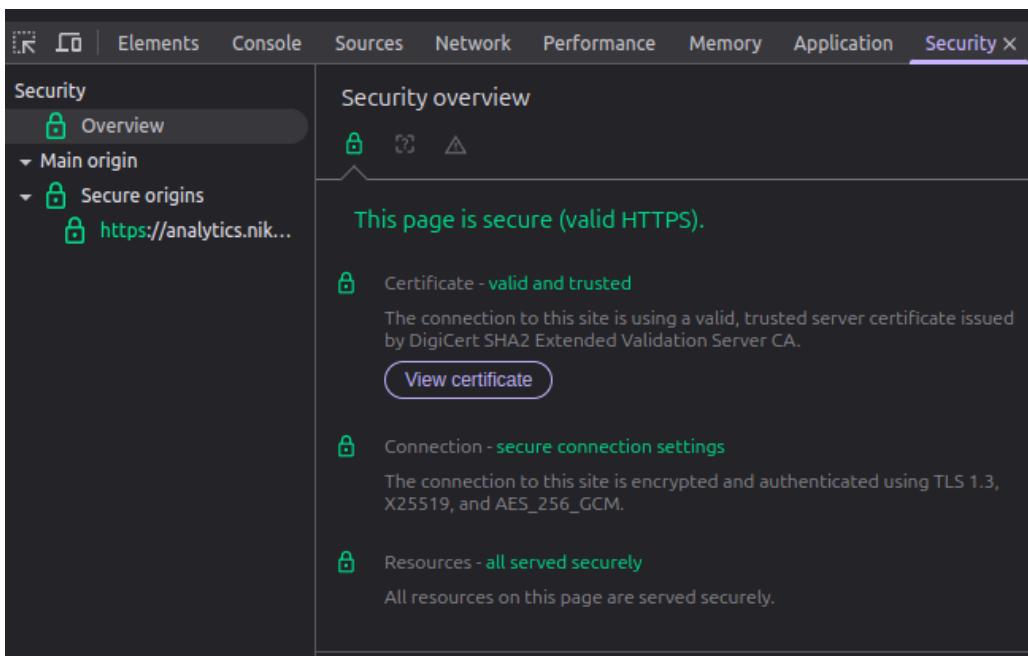


Figure 23: Inspeção do Site da Nike (Aba Security)

2.2.4. 404

De seguida, tentamos aceder a uma página inexistente no domínio da Nike. Se a página 404 Not Found não estivesse devidamente tratada, poderia revelar informações sobre a tecnologia ou a versão do servidor em uso. No entanto, o erro 404 estava corretamente configurado, não expondo nenhum detalhe sensível.

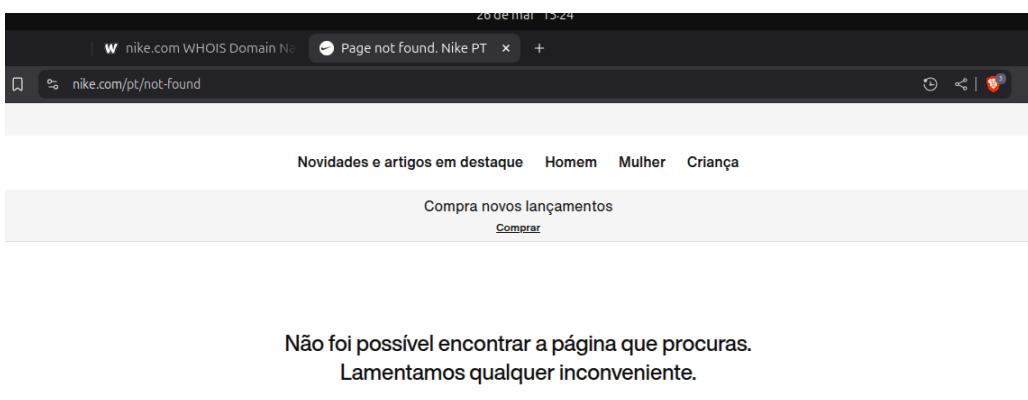


Figure 24: Nike 404

2.2.5. IP

Outra análise que realizámos foi executar um ping diretamente ao site da Nike, o que nos permitiu descobrir o IP associado ao seu DNS.

```

eduardo@eduardo-HP-Pavilion:~$ ping www.nike.com
PING e2785.x.akamaiedge.net (104.83.192.90) 56(84) bytes of data.
64 bytes from a104-83-192-90.deploy.static.akamaitechnologies.com (104.83.192.90)
: icmp_seq=1 ttl=53 time=18.8 ms
64 bytes from a104-83-192-90.deploy.static.akamaitechnologies.com (104.83.192.90)
: icmp_seq=2 ttl=53 time=38.8 ms
64 bytes from a104-83-192-90.deploy.static.akamaitechnologies.com (104.83.192.90)
: icmp_seq=3 ttl=53 time=84.2 ms
64 bytes from a104-83-192-90.deploy.static.akamaitechnologies.com (104.83.192.90)
: icmp_seq=4 ttl=53 time=132 ms
64 bytes from a104-83-192-90.deploy.static.akamaitechnologies.com (104.83.192.90)
: icmp_seq=5 ttl=53 time=24.8 ms
64 bytes from a104-83-192-90.deploy.static.akamaitechnologies.com (104.83.192.90)
: icmp_seq=6 ttl=53 time=105 ms
64 bytes from a104-83-192-90.deploy.static.akamaitechnologies.com (104.83.192.90)
: icmp_seq=7 ttl=53 time=42.9 ms
^C
--- e2785.x.akamaiedge.net ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6011ms
rtt min/avg/max/mdev = 18.800/63.788/132.484/40.369 ms
eduardo@eduardo-HP-Pavilion:~$ 

```

Figure 25: Ping ao site da Nike

Com o IP obtido, utilizámos motores de busca online para determinar a sua localização. Descobrimos que está associado a Madrid, Espanha, e que pertence à Akamai Technologies, o que sugere que se trata de um CDN (Content Delivery Network).

All IP Ranges > 104.0.0.0/8 > 104.83.0.0/16 > 104.83.192.0/24 > 104.83.192.90

104.83.192.90

Flag Madrid, Madrid, Spain

hosting webserver

Summary	
ASN	AS16625 - Akamai Technologies, Inc.
Hostname	a104-83-192-90.deploy.static.akamaitechnologies.com
Range	104.83.192.0/22
Company	Akamai International, BV
Hosted domains	0
Privacy	True
Anycast	False
ASN type	Hosting

Figure 26: Localização do IP da Nike

Também executámos um cURL via terminal para tentar obter mais informações sobre o servidor. Esta ferramenta permite enviar requisições HTTP e analisar as respostas do servidor. Através desta técnica, conseguimos confirmar que a Nike utiliza Next.js, uma vez que o cabeçalho X-Powered-By indica Next.js.

```

eduardo@eduardo-HP-Pavilion:~$ curl -I https://www.nike.com/pt/
HTTP/2 200
content-type: text/html; charset=UTF-8
x-commerce-region: us-east-1
x-powered-by: Next.js
x-branch-name: main
x-build-number: 915
x-commit-sha: edb07c742
x-environment: production
content-security-policy: frame-ancestors 'self' *.nike.com *.nikecloud.com *.nikedev.com
x-frame-options: sameorigin
accept-ch: sec-ch-ua-model, sec-ch-ua-platform-version, sec-ch-ua-full-version-list
permissions-policy: ch-ua-model="https://sdk-api-v1.singular.net", ch-ua-platform-version="https://sdk-api-v1.singular.net", ch-ua-full-version-list="https://sdk-api-v1.singular.net"
etag: "133aykclgn445r"
x-b3-traceid: 4ecf7e13346a2f472d7dd4bb13c4a4c
server: unified-edge-router
cache-control: max-age=900
expires: Wed, 26 Mar 2025 15:41:46 GMT
date: Wed, 26 Mar 2025 15:26:46 GMT
strict-transport-security: max-age=2628000 ; includeSubDomains
akamai-grn: 0.6d231102.1743002806.1ele4566
server-timing: ak_p; desc="1743002806372_34677613_505300326_20592_13694_30_80_15";dur=1

```

Figure 27: cURL ao site da Nike

2.2.6. Openssl

De seguida, realizámos uma ligação segura ao site da Nike utilizando o OpenSSL com o comando: “***openssl s_client -connect www.nike.com:443***”. Usamos a porta 443 porque é a porta padrão para conexões HTTPS.

```

Post-Handshake New Session Ticket arrived:
SSL-Session:
Protocol : TLSv1.3
Cipher   : TLS_AES_256_GCM_SHA384
Session-ID: 4835E53D1C69AA367B5C9D64AD20A353ABE777529FCC8E413050F65F1CC663AB
Session-ID-ctx:
Resumption PSK: 10BA1D2200555ABEA1EC8A7DF40A02A75B15181563D9C3EBBB944C19BAD0ADCE70A36FB7176FA6EF73CB70A44E09AFEC
PSK identity: None
PSK identity hint: None
SRP username: None
TLS session ticket lifetime hint: 83100 (seconds)
TLS session ticket:
0000 - 00 00 0a e1 37 e2 0a c1-43 09 47 1a 2c e4 c2 9c ....7...C.G.,...
0010 - 66 1e 1c 00 02 54 b3 eb-18 aa 3d 6d 9a c5 ea a3 f....T....=m....
0020 - f2 e9 3a 31 33 8e bd 22-32 b7 06 8b f2 dc e9 09 ..:13.."2.....
0030 - 14 3b 13 b6 f4 37 4f f2-eb 58 97 d7 64 cf a9 fb .;....70..X..d...
0040 - 86 18 0e 46 f6 4f 0a da-b3 5f d6 38 0c 2e fd 7c ...F.0....8...|
0050 - 1c d2 0e 0f 23 d7 1b 60-56 d9 8f 8d 17 01 84 4a .....#..`V.....|
0060 - dd 47 47 08 5d 3e 00-92 57 99 56 97 9c 61 55 ..GG..>..W.V..aU
0070 - 76 05 ce cb 1b eb ab ff-03 45 ee 86 1a b2 3e 36 v.....E....>6
0080 - c4 3f b4 0a 5b 26 d5 51-a5 8d cd bc d2 f5 10 fb ?...[& Q.....
0090 - f6 3c 01 c2 2d bc 6a 05-ad e9 96 40 0b 12 25 22 .<....j....@..%"
00a0 - 86 63 56 91 db bb c9 21-b0 0b de d0 a1 90 37 a6 .cV.....!.....7.
00b0 - 78 e8 db 16 2c 19 b9 52-5b 43 54 22 d8 a9 83 02 x.....,R[CT".....
00c0 - c7 61 5f 8d 5b 3c fb f2-29 da 5b ff 0a 0e 78 ca .a..[<..). [...x.
00d0 - 84 e1 5d 72 d2 44 2f 3f-2a e7 ee 30 e8 1f 07 7c ..]r.D/?*..0...| 

Start Time: 1743002941
Timeout   : 7200 (sec)
Verify return code: 0 (ok)
Extended master secret: no
Max Early Data: 0

```

Figure 28: OpenSSL

Através desta análise, confirmámos o uso de TLS 1.3 e da cifra AES-256 para encriptação das comunicações.

Por fim, utilizámos o comando whatweb, que permite identificar tecnologias web utilizadas num site. O resultado confirmou que a Nike está a utilizar serviços da Akamai, indicando que a empresa está a hospedar e a distribuir o seu conteúdo através desta rede de servidores, o que melhora a performance e segurança do site.

```

eduardo@eduardo-HP-Pavilion:~$ whatweb https://www.nike.com
https://www.nike.com [403 Forbidden] Akamai-Global-Host, Cookies[anonymousId,geoloc,ni_d], Country[UNITED STATES][US], HTTPServer[Akamai GHost], IP[104.83.192.90], Strict-Transport-Security[max-age=2628000 ; includeSubDomains], Title[Access Denied], UncommonHeaders[x-referer-error,server-timing,akamai-grn]

```

Figure 29: Análise com WhatWeb

Para corroborar todas as informações descobertas até agora, utilizámos o motor de busca **WhatCMS**. Esta ferramenta permite identificar qual o CMS (Content Management System) e outras tecnologias utilizadas por um site.

Através desta análise, conseguimos confirmar todos os dados que recolhemos ao longo desta fase da investigação.

The screenshot shows the WhatCMS interface with the URL 'whatcms.org/?s=www.nike.com' in the address bar. The main title is 'What CMS Is This Site Using?' with a subtitle 'Currently detecting 1540 website powering technologies'. A search bar contains 'nike.com' and a button 'Detect CMS'. Below is a table with a green header '✓ Success' and a 'JSON' link. The table lists the technologies used by Nike.com:

Category	Software	Version
Static Site Generator, CMS, Web Framework, Web Server	Next.js	
Programming Language	Node.js	
CDN	Akamai	

Figure 30: Análise do CMS da Nike

2.2.7. Exposição de Informação

Para verificar se conseguíamos encontrar algo que estivesse online mas não deveria, utilizámos novamente Google Dorks. Com o seguinte prompt de pesquisa, tentámos encontrar relatórios financeiros da Nike: “**financial report site:nike.com filetype:pdf**”

Encontrámos alguns resultados, como se pode ver a seguir:

The screenshot displays the front page of Nike's financial report. It features the Nike swoosh logo at the top center. Below it, there are two contact sections: 'Investor Contact' (Paul Trussell, investor.relations@nike.com) and 'Media Contact' (Virginia Rustique-Petteni, media.relations@nike.com). The main title is 'NIKE, INC. REPORTS FISCAL 2024 FOURTH QUARTER AND FULL YEAR RESULTS'. A paragraph below states: 'BEAVERTON, Ore., June 27, 2024 — NIKE, Inc. (NYSE:NKE) today reported financial results for its fiscal 2024 fourth quarter and full year ended May 31, 2024.' A bulleted list follows, detailing financial highlights for the quarter and year. At the bottom, a quote from John Donahoe is provided, followed by a statement from Matthew Friend.

Figure 31: Relatório financeiro da Nike

(In millions, except per share data)	THREE MONTHS ENDED		% Change	TWELVE MONTHS ENDED		% Change
	5/31/2024	5/31/2023		5/31/2024	5/31/2023	
Revenues	\$ 12,606	\$ 12,825	-2%	\$ 51,362	\$ 51,217	0%
Cost of sales	6,972	7,230	-4%	28,475	28,925	-2%
Gross profit	5,634	5,595	1%	22,887	22,292	3%
Gross margin	44.7 %	43.6 %		44.6 %	43.5 %	
Demand creation expense	1,091	1,092	0%	4,285	4,060	6%
Operating overhead expense	2,997	3,282	-9%	12,291	12,317	0%
Total selling and administrative expense	4,088	4,374	-7%	16,576	16,377	1%
% of revenues	32.4 %	34.1 %		32.3 %	32.0 %	
Interest expense (income), net	(53)	(28)	—	(161)	(6)	—
Other (income) expense, net	(127)	3	—	(228)	(280)	—
Income before income taxes	1,726	1,246	39%	6,700	6,201	8%
Income tax expense	226	215	5%	1,000	1,131	-12%
Effective tax rate	13.1 %	17.3 %		14.9 %	18.2 %	
NET INCOME	\$ 1,500	\$ 1,031	45%	\$ 5,700	\$ 5,070	12%
Earnings per common share:						
Basic	\$ 0.99	\$ 0.67	48%	\$ 3.76	\$ 3.27	15%
Diluted	\$ 0.99	\$ 0.66	50%	\$ 3.73	\$ 3.23	15%
Weighted average common shares outstanding:						
Basic	1,508.0	1,536.5		1,517.6	1,551.6	
Diluted	1,516.7	1,556.3		1,529.7	1,569.8	
Dividends declared per common share	\$ 0.370	\$ 0.340		\$ 1.450	\$ 1.325	

Figure 32: Relatório financeiro da Nike (2)

Embora fosse interessante, não consideramos relevante para o nosso caso de estudo.

2.2.8. Data Breaches

Realizámos ainda uma busca exaustiva utilizando Google Dorks, Shodan e BuiltWith para procurar versões utilizadas pela Nike, bem como possíveis data leaks ou data breaches de credenciais. Felizmente, não encontramos nada. Além disso, não houve notícias ou informações relativas a breaches.

2.2.9. Wappalyzer

Também utilizámos a extensão de browser Wappalyzer para tentar identificar as versões das aplicações utilizadas pela Nike. Através da leitura da documentação oficial do Wappalyzer, acreditamos firmemente que este recorre apenas a métodos passivos para detetar frameworks e versões utilizadas nos sites. Com esta análise, obtivemos apenas algumas informações que corroboram as descobertas feitas anteriormente.

2.2.10. Inferência Node.js

Para finalizar a nossa análise, tendo em conta o uso do Next.js pela Nike e a recente vulnerabilidade crítica descoberta no Next.js (**CVE-2025-29927: Next.js Middleware Bypass Vulnerability**), acreditamos que, se estiverem a usar as versões 14 ou 15, estarão de certeza a utilizar as versões mais recentes para mitigar a vulnerabilidade identificada. No entanto, caso estejam a usar versões entre o Next.js 11 e 13, é provável que tenham implementado uma mitigação manual do problema, tornando impossível inferir a versão específica utilizada, caso usem versões mais antigas do Next.js.

2.2.11. Conclusões

Com tudo o que investigámos, consideramos a Nike uma empresa altamente segura. Para corroborar essa nossa conclusão, procurámos por algum tipo de cyber rating e encontramos que a Nike recebeu uma pontuação de 818 de 950 na plataforma UpGuard, uma avaliação muito alta para a empresa.

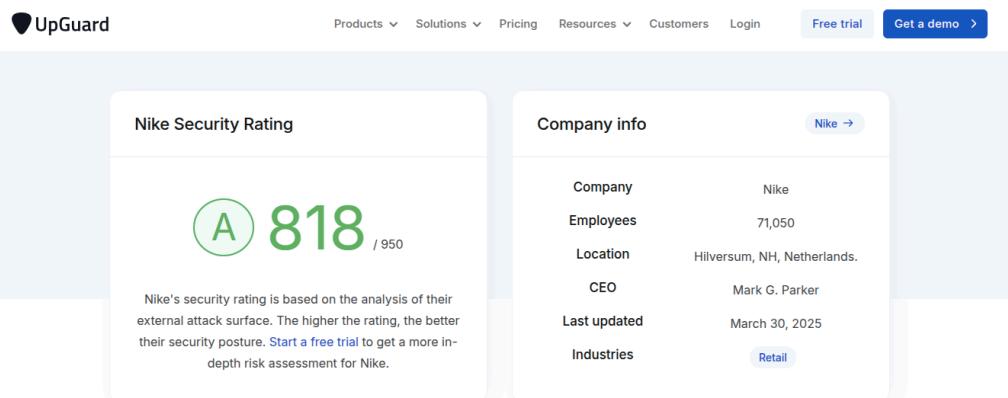


Figure 33: Cybersecurity rating da Nike

2.3. Conclusão Global da Parte A

Uma vez que já foram feitas conclusões para cada análise realizada (para a grande empresa e para a pequena), nesta conclusão global optámos por não voltar a referir detalhes técnicos, limitando-nos a destacar a comparação global.

A análise comparativa entre uma grande corporação, como a Nike, e uma empresa local de menor dimensão, como a Sintanet, revelou diferenças significativas na abordagem à segurança digital. As grandes empresas, como a Nike, adotam uma abordagem preventiva, investindo significativamente na sua segurança. Embora a sua superfície de ataque seja muito maior devido à sua escala, o elevado investimento permite-lhes mitigar eficazmente os riscos. Por outro lado, as pequenas empresas, como a Sintanet, frequentemente limitadas por recursos, têm uma superfície de ataque consideravelmente mais pequena, mas a falta de capacidade para investir em segurança coloca-as em risco, expondo-as a vulnerabilidades.

Posto isto, e embora os resultados obtidos, principalmente no caso da Nike, não tenham revelado grandes falhas (como seria de esperar), acreditamos ter estabelecido uma metodologia de trabalho eficaz e bastante sólida para recolher dados e gerar inferências úteis a partir das informações disponíveis.

Outro ponto que gostaríamos de abordar, embora não seja o foco deste relatório, refere-se à engenharia social. A extensa rede de colaboradores da Nike torna-a mais vulnerável, mesmo com as medidas de sensibilização adequadas. O elevado número de funcionários resulta numa superfície de ataque consideravelmente maior. Em contraste, a Sintanet apresenta uma superfície de ataque muito mais restrita, devido ao seu tamanho reduzido e à sua natureza local. Assim, caso a engenharia social fosse uma estratégia válida, seria muito exequível no caso da Nike, pois, entre tantos colaboradores, alguns poderiam ceder informações sensíveis. Já na Sintanet, a possibilidade de obter dados privilegiados ficaria limitada a um número muito restrito de funcionários, o que diminuiria substancialmente a probabilidade de sucesso.

3. Parte B

Nesta segunda parte do trabalho, foi realizada uma análise prática focada na varredura e identificação de vulnerabilidades em sistemas, dentro de um ambiente de testes controlado. O principal objetivo desta etapa é compreender como diferentes ferramentas e técnicas de auditoria podem ser aplicadas para detetar falhas de segurança num sistema alvo, avaliando os riscos associados e reforçando a postura de segurança dos mesmos.

Para garantir a segurança da rede local e preservar a integridade do ambiente de testes, foi utilizada uma rede privada isolada, implementada através de um ambiente de virtualização. O cenário de testes proposto inclui duas máquinas virtuais: uma com Kali Linux, que desempenha o papel de auditor, e outra com Metasploitable 2, configurada como sistema alvo.

A comunicação entre as máquinas foi configurada na gama de endereços IP 172.25.3.0/24, sendo o valor 3 correspondente ao número do grupo. Esta configuração permitiu uma simulação realista de um ambiente vulnerável, sem comprometer a segurança do sistema anfitrião, servindo de base para a aplicação de técnicas de varredura, análise de serviços expostos e avaliação de potenciais pontos de intrusão.

3.1. B1

A conexão foi estabelecida sem especificação manual da porta, tendo sido utilizada automaticamente a porta 23, sendo isto totalmente expectável, dado que a porta 23 é a predefinida para o protocolo Telnet. Foi também observado que o campo de checksum encontra-se desativado na captura efetuada.

Toda a comunicação entre cliente e servidor ocorre em *plaintext*, o que constitui uma vulnerabilidade, uma vez que permite a interceção e leitura direta dos dados transmitidos.

A sessão foi capturada com o Wireshark, sendo a análise feita com base nos ficheiros guardados. Para complementar, foram extraídas capturas de ecrã ilustrativas, onde se destacam os completeness flags, que indicam o estado e integridade das comunicações TCP, bem como as opções TCP negociadas durante o estabelecimento da ligação. No primeiro frame identificado como Telnet, é essencial observar as opções apresentadas no final do segmento, nomeadamente a negociação de capacidades entre cliente e servidor através dos comandos típicos do protocolo: DO, WILL, WON'T, DON'T. Estes comandos são fundamentais para o entendimento do funcionamento do Telnet, uma vez que determinam que funcionalidades (como ECHO) serão ativadas ou rejeitadas durante a sessão.

Paralelamente à comunicação Telnet, foram capturados pacotes DNS, entre os quais se destaca um standard query que acabou por ser retransmitido. Esta retransmissão pode indicar falhas temporárias na resolução de nomes ou ausência de resposta por parte do servidor DNS. Além disso, foram observadas respostas provenientes de mDNS (Multicast DNS), que são utilizadas para a resolução de nomes em redes locais sem a necessidade de um servidor DNS centralizado. Estas mensagens são comuns em ambientes onde dispositivos anunciam automaticamente os seus serviços, como acontece com o protocolo de host announcement ou browser protocol, usado por alguns sistemas para detetar e divulgar serviços de rede disponíveis.

As figuras abaixo ilustram alguns dos pontos mencionados: a primeira mostra os completeness flags associados à sessão Telnet, enquanto a segunda apresenta um frame DNS com retransmissão, incluindo respostas mDNS.

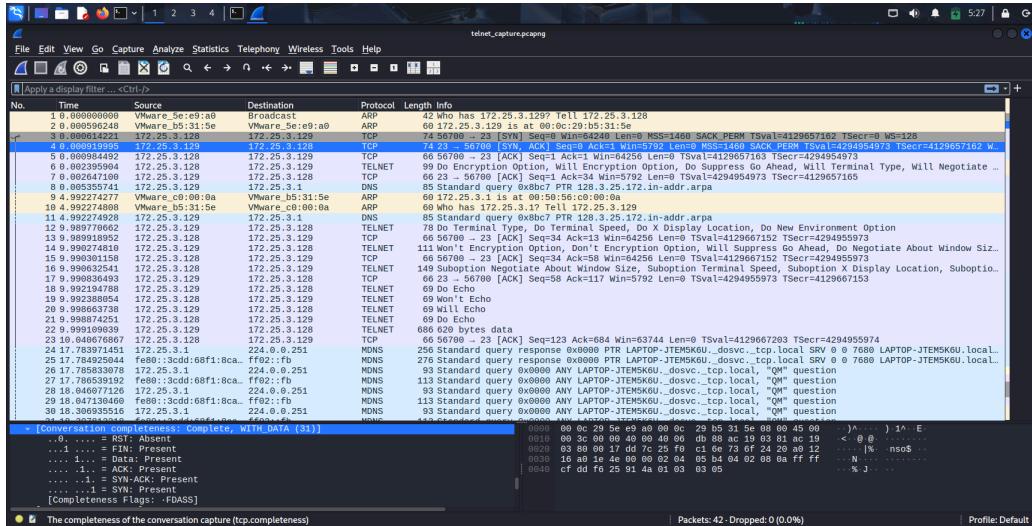


Figure 34: Flags de Completeness no Telnet

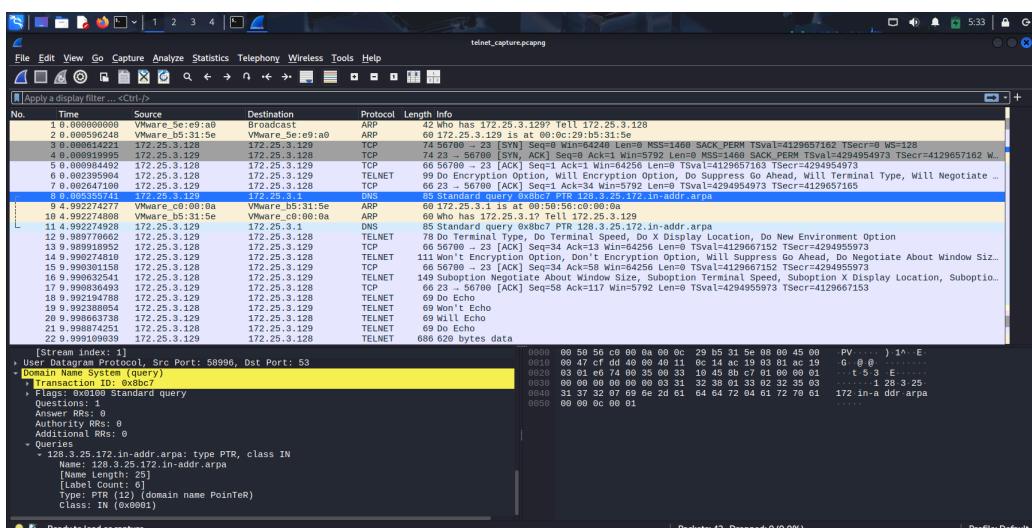


Figure 35: Frame DNS

3.2. B2

Para este exercício, utilizamos a ferramenta Nmap para realizar quatro varreduras distintas no sistema alvo, a explorar nas alíneas que se seguem.

```

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

```

Figure 36: Varreduras Nmap B2

3.2.1. B2.1

Foi realizada uma análise comparativa dos resultados das quatro varreduras Nmap ao host alvo, 172.25.3.129, um sistema Metasploitable 2. A primeira varredura teve como objetivo identificar portas abertas e serviços em execução, revelando 21 portas TCP ativas, incluindo serviços como FTP (vsftpd 2.3.4), SSH (OpenSSH 4.7p1), Telnet, HTTP (Apache 2.2.8), Samba, MySQL, VNC, IRC e Tomcat. Esta varredura permitiu também identificar o sistema operativo como Linux e obteve versões específicas dos serviços.

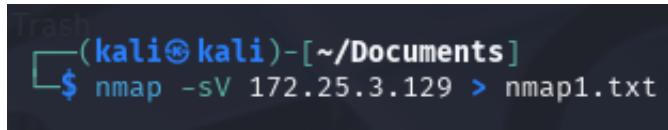
A screenshot of a terminal window titled 'Trash'. The command entered is '\$ nmap -sV 172.25.3.129 > nmap1.txt'.

Figure 37: Varredura 1 B2

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-07 05:56 EDT
Nmap scan report for 172.25.3.129
Host is up (0.0020s 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   open  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  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: 00:0C:29:B5:31:5E (VMware)
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 59.19 seconds
```

Figure 38: Resultado varredura 1 B2

A segunda varredura foi bastante limitada, incidindo apenas sobre a porta 80, com o intuito de verificar a presença do serviço HTTP, que confirmou a execução do Apache 2.2.8. Esta abordagem é útil apenas para uma verificação pontual da disponibilidade de um serviço web.

```
(kali㉿kali)-[~/Documents]
$ nmap -sV -p 80 172.25.3.129 > nmap2.txt

(kali㉿kali)-[~/Documents]
$ cat nmap2.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-07 06:00 EDT
Nmap scan report for 172.25.3.129
Host is up (0.00035s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
MAC Address: 00:0C:29:B5:31:5E (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/report.html
```

Figure 39: Varredura 2 e Resultado B2

Já a terceira varredura foi mais aprofundada, utilizando scripts de deteção de vulnerabilidades. Foram analisadas as mesmas portas da primeira varredura, mas com o diferencial de apresentar uma extensa lista de vulnerabilidades associadas a cada serviço, incluindo referências a CVEs e detalhes sobre possíveis exploits. Destacaram-se vulnerabilidades críticas como o backdoor no vsftpd 2.3.4 (CVE-2011-2523), falhas no OpenSSH, BIND e Apache, entre outras.

```
(kali㉿kali)-[~/Documents]
$ nmap -sV --script vulners 172.25.3.129 > nmap3.txt
```

Figure 40: Varredura 3

```

Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-07 06:05 EDT
Nmap scan report for 172.25.3.129
Host is up (0.0010s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ vulners:
|   vsftpd 2.3.4:
|     PACKETSTORM:162145      10.0
|     https://vulners.com/packetstorm/PACKETSTORM:162145      *EXPLOIT*
|     EDB-ID:49757      9.8      https://vulners.com/exploitdb/EDB-ID:49757
*_EXPLOIT*
|     CVE-2011-2523      9.8      https://vulners.com/cve/CVE-2011-2523
|     1337DAY-ID-36095      9.8      https://vulners.com/zdt/1337DAY-ID-36095
*_EXPLOIT*
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ vulners:
|   cpe:/a:openbsd:openssh:4.7p1:
|     2C119FFA-ECE0-5E14-A4A4-354A2C38071A      10.0
|     https://vulners.com/githubexploit/2C119FFA-ECE0-5E14-A4A4-354A2C38071A
*_EXPLOIT*
|     CVE-2023-38408      9.8      https://vulners.com/cve/CVE-2023-38408
|     CVE-2016-1908      9.8      https://vulners.com/cve/CVE-2016-1908
|     B8190CDB-3EB9-5631-9828-8064A1575B23      9.8
|     https://vulners.com/githubexploit/B8190CDB-3EB9-5631-9828-8064A1575B23
*_EXPLOIT*
|     8FC9C5AB-3968-5F3C-825E-E8DB5379A623      9.8
|     https://vulners.com/githubexploit/8FC9C5AB-3968-5F3C-825E-E8DB5379A623
*_EXPLOIT*
|     8AD01159-548E-546E-AA87-2DE89F3927EC      9.8
|     https://vulners.com/githubexploit/8AD01159-548E-546E-AA87-2DE89F3927EC
*_EXPLOIT*
|     5E6968B4-DBD6-57FA-BF6E-D9B2219DB27A      9.8
|     https://vulners.com/githubexploit/5E6968B4-DBD6-57FA-BF6E-D9B2219DB27A
*_EXPLOIT*
|     0221525F-07F5-5790-912D-F4B9E2D1B587      9.8
|     https://vulners.com/githubexploit/0221525F-07F5-5790-912D-F4B9E2D1B587
*_EXPLOIT*
|     95499236-C9FE-56A6-9D7D-E943A24B633A      8.9
|     https://vulners.com/githubexploit/95499236-C9FE-56A6-9D7D-E943A24B633A
*_EXPLOIT*
|     CVE-2015-5600      8.5      https://vulners.com/cve/CVE-2015-5600
|     SSV:78173      7.8      https://vulners.com/sebug/SSV:78173
*_EXPLOIT*
|     SSV:69983      7.8      https://vulners.com/sebug/SSV:69983
*_EXPLOIT*
|     PACKETSTORM:98796      7.8
|     https://vulners.com/packetstorm/PACKETSTORM:98796      *EXPLOIT*
|     PACKETSTORM:94556      7.8
|     https://vulners.com/packetstorm/PACKETSTORM:94556      *EXPLOIT*
|     PACKETSTORM:140070      7.8
|     https://vulners.com/packetstorm/PACKETSTORM:140070      *EXPLOIT*
|     PACKETSTORM:101052      7.8
|     https://vulners.com/packetstorm/PACKETSTORM:101052      *EXPLOIT*

```

Figure 41: Resultado varredura 3 B2 (continua)

A quarta varredura, por sua vez, utilizou o Nmap Scripting Engine (NSE) para recolher informações técnicas detalhadas sobre os serviços. Foi possível identificar, por exemplo, a permissão de login anónimo no FTP, chaves públicas disponíveis no SSH, suporte a comandos no SMTP, versão do BIND através do DNS, e informações do domínio no Samba. Também se obteve detalhes sobre os protocolos de autenticação no MySQL e no VNC, bem como a versão do kernel Linux.

```
$ nmap -A 172.25.3.129 > nmap4.txt
```

Figure 42: Varredura 4 B2

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-07 06:08 EDT
Nmap scan report for 172.25.3.129
Host is up (0.00075s 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:
|     STAT:
|       Connected to 172.25.3.128
|       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 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (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
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY,
ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
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)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_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   nfs
|   100003  2,3,4     2049/udp  nfs
|   100005  1,2,3     47283/tcp  mountd
|   100005  1,2,3     59621/udp mountd
|   100021  1,3,4     42670/udp nlockmgr
|   100021  1,3,4     60465/tcp  nlockmgr
|   100024  1          43539/tcp  status
|_ 100024  1          45389/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   open  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)
```

Figure 43: Resultado varredura 4 B2 (continua)

3.2.2. B2.2

As quatro varreduras Nmap geram diferentes níveis de tráfego e, por consequência, variam em termos de detectabilidade por parte de um sistema de deteção de intrusões em rede (NIDS), como o Suricata.

- nmap2 (varredura mínima à porta 80) produz tráfego muito limitado e específico. Esta abordagem é a menos ruidosa e, por isso, tem um impacto reduzido em termos de deteção.

Dependendo das regras configuradas no NIDS, pode passar despercebida, a não ser que existam alertas configurados para conexões suspeitas repetidas à porta 80.

- nmap1 (varredura geral com detecção de serviços) gera mais tráfego, já que envolve múltiplas tentativas de conexão e identificação de versões de serviços. Este tipo de atividade é comumente detetado por NIDS, especialmente se forem usadas técnicas como SYN scan, que são típicas de reconhecimento hostil.
- nmap3 (varredura com scripts de vulnerabilidades) tem impacto elevado em termos de tráfego e padrão de deteção. Scripts como os de identificação de CVEs geram tráfego com assinaturas claras e conhecidas de exploração ou enumeração de vulnerabilidades, sendo bastante propensos a gerar alertas num NIDS bem configurado.
- nmap4 (varredura com NSE focada em recolha técnica) também apresenta tráfego significativo, mas o seu impacto depende dos scripts usados. Muitos scripts do NSE imitam comportamentos de ataque ou exploração, o que pode desencadear alertas relacionados com enumeração, exploração de serviços ou recolha de credenciais.

3.2.3. B2.3

Segundo os logs de Suricata, durante o período de captura foram gerados 135 alertas e nenhum pacote foi descartado (0% de perda), o que indica uma monitorização eficaz da interface de rede. O motor foi iniciado com sucesso em modo IDS e carregou mais de 42 mil regras, incluindo regras IP-only, de payload e da camada de aplicação, o que reforça a capacidade do NIDS para detetar tráfego suspeito em diferentes camadas.

```
[74038 - Suricata-Main] 2025-04-07 07:13:54 Notice: suricata: This is Suricata
version 7.0.10 RELEASE running in SYSTEM mode
[74038 - Suricata-Main] 2025-04-07 07:13:54 Info: cpu: CPUs/cores online: 4
[74038 - Suricata-Main] 2025-04-07 07:13:54 Info: suricata: Setting engine mode
to IDS mode by default
[74038 - Suricata-Main] 2025-04-07 07:13:54 Info: exception-policy: master
exception-policy set to: auto
[74038 - Suricata-Main] 2025-04-07 07:13:54 Info: logopenfile: fast output
device (regular) initialized: fast.log
[74038 - Suricata-Main] 2025-04-07 07:13:54 Info: logopenfile: eve-log output
device (regular) initialized: eve.json
[74038 - Suricata-Main] 2025-04-07 07:13:54 Info: logopenfile: stats output
device (regular) initialized: stats.log
[74038 - Suricata-Main] 2025-04-07 07:14:01 Info: detect: 1 rule files
processed. 42826 rules successfully loaded, 0 rules failed, 0
[74038 - Suricata-Main] 2025-04-07 07:14:01 Info: threshold-config: Threshold
config parsed: 0 rule(s) found
[74038 - Suricata-Main] 2025-04-07 07:14:01 Info: detect: 42829 signatures
processed. 1249 are IP-only rules, 4334 are inspecting packet payload, 37029
inspect application layer, 109 are decoder event only
[74038 - Suricata-Main] 2025-04-07 07:14:14 Error: af-packet: fanout not
supported by kernel: Kernel too old or cluster-id 99 already in use.
[74038 - Suricata-Main] 2025-04-07 07:14:14 Warning: af-packet: eth0: AF_PACKET
tpacket-v3 is recommended for non-inline operation
[74038 - Suricata-Main] 2025-04-07 07:14:14 Info: runmodes: eth0: creating 1
thread
[74038 - Suricata-Main] 2025-04-07 07:14:14 Info: unix-manager: unix socket
'/var/run/suricata-command.socket'
[74253 - W#01-eth0] 2025-04-07 07:14:14 Info: ioctl: eth0: MTU 1500
[74038 - Suricata-Main] 2025-04-07 07:14:14 Notice: threads: Threads created ->
W: 1 FM: 1 FR: 1 Engine started.
[74038 - Suricata-Main] 2025-04-07 07:24:01 Notice: suricata: Signal Received.
Stopping engine.
[74038 - Suricata-Main] 2025-04-07 07:24:02 Info: suricata: time elapsed
587.578s
[74038 - Suricata-Main] 2025-04-07 07:24:03 Info: counters: Alerts: 135
[74038 - Suricata-Main] 2025-04-07 07:24:03 Notice: device: eth0: packets:
10856, drops: 0 (0.00%), invalid checksum: 0
```

Figure 44: Log suricata.txt B2

A quantidade de alertas sugere que o tráfego gerado pelas varreduras foi, de facto, detetado. Analisando o log “*fast.txt*” gerado pelo Suricata, é fácil reconhecer os 135 alertas mencionados anteriormente, estando claramente explícita a sua possível relação com varreduras Nmap, bem como detalhes da fonte, prioridade e *timestamps*. É razoável inferir que muitos dos alertas resultaram das varreduras mais ruidosas (nmap1, nmap3 e nmap4), que envolveram sondagens ativas a múltiplos serviços, identificação de versões e execução de scripts. Os alertas gerados demonstram a eficácia do NIDS em reconhecer essas atividades, validando a análise feita no ponto B2.2.

Portanto, pode concluir-se que as varreduras mais detalhadas tiveram impacto direto na geração de alertas pelo Suricata, o que comprova a sua alta detectabilidade. Já varreduras mais discretas, como a nmap2, poderão ter gerado poucos ou nenhum alertas, conforme esperado.

```

04/07/2025-07:14:35.365544  [**] [1:2260002:1] SURICATA Applayer Detect protocol
only one direction [**] [Classification: Generic Protocol Command Decode]
[Priority: 3] {TCP} 172.25.3.128:46974 -> 172.25.3.129:5432
04/07/2025-07:14:39.300042  [**] [1:2260002:1] SURICATA Applayer Detect protocol
only one direction [**] [Classification: Generic Protocol Command Decode]
[Priority: 3] {TCP} 172.25.3.128:56062 -> 172.25.3.129:25
04/07/2025-07:14:39.300232  [**] [1:2220006:1] SURICATA SMTP no server welcome
message [**] [Classification: Generic Protocol Command Decode] [Priority: 3]
{TCP} 172.25.3.129:25 -> 172.25.3.128:56062
04/07/2025-07:14:39.303623  [**] [1:2220000:1] SURICATA SMTP invalid reply [**]
[Classification: Generic Protocol Command Decode] [Priority: 3] {TCP}
172.25.3.129:25 -> 172.25.3.128:56062
04/07/2025-07:14:39.305456  [**] [1:2260002:1] SURICATA Applayer Detect protocol
only one direction [**] [Classification: Generic Protocol Command Decode]
[Priority: 3] {TCP} 172.25.3.129:514 -> 172.25.3.128:49232
04/07/2025-07:15:05.436620  [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent
Observed [**] [Classification: Web Application Attack] [Priority: 1] {TCP}
172.25.3.128:52914 -> 172.25.3.129:8180
04/07/2025-07:15:05.436940  [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent
Observed [**] [Classification: Web Application Attack] [Priority: 1] {TCP}
172.25.3.128:58686 -> 172.25.3.129:80
04/07/2025-07:15:05.437016  [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent
Observed [**] [Classification: Web Application Attack] [Priority: 1] {TCP}
172.25.3.128:58688 -> 172.25.3.129:80
04/07/2025-07:15:05.445531  [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent
Observed [**] [Classification: Web Application Attack] [Priority: 1] {TCP}
172.25.3.128:52910 -> 172.25.3.129:8180
04/07/2025-07:15:05.545569  [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent
Observed [**] [Classification: Web Application Attack] [Priority: 1] {TCP}
172.25.3.128:52932 -> 172.25.3.129:8180
04/07/2025-07:15:05.546054  [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent
Observed [**] [Classification: Web Application Attack] [Priority: 1] {TCP}
172.25.3.128:58700 -> 172.25.3.129:80
04/07/2025-07:15:05.595721  [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent
Observed [**] [Classification: Web Application Attack] [Priority: 1] {TCP}
172.25.3.128:52936 -> 172.25.3.129:8180
04/07/2025-07:16:25.564443  [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent
Observed [**] [Classification: Web Application Attack] [Priority: 1] {TCP}
172.25.3.128:46066 -> 172.25.3.129:80
04/07/2025-07:16:25.565887  [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent
Observed [**] [Classification: Web Application Attack] [Priority: 1] {TCP}
172.25.3.128:46088 -> 172.25.3.129:80
04/07/2025-07:16:25.577310  [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent
Observed [**] [Classification: Web Application Attack] [Priority: 1] {TCP}
172.25.3.128:46094 -> 172.25.3.129:80
04/07/2025-07:16:25.579062  [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent
Observed [**] [Classification: Web Application Attack] [Priority: 1] {TCP}
172.25.3.128:46108 -> 172.25.3.129:80
04/07/2025-07:19:25.957311  [**] [1:2260002:1] SURICATA Applayer Detect protocol
only one direction [**] [Classification: Generic Protocol Command Decode]
[Priority: 3] {TCP} 172.25.3.128:55758 -> 172.25.3.129:5432

```

Figure 45: Log *fast.txt* B2 (continua)

3.3. B3

Os levantamentos realizados na Parte A, utilizando métodos passivos e OSINT, oferecem vantagens significativas na otimização da varredura de sistemas alvo e na redução da sua detectabilidade.

Primeiramente, as técnicas passivas não geram tráfego de rede direto, o que diminui a probabilidade de ser detectado por sistemas de deteção de intrusões (NIDS). Informações obtidas de fontes públicas, como registos DNS, WHOIS e redes sociais, permitem identificar vulnerabilidades e configurações sem interação direta com o alvo, mantendo o tráfego de rede discreto.

Além disso, através de OSINT pode ser possível a obtenção de detalhes sobre a infraestrutura do alvo, como versões de software e serviços expostos, o que permite realizar varreduras ativas mais direcionadas e eficientes, evitando scans em sistemas seguros ou desnecessários. A análise de dados históricos também possibilita ajustar a abordagem de varredura, concentrando-se em áreas com maior probabilidade de falhas.

Resumidamente, os levantamentos passivos e OSINT otimizam as varreduras ativas ao fornecer informações estratégicas sem gerar tráfego detectável, aumentando a eficácia e reduzindo a visibilidade da operação. Desta forma, é possível realizar scans mais focados, que não geram tanto tráfego nem levantam tanta suspeita.

3.4. B4

No sistema alvo, foram adicionadas regras à firewall para bloqueio de tráfego externo TCP para os portos 513 (login) e 6000 (X11). De seguida, executaram-se as varreduras mencionadas na questão B2 novamente.

```
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 513 -j DROP  
[sudo] password for msfadmin:  
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 6000 -j DROP  
msfadmin@metasploitable:~$
```

Figure 46: Configuração Firewall no sistema alvo

```
(kali㉿kali)-[~/Documents]  
└─$ nmap -sV 172.25.3.129 > nmap1_fire.txt  
  
(kali㉿kali)-[~/Documents]  
└─$ nmap -sV -p 80 172.25.3.129 > nmap2_fire.txt  
  
(kali㉿kali)-[~/Documents]  
└─$ nmap -sV --script vulners 172.25.3.129 > nmap3_fire.txt  
  
(kali㉿kali)-[~/Documents]  
└─$ nmap -A 172.25.3.129 > nmap4_fire.txt
```

Figure 47: Varreduras Nmap B4

Na primeira varredura obtivemos um resultado dentro do esperado, sendo que, relativamente à pergunta B2, as únicas diferenças encontram-se nos portos 513 e 6000, onde a varredura não obteve qualquer resposta à tentativa de conexão, motivo pelo qual o estado em ambas ser *filtered*.

```

Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-07 10:07 EDT
Nmap scan report for 172.25.3.129
Host is up (0.00099s 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
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: 00:0C:29:B5:31:5E (VMware)
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 30.01 seconds

```

Figure 48: Resultado varredura 1 B4

Na segunda varredura, sendo que o foco incide somente no porto 80, o resultado é exatamente o mesmo que anteriormente, dado que não foram inseridas regras de filtragem no porto que serve http.

```

Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-07 10:09 EDT
Nmap scan report for 172.25.3.129
Host is up (0.00052s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.2.8 ((Ubuntu) DAV/2)
MAC Address: 00:0C:29:B5:31:5E (VMware)

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 13.49 seconds

```

Figure 49: Resultado varredura 2 B4

Na varredura com scripts de deteção de vulnerabilidades, o padrão mantém-se, isto é, o resultado apresenta-se de forma idêntica à varredura da pergunta B2, com exceção dos dois portos aos quais adicionamos as regras de bloqueio de tráfego, que passaram de *open* para *filtered*. Por exemplo, no porto 6000, previamente existia um aviso de *access denied*, indicando que estava acessível, o qual desapareceu nesta nova varredura.

```

https://vulnerables.com/postgresql/POSTGRESQL:CVE-2019-10209
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

```

Figure 50: Porto 6000 varredura 4 B4

```

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

```

Figure 51: Porto 6000 varredura 4 B2

A última varredura apresentou um comportamento análogo às restantes, como se pode comprovar pela imagem que se segue:

```

139/tcp open     netbios-ssn Samba smbd 3.0.20-Debian (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-3ubuntu5
| mysql-info:
| | Protocol: 10
| | Version: 5.0.51a-3ubuntu5
| | Thread ID: 33
| | Capabilities flags: 43564
| | Some Capabilities: Support41Auth, SupportsTransactions, SupportsCompression,
| | SwitchToSSLAfterHandshake, Speaks41ProtocolNew, ConnectWithDatabase,
| | LongColumnFlag
| | Status: Autocommit
|_| Salt: 3~F}feIzNUA$.[_L=,d4
5432/tcp open    postgresql PostgreSQL DB 8.3.0 - 8.3.7
| 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
|_|_ssl-date: 2025-04-07T11:41:59+00:00; -2h31m58s from scanner time.
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)

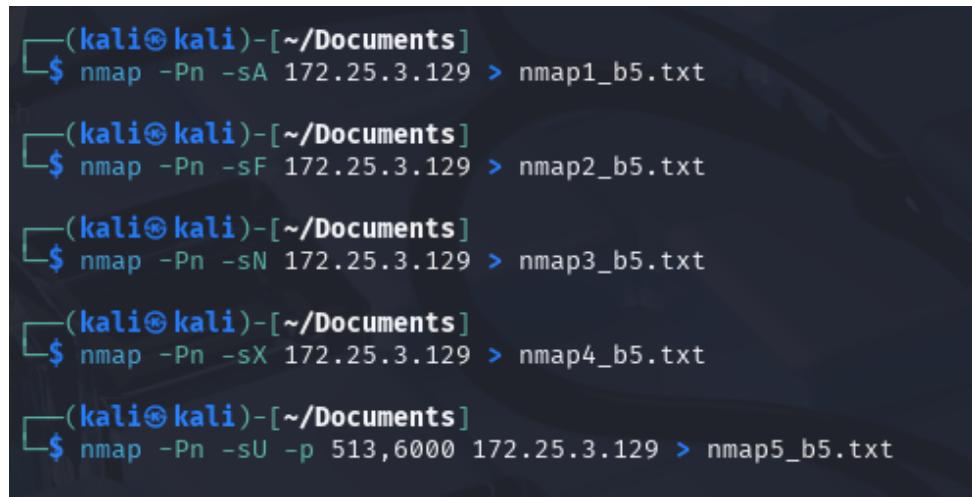
```

Figure 52: Resultado varredura 4 B4 (continua)

3.5. B5

Ainda com os portos 513 e 6000 bloqueados, realizamos cinco novas varreduras Nmap, explorando as flags ‘-Pn’ (No ping - Assume que o host alvo está ativo e passa diretamente para scan

de portos, útil quando se sabe que o host está ativo e Nmap diz que está *down*) e ‘-s[AFNXU]’, a analisar em detalhe de seguida.



```
(kali㉿kali)-[~/Documents]
$ nmap -Pn -sA 172.25.3.129 > nmap1_b5.txt

(kali㉿kali)-[~/Documents]
$ nmap -Pn -sF 172.25.3.129 > nmap2_b5.txt

(kali㉿kali)-[~/Documents]
$ nmap -Pn -sN 172.25.3.129 > nmap3_b5.txt

(kali㉿kali)-[~/Documents]
$ nmap -Pn -sX 172.25.3.129 > nmap4_b5.txt

(kali㉿kali)-[~/Documents]
$ nmap -Pn -sU -p 513,6000 172.25.3.129 > nmap5_b5.txt
```

Figure 53: varreduras Nmap B5

Para a primeira varredura foi utilizada a *flag* ‘-sA’, conhecida por *ACK scan*. Tem como função enviar pacotes com o bit ACK ativado, para detetar *firewalls*. Se o Nmap receber um RST, o porto está *unfiltered*. Caso contrário, se não obtiver resposta, o porto está *filtered*. Como seria de esperar, 998 dos 1000 portos estão *unfiltered*, sendo que os dois *filtered* são os que possuem as regras adicionadas em B4.

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-07 10:14 EDT
Nmap scan report for 172.25.3.129
Host is up (0.0029s latency).
Not shown: 998 unfiltered tcp ports (reset)
PORT      STATE      SERVICE
513/tcp    filtered  login
6000/tcp   filtered  X11
MAC Address: 00:0C:29:B5:31:5E (VMware)

Nmap done: 1 IP address (1 host up) scanned in 8.16 seconds
```

Figure 54: Resultado varredura 1 B5

Para a segunda varredura foi utilizada a *flag* ‘-sF’, conhecida por *FIN scan*. Tem como função enviar um pacote com o bit FIN ativo, sem estabelecer ligação, com o intuito de enganar *firewalls* que só filtram pacotes SYN. Analisando os resultados, podemos concluir que os pacotes FIN foram ignorados silenciosamente pelos portos abertos (segundo o RFC 793, se um porto aberto receber um pacote TCP sem a *flag* SYN, ele ignora silenciosamente) e foram bloqueados pelos portos com filtragem. O Nmap, não obtendo qualquer resposta de nenhum porto, não consegue determinar se se encontram abertos ou protegidos, apresentando o estado *open* | *filtered*. Os restantes 977 portos, no entanto, respondem com um pacote RST, de acordo com o RFC 793, indicando que estão fechados.

```

Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-07 10:15 EDT
Nmap scan report for 172.25.3.129
Host is up (0.0078s 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  ccproxy-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: 00:0C:29:B5:31:5E (VMware)

Nmap done: 1 IP address (1 host up) scanned in 8.32 seconds

```

Figure 55: Resultado varredura 2 B5

Na terceira varredura realizou-se um *NULL scan*, caracterizado pela presença da flag ‘-sN’. Tem como função enviar pacotes TCP sem flags, totalmente vazio, para tentar escapar *firewalls* que olham para o tipo de pacote. No entanto, o resultado foi exatamente o mesmo do *FIN scan*, pelo que se assume o mesmo comportamento por parte do *host* alvo.

```

Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-07 10:16 EDT
Nmap scan report for 172.25.3.129
Host is up (0.0056s 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  ccproxy-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: 00:0C:29:B5:31:5E (VMware)

Nmap done: 1 IP address (1 host up) scanned in 8.44 seconds

```

Figure 56: Resultado varredura 3 B5

Para a quarta varredura foi utilizada a flag ‘-sX’, conhecida por *Xmas scan*. Este envia pacotes com as flags FIN, PSH e URG ativas, de modo a tentar tirar proveito de comportamentos anómalos nos sistemas. Contudo, o resultado volta a repetir-se, pelo que voltamos a assumir o mesmo comportamento por parte da máquina alvo.

```

Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-07 10:16 EDT
Nmap scan report for 172.25.3.129
Host is up (0.0058s 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  ccproxy-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: 00:0C:29:B5:31:5E (VMware)

Nmap done: 1 IP address (1 host up) scanned in 8.35 seconds

```

Figure 57: Resultado varredura 4 B5

Na última varredura desta questão utilizamos a *flag* ‘-sU’ (*UDP scan*), focada nos portos aos quais adicionamos regras de bloqueio de tráfego TCP anteriormente. Como resultado, obtivemos a informação de que esses portos UDP se encontram fechados, que o porto 512 corre o serviço “who” (associado ao rlogin, normalmente) e o 6000 o serviço X11.

```

Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-07 10:17 EDT
Nmap scan report for 172.25.3.129
Host is up (0.00056s latency).

PORT      STATE      SERVICE
513/udp   closed    who
6000/udp   closed    X11
MAC Address: 00:0C:29:B5:31:5E (VMware)

Nmap done: 1 IP address (1 host up) scanned in 7.10 seconds

```

Figure 58: Resultado varredura 5 B5

3.6. B6

Para esta questão, utilizamos o *scanner* Nikto para varrer os serviços *web* a correr no *host* alvo, através do comando ‘nikto -h 172.25.3.129’. De modo a comparar o tráfego capturado, colocamos novamente o Suricata a escutar em modo IDS.

```

└─(kali㉿kali)-[~/Documents]
$ sudo suricata -c /etc/suricata/suricata.yaml -i eth0 -S /var/lib/suricata
/rules/*.rules -l ./log_nikto/
i: suricata: This is Suricata version 7.0.10 RELEASE running in SYSTEM mode
E: af-packet: fanout not supported by kernel: Kernel too old or cluster-id 99
already in use.
W: af-packet: eth0: AF_PACKET tpacket-v3 is recommended for non-inline operat
ion
i: threads: Threads created → W: 1 FM: 1 FR: 1 Engine started.

```

Figure 59: Comando Suricata B6

```

[91089 - Suricata-Main] 2025-04-07 10:19:27 Notice: suricata: This is Suricata
version 7.0.10 RELEASE running in SYSTEM mode
[91089 - Suricata-Main] 2025-04-07 10:19:27 Info: cpu: CPUs/cores online: 4
[91089 - Suricata-Main] 2025-04-07 10:19:27 Info: suricata: Setting engine mode
to IDS mode by default
[91089 - Suricata-Main] 2025-04-07 10:19:27 Info: exception-policy: master
exception-policy set to: auto
[91089 - Suricata-Main] 2025-04-07 10:19:27 Info: logopenfile: fast output
device (regular) initialized: fast.log
[91089 - Suricata-Main] 2025-04-07 10:19:27 Info: logopenfile: eve-log output
device (regular) initialized: eve.json
[91089 - Suricata-Main] 2025-04-07 10:19:27 Info: logopenfile: stats output
device (regular) initialized: stats.log
[91089 - Suricata-Main] 2025-04-07 10:19:43 Info: detect: 1 rule files
processed. 42826 rules successfully loaded, 0 rules failed, 0
[91089 - Suricata-Main] 2025-04-07 10:19:43 Info: threshold-config: Threshold
config parsed: 0 rule(s) found
[91089 - Suricata-Main] 2025-04-07 10:19:44 Info: detect: 42829 signatures
processed. 1249 are IP-only rules, 4334 are inspecting packet payload, 37029
inspect application layer, 109 are decoder event only
[91089 - Suricata-Main] 2025-04-07 10:20:11 Error: af-packet: fanout not
supported by kernel: Kernel too old or cluster-id 99 already in use.
[91089 - Suricata-Main] 2025-04-07 10:20:11 Warning: af-packet: eth0: AF_PACKET
tpacket-v3 is recommended for non-inline operation
[91089 - Suricata-Main] 2025-04-07 10:20:11 Info: runmodes: eth0: creating 1
thread
[91089 - Suricata-Main] 2025-04-07 10:20:11 Info: unix-manager: unix socket
'/var/run/suricata-command.socket'
[91450 - W#01-eth0] 2025-04-07 10:20:11 Info: ioctl: eth0: MTU 1500
[91089 - Suricata-Main] 2025-04-07 10:20:11 Notice: threads: Threads created ->
W: 1 FM: 1 FR: 1 Engine started.
[91089 - Suricata-Main] 2025-04-07 10:25:05 Notice: suricata: Signal Received.
Stopping engine.
[91089 - Suricata-Main] 2025-04-07 10:25:06 Info: suricata: time elapsed
295.246s
[91089 - Suricata-Main] 2025-04-07 10:25:07 Info: counters: Alerts: 23
[91089 - Suricata-Main] 2025-04-07 10:25:08 Notice: device: eth0: packets:
19926, drops: 0 (0.00%), invalid checksum: 0

```

Figure 60: Log suricata.txt B6

Como é possível visualizar pelo log suricata.txt, foram analisados 19926 pacotes (0% drop), e detetados 23 alertas. Dado o número quase duplicado de pacotes relativamente aos scans 3 e 4 da questão B2, é trivial concluir que o Nikto realiza uma varredura muito mais incidente, focada num domínio específico (web).

A varredura do Nikto apresentou como resultado inúmeras vulnerabilidades associadas ao serviço web do porto 80. Pela análise do log “fast.txt”, infere-se que este scan demonstra metodologias bastante mais intrusivas do que os realizados pelo Nmap, sendo que grande parte dos alertas remetem para “ET EXPLOIT”, cabeçalho que não apareceu em nenhum dos alertas relativos ao Nmap da questão B2.

```

- Nikto v2.5.0
-----
+ Target IP:          172.25.3.129
+ Target Hostname:   172.25.3.129
+ Target Port:        80
+ Start Time:        2025-04-07 10:25:32 (GMT-4)
-----
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user
agent to render the content of the site in a different fashion to the MIME type.
See:
https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-con
tent-type-header/
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows
attackers to easily brute force file names. The following alternatives for
'index' were found: index.php. See:
http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud
.com/vulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54).
Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause
false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST.
See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /?=PHPB885F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive
information via certain HTTP requests that contain specific QUERY strings. See:
OSVDB-12184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive
information via certain HTTP requests that contain specific QUERY strings. See:
OSVDB-12184
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive
information via certain HTTP requests that contain specific QUERY strings. See:
OSVDB-12184
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive
information via certain HTTP requests that contain specific QUERY strings. See:
OSVDB-12184
+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and
should be protected or limited to authorized hosts.
+ /phpMyAdmin/ChangeLog: Server may leak inodes via ETags, header found with
file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540, mtime: Tue Dec  9
12:24:00 2008. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should
be protected or limited to authorized hosts.
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was

```

```

found. This gives a lot of system information. See: CWE-552
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See:
https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases,
and should be protected or limited to authorized hosts.
+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be
protected or limited to authorized hosts. See: https://typo3.org/
+ /#wp-config.php#: #wp-config.php# file found. This file contains the
credentials.
+ 8910 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time:           2025-04-07 10:29:01 (GMT-4) (209 seconds)
-----
+ 1 host(s) tested

```

```

04/07/2025-10:22:02.894531  [**] [1:2016184:6] ET WEB_SERVER ColdFusion
administrator access [**] [Classification: Web Application Attack] [Priority: 1]
{TCP} 172.25.3.128:54442 -> 172.25.3.129:80
04/07/2025-10:22:08.159321  [**] [1:2221015:1] SURICATA HTTP Host header
ambiguous [**] [Classification: Generic Protocol Command Decode] [Priority: 3]
{TCP} 172.25.3.128:54468 -> 172.25.3.129:80
04/07/2025-10:22:52.531127  [**] [1:2016184:6] ET WEB_SERVER ColdFusion
administrator access [**] [Classification: Web Application Attack] [Priority: 1]
{TCP} 172.25.3.128:56232 -> 172.25.3.129:80
04/07/2025-10:24:00.456145  [**] [1:2260002:1] SURICATA Applayer Detect protocol
only one direction [**] [Classification: Generic Protocol Command Decode]
[Priority: 3] {TCP} 172.25.3.128:56324 -> 172.25.3.129:80
04/07/2025-10:24:05.209316  [**] [1:2056027:1] ET WEB_SPECIFIC_APPS Wordpress
LiteSpeed Cache Plugin debug.log Access Attempt (CVE-2024-44000) [**]
[Classification: Successful Credential Theft Detected] [Priority: 1] {TCP}
172.25.3.128:56366 -> 172.25.3.129:80
04/07/2025-10:24:14.427785  [**] [1:2016182:7] ET WEB_SERVER ColdFusion
componentutils access [**] [Classification: Web Application Attack] [Priority:
1] {TCP} 172.25.3.128:47656 -> 172.25.3.129:80
04/07/2025-10:24:29.002970  [**] [1:2031502:3] ET INFO Request to Hidden
Environment File - Inbound [**] [Classification: Misc activity] [Priority: 3]
{TCP} 172.25.3.128:39722 -> 172.25.3.129:80
04/07/2025-10:24:29.182447  [**] [1:2025756:3] ET EXPLOIT D-Link DSL-2750B - OS
Command Injection [**] [Classification: Attempted User Privilege Gain]
[Priority: 1] {TCP} 172.25.3.128:39722 -> 172.25.3.129:80
04/07/2025-10:24:29.182447  [**] [1:2049119:2] ET EXPLOIT D-Link DSL-2750B
Command Injection Attempt (CVE-2016-20017) [**] [Classification: Attempted
Administrator Privilege Gain] [Priority: 1] {TCP} 172.25.3.128:39722 ->
172.25.3.129:80
04/07/2025-10:24:29.438719  [**] [1:2033089:2] ET EXPLOIT Cisco RV320/RV325
Config Disclosure Attempt Inbound (CVE-2019-1653) [**] [Classification:
Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 172.25.3.128:39722
-> 172.25.3.129:80
04/07/2025-10:24:29.875925  [**] [1:2034005:1] ET EXPLOIT Fortinet
FortiOS/FortiProxy SSL VPN Web Portal Path Traversal (CVE-2018-13379) [**]
[Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP}
172.25.3.128:39722 -> 172.25.3.129:80
04/07/2025-10:24:29.958938  [**] [1:2221015:1] SURICATA HTTP Host header
ambiguous [**] [Classification: Generic Protocol Command Decode] [Priority: 3]
{TCP} 172.25.3.128:39728 -> 172.25.3.129:80
04/07/2025-10:24:29.958938  [**] [1:2221028:1] SURICATA HTTP Host header invalid
[**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP}
172.25.3.128:39728 -> 172.25.3.129:80
04/07/2025-10:24:29.990219  [**] [1:2029206:5] ET EXPLOIT Possible Citrix
Application Delivery Controller Arbitrary Code Execution Attempt
(CVE-2019-19781) [**] [Classification: Attempted Administrator Privilege Gain]
[Priority: 1] {TCP} 172.25.3.128:39728 -> 172.25.3.129:80
04/07/2025-10:24:29.990219  [**] [1:2035109:2] ET EXPLOIT Possible Citrix

```

```

Application Delivery Controller Arbitrary Code Execution Attempt
(CVE-2019-19781) M4 [**] [Classification: Attempted Administrator Privilege
Gain] [Priority: 1] {TCP} 172.25.3.128:39728 -> 172.25.3.129:80
04/07/2025-10:24:29.990219  [**] [1:2035110:2] ET EXPLOIT Citrix Application
Delivery Controller Arbitrary Code Execution Attempt Scanner Attempt
(CVE-2019-19781) [**] [Classification: Attempted Administrator Privilege Gain]
[Priority: 1] {TCP} 172.25.3.128:39728 -> 172.25.3.129:80
04/07/2025-10:24:30.171257  [**] [1:2030469:7] ET EXPLOIT F5 TMUI RCE
vulnerability CVE-2020-5902 Attempt M1 [**] [Classification: Attempted
Administrator Privilege Gain] [Priority: 1] {TCP} 172.25.3.128:39728 ->
172.25.3.129:80
04/07/2025-10:24:30.679984  [**] [1:2030483:4] ET EXPLOIT F5 TMUI RCE
vulnerability CVE-2020-5902 Attempt M2 [**] [Classification: Attempted
Administrator Privilege Gain] [Priority: 1] {TCP} 172.25.3.128:39728 ->
172.25.3.129:80
04/07/2025-10:24:30.848469  [**] [1:2221015:1] SURICATA HTTP Host header
ambiguous [**] [Classification: Generic Protocol Command Decode] [Priority: 3]
{TCP} 172.25.3.128:39728 -> 172.25.3.129:80
04/07/2025-10:24:30.997625  [**] [1:2030585:1] ET EXPLOIT Cisco ASA/Firepower

```

Figure 62: Log fast.txt B6

Após esta análise, podemos concluir face aos diferentes *scans* realizados. O Nmap com NSE (*Nmap Scripting Engine*) scripts realiza varreduras de vulnerabilidades em múltiplos serviços, sendo mais abrangente, mas com menor especialização em HTTP. Já o Nikto foca-se exclusivamente em servidores web, aplicando técnicas mais intrusivas e facilmente detetadas. Em termos de deteção por um sistema de prevenção de intrusões como o Suricata, o Nikto tende a gerar mais alertas específicos relacionados com tentativas de exploração web, enquanto o Nmap pode levantar alarmes mais genéricos de varredura e *fingerprinting* de serviços.

3.7. B7

Para a última varredura de vulnerabilidades, optamos por utilizar o OpenVAS. Para tal, tivemos inicialmente que instalar o gvm, correr o setup ‘gvm-setup’, a verificação ‘gvm-check-setup’ e, por último, iniciar o serviço com ‘gvm-start’.

Já dentro do serviço, de forma a conseguirmos analisar corretamente o alvo, adicionamos um novo *target*, o qual foi configurado com o IP do *host* alvo, neste caso 172.25.3.20, dado o scan ter sido corrido numa outra máquina. Por último, após a criação da *task* para a varredura do *target* criado, o sistema encontrava-se pronto a realizá-la.

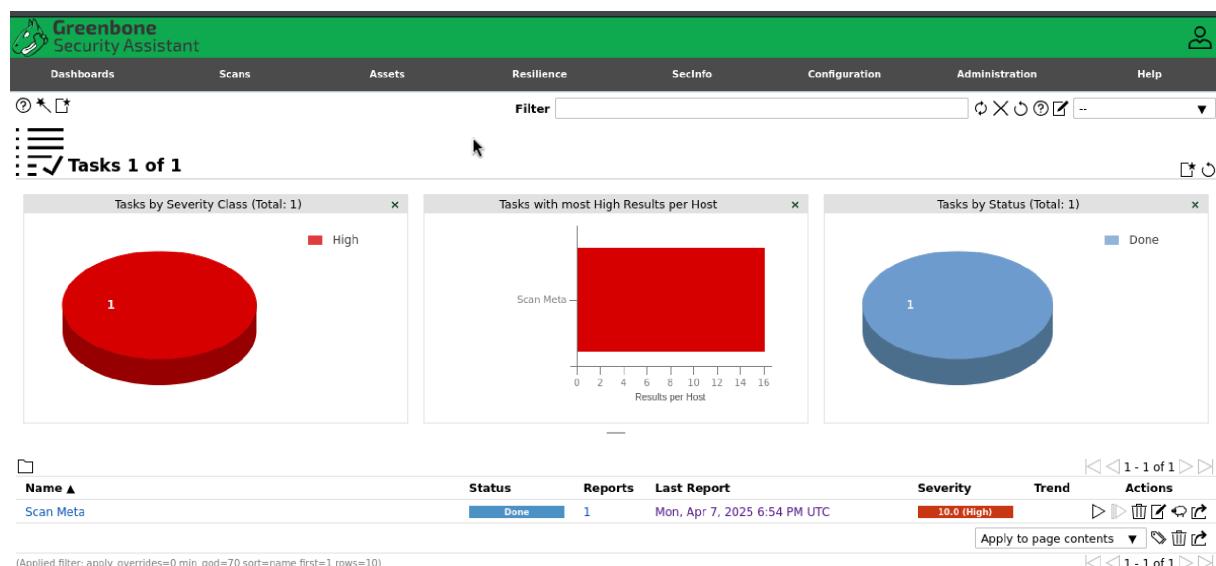


Figure 63: Scan OpenVas B7

A interface de utilização é bastante intuitiva e facilmente foi possível descarregar um relatório completo da varredura.

3.7.1. B7.1

Ao invés de resultados via linha de comando ou ficheiros .txt (estilo log), através do OpenVas conseguimos obter, sem esforço algum, um relatório PDF com 100 páginas, extremamente detalhado e organizado de todas as vulnerabilidades detetadas. Para além do normalmente obtido com as outras ferramentas, no relatório consta também uma visão geral da análise, bem como explicações mais detalhadas das vulnerabilidades, o impacto das mesmas e sistemas afetados, a forma de deteção, possíveis soluções e referências. Conclui-se, portanto, que o OpenVas demonstra-se como uma ferramenta bastante poderosa, não só pela quantidade de informação recolhida e gerada, mas também pela forma clara como esta é transmitida ao utilizador.

3.7.2. B7.2

Durante a análise comparativa entre os resultados do NIDS (Suricata) e o relatório gerado pelo OpenVAS, foi possível observar que alguns alertas gerados pelo Suricata não tiveram correspondência direta nas vulnerabilidades identificadas pelo OpenVAS. Esta diferença pode ser explicada por razões técnicas e operacionais que evidenciam a complementaridade entre as duas abordagens.

Em primeiro lugar, o NIDS opera de forma reativa e baseada em tráfego na rede, gerando alertas com base em assinaturas conhecidas de ataques, padrões de comportamento suspeito ou anomalias. Ou seja, o Suricata pode alertar para uma tentativa de exploração, varredura de portos ou uso de técnicas conhecidas, mesmo que o sistema alvo não esteja efetivamente vulnerável. Estas deteções refletem tentativas de ataque ou comportamentos anômalos que podem ou não ter sucesso, mas que levantam preocupações de segurança verdadeiras.

Por outro lado, ferramentas como o OpenVAS realizam uma análise ativa e direcionada aos serviços identificados no sistema alvo, tentando detetar vulnerabilidades conhecidas através de testes específicos e baseados em bases de dados de segurança. Se o serviço não apresentar falhas conhecidas ou for configurado de forma a não revelar informações sensíveis, o scanner não irá reportar nenhuma vulnerabilidade, mesmo que existam tentativas de exploração visíveis no tráfego monitorizado pelo NIDS.

4. Conclusão

Este trabalho prático proporcionou uma exploração aprofundada de técnicas de footprinting em contextos reais (Parte A) e de análise de vulnerabilidades em ambientes controlados (Parte B), permitindo consolidar conhecimentos teóricos através de experiências práticas.

Na Parte A, a análise entre uma grande corporação como a Nike e uma empresa local de menor dimensão como a Sintanet evidenciou diferenças marcantes nas abordagens à segurança digital. Enquanto as grandes empresas, apesar de uma superfície de ataque alargada, conseguem mitigá-la através de investimento robusto e estratégias preventivas, as pequenas empresas, mais limitadas em recursos, permanecem vulneráveis a ameaças significativas. Destacou-se ainda a relevância do fator humano, nomeadamente no contexto da engenharia social, onde a dimensão e dispersão das equipas se traduzem em diferentes níveis de exposição ao risco.

Na Parte B, a execução de varreduras ativas sobre o ambiente controlado Metasploitable 2 reforçou a importância da escolha criteriosa de ferramentas e metodologias. O Nmap mostrou-se uma solução versátil para o reconhecimento de serviços e deteção inicial de vulnerabilidades, enquanto o Nikto revelou grande utilidade na análise de servidores web, ainda que com uma abordagem mais intrusiva. O OpenVAS destacou-se pela sua abrangência e pelos relatórios estruturados com sugestões de mitigação, e o Suricata permitiu compreender o impacto de técnicas de evasão e a eficácia dos sistemas de deteção de intrusões.

Consideramos ter cumprido todos os objetivos propostos em ambas as partes do trabalho, tendo desenvolvido uma metodologia de pesquisa sólida na Parte A e, na Parte B, alcançado os resultados esperados, que puderam ser antecipados e confirmados com base no enquadramento teórico previamente estudado.

Este trabalho revelou-se extremamente importante para o nosso desenvolvimento enquanto estudantes, permitindo-nos aplicar, na prática, técnicas de OSINT, bem como abordagens mais interativas, como a utilização do Nmap. Destacamos ainda a relevância da capacidade de documentar de forma clara e estruturada tudo o que foi descoberto e analisado, uma competência essencial no contexto profissional da cibersegurança, onde a comunicação eficaz dos resultados é tão importante quanto a sua obtenção.