

Universidade do Minho

Mestrado em Engenharia Informática

Tecnologias de Segurança

Trabalho Prático 1 - Grupo 11

A74806 - João Amorim



06 de Março de 2024

Índice

1	Introdução	1
1.1	Contextualização	1
1.2	Objetivos	1
2	Parte A	2
2.1	Overview	2
2.2	Grande Corporação - Airbnb	3
2.2.1	Descrição da Empresa	3
2.2.2	Autenticação	3
2.2.3	Contactos	6
2.2.4	Redes Sociais	7
2.2.5	Ofertas de Emprego	10
2.2.6	WHOIS	12
2.2.7	DNS - host, dig, nslookup	13
2.3	Negócio Local - Pimacon DIY Construction Garden	15
2.3.1	Descrição da Empresa	15
2.3.2	Autenticação nas plataformas	15
2.3.3	Contactos	17
2.3.4	Redes Sociais	17
2.3.5	Ofertas de Emprego	18
2.3.6	Whois	18
2.3.7	DNS - host, dig, nslookup	19
2.4	Estratégias a Implementar e Conclusões	20
2.4.1	Airbnb	20
2.4.2	Pimacon	21
2.4.3	Conclusão	21
3	Parte B	22
3.1	Questão 1	22
3.1.1	Descoberta de Hosts e Dispositivos na Rede	22
3.1.2	Sistema Operativo	23
3.1.3	Port Scanning e Serviços	24
3.1.4	Vulnerabilidades dos Serviços	25
3.2	Questão 2	32
3.2.1	Scan das Vulnerabilidades	32
3.2.2	Vulnerabilidades - Serviços Principais	32
3.2.3	Outros serviços	40
3.2.4	Conclusão dos Scans	41

3.3	Questão 3	41
3.4	Questão 4	43
3.5	Questão 5	44
3.5.1	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep)	44
3.5.2	Apache Tomcat AJP Connector Request Injection (Ghostcat) . .	45
3.5.3	SMB Signing not required	46
3.5.4	Conclusão - Questão 5	47
4	Conclusão	49
4.1	Conclusões e Considerações Finais	49
4.2	Trabalho Futuro	49

Lista de Figuras

2.1	Política de criação de uma password forte no momento do registo	3
2.2	Tentativa de brute-forcing no login	4
2.3	Lista de sessões ativas	4
2.4	Autenticação multi factor com recurso a número de telemóvel	5
2.5	Término de sessão e acesso a rotas protegidas	6
2.6	Airbnb Support	7
2.7	Contactos do Airbnb	7
2.8	Tweet de prevenção para a existência impersonators	8
2.9	Página de suporte no X	8
2.10	Página do Facebook	8
2.11	Página do Instagram	9
2.12	Página do Youtube	9
2.13	Post no Instagram	10
2.14	Conteúdo partilhado no X	10
2.15	Página de Oferta de Emprego	11
2.16	Página exemplo da descrição de uma Oferta de Emprego	11
2.17	Execução do comando whois airbnb.com	12
2.18	Execução do comando whois airbnb.com	12
2.19	Execução do comando whois airbnb.com	13
2.20	Execução do comando host airbnb.com	13
2.21	Whois para domínio do Airbnb - 1º Endereço IP	14
2.22	Whois para domínio do Airbnb - 1º Endereço IP	14
2.23	Whois para domínio do Airbnb - 1º Endereço IP	15
2.24	Whois para domínio do Airbnb - 1º Endereço IP	15
2.25	Registo de conta na Pimacon	16
2.26	Conta com sessão iniciada	16
2.27	Logout efetuado	17
2.28	Página de contactos	17
2.29	Redes Sociais	18
2.30	Whois pimacon.com	18
2.31	Whois pimacon.com	19
2.32	host pimacon.com	19
2.33	whois 2.80.62.247	20
2.34	dig pimacon.com	20
2.35	nslookup pimacon.com	20
3.1	nmap -sn 172.24.11.0/24	22
3.2	nmap -O 172.24.11.2	23

3.3	nmap -sV 172.24.11.2	23
3.4	Wireshark - Sistema Operativo	24
3.5	nmap -sV 172.24.11.2	25
3.6	nmap -sU 172.24.11.2	25
3.7	SSH - CVE-2016-8858	26
3.8	MSRPC - CVE-2017-0143	27
3.9	SSL/HTTP	29
3.10	Apache Tomcat - CVE-2023-26044	30
3.11	ssl/unknown (Port 8031)	30
3.12	APACHE HTTPD - CVE-2007-6750	31
3.13	SSL/HTTPS?-?	31
3.14	Vulnerabilidades obtidas pelo Nessus	33
3.15	Vulnerabilidades para o Port 22	33
3.16	Vulnerabilidades para os Ports 135, 139 e 3306	34
3.17	Vulnerabilidades para o Port 445	34
3.18	Vulnerabilidades para o Port 3000	35
3.19	Vulnerabilidades para o Port 3389	35
3.20	Vulnerabilidades para o Port 4848	36
3.21	Vulnerabilidades para o Port 8009	37
3.22	Vulnerabilidades para o Port 8022	38
3.23	Vulnerabilidades para o Port 8383	39
3.24	Vulnerabilidades para o Port 8443	39
3.25	Vulnerabilidades para o Port 9200	40
3.26	Vulnerabilidades para ports restantes	41
3.27	IDS - Primeira vulnerabilidade	42
3.28	Wireshark - Primeira vulnerabilidade	42
3.29	IDS - Segunda vulnerabilidade	43
3.30	Wireshark - Segunda vulnerabilidade	43
3.31	Network Level Authentication	45
3.32	Soluções para a Vulnerabilidade	46
3.33	SMB Signing not required	46
3.34	Microsoft Network Server: Digitally Sign Communications (always)	47
3.35	Contagem das Vulnerabilidades - 1º Scan	47
3.36	Listagem das Vulnerabilidades - 1º Scan	47
3.37	Contagem das Vulnerabilidades - 2º Scan	48
3.38	Listagem das Vulnerabilidades - 1º Scan	48

1 Introdução

1.1 Contextualização

No âmbito deste trabalho prático, propõe-se uma análise abrangente da postura de segurança em sistemas e infraestruturas reais, utilizando técnicas de coleta passiva de informação como principal metodologia. Na primeira parte, concentra-se na aplicação de técnicas de coleta passiva, destacando-se como ferramenta essencial na avaliação da segurança de sistemas online. Já na segunda parte, será configurado um ambiente de testes dedicado à identificação de vulnerabilidades e fraquezas em sistemas remotos, por meio de técnicas e ferramentas de varredura ativa.

1.2 Objetivos

O objetivo principal deste trabalho consiste em analisar a postura de segurança em sistemas e infraestruturas reais, implementando técnicas de coleta passiva e varredura ativa de informações. Na primeira parte, visa-se compreender a abordagem adotada pelos administradores de sistemas para proteger suas infraestruturas online, utilizando a coleta passiva como ferramenta-chave. Na segunda parte, pretende-se configurar um ambiente de testes específico para identificar vulnerabilidades e fraquezas em sistemas remotos, aplicando técnicas de varredura ativa. Por meio dessas investigações, procura-se não apenas identificar potenciais falhas de segurança, mas também propor estratégias eficazes para fortalecer a postura de segurança desses sistemas frente a ameaças cibernéticas.

2 Parte A

2.1 Overview

Nesta primeira parte, tal como pedido no enunciado, foram escolhidas duas empresas, nomeadamente a Airbnb e a Pimacon, em que o objetivo é o de utilizar técnicas de busca passiva de informação que permitam identificar detalhes sobre os seus sistemas e infra-estruturas.

A análise de cada uma das empresas irá ser dividida em sete partes, nomeadamente:

- **Descrição da Empresa** - Breve descrição da empresa.
- **Autenticação** - Pesquisa de vulnerabilidades no que diz respeito à autenticação nas plataformas das empresas.
- **Contactos** - Pesquisa de vulnerabilidades no que diz respeito aos contactos disponibilizados pela empresa.
- **Redes Sociais** - Recolha de informações sobre conteúdo partilhado nas redes sociais que forneçam informações críticas sobre trabalhadores, contactos, locais físicos, entre outros.
- **Ofertas de Emprego** - Recolha de informações sobre ofertas de emprego por parte das empresas que forneçam informações críticas sobre as mesmas.
- **Whois** - Obtenção de informações como o registo de domínio, incluindo detalhes como o proprietário do domínio, informações de contacto associadas, data de registo, entre outros.
- **DNS - host, dig, nslookup** - Obtenção de informações sobre registros de DNS, como endereços IP associados a nomes de domínio.

No final, será feita uma avaliação dos dados obtidos e elaboração de estratégias que minimizem os riscos face aos métodos de busca passiva usados.

2.2 Grande Corporação - Airbnb

2.2.1 Descrição da Empresa

O Airbnb é uma plataforma online que facilita o aluguer de alojamentos pelo mundo fora, tendo sido fundada em 2008. A empresa permite que os viajantes reservem alojamentos únicos, desde quartos individuais a casas inteiras, diretamente aos anfitriões. Além disso, oferece experiências locais, como passeios e aulas, proporcionando aos viajantes uma forma única de se conectar com as comunidades locais. O Airbnb transformou a forma como as pessoas viajam, oferecendo uma alternativa personalizada e autêntica aos hotéis tradicionais.

Com uma receita anual de 9.917 bilhões de dólares em 2023, esta será a empresa escolhida para representar a grande corporação nesta primeira parte do trabalho prático.

2.2.2 Autenticação

No que diz respeito à autenticação na plataforma do Airbnb, começamos por observar a existência de uma política de password forte no momento do registo, obrigando o utilizador a criar uma password que não contenha o nome nem o email do utilizador, que contenha pelo menos 8 caracteres e que contenha pelo menos um número ou um símbolo.

A screenshot of a password creation form. At the top, there is a text input field labeled "Password" with a "Show" button to its right. Below the input field, there is a list of validation errors in red text:

- >Password strength: weak
- Can't contain your name or email address
- At least 8 characters
- Contains a number or symbol

Below the errors, there is a small explanatory text: "By selecting Agree and continue, I agree to Airbnb's [Terms of Service](#), [Payments Terms of Service](#), and [Nondiscrimination Policy](#) and acknowledge the [Privacy Policy](#)." At the bottom, there is a large red button with the text "Agree and continue".

Figura 2.1: Política de criação de uma password forte no momento do registo

Em relação ao login na plataforma, seria de esperar algum mecanismo de limitação de tentativas de entrada, sendo que este apenas envia um mail para o email que está a ser utilizado nas mesmas tentativas, após a terceira tentativa, deixando a plataforma exposta a ataques de brute-forcing na tentativa de acederem às contas de utilizadores.

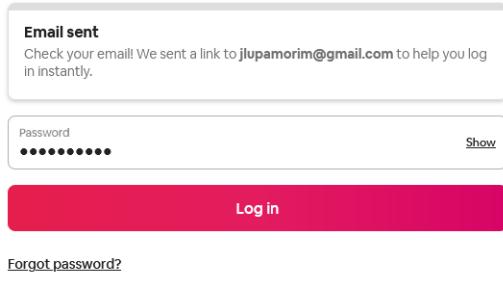


Figura 2.2: Tentativa de brute-forcing no login

Já dentro da plataforma, é dado ao utilizador a informação sobre as sessões que estão ativas, bem como uma segunda camada de proteção, também conhecida como autenticação de dois fatores (2FA), com recurso à conexão do número de telemóvel do utilizador com a conta, para onde será enviado um código de autenticação de cada vez que o utilizador tentar entrar na plataforma.

A screenshot of a "Device history" section. It shows a single session entry with a computer icon, the text "Session", and "CURRENT SESSION". To the right, there is a "Log out device" link and the timestamp "March 15, 2024 at 04:03".

Figura 2.3: Lista de sessões ativas

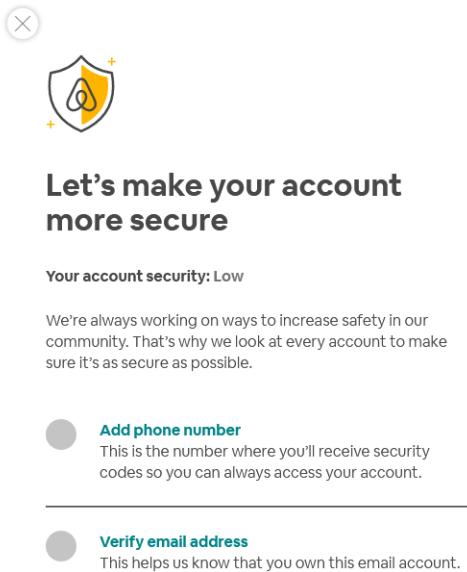


Figura 2.4: Autenticação multi factor com recurso a número de telemóvel

Finalmente, em relação ao término de sessão por parte do utilizador, de uma maneira muito simplista, é possível verificar que as rotas protegidas, que apenas poderiam ser acedidas pelos utilizadores respetivos, já não se encontram disponíveis, pelo que é possível dizer, com algum cuidado, que as sessões estão a ser encerradas corretamente. Neste caso, tentou-se aceder aos settings da conta do utilizador, sem sucesso.

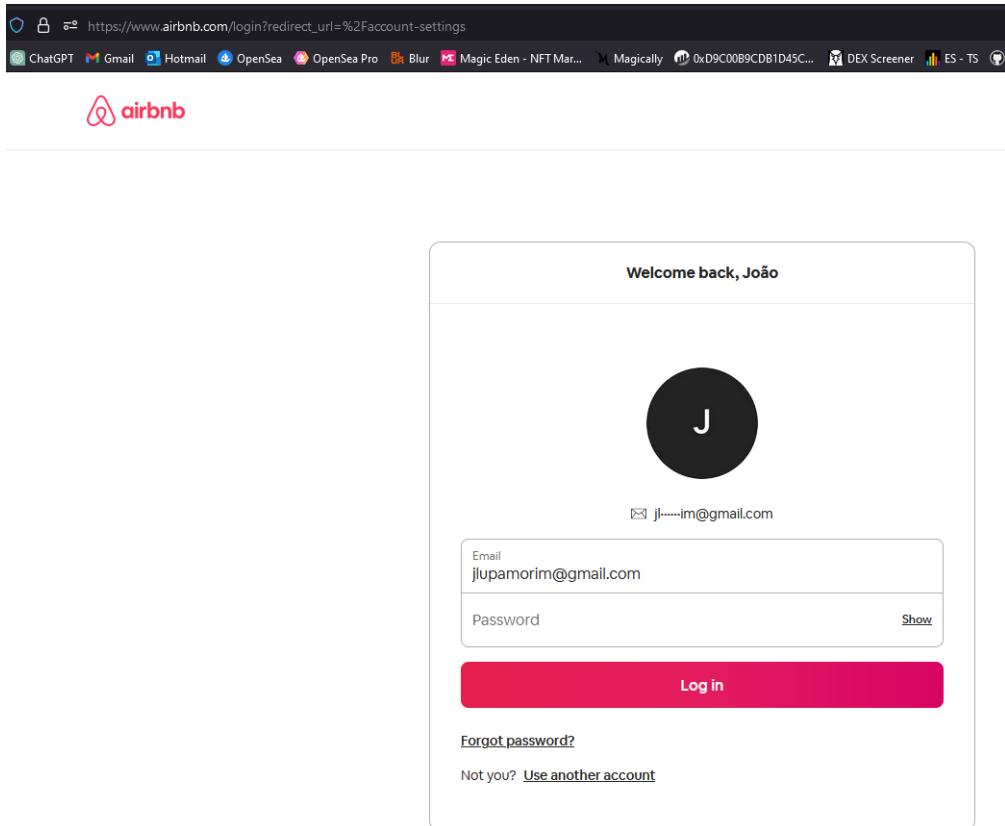


Figura 2.5: Término de sessão e acesso a rotas protegidas

De notar que seria interessante perceber também se existe um tempo de expiração para as tokens, fazendo com que as sessões sejam encerradas por inatividade. Dada a natureza do trabalho, foi algo que não foi explorado.

2.2.3 Contactos

No que diz respeito aos Contactos disponíveis pela plataforma, foi possível observar a existência de dois métodos de contacto:

- **Airbnb Support**
- **Contacto Telefónico**

Em relação ao "Airbnb Support", este permite que um utilizador crie, numa primeira fase, um ticket onde pode expor a situação em causa, em que as respostas que obtém são default, dependendo das opções que escolhe. Numa fase posterior, se for um assunto mais complicado e em que seja necessária a ajuda qualificada de trabalhadores do Airbnb, este ticket é então passado para um trabalhador disponível, onde o utilizador pode de facto ter contacto humano.

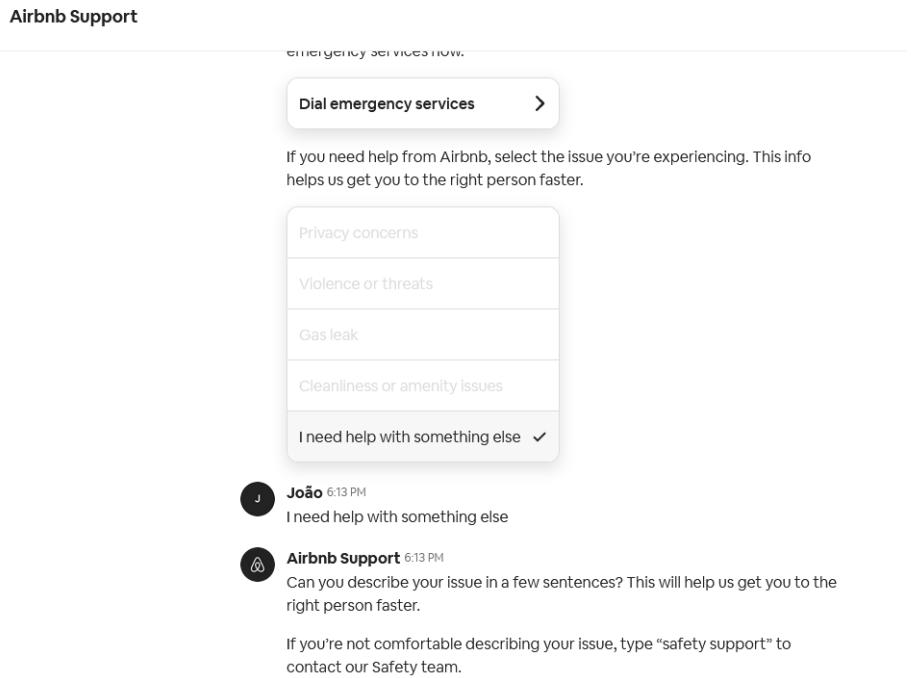


Figura 2.6: Airbnb Support

No que diz respeito ao contacto telefónico, o utilizador entra diretamente em contacto com um trabalhador do Airbnb onde pode expor a sua situação.

Contact Airbnb Customer Service

Need a little more help or have a complaint? [Contact us](#) by email, chat, or phone at 1-844-234-2500.

Figura 2.7: Contactos do Airbnb

Em qualquer uma destas situações, é possível que alguém a explorar vulnerabilidades na plataforma do Airbnb, use este possível contacto com humanos, nomeadamente trabalhadores do Airbnb, para que, por meios de "Social Engineering", consiga obter informações sobre vulnerabilidades que lhe permitam efetuar um ataque com sucesso. No caso do Airbnb Support, isto só acontecerá caso o atacante chegue ao ponto de contactar diretamente com um trabalhador, sendo que na primeira fase isto não é possível.

Para além dos dois métodos de contacto mencionados, é possível entrar em contacto com trabalhadores pertencentes ao Airbnb a partir das suas redes sociais, o que será visto na secção seguinte.

2.2.4 Redes Sociais

O Airbnb possuí neste momento quatro tipos de redes sociais, nomeadamente X (Twitter), Facebook, Instagram e Youtube. Em todas excepto no Youtube, é possível entrar

em contacto com quem estará eventualmente encarregue da manutenção das mesmas páginas, pelo que a situação de "Social Engineering" mencionada na secção anterior, poderá de facto acontecer aqui também. Existe ainda uma página no X chamada AirbnbHelp, destinada exclusivamente a apoio ao cliente.

É importante mencionar que é usual a existência de páginas de redes sociais que copiam os nomes das contas verdadeiras das redes sociais destas grandes empresas, sendo que o Airbnb vai mencionando em alguns posts que faz na página AirbnbHelp que o mesmo é um acontecimento regular.

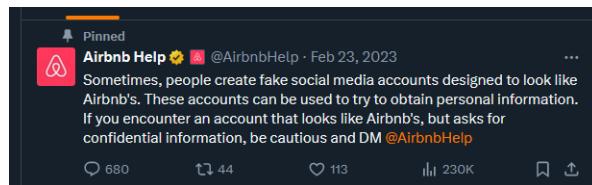


Figura 2.8: Tweet de prevenção para a existência impersonators



Figura 2.9: Página de suporte no X



Figura 2.10: Página do Facebook

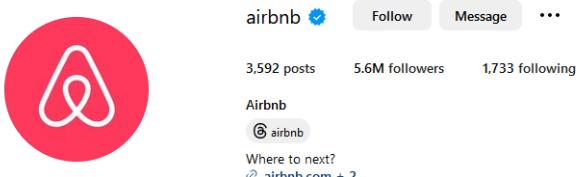


Figura 2.11: Página do Instagram

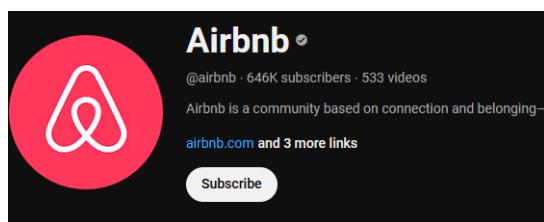


Figura 2.12: Página do Youtube

Em relação ao conteúdo divulgado nestas mesmas redes sociais, é aparente que apenas são partilhadas imagens e vídeos criados por equipas profissionais para divulgação de destinos de férias, assim como airbnb's disponíveis para aluguer na plataforma. Não parecem ser feitas publicações que divulguem informações sobre instalações da empresa, informações sobre os seus trabalhadores ou qualquer informação que algum atacante pudesse utilizar para explorar vulnerabilidades do Airbnb.

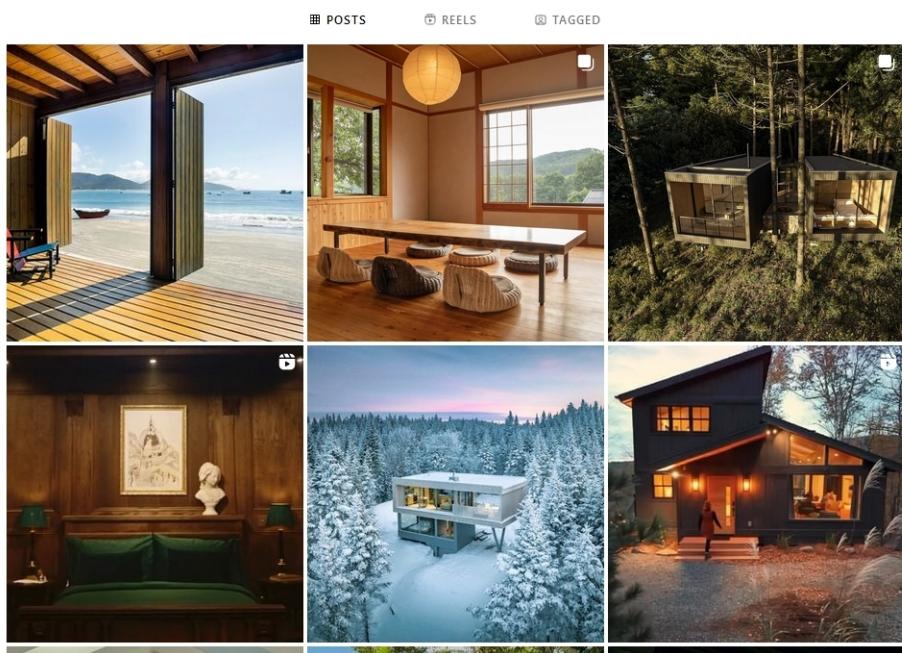


Figura 2.13: Post no Instagram



Figura 2.14: Conteúdo partilhado no X

2.2.5 Ofertas de Emprego

A plataforma do Airbnb disponibiliza informação sobre todas as ofertas de emprego existentes, assim como as localizações (países/cidades) às quais as mesmas dizem respeito,

sendo que estas ofertas de emprego vão desde funções relacionadas com Marketing a Engenheiros de Software.

The screenshot shows a job search interface with the following sections:

- Select location:** A dropdown menu showing "All Locations".
- DEPARTMENTS:**
 - All Departments (129)
 - Analytics (2)
 - Community Support (2)
 - Data Science (3)
 - Design (2)
 - Employee Experience (1)
 - Engineering (78)**
- FEATURED ROLES:**
 - Staff Frontend Engineer, Media Foundation** >
 - California, United States
 - Staff Technical Product Delivery Manager, Community Support AI** >
 - California, United States
 - Senior Staff Engineer, Community Support Products** >
 - China

Figura 2.15: Página de Oferta de Emprego

Para cada oferta de emprego, é feita uma descrição das funções a desempenhar, bem como ferramentas com as quais os candidatos têm que ter experiência, não fazendo no entanto menção a características mais específicas como versões das ferramentas/frameworks a serem utilizadas, o que é uma boa prática uma vez que atacantes à procura de explorar vulnerabilidades podem usar essas informações para explorar possíveis ataques com o uso de vulnerabilidades existentes para versões de software em específico. No que diz respeito a infraestruturas, não foi encontrada qualquer menção nesta secção de Ofertas de Emprego, nem em qualquer outra parte da plataforma.

Your Expertise:

- 9+ years of experience in Web / full-stack development, **with a strong focus on media-related technologies** (e.g. media processing libraries / frameworks, media players, knowledge of industry standards and best practices for media encoding and compression (e.g. formats and codecs), and a passion for creating engaging user experiences through media)
- Strong expertise building and maintaining high-performance and scalable Web frontend experiences using React, Typescript, Signals, HTML, and CSS
- Excellent problem-solving, debugging, and optimization skills
- Strong collaboration and communication abilities, with the ability to work effectively with cross-functional teams.
- An overwhelming desire and curiosity to learn!

Figura 2.16: Página exemplo da descrição de uma Oferta de Emprego

2.2.6 WHOIS

O WHOIS pode ser uma ferramenta útil como parte de um processo mais amplo de exploração de vulnerabilidades, especialmente na fase inicial de reconhecimento e coleta de informações sobre um alvo. Neste caso, uso do comando "whois airbnb.com" permite-nos encontrar uma série de informações pertinentes sobre a empresa, tais como o registo do domínio, incluindo o nome do registrador (MarkMonitor Inc.), datas importantes como a data de criação e data de expiração do registo, estado do domínio, servidores de nome associados e informações de contacto do registrador para relatar abusos.

```
L$ whois airbnb.com
Domain Name: AIRBNB.COM
Registry Domain ID: 1512196199_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2023-08-23T20:10:06Z
Creation Date: 2008-08-05T07:29:00Z
Registrar Expiry Date: 2024-08-05T07:29:00Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeletePr
hibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransf
erProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdatePr
hibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeletePr
hibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransf
erProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdatePr
hibited
Name Server: DNS1.P08.NSONE.NET
Name Server: DNS2.P08.NSONE.NET
Name Server: DNS3.P08.NSONE.NET
Name Server: DNS4.P08.NSONE.NET
Name Server: NS-1108.AWSDNS-10.ORG
Name Server: NS-158.AWSDNS-19.COM
Name Server: NS-1977.AWSDNS-55.CO.UK
Name Server: NS-756.AWSDNS-30.NET
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wi
cf/
```

Figura 2.17: Execução do comando whois airbnb.com

```
The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: airbnb.com
Registry Domain ID: 1512196199_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2024-03-06T22:44:13+0000
Creation Date: 2008-08-05T07:29:00+0000
Registrar Registration Expiration Date: 2024-08-05T00:00:00+0000
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdate
Prohibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTran
sferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDelete
Prohibited)
Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdate
Prohibited)
Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTran
sferProhibited)
Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDelete
Prohibited)
```

Figura 2.18: Execução do comando whois airbnb.com

```

Registrant Organization: Airbnb, Inc.
Registrant State/Province: CA
Registrant Country: US
Registrant Email: Select Request Email Form at https://domains.markmonitor.co
m/whois/airbnb.com
Admin Organization: Airbnb, Inc.
Admin State/Province: CA
Admin Country: US
Admin Email: Select Request Email Form at https://domains.markmonitor.com/who
is/airbnb.com
Tech Organization: Airbnb, Inc.
Tech State/Province: CA
Tech Country: US
Tech Email: Select Request Email Form at https://domains.markmonitor.com/who
is/airbnb.com
Name Server: ns-756.awsdns-30.net
Name Server: ns-1977.awsdns-55.co.uk
Name Server: dns2.p08.nsone.net
Name Server: ns-158.awsdns-19.com
Name Server: dns1.p08.nsone.net
Name Server: dns4.p08.nsone.net
Name Server: dns3.p08.nsone.net
Name Server: ns-1108.awsdns-10.org
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.n
et/

```

Figura 2.19: Execução do comando whois airbnb.com

É possível observar o uso de uma prática comum e recomendada, a da inclusão de informações de contato para relatar abusos (como abuso de marca, spam, phishing, etc.) nos resultados do "whois". Isto permite que indivíduos ou organizações relatem atividades abusivas referentes ao domínio diretamente ao registrador do domínio para investigação e ação apropriada.

É importante ressaltar que o WHOIS sozinho não é suficiente para identificar ou explorar vulnerabilidades no sistema ou domínio. É apenas uma das muitas ferramentas e fontes de informações que podem ser usadas na fase de reconhecimento.

2.2.7 DNS - host, dig, nslookup

Nesta secção, irão ser executados os comandos host, dig e nslookup, com o objetivo de obter mais informações sobre a empresa Airbnb.

Começando pelo comando "host airbnb.com", geralmente usado para obter o endereço IP associado a um nome de domínio, foi obtido o seguinte resultado:

```

└$ host airbnb.com
airbnb.com has address 52.44.131.61
airbnb.com has address 54.209.194.167
airbnb.com has address 54.147.55.57
airbnb.com mail is handled by 5 alt2.aspmx.l.google.com.
airbnb.com mail is handled by 1 aspmx.l.google.com.
airbnb.com mail is handled by 10 alt3.aspmx.l.google.com.
airbnb.com mail is handled by 10 alt4.aspmx.l.google.com.
airbnb.com mail is handled by 5 alt1.aspmx.l.google.com.

```

Figura 2.20: Execução do comando host airbnb.com

De acordo com o resultado obtido, é possível concluir que o Airbnb possui três endereços IP diferentes, em que cada endereço deverá corresponder a um servidor diferente. Em geral, isto acontece para empresas de grande escala para melhorar a performance da plataforma, permitindo por exemplo distribuir a carga de tráfego pelos vários servidores, existirem outros servidores online em caso de falha de um deles ou até para permitir que existam servidores distribuídos geograficamente de forma mais eficiente de acordo com o tráfego que chega aos mesmos.

De seguida, efetua-se novamente o comando "whois", mas desta vez sobre os endereços IP obtidos anteriormente (neste caso, apenas sobre o primeiro):

```

NetRange:      52.0.0.0 - 52.79.255.255
CIDR:         52.0.0.0/10, 52.64.0.0/12
NetName:       AT-88-Z
NetHandle:     NET-52-0-0-0-1
Parent:        NET52 (NET-52-0-0-0-0)
NetType:       Direct Allocation
OriginAS:      1
Organization:  Amazon Technologies Inc. (AT-88-Z)
RegDate:       1991-12-19
Updated:       2024-02-05
Comment:       Geofeed http://ip-ranges.amazonaws.com/geo-ip-feed.csv
Ref:          https://rdap.arin.net/registry/ip/52.0.0.0

OrgName:       Amazon Technologies Inc.
OrgId:        AT-88-Z
Address:      410 Terry Ave N.
City:          Seattle
StateProv:    WA
PostalCode:   98109
Country:      US
RegDate:      2011-12-08
Updated:      2024-01-24
Comment:      All abuse reports MUST include:
Comment:      * src IP
Comment:      * dest IP (your IP)
Comment:      * dest port
Comment:      * Accurate date/timestamp and timezone of activity
Comment:      * Intensity/frequency (short log extracts)
Comment:      * Your contact details (phone and email) Without these
Ref:          https://rdap.arin.net/registry/entity/AT-88-Z

```

Figura 2.21: Whois para domínio do Airbnb - 1º Endereço IP

```

OrgRoutingHandle: ARMP-ARIN
OrgRoutingName: AWS RPKI Management POC
OrgRoutingPhone: +1-206-555-0000
OrgRoutingEmail: aws-rpki-routing-poc@amazon.com
OrgRoutingRef: https://rdap.arin.net/registry/entity/ARMP-ARIN

OrgNOCHandle: AAN01-ARIN
OrgNOCName: Amazon AWS Network Operations
OrgNOCPhone: +1-206-555-0000
OrgNOCEmail: amzn-noc-contact@amazon.com
OrgNOCRef: https://rdap.arin.net/registry/entity/AAN01-ARIN

OrgTechHandle: AN024-ARIN
OrgTechName: Amazon EC2 Network Operations
OrgTechPhone: +1-206-555-0000
OrgTechEmail: amzn-noc-contact@amazon.com
OrgTechRef: https://rdap.arin.net/registry/entity/AN024-ARIN

OrgAbuseHandle: AEA8-ARIN
OrgAbuseName: Amazon EC2 Abuse
OrgAbusePhone: +1-206-555-0000
OrgAbuseEmail: abuse@amazonaws.com
OrgAbuseRef: https://rdap.arin.net/registry/entity/AEA8-ARIN

OrgRoutingHandle: IPROU3-ARIN
OrgRoutingName: IP Routing
OrgRoutingPhone: +1-206-555-0000
OrgRoutingEmail: aws-routing-poc@amazon.com
OrgRoutingRef: https://rdap.arin.net/registry/entity/IPROU3-ARIN

```

Figura 2.22: Whois para domínio do Airbnb - 1º Endereço IP

Tal como no primeiro "whois", são obtidas informações do mesmo tipo, mas desta vez com a adição de informações como o NetName, que indica o nome da rede associado ao bloco de endereços IP, o NetHandle, que é um identificador único atribuído ao bloco de endereços IP na base de dados de registro, o OrgName, que indica o nome da organização ou entidade que detém ou controla o bloco de endereços IP, neste caso a Amazon e finalmente o OrgId que é um identificador único atribuído à mesma organização.

Finalmente, são executados os comandos "dig airbnb.com" e "nslookup airbnb.com":

```

└$ dig airbnb.com
; <>> DiG 9.19.19-1-Debian <>> airbnb.com
;; global options: +cmd
;; Got answer:
;; →HEADER← opcode: QUERY, status: NOERROR, id: 27373
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1
;;
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;airbnb.com.           IN      A
;;
;; ANSWER SECTION:
airbnb.com.        60     IN      A      54.147.55.57
airbnb.com.        60     IN      A      54.209.194.167
airbnb.com.        60     IN      A      52.44.131.61

```

Figura 2.23: Whois para domínio do Airbnb - 1º Endereço IP

```

└$ nslookup airbnb.com
Server:    192.168.1.1
Address:   192.168.1.1#53

Non-authoritative answer:
Name:    airbnb.com
Address: 52.44.131.61
Name:    airbnb.com
Address: 54.209.194.167
Name:    airbnb.com
Address: 54.147.55.57

```

Figura 2.24: Whois para domínio do Airbnb - 1º Endereço IP

Estes comandos acabaram por não adicionar informação relevante aos dados que já tinham sido obtidos.

2.3 Negócio Local - Pimacon DIY Construction Garden

2.3.1 Descrição da Empresa

A Pimacon é uma empresa local sediada em Vila Nova de Famalicão, que oferece serviços de bricolage, construção e jardins, não só no sentido de ajudar os clientes com os objetivos que têm em termos de obras/remodelação, mas também no acompanhamento e controlo de qualidade de serviços efetuados pelos clientes. A Pimacon trata também do fornecimento de todo o tipo de materiais necessários para os serviços mencionados.

É uma empresa criada há vários anos, mas que conta apenas com uma fábrica/loja, oferecendo os seus serviços fisicamente e através da plataforma "pimacon.com", onde é possível requisitar serviços e efetuar encomendas de produtos.

2.3.2 Autenticação nas plataformas

Em relação à autenticação na plataforma da Pimacon, e começando com o processo de registo na plataforma, é possível observar imediatamente a inexistência de uma política de segurança forte para a Password utilizada no registo. Neste caso, foi possível efetuar o registo com uma password composta por 6 letras, todas minúsculas, o que é claramente pouco recomendado.

Registe aqui a sua conta

Nome*	Password*
João	*****
E-mail*	Confirmar Password*
jlupamorim@gmail.com	*****

Li e aceito os termos e condições

Criar conta

* Campos obrigatórios

[Esqueceu a sua password?](#)

Figura 2.25: Registo de conta na Pimacon

Já dentro da plataforma e com o Login efetuado, não existe qualquer camada adicional de segurança, existindo no entanto a possibilidade de alterar a password, tal como seria de esperar.

Em relação ao término de sessão, é possível observar que a sessão é encerrada corretamente, estando as rotas protegidas e que eram previamente acedidas pelo utilizador, tal como a página de gestão de conta, estão agora inacessíveis.

The screenshot shows the Pimacon website with a user session logged in as 'João'. The top navigation bar includes links for PIMAON, SERVIÇOS, COMO FAZER, CAMPANHAS, NOTÍCIAS, CONTACTOS, and a login dropdown menu with options like 'Gerir conta', 'As minhas Compras', 'Produtos pendentes', 'Produtos Vendidos', and 'Logout'. A red banner in the center of the page displays the text '////// Dados Pessoais /////'.

Below the banner, a navigation bar has tabs for 'Perfil' (selected), 'Moradas de Entrega', 'Newsletter', 'Dados Pessoais', and 'Contactos'. The 'Dados Pessoais' tab is active. The main content area shows a section titled 'Dados Inseridos' with fields for 'Nome*' containing 'João' and 'Nrº Contribuinte' containing '999999990'.

Figura 2.26: Conta com sessão iniciada

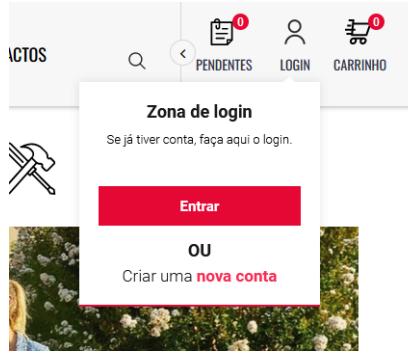


Figura 2.27: Logout efetuado

2.3.3 Contactos

No que diz respeito aos Contactos disponibilizados na plataforma, é possível obter o contacto de telefone da empresa, assim como o email. Tal como vimos no Airbnb, é possível efetuar ataques de Social Engineering através da rede fixa, ao entrar em contacto com um trabalhador da empresa, tentando obter informações críticas, a explorar vulnerabilidades já conhecidas ou até mesmo a levar os trabalhadores a fornecerem acesso aos atacantes aos sistemas da empresa. Através do email, será possível efetuar o mesmo, onde adicionalmente podem ser enviados, por exemplo, emails de phishing para obtenção de dados sensíveis, tais como informações de acesso de contas com acesso privilegiado na plataforma, informações de acesso a contas bancárias, entre outros.

Finalmente, é possível obter a morada do local físico da empresa, sendo que um atacante poderá usar essa informação para entrar em contacto direto com trabalhadores da empresa.



Figura 2.28: Página de contactos

2.3.4 Redes Sociais

Em termos de Redes Sociais, é possível verificar que a Pimacon usa Facebook, X, Instagram, Youtube e Pinterest.



Figura 2.29: Redes Sociais

À semelhança do Airbnb, é possível entrar em contacto com a empresa através destas plataformas e o conteúdo que é divulgado nas mesmas é também ele para publicitar os serviços e produtos oferecidos pela mesma, sem existirem publicações com informações potencialmente perigosas, tal como informações sobre trabalhadores. Existe no entanto um outro contacto divulgado no Facebook e que não se encontrava na plataforma, nomeadamente "marketing@pimacon.pt".

2.3.5 Ofertas de Emprego

Em termos de ofertas de emprego, não foi encontrada nenhuma referência à procura de trabalhadores para a Pimacon, sendo que esta, ou não se encontra de momento à procura de雇用 novos trabalhadores, ou é potencialmente um processo sobre o qual apenas se conseguirá obter informações contactando os vários contactos expostos até agora ou então indo até ao espaço físico da Pimacon. Tendo os contactos e sabendo a morada da loja, uma atacante poderia fazer uso dessas informações e tentar obter informações sobre eventuais Ofertas de Emprego com o objetivo de descobrir mais sobre a empresa.

2.3.6 Whois

Nesta secção e na próxima, irá ser feito o mesmo que foi feito para o Airbnb. Começando pelo comando "whois pimacon.com":

```
$ whois pimacon.com
Domain Name: PIMACON.COM
Registry Domain ID: 1589633763_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.no-ip.com
Registrar URL: http://www.noip.com
Updated Date: 2024-03-16T15:31:39Z
Creation Date: 2010-03-21T20:01:38Z
Registry Expiry Date: 2025-03-21T20:01:38Z
Registrar: Vitalwerks Internet Solutions, LLC DBA No-IP
Registrar IANA ID: 1327
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: STATIC-1.NO-IP.COM
Name Server: STATIC-2.NO-IP.COM
Name Server: STATIC-3.NO-IP.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
```

Figura 2.30: Whois pimacon.com

```
Registrars.
Domain Name: PIMACON.COM
Registry Domain ID: 1589633763_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.no-ip.com
Registrar URL: http://www.noip.com/whois/
Updated Date: 2024-03-16T15:31:39+00:00
Creation Date: 2010-03-21T20:01:38+00:00
Registrar Registration Expiration Date: 2025-03-21T20:01:38+00:00
Registrar: Vitalwerks Internet Solutions, LLC / No-IP.com
Registrar IANA ID: 1327
Registrar Abuse Contact Email: abuse@noip.com
Registrar Abuse Contact Phone: +1.7758531883
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Registrant Name: REDACTED, REDACTED
Registrant Organization:
Registrant Street: REDACTED
Registrant City: REDACTED
Registrant State/Province: trofa
Registrant Postal Code: REDACTED
Registrant Country: PT
Registrant Phone: REDACTED
Registrant FAX: REDACTED
Registrant Email: 382f41cd8755637e-1095844@temp-gdpr-privacy.noip.com
Admin Name: REDACTED, REDACTED
Admin Street: REDACTED
Admin Street: REDACTED
Admin City: REDACTED
Admin State/Province: REDACTED
Admin Postal Code: REDACTED
Admin Country: REDACTED
Admin Phone: REDACTED
Admin FAX: REDACTED
Admin Email: 382f41cd8755637e-1095844@temp-gdpr-privacy.noip.com
Tech Name: REDACTED, REDACTED
Tech Organization: REDACTED
Tech Street: REDACTED
Tech Street: REDACTED
Tech City: REDACTED
Tech State/Province: REDACTED
Tech Postal Code: REDACTED
Tech Country: REDACTED
Tech Phone: REDACTED
Tech FAX: REDACTED
Tech Email: 382f41cd8755637e-1095844@temp-gdpr-privacy.noip.com
Billing Name: REDACTED, REDACTED
Billing Organization: REDACTED
Billing Street: REDACTED
Billing Street: REDACTED
Billing City: REDACTED
Billing State/Province: REDACTED
Billing Postal Code: REDACTED
Billing Country: REDACTED
Billing Phone: REDACTED
```

Figura 2.31: Whois pimacon.com

Como é possível observar, os resultados obtidos são bastante semelhantes ao que foi feito ao Airbnb, sendo observável a adição de valores REDACTED a vários campos para esconder a informação referente a esses mesmos campos.

2.3.7 DNS - host, dig, nslookup

Novamente, fazendo uso do comando "host pimacon.com" para obtenção do endereço IP:

```
(kali㉿kali)-[~]
$ host pimacon.com
pimacon.com has address 2.80.62.247
```

Figura 2.32: host pimacon.com

E de seguida, os comandos "whois 2.80.62.247", "nslookup pimacon.com" e "dig pimacon.com", que novamente, apresenta o mesmo tipo de informações dos resultados obtidos para os mesmos comandos para a empresa Airbnb.

```

inetnum:      2.80.0.0 - 2.81.255.255
netname:      MEO-BROADBAND
descr:        PT Comunicacoes S.A.
descr:        Dynamic Address Range
country:      PT
remarks:      NCC#2010044050
admin-c:      TP3302-RIPE
tech-c:       TP3302-RIPE
status:       ASSIGNED PA
mnt-by:       TELEPAC-MNT
mnt-routes:   TELEPAC-MNT
created:     2011-02-02T12:59:27Z
last-modified: 2016-02-05T17:37:05Z
source:       RIPE

role:         MEO-RESIDENCIAL
org:          ORG-TCIS1-RIPE
address:     Local Internet Registry Management
address:     MEO SERVICOS DE COMUNICACOES E MULTIMEDIA S.A.
address:     Av. Fontes Pereira de Melo, 40 - 3 Bl A
address:     Forum Picos - 1069-300 Lisboa
address:     Portugal
phone:       +351-215000000
admin-c:     NPM17-RIPE
admin-c:     DPM37-RIPE
admin-c:     LAS102-RIPE
nic-hdl:    TP3302-RIPE
abuse-mailbox: abuse@mail.telepac.pt
mnt-by:     TELEPAC-MNT
created:   2002-08-12T09:57:20Z
last-modified: 2024-01-05T17:05:50Z
source:     RIPE # Filtered

% Information related to '2.80.0.0/14AS3243'

route:      2.80.0.0/14
descr:      PT Comunicacoes S.A.
origin:     AS3243
mnt-by:     TELEPAC-MNT
created:   2010-04-29T15:31:31Z
last-modified: 2014-01-31T16:18:48Z
source:     RIPE

```

Figura 2.33: whois 2.80.62.247

```

$ dig pimacon.com

; <>> DiG 9.19.1-Debian <>> pimacon.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 8839
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;pimacon.com.           IN      A

;; ANSWER SECTION:
pimacon.com.      60      IN      A      2.80.62.247

```

Figura 2.34: dig pimacon.com

```

$ nslookup pimacon.com
Server:    192.168.1.1
Address:   192.168.1.1#53

Non-authoritative answer:
Name:  pimacon.com
Address: 2.80.62.247

```

Figura 2.35: nslookup pimacon.com

2.4 Estratégias a Implementar e Conclusões

2.4.1 Airbnb

No que diz respeito à empresa Airbnb, de acordo com a busca passiva que foi feita, é seguro dizer que qualquer atacante terá grandes dificuldades em explorar alguma vulnerabilidade, sendo a vertente do Social Engineering a melhor hipótese que um atacante teria em obter informações críticas à segurança da Empresa.

Desde o contacto com o Live Support da empresa, à submissão de currículo e possível

entrevista de emprego, este contacto com trabalhadores do Airbnb será possivelmente a área mais sensível e propicia de exploração, pelo que será de extrema importância a criação de protocolos/planos de sensibilização e educação dos trabalhadores para eventuais contactos com atacantes que estejam de alguma forma à procura de informações para encontrarem vulnerabilidades, para que estes saibam identificar situações de perigo.

2.4.2 Pimacon

Em relação à Pimacon, para uma empresa de um negócio local, diria que existe de facto algum cuidado em manter informações sobre a empresa com alguma discrição, em que os contactos encontrados dizem respeito apenas a emails ou telefones fixos da empresa, as redes sociais não contêm informações sobre staff ou instrumentos utilizados

No entanto, existe um claro défice de segurança no que diz respeito à política de passwords, sendo que esta deveria obrigar o utilizador a utilizar passwords fortes, dificultando ataques de brute-forcing, e implementar mais uma camada de segurança como a adição de alguma autenticação multi-factor, considerando que a plataforma lida com encomendas e pagamentos online. Tal como no Airbnb, é de extrema importância garantir que os trabalhadores encarregues de atender os clientes na loja física, pelo telefone fixo e de abrir os mails recebidos, sejam consciencializados para a possibilidade da ocorrência de atacantes à procura de aceder a informações confidenciais ou até aos próprios sistemas da empresa

2.4.3 Conclusão

Depois de efetuado um estudo sobre as duas empresas, é principalmente visível a diferença existente entre implementações de uma grande empresa para uma empresa de um negócio local, sendo que no geral, a busca passiva efetuada mostra que até nem existem grandes diferenças a nível da possibilidade da exploração de vulnerabilidades.

Pode ainda existir uma maior diferença na qualidade e experiência de trabalhadores entre as duas empresas, sendo algo que os meios utilizados para a realização destas buscas passivas não nos permitem tirar conclusões.

3 Parte B

Nesta segunda parte, pretende-se criar um ambiente de teste composto por dois sistemas, um sistema auditor, correspondente a uma máquina virtual de Kali Linux, e a um sistema alvo, nomeadamente um sistema Metasploitable 3. O objetivo é o de utilizar técnicas e ferramentas de varredura ativa (scanning), a partir do sistema auditor, para encontrar e identificar vulnerabilidades e fraquezas no sistema alvo. Esta secção será dividida em 5 Questões, em que na primeira não serão usados Scanners de Vulnerabilidades, sendo estes apenas usados nas Questões 2 a 5, mais especificamente o Nessus. Será também utilizado um IDS, mais especificamente o Suricata assim como o Wireshark para análise de tráfego.

3.1 Questão 1

Nesta primeira questão, pretende-se identificar e detalhar vulnerabilidades e fraquezas do sistema alvo, o Metasploitable 3. Para isso, e tendo em conta que não é permitida a utilização de Scanners de Vulnerabilidades, será utilizada a ferramenta Nmap e serão seguidos os passos e estratégias identificados nos slides da Aula PL 02.

3.1.1 Descoberta de Hosts e Dispositivos na Rede

Vamos começar o processo por identificar os hosts e dispositivos presentes na rede. Tal como descrito no enunciado, com o objetivo de manter o ambiente de teste isolado da rede local, foram seguidas as instruções com a configuração para a topologia pretendida, onde são atribuídos os IP's 172.24.x.1 para a máquina Kali Linux e 172.24.x.2 para o máquina com o sistema Metasploitable 3, onde x corresponde a 11 (número do grupo).

Para identificar então os hosts e dispositivos presentes na rede, recorremos ao comando "nmap -sn 172.24.11.0/24", que envia um ping para todos os endereços IP dentro da faixa especificada (172.24.11.0 a 172.24.11.255). É obtido o seguinte resultado:

```
(kali㉿kali)-[~]
└─$ nmap -sn 172.24.11.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-20 12:27 EDT
Nmap scan report for 172.24.11.1
Host is up (0.0011s latency).
Nmap scan report for 172.24.11.2
Host is up (0.0010s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 2.63 seconds
```

Figura 3.1: nmap -sn 172.24.11.0/24

É possível verificar que os hosts encontrados correspondem aos sistemas Kali Linux e Metasploitable cujos IP's foram configurados de acordo com o enunciado, tal como seria de esperar.

3.1.2 Sistema Operativo

Tendo em conta que a maioria dos exploits existentes são respetivos a Sistemas Operativos específicos, será importante verificar qual é o Sistema Operativo do sistema alvo em questão. Para isto, vamos tentar obter informações das seguintes maneiras:

- Recurso ao comando "nmap -O 172.24.11.2- Este comando vai enviar uma série de pacotes de sondagem ao host especificado e analisará as respostas recebidas para tentar identificar características únicas do sistema operacional em execução.
- Application banner - A execução do comando "nmap -sV 172.24.11.2" vai identificar serviços com ports TCP abertas, incluindo as suas versões, em que estas poderão também fornecer informações sobre o OS em questão.
- Packet analysis - Finalmente, vai ser usado o Wireshark para analisar pacotes do tráfego gerado pelo sistema Metasploitable e verificar se existirão informações referentes ao OS.

nmap -O 172.24.11.2

O resultado obtido com o comando "nmap -O 172.24.11.2" foi o seguinte:

```
MAC Address: 08:00:27:7D:82:82 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7
OS CPE: cpe:/o:microsoft:windows_7::sp1
OS details: Microsoft Windows 7 SP1
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.35 seconds
```

Figura 3.2: nmap -O 172.24.11.2

nmap -sV 172.24.11.2

O resultado obtido com o comando "nmap -sV 172.24.11.2" foi o seguinte:

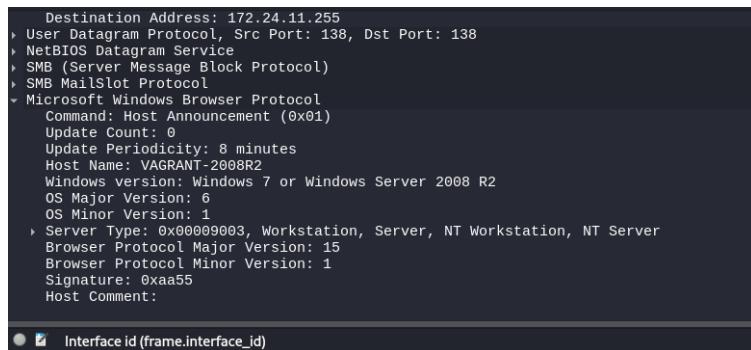
```
Not shown: 978 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
22/tcp    open  ssh              OpenSSH 7.1 (protocol 2.0)
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn      Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds    Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3000/tcp  open  http             WEBrick httpd 1.3.1 (Ruby 2.3.3 (2016-11-21))
3306/tcp  open  mysql            MySQL 5.5.20-log
3389/tcp  open  ms-wbt-server?
4348/tcp  open  ssl/http         Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
7676/tcp  open  java-message-service Java Message Service 3.01
8009/tcp  open  ajp13            Apache Jserv (Protocol v1.3)
8022/tcp  open  http             Apache Tomcat/Coyote JSP engine 1.1
8031/tcp  open  ssl/unknown
8080/tcp  open  http             Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
8181/tcp  open  ssl/http         Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
8383/tcp  open  http             Apache httpd
8443/tcp  open  ssl/https-alt?
9200/tcp  open  wap-wsp?
49152/tcp open  msrpc            Microsoft Windows RPC
49153/tcp open  msrpc            Microsoft Windows RPC
49154/tcp open  msrpc            Microsoft Windows RPC
49155/tcp open  unknown
49156/tcp open  msrpc            Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version, please submit
```

Figura 3.3: nmap -sV 172.24.11.2

Este comando é bastante importante uma vez que o seu resultado vai ser usado a seguir para a identificação dos serviços a correr nas portas abertas para posterior estudo das vulnerabilidades.

Packet Analysis

Para analisar pacotes que possivelmente forneçam informações sobre o OS do sistema alvo, é então usado o Wireshark:



The screenshot shows a Wireshark interface with a single selected packet. The packet details pane displays the following information:

- Destination Address: 172.24.11.255
- User Datagram Protocol, Src Port: 138, Dst Port: 138
- NetBIOS Datagram Service
- SMB (Server Message Block Protocol)
- SMB Mailslot Protocol
- Microsoft Windows Browser Protocol
 - Command: Host Announcement (0x01)
 - Update Count: 0
 - Update Periodicity: 8 minutes
 - Host Name: VAGRANT-2008R2
 - Windows version: Windows 7 or Windows Server 2008 R2
 - OS Major Version: 6
 - OS Minor Version: 1
 - Server Type: 0x000009003, Workstation, Server, NT Workstation, NT Server
 - Browser Protocol Major Version: 15
 - Browser Protocol Minor Version: 1
 - Signature: 0xaaf5
 - Host Comment:

Figura 3.4: Wireshark - Sistema Operativo

De acordo com todos os resultados obtidos até agora, é possível concluir que o Sistema Operativo do sistema alvo corresponde ao Windows 7, com a atualização do Windows 7 SP1 (Service Pack1) que inclui uma série de correções de segurança e melhorias de estabilidade para o Windows 7, assim como a inclusão de componentes do Windows Server 2008 R2.

3.1.3 Port Scanning e Serviços

Nesta secção, vamos então fazer um scanning dos ports e serviços presentes no sistema alvo ao executar comandos que enviam pacotes e que permitem a identificação de ports abertos, fechados ou "stealth".

Se um port estiver aberto, este responde afirmativamente ao pacote, indicando que existe um serviço ou aplicação a ouvir nesse mesmo port, enquanto que se estiver fechado, responde negativamente ao pacote enviado. Finalmente, se estiver num estado "stealth" não será obtida resposta.

De acordo com os slides, o comando "nmap -sS 172.24.11.2" permitiria descobrir quais os serviços a correr para determinados ports TCP, mas como o objetivo é o de explorar posteriormente as vulnerabilidades adjacentes aos serviços encontrados, usaremos antes os resultados já obtidos com o comando "nmap -sV 172.24.11.2", que nos dará informação sobre as versões dos respetivos serviços. Apresentando novamente os resultados do comando, temos:

```

Not shown: 978 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
22/tcp    open  ssh              OpenSSH 7.1 (protocol 2.0)
135/tcp   open  msrpc           Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds    Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3000/tcp  open  http             WEBrick httpd 1.3.1 (Ruby 2.3.3 (2016-11-21))
3306/tcp  open  mysql            MySQL 5.5.20-log
3389/tcp  open  ms-wbt-server?
4484/tcp  open  ssl/http         Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
7676/tcp  open  java-message-service Java Message Service 301
8009/tcp  open  ajp13            Apache Jserv (Protocol v1.3)
8022/tcp  open  http             Apache Tomcat/Coyote JSP engine 1.1
8031/tcp  open  ssl/unknown
8080/tcp  open  http             Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
8181/tcp  open  ssl/http         Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
8383/tcp  open  http             Apache httpd
8443/tcp  open  ssl/https-alt?
9200/tcp  open  wap-wsp?
49152/tcp open  msrpc           Microsoft Windows RPC vx2000application
49153/tcp open  msrpc           Microsoft Windows RPC vx2000application
49154/tcp open  msrpc           Microsoft Windows RPC emx2001com
49155/tcp open  unknown
49156/tcp open  msrpc           Microsoft Windows RPC vx2000application
1 service unrecognized despite returning data. If you know the service/version, please submit

```

Figura 3.5: nmap -sV 172.24.11.2

Dos 1000 ports TCP encontrados, é possível verificar a existência de 978 ports fechados e 22 ports abertos com serviços a correr e respetivas versões, sendo que apenas 1 dos serviços não é reconhecido. Inicialmente existiam 2 serviços não reconhecidos e novas tentativas de correr o comando "nmap -sV ..." permitiram reconhecer um dos 2 serviços, no entanto, um deles permaneceu no mesmo estado.

Apesar de ser referido nos slides que a maior parte das aplicações interessantes usa TCP para a comunicação, vamos verificar quais as portas abertas e com serviços a correr para UDP. Para isso é executado o comando "nmap -sU 172.24.11.2".

```

└─$ sudo nmap -sU 172.24.11.2
[sudo] password for kali:
Starting Nmap 7.94SNM ( https://nmap.org ) at 2024-03-20 17:04 EDT
Nmap scan report for 172.24.11.2
Host is up (0.00069s latency).
Not shown: 994 closed udp ports (port-unreach)
PORT      STATE      SERVICE
137/udp   open       netbios-ns
138/udp   open|filtered netbios-dgm
500/udp   open|filtered isakmp
4500/udp  open|filtered nat-t-ike
5353/udp  open|filtered zeroconf
5355/udp  open|filtered llmnr
MAC Address: 08:00:27:70:82:82 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 770.16 seconds

```

Figura 3.6: nmap -sU 172.24.11.2

Como podemos observar, em 1000 ports, existem 994 ports fechados, 5 ports de onde não se obteve resposta e apenas um port com um serviço correspondente ao netbios-ns.

Na próxima secção serão abordadas as vulnerabilidades e fraquezas mais recentes ou mais graves para cada um dos serviços apresentados nos ports abertos que foram identificados para portas TCP e UDP.

3.1.4 Vulnerabilidades dos Serviços

Para a identificação e caracterização das vulnerabilidades dos serviços encontrados, vão ser usadas duas metodologias.

Em primeiro lugar, foi corrido o comando "nmap --script "vulns-sV 172.24.11.2", sendo que a execução do mesmo acaba por não devolver vulnerabilidades para todos os serviços. Isto faz com que para os restantes serviços, a procura de vulnerabilidades será feita ao

procurar informações sobre vulnerabilidades para as versões dos serviços encontrados ou vulnerabilidades relacionadas com as integrações dos mesmos serviços com o Sistema Operativo da máquina do Metasploitable 3.

ssh (Port 22)

Para o serviço ssh, foram obtidas as seguintes vulnerabilidades (cerca de 80 no total):

```
22/tcp open ssh          OpenSSH 7.1 (protocol 2.0)
| vulners:
| cpe:/a:openbsd:openssh:7.1:
|   PRION: CVE-2016-8858      7.8      https://vulners.com/prion/PRION: CVE-2016-8858
|   PRION: CVE-2016-6515      7.8      https://vulners.com/prion/PRION: CVE-2016-6515
|   PACKETSTORM:140070       7.8      https://vulners.com/packetstorm/PACKETSTORM:140070      *EXPLOIT*
|   EXPLOITPACK:5BCA798C6BA71FAE29334297EC0B6A09      7.8      https://vulners.com/exploitpack/EXPLOITPACK:5BCA798C6BA71FAE29334297EC0B6A09      *EXPLOIT*
|   EDB-ID:40888      7.8      https://vulners.com/exploitdb/EDB-ID:40888      *EXPLOIT*
|   CVE-2016-8858      7.8      https://vulners.com/cve/CVE-2016-8858
|   CVE-2016-6515      7.8      https://vulners.com/cve/CVE-2016-6515
|   1337DAY-ID-26494      7.8      https://vulners.com/zdt/1337DAY-ID-26494      *EXPLOIT*
|   SSV:92579      7.5      https://vulners.com/seebug/SSV:92579      *EXPLOIT*
|   PRION: CVE-2016-1908      7.5      https://vulners.com/prion/PRION: CVE-2016-1908
|   PRION: CVE-2016-10009      7.5      https://vulners.com/prion/PRION: CVE-2016-10009
|   PACKETSTORM:173661      7.5      https://vulners.com/packetstorm/PACKETSTORM:173661      *EXPLOIT*
|   CVE-2016-1908      7.5      https://vulners.com/cve/CVE-2016-1908
|   CVE-2016-10009      7.5      https://vulners.com/cve/CVE-2016-10009
|   1337DAY-ID-26576      7.5      https://vulners.com/zdt/1337DAY-ID-26576      *EXPLOIT*
|   SSV:92582      7.2      https://vulners.com/seebug/SSV:92582      *EXPLOIT*
|   PRION: CVE-2016-10012      7.2      https://vulners.com/prion/PRION: CVE-2016-10012
|   PRION: CVE-2015-8325      7.2      https://vulners.com/prion/PRION: CVE-2015-8325
|   CVE-2016-10012      7.2      https://vulners.com/cve/CVE-2016-10012
|   CVE-2015-8325      7.2      https://vulners.com/cve/CVE-2015-8325
|   SSV:92580      6.9      https://vulners.com/seebug/SSV:92580      *EXPLOIT*
|   PRION: CVE-2016-10010      6.9      https://vulners.com/prion/PRION: CVE-2016-10010
|   CVE-2016-10010      6.9      https://vulners.com/cve/CVE-2016-10010
|   1337DAY-ID-26577      6.9      https://vulners.com/zdt/1337DAY-ID-26577      *EXPLOIT*
|   PRION: CVE-2019-6111      5.8      https://vulners.com/prion/PRION: CVE-2019-6111      5.8      https://vulners.com/exploitpack/EXPLOITPACK:98FE96309F9524BBC84C508837551A19      *EXPLOIT*
|   EXPLOITPACK:98FE96309F9524BBC84C508837551A19      5.8      https://vulners.com/exploitpack/EXPLOITPACK:98FE96309F9524BBC84C508837551A19      *EXPLOIT*
```

Figura 3.7: SSH - CVE-2016-8858

Tal como referido incialmente, utilizando o CVSS como factor de escolha para a vulnerabilidade, foi escolhida a vulnerabilidade CVE-2016-8858. [<https://vulners.com/prion/PRION: CVE-2016-8858>]

A CVE-2016-8858 afeta o OpenSSH, uma implementação amplamente utilizada do protocolo SSH. Esta foi descoberta em 2016, sendo classificada como uma vulnerabilidade de negação de serviço (Denial of Service). A vulnerabilidade reside na função `kex_input_kexinit` no arquivo `kex.c` nas versões 6.x e 7.x do OpenSSH até a versão 7.3 e permite que atacantes remotos causem uma negação de serviço, consumindo grandes quantidades de memória, ao enviar várias solicitações KEXINIT duplicadas. O KEXINIT é um componente importante da negociação de chaves no protocolo SSH, e a exploração dessa vulnerabilidade pode levar a um esgotamento de recursos no servidor OpenSSH, resultando numa interrupção do serviço para usuários legítimos.

É importante notar que, embora a CVE-2016-8858 possa levar a uma negação de serviço, a comunidade do OpenSSH não a considerou como um problema de segurança significativo, muito provavelmente devido à natureza específica da exploração da vulnerabilidade e à sua capacidade limitada de causar danos para além da interrupção temporária do serviço.

msrpc (Port 135)

O msrpc é um mecanismo de comunicação utilizado pelo sistema operacional Windows para permitir que processos em sistemas distribuídos comuniquem entre si de forma

remota.

Para este serviço, o script de procura de vulnerabilidades não devolveu nenhum resultado, pelo que foi preciso investigar se existiriam vulnerabilidades conhecidas para o OS em causa.

De acordo com as informações encontradas, existem várias vulnerabilidades, tal como CVE-2019-1226, CVE-2019-1290, CVE-2020-0610, em que todas partilham algumas semelhanças. Estas envolvem geralmente uma falha na validação de entrada ou no processamento de dados por parte do serviço RPC, onde acabam por permitir a execução de código arbitrário por um atacante, ao enviar dados especialmente manipulados para o serviço msrpc. Por exemplo, um atacante pode enviar uma solicitação RPC contendo dados maliciosos ou manipulados que exploram uma falha de buffer overflow, uma condição de corrida, uma referência de memória inválida, entre outros.

É importante também referir que este serviço não se encontra operacional apenas no port 135, mas também nos ports 49152, 49153, 49154 e 49516. Fica a questão de se o port 49155 com o serviço não reconhecido, classificado como Unknown, não seria também este um serviço msrpc.

netbios-ssn (Port 139)

Para o serviço netbios-ssn, tal como no anterior, não foram encontradas vulnerabilidades com o script. Após uma verificação das vulnerabilidades referentes ao OS do sistema alvo, encontramos as CVE-2009-3676, CVE-2016-3213, CVE-2016-3299, CVE-2017-0161 e CVE-2017-0174, sendo a CVE-2017-0161 a mais grave.

Esta consiste numa vulnerabilidade de execução remota de código que ocorre devido a uma falha no tratamento de objetos na memória do sistema durante o processamento de pacotes. Um atacante remoto poderia explorar essa vulnerabilidade enviando pacotes especialmente criados para o serviço, o que poderia resultar na execução de código arbitrário no sistema alvo.

microsoft-ds (Port 445)

Para este serviço, a informação sobre as vulnerabilidades obtidas só aparecem no fim da execução do comando, estando esta presente na imagem que se segue:

```
Host script results:
|_ smb-vuln-ms10-054: false
|_ smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_ Samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
smb-vuln-ms17-010:
  VULNERABLE: Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
  State: VULNERABLE
  IDs: CVE:CVE-2017-0143
  Risk factor: HIGH
  A critical remote code execution vulnerability exists in Microsoft SMBv1 servers (ms17-010).
  Disclosure date: 2017-03-14
  References:
    https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
    https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
    https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
```

Figura 3.8: MSRPC - CVE-2017-0143

A CVE-2017-0143, conhecida como EsteemAudit, é uma vulnerabilidade crítica que afeta o protocolo SMB no Windows. Esta permite que um atacante execute código arbitrário num sistema Windows vulnerável, sem a necessidade de autenticação. Como resultado, os atacantes podem ganhar controlo total sobre o dispositivo comprometido. Esta vulnerabilidade, assim como o EternalBlue CVE-2017-0144, uma vulnerabilidade muito semelhante à 0143, representa uma ameaça significativa à segurança dos sistemas Windows e foi amplamente explorada por criminosos cibernéticos para realizar ataques de alto impacto.

http (Port 3000)

No port 3000, o serviço HTTP presente corresponde ao WEBrick httpd 1.3.1 (Ruby 2.3.3). Uma vez que este serviço é parte integrante do Ruby, as vulnerabilidades são geralmente relatadas em relação ao próprio Ruby, no entanto, existe uma vulnerabilidade, a CVE-2017-17742, que envolve uma condição de negação de serviço no parser YAML em Ruby. Um atacante pode explorar essa falha para causar uma DoS, resultando numa interrupção do serviço, afetando assim aplicações web que usam o WEBrick como servidor HTTP.

mysql (Port 3306)

Novamente, não foram encontradas vulnerabilidades pelo script, sendo no entanto dada a versão do serviço mysql, nomeadamente o MySQL 5.5.20-log, permitindo que seja feita uma pesquisa para encontrar vulnerabilidades para esta versão.

No que diz respeito aos resultados encontrados, a vulnerabilidade CVE-2016-6662 parece ser a que teve mais impacto, em que esta permitia que um atacante comprometesse o servidor MySQL através de comandos SQL injetados, podendo levar à execução remota de código ou ações maliciosas na base de dados.

ms-wbt-server (Port 3389)

Para este serviço, não são apresentadas nenhuma vulnerabilidades nem existem informações sobre versões. No entanto, após alguma pesquisa, foram encontradas algumas vulnerabilidades, incluindo a CVE-2019-0708, mais conhecida como BlueKeep. Esta é uma vulnerabilidade crítica que afeta o serviço RDP em versões mais antigas do Windows, incluindo o Windows 7 e o Windows Server 2008. A BlueKeep permite a execução remota de código sem autenticação e poderia ser explorada para propagar malware.

ssl/http (Port 4848 + 8080 + 8181)

No port 4848, é possível observar um determinado serviço ssl/http a correr, mais especificamente o Oracle Glassfish 4.0 (Servlet 3.1 JSP 2.3; Java 1.8). Podemos também observar que os serviços nos ports 8080 e 8181 correm também uma instância do mesmo serviço, pelo que as vulnerabilidades encontradas, poderão de facto ser exploradas para esses ports também.

Em relação às vulnerabilidades encontradas, foi encontrado o seguinte:

```

http-server-header: GlassFish Server Open Source Edition 4.0
ssl-dh-params:
  VULNERABLE:
    Diffie-Hellman Key Exchange Insufficient Group Strength
      State: VULNERABLE
        Transport Layer Security (TLS) services that use Diffie-Hellman groups
        of insufficient strength, especially those using one of a few commonly
        shared groups, may be susceptible to passive eavesdropping attacks.
      Check results:
        WEAK DH GROUP 1
          Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA
          Modulus Type: Safe prime
          Modulus Source: RFC2409/Oakley Group 2
          Modulus Length: 1024
          Generator Length: 8
          Public Key Length: 1024
        References:
          https://weakdh.org

```

Figura 3.9: SSL/HTTP

Esta vulnerabilidade refere-se ao uso de grupos Diffie-Hellman (DH) com pouca força em serviços que utilizam o protocolo de segurança Transport Layer Security (TLS), como servidores web. No caso específico mencionado, foi identificado o uso do grupo DH fraco 1, com parâmetros que resultam numa chave pública de apenas 1024 bits. Grupos DH fracos como este podem ser vulneráveis a ataques de escuta passiva, nos quais um atacante pode interceptar e decifrar o tráfego criptografado.

java-message-service (Port 7676)

Para o serviço JMS, foi feita uma pesquisa de vulnerabilidades, uma vez que o script não encontrou qualquer informação. Foram encontradas algumas vulnerabilidades, nomeadamente a CVE-2016-3427, que é uma vulnerabilidade em bibliotecas Java que lidam com a desserialização de objetos. Os atacantes podem explorar essa vulnerabilidade para executar código arbitrário, o que pode afetar aplicativos que usam JMS para comunicação entre componentes. Existe também uma outra vulnerabilidade com um alto CVSS mas que requer a utilização do Apache ActiveMQ em conjunto com o JMS. Uma vez que o mesmo não aparece na lista de serviços para os ports abertos, foi então escolhida a primeira vulnerabilidade.

ajp13 (Port 8009)

Mais uma vez, não são devolvidas quaisquer vulnerabilidades pelo script, havendo no entanto referência da versão do serviço. Após uma pesquisa sobre o serviço Apache Jserv (Protocol v1.3) e possíveis vulnerabilidades, são encontradas várias vulnerabilidades, sendo a mais proeminente a CVE-2020-1938, mais conhecida como Ghostcat, com um CVSS de 9.8.

Esta vulnerabilidade afeta o conector AJP do Apache Tomcat e permite a leitura ou inclusão de arquivos em servidores afetados. Um atacante pode explorar essa falha para aceder a informações confidenciais ou executar ataques de inclusão de arquivos.

http (Port 8022)

Para o serviço do port 8022, foi obtido o serviço Apache Tomcat/Coyote JSP engine 1.1, cujas vulnerabilidades encontradas pelo script são apresentadas de seguida:

```

8022/tcp open http Apache Tomcat/Coyote JSP engine 1.1
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-server-header: Apache-Coyote/1.1
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| vulners:
|   cpe:/a:apache:coyote_http_connector:1.1:
|     PRION:CVE-2023-26044 5.0 https://vulners.com/prion/PRION:CVE-2023-26044
|       PRION:CVE-2022-36032 5.0 https://vulners.com/prion/PRION:CVE-2022-36032
|         OSV:VE-2023-26044 5.0 https://vulners.com/osv/OSV:VE-2023-26044
|           OSV:VE-2022-36032 5.0 https://vulners.com/osv/OSV:VE-2022-36032
|             OSV:BIT-APACHE-2021-31618 5.0 https://vulners.com/osv/OSV:BIT-APACHE-2021-31618

```

Figura 3.10: Apache Tomcat - CVE-2023-26044

Possuindo todas um CVSS de 5.0, foi estudada a vulnerabilidade CVE-2023-26044 em que esta é uma vulnerabilidade no servidor HTTP do ReactPHP. Pode causar um consumo elevado de CPU ao processar HTTP requests de tamanhos grandes, resultando em atrasos significativos no processamento de solicitações legítimas. Esta vulnerabilidade tem pouco ou nenhum impacto na configuração padrão, mas pode ser explorada ao usar explicitamente o RequestBodyBufferMiddleware com configurações muito grandes.

ssl/unknown (Port 8031)

Para o port 8031, não existe informação sobre o serviço a correr, existindo no entanto informações sobre uma vulnerabilidade afetando, tal como nos serviços dos ports 4848, 8080 e 8181, o algoritmo Diffie-Hellman.

```

8031/tcp open ssl/unknown
| ssl-dh-params:
|   VULNERABLE: Posted by James Forshaw, Project Zero
|     Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
|       State: VULNERABLE
|         Transport Layer Security (TLS) services that use anonymous technique which combined numerous issues
|           Diffie-Hellman key exchange only provide protection against passive eavesdropping, and are vulnerable to active man-in-the-middle attacks
|             which could completely compromise the confidentiality and integrity of any data exchanged over the resulting session.
|               Check results:
|                 ANONYMOUS DH GROUP 1
|                   Cipher Suite: TLS_DHE_anon_WITH_AES_128_CBC_SHA
|                     Modulus Type: Non-safe prime
|                       Modulus Source: sun.security.provider/768-bit DSA group with 160-bit prime order subgroup
|                         Modulus Length: 768
|                           Generator Length: 768
|                             Public Key Length: 768
|                               References:
|                                 https://www.ietf.org/rfc/rfc2246.txt

```

Figura 3.11: ssl/unknown (Port 8031)

Neste caso em específico, o script dá-nos informações sobre a vulnerabilidade em si, mais especificamente que serviços de Transport Layer Security (TLS) que utilizam apenas a troca de chaves Diffie-Hellman anônima fornecem proteção apenas contra escuta passiva e são vulneráveis a ataques ativos do tipo homem-no-meio, que poderiam comprometer completamente a confidencialidade e integridade de quaisquer dados trocados durante a sessão resultante.

http (Port 8383)

Para este port, existe um serviço http, mais especificamente o Apache httpd, para o qual o script conseguiu detetar vulnerabilidade CVE-2007-6750, conhecido como Slowloris.

```

8383/tcp open http      syn-ack ttl 128 Apache httpd
|_http-litespeed-sourcecode-download: Request with null byte did not work. This web server might not be vulnerable
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| http-slowloris-check:
| VULNERABLE:
| Slowloris DOS attack
| State: LIKELY VULNERABLE
| IDs: CVE: CVE-2007-6750
| Slowloris tries to keep many connections to the target web server open and hold them open as long as possible. It accomplishes this by opening connections to the target web server and sending a partial request. By doing so, it starves the http server's resources causing Denial Of Service.
| Disclosure date: 2009-09-17
| References:
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|   http://ha.ckers.org/slowloris/

```

Figura 3.12: APACHE HTTPD - CVE-2007-6750

O ataque Slowloris visa manter várias conexões abertas com o servidor web destino e mantê-las abertas pelo maior tempo possível ao enviar solicitações parciais. Com isto, o ataque esgota os recursos do servidor HTTP, causando uma negação de serviço.

ssl/https-alt (Port 8443)

Neste port, existe um serviço sobre o qual não existe grande informação, no entanto, mais uma vez, o script encontrou duas vulnerabilidades, em que uma delas é a CVE-2007-6750, mencionada no port anterior, e a outra é a do serviço no port 8031.

```

8443/tcp open ssl/https-alt?      syn-ack ttl 128
| ssl-dh-params:
| VULNERABLE:
| Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
| State: VULNERABLE
| Transport Layer Security (TLS) services that use anonymous Diffie-Hellman key exchange only provide protection against passive eavesdropping, and are vulnerable to active man-in-the-middle attacks which could completely compromise the confidentiality and integrity of any data exchanged over the resulting session.
| Check results:
| ANONYMOUS DH GROUP 1
|   Cipher Suite: TLS_DH_anon_WITH_AES_128_CBC_SHA
|   Modulus Type: Non-safe prime
|   Modulus Source: sun.security.provider/768-bit DSA group with 160-bit prime order subgroup
|   Modulus Length: 768
|   Generator Length: 768
|   Public Key Length: 768
| References:
|   https://www.ietf.org/rfc/rfc2246.txt
| http-slowloris-check:
| VULNERABLE:
| Slowloris DOS attack exercise, to see whether I can get code executing in a
| State: LIKELY VULNERABLE
| IDs: CVE: CVE-2007-6750
| Slowloris tries to keep many connections to the target web server open and hold them open as long as possible. It accomplishes this by opening connections to the target web server and sending a partial request. By doing so, it starves the http server's resources causing Denial Of Service.
| Disclosure date: 2009-09-17
| References:
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|   http://ha.ckers.org/slowloris/

```

Figura 3.13: SSL/HTTPS-?

wap-wsp? (Port 9200)

Finalmente, como último serviço TCP, o serviço na porta aparenta ser a versão 1.1.1 do Elastic Search, ao contrário do inicialmente apresentado, que se referia aos protocolos Wireless Application Protocol (WAP) - Wireless Session Protocol (WSP), causado provavelmente por um erro de classificação do nmap.

Para a versão do Elastic Search apresentada, não foi encontrada nenhuma vulnerabilidade pelo script. Depois de efetuado uma pesquisa, acabou por ser encontrada a CVE-2015-1427 (ElasticSearch - Search Groovy Sandbox Bypass), que permite que um atacante remoto execute scripts Groovy arbitrários no servidor Elasticsearch, o que pode levar à execução remota de código.

netbios-ns (Port 137)

Como único serviço UDP encontrado, e último serviço para verificação de vulnerabilidades, temos o netbios-ns. Para este, o script de vulnerabilidades do nmap não encontrou qualquer resultado, sendo que após alguma pesquisa, foi encontrada a vulnerabilidade CVE-1999-0621. Esta vulnerabilidade permite que um atacante remoto cause uma negação de serviço através do envio de pacotes UDP malformados para a porta 137, onde o serviço netbios-ns opera. Isto pode resultar na indisponibilidade do serviço NetBIOS e, potencialmente, de outros serviços dependentes do NetBIOS.

3.2 Questão 2

3.2.1 Scan das Vulnerabilidades

Para esta questão 2, é pedido que seja efetuado um processo de varredura activa ao sistema Metasploitable, usando o Nessus, Snort ou Suricata e Wireshark e que seja feita uma avaliação dos resultados obtidos. É pedido também que seja feita uma comparação entre os resultados obtidos e aquilo que foi obtido para o desenvolvimento da primeira questão.

Para dar início ao processo, começa-se por ligar o Wireshark para capturar o tráfego entre o sistema auditor e o sistema alvo, seguido pelo inicio do serviço Suricata, que foi escolhido no lugar do Snort por complicações relacionadas com a visualização dos logs após o scan e finalmente iniciando o scan por parte do Nessus.

Depois de efetuado o scan, foram obtidos os seguintes resultados:

Como é possível observar, um scan de cerca de 27 minutos, detetou uma série de vulnerabilidades. Dentro destas vulnerabilidades, 10 delas são consideradas de severidade crítica, 13 de severidade alta, 34 de severidade média e 4 de severidade baixa. Foram também encontradas 168 vulnerabilidades que não representam uma ameaça direta, com uma classificação de severidade "Info".

De seguida, vamos então fazer um estudo sobre os resultados obtidos.

3.2.2 Vulnerabilidades - Serviços Principais

Para esta primeira parte, vão ser abordadas as vulnerabilidades encontradas para os ports e respetivos serviços encontrados pelo nmap na primeira questão. Será feito para cada port, um levantamento das vulnerabilidades encontradas e uma comparação com os resultados obtidos na primeira questão.

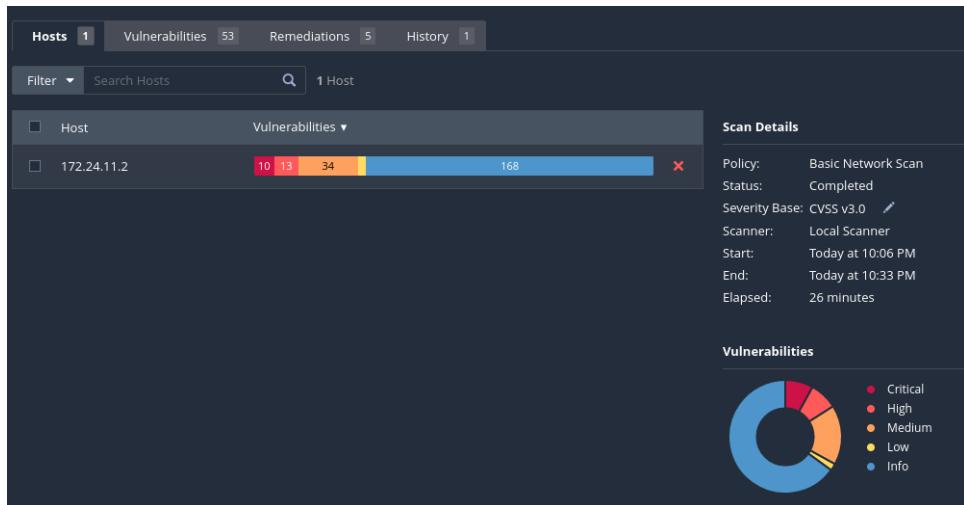


Figura 3.14: Vulnerabilidades obtidas pelo Nessus

ssh (Port 22)

Para o serviço ssh, foi encontrada uma única vulnerabilidade, a CVE-2023-48795, e 9 Infos sem qualquer fator de risco. Este é um resultado bastante diferente daquele obtido pelo nmap, sendo que este último obteve cerca de 80 possíveis vulnerabilidades.

Sev ▾	CVSS ▾	VPR ▾	Name ▾	Family ▾	Count ▾	⋮
<input type="checkbox"/> MIXED	Openbsd Openssh (Multiple Issues)	Misc.	2	<input type="radio"/> <input type="button" value=""/>
<input type="checkbox"/> INFO	SSH (Multiple Issues)	General	2	<input type="radio"/> <input type="button" value=""/>
<input type="checkbox"/> INFO	SSH (Multiple Issues)	Misc.	2	<input type="radio"/> <input type="button" value=""/>
<input type="checkbox"/> INFO	SSH (Multiple Issues)	Service detection	2	<input type="radio"/> <input type="button" value=""/>
<input type="checkbox"/> INFO		Nessus SYN scanner		Port scanners	1	<input type="radio"/> <input type="button" value=""/>
<input type="checkbox"/> INFO		Service Detection		Service detection	1	<input type="radio"/> <input type="button" value=""/>

Figura 3.15: Vulnerabilidades para o Port 22

Para a vulnerabilidade obtida, esta faz referência à possibilidade de um ataque man-in-the-middle conhecido como Terrapin, que permite a um atacante ultrapassar verificações de integridade e enfraquecer a segurança da conexão. Para as restantes vulnerabilidades do tipo "Info" encontradas, estas dizem respeito principalmente a possibilidades de obtenção de informações sobre o serviço, indicando quais são essas informações e como podem ser obtidas, por exemplo, indicando que é possível saber que o algoritmo SHA-1 HMAC é utilizado e que é possível obter informações sobre o serviço ao enviar pedidos de autenticação vazios.

msrpc (Port 135)

Para este serviço, agora identificado como epmap pelo scan do Nessus, foram encontradas apenas 2 vulnerabilidades do tipo "Info", o que vai de encontro ao encontrado pelo nmap. As vulnerabilidades apresentadas na primeira questão não estão aqui identificadas pelo que o sistema do Metasploitable não estará exposto às mesmas.

Sev	CVSS	VPR	Name	Family	Count	
□	INFO	...	Microsoft Windows SMB Service Detection	Windows	1	
□	INFO	...	Nessus SYN scanner	Port scanners	1	

Figura 3.16: Vulnerabilidades para os Ports 135, 139 e 3306

netbios-ssn (Port 139)

Para este serviço, foram encontradas as mesmas vulnerabilidades do tipo "Info" que aquelas encontradas no port 135. As vulnerabilidades mencionadas na questão 1 não fazem parte das vulnerabilidades encontradas pelo scan do Nessus.

microsoft-ds (Port 445)

O port 445, anteriormente detetado como o serviço microsoft-ds, foi agora identificado como o serviço CIFS, também ele uma implementação do protocolo SMB. Para este serviço, foram encontradas 11 vulnerabilidades, dentro delas 1 crítica, 1 média e 9 Infos. A vulnerabilidade crítica corresponde a um conjunto de vulnerabilidades que permite a execução remota de código existentes no SMBv1, nomeadamente CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148 e a média corresponde à falta de autenticação para o servidor remoto SMB.

Sev	CVSS	VPR	Name	Family	Count		
□	MIXED	Microsoft Windows (Multiple Issues)	Windows	2	
□	MIXED	SMB (Multiple Issues)	Misc.	2	
□	INFO	SMB (Multiple Issues)	Windows	5	
□	INFO	...	DCE Services Enumeration	Windows	1		
□	INFO	...	Nessus SYN scanner	Port scanners	1		

Figura 3.17: Vulnerabilidades para o Port 445

Em comparação com os resultados obtidos na primeira questão, podemos observar que ficaram a faltar as 3 vulnerabilidades críticas que o Nessus encontrou e que não foram incluídas na resposta à primeira questão, bem como a vulnerabilidade falta de autenticação.

http (Port 3000)

Neste port foram identificadas 4 vulnerabilidades do tipo Info

Sev ▾	CVSS ▾	VPR ▾	Name ▾	Family ▾	Count ▾	⚙️
INFO	HTTP (Multiple Issues)	Web Servers	2	🔗
INFO			Nessus SYN scanner	Port scanners	1	🔗
INFO			Service Detection (HELP Request)	Service detection	1	🔗

Figura 3.18: Vulnerabilidades para o Port 3000

Estas vulnerabilidades representam apenas caminhos para obtenção de informação sobre o serviço a correr, como tipos e versões, sem qualquer tipo de risco para a segurança. De notar que o Nessus mostra-nos que o serviço a correr é de facto o WEBrick 1.3.1 (Ruby 2.3.3) tal como identificado na primeira questão pelo nmap.

mysql(Port 3306)

Para este serviço, foram encontradas as mesmas vulnerabilidades do tipo "Info" que aquelas encontradas no port 135 e 139. As vulnerabilidades mencionadas na questão 1 não fazem parte das vulnerabilidades encontradas pelo scan do Nessus.

ms-wbt-server (Port 3389)

O serviço a correr no port 3389 é identificado como MSRDP em vez do ms-wbt-server identificado pelo nmap e é um dos serviços que se apresenta como sendo o mais vulnerável a ataques, com um total de 24 vulnerabilidades, entre elas 1 crítica, 4 altas, 7 médias, 1 baixa e 11 Infos.

Sev ▾	CVSS ▾	VPR ▾	Name ▾	Family ▾	Count ▾	⚙️
MIXED	Microsoft Windows (Multiple Issues)	Windows	3	🔗
HIGH	7.5	4.9	SSL Certificate Signed Using Weak Hashing Algorithm	General	1	🔗
MIXED	SSL (Multiple Issues)	General	9	🔗
MEDIUM	6.5	2.5	Remote Desktop Protocol Server Man-in-the-Middle Weakness	General	1	🔗
MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection	1	🔗
MIXED	Microsoft Windows (Multiple Issues)	Misc.	3	🔗
LOW	2.6 *		Terminal Services Encryption Level is not FIPS-140 Compliant	Misc.	1	🔗
INFO	TLS (Multiple Issues)	General	2	🔗
INFO			Nessus SYN scanner	Port scanners	1	🔗
INFO			RDP Screenshot	General	1	🔗
INFO			Remote Desktop Protocol Service Detection	Service detection	1	🔗

Figura 3.19: Vulnerabilidades para o Port 3389

Na primeira questão, foi mencionada a vulnerabilidade BlueKeep, que é de facto a da vulnerabilidade crítica encontrada pelo Nessus, que permite a execução remota de código sem necessidade de autenticação. As outras vulnerabilidades encontradas dizem respeito aos certificados SSL, como o uso de algoritmos fracos de hashing para o signing de certificados, cifras SSL de força média, ataques de man-in-the-middle, versões de TLS desatualizadas, entre outros.

ssl/http (Port 4848 + 8080 + 8181)

Estes ports foram identificados pelo nmap como estando a correr serviços do Oracle Glassfish 4.0, sendo que as vulnerabilidades mencionadas para um port, foram assumidas como verdadeiras para os outros ports. De acordo com o scan do Nessus, este não é de facto o caso uma vez que as vulnerabilidades encontradas para cada um dos ports são diferentes, com a exceção de algumas vulnerabilidades entre o port 4848 e o port 8181 que são iguais.

Começando pelo port 8080, apenas foram encontradas vulnerabilidades do tipo Info que não apresentam riscos de segurança, mas especificamente num total de 6. Estas permitem apenas obter informações sobre o serviço em causa.

Para o port 4848, o cenário já completamente diferente, uma vez que foram encontradas 3 vulnerabilidades altas, 6 médias, 1 baixa e 20 Infos.

Sev ▾	CVSS ▾	VPR ▾	Name ▾	Family ▾	Count ▾	
MIXED	SSL (Multiple Issues)	General	11	○ edit
HIGH	Oracle Glassfish Server (Multiple Issues)	CGI abuses	2	○ edit
MIXED	TLS (Multiple Issues)	Service detection	4	○ edit
LOW	3.7	4.5	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Misc.	1	○ edit
INFO	HTTP (Multiple Issues)	Web Servers	3	○ edit
INFO	Oracle Glassfish Server (Multiple Issues)	Web Servers	2	○ edit
INFO	TLS (Multiple Issues)	General	2	○ edit
INFO			Service Detection	Service detection	2	○ edit
INFO			Nessus SYN scanner	Port scanners	1	○ edit
INFO			SSL Service Requests Client Certificate	Service detection	1	○ edit
INFO			Web Server No 404 Error Code Check	Web Servers	1	○ edit

Figura 3.20: Vulnerabilidades para o Port 4848

Estas vulnerabilidades correspondem às mesmas vulnerabilidades SSL e TLS já mencionadas previamente, assim como o uso de módulos Diffie-Hellman de 1024bits ou menos, tal como mencionado nas secção de vulnerabilidades destes ports para a primeira questão. A grande diferença aqui encontra-se em duas vulnerabilidades de risco alto, nomeadamente Oracle GlassFish Server Path Traversal e Oracle GlassFish Server URL normalization Denial of Service, em que a primeira permite o envio de pedidos HTTP criados especificamente para a exploração e acesso a ficheiros e a segunda permite, através dos mesmos meios, um ataque de negação de serviço.

Finalmente para o port 8181, este é em parte semelhante ao port 4848 em termos das vulnerabilidades encontradas pelo scan, com a diferença de que este não possuí as 2 vulnerabilidades altas mencionadas no port 4848.

Em conclusão, existe de facto uma grande diferença nas vulnerabilidades existentes nestes serviços, especialmente entre os ports 4848 mais o 8181 e o port 8080, que provavelmente se deverá ao facto de possuírem configurações diferentes, como configurações de segurança, permissões de acesso, políticas de firewall, ou por estarem a hospedar aplicações ou serviços adicionais diferentes.

java-message-service (Port 7676)

Para este port, o scan não encontrou qualquer vulnerabilidade para além de 4 vulnerabilidades do tipo Info, o que vai de encontro com o facto de que o nmap também não encontrou qualquer vulnerabilidade. A vulnerabilidade mencionada na primeira questão, e que poderia ser algo explorada para este serviço, parece ser de facto algo que não será possível explorar.

ajp13 (Port 8009)

Neste serviço, o scan encontrou a seguinte vulnerabilidade:

The screenshot shows a Ghostcat report for a critical vulnerability. The title is "Apache Tomcat AJP Connector Request Injection (Ghostcat)". The "Description" section states: "A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE)." The "Solution" section advises: "Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later."

Figura 3.21: Vulnerabilidades para o Port 8009

Apesar de esta vulnerabilidade não ser apresentada pelo nmap, a versão indicada pelo mesmo faz parte das versões afetadas pelo Ghostcat, pelo que esta foi de facto a vulnerabilidade apresentada na primeira questão.

http (Port 8022)

Neste port, foi detetado o serviço Apache Tomcat/Coyote JSP Engine 1.1 tal como aquele identificado pelo nmap, em que foram encontradas 2 vulnerabilidades críticas, 1 alta, 1 média e as restantes 7 Info.

Sev ▾	CVSS ▾	VPR ▾	Name ▾	Family ▾	Count ▾	⚙
Critical	10.0 *	7.3	ManageEngine Desktop Central 8 / 9 < Build 91100 Multiple RCE	CGI abuses	1	🔗
Critical	9.8	5.9	ManageEngine Desktop Central < 10 Build 10.0.533 Integer Overflow	CGI abuses	1	🔗
High	8.8	6.7	ManageEngine Desktop Central 10 < Build 100282 Remote Privilege Escalation	CGI abuses	1	🔗
Medium	6.1	3.0	ManageEngine Desktop Central 9 < Build 92027 Multiple Vulnerabilities	CGI abuses	1	🔗
Info			ManageEngine Endpoint Central Detection	CGI abuses	1	🔗

Figura 3.22: Vulnerabilidades para o Port 8022

Ao contrário daquilo que foi encontrado pelo nmap como vulnerabilidades a que o serviço estaria exposto, as vulnerabilidades que põe a segurança em causa correspondem a versões desatualizadas do ManageEngine Desktop Central, o que provoca uma série de complicações como vulnerabilidades de execução remota de código, negação de serviço através do envio de pedidos HTTP, entre outros.

ssl/unknown (Port 8031)

Pare este port, não foi encontrada qualquer vulnerabilidade. O npm tinha-nos dado uma vulnerabilidade na troca de chaves Diffie-Hellman, no entanto, o scan não encontrou nada.

http (Port 8383)

Neste port, tal como visto na primeira questão, corre um Apache HTTP Server. Em termos de vulnerabilidades, este serviço corresponde a uma mistura do serviço no port 8181 e do port 8022, uma vez que contém todas as vulnerabilidades do port 8181 e contém as vulnerabilidades de risco mais alto que dizem respeito ao já mencionado ManageEngine Desktop Central, devido à sua versão desatualizada.

Sev	CVSS	VPR	Name	Family	Count	
MIXED	Zohocorp Manageengine Desktop Central (Multiple Issues)	CGI abuses	5	
MIXED	SSL (Multiple Issues)	General	10	
MIXED	IETF Md5 (Multiple Issues)	General	2	
MIXED	TLS (Multiple Issues)	Service detection	4	
LOW	3.7	4.5	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Misc.	1	
INFO	HTTP (Multiple Issues)	Web Servers	4	
INFO	TLS (Multiple Issues)	General	2	
INFO			Service Detection	Service detection	2	
INFO			Apache HTTP Server Version	Web Servers	1	
INFO			Nessus SYN scanner	Port scanners	1	
INFO			OpenSSL Detection	Service detection	1	
INFO			SolarWinds Server & Application Monitor (SAM) Detection	CGI abuses	1	

Figura 3.23: Vulnerabilidades para o Port 8383

De notar que a vulnerabilidade encontrada pelo nmap, relacionada com o ataque Slowloris, não foi detetada pelo scan do Nessus.

ssl/https-alt (Port 8443)

Para o port 8443, tal como no nmap, não foi possível obter qualquer informação sobre o serviço a correr, sendo apresentadas 8 vulnerabilidades, 2 de risco médio e 4 do tipo Info.

Sev	CVSS	VPR	Name	Family	Count	
MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection	1	
MEDIUM	5.9	3.6	SSL Anonymous Cipher Suites Supported	Service detection	1	
INFO	SSL (Multiple Issues)	General	2	
INFO	TLS (Multiple Issues)	General	2	
INFO			Nessus SYN scanner	Port scanners	1	
INFO			Service Detection	Service detection	1	

Figura 3.24: Vulnerabilidades para o Port 8443

Ao contrário do que o nmap apresentou como vulnerabilidades, nomeadamente no uso de TLS com troca de chaves Diffie-Hellman e na negação de serviços pelo uso de ataques Slowloris, o scan do Nessus devolveu como vulnerabilidades o uso de TLS 1.0, que contém vários falhas de design criptográfico, e no uso de cifras SSL anónimas pelo host remoto. A primeira é uma vulnerabilidade já encontrada no port 3389, 8181 e 8383, enquanto que a segunda se apresenta apenas para este serviço.

wap-wsp? (Port 9200)

Para o port 9200, foi detetado pelo Nessus o serviço Elasticsearch com a versão 1.1.1, com a vulnerabilidade Elasticsearch Transport Protocol Unspecified Remote Code Execution, tal como mencionado na primeira questão, assim como mais 1 vulnerabilidade crítica e 2 médias. Estas vulnerabilidades descrevem todas a possibilidade de execução remota de código e é sugerido que seja feito um upgrade da versão do Elasticsearch.

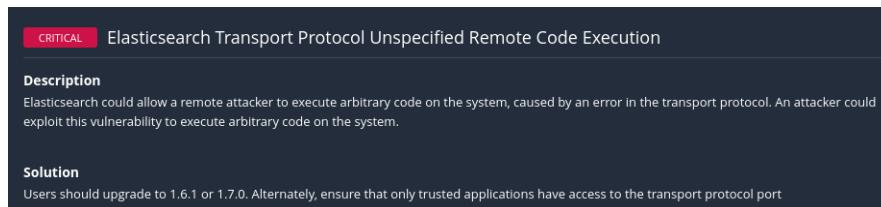


Figura 3.25: Vulnerabilidades para o Port 9200

netbios-ns (Port 137)

Finalmente, para o último port detetado pelo nmap, temos o serviço a correr no port UDP 137, para o qual foi apenas detetada uma vulnerabilidade Info, não tendo qualquer fator de risco para o sistema.

3.2.3 Outros serviços

Para finalizar o estudo do scan efetuado pelo Nessus, foi criado um filtro para verificar se existiria algum port aberto e com vulnerabilidades nos seus serviços que não tivesse sido apanhado pelo nmap, e foram encontrados os seguintes ports:

- 5985 - tcp / www
- 7676 - Tcp / ftp
- 49152 - tcp / dce-rpc
- 49153 - tcp / dce-rpc
- 49154 - tcp / dce-rpc
- 49169 - tcp / dce-rpc
- 49235 - tcp / dce-rpc
- 49236 - tcp / dce-rpc
- N/A - Port e serviço não identificados

Sev	CVSS	VPR	Name	Family	Count
INFO	HTTP (Multiple Issues)	Web Servers	4
INFO			DCE Services Enumeration	Windows	6
INFO			FTP Server Detection	Service detection	1
INFO			OS Identification	General	1
INFO			WS-Management Server Detection	Web Servers	1

Figura 3.26: Vulnerabilidades para ports restantes

Os serviços nestes ports estão expostos apenas a vulnerabilidades do tipo Info, que por sua vez não constituem um risco para a segurança do sistema.

3.2.4 Conclusão dos Scans

Depois de efetuados os scans com as duas ferramentas, é possível afirmar que ambas as ferramentas fornecem informações valiosas sobre os ports abertos, os serviços a correr nesses ports e as vulnerabilidades a que o sistema alvo poderá estar em risco por usar esses serviços.

Na primeira questão, foram obtidos os vários ports e respetivos serviços, sendo no entanto preciso a realização de pesquisas sobre potenciais vulnerabilidades que o serviço em causa poderia ter, quer para a versão do serviço a correr quer para o OS do sistema alvo, uma vez que o nmap não apresentava qualquer vulnerabilidade para muitos dos serviços.

Por outro lado, nesta segunda questão, o Nessus apresentou os vários ports e serviços inicialmente apresentados pelo nmap, com a diferença que apresentou as várias vulnerabilidades para cada um dos serviços, incluindo possíveis resoluções para as mesmas.

Em suma, é possível dizer que a ferramenta Nessus, quando comparada ao nmap, em conjunto com outro tipo de ferramentas como o Suricata e o Wireshark, é claramente mais eficiente e certamente a opção a escolher para a exploração de vulnerabilidade num sistema.

3.3 Questão 3

Nesta questão 3, pretende-se examinar o output do IDS gerado durante o scan do Nessus, bem como a captura de tráfego no Wireshark, para que sejam identificadas duas vulnerabilidades do sistema alvo. Para o exercício, vão ser escolhidas duas vulnerabilidades que não foram incluídas em nenhuma das duas primeiras questões, pelo menos para o port em questão, para evitar repetição de informação e também um pouco em preparação para a próxima questão.

Para a primeira vulnerabilidade, foi encontrado o seguinte:

```
03/26/2024-01:34:25.310198 [**] [1:2034649:1] ET EXPLOIT Apache log4j RCE Attempt (tcp ldap) (CVE-2021-44228) [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 172.24.11.1:40514 -> 172.24.11.2:8019
```

Figura 3.27: IDS - Primeira vulnerabilidade

A vulnerabilidade em questão está identificada como a CVE-2021-44228, com prioridade 1 (alta), também conhecida como Log4Shell, é uma vulnerabilidade crítica descoberta na framework de logging Log4j, que é amplamente utilizada em aplicações Java. Esta permite que um atacante execute código arbitrário remotamente em sistemas que usam o Log4j, simplesmente enviando pedidos HTTP ou outras mensagens que explorem a falha no mecanismo de logging. Isto pode levar a roubo de dados, instalação de malware, interrupção do serviço e comprometimento total do sistema.

Esta vulnerabilidade é considerada crítica devido à sua facilidade de exploração e ao amplo uso do Log4j em aplicações de empresas e em infraestruturas críticas.

Para o tráfego referente aos pacotes trocados que identificam a vulnerabilidade, foi encontrado o seguinte:

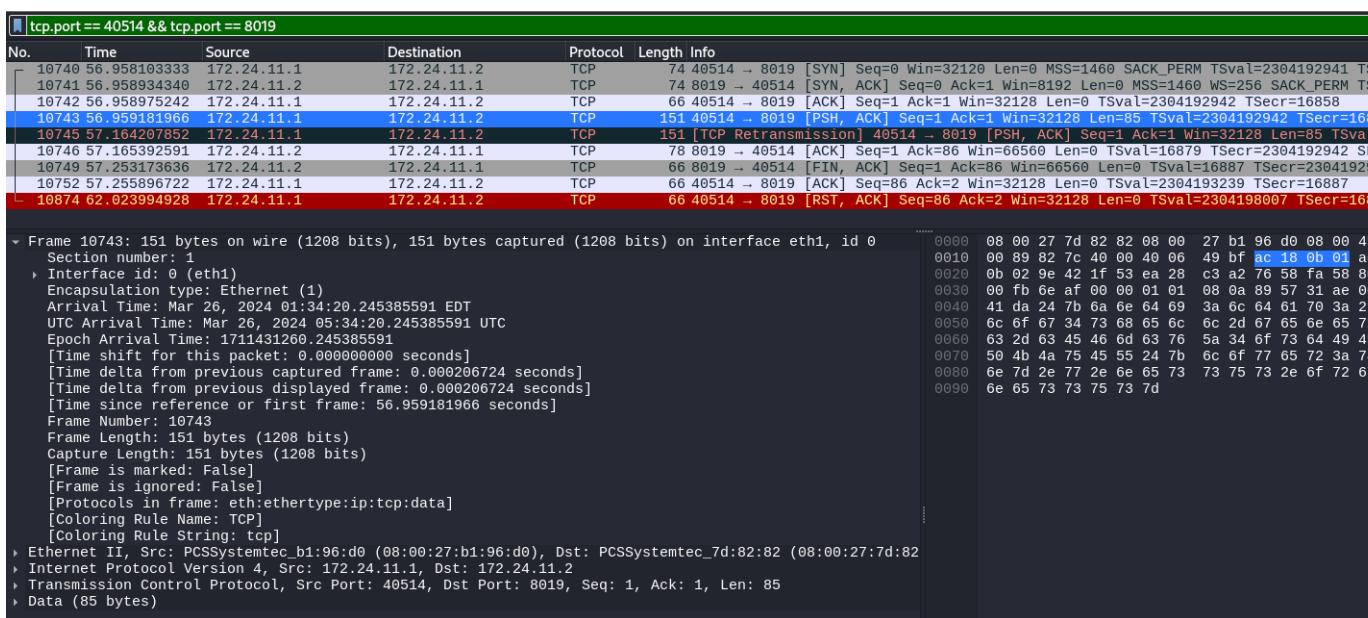


Figura 3.28: Wireshark - Primeira vulnerabilidade

Como segunda vulnerabilidade, foi encontrada a vulnerabilidade CVE-2021-21315, conhecida como "NodeJS System Information Library Command Injection Attempt". Esta envolve uma tentativa de ganho de privilégios de administrador através da exploração de uma falha de injeção de comandos em bibliotecas do NodeJS. Isso permite que um atacante execute comandos arbitrários no sistema afetado, potencialmente comprometendo a integridade e confidencialidade dos dados. Ao explorar esta vulnerabilidade, um atacante pode obter acesso não autorizado e realizar atividades maliciosas no sistema alvo, o que pode levar a consequências graves, incluindo comprometimento total do sistema e perda de dados sensíveis.

```
03/26/2024-02:00:22.600990 [**] [1:2034973:2] ET EXPLOIT NodeJS System Information Library Command Injection Attempt (CVE-2021-21315) [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 172.24.11.1:47958 -> 172.24.11.2:9200
```

Figura 3.29: IDS - Segunda vulnerabilidade

De acordo com a captura de tráfego efetuada pelo Wireshark, é possível observar o tráfego, referente à vulnerabilidade em causa, na imagem que se segue:

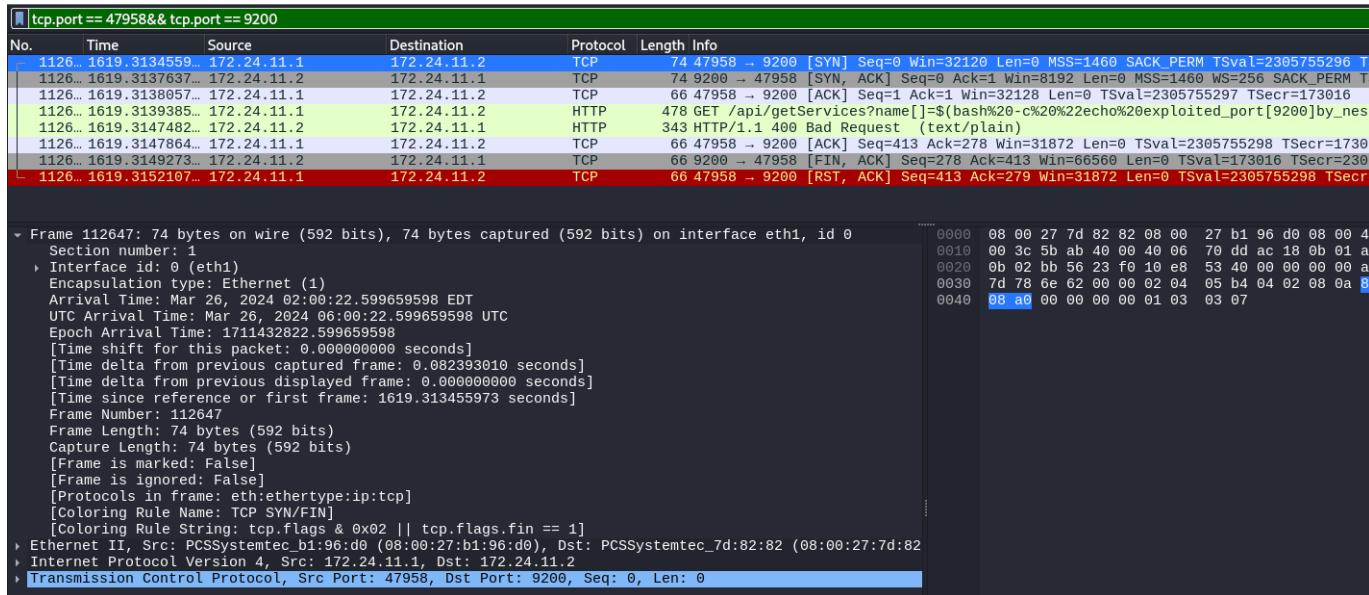


Figura 3.30: Wireshark - Segunda vulnerabilidade

3.4 Questão 4

As diferenças entre as notificações do IDS e as vulnerabilidades relatadas pelo scanner de vulnerabilidades Nessus podem ser atribuídas a uma variedade de fatores. Aqui estão algumas possíveis razões para essas diferenças:

- Falsos Positivos e Alertas do IDS: O IDS pode gerar alertas para atividades que não representam uma verdadeira ameaça de segurança, resultando em falsos positivos. Esses alertas podem ser acionados por atividades benignas que parecem maliciosas devido à interpretação do IDS. Por exemplo, determinadas assinaturas de IDS podem ser muito amplas e gerar alertas para tráfego benigno que se assemelha a ataques conhecidos. Nessas situações, o scanner de vulnerabilidades Nessus pode não encontrar nenhuma vulnerabilidade correspondente, pois não há uma vulnerabilidade real presente.
- Limitações de Varredura do Nessus: O Nessus pode não ser capaz de detectar todas as vulnerabilidades presentes no sistema alvo devido a limitações nas técnicas de varredura ou na cobertura das assinaturas de vulnerabilidades. Algumas

vulnerabilidades podem ser difíceis de detectar ou podem ser específicas para configurações ou ambientes particulares que o Nessus não consegue reproduzir durante a varredura.

- Diferentes Métodos de Detecção: O IDS e o Nessus usam diferentes métodos de detecção de vulnerabilidades. Enquanto o IDS se baseia em assinaturas de ameaças conhecidas, anomalias de tráfego ou análise heurística para gerar alertas, o Nessus depende principalmente de varreduras de portas, análise de serviços e exploração de vulnerabilidades conhecidas. Essas abordagens diferentes podem levar a discrepâncias nos resultados, onde o IDS detecta atividades suspeitas que o Nessus não identifica como vulnerabilidades.
- Falta de Atualizações ou Cobertura Limitada: A falta de atualizações do Nessus, mais especificamente as atualizações de plugins na sua base de dados, pode resultar numa cobertura limitada de ameaças e vulnerabilidades. Os plugins são essenciais para que o Nessus identifique e avalie as vulnerabilidades nos sistemas e redes. Se os plugins não forem atualizados regularmente para incluir as últimas ameaças e vulnerabilidades conhecidas, o Nessus pode não ser capaz de detectar todas as possíveis falhas de segurança presentes nos sistemas aos quais se efetuam os scans.

3.5 Questão 5

Nesta questão, é pedido que sejam escolhidas três vulnerabilidades identificadas pelo Nessus, com o objetivo de as corrigir no sistema Metasploitable 3. Como vimos ao longo desta secção, grande parte das vulnerabilidades mais graves correspondiam a versões desatualizadas que continham vulnerabilidades, havendo no entanto outras que poderiam ser corrigidas sem qualquer update de software. A ideia será encontrar vulnerabilidades e corrigi-las sem recorrer a qualquer update de versão, com o objetivo de dar alguma variedade ao problema em questão.

É importante mencionar que foram feitos scans adicionais, que devolveram o mesmo número de vulnerabilidades críticas, altas, médias e baixas, devolvendo apenas um número diferente de INFO's, pelo que podemos assumir que num eventual scan futuro, se a vulnerabilidade que resolvemos solucionar já não aparecer, que esta foi de facto solucionada.

Os resultados do scan por parte do Nessus depois das vulnerabilidade resolvidas será apresentado no final.

3.5.1 Microsoft RDP RCE (CVE-2019-0708) (BlueKeep)

Como primeira vulnerabilidade, foi escolhida a Microsoft RDP RCE (CVE-2019-0708) (BlueKeep), uma vulnerabilidade crítica presente na secção Microsoft Windows (Multiple Issues), com um CVSS de 9.8, sendo esta uma falha de segurança que permite a execução remota de código em sistemas Windows vulneráveis por meio do serviço Remote Desktop Protocol (RDP).

Na ferramenta Nessus, é possível observar para cada uma das vulnerabilidades, uma secção de soluções, sendo que para esta é dito que a Microsoft já lançou uma série de patches, nomeadamente para o OS em questão. Existem também referências a links para documentos, em que num dos documentos é referido o seguinte como possível solução para esta vulnerabilidade:

Enable Network Level Authentication (NLA) on systems running supported editions of Windows 7, Windows Server 2008, and Windows Server 2008 R2

Posto isto, procedeu-se ao indicado, acedendo a Advanced System Configurations -> System Properties -> Remote e escolhendo a opção "Allow connections only from computers running remote Desktop with Network Level Authentication (more secure)".

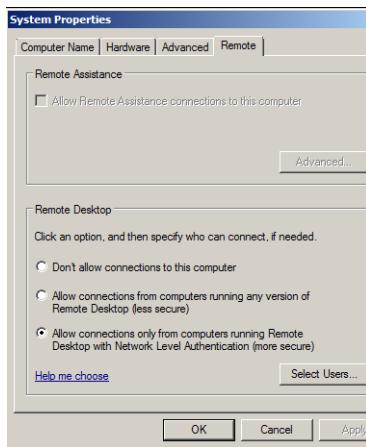


Figura 3.31: Network Level Authentication

3.5.2 Apache Tomcat AJP Connector Request Injection (Ghostcat)

Como segunda vulnerabilidade, foi escolhida mais uma vulnerabilidade crítica, nomeadamente a Apache Tomcat AJP Connector Request Injection (Ghostcat), uma vez que a Solução apresentada pelo Nessus fala de um upgrade da versão do servidor Tomcat ou então de atualizar a configuração do AJP para que este requeira autenticação, sendo a segunda opção aquilo que estamos à procura.

Tal como na vulnerabilidade anterior, o Nessus fornece documentação com os passos para a resolução do problema:

- If your site is **not** using the AJP Connector, disable it by commenting it out from the <TOMCAT_HOME>/conf/server.xml file as:

```
<!-- <Connector port="8009" protocol="AJP/1.3" redirectPort="8443" /> -->
```

Raw

- If AJP connector is required and cannot be commented/deactivated, then we recommend to set a secret password for the AJP conduit - Only requests from workers with the same secret keyword will be accepted. At the Tomcat side, edit conf/server.xml :

```
<Connector port="8009" protocol="AJP/1.3" redirectPort="8443" address="YOUR_TOMCAT_IP_ADDRESS" secret="YOUR_AJP_SECRET" />
```

Raw

Note that `YOUR_AJP_SECRET` must be changed to a value that is highly secure and cannot be easily guessed.

Figura 3.32: Soluções para a Vulnerabilidade

Decidindo deixar o AJP Connector a correr, foi escolhida inicialmente a segunda opção em que é criada uma secret key, o que obriga a que seja obrigatória a autenticação por parte de um cliente que se tente conectar ao conector AJP.

Depois de efetuada a alteração adicionando a secret key e de correr o scan do Nessus, a vulnerabilidade continuou presente. Posto isto, foi necessário recorrer à primeira opção em que se comentou no ficheiro de configuração a linha que faz referência ao conector AJP. Efetuado novamente o scan, o Nessus deixou de detetar a vulnerabilidade tal como pretendido, no entanto, o Tomcat deixará de aceitar conexões AJP nesse port.

3.5.3 SMB Signing not required

Para terceira e última vulnerabilidade, foi escolhida a vulnerabilidade SMB Signing not required, presente na secção do scan "SMB (Multiple Issues)", uma vez que já não havia mais nenhuma de risco crítico que fosse resolvida sem ser com upgrade de versões e que o enunciado pedia que fosse corrigida uma vulnerabilidade de risco médio.

Esta é uma vulnerabilidade em que um atacante consegue executar man-in-the-middle attacks pela falta de autenticação no servidor SMB remoto. Para a sua resolução, foi seguido aquilo que a página da vulnerabilidade do Nessus nos apresenta:

MEDIUM SMB Signing not required

Description
Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

Solution
Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

Figura 3.33: SMB Signing not required

Tal como é possível observar na imagem, é preciso alterar as definições referentes ao "Microsoft Network Server: Digitally Sign Communications (always)", de maneira a que esta opção esteja de facto enabled. Isto é feito ao navegar até ao Editor de Diretivas de Segurança local (Win + R (secpol.msc)), depois Políticas Locais -> Opções de Segurança. Uma vez nesta zona, só é preciso editar o campo correspondente à definição mencionada em cima de modo a que esta fique Enabled, tal como na imagem seguinte:

Microsoft network server: Amount of idle time required before su...	15 minutes
Microsoft network server: Digitally sign communications (always)	Enabled
Microsoft network server: Digitally sign communications (if client a...	Disabled
Microsoft network server: Disconnect clients when logon hours e...	Enabled
Microsoft network server: Server SPN target name validation level	Not Defined

Figura 3.34: Microsoft Network Server: Digitally Sign Communications (always)

3.5.4 Conclusão - Questão 5

Uma vez concluídas as correções das 3 vulnerabilidades escolhidas, resta apresentar as provas dessa mesma correção. Isto será feito recorrendo a uma imagem do primeiro scan efetuado, onde todas as vulnerabilidades estavam presentes, e comparando-a a uma imagem do scan onde as vulnerabilidades já se encontram de facto corrigidas.



Figura 3.35: Contagem das Vulnerabilidades - 1º Scan

Vulnerability Type	Severity	Impact	Description	Databases	Count	Actions
Protocol Issues	Critical	9.8	Elasticsearch Transport Protocol Unspecified Remote Code Execution		1	<input type="radio"/> <input type="checkbox"/>
Protocol Issues	Mixed	...	Zohocorp Manageengine Desktop Central (Multiple Issues)	CGI abuses	10	<input type="radio"/> <input type="checkbox"/>
Protocol Issues	Mixed	...	Microsoft Windows (Multiple Issues)	Windows	8	<input type="radio"/> <input type="checkbox"/>
Protocol Issues	Mixed	...	Elasticsearch (Multiple Issues)	CGI abuses	4	<input type="radio"/> <input type="checkbox"/>
Protocol Issues	Mixed	...	Apache Tomcat (Multiple Issues)	Web Servers	2	<input type="radio"/> <input type="checkbox"/>
Protocol Issues	Mixed	...	SSL (Multiple Issues)	General	43	<input type="radio"/> <input type="checkbox"/>
Protocol Issues	Mixed	...	IETF Md5 (Multiple Issues)	General	3	<input type="radio"/> <input type="checkbox"/>
Protocol Issues	High	...	Oracle Glassfish Server (Multiple Issues)	CGI abuses	2	<input type="radio"/> <input type="checkbox"/>
Protocol Issues	Medium	6.5	Remote Desktop Protocol Server Man-in-the-Middle Weakness	General	1	<input type="radio"/> <input type="checkbox"/>
Protocol Issues	Medium	5.9	SSL Anonymous Cipher Suites Supported	Service detection	1	<input type="radio"/> <input type="checkbox"/>
Protocol Issues	Mixed	...	TLS (Multiple Issues)	Service detection	14	<input type="radio"/> <input type="checkbox"/>
Protocol Issues	Mixed	...	Microsoft Windows (Multiple Issues)	Misc.	3	<input type="radio"/> <input type="checkbox"/>
Protocol Issues	Mixed	...	Openbsd Openssh (Multiple Issues)	Misc.	2	<input type="radio"/> <input type="checkbox"/>
Protocol Issues	Mixed	...	SMB (Multiple Issues)	Misc.	2	<input type="radio"/> <input type="checkbox"/>
Protocol Issues	Low	3.7	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Misc.	3	<input type="radio"/> <input type="checkbox"/>
Protocol Issues	Low	2.6 *	Terminal Services Encryption Level is not FIPS-140 Compliant	Misc.	1	<input type="radio"/> <input type="checkbox"/>
Protocol Issues	Informational	...	HTTP (Multiple Issues)	Web Servers	24	<input type="radio"/> <input type="checkbox"/>

Figura 3.36: Listagem das Vulnerabilidades - 1º Scan

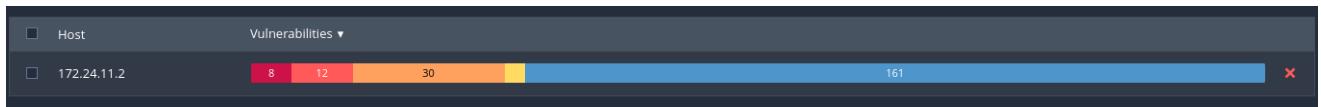


Figura 3.37: Contagem das Vulnerabilidades - 2º Scan

Sev	CVSS	VPR	Name	Family	Count	Actions
CRITICAL	9.8	6.7	Elasticsearch Transport Protocol Unspecified Remote Code Execution	Databases	1	
MIXED	Zohocorp Manageengine Desktop Central (Multiple Issues)	CGI abuses	10	
MIXED	Microsoft Windows (Multiple Issues)	Windows	6	
MIXED	Elasticsearch (Multiple Issues)	CGI abuses	4	
MIXED	SSL (Multiple Issues)	General	43	
MIXED	IETF Md5 (Multiple Issues)	General	3	
HIGH	Oracle Glassfish Server (Multiple Issues)	CGI abuses	2	
MEDIUM	5.9	3.6	SSL Anonymous Cipher Suites Supported	Service detection	1	
MIXED	TLS (Multiple Issues)	Service detection	14	
MIXED	Openbsd Openssh (Multiple Issues)	Misc.	2	
LOW	3.7	4.5	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Misc.	3	
INFO	HTTP (Multiple Issues)	Web Servers	22	

Figura 3.38: Listagem das Vulnerabilidades - 1º Scan

Como podemos ver pelas 4 imagens, as vulnerabilidades críticas BlueKeep e Ghostcat, inseridas respetivamente nas secções Microsoft Windows (Multiple Issues) e Apache Tomcat (Multiple Issues), desapareceram, bem como a vulnerabilidade média do SMB Signing presente na secção do SMB (Multiple Issues). De notar que pelas alterações que foram efetuadas, houve outras vulnerabilidades corrigidas, nomeadamente 1 alta, 3 médias e 1 baixa, uma vez que estas vulnerabilidades estavam de certo modo ligadas às alterações que foram feitas.

4 Conclusão

4.1 Conclusões e Considerações Finais

Neste trabalho prático sobre tecnologias de segurança, exploramos duas abordagens distintas para avaliar e fortalecer a postura de segurança de sistemas e infraestruturas. Na primeira parte, empregamos técnicas de coleta passiva de informações para investigar os sistemas de duas entidades diferentes. Ao analisar os resultados, identificamos algumas discrepâncias nas práticas de segurança adotadas, destacando riscos potenciais e fornecendo recomendações para reforçar a segurança.

Na segunda parte, concentramo-nos na identificação de vulnerabilidades num ambiente controlado, utilizando ferramentas e técnicas de varredura ativa como o Nessus e o Suricata, cujos resultados da varredura, nos permitiram destacar vulnerabilidades críticas, médias ou informativas presentes no sistema alvo.

No fundo, este trabalho prático reforçou a necessidade de uma abordagem proativa para fortalecer a segurança de um sistema, enfatizando a importância da deteção precoce e da correção eficaz de vulnerabilidades. Ao implementar as recomendações fornecidas para as vulnerabilidades encontradas e mantendo uma vigilância contínua sobre as ameaças emergentes, as organizações podem melhorar significativamente a sua resiliência contra ataques cibernéticos.

4.2 Trabalho Futuro

Para trabalhos futuros, seria interessante efetuar este tipo de análise em maior escala, em diferentes ambientes ou em sistemas mais complexos, tendo em conta que este trabalho foi realizado num ambiente controlado cujo objetivo é o de apenas simular a realidade. Seria também interessante efetuar uma pesquisa sobre outro tipo de ferramentas e técnicas que permitam a deteção, identificação e caracterização de ameaças.