

Universidade do Minho

MESTRADO EM ENGENHARIA INFORMÁTICA

Tecnologias de segurança

Trabalho prático 1

Grupo 1

RUI CARLOS AZEVEDO CARVALHO - PG47633
DANIEL BARBOSA MIRANDA - PG47123
ANA LUÍSA LIRA TOMÉ CARNEIRO - PG46983

Contents

Parte A	2	
1	Análise de uma grande corporação - Blizzard.com	2
1.1	Exploração do website e informações da empresa	2
1.2	Vagas de emprego	5
1.3	Whois	7
1.4	DNS	8
2	Análise de um negócio local - 360imprimir.pt	10
2.1	Exploração do website e informações da empresa	10
2.2	Vagas de emprego	12
2.3	Whois	12
2.4	DNS	13
Parte B	15	
1	Questão 1	15
1.1	Serviços	15
1.2	Vulnerabilidades dos serviços	17
2	Questão 2	22
2.1	Vulnerabilidades	23
2.2	Resumo	30
3	Questão 3	31
4	Questão 4	32
5	Questão 5	33
5.1	Resultado do scanner antes da correção de vulnerabilidades . . .	33
5.2	Correção da vulnerabilidade com classificação <i>low</i>	33
5.3	Correção da vulnerabilidade com classificação <i>medium</i>	35
5.4	Correção da vulnerabilidade com classificação <i>critical</i>	35
5.5	Resultado do scanner depois da correção de vulnerabilidades . .	36
5.6	Discussão das soluções	37
Anexos	38	
1	Anexo A	38
2	Anexo B	40

Parte A

1 Análise de uma grande corporação - Blizzard.com

1.1 Exploração do website e informações da empresa

Após uma exploração aprofundada do website não foi possível obter contactos telefónicos da mesma, sendo que os únicos meios comunicação que foram encontrados com a empresa foram os das três imagens seguintes.

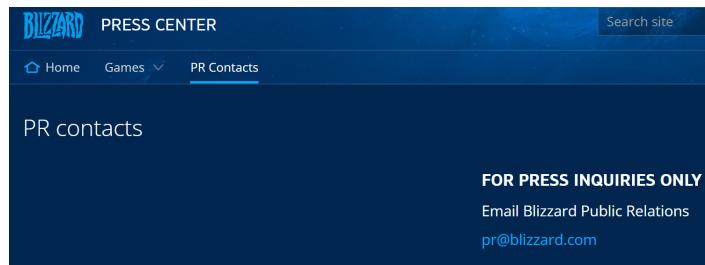


Figure 1: Contactos Conferência - Blizzard [1]

Esta primeira, possui apenas um contacto visando apenas conferências de imprensa.[1]

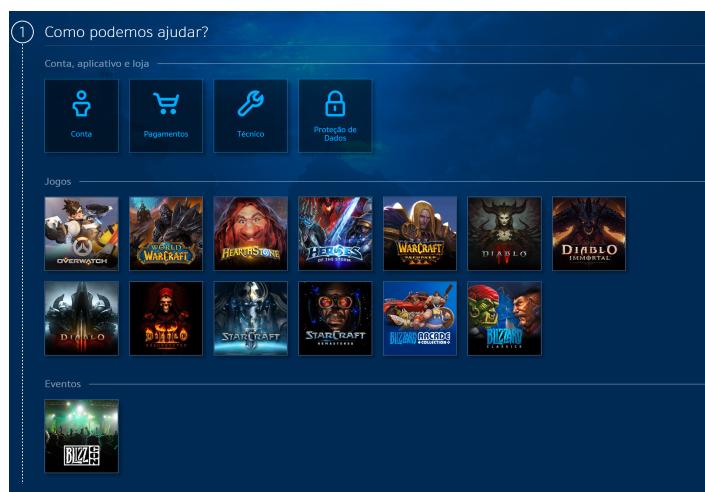


Figure 2: Contacto suporte ao utilizador - Blizzard[1]

Por sua vez, este método de contacto destina-se ao suporte dos seus consumidores e funciona sob um sistema de *tickets*, sendo que a empresa não necessita de fornecer os

seus dados ao consumidor, o que pode ser interpretado como uma boa prática a nível de proteção.[1]

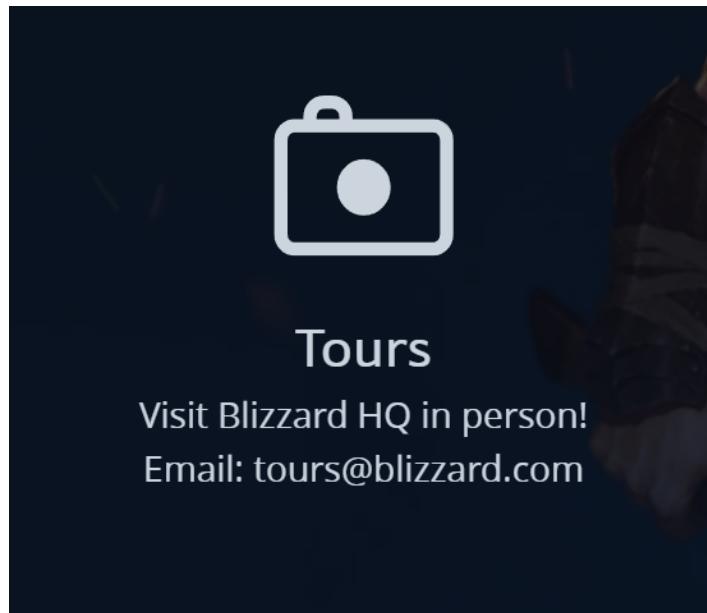


Figure 3: Contacto *tour* - Blizzard[1]

Este último serve como forma de informar o desejo de participar numa visita guiada à sede da Blizzard. Através de algumas pesquisas no YouTube é possível observar em pequenos vídeos desta visita em que são mostradas algumas das infraestruturas da empresas. Apesar de ao relance não haver nada de relevante, um possível atacante talvez possa efetuar esta visita e retirar algumas informações que possam ser pertinentes para si, pelo que a empresa em questão deverá tomar cuidado com aquilo que expõe.[1]

No que toca à identificação de membros da empresa, estes podem ser identificados sobretudo numa hiperligação associada ao seu *website*, na qual podemos observar alguns dos membros assim como os seus cargos na empresa assim como demonstrado a seguir.[2]



Figure 4: Teamleaders - Blizzard[2]

Ao selecionar um membro ocorre um redirecionamento para uma página onde se pode observar uma breve descrição da sua carreira.[2]



Figure 5: Exemplo Teamleader - Blizzard[2]

Também a nível de redes sociais da Blizzard, através das publicações da mesma nomeadamente no **Twitter**, é possível adquirir mais um conjunto de pessoas que fazem parte dos seus trabalhadores.[3]

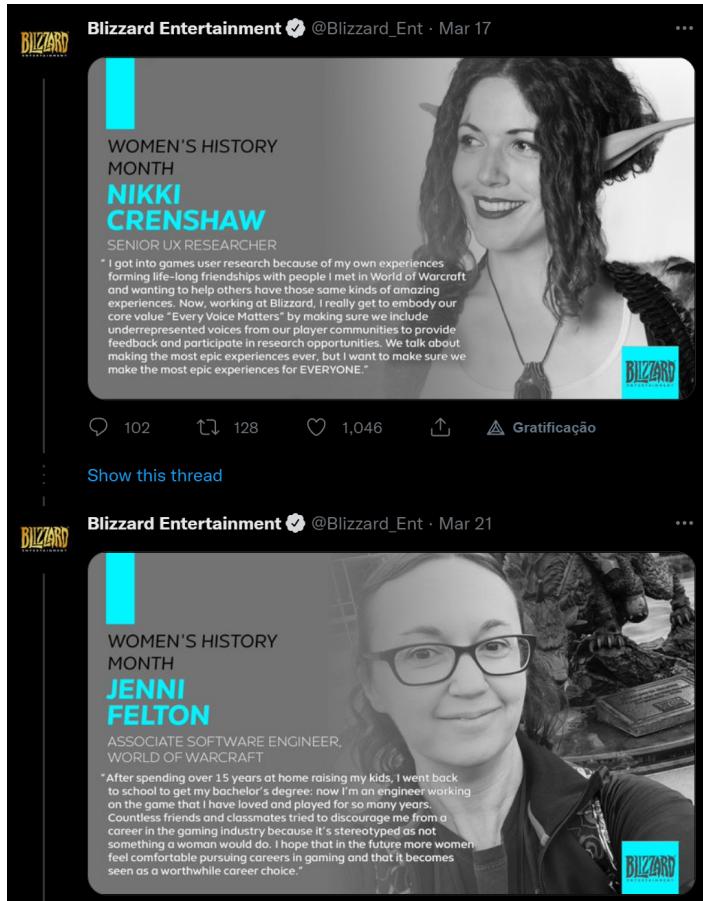


Figure 6: Twitter - Blizzard[3]

Esta prática de exposição de membros pode permitir a um atacante espiar os perfis de redes sociais de cada um desses membros e possivelmente obter alguma informação, partilhada inocentemente, sobre o que estes poderão estar a desenvolver.

1.2 Vagas de emprego

A seguinte tabela foi construída com base nas ofertas de emprego da empresa, focando-se nos linguagens de programação e ferramentas contidas nos requisitos dos diversos cargos apresentados.[4]

Linguagens	Ferramentas
SQL R Python MATLAB SPARK C++ Java C# SAS Scala Lua HTML CSS XML JavaScript C Rust OCaml Scala F# Haskell Go Kotlin Swift Objective-C Perl	Tableau Jira Data Studio Looker Unity Adobe Suite Figma JIRA Sketch Framer Principle Zeplin Flinto TestRail MS Office Confluence WWise Reaper AVID Kibana Elasticsearch Speedtree Zbrush Maya Unreal Ansible Terragrunt Terraform Puppet Service Mesh CMake SCons LibreMNS

Figure 7: Vagas de emprego - Blizzard[4]

Apesar de fornecerem várias informações relativas ao software que será utilizado, não mencionam as suas versões o que pode ser considerado bom, dado que dificulta um possível atacante de procurar vulnerabilidades desse software e dar "exploit" nelas. Por outro lado ao candidatar-se para as vagas de emprego em questão, o candidato pode averiguar qual o produto da Blizzard associado a essa vaga, o que permite saber qual o software utilizado nesse produto.

Relativamente a infraestruturas não existem informações concretas excluindo duas, da qual as primeiras datam de 2009 e são apenas relativas ao produto mais popular da empresa na altura, e portanto já não se encontram válidas e, as segundas e mais recentes na de um artigo oficial de 2018.[5][6]

- Blizzard Online Network Services run in 10 data centers around the world, including facilities in Washington, California, Texas, Massachusetts, France, Germany, Sweden, South Korea, China, and Taiwan.
- Blizzard uses 20,000 systems and 1.3 petabytes of storage to power its gaming operations.
- WoW's infrastructure includes 13,250 server blades, 75,000 CPU cores, and 112.5 terabytes of blade RAM.
- The Blizzard network is managed by a staff of 68 people.
- The company's gaming infrastructure is monitored from a global network operating center (GNOC), which like many NOCs, features televisions tuned to the weather stations to track potential uptime threats across its data center footprint.

Figure 8: Infraestruturas 2009 - Blizzard

The OpsCenter is the Night's Watch of Blizzard's Sanctuary, Azeroth, Nexus or whatever realm you call home. We monitor over 40,000 servers spread across 27 global data centers with millions of players relying on us to keep things running smoothly. We proactively monitor issues and fix them before they impact our players to make sure every experience is EPIC!

Figure 9: Infraestruturas 2018 - Blizzard

Por fim, efetuou-se uma inspeção ao código fonte das diferentes páginas do *website* da empresa. Apesar disso não foram encontradas informações relevantes, visto que apenas se tratavam de scripts e código HTML/CSS. As chamadas dos scripts mencionavam outras páginas, mas ao tentar aceder a estas o acesso era negado, demonstrando que no que toca a esse aspecto a página encontra-se segura.

1.3 Whois

Através do comando `whois blizzard.com` podemos descobrir uma vasta quantidade de informações sobre a empresa relativamente a contactos, domínios, endereços, datas, entre outros, assim como pode ser visualizado abaixo.

A exposição destes dados para o público poderia ser perigosa, principalmente no que toca aos contactos fornecidos com o uso deste comando, visto que estariam vulneráveis a *spammers*. No entanto, pode-se verificar o uso de contactos *abuse*, que permite proteger contra os mesmos uma vez que funciona sobre um canal que identifica automaticamente *spam* e reporta os autores do mesmo. Posto isto, pode-se dizer que é uma ótima prática, uma vez que acabam por não ficar vulneráveis.

```
rhezzus@RhEzZuS:~$ whois blizzard.com
Domain Name: BLIZZARD.COM
Registry Domain ID: 2180864_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2022-02-14T19:27:35Z
Creation Date: 1994-12-09T05:00:00Z
Registry Expiry Date: 2030-12-08T05:00:00Z
Registrar: Network Solutions, LLC
Registrar IANA ID: 2
Registrar Abuse Contact Email: abuse@web.com
Registrar Abuse Contact Phone: +1.8003337680
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: NS-EAST.CERF.NET
Name Server: NS-WEST.CERF.NET
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2022-03-14T17:14:12Z <<
```

Figure 10: Whois - Blizzard

```

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: BLIZZARD.COM
Registry Domain ID: 2100864_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2022-02-14T19:27:44Z
Creation Date: 1994-12-09T05:00:00Z
Registrar Registration Expiration Date: 2030-12-08T05:00:00Z
Registrar: Network Solutions, LLC
Registrar IANA ID: 2
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Blizzard Entertainment
Registrant Organization: Blizzard Entertainment
Registrant Street: 16215 ALTON PKWY
Registrant City: IRVINE
Registrant State/Province: CA
Registrant Postal Code: 92618-3616
Registrant Country: US
Registrant Phone: +1.9499551380
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: domainnameadmin-us@blizzard.com
Registry Admin ID:
Admin Name: Blizzard Entertainment
Admin Organization: Blizzard Entertainment
Admin Street: 16215 ALTON PKWY
Admin City: IRVINE

```

Figure 11: Whois - Blizzard

```

Admin Street: 16215 ALTON PKWY
Admin City: IRVINE
Admin State/Province: CA
Admin Postal Code: 92618-3616
Admin Country: US
Admin Phone: +1.9499551380
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: domainnameadmin-us@blizzard.com
Registry Tech ID:
Tech Name: Blizzard Entertainment
Tech Organization: Blizzard Entertainment
Tech Street: 16215 ALTON PKWY
Tech City: IRVINE
Tech State/Province: CA
Tech Postal Code: 92618-3616
Tech Country: US
Tech Phone: +1.9499551380
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: domainnameadmin-us@blizzard.com
Name Server: NS-EAST.CERF.NET
Name Server: NS-WEST.CERF.NET
DNSSEC: unsigned
Registrar Abuse Contact Email: domain.operations@web.com
Registrar Abuse Contact Phone: +1.8777228662
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2022-03-14T17:14:28Z <<<

```

Figure 12: Whois - Blizzard

1.4 DNS

Com o comando *host* foi possível obter o endereço IP do domínio da Blizzard.

```
rhezzus@RhEzzus:~$ host blizzard.com
blizzard.com has address 137.221.106.104
blizzard.com mail is handled by 0 mxb-00381101.gslb.pphosted.com.
blizzard.com mail is handled by 0 mxa-00381101.gslb.pphosted.com.
```

Figure 13: Host - Blizzard

Utilizou-se o comando *whois 137.221.106.104*, para obter informações acerca desse domínio obtendo algumas informações como nome da organização do domínio, a sua localização algumas datas, entre outros. Mais uma vez é possível denotar o uso de contactos *abuse*, o minimiza a informação exposta de forma significativa.

```

NetRange:      137.221.0.0 - 137.224.255.255
CIDR:         137.222.0.0/15, 137.224.0.0/16, 137.221.0.0/16
NetName:       RIPE-ERX-137-221-0-0
NetHandle:     NET-137-221-0-0-1
Parent:        NET137 (NET-137-0-0-0-0)
NetType:       Early Registrations, Transferred to RIPE NCC
OriginAS:
Organization: RIPE Network Coordination Centre (RIPE)
RegDate:      2004-02-18
Updated:      2004-02-18
Comment:      These addresses have been further assigned to users in
Comment:      the RIPE NCC region. Contact information can be found in
Comment:      the RIPE database at http://www.ripe.net/whois
Ref:          https://rdap.arin.net/registry/ip/137.221.0.0

ResourceLink: https://apps.db.ripe.net/search/query.html
ResourceLink: whois.ripe.net

OrgName:      RIPE Network Coordination Centre
OrgId:        RIPE
Address:      P.O. Box 10096
City:         Amsterdam
StateProv:
PostalCode:   1001EB
Country:      NL
RegDate:
Updated:      2013-07-29
Ref:          https://rdap.arin.net/registry/entity/RIPE

ReferralServer: whois://whois.ripe.net
ResouceLink:  https://apps.db.ripe.net/search/query.html

OrgAbuseHandle: ABUSE3850-ARIN
OrgAbuseName:  Abuse Contact
OrgAbusePhone: +31205354444
OrgAbuseEmail: abuse@ripe.net
OrgAbuseRef:   https://rdap.arin.net/registry/entity/ABUSE3850-ARIN

OrgTechHandle: RNO29-ARIN
OrgTechName:   RIPE NCC Operations
OrgTechPhone:  +31 20 535 4444
OrgTechEmail:  hostmaster@ripe.net
OrgTechRef:    https://rdap.arin.net/registry/entity/RNO29-ARIN

```

Figure 14: Whois - Domínio da Blizzard

```

Found a referral to whois.ripe.net.

% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: this output has been filtered.
%        To receive output for a database update, use the "-B" flag.

% Information related to '137.221.96.0 - 137.221.127.255'

% Abuse contact for '137.221.96.0 - 137.221.127.255' is 'peering@blizzard.com'

inetnum:      137.221.96.0 - 137.221.127.255
netname:      BLIZZARD
country:      NL
admin-c:      BP5978-RIPE
tech-c:       BP5978-RIPE
status:       ASSIGNED PA
mnt-by:       MNT-BLIZZARD
created:      2018-08-27T19:58:14Z
last-modified: 2018-08-27T19:58:14Z
source:       RIPE

person:       Blizzard Peering
address:      1 Blizzard Way
phone:        +1-949-955-1380
nic-hdl:      BP5978-RIPE
mnt-by:       MNT-BLIZZARD
created:      2016-09-07T17:19:11Z
last-modified: 2018-08-24T18:24:09Z
source:       RIPE # Filtered

```

Figure 15: Whois - Domínio da Blizzard

Também se recorreu aos comandos *dig blizzard.com* e *nslookup blizzard.com*, contudo não foi possível adquirir informações muito relevantes, para além das que já se possuía.

```
rhezzus@RhEZZuS:~$ dig blizzard.com
; <>> DiG 9.16.15-Ubuntu <>> blizzard.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 2914
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;;
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: udp: 65494
;; QUESTION SECTION:
;blizzard.com.           IN      A
;;
;; ANSWER SECTION:
blizzard.com.        107     IN      A      137.221.106.104
;;
;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: qua mar 23 20:27:42 WET 2022
;; MSG SIZE  rcvd: 57
```

Figure 16: Dig - Blizzard

```
rhezzus@RhEZZuS:~$ nslookup blizzard.com
Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
Name:   blizzard.com
Address: 137.221.106.104
```

Figure 17: Nslookup - Blizzard

2 Análise de um negócio local - 360imprimir.pt

2.1 Exploração do website e informações da empresa

Quanto a esta segunda empresa, através do seu website foi possível obter informações relativas à sua proprietária, localização da sede, e localização da delegação comercial e NIPC (equivalente ao NIF).[7]

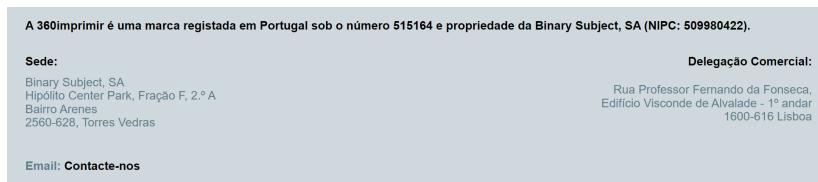


Figure 18: Quem Somos - 360imprimir[8]

Relativamente a contactos não foi encontrado nenhum número telefónico nem de email. Apesar de na imagem acima mencionar "Email: Contacte-nos", quando se seleciona esta opção é-se redirecionado para um sistema de *tickets* semelhante ao da empresa anterior, sendo mais uma vez uma boa forma de esconder contactos.[7]

Figure 19: Contacto suporte ao utilizador - 360imprimir[7]

Apesar disso, nas redes sociais da página, nomeadamente Facebook é possível obter o email da empresa, invalidando um dos pontos positivos do sistema de *tickets*, a revelação de menos dados.[8]



Figure 20: Facebook - 360imprimir

Através de pesquisas no motor de busca também se conseguiu obter algumas informações relativas a investimentos efetuados na empresa, assim como os seus investidores, tal como se pode observar na figura abaixo.[9]



Figure 21: Investimento - 360imprimir[9]

Relativamente a membros da equipa da empresa é possível saber quantos são pela hiperligação do [Linkedin](#) e também a identidade de alguns dos mesmos através da hiperligação[10][11].

A conclusão relativa a prática mantém-se, dado que um ou vários atacantes dedicados poderão aplicar técnicas de espionagem aos e possivelmente obter alguma informação sobre o trabalho que estes estarão a fazer.

Tal como no caso da empresa anterior, efetuou-se uma inspeção ao código fonte das diferentes páginas do *website* da empresa. Neste caso, partes do código fonte da página faziam referência a outra página cuja aparência era exatamente igual a si. Neste novo site é possível observar os scripts e HTML/CSS utilizados no código fonte, mas para além disso também foi possível aceder a mais nada, apresentando também segurança nesse aspeto.

2.2 Vagas de emprego

Linguagens	Ferramentas
C# SQL Javascript UML	Jenkins Selenium TeamCity ASP.Net.MVC Frameworks Web

Figure 22: Vagas de emprego - 360imprimir[7]

Em comparação com a empresa anterior, as vagas de emprego desta empresa são bastante menos, dada a diferença da dimensão de ambas, sendo consequentemente menos o número de linguagens e ferramentas com que os trabalhadores operam.

Tal como no caso anterior, um aspeto positivo a denotar é o facto de nos requisitos destas vagas não ser mencionada a versão específica de cada ferramenta, o que poderá dificultar a exploração de vulnerabilidades e *exploits* por parte de um possível atacante.[7]

2.3 Whois

À semelhança do caso da empresa anterior, utilizou-se o comando `whois 360imprimir.pt` pelo que se obtiveram bastante menos dados em comparação, o que provavelmente deve-se ao facto da diferença da dimensão das duas no mercado, sendo que a base de dados *whois* não possui tanta informação sobre esta.

Um ponto positivo que se pode denotar nestas informações é a falta de contactos telefónicos o que reduz substancialmente os ataques a que poderiam estar expostos, além de que, tal como na Blizzard, também é possível observar o uso de contactos *abuse*.

```
rhezzus@RhEZZuS: $ whois 360imprimir.pt
Domain: 360imprimir.pt
Domain Status: Registered
Creation Date: 24/04/2013 09:04:14
Expiration Date: 23/04/2023 23:59:14
Owner Name: BINARY SUBJECT - LDA
Owner Address: Hipólitio Center Park, Fração F, 2.º A, Bairro Arenes,
Owner Locality: Torres Vedras
Owner ZipCode: 2560-046
Owner Locality ZipCode: Torres Vedras
Owner Country Code: PT
Owner Email: postmaster@360imprimir.pt, abuse@360imprimir.pt
Admin Name: DMNS - DOMINIOS, S.A.
Admin Address: Parque Multiusos, Areal Gordo, Lote 3A
Admin Locality: Faro
Admin ZipCode: 8005-409
Admin Locality ZipCode: Faro
Admin Country Code: PT
Admin Email: dns@dominios.pt, mailmanager@dominios.pt
Name Server: dave.ns.cloudflare.com | IPv4: and IPv6:
Name Server: jean.ns.cloudflare.com | IPv4: and IPv6:
```

Figure 23: Whois - 360imprimir

2.4 DNS

O comando *host* possibilitou a obtenção do endereço IP do domínio da 360imprimir.

```
rhezzus@RhEZZuS: $ host 360imprimir.pt
360imprimir.pt has address 13.73.146.112
360imprimir.pt mail is handled by 0 360imprimir-pt.mail.protection.outlook.com.
```

Figure 24: Host - 360imprimir

De seguida, com o comando *whois 13.73.146.112*, para obter informações acerca desse domínio e verificou-se que este é propriedade da Microsoft, e como esperado não revela informações pertinentes, sendo que, mais uma vez, pode-se observar o uso de contactos *abuse*.

```
OrgDNSHandle: YSRH-ARIN
OrgDNSName: Yalamati, Sree Raghu Harsha
OrgDNSPhone: +917702220771
OrgDNSEmail: v-raghuy@microsoft.com
OrgDNSRef: https://rdap.arin.net/registry/entity/YSRH-ARIN

OrgTechHandle: MRPD-ARIN
OrgTechName: Microsoft Routing, Peering, and DNS
OrgTechPhone: +1-425-882-8080
OrgTechEmail: IOC@microsoft.com
OrgTechRef: https://rdap.arin.net/registry/entity/MRPD-ARIN

OrgTechHandle: IPHO55-ARIN
OrgTechName: IPHostmaster, IPHostmaster
OrgTechPhone: +1-425-538-6637
OrgTechEmail: iphostmaster@microsoft.com
OrgTechRef: https://rdap.arin.net/registry/entity/IPHO55-ARIN

OrgAbuseHandle: MAC74-ARIN
OrgAbuseName: Microsoft Abuse Contact
OrgAbusePhone: +1-425-882-8080
OrgAbuseEmail: abuse@microsoft.com
OrgAbuseRef: https://rdap.arin.net/registry/entity/MAC74-ARIN
```

Figure 25: Whois - Domínio da 360imprimir

```

OrgDNSHandle: YSRH-ARIN
OrgDNSName: Yalamati, Sree Raghu Harsha
OrgDNSPhone: +917702220771
OrgDNSEmail: v-raghuy@microsoft.com
OrgDNSRef: https://rdap.arin.net/registry/entity/YSRH-ARIN

OrgTechHandle: MRPD-ARIN
OrgTechName: Microsoft Routing, Peering, and DNS
OrgTechPhone: +1-425-882-8080
OrgTechEmail: IOC@microsoft.com
OrgTechRef: https://rdap.arin.net/registry/entity/MRPD-ARIN

OrgTechHandle: IPHOSS-ARIN
OrgTechName: IPHostmaster, IPHostmaster
OrgTechPhone: +1-425-538-6637
OrgTechEmail: iphostmaster@microsoft.com
OrgTechRef: https://rdap.arin.net/registry/entity/IPHOSS-ARIN

OrgAbuseHandle: MAC74-ARIN
OrgAbuseName: Microsoft Abuse Contact
OrgAbusePhone: +1-425-882-8080
OrgAbuseEmail: abuse@microsoft.com
OrgAbuseRef: https://rdap.arin.net/registry/entity/MAC74-ARIN

```

Figure 26: Whois - Domínio da 360imprimir

Com os comandos `dig 360imprimir.pt` e `nslookup 360imprimir.pt`, tal como para a empresa anterior, não foi possível adquirir informações muito relevantes, para além das que já se possuía.

```

rhezzus@RhEzzuS: $ dig 360imprimir.pt

; <>> DiG 9.16.15-Ubuntu <>> 360imprimir.pt
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 42493
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;360imprimir.pt.           IN      A

;; ANSWER SECTION:
360imprimir.pt.        109     IN      A      13.73.146.112

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: seg mar 14 16:56:50 WET 2022
;; MSG SIZE  rcvd: 59

```

Figure 27: Dig - 360imprimir.pt

```

rhezzus@RhEzzuS:~$ nslookup 360imprimir.pt
Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
Name:   360imprimir.pt
Address: 13.73.146.112

```

Figure 28: Nslookup - 360imprimir

Parte B

1 Questão 1

A ferramenta selecionada de forma a identificar as vulnerabilidades associadas aos serviços presentes no sistema Metasploitable foi o Nmap. Com este scanner foi possível descobrir *ports* e serviços presentes no sistema vulnerável através do envio de pacotes e da respetiva análise das respostas.

1.1 Serviços

Para identificar os serviços com *ports* TCP abertas no sistema metasploitable foi utilizado o comando:

```
$ nmap -sV 172.20.1.2
```

Com este comando é possível verificar que serviços estão correndo em cerca de 1000 *ports* TCP que estejam abertas para o exterior e desta forma identificar possíveis entradas no sistema através de vulnerabilidades encontradas nestes serviços. Na figura abaixo encontra-se os vários serviços, respetivas *ports* e versões de cada serviço encontradas no sistema.

Not shown: 980 closed tcp ports (reset)			
PORT	STATE	SERVICE	REASON
22/tcp	open	ssh	syn-ack ttl 128 OpenSSH 7.1 (protocol 2.0)
135/tcp	open	msrpc	syn-ack ttl 128 Microsoft Windows RPC
139/tcp	open	netbios-ssn	syn-ack ttl 128 Microsoft Windows netbios-ssn
445/tcp	open	microsoft-ds	syn-ack ttl 128 Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3306/tcp	open	mysql	syn-ack ttl 128 MySQL (blocked - too many connection errors)
3389/tcp	open	ssl/ms-wbt-server?	syn-ack ttl 128
4848/tcp	open	ssl/http	syn-ack ttl 128 Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
7676/tcp	open	java-message-service	syn-ack ttl 128 Java Message Service 3.01
8009/tcp	open	ajp13	syn-ack ttl 128 Apache Jserv (Protocol v1.3)
8022/tcp	open	http	syn-ack ttl 128 Apache Tomcat/Coyote JSP engine 1.1
8031/tcp	open	ssl/unknown	syn-ack ttl 128
8080/tcp	open	http	syn-ack ttl 128 Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
8181/tcp	open	ssl/http	syn-ack ttl 128 Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
8383/tcp	open	http	syn-ack ttl 128 Apache httpd
8443/tcp	open	ssl/https-alt?	syn-ack ttl 128
9200/tcp	open	wap-wsp?	syn-ack ttl 128
49152/tcp	open	msrpc	syn-ack ttl 128 Microsoft Windows RPC
49153/tcp	open	msrpc	syn-ack ttl 128 Microsoft Windows RPC
49154/tcp	open	msrpc	syn-ack ttl 128 Microsoft Windows RPC
49155/tcp	open	msrpc	syn-ack ttl 128 Microsoft Windows RPC

Figure 29: Serviços TCP a correr no sistema metasploitable

Pela figura apresentada podemos ver um conjunto variado de serviços que podem estar vulneráveis ao exterior, como por exemplo mysql. Além destas *ports* abertas, foi

possível identificar 980 portas que se encontram fechadas ao exterior. Desta forma, quanto maior for o número de portas fechadas, menor a probabilidade de um atacante conseguir entrar no sistema a partir do exterior.

Para identificar os serviços com *ports* UDP abertas no sistema metasploitable foi utilizado o comando:

```
$ nmap -sU 172.20.1.2
```

Desta forma é possível identificar entradas no sistema em cerca de 1000 *ports* UDP. Apesar da maioria das comunicações sobre a internet ser realizada sobre TCP, existem vários serviços que correm sobre UDP que podem ser muito explorados por atacantes. Na figura abaixo encontra-se os vários serviços e as respetivas *ports* UDP encontradas no sistema.

```
Nmap scan report for 172.20.1.2
Host is up, received arp-response (0.00089s latency).
Scanned at 2022-03-17 23:58:56 WET for 284s
Not shown: 994 closed udp ports (port-unreach)
PORT      STATE      SERVICE      REASON
137/udp    open       netbios-ns   udp-response ttl 128
138/udp    open|filtered netbios-dgm  no-response
500/udp    open|filtered isakmp     no-response
4500/udp   open|filtered nat-t-ike  no-response
5353/udp   open|filtered zeroconf   no-response
5355/udp   open|filtered llmnr     no-response
MAC Address: 08:00:27:A7:DD:76 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 284.77 seconds
Raw packets sent: 1181 (57.449KB) | Rcvd: 1012 (74.596KB)
```

Figure 30: Serviços UDP a correr no sistema metasploitable

Pela figura apresentada podemos ver um conjunto variado de serviços que podem estar vulneráveis ao exterior, como por exemplo netbios. É também possível identificar 5 *ports* que não responderam aos pacotes retransmitidos pelo nmap (*state open/filtered*). Isto pode significar que a porta pode estar aberta ou os filtros de pacotes presentes nestas *ports* podem estar a bloquear a comunicação. Além destas *ports*, foi possível identificar 994 portas que se encontram fechadas ao exterior.

Além dos serviços é possível identificar o sistema operativo usado pelo o sistema, que pode ser obtido através dos comandos.

```
$ nmap -O 172.20.1.2
$ nmap -vv --reason -A --privileged 172.20.1.2
```

Os *outputs* com a informação sobre a versão do sistema operativo que está a ser utilizado no sistema metasploitable encontram-se nas seguintes imagens.

```
MAC Address: 08:00:27:A7:DD:76 (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
```

Figure 31: Informação com o OS do sistema metasploitable

```

smb-os-discovery:
OS: Windows Server 2008 R2 Standard 7601 Service Pack 1 (Windows Server 2008 R2 Standard 6.1)
OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
Computer name: vagrant-2008R2
NetBIOS computer name: VAGRANT-2008R2\x00
Workgroup: WORKGROUP\x00
System time: 2022-03-17T11:57:18-07:00

```

Figure 32: Informação extra com o OS do sistema metasploitable

Tal como podemos ver nas figuras o sistema metasploitable tem como OS o Microsoft Windows 7 que possui funcionalidades associadas ao Windows 7 SP1 e ao Windows Server 2008 R2 SP1.

1.2 Vulnerabilidades dos serviços

Serviços TCP

ssh: Através da identificação da versão do ssh utilizada pelo sistema metasploitable conseguimos explorar diversas vulnerabilidades associadas à versão em questão. Utilizando o comando

```
$ nmap -vv --reason --script "vuln" -sV 172.20.1.2
```

conseguimos obter diversas vulnerabilidades associadas a cada serviço presente no sistema metasploitable. No caso do serviço ssh obtivemos o seguinte *output*.

```

PORT      STATE SERVICE          REASON      VERSION
22/tcp    open  ssh              syn-ack ttl 128 OpenSSH 7.1 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:7.1:
|     PACKETSTORM:140070 7.8 https://vulners.com/packetstorm/PACKETSTORM:140070      *EXPLOIT*
|     EXPLOITPACK:5BCA798C6BA71FAE29334297EC0B6A09 7.8 https://vulners.com/exploitpack/EXPLOITPACK:5BCA798C6BA71FAE29334
297EC0B6A09 *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*
|       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*
|       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*
|       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*
|       MSF:ILITIES/UBUNTU-CVE-2019-6111/ 5.8 https://vulners.com/metasploit/MSF:ILITIES/UBUNTU-CVE-2019-6111/      *

```

Figure 33: Vulnerabilidades do serviço ssh

Nesta imagem podemos ver diversas vulnerabilidades associadas à versão 7.1 do OpenSSH que pode ser explorada por atacantes para comprometer não só o serviço como todo o sistema. As vulnerabilidades mais graves, de avaliação 7.8, dizem respeito a falhas no serviço que podem provocar *denial of service* (DOS). Uma dessas falhas permite que atacantes enviem mensagem KEXINIT (Key exchange init) duplicadas que causam consumo de memória provocando um ataque DOS[12]. Outra falha acontece pois o serviço não limita o tamanho de *passwords* de autenticação permitido ao atacante introduzir uma *string* longa causando um aumento elevado do consumo do CPU e consequente ataque DOS[13].

msrpc: Neste serviço corre o Microsoft Windows RPC que tem como objetivo criar programas distribuídos entre clientes e servidor. Esta tecnologia apesar de poderosa tem algumas vulnerabilidades especialmente quando associada à versão do sistema

operativo utilizado pelo sistema de metasploitable. A vulnerabilidade mais grave encontrada associada a esta tecnologia é identificada como CVE-2022-21922 e permite a utilizadores remotos executarem código arbitrário no sistema alvo. Esta vulnerabilidade é resultante de um erro nesta tecnologia RPC que através de dados especialmente modificados enviados ao RPC, corrompe a memória e executa código arbitrário no sistema[14]. Um atacante pode utilizar esta vulnerabilidade do serviço que corre na port 135, 49152, 49153, 49154 e 49155 para comprometer todo o sistema metasploitable.

netbios-ssn: Nesta port corre o Microsoft Windows netbios-ssn que quando associado à versão do OS a correr no sistema metasploitable possui uma vulnerabilidade alta com identificador CVE-2017-0161. Esta vulnerabilidade está associada a *race conditions* que podem levar à execução de código arbitrário remotamente. Para isso é necessário que o atacante envie dados especialmente modificados que acabem por executar código arbitrário no sistema e consequentemente comprometer o mesmo.[15]

microsoft-ds: Na port 445 corre o serviço Microsoft DS onde é usado o SMB (Server Message Block) que tem como objetivo partilhar recursos na rede e executar comandos remotamente. Quando este serviço está associado ao OS presente no sistema do metasploitable, poderá conter algumas vulnerabilidades que poderão comprometer o sistema. Umas delas identificada com CVE-2017-0143 foi encontrada através do comando apresentado acima. Esta vulnerabilidade permite que código arbitrário seja executado remotamente através do envio de pacotes especialmente modificados tal como está expresso no output do comando.

```
| 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://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|   https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
```

Figure 34: Vulnerabilidades do serviço SMB

msql: A partir do comando apresentado acima, podemos determinar a versão do mysql que correr no sistema metasploitable. Podemos ver pela imagem que a versão do msqsl a correr na port 3306 é a MySQL 5.5.20-log.

```
3306/tcp open mysql              syn-ack ttl 128 MySQL 5.5.20-log
| mysql-info:
|   Protocol: 10
|   Version: 5.5.20-log
|   Thread ID: 14
|   Capabilities flags: 63487
```

Figure 35: Versão do serviço Mysql

Como esta versão não é a mais atual, a partir de uma pesquisa poderemos aceder a um conjunto de vulnerabilidades associadas a esta versão que foram resolvidas nas versões posteriores. Nesta versão é possível que um utilizador autenticado remoto

consiga aceder a um comprometer a confidencialidade, integridade e disponibilidade do esquema de informação da plataforma SQL[16]

ssl/ms-wbt-server: Na port 3389 corre um serviço responsável por fornecer ao utilizador uma interface gráfica de forma a conectar a um outro computador sobre uma conexão de rede. Para isso é necessário que o utilizador implemente o RDP (Remote Desktop Protocol), contudo este protocolo apresenta algumas vulnerabilidades principalmente quando associado à versão de OS a correr no sistema. A vulnerabilidade mais grave encontrada permite a um utilizador não autorizado de executar código arbitrário através do envio de dados especialmente modificados.[21]

ssl-http: Neste serviço corre o Oracle GlassFish Server 3.1, Java 1.8 e o Java Service Page (JSP) com a versão 2.3. Esta versão do serviço é utilizado por em diversos outros serviços no sistema metasploitable, e podemos analisar as suas vulnerabilidades a partir do comando apresentado acima.

A vulnerabilidade encontrada no Oracle GlassFish Server 3.1 é identificada com CVE-2011-3368 e permite a utilizadores remotos acesso a servidores internos através do envio de pedidos especialmente modificados, tal como podemos ver na figura com o output do comando utilizado.

```
|_ http-server-header: GlassFish Server Open Source Edition 4.0
| http-vuln-cve2011-3368:
| VULNERABLE:
| Apache mod_proxy Reverse Proxy Security Bypass
| State: VULNERABLE
| IDs: BID:49957 CVE:CVE-2011-3368
| An exposure was reported affecting the use of Apache HTTP Server in
| reverse proxy mode. The exposure could inadvertently expose internal
| servers to remote users who send carefully crafted requests.
| Disclosure date: 2011-10-05
| References:
|   https://www.securityfocus.com/bid/49957
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3368
```

Figure 36: Vulnerabilidades do Oracle GlassFish Server 3.1

Outra vulnerabilidade encontrada neste serviço diz respeito ao uso do algoritmo Diffie-Hellman para a permuta de chaves de forma a obter uma chave partilhada comum entre as entidades da comunicação. O uso desta algoritmo no serviço é feita de forma insegura e vulnerável, pois utiliza parâmetros utilizados no algoritmo com comprimentos insuficientemente grandes para suportarem ataques por força bruta, permitindo ao atacante decifrar a comunicação entre as entidades. Esta vulnerabilidade torna o canal de comunicação suscetível a ataques *eavesdropping*, tal como podemos ver na imagem abaixo.

```

| 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_3DES_EDE_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

```

Figure 37: Vulnerabilidades do serviço ssl/http na port 4848

Para as *ports* 8080 e 8181 que também correm a mesma versão do serviço é possível podemos admitir que as vulnerabilidades associadas a esta *port*, também ocorrem nas restantes *ports* associadas à mesma versão do serviço.

java-message-service: Na *port* 7676 corre uma API de Java que faz de *middleware* entre duas aplicações, permitindo que ambas consigam comunicar entre si. A versão apresentada (301) permite que atacantes consigam causar um ataque DOS através do uso de libertação de memória em *buffers*[17].

ajp13: Neste serviço corre o protocolo binário da Apache Jserv (Protocol v1.3) que envia pedidos de um servidor WEB para um servidor aplicacional. permitindo, desta forma, a servidores da Apache comunicar com softwares aplicacionais do Tomcat. Este serviço como está numa *port* aberta a entidades externas, faz com que o Tomcat esteja suscetível à vulnerabilidade Ghostcat. Nesta vulnerabilidade o atacante consegue ler ficheiros de configurações e de *source code* de todas as *apps* desenvolvidas no Tomcat. Desta forma, se uma aplicação permitir a um utilizador fazer upload de ficheiros é possível que um atacante faça upload de um ficheiro malicioso no servidor e que, através da exploração desta vulnerabilidade, consiga executar código remotamente.[18]

http (*port* 8022): Nesta *port* corre o serviço http com a Apache Tomcat/Coyote JSP engine 1.1. O Tomcat tal como já foi referido anteriormente é um software que permite correr aplicações Java no browser. O Coyote é um servidor web que fornece serviços a aplicações do Tomcat, funcionando de forma semelhante a servidores web da Apache só que para JavaServer Pages (JSP). Como forma de terminar a versão do Tomcat a correr nesta *port* utilizou-se o seguinte comando para obter o output abaixo.

```
$ nmap -sV -sC -p- -T4 -oA jerry 172.20.1.2
```

```

8282/tcp  open  http          Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat/8.0.33
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat

```

Figure 38: Versão do Tomcat

Podemos ver pela imagem que a versão do Tomcat a correr nesta *port* é o 8.0.33. Nesta versão é possível encontrar alguma vulnerabilidades não só associadas à versão do Tomcat como também ao Coyote Engine 1.1. Uma das vulnerabilidades pode permitir a atacantes realizar ataque DOS provocados pelo o consumo de recursos através do envio de pedidos com o registo do tamanho da mensagem especialmente modificada.[19]

ssl/unknown: Apesar de nesta *port* não conseguirmos ter acesso à versão do serviço a correr nela, a ferramenta nmap, utilizando o comando já apresentado, identificou uma vulnerabilidade presente no algoritmo de *Diffie-Hellman*, semelhante ao que foi encontrado no serviço ssh/http, tal como podemos ver na figura seguinte.

```
8031/tcp open ssl/unknown      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
```

Figure 39: Vulnerabilidades do serviço ssl/unknown na *port* 8031

O uso desta algoritmo torna a *port* insegura e vulnerável, pois só protege a *port* contra ataques de *evesdropping* sendo vulnerável a ataques de man-in-the-middle que pode comprometer a integridade e confidencialidade dos dados trocados por esta *port*. Isto acontece pois o algoritmo que corre nesta *port* não verifica a identidade da entidade com quem está a comunicar, permitindo a um atacante interserir a troca de chaves e fazer-se passar pela a outra entidade da comunicação.

http (*port* 8383): Nesta *port* corre a versão Apache Httpd que segundo a ferramenta nmap possui uma vulnerabilidade que permite a atacantes causarem um ataque DOS através do envio de pedidos parciais http especialmente modificados de forma esgotarem os recursos do servidor http, tal como está na figura abaixo obtida utilizando o comando previamente referido.

```

8383/tcp open http                  syn-ack ttl 128 Apache httpd
| 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/

```

Figure 40: Vulnerabilidades do serviço http na port 8383

Serviços UDP

netbios O protocolo Netbios funciona em todas as versões atuais do Windows e é usado para a partilha de ficheiros. A port 137 é utilizada como *name service* do Netbios cuja as funcionalidades consistem em registar e resolver nomes a serem utilizados pelo NetBios. Este *name service* não realiza autenticação permitindo a utilizadores remotos causar *denial of service* através do uso malicioso de mecanismos como o *name confict* e *name released*, causando ao *name service* por concluir que o nome do utilizador estava em conflito. Desta forma, impossibilitaria o *name service* de resolver mais nomes na rede, fazendo com que não conseguisse responder a mais regtos. [20]

2 Questão 2

Para a realização desta pergunta foi utilizado o *scanner* de vulnerabilidade Nessus, que verifica as vulnerabilidades de segurança relacionadas com o sistema de metasploitable. Juntamente com este *scanner* foi utilizado o sistema de deteção de intrusão, Snort e o analisador de tráfego, Wireshark, que captura a comunicação entre as entidades.

Começou-se por ligar tanto o wireshark como o snort de for a analisar e capturar o tráfego em tempo real. O Nessus ao analisar esta interação vai verificar e avaliar as vulnerabilidades encontradas no sistema metasploitable, obtendo o seguinte resumo da análise.

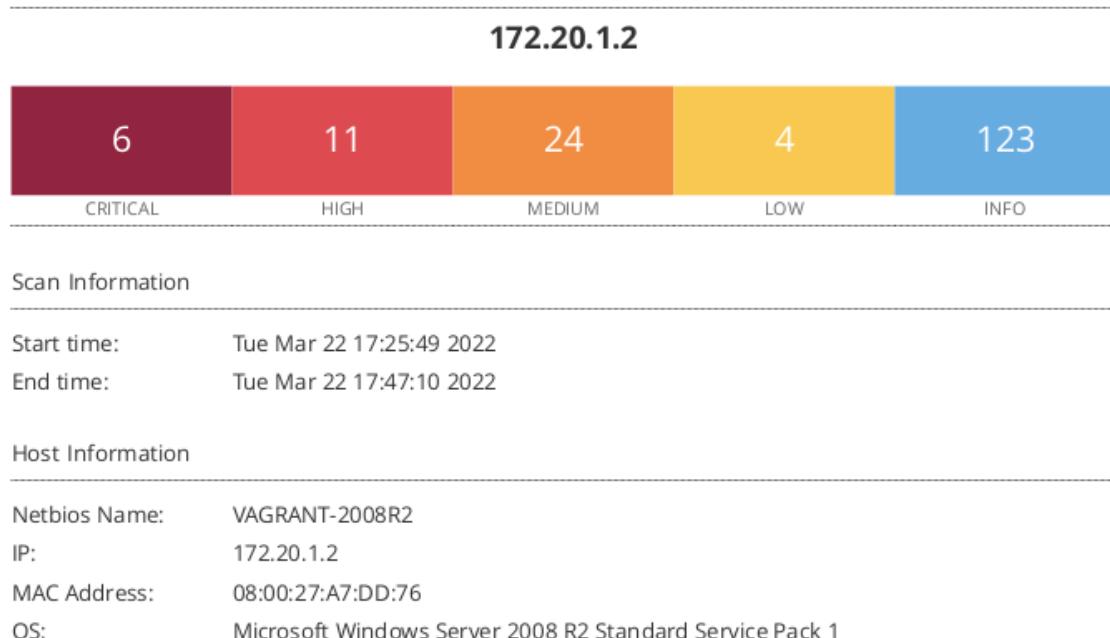


Figure 41: Resumo da análise do Nessus ao sistema metasploitable

A análise realizada conclui que o sistema metasploitable tem um risco crítico de ser acedido a partir do exterior por utilizadores não autenticados no sistema, devido ao elevado número de vulnerabilidades presentes nos diversos serviços abertos ao exterior. A análise de vulnerabilidades conclui que existem cerca de 46 vulnerabilidades, sendo que 6 são de nível crítico, 11 são de risco alto, 24 são de risco médio e 4 são de nível baixo, tal como podemos ver na figura acima. Foi também possível identificar 123 informações adicionais relacionadas com os serviços a correr no sistema.

2.1 Vulnerabilidades

TCP

tcp/22/ssh Para este serviço o Nessus detetou algumas informações adicionais que podem ser convenientes para tentar perceber o funcionamento do serviço no sistema. Detetou que no serviço ssh era implementado o algoritmo DH (Diffie-Hellman) para troca de chaves e o algoritmo SHA-1, que apesar de ser desaconselhado pelo o NIST, é usado nas funções de autenticação HMAC deste serviço. O nessus também detetou algumas informações relacionadas com a existência de um autenticação necessário para utilizar o serviço.

Ao contrário daquilo que foi determinado na questão 1, o serviço ssh, segundo o Nessus, não apresenta nenhuma vulnerabilidade para o exterior. Apesar de ser implementado com algoritmos não aconselhados, este não traz riscos para o sistema.

INFO SSH Algorithms and Languages Supported

Description

This script detects which algorithms and languages are supported by the remote service for encrypting communications.

Output

```
Nessus negotiated the following encryption algorithm with the server :  
The server supports the following options for kex_algorithms :  
curve25519-sha256@libssh.org  
dime-hellman-group-exchange-sha256  
dime-hellman-group14-sha1  
ecdh-sha2-nistp256  
ecdh-sha2-nistp384  
ecdh-sha2-nistp521  
The server supports the following options for server_host_key_algorithms :  
ecdsa-sha2-nistp521  
ssh-rsa
```

(a) Informação sobre o algoritmo DH

INFO SSH SHA-1 HMAC Algorithms Enabled

Description

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Although NIST has formally deprecated use of SHA-1 for digital signatures, SHA-1 is still considered secure for HMAC as the security of HMAC does not rely on the underlying hash function being resistant to collisions.

Note that this plugin only checks for the options of the remote SSH server.

(b) Informação sobre o algoritmo SHA-1

Figure 42: Informações sobre o SSH

tcp/135/enmap: Nesta *port* não foi encontrada nenhuma vulnerabilidade associada ao serviço. Ao contrário do que foi previsto com o nmap, o serviço Microsoft Windows RPC a correr nesta *port* pode não estar associado à vulnerabilidade identificada com CVE-2022-21922 que por ser recente, os *scripts* e *pluggins* do Nessus ainda não conseguem identificar tal vulnerabilidade.

tcp/139/smb: Nesta *port*, tal como foi identificado pelo nmap, corre o serviço do netbios. Ao contrário do que foi identificado como uma possível vulnerabilidade na pergunta 1, este serviço segundo o Nessus não possui qualquer falha associada. Isto pode acontecer pois o sistema metasploitable pode implementar métodos como o uso de firewalls que protegem o sistema contra a exploração da vulnerabilidade mencionada na pergunta 1.[15]

tcp/445/cifs: O serviço identificado tanto pelo Nessus como pelo nmap acorreu na *port* 445 foi o serviço da Microsoft que está associado ao SMBv1 (Server Message Block). Este serviço, tal como foi identificado por ambas as ferramentas, possui uma vulnerabilidade de nível alto que permite a atacantes enviarem pacotes especialmente modificados de forma executarem código arbitrário remotamente ou a expor informação sensível (figura a). O Nessus também identificou uma vulnerabilidade de risco médio que permite a um utilizar não autenticado explorar o facto deste serviço não necessitar autenticação para estabelecer um ataque *man-in-the-middle* (figura b).

HIGH

MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION)

Description

The remote Windows host is affected by the following vulnerabilities :

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)

- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

(a) Vulnerabilidade alta associada ao SMBv1

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.

(b) Vulnerabilidade média associada ao SMBv1

Figure 43: Vulnerabilidades associadas ao SMB

tcp/3306/mysql: Nesta *port*, tal como foi identificado pelo nmap, corre o serviço do Mysql. Ao contrário do que foi identificado como uma possível vulnerabilidade na pergunta 1, este serviço segundo o Nessus não possui qualquer falha associada. Isto pode acontecer pois o sistema metasploitable pode implementar métodos que protegem o sistema contra a exploração da vulnerabilidade mencionada na pergunta 1.

tcp/3389/rdp Foi identificado pelo nmap e pelo nessus que o serviço a correr na *port* 3389 é o protocolo RDP (Remote Desktop Protocol). Este serviço tem cerca de 13 vulnerabilidades que foram identificadas pelo nessus, uma delas que podemos ver na pergunta 1, corresponde a uma falha crítica que permite a utilizadores não autorizados de executarem código arbitrário no sistema através desta *port*. É também possível encontrar cerca de 4 vulnerabilidades de risco elevado, sendo que duas delas correspondem a falhas que permitem aos utilizadores o envio de pacotes especialmente modificados de forma a comprometer o sistema (CVE-2012-0002, CVE-2012-0152 e CVE-2014-6321) e as outras duas dizem respeito ao uso de algoritmos fracos para as funções de *hash* e de assinatura que são vulneráveis a ataques de colisão (CVE-2004-2761 e CVE-2016-2183). É ainda possível encontrar 7 vulnerabilidades de risco médio que podem permitir ataques *man in the middle* devido à falta de autenticação de utilizadores, ao uso de certificados pelo servidor que podem não ser de confiança e à falta de uma autenticação NLA (Network Level Authentication) (CVE-2005-1794). Existem ainda vulnerabilidades de nível médio que usam cifras com baixa aleatoriedade nos valores gerados (CVE-2013-2566, CVE-2015-2808), que utilizam um versão antiga do TLS para a comunicação e que usa fracos métodos de criptografia permitindo a atacantes terem acesso a informação de uma comunicação privada (*eavesdropping*). Finalmente, nesta port é ainda possível identificar uma vulnerabilidade de nível baixo que corresponde à não compatibilidade do sistema com o padrão de segurança proposto pelo governo dos EUA usado para aprovar módulos criptográficos, FIPS-140. Na figura

abaixo encontram-se algumas das vulnerabilidades encontradas neste serviço.

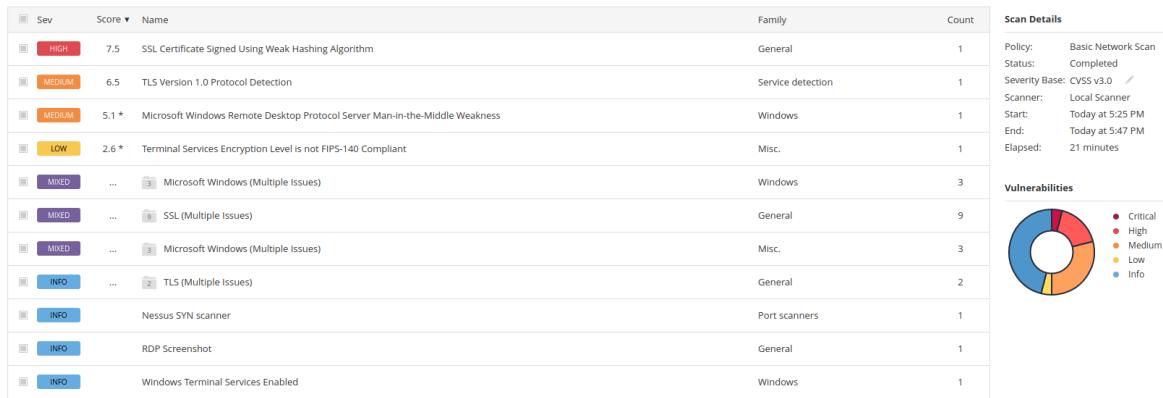


Figure 44: Algumas das vulnerabilidades associadas a esta *port* 3389

tcp/4848/www Nesta *port*, tal como foi identificado pelo nmap e pelo nessus, existe um serviço que corre o Oracle Glassfish. O nessus encontrou cerca de 8 vulnerabilidades associadas a esta *port*, 3 delas de nível alto, 4 de risco médio e 1 de nível baixo. Uma das falhas classificadas com risco alto pode ser causada devido ao envio de pacotes especialmente modificados que permitem a atacantes acederem a ficheiros arbitrários no *host* remotamente. A pesar do nmap ter identificado uma vulnerabilidade semelhante (CVE-2011-3368), o nessus conseguiu identificar uma vulnerabilidade mais recente (CVE-2017-1000028) associada a este serviço. Outra das falhas classificadas com nível alto consiste na possibilidade de atacantes provocarem ataques DOS através do envio de um pedido HTTP especialmente alterado. A última vulnerabilidade alta encontrada pelo nessus tem haver com o uso de cifras SSL de força média que utilizam comprimentos de chaves abaixo do recomendável. Isto faz com que os métodos criptográficos associados a esta *port* não tenham força suficiente. Além destas vulnerabilidades foram também encontradas falhas de risco médio que estão associadas ao uso de certificados que não são de confiança nem correspondem ao host respetivo e ao uso de uma versão do TLS que está descontinuada. Finalmente, nesta *port* também está associada uma vulnerabilidade de risco baixo, que também foi identificada na pergunta 1 e que corresponde ao uso do algoritmo DH com chaves de comprimento insuficiente, sendo por isso fácil a um atacante conseguir descobrir a chave partilhada entre as entidades. Na figura abaixo encontram-se algumas das vulnerabilidades encontradas neste serviço.



Figure 45: Algumas das vulnerabilidades associadas a esta *port* 4848

tcp/7676/imqbrokerd: Ao contrário do que foi identificado como uma possível vulnerabilidade na pergunta 1, este serviço segundo o Nessus não possui qualquer falha associada. Isto pode acontecer pois o sistema metasploitable pode implementar métodos que protegem o sistema contra a exploração da vulnerabilidade mencionada na pergunta 1.

tcp/8009/ Nesta *port*, foi identificado o serviço que corre o protocolo binário Apache Jser e uma vulnerabilidade crítica associada a este. Esta falha, apesar de não ter sido identificada pelo nmap, foi referida na pergunta 1 e diz respeito à vulnerabilidade mais conhecida como Ghostcat. Esta falha permite a utilizadores remotos não autenticados de fazerem upload de um JSP malicioso causando a execução de código remotamente. Na figura abaixo encontram a informação recolhida acerca da vulnerabilidade encontrada neste serviço.

Vulnerabilities

134862 - Apache Tomcat AJP Connector Request Injection (Ghostcat)

Synopsis

There is a vulnerable AJP connector listening on the remote host.

Description

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).

Figure 46: Vulnerabilidade Ghostcat na *port* 8009

tcp/8181/www: Nesta *port*, corre um serviço www, onde o nessus encontrou cerca de 6 vulnerabilidades associadas a esta *port*, 1 nível alto, 4 de risco médio e 1 de nível baixo. A falha classificada com risco alto pode ser causada devido ao uso de cifras SSL de força média que utilizam comprimentos de chaves abaixo do recomendável. A pesar do nmap ter identificado esta *port* como aberta, esta ferramenta não identificou nenhuma vulnerabilidade associada ao serviço, ao contrário do nessus conseguiu identificar a vulnerabilidade CVE-2016-2183. Além desta vulnerabilidade foram também encontradas falhas de risco médio que estão associadas ao uso de certificados que não são de confiança nem correspondem ao host respetivo e ao uso de uma versão do TLS que está descontinuada. Finalmente, nesta *port* também está associada uma vulnerabilidade de risco baixo que corresponde ao uso do algoritmo DH com chaves de comprimento insuficiente, sendo por isso fácil a um atacante conseguir descobrir a chave partilhada entre as entidades. Na figura abaixo encontram-se algumas das vulnerabilidades encontradas neste serviço.

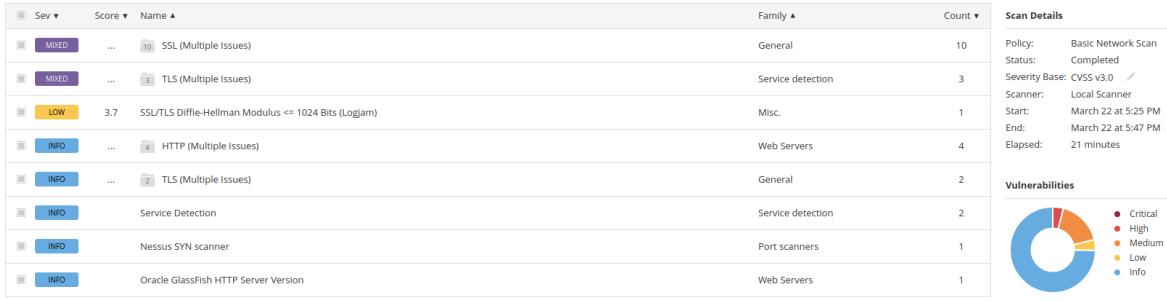


Figure 47: Algumas das vulnerabilidades associadas à *port 8181*

tcp/8383: Nesta *port*, corre um serviço www, onde o nessus encontrou cerca de 8 vulnerabilidades associadas a esta *port*, 2 nível alto, 5 de risco médio e 1 de nível baixo. Uma das falhas classificada com risco alto corresponde ao uso de algoritmos hash fracos tornando o sistema vulnerável a ataques de colisão. A outra vulnerabilidade de risco alto corresponde cifras SSL de força média que utilizam comprimentos de chaves abaixo do recomendável. Além desta vulnerabilidade foram também encontradas falhas de risco médio que estão associadas ao uso de certificados que não são de confiança, que já expiraram e que não correspondem ao *host* respetivo e ao uso de uma versão do TLS que está descontinuada. Finalmente, nesta *port* também está associada uma vulnerabilidade de risco baixo que corresponde ao uso do algoritmo DH com chaves de comprimento insuficiente, sendo por isso fácil a um atacante conseguir descobrir a chave partilhada entre as entidades. Apesar do nmap ter identificado uma vulnerabilidade associada ao identificador CVE-2007-6750, o nessus não identificou nenhuma vulnerabilidade semelhante. Na figura abaixo encontram-se algumas das vulnerabilidades encontradas neste serviço.

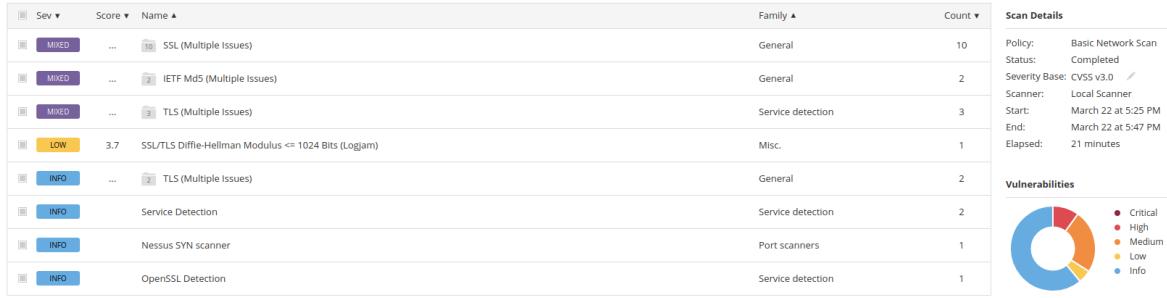


Figure 48: Algumas das vulnerabilidades associadas à *port 8383*

tcp/9200/elasticsearch: Nesta *port*, o nmap não identificou nenhuma versão associada ao serviço wap-wsp que corresponde ao protocolo Wireless Session Protocol. Contudo, o nessus identificou que neste serviço corre o ElasticSearch onde foi identificado cerca de 4 vulnerabilidades, 2 delas de risco crítico e outras 2 de risco médio. As duas falhas de nível crítico permitem a atacantes remotos executarem código arbitrário no sistema a partir de um erro no protocolo de transporte (CVE-2015-5377). As vulnerabilidades restantes de nível médio permitem a atacantes executarem código remoto e acederem e manipularem ficheiros devido, principalmente, a problemas associados à versão do ElasticSearch a correr nesta *port*. Na figura abaixo encontram-se algumas das vulnerabilidades encontradas neste serviço.

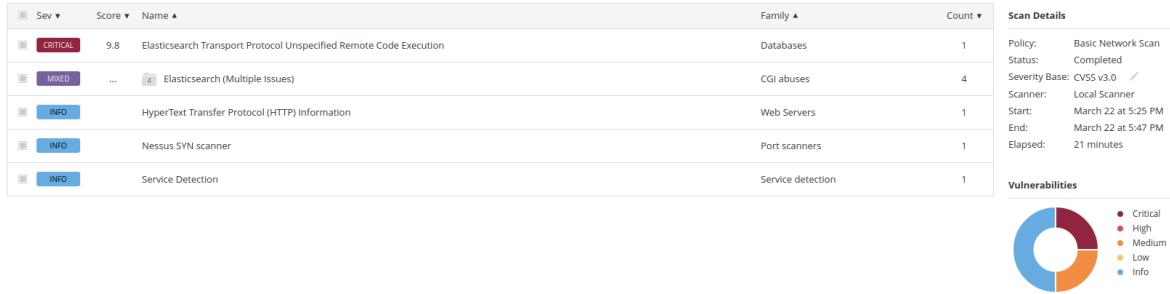


Figure 49: Algumas das vulnerabilidades associadas à *port* 9200

tcp/49157/dce-rpc: Utilizando o nmap não foi possível identificar a *port* 49157 como uma *port* aberta ao exterior, no entanto o nessus não só identificou esta *port* como aberta como ainda identificou 1 vulnerabilidade de risco médio que permite a atacantes realizarem ataques *man-in-the-middle* devido à inadequada autenticação nos canais RPC (Remote Procedure Call). Desta forma um atacante consegue forçar a autenticação no canal, permitindo ao utilizador malicioso fazer-se passar por uma das entidades na comunicação. Na figura abaixo encontram-se informação relacionada com a vulnerabilidade encontradas neste serviço.

90510 - MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)

Synopsis

The remote Windows host is affected by an elevation of privilege vulnerability.

Description

The remote Windows host is affected by an elevation of privilege vulnerability in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker able to intercept communications between a client and a server hosting a SAM database can exploit this to force the authentication level to downgrade, allowing the attacker to impersonate an authenticated user and access the SAM database.

Figure 50: Vulnerabilidade associadas à *port* 49157

tcp/0: Esta *port* também não foi identificada pelo nmap, mas corresponde a uma *port* reservada para tráfego TCP/IP que o nessus usa para identificar vulnerabilidades associadas com o sistema operativo do metasploitable. Nesta *port*, foi identificada uma vulnerabilidade crítica associada à versão antiga do OS presente no sistema que contém diversos problemas e falhas que foram mitigadas nas versões mais recentes desse OS. Na figura abaixo encontram-se informação relacionada com a vulnerabilidade encontradas nesta *port*.

108797 - Unsupported Windows OS (remote)

Synopsis

The remote OS or service pack is no longer supported.

Description

The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities.

Figure 51: Vulnerabilidade associadas à *port 0*

UDP

udp/5355: O nmap identificou a *port 5355* como uma *port* aberta/filtrada ao exterior, não sendo desta forma possível identificar vulnerabilidades associadas ao serviço UDP a correr nesta *port*. No entanto o nessus não só identificou esta *port* como aberta como ainda identificou 1 vulnerabilidade de risco crítico que permite a atacantes executarem código arbitrário remotamente devido a uma falha na instalação do serviço de DNS do windows. Na figura abaixo encontram-se informações relacionadas com a vulnerabilidade encontradas nesta *port*.

53514 - MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)

Synopsis

Arbitrary code can be executed on the remote host through the installed Windows DNS client.

Description

A flaw in the way the installed Windows DNS client processes Link-local Multicast Name Resolution (LLMNR) queries can be exploited to execute arbitrary code in the context of the NetworkService account.

Note that Windows XP and 2003 do not support LLMNR and successful exploitation on those platforms requires local access and the ability to run a special application. On Windows Vista, 2008, 7, and 2008 R2, however, the issue can be exploited remotely.

Figure 52: Vulnerabilidade associadas à *port 5355*

2.2 Resumo

Tal como podemos ver pelas secções anteriores e pela pergunta 1, o nmap e o nessus são ferramentas poderosas que permitem a utilizadores descobrir mais sobre as vulnerabilidades e falhas que podem ser exploradas por utilizadores maliciosos a partir do exterior. Contudo, apesar do nmap e nessus em alguns serviços identificaram as mesmas vulnerabilidades, na sua maioria foi necessário a pesquisa de falhas associadas às versões dos serviços disponíveis, durante a realização da pergunta 1, para ter uma noção das possíveis vulnerabilidades. Com o nessus, essa pesquisa não é tão necessária pois o nessus cria um relatório detalhado com todas as vulnerabilidades e respetivos

serviços comprometidos. É também possível verificar uma diferença entre as *ports* identificadas pelo o nmap e pelo nessus. A *port* 8022 e 8031 identificados pelo o nmap como possíveis serviços comprometidos por falhas não foram identificadas pelo o nessus como *ports* abertas ao exterior. As *ports* 9200, 5355 e 49157, foram identificadas pelo o nessus como *ports* com vulnerabilidades ao contrário do nmap que as não identificou como *ports* abertas. Conclui-se desta forma que o nmap é uma ferramenta mais conveniente quando queremos listar serviços disponíveis para o exterior o nessus é uma ferramenta mais utilizada para identificar detalhadamente vulnerabilidades associadas aos serviços a correr no sistema.

3 Questão 3

O primeiro evento identificado consiste num ”SNMP Request tcp” com classificado como uma tentativa de *leak* de informação cuja prioridade indicada pelo *output* do IDS é 2:

```
[**] [1:1418:11] SNMP request tcp [**]
[Classification: Attempted Information Leak] [Priority: 2]
03-23-11:46:26.790723 172.20.1.1:49219 → 172.20.1.2:161
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:48 DF
*****S* Seq: 0x322646BB Ack: 0x0 Win: 0x1000 TcpLen: 28
TCP Options (4) ⇒ MSS: 1460 NOP NOP SackOK
[Xref ⇒ http://cve.mitre.org/cgi-bin/cvename.cgi?name=2002-0013][Xref ⇒ http://cve.mitre.org/cgi-bin
tp://www.securityfocus.com/bid/4088]
```

Figure 53: Alerta gerado pelo IDS acerca do primeiro evento selecionado

A figura que se segue permite observar o tráfego relacionado com este alerta, através da aplicação do filtro no wireshark: snmp.

No.	Time	Source	Destination	Protocol	Length	Info
219	23.701283354	172.20.1.1	172.20.1.2	SNMP	85	get-next-request 1.3.6.1.2.1.1.1.0
220	23.701469549	172.20.1.2	172.20.1.1	ICMP	113	Destination unreachable (Port unreachable)
221	23.701626837	172.20.1.1	172.20.1.2	SNMP	85	get-next-request 1.3.6.1.2.1.1.1.0

Figure 54: Tráfego capturado no wireshark relacionado com o primeiro evento selecionado

A partir da figura acima é possível observar o envio do pacote SNMP, sendo que, o pedido efetuado é de ”Get-next-request”. Este pedido foi enviado pela porta 49219 do sistema auditor (Kali) para a porta 161 da VM onde está instalado o metasploitable. Por conseguinte, a resposta que foi recebida foi um pacote ICMP com a informação de que a porta não em questão (161) não estava acessível. Por conseguinte, foi enviado outra vez um novo pacote SNMP igual ao anterior para o qual não foi devolvida nenhuma resposta.

Tal como se pode observar pelo alerta gerado na figura seguinte, existem dois CVE associados a esta vulnerabilidade: CVE-2002-0012 e CVE-2002-0013. Estas vulnerabilidades estão relacionadas com o facto de algumas implementações do SNMP possibilitem a execução de ataques *denial of service* através de pedidos do tipo ”GetRequest”, ”GetNextRequest” e ”SetRequest”.

Já o segundo evento que foi escolhido é o seguinte:

```
[**] [1:249:8] DDOS mstream client to handler [**]
[Classification: Attempted Denial of Service] [Priority: 2]
03-23-11:46:27.270555 172.20.1.1:64739 -> 172.20.1.2:15104
TCP TTL:64 TOS:0x0 ID:0 Iplen:20 DgmLen:48 DF
*****S* Seq: 0x51F8ED8B Ack: 0x0 Win: 0x1000 TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2000-0138][Xref => http://www.whitehats.com/inf
```

Figure 55: Alerta gerado pelo IDS acerca do segundo evento selecionado

Através desta figura é possível observar que, o alerta indicado pelo IDS classifica-se como uma tentativa de DDOS, com prioridade 2. A sua descrição indica a existência de um *client* mstream que é passado para um *handler*.

tcp.port == 15104						
No.	Time	Source	Destination	Protocol	Length	Info
5843	26.214670701	172.20.1.1	172.20.1.2	TCP	62	64739 -> 15104 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
5850	26.214873327	172.20.1.2	172.20.1.1	TCP	60	15104 -> 64739 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Figure 56: Tráfego capturado no wireshark relacionado com o segundo evento selecionado

Neste foi enviado um SYN da máquina virtual onde o sistema auditor está instalado a partir da porta 64739 para a porta 15104 da VM onde está instalado o metasploitable. Este último respondeu com um SYN ACK.

O CVE associado a esta vulnerabilidade é o CVE-2000-0138. Esta indica que o sistema metasploitable possui um agente que permite ataques DDOS, sendo este agente o mstream.

4 Questão 4

O motivo pelo qual certas notificações que são apresentadas pelo IDS não aparecem como vulnerabilidades no relatório do Scanner (Nessus) assenta essencialmente no modo de funcionamento de ambas as ferramentas.

De facto, um IDS é um sistema que analisa o tráfego que passa através de uma interface e procura verificar se estão a ser comunicados pacotes maliciosos. Como neste caso o snort é um NIDS baseado em assinaturas, este consegue detetar tráfego malicioso através da comparação com assinaturas que conhece na sua base de dados. Por conseguinte, assim que esta ferramenta deteta este tipo de tráfego, envia uma notificação para o utilizador para o avisar que tal aconteceu.

O Nessus opera sobre um sistema de *plugins*, em que, consoante novas vulnerabilidades são descobertas são criados *plugins* que contenham informação das mesmas, assim como um conjunto de ações a tomar caso elas ocorram. Assim sendo, poderá ainda não ter sido desenvolvido um *plugin* para a vulnerabilidade pela qual esta não será identificada no scanner mesmo gerando uma notificação no IDS.[24]

Ora, apesar do tráfego que passa pela interface ter sido detetado e o sistema poder, de facto, estar a ser atacado não significa que este esteja vulnerável ao ataque, daí o Scanner não detetar vulnerabilidades que possam ser exploradas pelo ataque detetado pelo IDS. Além disso, devido a limitações do Scanner, este pode falhar em analisar vulnerabilidades do lado do cliente assim como os dispositivos que apenas estão conectados à rede de forma intermitente.[25]

5 Questão 5

5.1 Resultado do scanner antes da correção de vulnerabilidades

Antes da escolha e correção de vulnerabilidades efetuou-se uma varredura no sistema metasploitable onde foram encontradas 7 vulnerabilidades críticas, 7 com classificação alta, 15 de classificação média e 2 com baixa classificação, tal como se pode observar na seguinte figura:

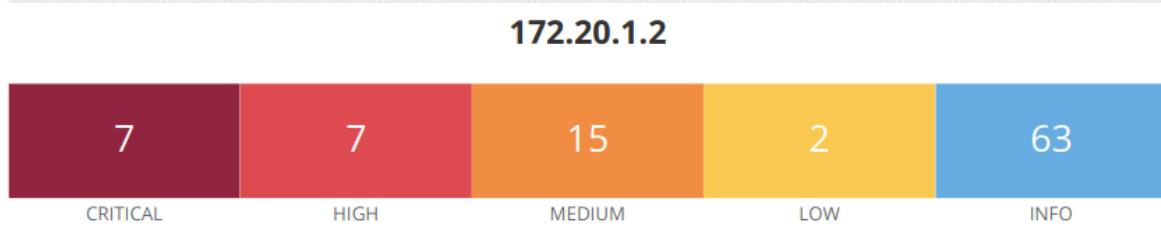


Figure 57: Número de vulnerabilidades por classificação antes de efetuar qualquer correção

A lista completa das vulnerabilidades encontradas neste processo encontra-se no Anexo A.

5.2 Correção da vulnerabilidade com classificação *low*

A primeira vulnerabilidade que foi escolhida está classificada como *low* e está associada ao facto de que o nível de segurança presente nas cifras dos serviços remotes não vai ao encontro do *standard FIPS-140*. Na seguinte figura está presente a descrição fornecida pelo *output* da varredura do Nessus, sendo que, existe uma solução que aponta no sentido de se alterar o nível do RDP (Remote Desktop Protocol).

The screenshot shows a Nessus scan result for a host at 172.20.1.2. A specific vulnerability is highlighted with a yellow box labeled "LOW".

LOW Terminal Services Encryption Level is not FIPS-140 Compliant

Description
The encryption setting used by the remote Terminal Services service is not FIPS-140 compliant.

Solution
Change RDP encryption level to :
4. FIPS Compliant

Figure 58: Vulnerabilidade de classificação baixa que vai ser corrigida

Ora, para implementar esta solução foram seguidos os passos presentes na documentação da Microsoft, que são os seguintes [26]:

- clicar no botão start do windows e utilizar a opção ”Administrative tools”, prosseguindo com a escolha da opção ”Remote Desktop Services” e por fim ”Remote Desktop Session Host Configuration”
- Já no menu de conexões clicar na conexão presente na lista e nas suas propriedades, sob a aba ”general” deve-se ativar a opção que indica ”FIPS Compliant” no menu *drop-down*.

A seguinte figura ilustra o processo inicial para chegar ao menu das conexões:

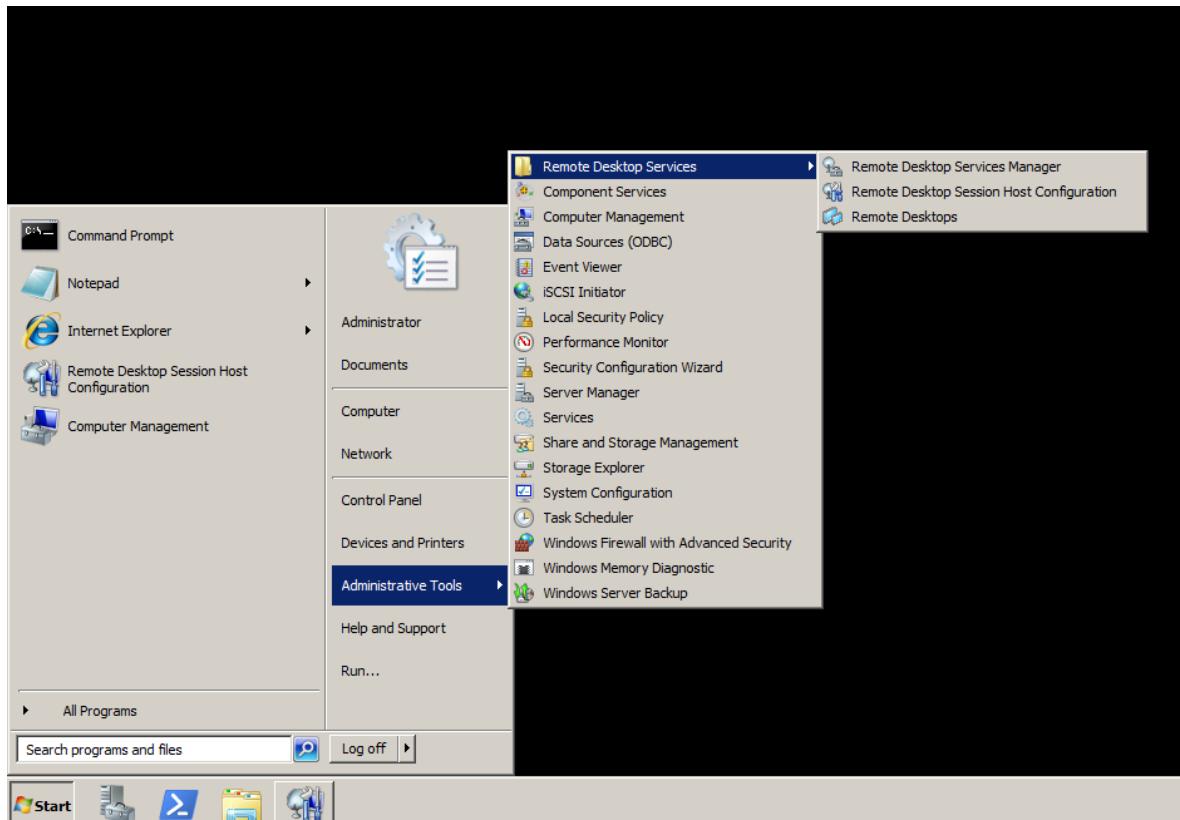


Figure 59: Sequências de opções que devem ser selecionadas para chegar ao menu de conexões remotas

Por conseguinte, a conexão que deve ser utilizada é que esta presente na imagem abaixo (RDP-Tcp):

Connections		
Connection Name	Connection Type	Transport
RDP-Tcp	Microsoft RDP 7.1	tcp

Figure 60: Conexão que vai ser alterada para corrigir vulnerabilidades

O último passo é então a ativação da opção que permite corrigir esta vulnerabilidade:

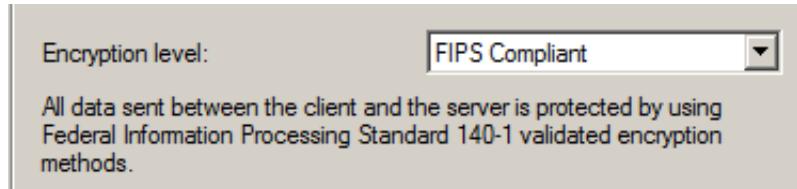


Figure 61: Alteração do nível de *encryption* para FIPS Compliant

5.3 Correção da vulnerabilidade com classificação *medium*

A segunda vulnerabilidade que foi escolhida para ser corrigida está classificada como ”medium” e vai ao encontro da possibilidade de poder ser efetuado um ataque *man-in-the-middle*, pois o cliente RDP presente nos serviços deste sistema não realiza validação da identidade do servidor, com o qual vai comunicar, aquando da definição da cifra que vai ser utilizada. Desta forma, um atacante que consiga interceptar mensagens com informação privada pode decifrá-las, pois não existem autenticação entre este e o cliente RDP do sistema.

Na seguinte figura está presente a descrição do Nessus sobre esta vulnerabilidade, sendo que, a solução que está apontada é a de ativar a opção; ”Allow connections only from computers running Remote Desktop with Network Level Authentication”.

MEDIUM Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness

Description
The remote version of the Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man-in-the-middle (MitM) attack. The RDP client makes no effort to validate the identity of the server when setting up encryption. An attacker with the ability to intercept traffic from the RDP server can establish encryption with the client and server without being detected. A MitM attack of this nature would allow the attacker to obtain any sensitive information transmitted, including authentication credentials.

This flaw exists because the RDP server stores a hard-coded RSA private key in the msasn1.dll library. Any local user with access to this file (on any Windows system) can retrieve the key and use it for this attack.

Solution

- Force the use of SSL as a transport layer for this service if supported, or/and
- Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.

Figure 62: Vulnerabilidade de classificação média identificada pelo Nessus

De facto, esta opção encontra-se no menu utilizado anteriormente sendo uma outra opção presente na aba ”general” da conexão indicada:

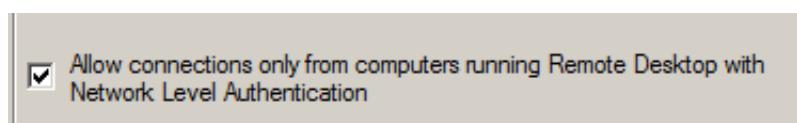


Figure 63: Opção que permite corrigir a segunda vulnerabilidade

5.4 Correção da vulnerabilidade com classificação *critical*

A última vulnerabilidade escolhida foi definida como crítica no relatório do Nessus e tem que ver com uma vulnerabilidade no connector AJP, cuja exploração desta já foi mencionada neste documento.

CRITICAL Apache Tomcat AJP Connector Request Injection (Ghostcat)

Description
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).

Solution
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.

Figure 64: Vulnerabilidade crítica identificada pelo Nessus

Assim sendo, prosseguiu-se com a correção da vulnerabilidade através da alteração do ficheiro de configuração, onde se comentou a linha que indica que o conector AJP utiliza a porta 8009 que é a porta que pode ser explorada por um atacante [27]:

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

Figure 65: Correção efetuada para a vulnerabilidade crítica

Ainda na documentação que foi seguida existe uma segunda possibilidade para alterar o ficheiro de configuração que seria introduzir um segredo que seria necessário para utilizar este serviço caso algum outro sistema externo o quisesse fazer, tal como se encontra na seguinte figura:

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

Figure 66: Adição de um segredo ao conector AJP na porta 8009

De facto, não se optou por esta abordagem, pois é necessário garantir que este segredo não é passível de ser descoberto nem adivinhado e caso não seja criado de forma correta pode levar a que a vulnerabilidade possa continuar a ser explorada.

5.5 Resultado do scanner depois da correção de vulnerabilidades

Por fim, voltou a efetuar-se a varredura, onde se verificou uma diminuição em todas as categorias de vulnerabilidades:

172.20.1.2



Figure 67: Número de vulnerabilidades por classificação após a correção das vulnerabilidades

A lista de vulnerabilidades completa apresenta-se no Anexo B e é possível observar através desta que as vulnerabilidades escolhidas para serem corrigidas já não aparecem na lista.

5.6 Discussão das soluções

Em todos os casos as vulnerabilidades apontadas pelo relatório do Nessus foram resolvidas e não voltaram a ser indicadas na segunda varredura.

Numa primeira instância, a resolução das vulnerabilidades que tem que ver com o RDP (classificação *low* e *medium*), foram alteradas no sentido de conferir maior segurança ao sistema. A ativação ”Allow connections only from computers running Remote Desktop with Network Level Authentication” apenas permite ao sistema aceitar conexões remotas caso haja uma autenticação prévia o que protege o sistema de atividade maliciosa [26]. Já o aumento do nível de *encryption* para ”FIPS Compliant” permite seguir um *standard* que obriga que certos requisitos aplicados a módulos criptográficos sejam seguidos [28].

Por outro lado, a última solução permite desligar o serviço Apache Tomcat através do conector AJP associado à porta 8009 do sistema. Ora, esta solução corrige, de facto, a vulnerabilidade mas torna o serviço inacessível caso este seja necessário. A outra solução indicada, que implementa um segredo para utilizar esse conector, pode ser mais útil caso o serviço seja necessário, apesar de haver mais dificuldades na sua implementação, pois é necessário garantir a segurança deste segredo quer ao nível criptográfico quer ao nível de não ser intercetado por alguém que pretenda realizar um ataque.

Anexos

1 Anexo A

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	9.8	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	119499	Elasticsearch ESA-2015-06
CRITICAL	9.8	105752	Elasticsearch Transport Protocol Unspecified Remote Code Execution
CRITICAL	9.8	125313	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (unprivileged check)
CRITICAL	9.8	108797	Unsupported Windows OS (remote)
CRITICAL	10.0*	53514	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)
CRITICAL	10.0*	90192	ManageEngine Desktop Central 8 / 9 < Build 91100 Multiple RCE
HIGH	8.8	79638	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (unprivileged check)
HIGH	8.1	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (unprivileged check)
HIGH	7.5	110192	Oracle GlassFish Server Path Traversal
HIGH	7.5	110612	Oracle GlassFish Server URL normalization Denial of Service
HIGH	7.5	35291	SSL Certificate Signed Using Weak Hashing Algorithm
HIGH	7.5	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	9.3*	58435	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (unprivileged check)
MEDIUM	6.8	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (unprivileged check)

Figure 68: Lista de vulnerabilidades antes da correção das vulnerabilidades

MEDIUM	6.5	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.1	108752	ManageEngine Desktop Central 9 < Build 92027 Multiple Vulnerabilities
MEDIUM	5.9	31705	SSL Anonymous Cipher Suites Supported
MEDIUM	5.9	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	101025	Elasticsearch Unrestricted Access Information Disclosure
MEDIUM	5.3	57608	SMB Signing not required
MEDIUM	5.3	15901	SSL Certificate Expiry
MEDIUM	5.3	45411	SSL Certificate with Wrong Hostname
MEDIUM	4.0	58453	Terminal Services Doesn't Use Network Level Authentication (NLA) Only
MEDIUM	6.8*	76572	Elasticsearch 'source' Parameter RCE
MEDIUM	5.1*	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
MEDIUM	6.4*	57582	SSL Self-Signed Certificate
MEDIUM	4.3*	57690	Terminal Services Encryption Level is Medium or Low
LOW	3.7	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
LOW	2.6*	30218	Terminal Services Encryption Level is not FIPS-140 Compliant

Figure 69: Lista de vulnerabilidades antes da correção das vulnerabilidades

2 Anexo B

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	9.8	119499	Elasticsearch ESA-2015-06
CRITICAL	9.8	105752	Elasticsearch Transport Protocol Unspecified Remote Code Execution
CRITICAL	9.8	108797	Unsupported Windows OS (remote)
CRITICAL	10.0*	90192	ManageEngine Desktop Central 8 / 9 < Build 91100 Multiple RCE
HIGH	8.8	79638	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (unprivileged check)
HIGH	8.1	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (unprivileged check)
HIGH	7.5	110192	Oracle GlassFish Server Path Traversal
HIGH	7.5	110612	Oracle GlassFish Server URL normalization Denial of Service
HIGH	7.5	35291	SSL Certificate Signed Using Weak Hashing Algorithm
HIGH	7.5	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	6.8	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (unprivileged check)
MEDIUM	6.5	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.1	108752	ManageEngine Desktop Central 9 < Build 92027 Multiple Vulnerabilities
MEDIUM	5.9	31705	SSL Anonymous Cipher Suites Supported
MEDIUM	5.3	101025	Elasticsearch Unrestricted Access Information Disclosure

Figure 70: Lista de vulnerabilidades após a correção das vulnerabilidades

MEDIUM	5.3	57608	SMB Signing not required
MEDIUM	5.3	15901	SSL Certificate Expiry
MEDIUM	5.3	45411	SSL Certificate with Wrong Hostname
MEDIUM	6.8*	76572	Elasticsearch 'source' Parameter RCE
MEDIUM	6.4*	57582	SSL Self-Signed Certificate
LOW	3.7	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)

Figure 71: Lista de vulnerabilidades após a correção das vulnerabilidades

Bibliography

- [1] "Blizzard" [online]. Disponível em: <https://www.blizzard.com/en-us/> [Acedido em março de 2022].
- [2] "Leadership" [online]. Disponível em: <https://www.activisionblizzard.com/leadership> [Acedido em março de 2022].
- [3] "Blizzard Entertainment" [online]. Disponível em: https://twitter.com/blizzard_ent [Acedido em março de 2022].
- [4] "FIND YOUR PEOPLE" [online]. Disponível em: <https://careers.blizzard.com/global/en> [Acedido em março de 2022].
- [5] "WoW's Back End: 10 Data Centers, 75,000 Cores" [online]. Disponível em: <https://www.datacenterknowledge.com/archives/2009/11/25/wows-back-end-10-data-centers-75000-cores> [Acedido em março de 2022].
- [6] "LIFE AT BLIZZARD: GLOBAL NETWORK OPERATIONS CENTER (GNOC)" [online]. Disponível em: <https://news.blizzard.com/en-us/blizzard/21700686/life-at-blizzard-global-network-operations-center-gnoc> [Acedido em março de 2022].
- [7] "360imprimir" [online]. Disponível em: <https://www.360imprimir.pt/> [Acedido em março de 2022].
- [8] "360imprimir" [online]. Disponível em: <https://pt-pt.facebook.com/360imprimirPT/> [Acedido em março de 2022].
- [9] "360imprimir" [online]. Disponível em: https://www.200m.pt/pt-pt/case_study/binary-subject-s-a-360imprimir/ [Acedido em março de 2022].
- [10] "360imprimir" [online]. Disponível em: <https://pt.linkedin.com/company/360imprimir/> [Acedido em março de 2022].
- [11] "360imprimir" [online]. Disponível em: <https://www.linkedin.com/company/360imprimir/people/> [Acedido em março de 2022].
- [12] "CVE-2016-8858" [online]. Disponível em: <https://vulners.com/cve/CVE-2016-8858> [Acedido em março de 2022].
- [13] "CVE-2016-6515" [online]. Disponível em: <https://vulners.com/cve/CVE-2016-6515> [Acedido em março de 2022].

- [14] "CVE-2022-21922" [online]. Disponível em: <https://www.cybersecurity-help.cz/vdb/SB2022011181> [Acedido em março de 2022].
- [15] "CVE-2017-0161" [online]. Disponível em: <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2017-0161> [Acedido em março de 2022].
- [16] "CVE-2012-3163" [online]. Disponível em: <https://nvd.nist.gov/vuln/detail/CVE-2012-3163#vulnCurrentDescriptionTitle> [Acedido em março de 2022].
- [17] "CVE-2007-1944" [online]. Disponível em: <https://www.cvedetails.com/cve/CVE-2007-1944/> [Acedido em março de 2022].
- [18] "CVE-2020-1938" [online]. Disponível em: <https://www.chaitin.cn/en/ghostcat> [Acedido em março de 2022].
- [19] "CVE-2014-0075" [online]. Disponível em: <https://nvd.nist.gov/vuln/detail/CVE-2014-0075> [Acedido em março de 2022].
- [20] "CVE-2000-0673" [online]. Disponível em: <https://docs.microsoft.com/en-us/security-updates/securitybulletins/2000/ms00-047> [Acedido em março de 2022].
- [21] "CVE-2019-0708" [online]. Disponível em: <https://www.cvedetails.com/cve/CVE-2019-0708/> [Acedido em março de 2022].
- [22] "CVE-2002-0013 Detail" [online]. Disponível em: <https://nvd.nist.gov/vuln/detail/CVE-2002-0013> [Acedido em março de 2022].
- [23] "CVE-2002-0012 Detail" [online]. Disponível em: <https://nvd.nist.gov/vuln/detail/CVE-2002-0012> [Acedido em março de 2022].
- [24] "Plugins" [online]. Disponível em: <https://www.tenable.com/plugins> [Acedido em março de 2022].
- [25] "Traditional Active Scans (Non-credentialed)" [online]. Disponível em: <https://docs.tenable.com/nessusagent/Content/TraditionalScansUncredentialed.htm> [Acedido em março de 2022].
- [26] "Configure Network Level Authentication for Remote Desktop Services Connections" [online]. Disponível em: [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732713\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732713(v=ws.11)) [Acedido em março de 2022].
- [27] "AJP File Read/Inclusion in Apache Tomcat (CVE-2020-1938) and Undertow (CVE-2020-1745)" [online]. Disponível em: <https://access.redhat.com/solutions/4851251> [Acedido em março de 2022].
- [28] "Security Requirements for Cryptographic Modules" [online]. Disponível em: <https://csrc.nist.gov/publications/detail/fips/140/2/final> [Acedido em março de 2022].