

Tecnologia de Segurança

27 de Dezembro de 2020

Trabalho Prático 2 - Grupo 7

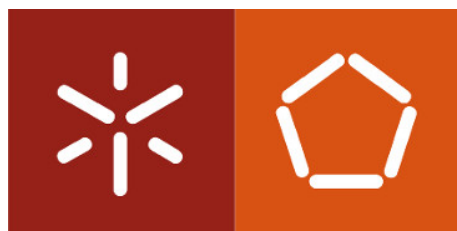
a83899

André Morais

a84485

Tiago Magalhães

Passive Information Gathering & PenTest - Scanning



Mestrado Integrado em Engenharia Informática
Universidade do Minho

Conteúdo

1	Introdução	2
2	Passive Information Gathering	3
2.1	Esposende 2000	4
2.2	Continente	6
3	PenTest - Scanning	7
3.1	Questão 1	7
3.1.1	OpenSSH 7.1 (protocol 2.0)	10
3.1.2	Microsoft Windows RPC	10
3.1.3	Microsoft Windows netbios-ssn	10
3.1.4	Microsoft Windows Server 2008 R2	10
3.1.5	MySQL 5.5.20	11
3.1.6	Apache Jserv (Protocol v1.3)	11
3.1.7	Apache Tomcat/Coyote JSP engine 1.1	11
3.1.8	Sun GlassFish Open Source Edition 4.0	11
3.2	Questão 2	12
3.3	Questão 3	15
3.4	Questão 4	18
3.5	Questão 5	19
3.5.1	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)	19
3.5.2	Apache Tomcat AJP Connector Request Injection (Ghostcat)	21
3.5.3	SMB Signing not required	22
4	Conclusão	23

1 Introdução

Este trabalho foi dividido em duas partes. Numa primeira parte onde aplicamos a primeira etapa de *footprinting* de *penetration testing* que é *passive (reconnaissance)* com o objetivo de tentar descobrir o máximo de informação sobre duas empresas, uma local e outra de maiores dimensões sem entrar em contacto diretamente com o sistema computacional destas.

Na segunda parte do trabalho, era necessário utilizar técnicas de *Scanning*(segunda etapa de *footprinting*) para responder às questões solicitadas pelos professores. Aqui já existe uma interação direta (ativa) com o sistema computacional, de modo a identificar possíveis ameaças e vulnerabilidades.

2 Passive Information Gathering

No âmbito da unidade curricular de Tecnologia de Segurança foi-nos proposto o uso de técnicas de busca passiva de informação que permitam identificar detalhes sobre os sistemas e infra-estrutura (Passive Information Gathering) através de diferentes técnicas:

- Análise de informações de registo do domínio(*whois* <https://lookup.icann.org/>);
- DNS
- Análise da página web;
- Motores de busca(*google,shodan.io*)

Escolhemos como alvo deste estudo para realizar buscas de informações duas empresas de diferentes dimensões:

- Esposende 2000 como negócio local
- Continente como empresa nacional

2.1 Esposende 2000

Esposende 2000 é uma empresa que fornece serviços como ginásio e piscinas.

Usando a ferramenta **nslookup**, obtivemos o endereço do respetivo site, como podemos observar na Figura 1.

```
morais@DESKTOP-OR2ENKF:/mnt/c/Users/andre$ nslookup www.esposende2000.pt
Server:      192.168.1.1
Address:     192.168.1.1#53

Non-authoritative answer:
www.esposende2000.pt  canonical name = esposende2000.pt.
Name:   esposende2000.pt
Address: 94.46.167.25
```

Figura 1: nslookup query

Depois, com a ajuda da ferramenta **whois.domaintools.com**, conseguimos obter algumas informações pessoais, cujo as quais não deveriam ser tão facilmente encontradas, como o nome da pessoa que trata do hosting do site (Figura 2 e 3).

Atualmente, a informação digital é um dos principais produtos da nossa era e necessita de ser convenientemente protegida. Com a exposição destes pequenos dados, pode haver terceiros que tirem proveito através de engenharia social.

IP Information for 94.46.167.25

— Quick Stats

IP Location	Portugal Lisbon Almouroltec Servicos De Informatica E Internet Lda
ASN	AS24768 ALMOUROLTEC, PT (registered Nov 12, 2009)
Resolve Host	cp1.signed.pt
Whois Server	whois.ripe.net
IP Address	94.46.167.25
Reverse IP	294 websites use this address.

% Abuse contact for '94.46.167.0 - 94.46.167.255' is 'abuse@ptisp.pt'

inetnum:	94.46.167.0 - 94.46.167.255
netname:	PT-ALMOUROLTEC
descr:	LIS DEDICATED SERVERS IP SPACE
country:	PT
admin-c:	LUIS-RIPE
tech-c:	LUIS-RIPE
status:	ASSIGNED PA
mnt-by:	MNT-ALMOUROLTEC
created:	2017-01-30T15:23:58Z
last-modified:	2017-01-30T15:23:58Z
source:	RIPE
person:	Luis Inverno
address:	Estrada Nacional n3
address:	2250-028 Constancia
address:	Portugal
fax-no:	+351 249739154
phone:	+351 249739099
nic-hdl:	LUIS-RIPE
mnt-by:	MNT-ALMOUROLTEC
created:	2013-01-22T15:02:18Z
last-modified:	2017-10-30T22:24:12Z
source:	RIPE
route:	94.46.160.0/20
descr:	ALMOUROLTEC SERVICOS DE INFORMATICA E INTERNET LDA
origin:	AS24768
mnt-by:	MNT-ALMOUROLTEC
created:	2015-01-29T20:56:30Z
last-modified:	2015-01-29T20:56:30Z
source:	RIPE

Figura 2: whois.domaintools.com/94.46.167.25

Informações da Almouroltec - Serviços de Informática e Internet Lda

NIF	502665696	Morada da Sede	Est Nacional 3 Constança 2250-028 Constança
Forma Jurídica	Sociedade por Quotas	Capital Social	Indisponível
Data Constituição	Anterior a 2006	CAE	62020 - Actividades de consultoria em informática
Última Atualização	28/09/2020	Atos Disponíveis	18 Atos societários
Designações Anteriores	2003 - José Luís Inverno - Investimentos Imobiliários, Lda 2003 - Almouroltec - Serviços de Informática e Internet, Lda		
Balanço Disponível	2019, 2018, 2017, 2016, 2015, 2014, 2012, 2011, 2010, 2009, 2008, 2007, 2006 - Consultar		

Figura 3

Numa última procura, com uso do **shodan.io**¹ conseguimos descobrir algumas tecnologias usadas pelos serviços alojados no *host* do site, o que com uma grande probabilidade podem corresponder aos do *website*, como se observa na Figura 4.

De referir, que pode ser perigoso a exposição destas mesmas, pois sabendo as tecnologias usadas, facilmente se descobrem as respetivas vulnerabilidades, deixando este site com falhas na segurança ou até mesmo na sua funcionalidade.

⚡ Web Technologies
















 animate.css
 Bootstrap
 Font Awesome
 Google Tag Manager
 jQuery
 jQuery Migrate
 MySQL
 OWL Carousel
 PHP
 Slick
 TrackJS
 Underscore.js
 WordPress
 WP Rocket
 wpBakery

Figura 4: Tecnologias usadas

¹mecanismo de pesquisa que permite ao usuário encontrar tipos específicos de computadores conectados à Internet usando uma variedade de filtros.

2.2 Continente

Escolhemos, também, o a empresa Continente, devido à sua grandeza no nosso país e ficamos intrigados se haveria ou não, *leaks* de informações.

Começamos então por obter o endereço dos domínio.

```
morais@DESKTOP-OR2ENKF:/mnt/c/Users/andre$ nslookup www.continente.pt
Server:      192.168.1.1
Address:     192.168.1.1#53

Non-authoritative answer:
www.continente.pt    canonical name = www-continente-pt.sonaemc.prod2.reblaze.com.
Name:   www-continente-pt.sonaemc.prod2.reblaze.com
Address: 35.244.167.140
```

Figura 5: nslookup query

Os passos para obtenção de informação foram idênticos, mas com resultados diferentes, como era de esperar.

O continente tem o seu site hospedado na **Google Cloud** e esta não revela nenhuma informação pessoal sobre os responsáveis da administração do host. É normal que empresas com grandes dimensões tenham de alocar os seus servidores em sítios com prestígio e conhecidos como a Google, sabendo que o risco da falha de segurança é menor. Também com o uso do **shodan.io** não detetamos quaisquer tipo de serviços no *host* do *website* nem tecnologias utilizadas.



IP Information for 35.244.167.140	
— Quick Stats	
IP Location	 United States Of America Kansas City Google Llc
ASN	 AS15169 GOOGLE, US (registered Mar 30, 2000)
Resolve Host	140.167.244.35.bc.googleusercontent.com
Whois Server	whois.arin.net
IP Address	35.244.167.140
Reverse IP	4 websites use this address.
<div>NetRange: 35.208.0.0 - 35.247.255.255</div> <div>CIDR: 35.240.0.0/13, 35.224.0.0/12, 35.208.0.0/12</div> <div>NetName: GOOGLE-CLOUD</div> <div>NetHandle: NET-35-208-0-0-1</div> <div>Parent: NET35 (NET-35-0-0-0)</div> <div>NetType: Direct Allocation</div> <div>OriginAS:</div> <div>Organization: Google LLC (GOOGL-2)</div> <div>RegDate: 2017-09-29</div> <div>Updated: 2018-01-24</div> <div>Comment: *** The IP addresses under this Org-ID are in use by Google Cloud customers ***</div> <div>Comment:</div> <div>Comment: Direct all copyright and legal complaints to</div> <div>Comment: https://support.google.com/legal/go/report</div> <div>Comment:</div> <div>Comment: Direct all spam and abuse complaints to</div> <div>Comment: https://support.google.com/code/go/gce_abuse_report</div> <div>Comment:</div> <div>Comment: For fastest response, use the relevant forms above.</div> <div>Comment:</div> <div>Comment: Complaints can also be sent to the GC Abuse desk</div> <div>Comment: (google-cloud-compliance@google.com)</div> <div>Comment: but may have longer turnaround times.</div> <div>Ref: https://rdap.arin.net/registry/ip/35.208.0.0</div> <div>OrgName: Google LLC</div> <div>OrgId: GOOGL-2</div> <div>Address: 1600 Amphitheatre Parkway</div> <div>City: Mountain View</div> <div>StateProv: CA</div> <div>PostalCode: 94043</div> <div>Country: US</div>	

Figura 6: whois.domaintools.com/35.244.167.140

3 PenTest - Scanning

Para a concretização do Penetration Testing foi necessário a instalação e configuração de um ambiente de Pentest. Na realização destas atividades utilizamos diversas ferramentas, como:

- Nmap
- Nessus
- Snort
- Wireshark

3.1 Questão 1

Nesta questão usamos apenas a ferramenta **nmap** que permite "varrer" as portas e identificar os respectivos serviços.

Para identificar as vulnerabilidades/fraquezas, precisamos de saber as versões dos serviços. Consequentemente, utilizamos o comando **nmap -sV *target*** que faz uma varredura as portas, identificando o serviço em cada uma delas, assim como a sua versão. Houve um serviço que o nmap não conseguiu reconhecer como está exposto na Figura 7


```

tiagokali@tiagokali:~$ sudo nmap -sV 172.20.7.2
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-20 16:30 WET
Nmap scan report for 172.20.7.2
Host is up (0.000089s latency).
Not shown: 981 closed ports
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
3306/tcp   open  mysql             MySQL 5.5.20-log
3389/tcp   open  tcpwrapped
4848/tcp   open  ssl/appserv-http?
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             Sun GlassFish Open Source Edition 4.0
8181/tcp   open  ssl/intermapper?
8383/tcp   open  ssl/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
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port9200-TCP:V=7.91%I=7%D=12/20%Time=5FDF7C24%P=x86_64-pc-linux-gnu%r(G
SF:etRequest,190,"HTTP/1.0\x20200\x200K\r\nContent-Type:\x20application/j
SF:son;\x20charset=UTF-8\r\nContent-Length:\x20313\r\n\r\n{\r\n\x20\x20"s
SF:tatus"\x20:\x20200,\r\n\x20\x20"name"\x20:\x20"Captain\x20Ultra",\
SF:r\n\x20\x20"version"\x20:\x20{\r\n\x20\x20\x20\x20"number"\x20:\x20
SF:"1\1\1",\r\n\x20\x20\x20\x20"build_hash"\x20:\x20"f1585f096d3f39
SF:85e73456debdca0745f512bbc",\r\n\x20\x20\x20\x20"build_timestamp"\x2
SF:0:\x20"2014-04-16T14:27:12Z",\r\n\x20\x20\x20\x20"build_snapshot"\x
SF:20:\x20false,\r\n\x20\x20\x20\x20"lucene_version"\x20:\x20"4.7"\r\
SF:n\x20\x20},\r\n\x20\x20"tagline"\x20:\x20"You\x20Know,\x20for\x20Sea
SF:rch"\r\n}\n")%r(HTTPOptions,4F,"HTTP/1.0\x20200\x200K\r\nContent-Type
SF::\x20text/plain;\x20charset=UTF-8\r\nContent-Length:\x200\r\n\r\n")%r(R
SF:TSPRequest,4F,"HTTP/1.1\x20200\x200K\r\nContent-Type:\x20text/plain;\x
SF:20charset=UTF-8\r\nContent-Length:\x200\r\n\r\n")%r(FourOhFourRequest,A
SF:9,"HTTP/1.0\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain;\x
SF:20charset=UTF-8\r\nContent-Length:\x2080\r\n\r\nNo\x20handler\x20found\
SF:x20for\x20uri\x20[/nice%20ports%2C/Tri%6Eity\1.txt%2ebak\])\x20and\x20me
SF:thod\x20[GET]")%r(SIPOptions,4F,"HTTP/1.1\x20200\x200K\r\nContent-Ty
SF:pe:\x20text/plain;\x20charset=UTF-8\r\nContent-Length:\x200\r\n\r\n");
MAC Address: 08:00:27:A0:6A:93 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 131.95 seconds

```

Figura 7: nmap -sV target

Também foi necessário identificar o sistema operativo que corria no metasploitable 3, pois é preciso saber se as vulnerabilidades afetam este s.o.. O comando **nmap -O target** ajuda-nos nesta questão (Figura 8).

```
tiagokali@tiagokali:~$ sudo nmap -O 172.20.7.2
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-20 16:28 WET
Nmap scan report for 172.20.7.2
Host is up (0.00032s latency).
Not shown: 981 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
3306/tcp   open  mysql
3389/tcp   open  ms-wbt-server
4848/tcp   open  appserv-http
7676/tcp   open  imqbrokerd
8009/tcp   open  ajp13
8022/tcp   open  oa-system
8031/tcp   open  unknown
8080/tcp   open  http-proxy
8181/tcp   open  intermapper
8383/tcp   open  m2mservices
8443/tcp   open  https-alt
9200/tcp   open  wap-wsp
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
MAC Address: 08:00:27:A0:6A:93 (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 16.97 seconds
```

Figura 8: **nmap -O target**

De forma a obtermos mais informações acerca do sistema operativo do metasploitable 3 utilizamos agora a flag -A:

```
Host script results:
--_clock-skew: mean: 1h08m34s, deviation: 3h01m26s, median: 0s
--nbstat: NetBIOS name: VAGRANT-2008R2, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:5c:00:6d (Oracle VirtualBox virtual NIC)
--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: 2020-12-20T09:57:37-08:00
--smb-security-mode:
  account_used: <blank>
  authentication_level: user
  challenge_response: supported
  message_signing: disabled (dangerous, but default)
--smb2-security-mode:
  2.02:
    Message signing enabled but not required
--smb2-time:
  date: 2020-12-20T17:57:34
  start_date: 2020-12-20T17:13:21

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 131.49 seconds
```

Figura 9: **nmap -A target**

3.1.1 OpenSSH 7.1 (protocol 2.0)

OpenSSH é um conjunto de softwares de rede relacionado à segurança que provém a criptografia em sessões de comunicações numa rede usando o protocolo SSH.

- **CVE:** CVE-2016-6515
- **Descrição:** A função *auth_password* no *auth-passwd.c* em *sshd* no OpenSSH antes do 7.3 não limita o tamanho das passwords de autenticação, o que permite aos atacantes de provocar um denial of service através de uma string grande
- **Base Score:** 7.5 HIGH

3.1.2 Microsoft Windows RPC

Microsoft RPC é uma versão modificada do DCE/RPC. As inclusões incluem suporte parcial para cadeias UCS-2, handlers implícitos e cálculos complexos nos paradigmas de estrutura já presentes no DCE/RPC

- **CVE:** CVE-2016-0178
- **Descrição:** O RPC não trata devidamente das *free operations*, o que permite a atacantes remotos para executar código arbitrário via pedidos RPC mal formados , ou seja, "*RPC Network Data Representation Engine Elevation of Privilege Vulnerability.*"
- **Base Score:** 8.8 HIGH

3.1.3 Microsoft Windows netbios-ssn

É uma API que fornece serviços relacionados com a camada de sessão, permitindo que as aplicações em computadores separados comuniquem numa rede local

- **CVE:** CVE-2019-0543
- **Descrição:** Existe uma vulnerabilidade de elevação de privilégios quando o Windows lida inapropriadamente com pedidos de autenticação
- **Base Score:** 7.8 HIGH

3.1.4 Microsoft Windows Server 2008 R2

O Windows Server 2008 R2 é um sistema operacional, produzido pela Microsoft.

- **CVE:** CVE-2018-8553
- **Descrição:** Existe uma vulnerabilidade na execução de um código remoto que faz com que o Microsoft Graphics Components lida com objetos em memória
- **Base Score:** 7.8 High

3.1.5 MySQL 5.5.20

O MySQL é um sistema de gerenciamento de base de dados, que utiliza a linguagem SQL como interface.

- **CVE:** CVE-2012-0882
- **Descrição:** Buffer overflow no yaSSL, usado no MySQL 5.5.20, permite a atacantes remotos de executar código arbitrário através de vetores não especificados.
- **Base Score:** 7.5 High

3.1.6 Apache Jserv (Protocol v1.3)

O Apache Jserv Protocol é um protocolo que pode fazer pedidos proxy de entrada de um servidor da Web para um servidor de aplicações que fica atrás do servidor da Web

- **CVE:** CVE-2020-1938
- **Descrição:** Esta uma vulnerabilidade LFI(Local File Intrusion) no Apache Jserver Protocol service. Um atacante pode explorar esta vulnerabilidade e ler conteúdos dos ficheiros de configuração e do código fonte de todas as webapps implementadas no Tomcat
- **Base Score:** 9.8 Critical

3.1.7 Apache Tomcat/Coyote JSP engine 1.1

O Apache Tomcat fornece software para correr Java applets no browser. O coyote é um web server autossuficiente (stand-alone) que fornece servlets para os applets do Tomcat, ou seja, funciona como um Apache web server, mas para JavaServer Pages (JSP)

- **CVE:** CVE-2014-0227
- **Descrição:** java/org/apache/coyote/http11/filters/ChunkedInputFilter.java em Apache Tomcat 6.x before 6.0.42, 7.x before 7.0.55, and 8.x before 8.0.9 nao lida bem com várias tentativas para continuar a ler dados após um erro,o que permite a atacantes remotos enviar HTTP request para causar Denial of Service.
- **Base Score:** 6.4 Medium(CVSS 2.0)

3.1.8 Sun GlassFish Open Source Edition 4.0

GlassFish é um servidor de aplicação open source liderado pela Sun Microsystems para a plataforma Java EE. GlassFish é software livre.

Não foi encontrada nenhuma vulnerabilidade para esta edição do Sun GlasshFish Open Source.

3.2 Questão 2

Para a varredura ativa do Sistema Mestasploitable 3 usamos o **Nessus** como ferramenta. O resultado apresentou várias vulnerabilidades de diferentes níveis de prioridade. Assim temos:

- **Critical**: Vulnerabilidades críticas ao sistema. Neste caso um atacante tem poder de leitura e escrita sobre ficheiros da máquina do utilizador. O base score do CVSSv3 está entre **9.0-10.0**;
- **High**: Vulnerabilidade de nível alto. São vulnerabilidades difíceis de explorar, mas podem resultar de acessos de elevado privilégio, podendo resultar em perda ou fuga de dados. O base score do CVSSv3 está entre **7.0-8.9**;
- **Medium**: Vulnerabilidade de nível médio. Para explorar estas vulnerabilidades é necessário ter privilégios de utilizador, assim como estar na mesma rede que a vítima. O base score do CVSSv3 está entre **4.0-6.9**;
- **Low**: Vulnerabilidade de nível baixo. Vulnerabilidades que, quando exploradas, têm um impacto muito baixo no sistema alvo. O base score do CVSSv3 está entre **0.1-3.9**;
- **Info**: Apenas informa ao utilizador que existem serviços que podem ser considerados vulneráveis. Identifica que alguma informação da máquina pode ser descoberta. O base score do CVSSv3 é de **0**;

Após o scan do Nessus, obtivemos uma barra com o número de vulnerabilidades que eram 170 e suas respetivas classificações.



Figura 10: Número de vulnerabilidades agrupadas por classificação

Podemos ver mais detalhadamente estas mesmas vulnerabilidades apresentadas no gráfico, se clicarmos nas vulnerabilidades também conseguimos ver o CVE associados a elas bem como documentação para possíveis soluções.

<input type="checkbox"/>	CRITICAL	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)	Windows	1		
<input type="checkbox"/>	CRITICAL	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)	Windows	1		
<input type="checkbox"/>	CRITICAL	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)	Windows	1		
<input type="checkbox"/>	CRITICAL	Unsupported Windows OS (remote)	Windows	1		

Figura 11: Vulnerabilidades *Critical*

<input type="checkbox"/>	HIGH	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)	Windows	1	🔄	✎
<input type="checkbox"/>	HIGH	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMAN...)	Windows	1	🔄	✎
<input type="checkbox"/>	HIGH	Elasticsearch ESA-2015-06	CGI abuses	1	🔄	✎
<input type="checkbox"/>	HIGH	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1	🔄	✎
<input type="checkbox"/>	HIGH	Elasticsearch Transport Protocol Unspecified Remote Code Execution	Databases	1	🔄	✎

Figura 12: Vulnerabilidades *High*

<input type="checkbox"/>	MEDIUM	SSL Certificate Cannot Be Trusted	General	4	🔄	✎
<input type="checkbox"/>	MEDIUM	SSL Medium Strength Cipher Suites Supported (SWEET32)	General	4	🔄	✎
<input type="checkbox"/>	MEDIUM	SSL Self-Signed Certificate	General	4	🔄	✎
<input type="checkbox"/>	MEDIUM	SSL Certificate with Wrong Hostname	General	3	🔄	✎
<input type="checkbox"/>	MEDIUM	SSL Certificate Expiry	General	1	🔄	✎
<input type="checkbox"/>	MEDIUM	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	General	1	🔄	✎

Figura 13: Vulnerabilidades *Medium*

<input type="checkbox"/>	LOW	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Misc.	3	🔄	✎
<input type="checkbox"/>	LOW	Terminal Services Encryption Level is not FIPS-140 Compliant	Misc.	1	🔄	✎

Figura 14: Vulnerabilidades *Low*

<input type="checkbox"/>	INFO	Nessus SYN scanner	Port scanners	17	🔄	✎
<input type="checkbox"/>	INFO	4 HTTP (Multiple Issues)	Web Servers	13	🔄	✎
<input type="checkbox"/>	INFO	Service Detection	Service detection	12	🔄	✎
<input type="checkbox"/>	INFO	7 SMB (Multiple Issues)	Windows	8	🔄	✎
<input type="checkbox"/>	INFO	DCE Services Enumeration	Windows	8	🔄	✎
<input type="checkbox"/>	INFO	2 Oracle Glassfish Server (Multiple Issues)	Web Servers	4	🔄	✎
<input type="checkbox"/>	INFO	SSL / TLS Versions Supported	General	4	🔄	✎

Figura 15: *Info* de possíveis vulnerabilidades

Podemos observar que o sistema ao qual foi feito uma varredura encontra-se cheio de vulnerabilidades sendo muita destas de prioridade Crítica, estas são recomendadas que se encontre logo uma solução, já que de acordo com o seu CVSS apresentam um maior risco para o sistema.

Em relação à questão 1 o Nessus conseguiu detetar essas vulnerabilidades apontadas como por exemplo: *GhostCat*, além de que fornece as vulnerabilidades organizadas por ordem de prioridade, também consegue associar o CVE e possíveis soluções o que automatiza o trabalho humano.

Concluimos então, que o sistema tinha mais vulnerabilidades do que pensávamos enquanto procurávamos na questão 1 por estas.

3.3 Questão 3

Através da análise do output do Snort, através do ficheiro **alert.full**, indentificamos vários tráfegos anómalos, entres os quais, era para ser escolhidos apenas dois.

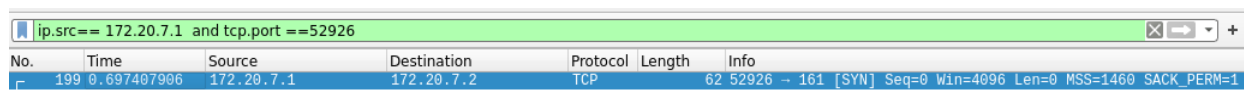
Primeiramente vimos uma tentativa de *leak* de informação. O output correspondente foi:

```
[**] [1:1418:11] SNMP request tcp [**]  
[Classification: Attempted Information Leak] [Priority: 2]  
12/21-16:10:38.430607 08:00:27:14:BF:19 → 08:00:27:5C:00:6D type:0x800 len:0x3E  
172.20.7.1:52926 → 172.20.7.2:161 TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:48 DF  
*****S* Seq: 0x55C8A50F 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/cvename.cgi?name=2002-0012][Xref ⇒ http://www.securityfocus.com/bid/4132][Xref ⇒ http://www.securityfocus.com/bid/4089][Xref ⇒ http://www.securityfocus.com/bid/4088]
```

Figura 16: Output do Snort de Information Leak

Essa tentativa partiu da máquina com ip *172.20.7.1* através da porta *52926*, e o destino foi a máquina com ip *172.20.7.2* na porta *161*.

No Wireshark aplicamos um filtro de pesquisa como podemos verificar na imagem seguinte, devolvendo um pacote SYN



The image shows a Wireshark packet capture window with a filter bar set to 'ip.src == 172.20.7.1 and tcp.port == 52926'. The packet list shows a single packet (No. 199) at time 0.697407906, from source 172.20.7.1 to destination 172.20.7.2, protocol TCP, length 62. The packet details show a SYN flag, sequence number 0, window size 4096, and MSS 1460.

No.	Time	Source	Destination	Protocol	Length	Info
199	0.697407906	172.20.7.1	172.20.7.2	TCP	62	52926 → 161 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1

Figura 17: Pacote TCP de Information Leaks

Através das duas primeiras referências do Information Leak chegamos às vulnerabilidades cujo CVE são CVE-2002-013 e CVE-2002-012, respetivamente:


Current Description

Vulnerabilities in a large number of SNMP implementations allow remote attackers to cause a denial of service or gain privileges via SNMPv1 trap handling, as demonstrated by the PROTON c06-SNMPv1 test suite. NOTE: It is highly likely that this candidate will be SPLIT into multiple candidates, one or more for each vendor. This and other SNMP-related candidates will be updated when more accurate information is available.

[+View Analysis Description](#)

Severity CVSS Version 3.x CVSS Version 2.0

CVSS 2.0 Severity and Metrics:

 **NIST:** NVD **Base Score:** 10.0 HIGH **Vector:** (AV:N/AC:L/Au:N/C:C/I:C/A:C)

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

Figura 18: CVE-2002-012


Current Description

Vulnerabilities in the SNMPv1 request handling of a large number of SNMP implementations allow remote attackers to cause a denial of service or gain privileges via (1) GetRequest, (2) GetNextRequest, and (3) SetRequest messages, as demonstrated by the PROTON c06-SNMPv1 test suite. NOTE: It is highly likely that this candidate will be SPLIT into multiple candidates, one or more for each vendor. This and other SNMP-related candidates will be updated when more accurate information is available.

[+View Analysis Description](#)

Severity CVSS Version 3.x CVSS Version 2.0

CVSS 2.0 Severity and Metrics:

 **NIST:** NVD **Base Score:** 10.0 HIGH **Vector:** (AV:N/AC:L/Au:N/C:C/I:C/A:C)

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

Figura 19: CVE-2002-013

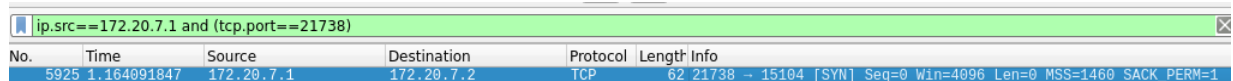
Uma outra anomalia foi uma tentativa de Denial of Service:

```
[**] [1:249:8] DDOS mstream client to handler [**]  
[Classification: Attempted Denial of Service] [Priority: 2]  
12/21-16:10:38.897291 08:00:27:14:BF:19 → 08:00:27:5C:00:6D type:0x800 len:0x3E  
172.20.7.1:21738 → 172.20.7.2:15104 TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:48 DF  
*****S* Seq: 0xD9BB0716 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/info/IDS111]
```

Figura 20: Output do Snort de Denial of Service

Mais uma vez podemos confirmar a tentativa de DOS feita pela mesma máquina e com o mesmo destino, mas em portas diferentes, respetivamente, a porta 21738 e 15104.

No Wireshark aplicamos um filtro de pesquisa parecido ao anterior, devolvendo também um pacote SYN



No.	Time	Source	Destination	Protocol	Length	Info
5925	1.164091847	172.20.7.1	172.20.7.2	TCP	62	21738 → 15104 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1

Figura 21: Pacote TCP do Denial of Service

Através do output do Denial of Service chegamos à vulnerabilidade CVE-2000-0138 :

Current Description

A system has a distributed denial of service (DDOS) attack master, agent, or zombie installed, such as (1) Trinoo, (2) Tribe Flood Network (TFN), (3) Tribe Flood Network 2000 (TFN2K), (4) stacheldraht, (5) mstream, or (6) shaft.


[+View Analysis Description](#)

Severity

CVSS Version 3.x

CVSS Version 2.0

CVSS 2.0 Severity and Metrics:

 **NIST: NVD**

Base Score: 5.0 MEDIUM

Vector: (AV:N/AC:L/Au:N/C:N/I:N/A:P)

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

Figura 22: CVE-2000-0138

3.4 Questão 4

O IDS pode ter um papel vital na segurança da informação no geral ao examinar o tráfego na rede, a fim de detectar e prevenir os acessos não autorizados na mesma, protegendo a mesma da exploração das vulnerabilidades.

Enquanto que o Nessus verifica portas e serviços que possam estar a correr nestas e também o sistema operativo e as associa vulnerabilidades que se encontram presentes em bases de dados, o IDS tira vantagem do tráfego de pacotes TCP para identificar possíveis intrusos em tempo real que tentam aceder à máquina indevidamente alertando quando existe algum comportamento estranho como elevado tráfego de acordo com regras definidas, podendo este, portanto, notificar sem existir um serviço a correr que apresente uma vulnerabilidade o que no Nessus não acontece.

Como o Nessus só verifica os serviços o IDS consegue detetar vulnerabilidades não tanto associadas ao lado aplicacional como *DDOS*, tráfego excessivo por exemplo TCP que pode indicar *scanning*. Com isto um problema significativo são os falsos alarmes que podem ser provocados por algumas regras demasiado genéricas ou tráfego de máquinas autorizadas na rede, que correspondem a legitimar serviços que foram mal classificadas como maliciosos pelo IDS. Reconhecer os alarmes verdadeiros de uma grande quantidade de alarmes é muito complicado e é uma tarefa que consome muito tempo.

3.5 Questão 5

O objetivo desta última questão era solucionar uma vulnerabilidade com um nível *Critical*, outro com nível *Medium* e outro com nível à nossa escolha. Foram selecionadas as seguintes vulnerabilidades, respetivamente:

- Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (unauthenticated check) - *Critical*
- Apache Tomcat AJP Connector Request Injection (Ghostcat) - *High*
- SMB Signing not required - *Medium*

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

De modo a mitigar esta vulnerabilidade, segundo a documentação ² era aconselhável ativar Network Level Authentication, com fim a bloquear os atacantes que tinham como objetivo explorar esta vulnerabilidade.

Com este serviço de autenticação ativo o atacante tem de se autenticar com uma conta que tem realmente acesso à máquina antes de conseguir explorar a vulnerabilidade. Na figura abaixo encontra-se a maneira como ativamos este mecanismo de autenticação.

²Documentação : <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2019-0708>

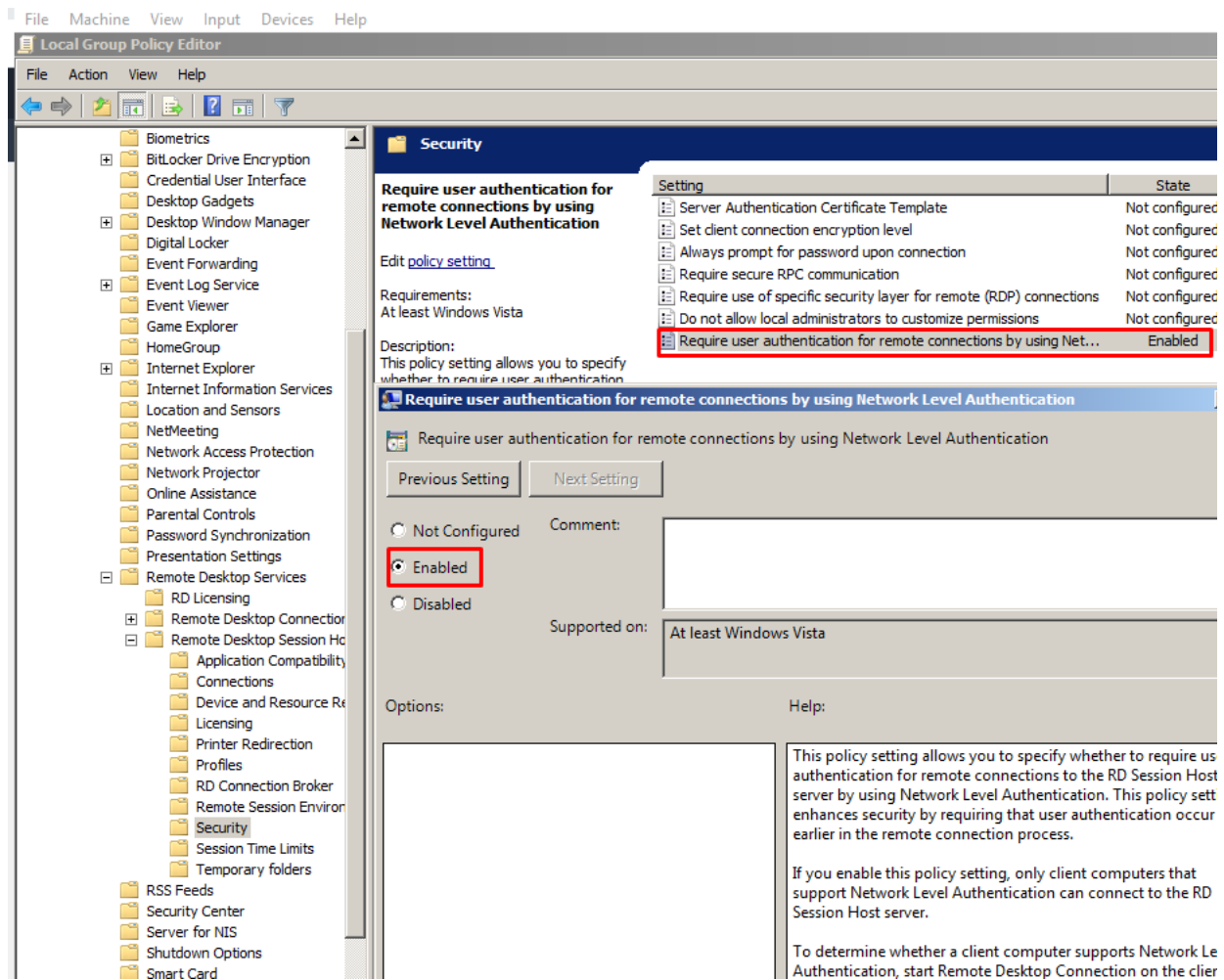


Figura 23: Enable NLA

Após esta alteração podemos ver que essa vulnerabilidade já não foi assinalada pelo Nessus

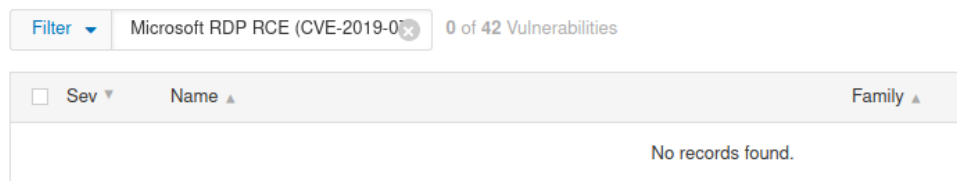


Figura 24: Vulnerabilidade *Microsoft RDP RCE (uncredentialed check)* removida

3.5.2 Apache Tomcat AJP Connector Request Injection (Ghostcat)

Um atacante não autenticado remoto pode explorar esta vulnerabilidade de ler os ficheiros de uma aplicação web de um ser server vulnerável. Em instâncias onde o server vulnerável permite upload de ficheiros, um atacante pode dar upload a código malicioso de JavaServer Pages (JSP).

Filter		ector Request Injection (Ghostcat)	1 of 42 Vulnerabilities	
<input type="checkbox"/>	Sev	Name	Family	Count
<input type="checkbox"/>	HIGH	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1

Figura 25: Vulnerabilidade *Apache Tomcat AJP Connector Request Injection (Ghostcat)*

Uma das maneiras de resolver esta vulnerabilidade é através do uso de credenciais no AJP protocol, uma vez que o *connector* AJP encontra-se por "default" ativado, e como este está ativo sem nenhum mecanismo de segurança ele encontra-se exposto. Ao colocarmos as configurações abaixo força o tomcat a ter um segredo com o conector AJP.

```
<!-- Define an AJP 1.3 Connector on port 8009 -->
<Connector port="8009" protocol="AJP/1.3" redirectPort="8443" address="127.0.0.1" secret="vagrant" />
<!-- An Engine represents the entry point (within Catalina) that processes
every request. The Engine implementation for Tomcat stand alone
analyzes the HTTP headers included with the request, and passes them
on to the appropriate Host (virtual host).
Documentation at /docs/config/engine.html -->
```

Figura 26: server.xml

Como podemos ver, após esta ação, não foi detetada essa vulnerabilidade:

Filter	Apache Tomcat AJP Connector	0 of 40 Vulnerabilities
<input type="checkbox"/> Sev	Name	Family
No records found.		

Figura 27: Vulnerabilidade removida

3.5.3 SMB Signing not required

Nos servers SMB remotos não era necessário a autenticação. Um atacante não autenticado remoto pode explorar isto para conduzir um *man-in-the-middle* ataque contra o SMB server

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 28: Vulnerabilidade *SMB Signing not required*

A solução passa por impor uma mensagem de login na configuração do host. Basta ativar o Digitally Sign Communications ('always')

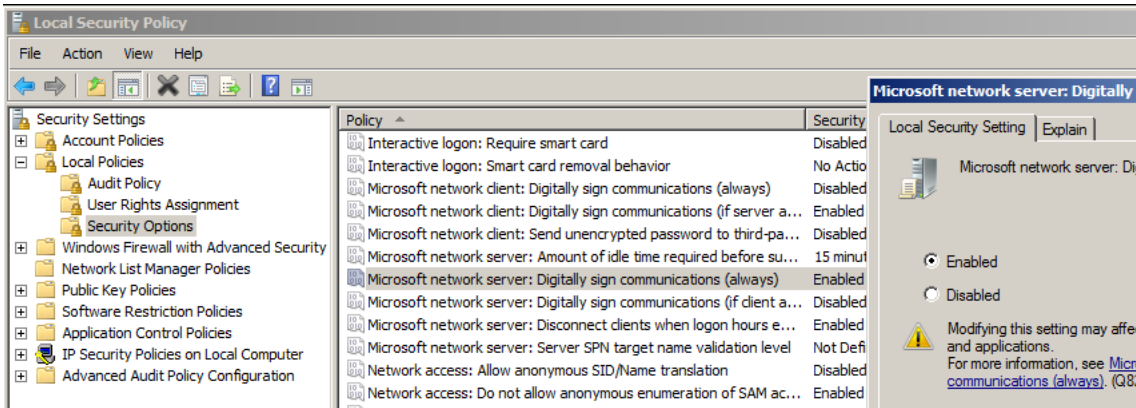


Figura 29: Enable Digitally Sign Communications

Após esta alteração a vulnerabilidade não foi detetada:

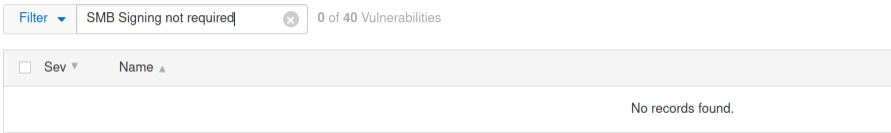


Figura 30: Vulnerabilidade removida

4 Conclusão

Este trabalho permitiu consolidar a matéria lecionada nas aulas da unidade curricular, neste caso *Penetration test* focando especialmente na etapa de *footprinting*. Isto permitiu-nos perceber como estes testes podem ser importantes para empresas/aplicações de modo a identificar as suas vulnerabilidades e ameaças com o objetivo de melhorar a sua segurança .

Além disto, este trabalho ajudou-nos a ter noções mais práticas do como funcionam algumas técnicas de obtenção de informação e ferramentas de *scanning*.