



UNIVERSIDADE DO MINHO

DEPARTAMENTO DE INFORMÁTICA

MESTRADO EM ENGENHARIA INFORMÁTICA

CRİPTOGRAFIA E SEGURANÇA DE INFORMAÇÃO

Tecnologias de Segurança

Trabalho Prático 1

Grupo Nº11

Ariana Lousada (PG47034) Luís Carneiro (PG46541)
Rui Cardoso (PG42849)

27 de março de 2022

Resumo

O presente documento descreve sucintamente a utilização de várias ferramentas de *scanning* assim como a análise de resultados ao longo do primeiro trabalho prático inserido na unidade curricular Tecnologias de Segurança, pertencente ao perfil de Criptografia e Segurança da Informação inserido no Mestrado em Engenharia Informática da Universidade do Minho. Este trabalho prático teve como principal foco o uso de técnicas para coleta passiva de informação como ferramenta de análise da postura de segurança em sistemas e infra-estruturas reais e de técnicas e ferramentas de varredura activa, usadas como estratégia de identificação de vulnerabilidades e fraquezas de um sistema remoto (num ambiente anteriormente configurado).

Conteúdo

1	Parte A	3
1.1	Amazon	3
1.2	Degema	5
2	Parte B	8
2.1	Questão 1	8
2.2	Questão 2	10
2.3	Questão 3	13
2.4	Questão 4	15
2.5	Questão 5	15
3	Referências	19

Lista de Figuras

1.1	Informação da Amazon obtida através da ferramenta Whois	3
1.2	Informação da Amazon obtida através da ferramenta Whois	4
1.3	Excerto da informação da Amazon obtida através da ferramenta Whois	4
1.4	Informação obtida com a utilização da ferramenta Nmap(com a opção -sS) (para descobrir endereços IP e portas utilizadas para comunicações TCP)	5
1.5	Informação obtida com a utilização da ferramenta Nmap(com a opção -O) (consulta de sistemas operativos utilizados por parte da empresa)	5
1.6	Informação obtida com a utilização da ferramenta Nmap(com a opção -sV) (consulta das versões dos serviços associados a portas abertas)	5
1.7	Informação obtida através da ferramenta Whois	6
1.8	Informação obtida através da ferramenta Whois	6
1.9	Informação obtida com a utilização da ferramenta Nmap(com a opção -sV)	7
2.1	Ipconfig do Sistema Metasploitable 3	8
2.2	Serviços utilizados pelo Sistema Metasploitable 3	9
2.3	Informação do <i>scan</i> de <i>Host Discovery</i>	10
2.4	Vulnerabilidades do <i>Network Scan</i> (1)	11
2.5	Vulnerabilidades do <i>Network Scan</i> (2)	11
2.6	Vulnerabilidades do <i>Network Scan</i> (3)	12
2.7	Remediações sugeridas do <i>Network Scan</i> (3)	12
2.8	10 vulnerabilidades mais severas classificadas pelo VPR	13
2.9	Inspeção do pacote do primeiro evento capturado pelo Wireshark	14
2.10	Inspeção do protocolo SNMP no pacote do primeiro evento capturado pelo Wireshark	14
2.11	Inspeção do pacote do segundo evento capturado pelo Wireshark	15
2.12	Inspeção do protocolo TFTP no pacote do segundo evento capturado pelo Wireshark	15
2.13	Exemplo de uma vulnerabilidade crítica classificada pelo Nessus	16
2.14	Exemplo da solução de uma vulnerabilidade crítica classificada pelo Nessus	16
2.15	Exemplo de uma vulnerabilidade média classificada pelo Nessus	17
2.16	Firewall desactivada	17
2.17	Firewall activada	18
2.18	Exemplo de outra vulnerabilidade média classificada pelo Nessus	18

Capítulo 1

Parte A

Como alvo de pesquisa por busca passiva para análise deste trabalho prático escolheu-se como grande corporação a Amazon e como negócio local a hamburgueria Degema. De modo a analisar passivamente estas empresas utilizaram-se ferramentas como o Nmap e Whois. Também se analisaram os *websites* de cada empresa, consultando o tipo de informação exposta como contactos, entidades de funcionários e ofertas de emprego.

1.1 Amazon

Para analisar os sistemas e infraestruturas da Amazon começou-se por analisar o *website* oficial da empresa. A empresa não expõe qualquer informação de funcionários ou de CEO's publicamente, o que ajuda na proteção da própria empresa. Para além disto, apenas são utilizados emails gerais, o que também contribui para uma melhor segurança.

Na secção de ofertas de emprego também não são mencionadas ferramentas em específico que a empresa utiliza, apenas as linguagens de programação. Contudo, existem algumas vagas de emprego que pedem como requisito básico experiência em sistemas Linux/Unix. Com esta informação, um atacante pode tentar atacar a empresa explorando vulnerabilidades próprias desse tipo de sistemas.

De seguida, consultou-se os endereços IP da empresa com a utilização da ferramenta Whois.

Whois Record for Amazon.com

— Domain Profile

Registrant	Hostmaster, Amazon Legal Dept.
Registrant Org	Amazon Technologies, Inc.
Registrant Country	us
Registrar	MarkMonitor, Inc. MarkMonitor Inc. IANA ID: 292 URL: http://www.markmonitor.com Whois Server: whois.markmonitor.com abusecomplaints@markmonitor.com (p) 12083895770

Figura 1.1: Informação da Amazon obtida através da ferramenta Whois



IP Address	99.86.32.31 - 1 other site is hosted on this server
IP Location	 - Washington - Seattle - Amazon.com Inc.
ASN	 AS16509 AMAZON-02, US (registered May 04, 2000)
Domain Status	Registered And Active Website
IP History	473 changes on 473 unique IP addresses over 18 years
Registrar History	2 registrars with 1 drop

Figura 1.2: Informação da Amazon obtida através da ferramenta Whois

```

NetRange: 99.85.128.0 - 99.87.191.255
CIDR: 99.86.0.0/16, 99.85.128.0/17, 99.87.0.0/17, 99.87.128.0/18
NetName: AMAZO-4
NetHandle: NET-99-85-128-0-1
Parent: NET99 (NET-99-0-0-0-0)
NetType: Direct Allocation
OriginAS: AS16509
Organization: Amazon.com, Inc. (AMAZO-4)
RegDate: 2018-01-10
Updated: 2018-01-11
Ref: https://rdap.arin.net/registry/ip/99.85.128.0

OrgName: Amazon.com, Inc.
OrgId: AMAZO-4
Address: Amazon Web Services, Inc.
Address: P.O. Box 81226
City: Seattle
StateProv: WA
PostalCode: 98108-1226
Country: US
RegDate: 2005-09-29
Updated: 2021-09-30
Comment: For details of this service please see
Comment: http://ec2.amazonaws.com
Ref: https://rdap.arin.net/registry/entity/AMAZO-4

OrgRoutingHandle: IPROU3-ARIN
OrgRoutingName: IP Routing
OrgRoutingPhone: +1-206-266-4064
OrgRoutingEmail: aws-routing-poc@amazon.com
OrgRoutingRef: https://rdap.arin.net/registry/entity/IPROU3-ARIN

OrgNOCHandle: AAN01-ARIN
OrgNOCName: Amazon AWS Network Operations
OrgNOCPhone: +1-206-266-4064
OrgNOCEmail: amzn-noc-contact@amazon.com
OrgNOCRef: https://rdap.arin.net/registry/entity/AAN01-ARIN

OrgAbuseHandle: AEAB-ARIN
OrgAbuseName: Amazon EC2 Abuse
OrgAbusePhone: +1-206-266-4064
OrgAbuseEmail: abuse@amazonaws.com
OrgAbuseRef: https://rdap.arin.net/registry/entity/AEAB-ARIN

OrgRoutingHandle: ARMP-ARIN
OrgRoutingName: AWS RPKI Management POC
OrgRoutingPhone: +1-206-266-4064
OrgRoutingEmail: aws-rpki-routing-poc@amazon.com
OrgRoutingRef: https://rdap.arin.net/registry/entity/ARMP-ARIN

```

Figura 1.3: Excerto da informação da Amazon obtida através da ferramenta Whois

Através desta ferramenta foi possível obter a gama dos endereços IP da empresa, assim como a sua localização, serviços de DNS e *nameservers*. A empresa tem no total 6 nameservers próprios e usa como serviço de DNS o MarkMonitor.

De seguida utilizou-se a ferramenta Nmap.

```

(kali㉿kali)-[~]
$ sudo nmap -sS 99.86.32.31
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-19 20:51 EDT
Nmap scan report for server-99-86-32-31.sea19.r.cloudfront.net (99.86.32.31)
Host is up (0.021s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
Nmap done: 1 IP address (1 host up) scanned in 16.12 seconds

```

Figura 1.4: Informação obtida com a utilização da ferramenta Nmap (com a opção -sS) (para descobrir endereços IP e portas utilizadas para comunicações TCP)

```

(kali㉿kali)-[~]
$ sudo nmap -O 99.86.32.31
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-19 20:54 EDT
Nmap scan report for server-99-86-32-31.sea19.r.cloudfront.net (99.86.32.31)
Host is up (0.10s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
Warning: OSscan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (98%), QEMU (92%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (98%), QEMU user mode network gateway (92%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.41 seconds

```

Figura 1.5: Informação obtida com a utilização da ferramenta Nmap (com a opção -O) (consulta de sistemas operativos utilizados por parte da empresa)

```

(kali㉿kali)-[~]
$ sudo nmap -sV 99.86.32.31
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-19 20:52 EDT
Nmap scan report for server-99-86-32-31.sea19.r.cloudfront.net (99.86.32.31)
Host is up (0.021s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Amazon CloudFront httpd
443/tcp   open  ssl/http  Amazon CloudFront httpd
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 32.14 seconds

```

Figura 1.6: Informação obtida com a utilização da ferramenta Nmap (com a opção -sV) (consulta das versões dos serviços associados a portas abertas)

Analisando as figuras anteriores, viu-se que não é possível obter qualquer tipo de informação através da ferramenta Nmap. É possível que a empresa implemente algum mecanismo de defesa contra esta ferramenta que impossibilite a sua utilização.

Uma vez que a empresa em geral tem boas táticas de segurança implementadas, as únicas implementações adicionais seriam utilizar o *whois privacy* (de modo a não ser possível obter qualquer tipo de informação através da ferramenta Whois) e remover a referência a sistemas Unix das ofertas de emprego.

1.2 Degema

Para analisar o negócio local escolhido, começou-se por analisar o *website* da hamburgueria. Tal como na Amazon, não existem quaisquer contactos expostos publicamente.

Como anteriormente, utilizou-se em primeiro lugar a ferramenta Whois.

— Domain Profile

Registrar Status	taken	
Name Servers	NS1.PTSERVIDOR.NET (has 6,879 domains) NS2.PTSERVIDOR.NET (has 6,879 domains) NS3.PTSERVIDOR.NET (has 6,879 domains)	↷
Tech Contact	—	
IP Address	185.32.188.15 - 475 other sites hosted on this server	↷
IP Location	🇵🇹 - Lisboa - Lisboa - Sampling Line Lda - Ptservidor	
ASN	🇵🇹 AS62416 PTSERVIDOR, PT (registered Sep 27, 2013)	
Hosting History	3 changes on 4 unique name servers over 9 years	↷

— Website

Figura 1.7: Informação obtida através da ferramenta Whois

```
% Information related to '185.32.188.0 - 185.32.188.255'
% Abuse contact for '185.32.188.0 - 185.32.188.255' is 'abuse@ptservidor.pt'

inetnum:        185.32.188.0 - 185.32.188.255
netname:        PT-PTSERVIDOR
descr:          Sampling Line, Lda - PTServidor
descr:          *****
descr:          * In case of issues related with SPAM, DDoS, portscans
descr:          * or others, feel free to contact us with relevant info:
descr:          * abuse@ptservidor.pt
descr:          *****
descr:          country:      PT
admin-c:        SLSI-RIPE
tech-c:         SLSI-RIPE
status:         ASSIGNED PA
mnt-by:         PTSERVIDOR-MNT
mnt-lower:      PTSERVIDOR-MNT
mnt-domains:    PTSERVIDOR-MNT
mnt-routes:     PTSERVIDOR-MNT
created:        2014-01-29T18:21:58Z
last-modified:  2014-01-29T18:21:58Z
source:        RIPE # Filtered

role:           Sampling Line Lda
address:        Av. Amalia Rodrigues N6-D
address:        2675-432 Odivelas
address:        Portugal
phone:          +351 21 4099802
phone:          +351 92 9258249
admin-c:        AL11183-RIPE
admin-c:        FE2447-RIPE
tech-c:         AL11183-RIPE
tech-c:         FE2447-RIPE
abuse-mailbox:  abuse@ptservidor.pt
nic-hdl:        SLSI-RIPE
mnt-by:         PTSERVIDOR-MNT
created:        2014-01-29T12:37:27Z
last-modified:  2017-09-20T14:45:49Z
source:        RIPE # Filtered

% Information related to '185.32.188.0/24AS62416'

route:          185.32.188.0/24
descr:          Sampling Line, Lda - PTServidor
origin:         AS62416
mnt-by:         PTSERVIDOR-MNT
created:        2019-12-31T12:44:44Z
last-modified:  2019-12-31T12:44:44Z
source:        RIPE
```

Figura 1.8: Informação obtida através da ferramenta Whois

Com esta ferramenta podemos obter o endereço IP, assim como a sua localização(Lisboa, Portugal).

Este negócio tem 3 *nameservers* próprios mas não usa qualquer serviço de DNS ou registrar.

De seguida, utilizou-se a ferramenta Nmap com a opção `-sV`, de modo a consultar as versões dos serviços associados.

```
(kali@kali)-[~]
$ sudo nmap -sV 185.32.188.15
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-19 18:36 EDT
Nmap scan report for stargate.ptservidor.net (185.32.188.15)
Host is up (0.0094s latency).
Not shown: 989 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Pure-FTPd
25/tcp    open  smtp?
53/tcp    open  domain   PowerDNS Authoritative Server 4.4.1
80/tcp    open  http     nginx
110/tcp   open  pop3     Dovecot pop3d
143/tcp   open  imap     Dovecot imapd
443/tcp   open  ssl/http nginx
465/tcp   open  ssl/smtp Exim smtpd 4.94.2
587/tcp   open  smtp     Exim smtpd 4.94.2
993/tcp   open  ssl/imap Dovecot imapd
995/tcp   open  ssl/pop3 Dovecot pop3d

Service detection performed. Please report any incorrect results at https://nmap.org/submi
t/ .
Nmap done: 1 IP address (1 host up) scanned in 171.87 seconds
```

Figura 1.9: Informação obtida com a utilização da ferramenta Nmap (com a opção `-sV`)

Existem algumas estratégias de baixo custo que permitem ocultar informações relevantes dos métodos de pesquisa passiva que o negócio Degema poderia utilizar:

- Utilizar um VPN para esconder o endereço IP do servidor;
- Utilizar o *whois Privacy* já anteriormente mencionado.
- Utilizar mecanismos de defesa contra a utilização da ferramenta Nmap. Com a figura 1.9 podem-se consultar os vários serviços utilizados pelo negócio. Isto pode possibilitar ataques com alvo nesses serviços.
- Evitar colocar informações sensíveis, como nomes verdadeiros e emails pessoais. O mais aconselhado será utilizar emails gerais.

Capítulo 2

Parte B

2.1 Questão 1

Selecione um conjunto de ferramentas e técnicas de varredura activa para identificar e detalhar vulnerabilidades e fraquezas para as quais o Sistema Metasploitable 3 está exposto. A sua resposta deverá listar os serviços a correr neste sistema e as vulnerabilidades e/ou fraquezas relacionados a cada um. Para os serviços com diferentes vulnerabilidades, escolha a mais recente ou a mais grave.

Na máquina que se utilizou para elaborar a resposta a esta questão, alterou-se a configuração ip do sistema Metasploitable 3 para a seguinte:

```
PS C:\Users\vagrant> netsh int ip set address "local area connection" static 172.20.11.2 255.255.255.0 172.20.11.1
PS C:\Users\vagrant> ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::c84e:4043:ee76:3786%11
    IPv4 Address. . . . . : 172.20.11.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 172.20.11.1

Tunnel adapter isatap.{2AC9D7FD-F063-48EA-8738-110021736847}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter Local Area Connection* 9:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 
PS C:\Users\vagrant> _
```

Figura 2.1: Ipconfig do Sistema Metasploitable 3

De modo a ser possível consultar os serviços utilizados pelo sistema, utilizou-se a ferramenta Nmap com a opção `-sV`.

```

(kali@kali)-[~]
$ sudo nmap -sV 172.20.11.2
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-21 14:31 EDT
Nmap scan report for endpriv101.scom3.uminho.pt (172.20.11.2)
Host is up (0.0058s latency).
Not shown: 980 filtered tcp ports (no-response)
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  ssl/ms-wbt-server?
4848/tcp   open  ssl/http       Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
7676/tcp   open  java-message-service
8009/tcp   open  ajp13          Apache Jserv (Protocol v1.3)
8022/tcp   open  http           Apache Tomcat/Coyote JSP engine 1.1
8031/tcp   open  ssl/unknown
8080/tcp   open  http           Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
8181/tcp   open  ssl/http       Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
8383/tcp   open  http           Apache httpd
8443/tcp   open  ssl/https-alt?
9200/tcp   open  wap-wsp?
49152/tcp open  msrpc          Microsoft Windows RPC
49153/tcp open  msrpc          Microsoft Windows RPC
49154/tcp open  msrpc          Microsoft Windows RPC
49157/tcp open  unknown

```

Figura 2.2: Serviços utilizados pelo Sistema Metasploitable 3

De modo a detetar as vulnerabilidades mais graves e/ou recentes, recorreu-se ao CVE, pesquisando por cada um destes serviços em particular.

ssh

A vulnerabilidade mais recente deste serviço(CVE-2011-0766) está relacionada com o gerador aleatório na aplicação Crypto nas versões anteriores à 2.0.2.2. Esta vulnerabilidade tem um score CVSS de 7.8.

O gerador aleatório utilizava *seeds* previsíveis, o que permitia a um atacante adivinhar mais facilmente o host DSA e as chaves SSH.

msrpc

A vulnerabilidade mais recente deste serviço(CVE-2018-8407) foi detetada em 2020 e expõe informação devido à inicialização incorreta do Kernel Remote Procedure Call Provider. Esta vulnerabilidade tem um score CVSS de 2.1.

netbios-ssn

A vulnerabilidade mais recente deste serviço(CVE-2017-0174) foi detetada em 2017 e torna o sistema vulnerável a ataques de negação de serviço quando pacotes NetBIOS são tratados de maneira imprópria.

microsoft-ds

A vulnerabilidade mais recente deste serviço(CVE-2002-0597) foi detetada em 2002. Com esta vulnerabilidade o serviço LANMAN permite ataques de negação de serviço através de exaustão de CPU/-memória através do envio de data mal construída para o microsoft-ds. Esta vulnerabilidade tem um score CVSS de 5.0.

mysql

A vulnerabilidade mais recente deste serviço(CVE-2022-21378) foi detetada em 2022. Esta vulnerabilidade pode ser facilmente explorada por atacantes e atribui-lhes permissões de nível significativo para vários protocolos que podem comprometer o servidor MySQL. Alguns ataques podem ter como consequências *shutdown* repetitivo do servidor(DoS) assim como alteração não autorizada de dados.

Esta vulnerabilidade tem um score CVSS de 5.5.

java-message-service

A vulnerabilidade mais recente deste serviço(CVE-2007-1944) foi detetada em 2007. Esta vulnerabilidade afeta as versões anteriores à 6.1.0.7 do JMS e permite ataques de negação de serviço através de vetores desconhecidos.

Esta vulnerabilidade tem um score CVSS de 5.0.

ajp13

A vulnerabilidade mais recente deste serviço(CVE-2011-3190) foi detetada em 2011.

Esta vulnerabilidade pode permitir em algumas implementações do conetor do protocolo AJP no Apache Tomcat *spoofing* de *requests* AJP, *bypass authentication* e a obtenção de informação sensível.

Esta vulnerabilidade tem um score CVSS de 7.5.

http

A vulnerabilidade mais recente deste serviço(CVE-2022-23943) foi detetada em 2022.

Esta vulnerabilidade consiste numa possibilidade de escrita *out-of-bounds*. Isto pode permitir a um atacante reescrever memória da *heap* com dados à sua escolha.

Esta vulnerabilidade tem um score CVSS de 7.5.

2.2 Questão 2

Discuta os resultados globais do processo de varredura activa ao Sistema Mestasploitable 3. Avalie também as diferenças entre o resultado do sistema automático de identificação de vulnerabilidades e o resultado que obteve no item Q1 da Parte B deste enunciado.

Para a varredura ativa foram feitos dois testes, o *Host Discovery*, que determina as portas abertas de um ou mais hosts, e o *Basic Network Scan*, que faz um *scan* genérico ao sistema.

O teste de *Host Discovery* verificou que, através de uma *ARP who-is query*, o *remote host* estava disponível, com o endereço de hardware 08:00:27:a4:cd:9b. De seguida, as portas 135, 139, 445, 49152, 49153, 49154, 49162, 49192 e 49198 iriam ser testadas. No entanto, por motivos desconhecidos, como é possível ver na figura 2.3, o *port scanner* não estava ativado.

```
Information about this scan :

Nessus version : 10.1.1
Nessus build : X20061
Plugin feed version : 202203242013
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : ubuntu1110-x86-64
Scan type : Normal
Scan name : Teste scan Metasploit 172.20.11.2
Scan policy used : Host Discovery
Scanner IP : 172.20.11.1

WARNING : No port scanner was enabled during the scan. This may
lead to incomplete results.

Port range : default
Ping RTT : 165.064 ms
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 256
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2022/3/25 15:30 WET
Scan duration : 20 sec
```

Figura 2.3: Informação do *scan* de *Host Discovery*

Já o *Basic Network Scan* encontrou um total de 212 vulnerabilidades isoladas, sendo que 161 eram meramente informativas, 4 tinham gravidade baixa, 28 média, 11 alta e 8 eram críticas. Quando agrupadas por nome, foram encontradas 50. Foram sugeridas 5 remediações e o *Vulnerability Priority Rating System* classificou o nível de ameaça como crítico, sendo que 9.8 era o *score* mais alto.

<input type="checkbox"/> Sev	Score	Name	Family	Count	
<input type="checkbox"/> CRITICAL	9.8	Elasticsearch Transport Protocol Unspecified Remote Co...	Databases	1	
<input type="checkbox"/> MIXED	...	Microsoft Windows (Multiple Issues)	Windows	8	
<input type="checkbox"/> MIXED	...	Zohocorp Manageengine Desktop Central (Multiple...	CGI abuses	6	
<input type="checkbox"/> MIXED	...	Elasticsearch (Multiple Issues)	CGI abuses	4	
<input type="checkbox"/> MIXED	...	Apache Tomcat (Multiple Issues)	Web Servers	2	
<input type="checkbox"/> MIXED	...	SSL (Multiple Issues)	General	41	
<input type="checkbox"/> MIXED	...	IETF Md5 (Multiple Issues)	General	3	
<input type="checkbox"/> HIGH	...	Oracle Glassfish Server (Multiple Issues)	CGI abuses	2	
<input type="checkbox"/> MEDIUM	5.1 *	Microsoft Windows Remote Desktop Protocol Server Ma...	Windows	1	
<input type="checkbox"/> MIXED	...	TLS (Multiple Issues)	Service detection	11	
<input type="checkbox"/> MIXED	...	Microsoft Windows (Multiple Issues)	Misc.	4	
<input type="checkbox"/> MIXED	...	SSL (Multiple Issues)	Service detection	2	
<input type="checkbox"/> LOW	3.7	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Misc.	3	
<input type="checkbox"/> LOW	2.6 *	Terminal Services Encryption Level is not FIPS-140 Comp...	Misc.	1	

Figura 2.4: Vulnerabilidades do *Network Scan* (1)

<input type="checkbox"/> INFO	...	HTTP (Multiple Issues)	Web Servers	22	
<input type="checkbox"/> INFO	...	TLS (Multiple Issues)	General	10	
<input type="checkbox"/> INFO	...	SMB (Multiple Issues)	Windows	7	
<input type="checkbox"/> INFO	...	Oracle Glassfish Server (Multiple Issues)	Web Servers	4	
<input type="checkbox"/> INFO	...	SSH (Multiple Issues)	General	2	
<input type="checkbox"/> INFO	...	SSH (Multiple Issues)	Misc.	2	
<input type="checkbox"/> INFO	...	SSH (Multiple Issues)	Service detection	2	
<input type="checkbox"/> INFO	...	Web Server (Multiple Issues)	Web Servers	2	
<input type="checkbox"/> INFO		Nessus SYN scanner	Port scanners	23	
<input type="checkbox"/> INFO		Service Detection	Service detection	14	
<input type="checkbox"/> INFO		DCE Services Enumeration	Windows	8	
<input type="checkbox"/> INFO		Unknown Service Detection: Banner Retrieval	Service detection	3	
<input type="checkbox"/> INFO		AJP Connector Detection	Service detection	1	
<input type="checkbox"/> INFO		Apache HTTP Server Version	Web Servers	1	
<input type="checkbox"/> INFO		Common Platform Enumeration (CPE)	General	1	

Figura 2.5: Vulnerabilidades do *Network Scan* (2)

<input type="checkbox"/>	INFO	Device Type	General	1	🔄	✎
<input type="checkbox"/>	INFO	Ethernet Card Manufacturer Detection	Misc.	1	🔄	✎
<input type="checkbox"/>	INFO	Ethernet MAC Addresses	General	1	🔄	✎
<input type="checkbox"/>	INFO	ICMP Timestamp Request Remote Date Disclosure	General	1	🔄	✎
<input type="checkbox"/>	INFO	Link-Local Multicast Name Resolution (LLMNR) Detection	Service detection	1	🔄	✎
<input type="checkbox"/>	INFO	Nessus Scan Information	Settings	1	🔄	✎
<input type="checkbox"/>	INFO	Nessus Windows Scan Not Performed with Admin Privile...	Settings	1	🔄	✎
<input type="checkbox"/>	INFO	NetBIOS Multiple IP Address Enumeration	Windows	1	🔄	✎
<input type="checkbox"/>	INFO	OpenSSL Detection	Service detection	1	🔄	✎
<input type="checkbox"/>	INFO	OS Identification	General	1	🔄	✎
<input type="checkbox"/>	INFO	OS Security Patch Assessment Not Available	Settings	1	🔄	✎
<input type="checkbox"/>	INFO	Patch Report	General	1	🔄	✎
<input type="checkbox"/>	INFO	RDP Screenshot	General	1	🔄	✎
<input type="checkbox"/>	INFO	Server Message Block (SMB) Protocol Version 1 Enabled ...	Misc.	1	🔄	✎
<input type="checkbox"/>	INFO	Service Detection (GET request)	Service detection	1	🔄	✎

Figura 2.6: Vulnerabilidades do *Network Scan* (3)

Action	Vulns •	Hosts
ManageEngine Desktop Central 9 < Build 92027 Multiple Vulnerabilities: Upgrade to ManageEngine Desktop Central version 9 build 92027 or later.	3	1
Apache Tomcat AJP Connector Request Injection (Ghostcat): 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.	2	1
Elasticsearch ESA-2015-06: Users should upgrade to 1.6.1 or 1.7.0. Alternately, ensure that only trusted applications have access to the transport protocol port.	2	1
Elasticsearch Transport Protocol Unspecified Remote Code Execution: Users should upgrade to 1.6.1 or 1.7.0. Alternately, ensure that only trusted applications have access to the transport protocol port	2	1
Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check): Microsoft has released a set of patches for Windows XP, 2003, 2008, 7, and 2008 R2.	2	1

Figura 2.7: Remediações sugeridas do *Network Scan* (3)



Assessed Threat Level: **Critical**

The following vulnerabilities are ranked by Tenable's patented Vulnerability Priority Rating (VPR) system. The findings listed below detail the top ten vulnerabilities, providing a prioritized view to help guide remediation to effectively reduce risk. Click on each finding to show further details along with the impacted hosts. To learn more about Tenable's VPR scoring system, see [Predictive Prioritization](#).

VPR Severity	Name	Reasons	VPR Score	Hosts
CRITICAL	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETER...	Security Research	9.8	1
CRITICAL	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)	Social Media; Security Research...	9.8	1
CRITICAL	Elasticsearch 'source' Parameter RCE	Security Research	9.7	1
CRITICAL	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Social Media; Mainstream Medi...	9.6	1
CRITICAL	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Executi...	Security Research	9.5	1
HIGH	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992...	No recorded events	7.4	1
HIGH	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution ...	No recorded events	7.3	1
HIGH	ManageEngine Desktop Central 8 / 9 < Build 91100 Multiple RCE	No recorded events	7.3	1
MEDIUM	Elasticsearch Transport Protocol Unspecified Remote Code Execution	No recorded events	6.7	1
MEDIUM	Elasticsearch ESA-2015-06	No recorded events	6.7	1

Figura 2.8: 10 vulnerabilidades mais severas classificadas pelo VPR

Em relação às diferenças encontradas, ao pesquisar pelo CVE não foram encontradas nenhuma das vulnerabilidades específicas mencionadas na questão 1.

Foram, no entanto, encontradas outras vulnerabilidades para alguns dos serviços mencionados: 6 informativas para o ssh, 3 informativas e 1 alta para o netbios-ssn (caso seja usado SSN por cima do NetBIOS API) e 15 informativas para o http.

Finalmente, houveram algumas vulnerabilidades apenas descobertas através do Nessus. As mais graves, com uma severidade crítica, afetavam o Microsoft Windows, o Elastic Search e o Apache Tomcat.

2.3 Questão 3

Examine o output do IDS e escolha dois eventos identificados como tráfego anômalo. Para cada evento escolhido, identifique o respetivo tráfego capturado via Analisador de tráfego e o descreva. Se possível, inclua o CVE da vulnerabilidade e o método de identificação usado pelo scanner.

Ambos os eventos identificados foram detetados na fase de *Network Scanning*.

O primeiro evento consiste numa tentativa de acesso com um pacote SNMP a estatísticas importantes da rede guardadas no dispositivo. O pedido SNMP consiste nas credenciais do utilizador e no pedido SNMP GET. A *community string* é utilizada para autenticar o utilizador. Caso a predefinida, que é a *public*, não tiver sido mudada, a informação chave da rede fica exposta.

O CVE da vulnerabilidade é o CVE-2002-0012, que permite a atacantes remotos que causem um *denial of service* ou ganhem privilégios via SNMPv1 *trap holding*.

O método de identificação foi baseado em regras, visto ter associado o evento à vulnerabilidade já conhecida.

```
[**] [1:1411:10] SNMP public access udp [**]
[Classification: Attempted Information Leak] [Priority: 2]
03/25-15:41:38.016452 172.20.11.1:44038 -> 172.20.11.2:161
UDP TTL:64 TOS:0x0 ID:31394 IpLen:20 DgmLen:71 DF
Len: 43
[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://cve.mitre.org/cgi-bin/cvename.cgi?name
=1999-0517] [Xref => http://www.securityfocus.com/bid/4089] [Xref => http://www.securityfocus
.com/bid/4088] [Xref => http://www.securityfocus.com/bid/2112]
```

No.	Time	Source	Destination	Protocol	Length	Info
218	7.917020093	172.20.11.1	172.20.11.2	SNMP	85	get-next-request 1.3.6.1.2.1.1.1.0

Frame 218: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface vboxnet0, id 0

> Interface id: 0 (vboxnet0)

Encapsulation type: Ethernet (1)

Arrival Time: Mar 25, 2022 15:41:38.016452883 WET

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1648222898.016452883 seconds

[Time delta from previous captured frame: 0.000922663 seconds]

[Time delta from previous displayed frame: 0.000922663 seconds]

[Time since reference or first frame: 7.917020093 seconds]

Frame Number: 218

Frame Length: 85 bytes (680 bits)

Capture Length: 85 bytes (680 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:udp:snmp]

[Coloring Rule Name: UDP]

[Coloring Rule String: udp]

> Ethernet II, Src: 0a:00:27:00:00:00 (0a:00:27:00:00:00), Dst: PcsCompu_a4:cd:9b (08:00:27:a4:cd:9b)

> Internet Protocol Version 4, Src: 172.20.11.1, Dst: 172.20.11.2

> User Datagram Protocol, Src Port: 44038, Dst Port: 161

0000	08 00 27 a4 cd 9b 0a 00 27 00 00 00 08 00 45 00E..
0010	00 47 7a a2 40 00 00 11 51 d8 ac 14 0b 01 ac 14	Gz@@.Q.....
0020	0b 02 ac 06 00 a1 00 33 3f 3c 30 29 02 01 01 043?<0)....
0030	06 70 75 62 6c 69 63 a1 1c 02 04 40 c6 8e 11 02	..public....@....
0040	01 00 02 01 00 30 0e 30 0c 06 08 2b 06 01 02 010.0.....
0050	01 01 00 05 00

Figura 2.9: Inspeção do pacote do primeiro evento capturado pelo Wireshark

Simple Network Management Protocol
version: v2c (1)
community: public
data: get-next-request (1)
get-next-request
request-id: 1086754321
error-status: noError (0)
error-index: 0
variable-bindings: 1 item
1.3.6.1.2.1.1.1.0: Value (Null)
Object Name: 1.3.6.1.2.1.1.1.0 (iso.3.6.1.2.1.1.1.0)
Value (Null)

Figura 2.10: Inspeção do protocolo SNMP no pacote do primeiro evento capturado pelo Wireshark

No segundo evento, o Snort avisa que o pedido Get TFTP pode ser malicioso. Para contextualizar, o TFTP é um protocolo simples de transferência de arquivos. É normalmente usado para carregar as configurações para routers, ou até para situações do tipo *boot-from-network*, que permite que um sistema faça boot a partir da rede em vez do disco local.

O Nessus não apresenta o CVE deste evento, até porque nem tem a certeza se o pedido é malicioso ou não.

O método de identificação foi baseado em rede, visto que foi identificada uma atividade suspeita na interface sujeita à monitorização.

```

[**] [1:1444:3] TFTP Get [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
03/25-15:45:29.059213 172.20.11.1:35269 -> 172.20.11.2:69
UDP TTL:64 TOS:0x0 ID:54500 IpLen:20 DgmLen:56 DF
Len: 28

```


No.	Time	Source	Destination	Protocol	Length	Info
14721	238.959780320	172.20.11.1	172.20.11.2	TFTP	70	Read Request, File: nessus1799060112, Transfer type: netascii
Frame 14721: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface vboxnet0, id 0 > Interface id: 0 (vboxnet0) - Encapsulation type: Ethernet (1) - Arrival Time: Mar 25, 2022 15:45:29.059213110 WET - [Time shift for this packet: 0.000000000 seconds] - Epoch Time: 1648223129.059213110 seconds - [Time delta from previous captured frame: 1.166381040 seconds] - [Time delta from previous displayed frame: 1.166381040 seconds] - [Time since reference or first frame: 238.959780320 seconds] - Frame Number: 14721 - Frame Length: 70 bytes (560 bits) - Capture Length: 70 bytes (560 bits) - [Frame is marked: False] - [Frame is ignored: False] - [Protocols in frame: eth:ethertype:ip:udp:tftp] - [Coloring Rule Name: UDP] - [Coloring Rule String: udp] > Ethernet II, Src: 0a:00:27:00:00:00 (0a:00:27:00:00:00), Dst: PcsCompu_a4:cd:9b (08:00:27:a4:cd:9b) > Internet Protocol Version 4, Src: 172.20.11.1, Dst: 172.20.11.2 > User Datagram Protocol, Src Port: 35269, Dst Port: 69 > Trivial File Transfer Protocol						

Figura 2.11: Inspeção do pacote do segundo evento capturado pelo Wireshark

Trivial File Transfer Protocol
- Opcode: Read Request (1)
- Source File: nessus1799060112
- Type: netascii

Figura 2.12: Inspeção do protocolo TFTP no pacote do segundo evento capturado pelo Wireshark

2.4 Questão 4

Observe que algumas notificações do IDS não possuem vulnerabilidade correspondente no relatório do Scanner de vulnerabilidades. Apresente e discuta as possíveis razões para estas diferenças.

Isto deve-se ao facto de o IDS e o scanner de vulnerabilidades procurarem vulnerabilidades de modos diferentes.

O scanner de vulnerabilidade é uma ferramenta automática que analisa determinado sistema activamente à procura de fraquezas.

O IDS analisa o tráfico da rede de um host ou uma infraestrutura de rede tentando encontrar actividades anormais. Fá-lo através de vários métodos como detectores de anomalias, detectores baseados em regras e baseados em assinaturas. Estes têm de ser actualizados com frequência.

Cada um têm as suas vantagens e desvantagens: o IDS, dependendo do tipo de configuração, pode ter falsos positivos, mas também pode tentar descobrir ataques novos ainda não conhecidos e usados pelo scanner de vulnerabilidades. Para além disto o scanner de vulnerabilidades também pode acusar falsos positivos.

Tendo isto em conta é normal que possam existir diferenças nas notificações de ambos os métodos sendo o ideal usar uma combinação dos dois.

2.5 Questão 5

Escolha três vulnerabilidades identificadas pelo Scanner de vulnerabilidades, sendo, pelo menos, uma classificada como High/Critical e uma classificada como Medium. Pesquise a documentação referente às formas de corrigir a fonte do problema e efetue os procedimentos necessários para tal. Ao final dos procedimentos escolhidos para cada vulnerabilidade, execute uma nova varredura para garantir que estas já não são identificadas. Discuta a solução dada e inclua os ficheiros resultantes da varredura antes e depois das respectivas correções.

Grande parte das vulnerabilidades encontradas no sistema devem-se ao facto de este estar desactualizado desde 2008.

Uma actualização do sistema, como recomendado em quase todas as soluções do Nessus, resolveria as vulnerabilidades.

Na seguinte imagem vê-se mais concretamente uma vulnerabilidade classificada como *critical*:



Figura 2.13: Exemplo de uma vulnerabilidade crítica classificada pelo Nessus

E a solução sugerida pelo Nessus:

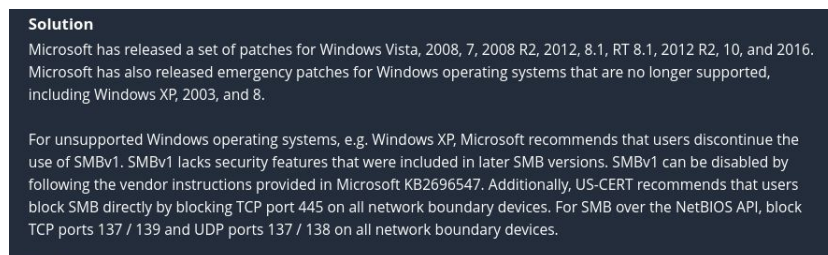


Figura 2.14: Exemplo da solução de uma vulnerabilidade crítica classificada pelo Nessus

Esta vulnerabilidade permite a execução remota de código através do SMBv1.

A recomendação do Nessus é actualizar o sistema operativo. No entanto, como o sistema não tem uma licença activa do Windows, isto é impossível. Também recomenda bloquear as portas TCP 445, 137/139 e UDP 137/138.

A máquina tem a Firewall do Windows desactivada: após a ativação da mesma e voltando a correr o scan com o Nessus a vulnerabilidade desaparece.

Um exemplo de uma vulnerabilidade do tipo médio é a seguinte:



Figura 2.15: Exemplo de uma vulnerabilidade média classificada pelo Nessus

Esta vulnerabilidade encontra-se no uso do cliente de RDP e permite a um atacante obter informação sensível como passwords, através de um ataque *man-in-the-middle*.

Uma das soluções propostas pelo Nessus é forçar o uso de SSL e/ou permitir uma conexão apenas de computadores com autenticação de rede.

Isto também pode ser resolvido re-activando a Firewall do Windows.

Para activar a Firewall do Windows apenas é necessário abrir as definições de Firewall e seleccionar a opção 'Utilizar definições recomendadas'.

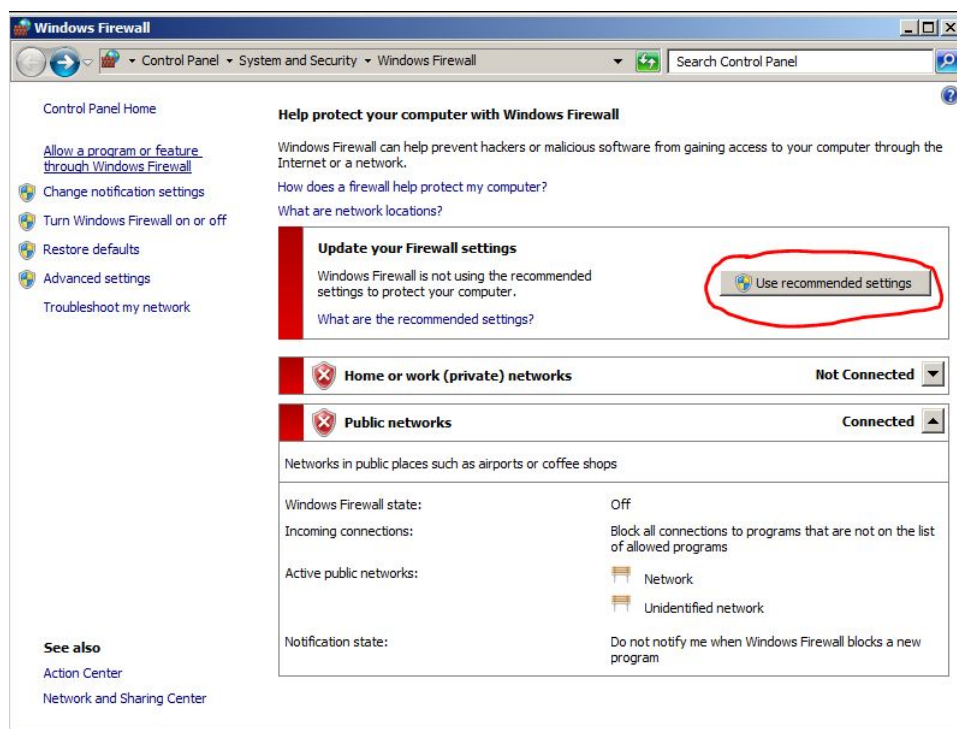


Figura 2.16: Firewall desactivada

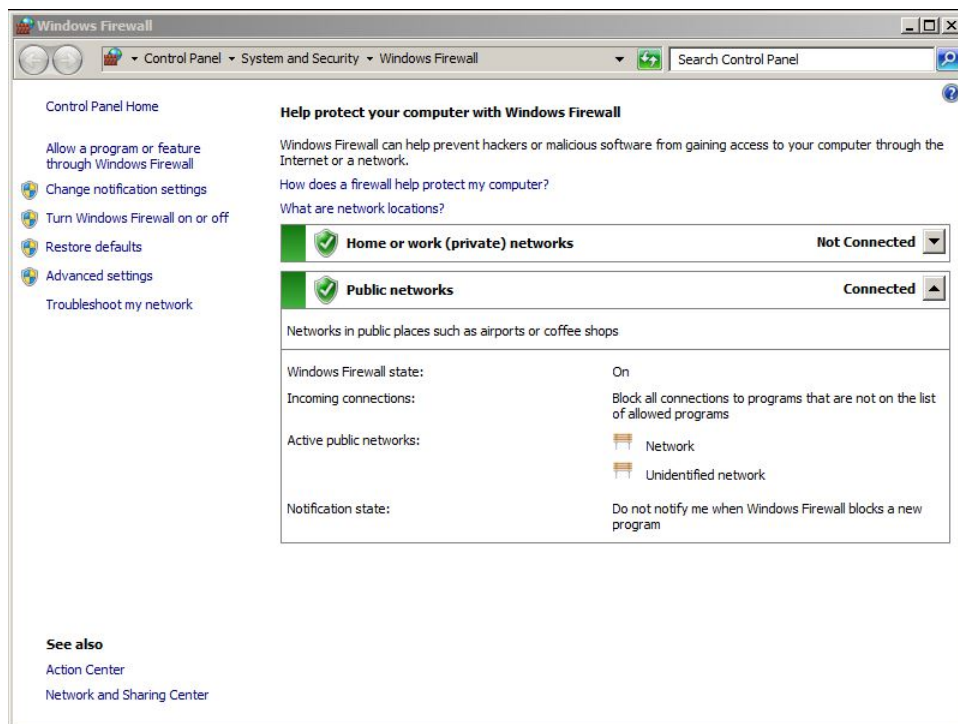


Figura 2.17: Firewall activada

Outro exemplo de uma vulnerabilidade do tipo médio é:

MEDIUM
TLS Version 1.0 Protocol Detection

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

See Also

<https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00>

Figura 2.18: Exemplo de outra vulnerabilidade média classificada pelo Nessus

A tecnologia TLS 1.0 tem um número elevado de vulnerabilidades criptográficas e não deve ser usada. A solução recomendada é desactivar o suporte de TLS 1.0 e activar o suporte de TLS 1.2 e 1.3.

Isto pode ser feito seguindo o seguinte tutorial: <https://windowsreport.com/windows-server-enable-tls/>

Capítulo 3

Referências

- Parte A

- https://www.amazon.jobs/en/search?base_query=software&loc_query=&latitude=&longitude=&loc_group_id=&invalid_location=false&country=&city=®ion=&county=
- <https://whois.domaintools.com/amazon.com>

- Parte B

- Questão 1

- * https://www.cvedetails.com/vulnerability-list/vendor_id-120/product_id-202/SSH-SSH.html
- * <https://www.cvedetails.com/cve/CVE-2011-0766/>
- * <https://www.cvedetails.com/bugtraq-bid/105794/Microsoft-Windows-MSRPC-CVE-2018-8407-Local-Information-Disc.html>
- * <https://www.cvedetails.com/cve/CVE-2017-0174/>
- * <https://www.cvedetails.com/cve/CVE-2002-0597/>
- * <https://www.cvedetails.com/cve/CVE-2022-21378/>
- * <https://www.cvedetails.com/cve/CVE-2007-1944/>
- * <https://www.cvedetails.com/cve/CVE-2011-3190/>
- * <https://www.cvedetails.com/cve/CVE-2022-23943/>

- Questão 3

- * <https://www.dnsstuff.com/snmp-community-string#what-is-an-snmp-community-string>
- * <https://seclists.org/snort/2003/q1/2822>
- * <https://cve.mitre.org/cgi-bin/cvename.cgi?name=2002-0012>
- * <https://seclists.org/snort/2003/q1/2708>
- * <https://www.minitool.com/backup-tips/boot-from-lan.html>