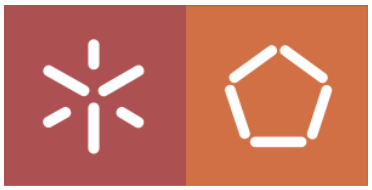


Universidade do Minho
Escola de Engenharia

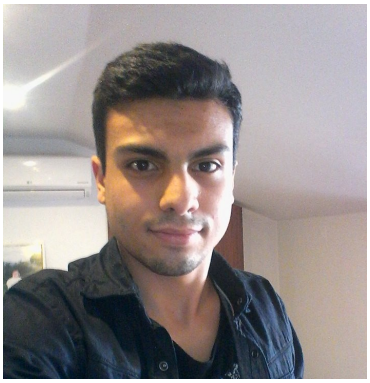
Universidade do Minho
Mestrado Integrado em Engenharia Informática

Tecnologia de Segurança

Trabalho prático 2

22 Dezembro 2020

Ana Margarida Campos
(A85166)



Nuno Pereira
(PG42846)

Contents

List of Figures

Introdução

1.1 Contextualização

O presente relatório foi elaborado no âmbito do segundo Trabalho Prático da Unidade Curricular de Tecnologia de Segurança, que se insere no 1º semestre do 4º ano do Mestrado Integrado em Engenharia Informática (1º ano MEI).

1.2 Objetivos e Trabalho Proposto

Este trabalho prático encontra-se dividido em duas partes independentes. A primeira parte consiste no uso de técnicas para a coleta passiva de informação de duas empresas, uma grannde corporação e um negócio local. A grande corporação escolhida foi a empresa de comunicações e entretenimento ,**NOS**, e o negócio local uma empresa de venda e arranjo de aparelhos informáticos, a **Fonetel**. A segunda parte do trabalho tem como objetivo a configuração de um ambiente de testes no qual são usadas técnicas e ferramentes de varredura ativa para identificar possíveis vulnerabilidades e fraquezas do sistema *Mestasploitable 3*.

1.3 Estrutura do Relatório

O relatório deste trabalho encontra-se dividido em duas partes (Parte A e parte B). A primeira parte é inicializada com uma breve defenição do processo de *Footprinting* seguida da coleta passiva de informações de ambas as empresas escolhidas. A segunda parte consiste na resolução das 5 questões do enunciado com o uso de ferramentas como o Nessus, Snort e wireshark.

Parte A

2.1 *Footprinting*

Footprinting refere-se ao processo de coletar o máximo de informações possíveis sobre um sistema ou empresa. Permite que um atacante crie um perfil quase completo do sistema de segurança da organização. Algumas das técnicas usadas no proceso de *Footprinting* são:

- Consultas DNS
- Enumeração em rede
- Consultas de rede
- Identificação do sistema operativo
- Inquéritos Organizacionais
- Ping scan
- Consultas dos Pontos de Contacto
- Varrer portas
- Consultas de registo (consultas WHOIS)
- Consultas SNMP

No proceso de coleta de informações, a empresa em questão não saberá deste processo pois apenas se utilizam comandos e pesquisas na internet até obter diversas informações como endereços IP, nomes de domínio e subdomínio, dispositivos e tecnologias usadas, contactos, funcionários e muito mais.

2.2 NOS

A grande corporação escolhida é a empresa NOS. A NOS é uma empresa de comunicações e entretenimento Portuguesa criada através da fusão de duas empresas: a ZON e a Optimus. Apenas em 16 de Maio de 2014 foi apresentada a NOS, a marca resultante desta fusão. Esta empresa tem mais de 4 milhões de clientes móveis, mais de 1,54 milhões de clientes de televisão, 1,6 milhões de clientes de telefone fixo e 1,145 milhões de clientes de internet de banda larga fixa.

De modo a fazer uma coleta passiva de informações que permitem identificar detalhes sobre a empresa, primeiramente, foi pesquisado na *web* o nome da empresa de modo a obter o site correto da mesma. Depois foram utilizados comandos no terminal e pesquisa na web para obter mais informações pretinentes. De seguida é apresentada a análise elaborada.

2.2.1 Comando *nmap -sS*

De maneira a descobrir informações sobre os endereços IP utilizados foi utilizado o comando *nmap -sS*. Este é um *security scanner* que neste caso comunica a partir da comunicação TCP e usa *TCP three-way handshake* para identificar portas abertas. As informações recolhidas encontram-se na figura seguinte.

```
margarida@Kali:~$ sudo nmap -sS  nos.pt
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-06 10:55 WET
Nmap scan report for nos.pt (212.113.183.252)
Host is up (0.0067s latency).
rDNS record for 212.113.183.252: a212-113-183-252.netcabo.pt
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 4.85 seconds
```

Figure 2.1: nmap -sS nos.pt

Com base na figura podemos verificar que o endereço IP é 212.113.183.252. Também podemos verificar as portas abertas: 80/tcp com serviço http e 443/tcp com serviço https.

2.2.2 Comando *whois*

Através do endereço IP obtido no comando anterior, foi utilizado o comando *whois* para obter mais informações. Este é um protocolo de consulta e resposta baseado em TCP que é normalmente usado para fornecer serviços de informação aos utilizadores. Retorna informações sobre os nomes de domínio registados, um bloco de endereços IP, servidores de nomes e mais informações relativas ao domínio. A figura 2.4 mostra as informações obtidas.

Com este comando obtemos informações importantes nomeadamente datas, moradas, contactos da empresa, número de fax. Através dos contactos obtidos recorremos ao site *sync.me* de modo a descobrir a quem pertencem estes contactos.

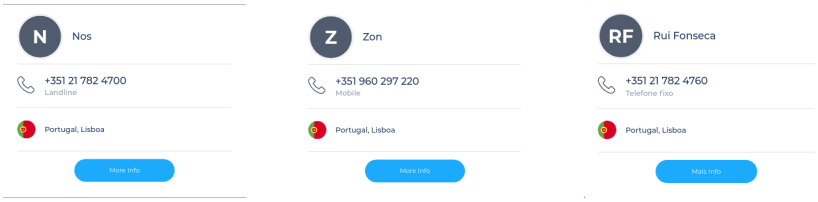


Figure 2.2: Contactos associados à Nos

Dois dos contactos obtidos através do *whois* correspondem a contactos da empresa. No entanto um deles está associado a uma pessoa. Pesquisamos pelo nome Rui Fonseca e encontramos o seu Linkedin. Este encontra-se atualmente na empresa NOS como *Senior Network Engineer* e na empresa desempenha a função de *Responsible for RD for Core IP Networks*.

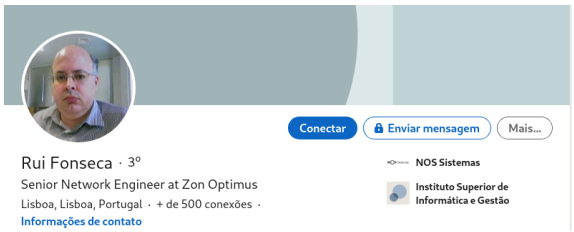


Figure 2.3: LinkedIn Rui Fonseca

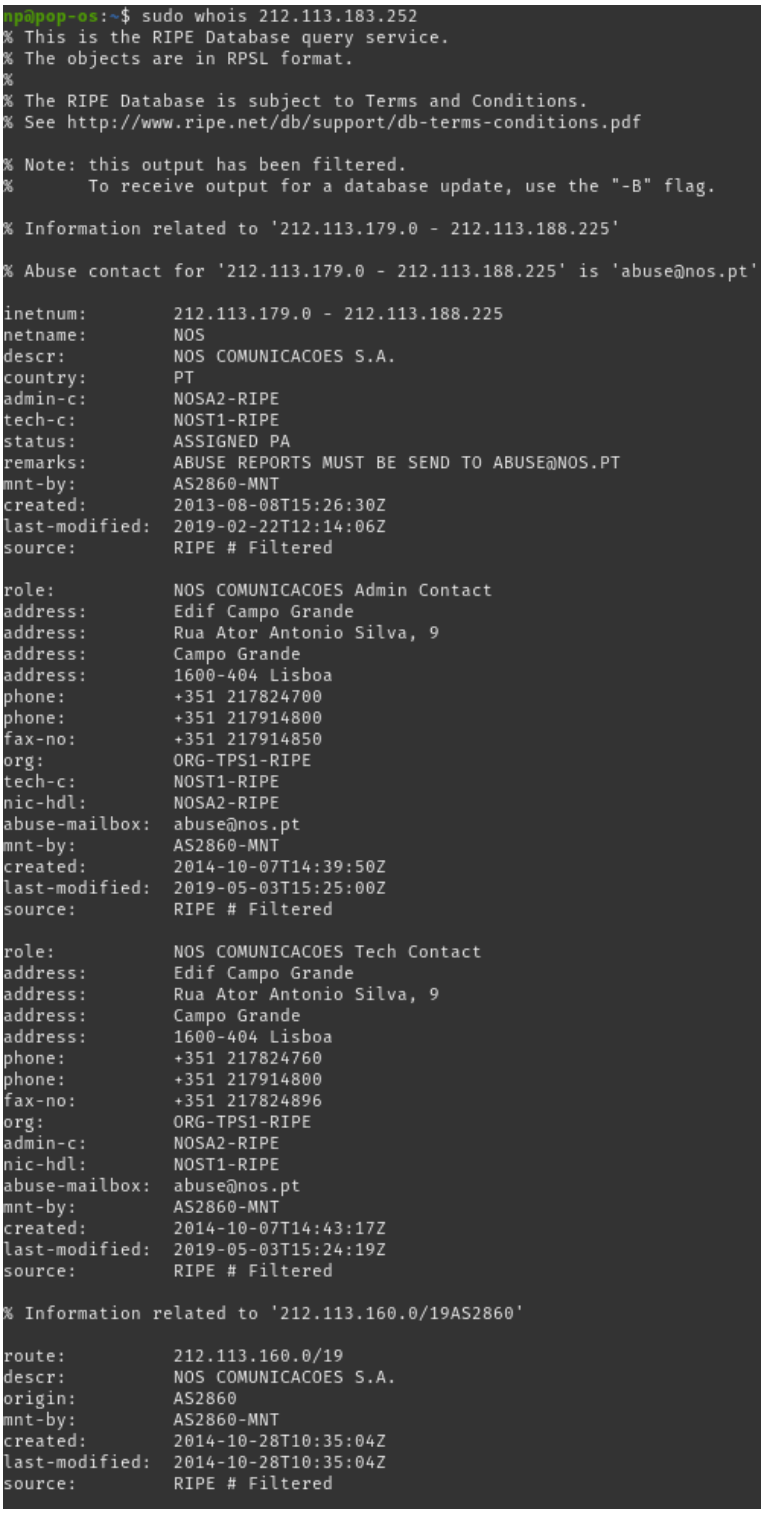


Figure 2.4: whois 212.113.183.252

2.2.3 Comando *nmap -O*

De modo a obter informações sobre os sitemas operativos utilizados pela empresa foi utilizado o comando *nmap -O*. Este comando permite descobrir os sistemas operativos associados o que depois poderá permitir a um atacantes a exploração das vulnerabilidades associadas aos mesmos. Neste caso é utilizado linux nas versões 3 e 4.

```
apapop-os:~$ sudo nmap -O 212.113.183.252
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-06 11:10 WET
Nmap scan report for a212-113-183-252.netcabo.pt (212.113.183.252)
Host is up (0.064s latency).
Not shown: 998 filtered ports
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: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.10 - 4.11, Linux 3.2 - 4.9
```

Figure 2.5: nmap -O 212.113.183.252

2.2.4 Análise da página Web

De maneira a obter mais informações relevantes da empresa fizemos uma análise à sua página web, *www.nos.pt*. Através da página conseguimos obter dados relevantes nomeadamente o contacto principal da empresa (mostrado também no comando *whois*) e as moradas dos diferentes polos da empresa. Também é possível ver quais os administradores executivos e não executivos.

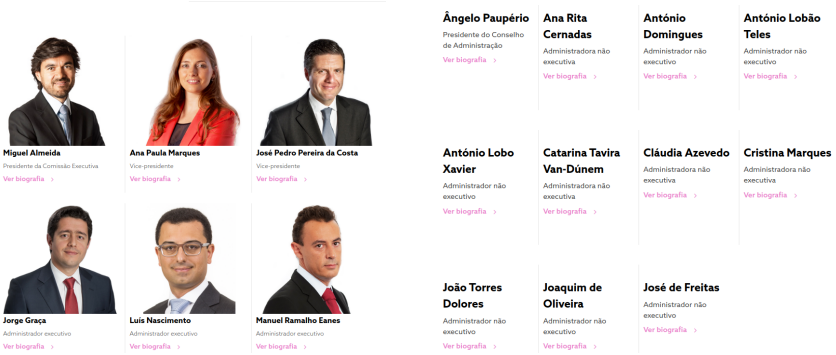


Figure 2.6: Administradores executivos e não executivos

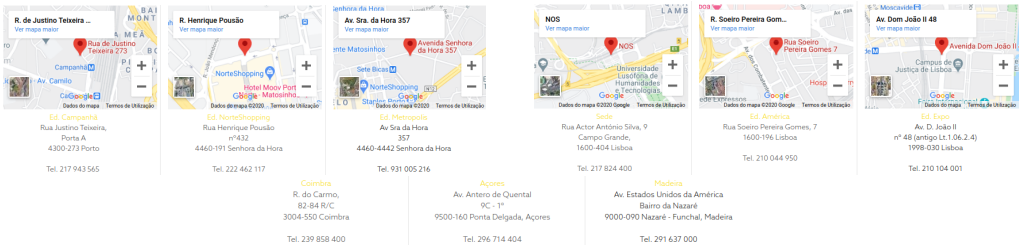


Figure 2.7: Moradas dos diferentes Polos

No site também é possível visualizar diversas propostas de emprego. Na figura seguinte encontra-se uma proposta de emprego para o cargo de arquiteto de redes e segurança de DataCenter. Com base nesta proposta conseguimos obter informações sobre as várias tecnologias de segurança de redes utilizada pela empresa.

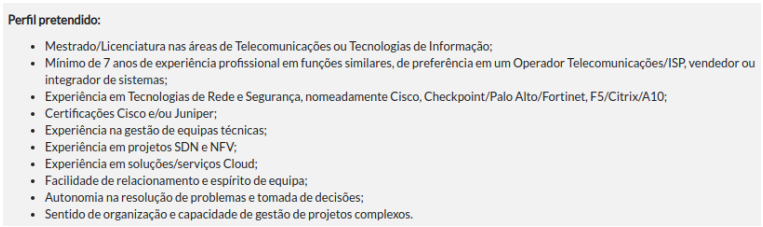


Figure 2.8: WayBackMachine

2.2.5 WayBackMachine

Recorremos ao arquivo de internet *WayBackMachine* e através deste site podemos ter acesso ao estado da página web da NOS em datas anteriores. É possível visualizar o site da NOS desde a sua criação até à atualidade.

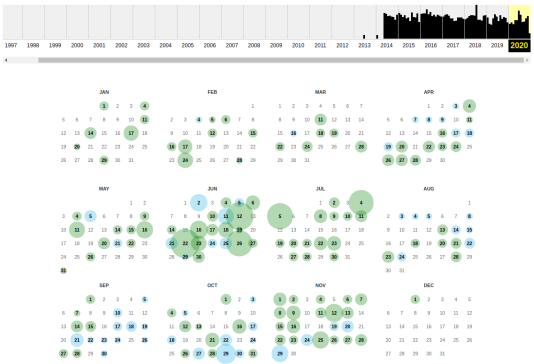


Figure 2.9: WayBackMachine

2.2.6 Censys

De modo a obter mais informações da empresa em questão recorremos ao site Censys. Com base nesta pesquisa conseguimos saber a versão e o conjunto de cifras utillizadas no TLS *Handshake*, que é imune à vulnerabilidade *Heartbleed*, conseguimos ver quais as configurações criptográficas utilizadas (DHE) e os certificados utilizados entre comunicações.

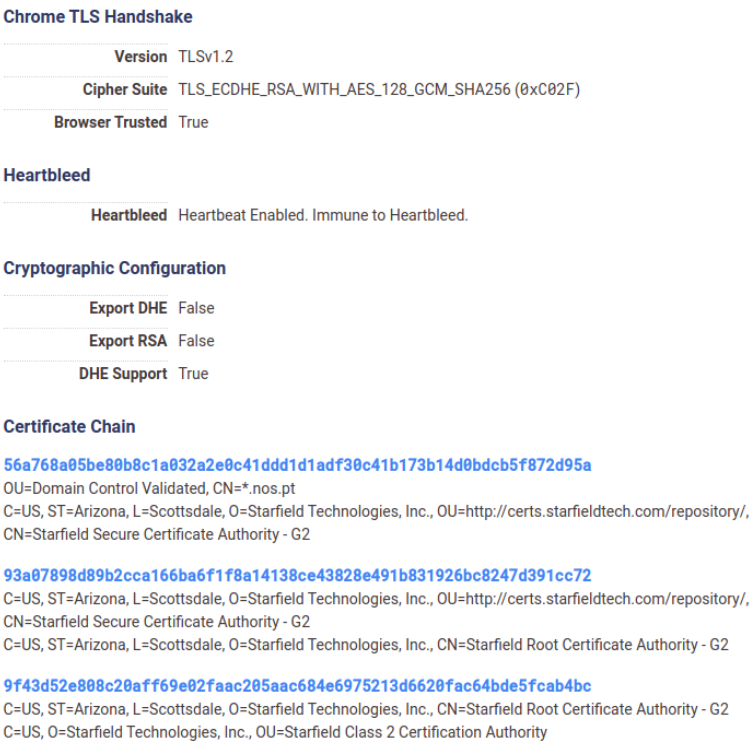


Figure 2.10: Censys

2.3 Fonetel

O negócio local escolhido para o desenvolvimento deste trabalho foi a empresa Fonetel. Esta é uma empresa de arranjo e venda de aparelhos informáticos como telemóveis, computadores, teclados e muitos mais.

Partindo para a coleta passiva de informações que permitem identificar detalhes sobre esta empresa, primeiramente, foi pesquisado na *web* o nome da empresa de modo a obter o site correto da mesma. Depois foram utilizados comandos no terminal e pesquisa na web para obter mais informações pretinentes. De seguida é apresentada a análise elaborada.

2.3.1 Comando *nmap -sS*

Começamos esta coleta de informações executando o comando *nmap -sS* no terminal para descobrir endereços IP e as portas usadas pela mesma para comunicações TCP. As informações obtidas encontram-se na figura seguinte:

```
margarida@Kali:~$ sudo nmap -sS fonetel.pt
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-07 15:31 WET
Nmap scan report for fonetel.pt (185.12.116.72)
Host is up (0.013s latency).
rDNS record for 185.12.116.72: cpanel72.dnscpanel.com
Not shown: 990 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
25/tcp   open  smtp
80/tcp   open  http
110/tcp  open  pop3
143/tcp  open  imap
443/tcp  open  https
587/tcp  open  submission
993/tcp  open  imaps
995/tcp  open  pop3s
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 4.98 seconds
```

Figure 2.11: nmap -sS fonetel.pt

A partir deste comando podemos observar que o endereço IP da empresa é 185.12.116.72 e também podemos observar na figura as diferentes conexões TCP.

2.3.2 Comando *whois*

Após descobrir qual o IP associado foi executado o comando *whois* de modo a obter informações mais detalhadas. O resultado da execução deste comando é visível na figura 2.13. Obtivemos diversos dados nomeadamente datas, contactos telefónicos, dois nomes de pessoas (Nuno Matias e Rui Silva), moradas e decrições. A partir destes dados observamos que a empresa comprou os serviços de alojamento Web a outra empresa, dominios.pt. Na pesquisa pelos dois nomes resultantes da execução do comando verificamos que ambos estão relacionados com a empresa de alojamento Web e não com a Fonetel. Os contactos/moradas e outras informações obtidas com *whois* também pertencem à domínios.pt.

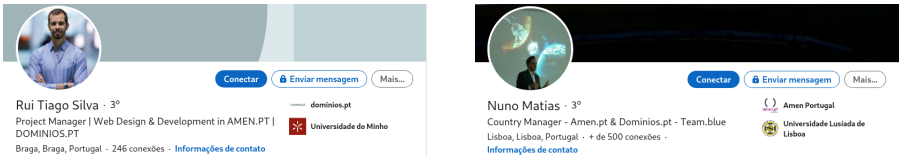


Figure 2.12: Linkedin de indivíduos da dominios.pt

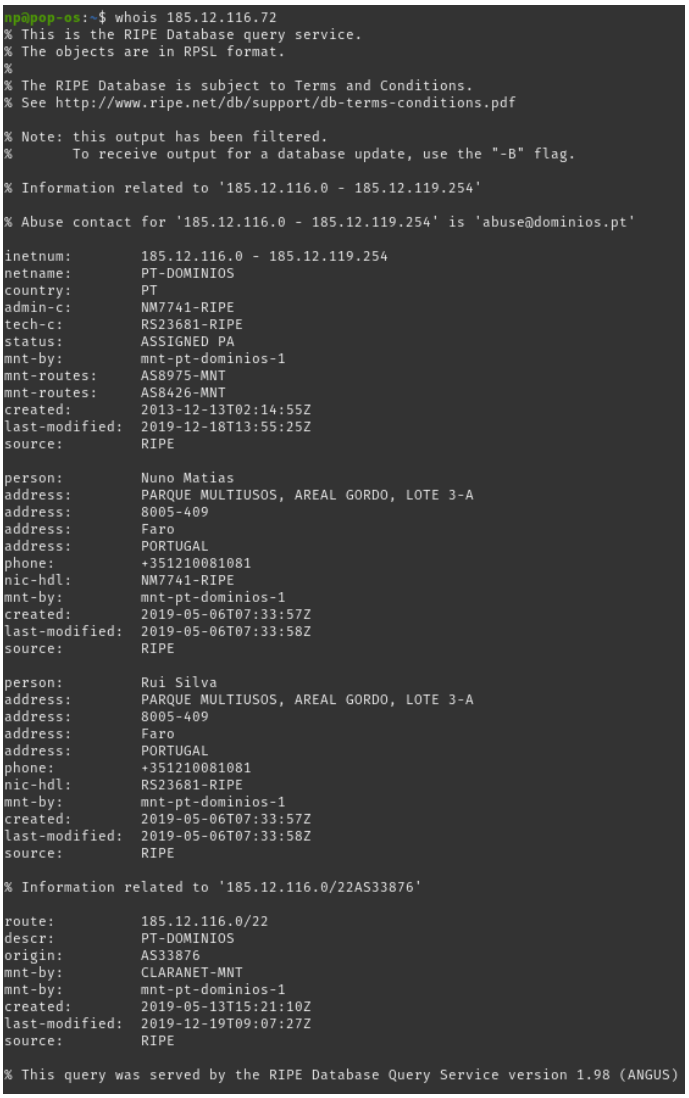


Figure 2.13: whois 185.12.116.72

2.3.3 Comando *nmap -O*

De modo a obter informações sobre os sitemas operativos utilizados pelo domínio foi utilizado o comando *nmap -O*. Este comando permite descobrir os sistemas operativos associados ao domínio, o que depois poderá permitir a um atacantes a exploração das vulnerabilidades associadas aos mesmos. Neste caso é utilizado linux nas versões 3 e 4. Também é possível observar as portas abertas do servidor o que também poderá ser suscetível a ataques.

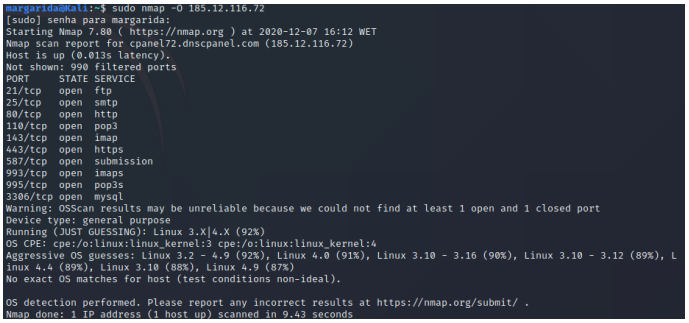


Figure 2.14: nmap -O 185.12.116.72

2.3.4 Comando *nmap -sV*

Foi executado o comando *nmap -sV* de modo a descobrir as versões dos serviços associados às portas abertas. Isto permitiria a um atacante procurar vulnerabilidades e fraquezas dessas versões para um possível ataque.

```
np@pop-os:~$ nmap -sV  fonetel.pt
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-07 16:36 WET
Nmap scan report for fonetel.pt (185.12.116.72)
Host is up (0.015s latency).
Not shown: 990 filtered ports
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     Pure-FTPd
25/tcp   open  smtp?
80/tcp   open  http    Apache httpd
110/tcp  open  pop3    Dovecot pop3d
143/tcp  open  imap    Dovecot imapd
443/tcp  open  ssl/ssl Apache httpd (SSL-only mode)
587/tcp  open  smtp    Exim smtpd 4.93
993/tcp  open  imaps?
995/tcp  open  pop3s?
3306/tcp open  mysql   MySQL 5.5.5-10.3.24-MariaDB-cll-lve
Service Info: Host: cpanel72.dnscpanel.com
```

Figure 2.15: nmap -sV 185.12.116.72

2.3.5 Análise da página Web

Para tentar obter mais informações pretinentes referentes à empresa Fonetel, fizemos uma análise à sua página web, *fonetel.pt*. Através da página conseguimos obter os contactos telefónicos, e-mails eletrónicos da empresa, moradas das diferentes lojas associadas à mesma e a página do facebook.

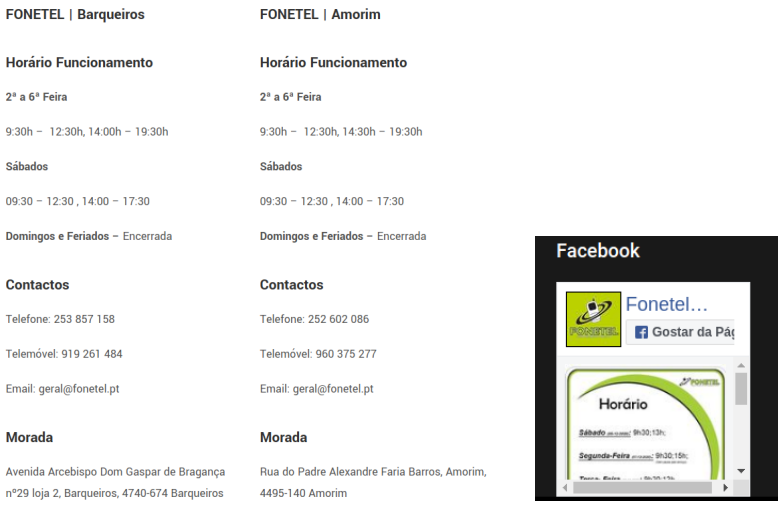


Figure 2.16: Informações página Web

2.3.6 Censys

Recorremos ao site Censys de modo a tentar encontrar mais informações. Com base nesta pesquisa conseguimos saber a versão e o conjunto de cifras utillizadas no TLS *Handshake*, que é imune à vulnerabilidade *Heartbleed*, conseguimos ver que não utiliza nenhuma das configurações criptográficas lá indicadas (DHE e RSA) e podemos ver os certificados utilizados entre comunicações.

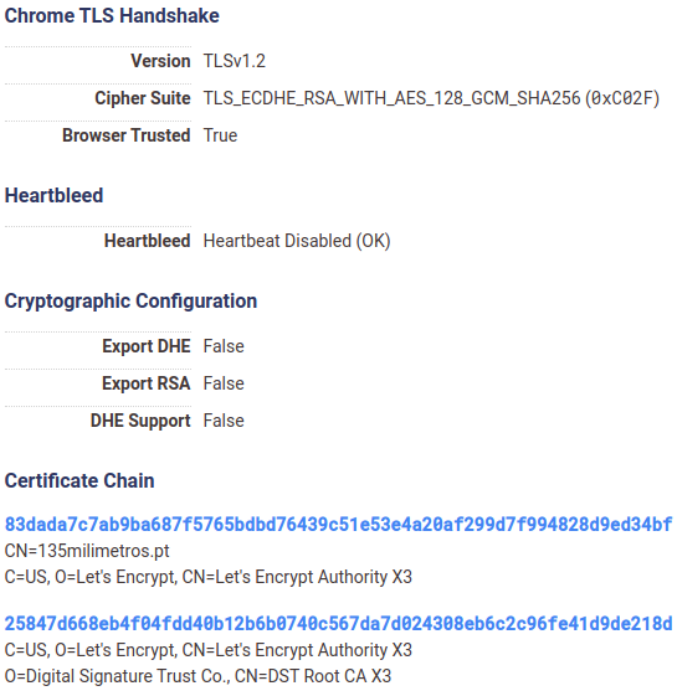


Figure 2.17: nmap -sV 185.12.116.72

2.4 Diferenças entre as duas empresas

Foi possível obter mais informações da grande corporação, a empresa NOS, do que do negócio local, Fonetel. Isto deve-se especialmente ao facto da empresa Fonetel ter o seu servidor gerênciado por outra empresa. Também no que toca a pesquisas *Web*, foram encontrados muitas mais informações relativas à grande empresa.

2.5 Estratégias destinadas a fortalecer a postura de segurança de mecanismos de pesquisa passiva

Existem algumas estratégias que permitem ocultar informações relevantes e por vezes pessoais dos métodos de pesquisa passiva. Algumas delas são:

- uso de e-mails gerais em vez de pessoais;
- evitar o uso de nomes verdadeiros;
- não colocar informações sensíveis na *web*;
- se possível utilizar uma VPN de forma a esconder o IP do servidor;
- utilizar o *whois Privacy*.

Parte B

Após instalar os programas necessários para esta parte (*Nessus* e *Snort*) foi necessário estabelecer a conexão entre as máquinas virtuais. Para tal foi foi executado o comando da figura seguinte:

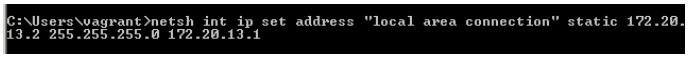


Figure 3.1: Estabelecimento da conexão entre máquinas virtuais

De modo a confirmar que estava bem configurado, foram executados os comandos *ipconfig* que mostra as configurações dos Ip's e por aí podemos confirmar que ambos se encontram ligados à mesma rede, e foram executados comandos *ping* em ambas as máquinas virtuais para demonstrar que a comunicação era possível. Tais execuções encontram-se nas figuras seguintes:

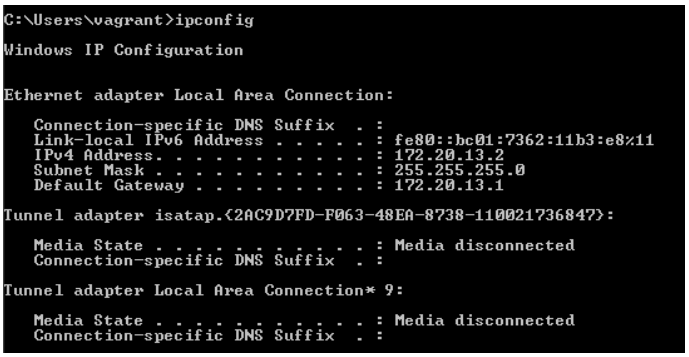


Figure 3.2: ipconfig

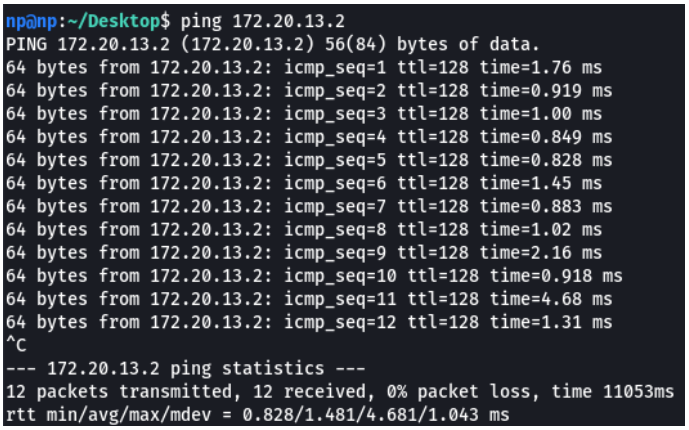


Figure 3.3: ping 172.20.13.2

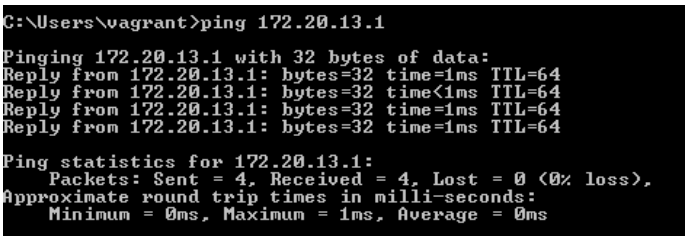


Figure 3.4: ping 172.20.13.1

3.1 Resolução das questões

Q1:

Recorreu-se ao comando *nmap -sV* de modo a conseguir saber quais os serviços a correr no sistema. A imagem seguinte mostra o resultado da execução do comando onde é possível ver a lista dos diferentes serviços TCP.

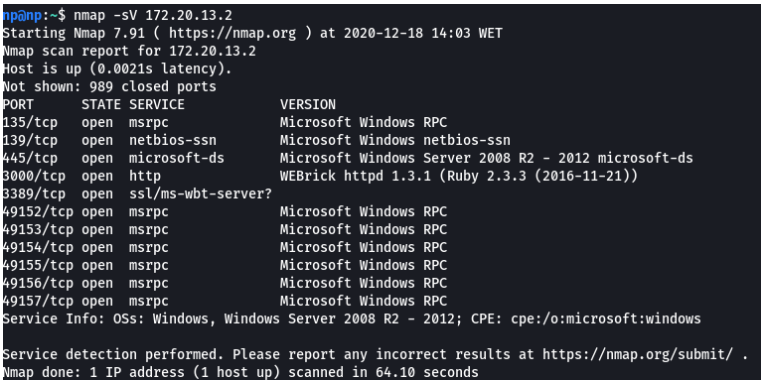


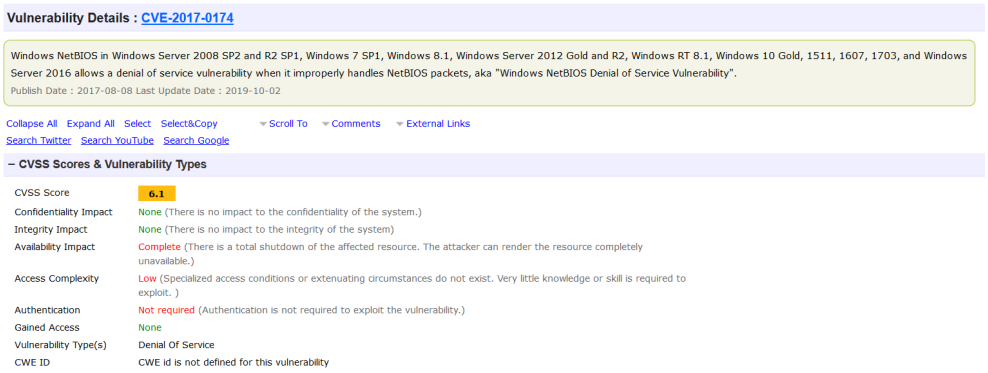
Figure 3.5: nmap -sV 172.20.13.2

De seguida são apresentadas as vulnerabilidades e fraquezas mais recentes ou mais graves relacionados com cada um dos serviços expostos em cima:

- **msrpc**: A vulnerabilidade encontrada para este serviço caracteriza-se por ser do tipo *Information Disclosure*. Acontece quando o driver *Kernel Remote Procedure Call Provider* inicializa indevidamente objetos na memória.

Figure 3.6: CVE-2018-8407

- **netbios-ssn**: Para este serviço a vulnerabilidade encontrada é do tipo *Denial of Service*. Esta acontece quando os pacotes netbios são manipulados indevidamente.



Vulnerability Details : CVE-2017-0174

Windows NetBIOS in Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows a denial of service vulnerability when it improperly handles NetBIOS packets, aka "Windows NetBIOS Denial of Service Vulnerability".

Publish Date : 2017-08-08 Last Update Date : 2019-10-02

Collapse All Expand All Select Select&Copy Scroll To Comments External Links

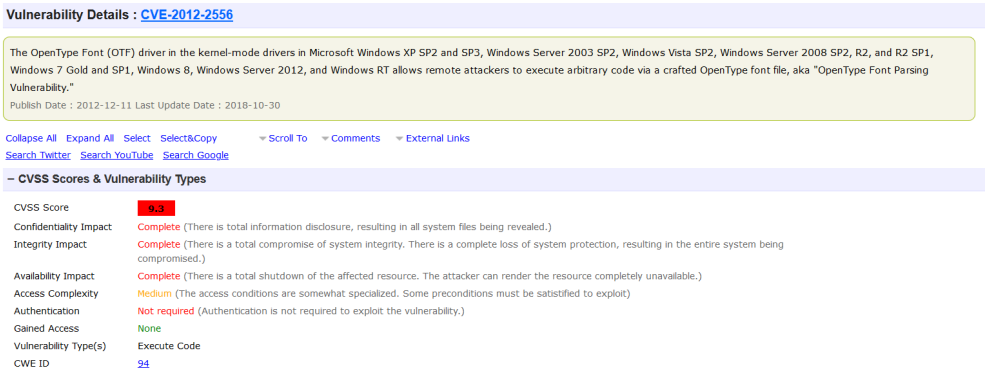
Search Twitter Search YouTube Search Google

– CVSS Scores & Vulnerability Types

CVSS Score	6.1
Confidentiality Impact	None (There is no impact to the confidentiality of the system.)
Integrity Impact	None (There is no impact to the integrity of the system)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Denial Of Service
CWE ID	CWE id is not defined for this vulnerability

Figure 3.7: CVE-2017-0174

- **microsoft-ds**: Uma fraqueza grave encontrada para este serviço compromete a integridade e pode também revelar diversas informações. Esta permite a atacantes executar código arbitrário via *Open Type Font*.



Vulnerability Details : CVE-2012-2556

The OpenType Font (OTF) driver in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1, Windows 8, Windows Server 2012, and Windows RT allows remote attackers to execute arbitrary code via a crafted OpenType font file, aka "OpenType Font Parsing Vulnerability."

Publish Date : 2012-12-11 Last Update Date : 2018-10-30

Collapse All Expand All Select Select&Copy Scroll To Comments External Links

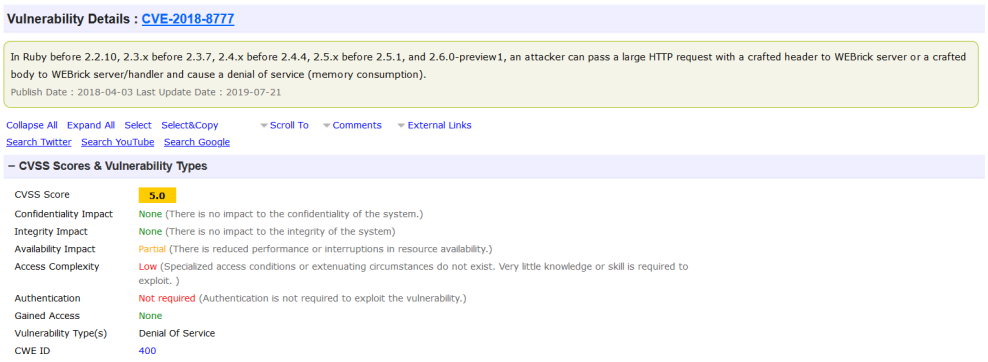
Search Twitter Search YouTube Search Google

– CVSS Scores & Vulnerability Types

CVSS Score	9.3
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Medium (The access conditions are somewhat specialized. Some preconditions must be satistified to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Execute Code
CWE ID	94

Figure 3.8: CVE-2012-2556

- **http**: Uma vulnerabilidade encontrada para uma das versões deste serviço é do tipo *Denial of Service*. Nesta vulnerabilidade um atacante pode passar um um http *request* maior que o normal com um *header* por ele construído e enviá-lo para o *WEBrick*.



Vulnerability Details : CVE-2018-8777

In Ruby before 2.2.10, 2.3.x before 2.3.7, 2.4.x before 2.4.4, 2.5.x before 2.5.1, and 2.6.0-preview1, an attacker can pass a large HTTP request with a crafted header to WEBrick server or a crafted body to WEBrick server/handler and cause a denial of service (memory consumption).

Publish Date : 2018-04-03 Last Update Date : 2019-07-21

Collapse All Expand All Select Select&Copy Scroll To Comments External Links

Search Twitter Search YouTube Search Google

– CVSS Scores & Vulnerability Types

CVSS Score	5.0
Confidentiality Impact	None (There is no impact to the confidentiality of the system.)
Integrity Impact	None (There is no impact to the integrity of the system)
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Denial Of Service
CWE ID	400

Figure 3.9: CVE-2018-8777

- **ssl**: Uma vulnerabilidade destacada para o serviço de ssl caracteriza-se por a componente de ssl de certas versões do *Windows* (presentes na imagem) não conseguirem tratar adequadamente os pacotes cifrados o que permite aos atacantes levarem a cabo um ataque do tipo *man-in-the-middle* que conduzem a ataques de *downgrade* de sessões sslV3 para sslV2 ou sessões TLS intercetantdo *handshakes* e injetando conteúdo.

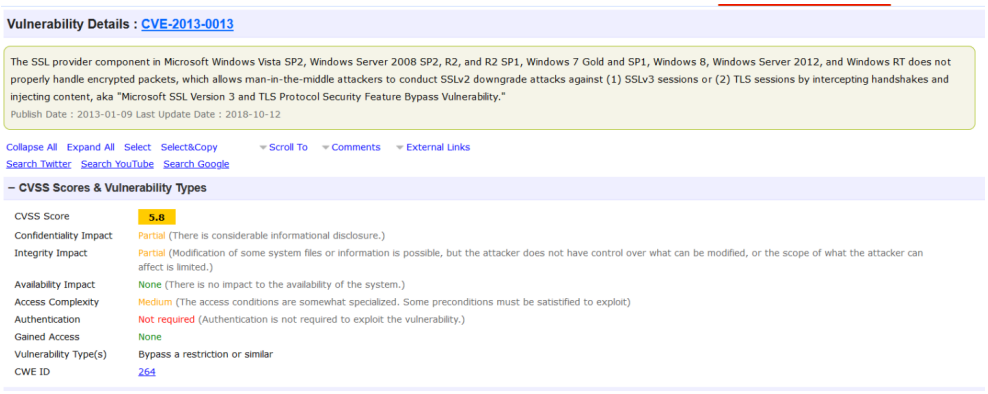


Figure 3.10: CVE-2013-0013

Q2:

De modo a conseguirmos ver o resultado da utilização de um scanner de varredura ativa e avaliar as diferenças entre o resultado do sistema automático de identificação de vulnerabilidades e o resultado que obtivemos no item Q1, recorremos ao Nessus. Fazendo o *basic scan* ao *host*: 120.20.13.2 obtivemos os seguintes resultados:

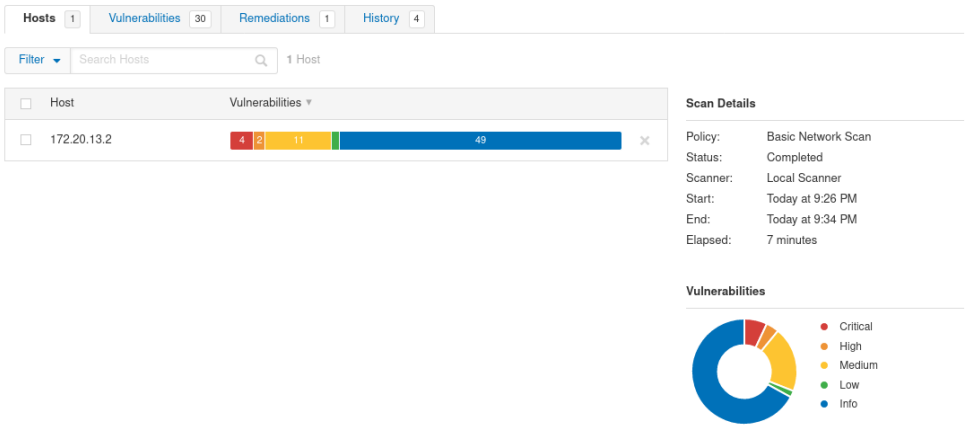


Figure 3.11: *Network Scan*

Este scan fornece-nos várias informações sobre as vulnerabilidades presentes no Metasploitable3-win2k8. Divide-as por classificação com seguinte configuração:

- 4 vulnerabilidades criticas
- 2 vulnerabilidades altas
- 11 vulnerabilidades médias
- 1 vulnerabilidade baixa
- 49 iformações

O scan motra-nos as diferentes vulnerabilidades que recolheu, tal é possível ver na figura seguinte:

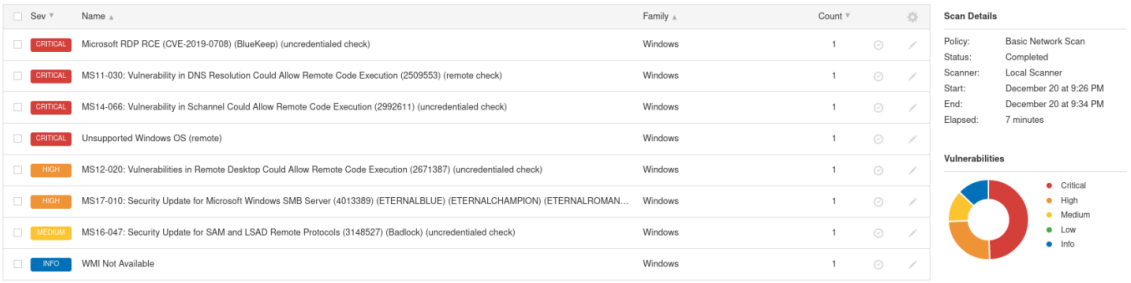


Figure 3.12: Vulnerabilidades Nessus

Em cada uma destas vulnerabilidades temos a descrição, solução e CVE, como podemos verificar na figura 3.13, em que o host é afetado por execução de código remoto em RDP.

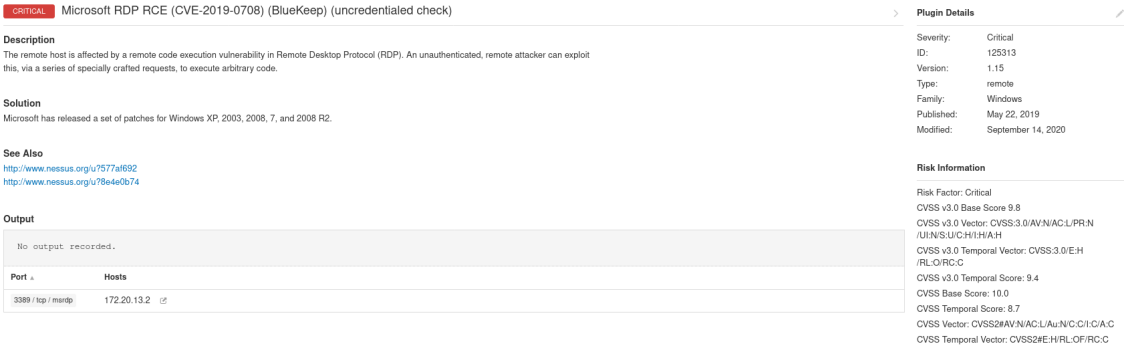


Figure 3.13: Vulnerabilidade crítica

Podemos então concluir que o Nessus, programa de verificação de falhas e ou vulnerabilidades de segurança é mais completo que o nmap, que é apenas um port scan utilizado para avaliar a segurança e descobrir serviços ou servidores de uma rede de computadores, este dá-nos apenas serviços e a sua versão.

Q3:

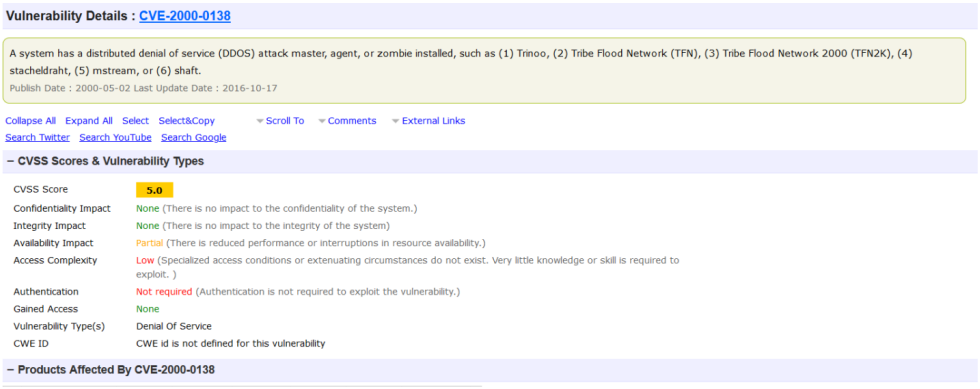
Para responder a esta questão foi necessário analisar o ficheiro *alert.full* produzido pelo Snort e posteriormente a análise dos eventos no *wireshark*. Os dois eventos escolhidos identificados como tráfego anómalo são os seguintes:

- Evento 1:

```
[**] [1:249:8] DDOS mstream client to handler [**]
[Classification: Attempted Denial of Service] [Priority: 2]
12/21-15:24:42.909122 172.20.13.1:26504 → 172.20.13.2:15104
TCP TTL:64 TOS:0×0 ID:0 IpLen:20 DgmLen:48 DF
******S* Seq: 0×E4203344  Ack: 0×0  Win: 0×1000  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]
```

Figure 3.14: Evento 1 tráfego anómalo

O Snort disponibiliza o link para o CVE de cada evento. O CVE para este evento é possível de visualizar na figura 3.15 e corresponde a uma vulnerabilidade do tipo *Deniel of Service*.



Vulnerability Details : CVE-2000-0138

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.

Publish Date : 2000-05-02 Last Update Date : 2016-10-17

Collapse All Expand All Select Select&Copy Scroll To Comments External Links

Search Twitter Search YouTube Search Google

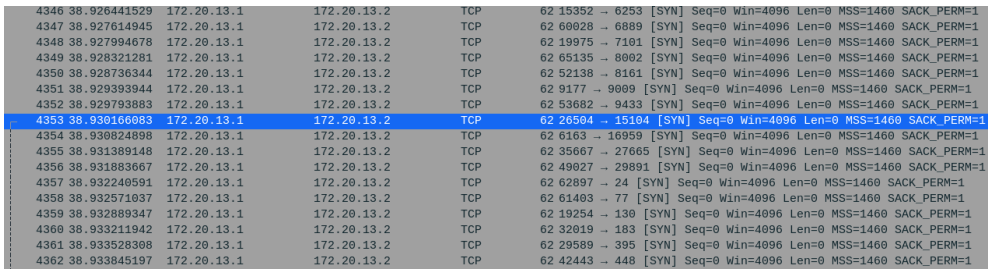
– CVSS Scores & Vulnerability Types

CVSS Score	5.0
Confidentiality Impact	None (There is no impact to the confidentiality of the system.)
Integrity Impact	None (There is no impact to the integrity of the system)
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Denial Of Service
CWE ID	CWE id is not defined for this vulnerability

– Products Affected By CVE-2000-0138

Figure 3.15: CVE-2000-0138

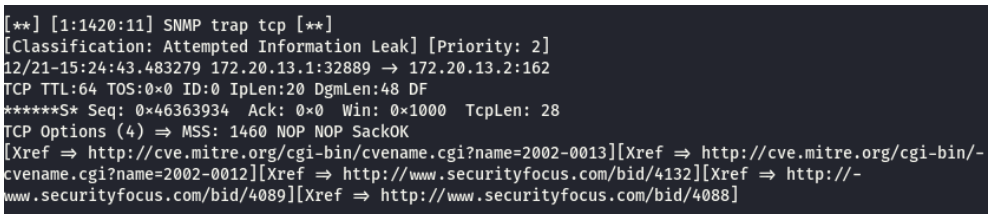
Na figura seguinte, captura do tráfego do *wireshark*, podemos confirmar que se trata de um ataque de *Deniel of Service*, tentativa de sobrecarregar o sistema com *requests* de conexão até que o tráfego normal seja incapaz de ser processado, o que resulta na negação dos serviços ao utilizador, isto porque podemos verificar a partir da figura que o pacote a ser transmitido em todas as conexões da imagem é o mesmo, apenas mudam as portas.



```
4346 38.926441529  172.20.13.1  172.20.13.2  TCP  62 15352 → 6253 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
4347 38.927614945  172.20.13.1  172.20.13.2  TCP  62 60028 → 6889 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
4348 38.927994678  172.20.13.1  172.20.13.2  TCP  62 19975 → 7101 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
4349 38.928321281  172.20.13.1  172.20.13.2  TCP  62 65135 → 8002 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
4350 38.928736344  172.20.13.1  172.20.13.2  TCP  62 52138 → 8161 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
4351 38.929393944  172.20.13.1  172.20.13.2  TCP  62 9177 → 9009 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
4352 38.929793883  172.20.13.1  172.20.13.2  TCP  62 53682 → 9433 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
4353 38.930166083  172.20.13.1  172.20.13.2  TCP  62 26504 → 15104 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
4354 38.930824898  172.20.13.1  172.20.13.2  TCP  62 6163 → 16959 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
4355 38.931389148  172.20.13.1  172.20.13.2  TCP  62 35667 → 27665 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
4356 38.931883667  172.20.13.1  172.20.13.2  TCP  62 49027 → 29891 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
4357 38.932240591  172.20.13.1  172.20.13.2  TCP  62 62897 → 24 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
4358 38.932571037  172.20.13.1  172.20.13.2  TCP  62 61403 → 77 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
4359 38.932889347  172.20.13.1  172.20.13.2  TCP  62 19254 → 130 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
4360 38.933211942  172.20.13.1  172.20.13.2  TCP  62 32019 → 183 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
4361 38.933528308  172.20.13.1  172.20.13.2  TCP  62 29589 → 395 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
4362 38.933845197  172.20.13.1  172.20.13.2  TCP  62 42443 → 448 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
```

Figure 3.16: Tráfego wireshark evento 1

- Evento 2:



```
[**] [1:1420:11] SNMP trap tcp [**]
[Classification: Attempted Information Leak] [Priority: 2]
12/21-15:24:43.483279 172.20.13.1:32889 → 172.20.13.2:162
TCP TTL:64 TOS:0×0 ID:0 IpLen:20 DgmLen:48 DF
******S* Seq: 0×46363934  Ack: 0×0  Win: 0×1000  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]
```

Figure 3.17: Evento 2 tráfego anómalo

Neste evento o Snort detetou duas vulnerabilidades. O primeiro CVE deste evento tem a máxima pontuação o que significa que é bastante grave. Este resulta da implementação do SNMP que permite a atacantes remotos levar a cabo um ataque do tipo *Deniel of Service* ou ganhar previlégios através de *GetRequest*, *GetNextRequest* e *SetRequest messages*.

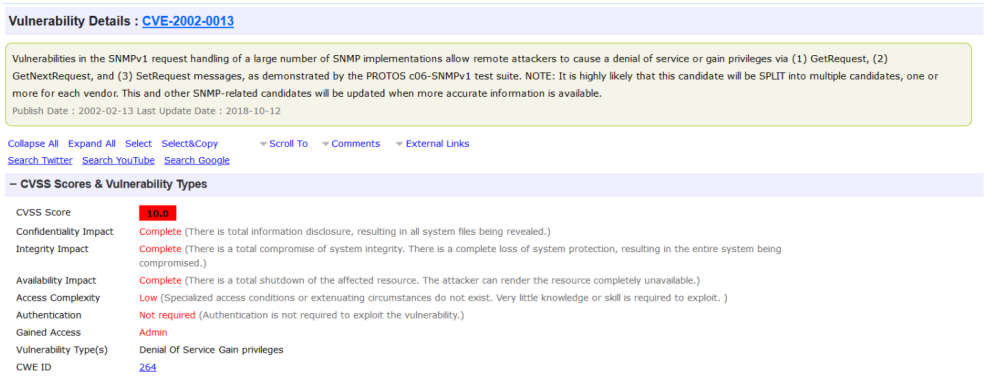


Figure 3.18: CVE-2002-0013

O segundo CVE deste evento tem também uma pontuação máxima. É muito semelhante ao anterior mas neste caso o atacante pode ganhar previlégios através de SNMPv1 *trap handling*.

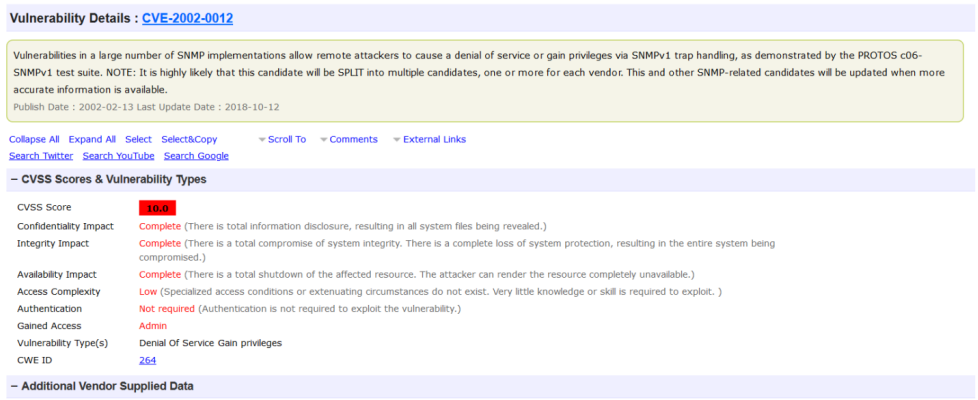


Figure 3.19: CVE-2002-0012

No analisador de tráfego *wireshark* é possível ver o respetivo tráfego deste evento. Tal é possível visualizar na figura seguinte:

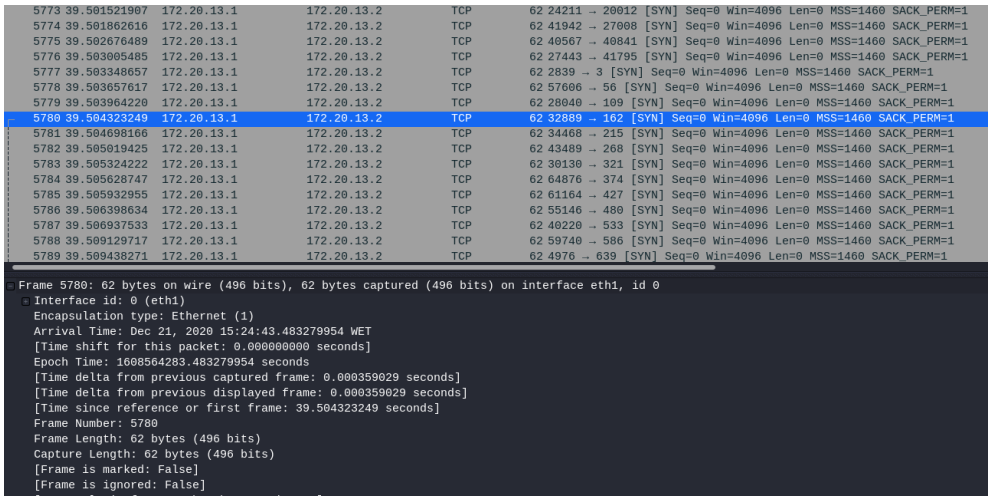


Figure 3.20: Tráfego wireshark evento 2

Q4:

O motivo pelo qual algumas notificações do IDS não possuem vulnerabilidades correspondentes no relatório de *Scanner* de vulnerabilidades (Nessus), é que a ferramenta Snort é utilizada essencialmente para alertar qualquer tráfego que considere anómalo quer a porta TCP seja aberta ou fechada. Por contrapartida, o Nessus apenas alerta as vulnerabilidadades de portas abertas.

Q5:

Para responder a esta questão escolhemos 3 vulnerabilidades, uma classificada como *Critical*, outro como *High* e uma última como *Medium*. De seguida são apresentadas estas vulnerabilidades:

- **Vulnerabilidade *Critical***: Esta fraqueza implica que um sistema possa ser atacado por uma vulnerabilidade de execução de código remoto no *Remote Desktop Protocol* (RDP).Um atacante não autenticado pode explorar isto, através de uma série de pedidos especialmente formulados, para executar código arbitrário. É possível ver a vulnerabilidade na figura seguinte:

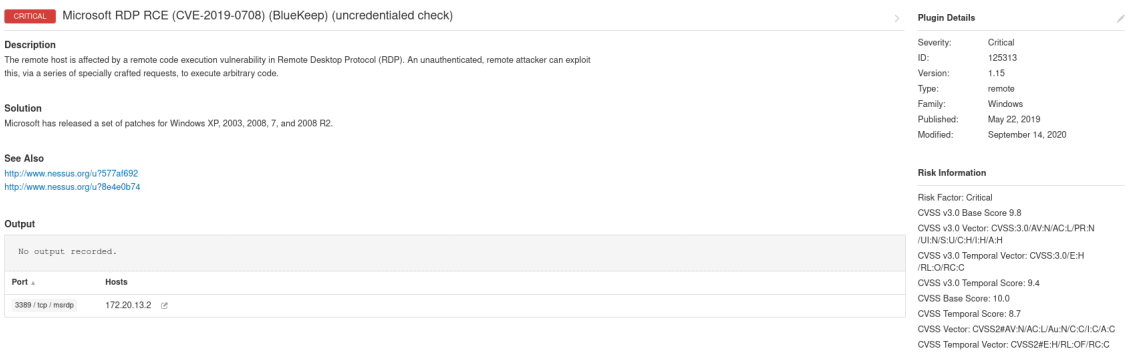


Figure 3.21: Vulnerabilidade *Critical*

A solução encontrada para resolver esta fraqueza consiste em instalar o *patch* de segurança KB4499175.

- **Vulnerabilidade *High***: Esta vulnerabilidade indica que existe uma vulnerabilidade arbitrária de código remoto na implementação do *Remote Desktop Protocol* (RDP) no sistema remoto do Windows. A vulnerabilidade deve-se à forma como o RDP acede a um objecto em memória que foi incorrectamente inicializado ou apagado. Se o RDP tiver sido ativado no sistema afectado, um atacante não autenticado poderia aproveitar esta vulnerabilidade para levar o sistema a executar código arbitrário, enviando-lhe uma sequência de pacotes RDP especialmente criados. Este *plugin* também verifica a vulnerabilidade de negação de serviço no Microsoft Terminal Server. A vulnerabilidade é exposta na figura 3.22.

A solução encontrada para resolver esta fraqueza consiste na instalação do *patch* de segurança KB2621440.

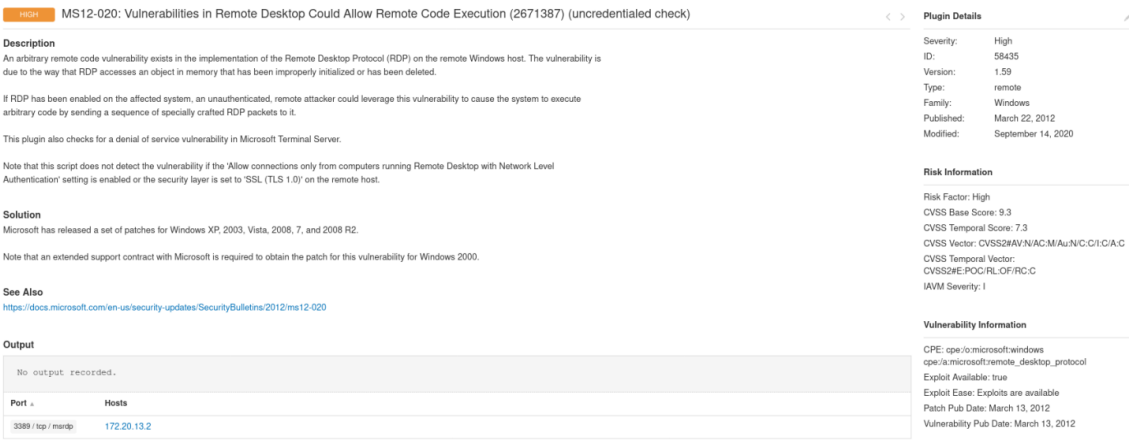


Figure 3.22: Vulnerabilidade *High*

- **Vulnerabilidade *Medium***: Nesta fraqueza o Windows é afectado por uma elevação de privilégios nos protocolos *Security Account Manager* (SAM) e *Local Security Authority (Domain Policy)* (LSAD) devido a uma negociação inadequada do nível de autenticação sobre os canais de *Remote Procedure Call* (RPC). Um atacante *man-in-the-middle* é capaz de interceptar comunicações entre um cliente e um servidor que possui uma base de dados SAM e pode explorá-lo para forçar o nível de autenticação a baixar, permitindo ao atacante fazer-se passar por um utilizador autenticado e aceder à base de dados SAM.

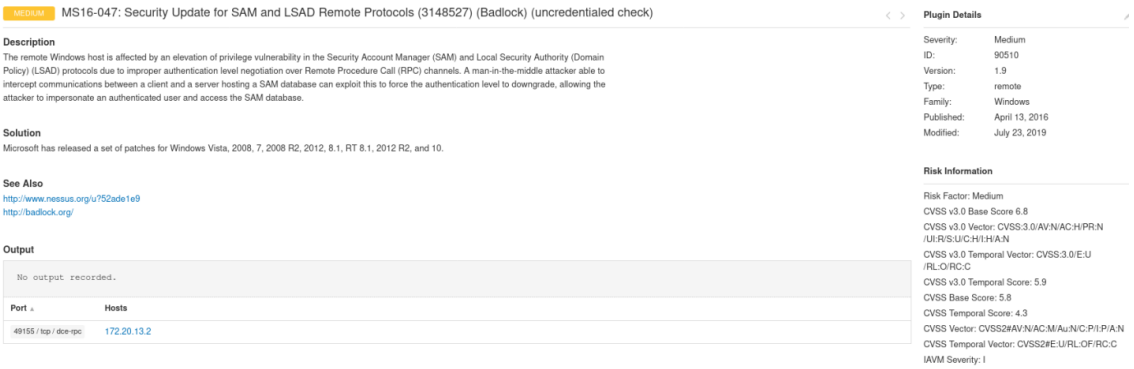


Figure 3.23: Vulnerabilidade *Medium*

A solução encontrada para resolver esta fraqueza seria a instalação do *patch* de segurança KB2621440.

Devido a problemas técnicos em ambos os computadores do grupo, não foi possível resolver as vulnerabilidades encontradas a partir das soluções apresentadas. Isto porque no caso de um dos elementos a máquina virtual relativa à *Metasploitable 3*, ficou muito lenta e como ela se desliga após 10 minutos impossibilitou a resolução da questão. Após várias reinstalações e após o aumento dos recursos da máquina o mesmo se sucedeu. O outro caso envolveu problemas de memória no computador que impossibilitou a instalação de uma das máquinas virtuais.

Conclusão

Com a elaboração deste trabalho foi nos possível aplicar conhecimentos obtidos nas aulas práticas desta unidade curricular. Conseguimos aprofundar conhecimentos sobre a coleta passiva de informações que nos permitiu identificar detalhes sobre duas empresas e identificar as respetivas estratégias para fortalecer a postura de segurança das mesmas. Também nos foi possível concluir que existem várias maneiras de encontrar e identificar várias ameaças através de ferramentas diversas.