



**Universidade do Minho**  
Escola de Engenharia

Universidade do Minho  
Mestrado Integrado em Engenharia Informática

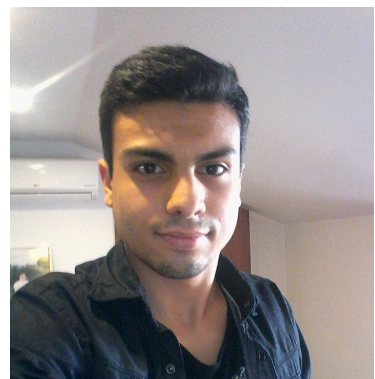
## **Tecnologia de Segurança**

### **Trabalho prático 2**

22 Dezembro 2020



Ana Margarida Campos  
(A85166)



Nuno Pereira  
(PG42846)

# Contents

<b>1</b>	<b>Introdução</b>	<b>5</b>
1.1	Contextualização . . . . .	5
1.2	Objetivos e Trabalho Proposto . . . . .	5
1.3	Estrutura do Relatório . . . . .	5
<b>2</b>	<b>Parte A</b>	<b>6</b>
2.1	<i>Footprinting</i> . . . . .	6
2.2	NOS . . . . .	6
2.2.1	Comando <i>nmap -sS</i> . . . . .	7
2.2.2	Comando <i>whois</i> . . . . .	7
2.2.3	Comando <i>nmap -O</i> . . . . .	8
2.2.4	Análise da página Web . . . . .	9
2.2.5	WayBackMachine . . . . .	10
2.2.6	Censys . . . . .	10
2.3	Fonetel . . . . .	11
2.3.1	Comando <i>nmap -sS</i> . . . . .	11
2.3.2	Comando <i>whois</i> . . . . .	11
2.3.3	Comando <i>nmap -O</i> . . . . .	12
2.3.4	Comando <i>nmap -sV</i> . . . . .	13
2.3.5	Análise da página Web . . . . .	13
2.3.6	Censys . . . . .	13
2.4	Diferenças entre as duas empresas . . . . .	14
2.5	Estratégias destinadas a fortalecer a postura de segurança de mecanismos de pesquisa passiva . . . . .	14
<b>3</b>	<b>Parte B</b>	<b>15</b>
3.1	Resolução das questões . . . . .	16
<b>4</b>	<b>Conclusão</b>	<b>24</b>

# List of Figures

2.1	nmap -sS nos.pt . . . . .	7
2.2	Contactos associados à Nos . . . . .	7
2.3	LinkedIn Rui Fonseca . . . . .	7
2.4	whois 212.113.183.252 . . . . .	8
2.5	nmap -O 212.113.183.252 . . . . .	9
2.6	Administradores executivos e não executivos . . . . .	9
2.7	Moradas dos diferentes Polos . . . . .	9
2.8	WayBackMachine . . . . .	9
2.9	WayBackMachine . . . . .	10
2.10	Censys . . . . .	10
2.11	nmap -sS fonetel.pt . . . . .	11
2.12	LinkedIn de indivíduos da dominios.pt . . . . .	11
2.13	whois 185.12.116.72 . . . . .	12
2.14	nmap -O 185.12.116.72 . . . . .	12
2.15	nmap -sV 185.12.116.72 . . . . .	13
2.16	Informações página Web . . . . .	13
2.17	nmap -sV 185.12.116.72 . . . . .	14
3.1	Estabelecimento da conexão entre máquinas virtuais . . . . .	15
3.2	ipconfig . . . . .	15
3.3	ping 172.20.13.2 . . . . .	15
3.4	ping 172.20.13.1 . . . . .	16
3.5	nmap -sV 172.20.13.2 . . . . .	16
3.6	CVE-2018-8407 . . . . .	16
3.7	CVE-2017-0174 . . . . .	17
3.8	CVE-2012-2556 . . . . .	17
3.9	CVE-2018-8777 . . . . .	17
3.10	CVE-2013-0013 . . . . .	18
3.11	<i>Network Scan</i> . . . . .	18
3.12	Vulnerabilidades Nessus . . . . .	19
3.13	Vulnerabilidade crítica . . . . .	19
3.14	Evento 1 tráfego anómalo . . . . .	19
3.15	CVE-2000-0138 . . . . .	20
3.16	Tráfego wireshark evento 1 . . . . .	20
3.17	Evento 2 tráfego anómalo . . . . .	20
3.18	CVE-2002-0013 . . . . .	21
3.19	CVE-2002-0012 . . . . .	21
3.20	Tráfego wireshark evento 2 . . . . .	21
3.21	Vulnerabilidade <i>Critical</i> . . . . .	22
3.22	Vulnerabilidade <i>High</i> . . . . .	23

3.23 Vulnerabilidade <i>Medium</i> . . . . .	23
--	----

# 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 grande 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 ferramentas 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 definição 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 processo 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 processo 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 pertinentes. 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 recorreremos ao site *sync.me* de modo a descobrir a quem pertencem estes contactos.

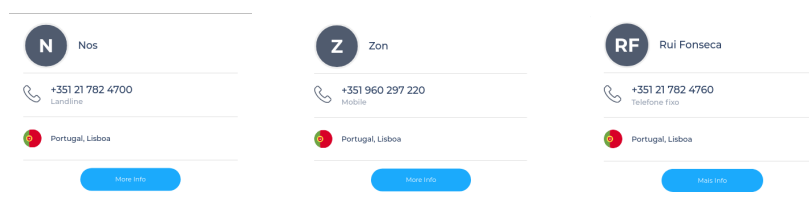


Figure 2.2: Contactos associados à Nos

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*.

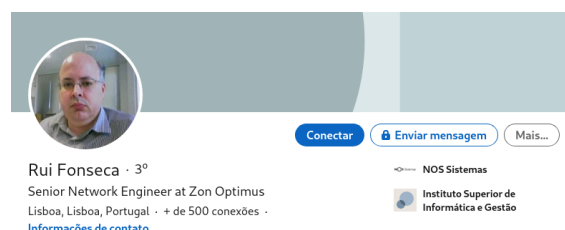


Figure 2.3: LinkedIn Rui Fonseca

```

ap@pop-os:~$ sudo whois 212.113.183.252
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

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

% Information related to '212.113.179.0 - 212.113.188.225'

% Abuse contact for '212.113.179.0 - 212.113.188.225' is 'abuse@nos.pt'

inetnum:        212.113.179.0 - 212.113.188.225
netname:        NOS
descr:          NOS COMUNICACOES S.A.
country:        PT
admin-c:        NOSA2-RIPE
tech-c:         NOST1-RIPE
status:         ASSIGNED PA
remarks:        ABUSE REPORTS MUST BE SEND TO ABUSE@NOS.PT
mnt-by:         AS2860-MNT
created:        2013-08-08T15:26:30Z
last-modified:  2019-02-22T12:14:06Z
source:         RIPE # Filtered

role:           NOS COMUNICACOES Admin Contact
address:        Edif Campo Grande
address:        Rua Ator Antonio Silva, 9
address:        Campo Grande
address:        1600-404 Lisboa
phone:          +351 217824700
phone:          +351 217914800
fax-no:         +351 217914850
org:            ORG-TPS1-RIPE
tech-c:         NOST1-RIPE
nic-hdl:        NOSA2-RIPE
abuse-mailbox:  abuse@nos.pt
mnt-by:         AS2860-MNT
created:        2014-10-07T14:39:50Z
last-modified:  2019-05-03T15:25:00Z
source:         RIPE # Filtered

role:           NOS COMUNICACOES Tech Contact
address:        Edif Campo Grande
address:        Rua Ator Antonio Silva, 9
address:        Campo Grande
address:        1600-404 Lisboa
phone:          +351 217824760
phone:          +351 217914800
fax-no:         +351 217824896
org:            ORG-TPS1-RIPE
admin-c:        NOSA2-RIPE
nic-hdl:        NOST1-RIPE
abuse-mailbox:  abuse@nos.pt
mnt-by:         AS2860-MNT
created:        2014-10-07T14:43:17Z
last-modified:  2019-05-03T15:24:19Z
source:         RIPE # Filtered

% Information related to '212.113.160.0/19AS2860'

route:          212.113.160.0/19
descr:          NOS COMUNICACOES S.A.
origin:         AS2860
mnt-by:         AS2860-MNT
created:        2014-10-28T10:35:04Z
last-modified:  2014-10-28T10:35:04Z
source:         RIPE # Filtered

```

Figure 2.4: whois 212.113.183.252

### 2.2.3 Comando *nmap -O*

De modo a obter informações sobre os sistemas 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.



```

p@pop-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.

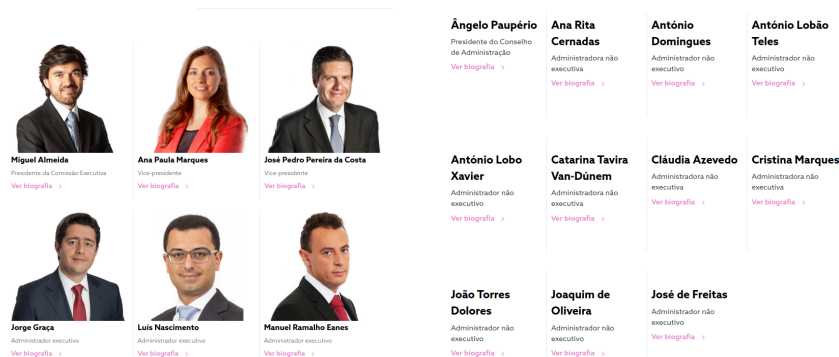


Figure 2.6: Administradores executivos e não executivos

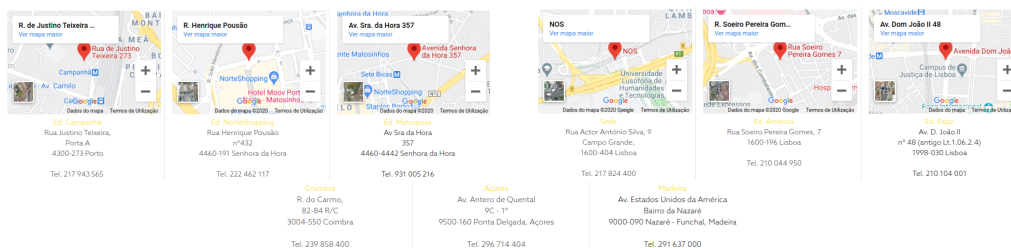


Figure 2.7: Moradas dos diferentes Polos

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.

**Perfil pretendido:**

- Mestrado/Licenciatura nas áreas de Telecomunicações ou Tecnologias de Informação;
- Mínimo de 7 anos de experiência profissional em funções similares, de preferência em um Operador Telecomunicações/ISP, vendedor ou integrador de sistemas;
- Experiência em Tecnologias de Rede e Segurança, nomeadamente Cisco, Checkpoint/Palo Alto/Fortinet, F5/Citrix/A10;
- Certificações Cisco e/ou Juniper;
- Experiência na gestão de equipas técnicas;
- Experiência em projetos SDN e NFV;
- Experiência em soluções/serviços Cloud;
- Facilidade de relacionamento e espírito de equipa;
- Autonomia na resolução de problemas e tomada de decisões;
- Sentido de organização e capacidade de gestão de projetos complexos.

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.

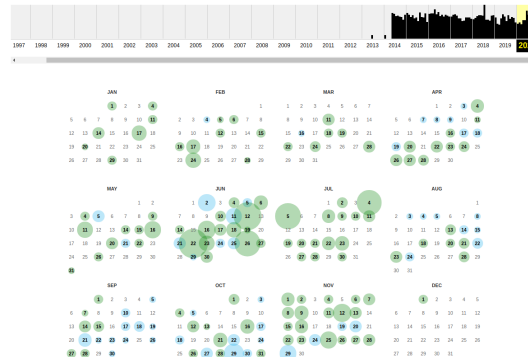


Figure 2.9: WayBackMachine

### 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 utilizadas no TLS *Handshake*, que é imune à vulnerabilidade *Heartbleed*, conseguimos ver quais as configurações criptográficas utilizadas (DHE) e os certificados utilizados entre comunicações.

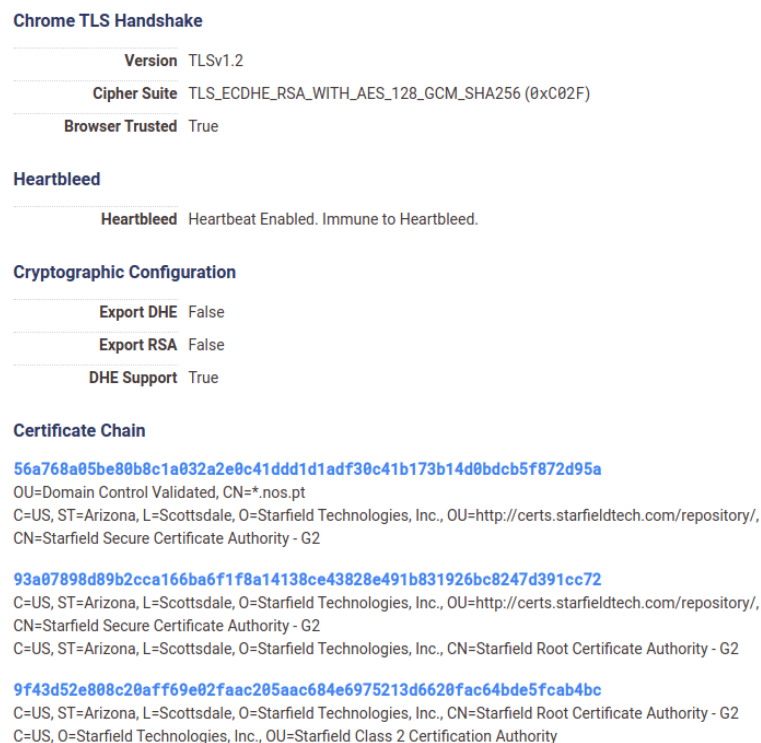


Figure 2.10: Censys

## 2.3 Fonotel

O negócio local escolhido para o desenvolvimento deste trabalho foi a empresa Fonotel. 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 pertinentes. 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 fonotel.pt
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-07 15:31 WET
Nmap scan report for fonotel.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 fonotel.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 decrifições. 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 Fonotel. Os contactos/moradas e outras informações obtidas com *whois* também pertencem à dominios.pt.

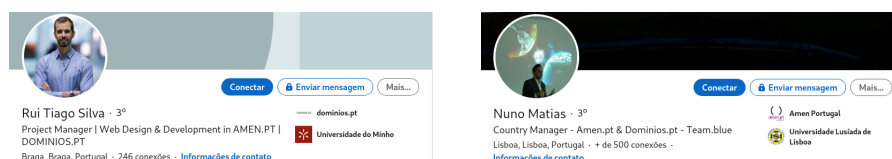


Figure 2.12: LinkedIn de indivíduos da dominios.pt

```

sp@pop-os:~$ whois 185.12.116.72
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf
%
% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.
%
% Information related to '185.12.116.0 - 185.12.119.254'
% Abuse contact for '185.12.116.0 - 185.12.119.254' is 'abuse@dominios.pt'

inetnum:        185.12.116.0 - 185.12.119.254
netname:        PT-DOMINIOS
country:        PT
admin-c:        NM7741-RIPE
tech-c:         RS23681-RIPE
status:         ASSIGNED PA
mnt-by:         mnt-pt-dominios-1
mnt-routes:     AS8975-MNT
mnt-routes:     AS8426-MNT
created:        2013-12-13T02:14:55Z
last-modified:  2019-12-18T13:55:25Z
source:        RIPE

person:         Nuno Matias
address:        PARQUE MULTIUSOS, AREAL GORDO, LOTE 3-A
address:        8005-409
address:        Faro
address:        PORTUGAL
phone:          +351210081081
nic-hdl:        NM7741-RIPE
mnt-by:         mnt-pt-dominios-1
created:        2019-05-06T07:33:57Z
last-modified:  2019-05-06T07:33:58Z
source:        RIPE

person:         Rui Silva
address:        PARQUE MULTIUSOS, AREAL GORDO, LOTE 3-A
address:        8005-409
address:        Faro
address:        PORTUGAL
phone:          +351210081081
nic-hdl:        RS23681-RIPE
mnt-by:         mnt-pt-dominios-1
created:        2019-05-06T07:33:57Z
last-modified:  2019-05-06T07:33:58Z
source:        RIPE

% Information related to '185.12.116.0/22AS33876'

route:          185.12.116.0/22
descr:          PT-DOMINIOS
origin:         AS33876
mnt-by:         CLARANET-MNT
mnt-by:         mnt-pt-dominios-1
created:        2019-05-13T15:21:10Z
last-modified:  2019-12-19T09:07:27Z
source:        RIPE

% This query was served by the RIPE Database Query Service version 1.98 (ANGUS)

```

Figure 2.13: whois 185.12.116.72

### 2.3.3 Comando *nmap -O*

De modo a obter informações sobre os sistemas 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.

```

margarida@kali:~$ sudo nmap -O 185.12.116.72
[sudo] senha para margarida:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-07 16:12 WET
Nmap scan report for cpanel72.dnscpanel.com (185.12.116.72)
Host is up (0.013s latency).
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
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Linux 3.X|4.X (92%)
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
Aggressive OS guesses: Linux 3.2 - 4.9 (92%), Linux 4.0 (91%), Linux 3.10 - 3.16 (90%), Linux 3.10 - 3.12 (89%), L
inux 4.4 (89%), Linux 3.10 (88%), Linux 4.9 (87%)
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 9.43 seconds

```

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 pertinentes 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.

FONETEL   Barqueiros	FONETEL   Amorim
<b>Horário Funcionamento</b>	<b>Horário Funcionamento</b>
2ª a 6ª Feira	2ª a 6ª Feira
9:30h - 12:30h, 14:00h - 19:30h	9:30h - 12:30h, 14:30h - 19:30h
<b>Sábados</b>	<b>Sábados</b>
09:30 - 12:30, 14:00 - 17:30	09:30 - 12:30, 14:00 - 17:30
<b>Domingos e Feriados</b> - Encerrada	<b>Domingos e Feriados</b> - Encerrada
<b>Contactos</b>	<b>Contactos</b>
Telefone: 253 857 158	Telefone: 252 602 086
Telemóvel: 919 261 484	Telemóvel: 960 375 277
Email: geral@fonetel.pt	Email: geral@fonetel.pt
<b>Morada</b>	<b>Morada</b>
Avenida Arcebispo Dom Gaspar de Bragança nº29 loja 2, Barqueiros, 4740-674 Barqueiros	Rua do Padre Alexandre Faria Barros, Amorim, 4495-140 Amorim



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 utilizadas 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.

<b>Chrome TLS Handshake</b>	
Version	TLSv1.2
Cipher Suite	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xC02F)
Browser Trusted	True
<b>Heartbleed</b>	
Heartbleed	Heartbeat Disabled (OK)
<b>Cryptographic Configuration</b>	
Export DHE	False
Export RSA	False
DHE Support	False
<b>Certificate Chain</b>	
83dada7c7ab9ba687f5765bdb76439c51e53e4a20af299d7f994828d9ed34bf	
CN=135milímetros.pt	
C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3	
25847d668eb4f04fdd40b12b6b0740c567da7d024308eb6c2c96fe41d9de218d	
C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3	
O=Digital Signature Trust Co., CN=DST Root CA X3	

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 gerenciado 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 executado o comando da figura seguinte:

```
C:\Users\vagrant>netsh int ip set address "local area connection" static 172.20.13.2 255.255.255.0 172.20.13.1
```

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:

```
C:\Users\vagrant>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::bc01:7362:11b3:e8%11
    IPv4 Address. . . . . : 172.20.13.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 172.20.13.1

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  . :
```

Figure 3.2: ipconfig

```
np@np:~/Desktop$ ping 172.20.13.2
PING 172.20.13.2 (172.20.13.2) 56(84) bytes of data.
64 bytes from 172.20.13.2: icmp_seq=1 ttl=128 time=1.76 ms
64 bytes from 172.20.13.2: icmp_seq=2 ttl=128 time=0.919 ms
64 bytes from 172.20.13.2: icmp_seq=3 ttl=128 time=1.00 ms
64 bytes from 172.20.13.2: icmp_seq=4 ttl=128 time=0.849 ms
64 bytes from 172.20.13.2: icmp_seq=5 ttl=128 time=0.828 ms
64 bytes from 172.20.13.2: icmp_seq=6 ttl=128 time=1.45 ms
64 bytes from 172.20.13.2: icmp_seq=7 ttl=128 time=0.883 ms
64 bytes from 172.20.13.2: icmp_seq=8 ttl=128 time=1.02 ms
64 bytes from 172.20.13.2: icmp_seq=9 ttl=128 time=2.16 ms
64 bytes from 172.20.13.2: icmp_seq=10 ttl=128 time=0.918 ms
64 bytes from 172.20.13.2: icmp_seq=11 ttl=128 time=4.68 ms
64 bytes from 172.20.13.2: icmp_seq=12 ttl=128 time=1.31 ms
^C
--- 172.20.13.2 ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 11053ms
rtt min/avg/max/mdev = 0.828/1.481/4.681/1.043 ms
```

Figure 3.3: ping 172.20.13.2

```
C:\Users\vagrant>ping 172.20.13.1

Pinging 172.20.13.1 with 32 bytes of data:
Reply from 172.20.13.1: bytes=32 time=1ms TTL=64
Reply from 172.20.13.1: bytes=32 time<1ms TTL=64
Reply from 172.20.13.1: bytes=32 time=1ms TTL=64
Reply from 172.20.13.1: bytes=32 time=1ms TTL=64

Ping statistics for 172.20.13.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

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.

```
hpa@mp:~$ nmap -sV 172.20.13.2
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-18 14:03 WET
Nmap scan report for 172.20.13.2
Host is up (0.0021s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE          VERSION
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds     Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3000/tcp  open  http             WEBrick httpd 1.3.1 (Ruby 2.3.3 (2016-11-21))
3389/tcp  open  ssl/ms-wbt-server?
49152/tcp open  msrpc            Microsoft Windows RPC
49153/tcp open  msrpc            Microsoft Windows RPC
49154/tcp open  msrpc            Microsoft Windows RPC
49155/tcp open  msrpc            Microsoft Windows RPC
49156/tcp open  msrpc            Microsoft Windows RPC
49157/tcp open  msrpc            Microsoft Windows RPC
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 64.10 seconds
```

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.

Vulnerability Details : [CVE-2018-8407](#)

An information disclosure vulnerability exists when "Kernel Remote Procedure Call Provider" driver improperly initializes objects in memory, aka "MSRPC Information Disclosure Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers.

Publish Date : 2018-11-13 Last Update Date : 2018-12-13

[Collapse All](#) [Expand All](#) [Select](#) [Select&Copy](#) [Scroll To](#) [Comments](#) [External Links](#)  
[Search Twitter](#) [Search YouTube](#) [Search Google](#)

– CVSS Scores & Vulnerability Types

CVSS Score	<b>2.1</b>
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	None (There is no impact to the integrity of the system.)
Availability Impact	None (There is no impact to the availability of the system.)
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)	Obtain Information
CWE ID	<a href="#">200</a>

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 : <a href="#">CVE-2017-0174</a>	
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	
<a href="#">Collapse All</a> <a href="#">Expand All</a> <a href="#">Select</a> <a href="#">Select&amp;Copy</a> <a href="#">Scroll To</a> <a href="#">Comments</a> <a href="#">External Links</a> <a href="#">Search Twitter</a> <a href="#">Search YouTube</a> <a href="#">Search Google</a>	
- CVSS Scores & Vulnerability Types	
CVSS Score	<b>6.1</b>
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	<b>Complete</b> (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	<b>Low</b> (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	<b>Not required</b> (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 : <a href="#">CVE-2012-2556</a>	
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	
<a href="#">Collapse All</a> <a href="#">Expand All</a> <a href="#">Select</a> <a href="#">Select&amp;Copy</a> <a href="#">Scroll To</a> <a href="#">Comments</a> <a href="#">External Links</a> <a href="#">Search Twitter</a> <a href="#">Search YouTube</a> <a href="#">Search Google</a>	
- CVSS Scores & Vulnerability Types	
CVSS Score	<b>9.3</b>
Confidentiality Impact	<b>Complete</b> (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	<b>Complete</b> (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	<b>Complete</b> (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	<b>Medium</b> (The access conditions are somewhat specialized. Some preconditions must be satisfied to exploit)
Authentication	<b>Not required</b> (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Execute Code
CWE ID	<a href="#">24</a>

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 : <a href="#">CVE-2018-8777</a>	
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	
<a href="#">Collapse All</a> <a href="#">Expand All</a> <a href="#">Select</a> <a href="#">Select&amp;Copy</a> <a href="#">Scroll To</a> <a href="#">Comments</a> <a href="#">External Links</a> <a href="#">Search Twitter</a> <a href="#">Search YouTube</a> <a href="#">Search Google</a>	
- CVSS Scores & Vulnerability Types	
CVSS Score	<b>5.0</b>
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	<b>Partial</b> (There is reduced performance or interruptions in resource availability.)
Access Complexity	<b>Low</b> (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	<b>Not required</b> (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Denial Of Service
CWE ID	<a href="#">400</a>

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 interceptando *handshakes* e injetando conteúdo.

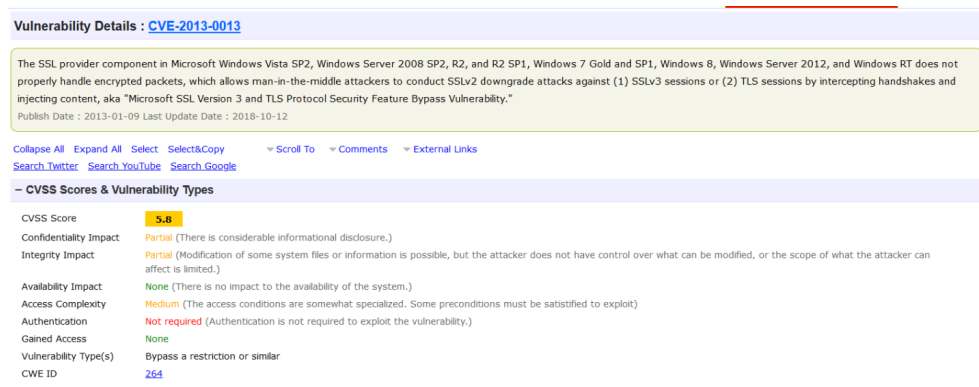


Figure 3.10: CVE-2013-0013

## 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, recorreremos ao Nessus. Fazendo o *basic scan* ao *host*: 120.20.13.2 obtivemos os seguintes resultados:

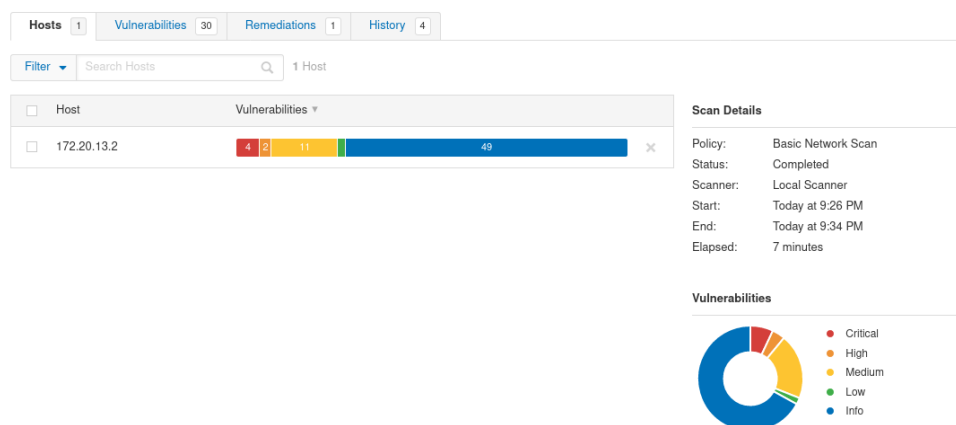


Figure 3.11: Network Scan

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

- 4 vulnerabilidades críticas
- 2 vulnerabilidades altas
- 11 vulnerabilidades médias
- 1 vulnerabilidade baixa
- 49 informações

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

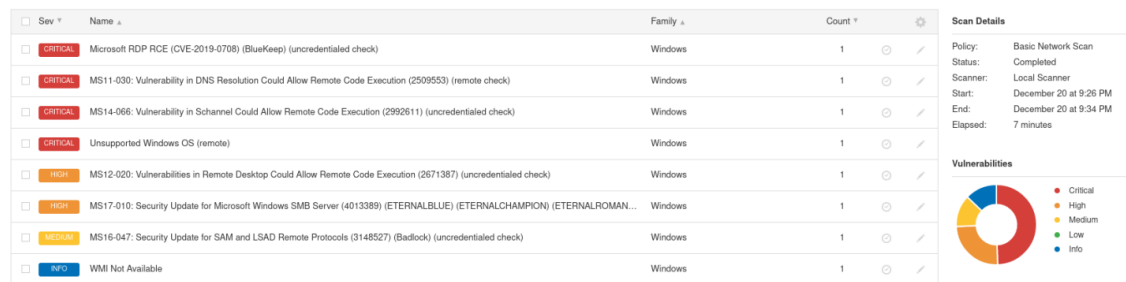


Figure 3.12: Vulnerabilidades Nessus

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.

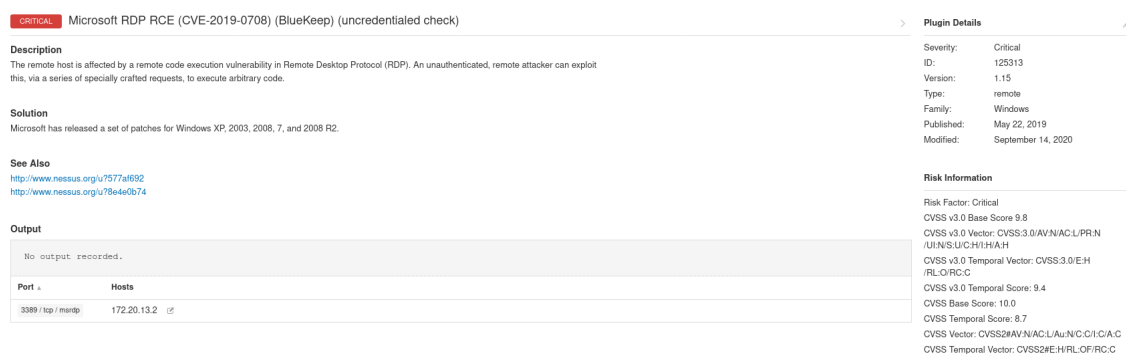


Figure 3.13: Vulnerabilidade crítica

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:0x0 ID:0 IpLen:20 DgmLen:48 DF
*****S* Seq: 0xE4203344 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/-IDS1111]
```

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 *Denial 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 *Denial 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	38.930160083	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	38.930824098	172.20.13.1	172.20.13.2	TCP	62	6163	→	10959	[SYN]	Seq=0	Win=4096	Len=0	MSS=1460	SACK_PERM=1
4355	38.931089148	172.20.13.1	172.20.13.2	TCP	62	35867	→	27605	[SYN]	Seq=0	Win=4096	Len=0	MSS=1460	SACK_PERM=1
4356	38.931083667	172.20.13.1	172.20.13.2	TCP	62	49027	→	28091	[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	38.932899347	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	38.933528368	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:0x0 ID:0 IPLen:20 DgmLen:48 DF
*****S* Seq: 0x46363934 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]
```

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 *Denial of Service* ou ganhar privilégios através de *GetRequest*, *GetNextRequest* e *SetRequest messages*.

**Vulnerability Details : CVE-2002-0013**

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.

Publish Date : 2002-02-13 Last Update Date : 2018-10-12

[Collapse All](#) [Expand All](#) [Select](#) [Select&Copy](#) [Scroll To](#) [Comments](#) [External Links](#)  
[Search Twitter](#) [Search YouTube](#) [Search Google](#)

**CVSS Scores & Vulnerability Types**

CVSS Score **10.0**

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 **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 **Admin**

Vulnerability Type(s) **Denial Of Service Gain privileges**

CWE ID **264**

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 privilégios através de SNMPv1 *trap handling*.

**Vulnerability Details : CVE-2002-0012**

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.

Publish Date : 2002-02-13 Last Update Date : 2018-10-12

[Collapse All](#) [Expand All](#) [Select](#) [Select&Copy](#) [Scroll To](#) [Comments](#) [External Links](#)  
[Search Twitter](#) [Search YouTube](#) [Search Google](#)

**CVSS Scores & Vulnerability Types**

CVSS Score **10.0**

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 **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 **Admin**

Vulnerability Type(s) **Denial Of Service Gain privileges**

CWE ID **264**

**Additional Vendor Supplied Data**

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:

No.	Time	Source	Destination	Protocol	Length	Info
5773	39.501521907	172.20.13.1	172.20.13.2	TCP	62	24211 → 20012 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
5774	39.501862616	172.20.13.1	172.20.13.2	TCP	62	41942 → 27008 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
5775	39.502676489	172.20.13.1	172.20.13.2	TCP	62	40567 → 40841 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
5776	39.503095405	172.20.13.1	172.20.13.2	TCP	62	27443 → 41795 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
5777	39.503340657	172.20.13.1	172.20.13.2	TCP	62	2839 → 3 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
5778	39.503657617	172.20.13.1	172.20.13.2	TCP	62	57666 → 56 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
5779	39.503964229	172.20.13.1	172.20.13.2	TCP	62	28040 → 109 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
5780	39.504323249	172.20.13.1	172.20.13.2	TCP	62	32889 → 162 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
5781	39.504698166	172.20.13.1	172.20.13.2	TCP	62	34468 → 215 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
5782	39.505019425	172.20.13.1	172.20.13.2	TCP	62	43489 → 268 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
5783	39.505324222	172.20.13.1	172.20.13.2	TCP	62	30130 → 321 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
5784	39.505628747	172.20.13.1	172.20.13.2	TCP	62	64876 → 374 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
5785	39.505932955	172.20.13.1	172.20.13.2	TCP	62	61164 → 427 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
5786	39.506398634	172.20.13.1	172.20.13.2	TCP	62	55146 → 480 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
5787	39.506937533	172.20.13.1	172.20.13.2	TCP	62	40220 → 533 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
5788	39.509129717	172.20.13.1	172.20.13.2	TCP	62	59740 → 586 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
5789	39.509438271	172.20.13.1	172.20.13.2	TCP	62	4976 → 639 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1

```

Frame 5780: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface eth1, id 0
  Interface id: 0 (eth1)
  Encapsulation type: Ethernet (1)
  Arrival Time: Dec 21, 2020 15:24:43.483279954 WET
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1608964283.483279954 seconds
  [Time delta from previous captured frame: 0.000359029 seconds]
  [Time delta from previous displayed frame: 0.000359029 seconds]
  [Time since reference or first frame: 39.504323249 seconds]
  Frame Number: 5780
  Frame Length: 62 bytes (496 bits)
  Capture Length: 62 bytes (496 bits)
  [Frame is marked: False]
  [Frame is ignored: False]

```

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 vulnerabilidades 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:

**CRITICAL** Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)

**Description**  
The remote host is affected by a remote code execution vulnerability in Remote Desktop Protocol (RDP). An unauthenticated, remote attacker can exploit this, via a series of specially crafted requests, to execute arbitrary code.

**Solution**  
Microsoft has released a set of patches for Windows XP, 2003, 2008, 7, and 2008 R2.

**See Also**  
<http://www.nessus.org/u?577a1692>  
<http://www.nessus.org/u?8e4e0b74>

**Output**  
No output recorded.

Port	Hosts
3389 / rdp / mrdp	172.20.13.2

**Plugin Details**

Severity: Critical  
ID: 125313  
Version: 1.15  
Type: remote  
Family: Windows  
Published: May 22, 2019  
Modified: September 14, 2020

**Risk Information**

Risk Factor: Critical  
CVSS v3.0 Base Score: 9.8  
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H  
CVSS v3.0 Temporal Vector: CVSS:3.0/E:H/RL:Q/RC:C  
CVSS v3.0 Temporal Score: 9.4  
CVSS Base Score: 10.0  
CVSS Temporal Score: 8.7  
CVSS Vector: CVSS:3.0/AV:N/AC:L/Au:N/C:H/I:C/A:C  
CVSS Temporal Vector: CVSS:3.0/E:H/RL:Q/RC:C

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.

High

MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (uncredentialed check)

Severity: High

ID: 58435

Version: 1.59

Type: remote

Family: Windows

Published: March 22, 2012

Modified: September 14, 2020

Risk Information

Risk Factor: High

CVSS Base Score: 9.3

CVSS Temporal Score: 7.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:V

CVSS Temporal Vector: CVSS2#E:POC/RL:OF/RC:C

IAVM Severity: I

Vulnerability Information

CPE: cpe:/o:microsoft:windows

cpe:/a:microsoft:remote\_desktop\_protocol

Exploit Available: true

Exploit Ease: Exploits are available

Patch Pub Date: March 13, 2012

Vulnerability Pub Date: March 13, 2012

Description

An arbitrary remote code vulnerability exists in the implementation of the Remote Desktop Protocol (RDP) on the remote Windows host. The vulnerability is due to the way that RDP accesses an object in memory that has been improperly initialized or has been deleted.

If RDP has been enabled on the affected system, an unauthenticated, remote attacker could leverage this vulnerability to cause the system to execute arbitrary code by sending a sequence of specially crafted RDP packets to it.

This plugin also checks for a denial of service vulnerability in Microsoft Terminal Server.

Note that this script does not detect the vulnerability if the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting is enabled or the security layer is set to 'SSL (TLS 1.0)' on the remote host.

Solution

Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2.

Note that an extended support contract with Microsoft is required to obtain the patch for this vulnerability for Windows 2000.

See Also

<https://docs.microsoft.com/en-us/securityupdates/SecurityBulletins/2012/ms12-020>

Output

No output recorded.

Port	Hosts
3389 / tcp / rdp	172.20.13.2

- **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.

MEDIUM	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)	<div> <div>&lt;</div> <div>&gt;</div> <div>Plugin Details</div> </div>
<b>Description</b>  The remote Windows host is affected by an elevation of privilege vulnerability in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker able to intercept communications between a client and a server hosting a SAM database can exploit this to force the authentication level to downgrade, allowing the attacker to impersonate an authenticated user and access the SAM database.		<div> <div>Severity:</div> <div>Medium</div> </div> <div> <div>ID:</div> <div>90510</div> </div> <div> <div>Version:</div> <div>1.9</div> </div> <div> <div>Type:</div> <div>remote</div> </div> <div> <div>Family:</div> <div>Windows</div> </div> <div> <div>Published:</div> <div>April 13, 2016</div> </div> <div> <div>Modified:</div> <div>July 23, 2019</div> </div>
<b>Solution</b>  Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10.		<div> <div>Risk Information</div> </div>
<b>See Also</b>  <a href="http://www.nessus.org/u/752ade1e9">http://www.nessus.org/u/752ade1e9</a> <a href="http://badlock.org/">http://badlock.org/</a>		<div> <div>Risk Factor: Medium</div> </div>
		<div> <div>CVSS v3.0 Base Score: 6.8</div> </div>
		<div> <div>CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N</div> </div>
		<div> <div>CVSS v3.0 Temporal Score: CVSS:3.0/E:U/RL:O/RC:C</div> </div>
		<div> <div>CVSS v3.0 Temporal Score: 5.9</div> </div>
		<div> <div>CVSS Base Score: 5.8</div> </div>
		<div> <div>CVSS Temporal Score: 4.3</div> </div>
		<div> <div>CVSS Vector: CVSS2#AV:N/AC:M/A:N/C:P/I:P/A:N</div> </div>

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 respectivas 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.