

Curso de hacking tools: Blue Team

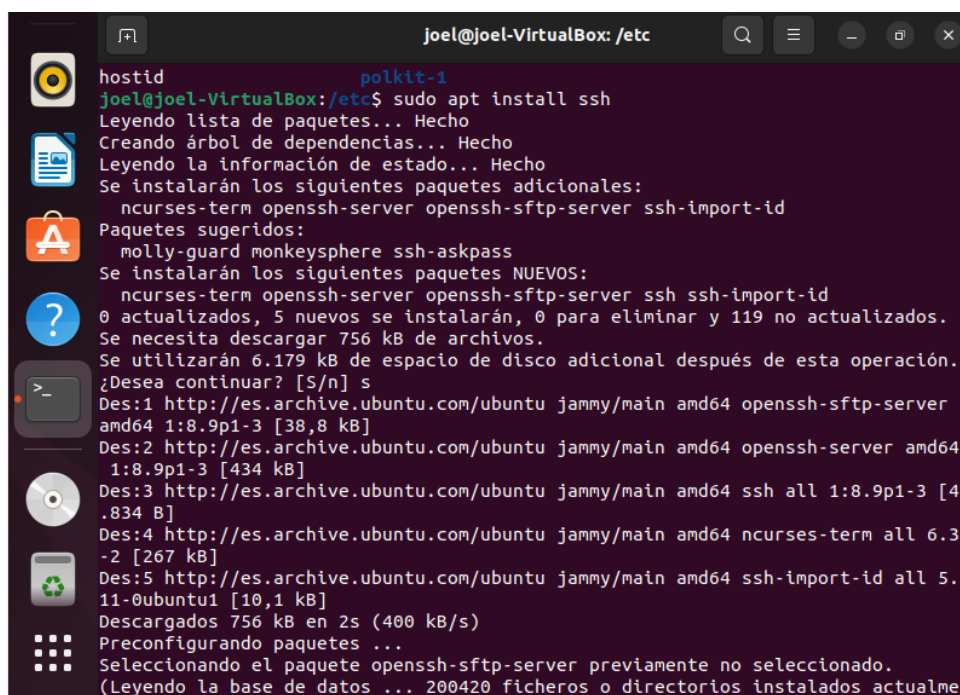
En este curso he aprendido sobre el manejo de Linux, creando conexiones remotas, servidor proxy-caché mediante Squid, IPTables, Metasploit.

Sobre el manejo de linux he repasado conceptos vistos durante el curso como la creación de usuarios, grupos, así como la gestión de permisos de los mismos.

En la parte de acceso remoto he aprendido a la creación de un acceso remoto evitando el uso de telnet ya que mediante este se establece una conexión insegura ya que es una conexión plana por lo cual si existiera un atacante realizando un ataque de man in the middle podría capturar esa información sin problema, utilizando ssh mediante la creación de una conexión por túnel.

Aquí una práctica

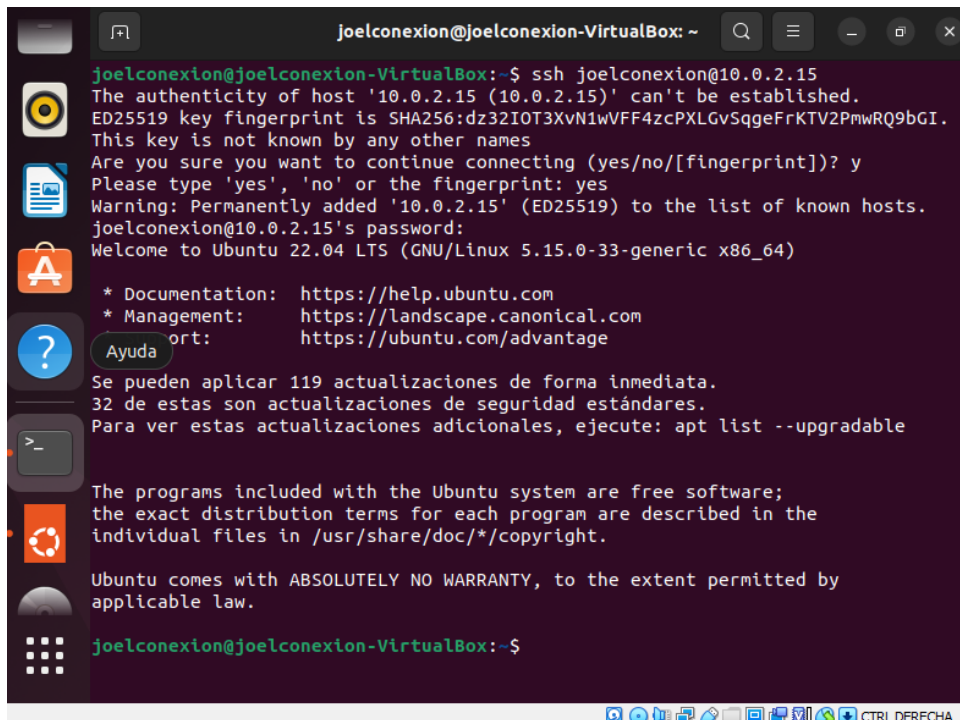
Primero instalmos ssh mediante `sudo apt install ssh`



```
joel@joel-VirtualBox: /etc
joel@joel-VirtualBox:~$ sudo apt install ssh
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
ncurses-term openssh-server openssh-sftp-server ssh-import-id
Paquetes sugeridos:
molly-guard monkeysphere ssh-askpass
Se instalarán los siguientes paquetes NUEVOS:
ncurses-term openssh-server openssh-sftp-server ssh ssh-import-id
0 actualizados, 5 nuevos se instalarán, 0 para eliminar y 119 no actualizados.
Se necesita descargar 756 kB de archivos.
Se utilizarán 6.179 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
Des:1 http://es.archive.ubuntu.com/ubuntu jammy/main amd64 openssh-sftp-server
amd64 1:8.9p1-3 [38,8 kB]
Des:2 http://es.archive.ubuntu.com/ubuntu jammy/main amd64 openssh-server amd64
1:8.9p1-3 [434 kB]
Des:3 http://es.archive.ubuntu.com/ubuntu jammy/main amd64 ssh all 1:8.9p1-3 [4
.834 B]
Des:4 http://es.archive.ubuntu.com/ubuntu jammy/main amd64 ncurses-term all 6.3
-2 [267 kB]
Des:5 http://es.archive.ubuntu.com/ubuntu jammy/main amd64 ssh-import-id all 5.
11-0ubuntu1 [10,1 kB]
Descargados 756 kB en 2s (400 kB/s)
Preconfigurando paquetes ...
Seleccionando el paquete openssh-sftp-server previamente no seleccionado.
(Leyendo la base de datos ... 200420 ficheros o directorios instalados actualme
```

Una vez instalado podríamos cambiar la configuración, como por ejemplo el puerto mediante el fichero `sshd_config`

Mediante `ssh nombreDeUsuario@ipServidor` nos podemos conectar al servidor creado



```
joelconexion@joelconexion-VirtualBox: ~  
joelconexion@joelconexion-VirtualBox:~$ ssh joelconexion@10.0.2.15  
The authenticity of host '10.0.2.15 (10.0.2.15)' can't be established.  
ED25519 key fingerprint is SHA256:dz32IOT3XvN1wVFF4zcPXLGvSqgeFrKTV2PmWRQ9bGI.  
This key is not known by any other names  
Are you sure you want to continue connecting (yes/no/[fingerprint])? y  
Please type 'yes', 'no' or the fingerprint: yes  
Warning: Permanently added '10.0.2.15' (ED25519) to the list of known hosts.  
joelconexion@10.0.2.15's password:  
Welcome to Ubuntu 22.04 LTS (GNU/Linux 5.15.0-33-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/advantage  
  
Se pueden aplicar 119 actualizaciones de forma inmediata.  
32 de estas son actualizaciones de seguridad estándares.  
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
joelconexion@joelconexion-VirtualBox:~$
```

Sobre squid he visto que es una herramienta para crear un servidor proxy-caché, esto es un servidor situado entre la máquina del usuario y otra red que actúa como protección separando las dos redes y como zona caché para acelerar el acceso a páginas web o poder restringir el acceso a contenidos.

Sus funciones más importantes son:

- Permite el acceso web a máquinas privadas (IP privada) que no están conectadas directamente a Internet.
- Controla el acceso web aplicando reglas.
- Registra el tráfico web desde la red local hacia el exterior.
- Controla el contenido web visitado y descargado.
- Controla la seguridad de la red local ante posibles ataques, intrusiones en el sistema, etc.
- Funciona como un caché de páginas web. Es decir, almacena las páginas web visitadas por los usuarios y de esta manera las puede enviar a otros usuarios sin tener que acceder a Internet de nuevo.
- Guarda en caché las peticiones DNS e implementa una caché para las conexiones fallidas.
- Registra logs de todas las peticiones.

Sus ventajas son las siguientes:

- Reduce los tiempos de respuesta.
- Si la página web que se solicita está en la caché del servidor, ésta se sirve sin necesidad de acceder de nuevo al servidor original, con lo cual se ahorra tiempo.
- Disminuye el tráfico en la red y el consumo de ancho de banda.
- Cortafuegos.
- Si la página web está almacenada en la caché del servidor, la petición no sale de la red local y no será necesario hacer uso de la línea exterior consiguiendo así un ahorro en la utilización del ancho de banda.

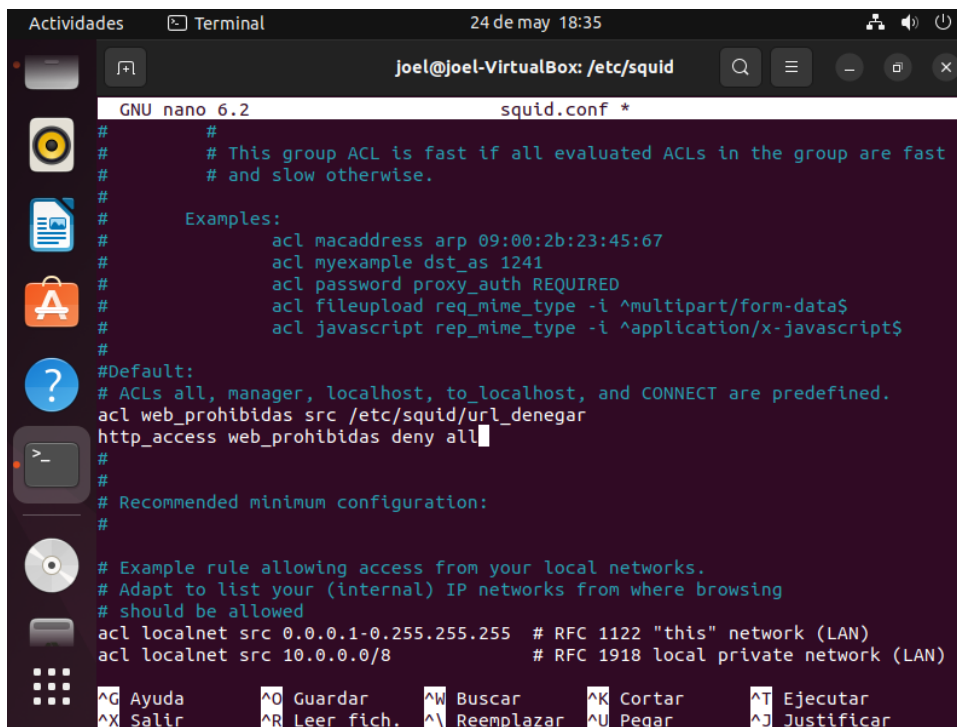
- Cuando se utiliza un servidor proxy-caché, éste comunica con el exterior, y puede funcionar como cortafuegos, lo cual aumentará la seguridad del usuario respecto a la información a la que se acceda.
- Filtrado de servicios.
- Es posible configurar el servidor proxy-caché dejando sólo disponibles aquellos servicios (HTTP, FTP...) que se consideren necesarios.
- Soporta el protocolo ICP que permite integrar cachés que colaboran y permite crear jerarquías de cachés y el intercambio de datos.

Una práctica con squid

En esta práctica el objetivo es denegar el acceso a ciertas páginas

Primero instalamos squid con `apt install squid`.

En el fichero `squid.conf` ponemos lo siguiente



The screenshot shows a terminal window titled 'joel@joel-VirtualBox: /etc/squid' with a nano 6.2 editor open to the file 'squid.conf'. The configuration includes several ACLs and an http_access rule. The terminal window has a dark theme and shows system icons on the left and top right.

```

#
# This group ACL is fast if all evaluated ACLs in the group are fast
# and slow otherwise.
#
Examples:
#
acl macaddress arp 09:00:2b:23:45:67
acl myexample dst_as 1241
acl password proxy_auth REQUIRED
acl fileupload req_mime_type -i ^multipart/form-data$
acl javascript rep_mime_type -i ^application/x-javascript$
#
#Default:
# ACLs all, manager, localhost, to_localhost, and CONNECT are predefined.
acl web_prohibidas src /etc/squid/url_denegar
http_access web_prohibidas deny all
#
# Recommended minimum configuration:
#
# Example rule allowing access from your local networks.
# Adapt to list your (internal) IP networks from where browsing
# should be allowed
acl localnet src 0.0.0.1-0.255.255.255 # RFC 1122 "this" network (LAN)
acl localnet src 10.0.0.0/8 # RFC 1918 local private network (LAN)

```

At the bottom of the terminal, there is a keyboard shortcuts menu:

^G Ayuda	^O Guardar	^W Buscar	^K Cortar	^T Ejecutar
^X Salir	^R Leer fich.	^A Reemplazar	^U Pegar	^J Justificar

Para volver a habilitar el acceso pondríamos `http_access allow all`

Después debemos configurar el proxy para cada usuario y con esto le estaríamos denegando el acceso a las páginas indicadas además de que nos quedaríamos con un log de sus acciones.

Sobre IPTables

- Es una utilidad de línea de órdenes para configurar el cortafuegos del kernel de Linux implementado como parte del proyecto Netfilter.
- El término iptables también se usa comúnmente para referirse a dicho cortafuegos del kernel.
- Puede configurarse directamente con iptables, o usando uno de los muchos frontends existentes de consola y gráficos.

- El término iptables se usa para IPv4, y el término ip6tables para IPv6.
- Tanto iptables como ip6tables tienen la misma sintaxis, pero algunas opciones son específicas de IPv4 o de IPv6.
- Para trabajar con iptables es necesario tener permisos administrativos, por lo que deberemos usar sudo.
- No hay un límite respecto de cuán anidadas pueden estar las cadenas.
- Hay tres cadenas básicas /INPUT, OUTPUT y FORWARD y el usuario puede crear tantas como desee.
- Una regla puede ser simplemente un puntero a una cadena.
- `--SYNTAXIS= -> iptables [tabla] [COMANDOS] reglas DESTINO`

1. Filter table (tabla de filtros). Esta tabla es por la cual pasan todos los paquetes sin distinción y es la responsable del filtrado. Contiene las siguientes cadenas:

a) INPUT: los paquetes que sean destinados al sistema atraviesan esta cadena.

b) OUTPUT: todos los paquetes que han sido creados por el sistema pasan por esta cadena.

c) FORWARD: todos los paquetes que simplemente pasan por el sistema para ser encaminados a su destino.

2. Nat table (tabla de traducción de direcciones de red).

- Esta tabla tiene a su encargo configurar las reglas de escritura de direcciones o de los puertos de los paquetes.

- El primer paquete que entre al sistema de cualquier conexión pasa a través de esta tabla; los veredictos determinan cómo van a reescribirse todos los paquetes de la conexión.

- Contiene las siguientes cadenas redefinidas:

a) PREROUTING chain (Cadena de PRERUTEO): los paquetes revisados en esta regla antes de que sea consultada del ruteo local, principalmente el DNT (destination-NAT).

b) POSTROUTING chain (Cadena de POSTRUTEO): los paquetes al salir pasan por esta cadena después de tomar la decisión del ruteo, principalmente el SNT (source-NAT).

c) OUTPUT chain (Cadena de SALIDA): permite hacer un DNAT solamente en los paquetes generados.

3. Mangle table (Tabla de destrozo): esta tabla ajusta las opciones de los paquetes. Todos los paquetes pasan por esta table. Está diseñada para fines avanzados, por eso todas las cadenas están pre definidas.

a) PREROUTING chain (Cadena de PRERUTEO): Todos los paquetes que logran entrar a este sistema, antes de que el ruteo decida si el paquete debe ser reenviado (cadena de REENVÍO) o si tiene destino local (Cadena de ENTRADA).

b) INPUT chain (Cadena de ENTRADA): Todos los paquetes destinados para este sistema pasan a través de esta cadena.

c) FORWARD chain (Cadena de REDIRECCIÓN): Todos los paquetes que exactamente pasan por este sistema pasan a través de esta cadena.

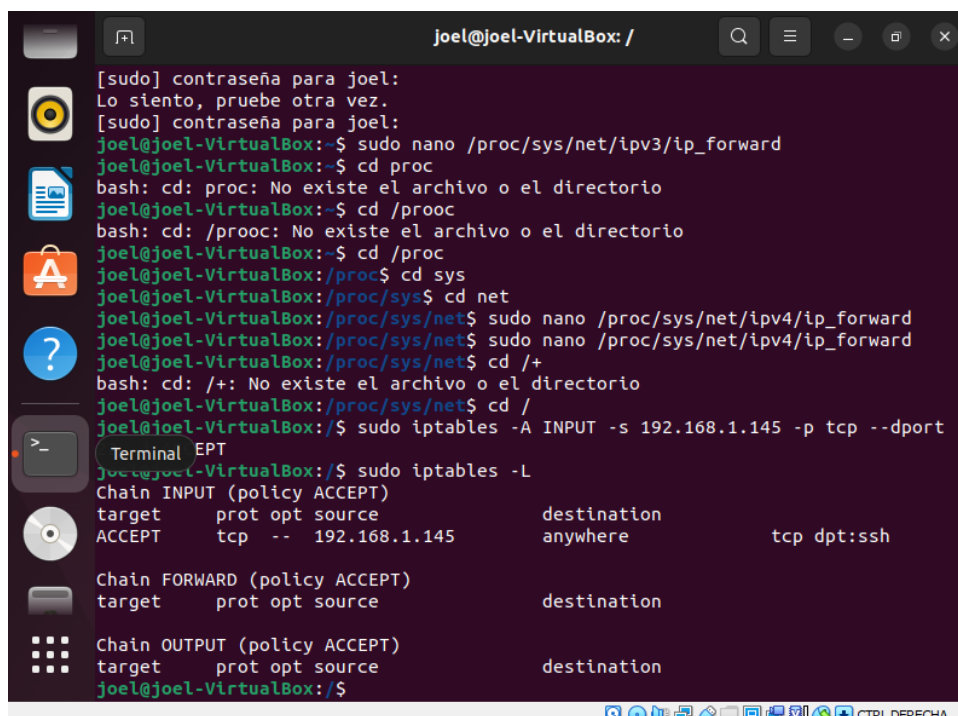
d) OUTPUT chain (Cadena de SALIDA): Todos los paquetes creados en este sistema pasan a través de esta cadena.

e) POSTROUTING chain (Cadena de POSTRUTEO): Todos los paquetes que abandonan este sistema a través de esta cadena. Además de las cadenas ya incorporadas, el usuario puede crear todas las cadenas definidas por el usuario que quiera dentro de cada tabla, las cuales permiten agrupar las reglas en forma lógica.

Práctica

Modificamos el archivo `ip_forward` y lo ponemos a 1

Creamos una regla con el comando `sudo iptables -A INPUT -s ipMaquinaQueConecta -p tcp -dport 22 -j ACCEPT`



```
joel@joel-VirtualBox: /  
[sudo] contraseña para joel:  
Lo siento, pruebe otra vez.  
[sudo] contraseña para joel:  
joel@joel-VirtualBox:~$ sudo nano /proc/sys/net/ipv3/ip_forward  
joel@joel-VirtualBox:~$ cd proc  
bash: cd: proc: No existe el archivo o el directorio  
joel@joel-VirtualBox:~$ cd /proc  
bash: cd: /proc: No existe el archivo o el directorio  
joel@joel-VirtualBox:~$ cd /proc  
joel@joel-VirtualBox:/proc$ cd sys  
joel@joel-VirtualBox:/proc/sys$ cd net  
joel@joel-VirtualBox:/proc/sys/net$ sudo nano /proc/sys/net/ipv4/ip_forward  
joel@joel-VirtualBox:/proc/sys/net$ sudo nano /proc/sys/net/ipv4/ip_forward  
joel@joel-VirtualBox:/proc/sys/net$ cd /+  
bash: cd: /+: No existe el archivo o el directorio  
joel@joel-VirtualBox:/proc/sys/net$ cd /  
joel@joel-VirtualBox:/$ sudo iptables -A INPUT -s 192.168.1.145 -p tcp --dport  
Terminal EPT  
joel@joel-VirtualBox:/$ sudo iptables -L  
Chain INPUT (policy ACCEPT)  
target    prot opt source                destination          tcp dpt:ssh  
ACCEPT    tcp  --  192.168.1.145          anywhere             tcp dpt:ssh  
  
Chain FORWARD (policy ACCEPT)  
target    prot opt source                destination  
  
Chain OUTPUT (policy ACCEPT)  
target    prot opt source                destination  
joel@joel-VirtualBox:/$
```

Podemos ver cómo ha aparecido lo añadido en la parte de INPUT

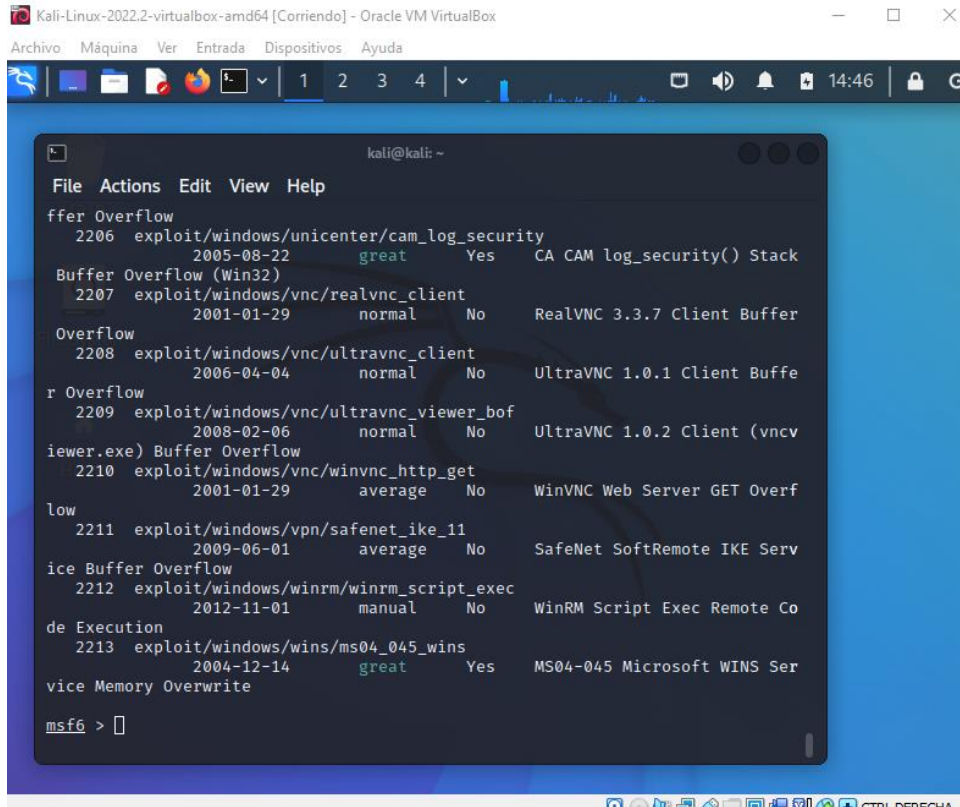
Metasploit es una herramienta que nos ayudará durante la etapa del hacking para atacar tanto a Linux como Windows

Debemos diferenciar exploit de payload

- Exploit: Su nombre viene de "Explotar", "Explotación", etc. Existen una serie de vulnerabilidades que como puntos débiles que son, si los forzamos y sabemos desarrollar conseguiremos vulnerar y por tanto tener acceso a sus recursos, datos, poder controlarlos, incluso destruirlos, etc.

- **Payload:** Es este software o código, que nos ayuda a aprovecharnos de las debilidades del sistema una vez que ya lo hemos vulnerado. Utilizando el ejemplo anterior, una vez que ya hemos accedido al fortín a través de la ventana abierta, el Payload será quien nos ayude a aprovechar la oportunidad que se nos presenta. Un payload nos ayudará a abrir las puertas que nos encontramos dentro de esta nueva habitación, otro nos ayudará a conseguir datos valiosos, otro a abrir otras ventanas para tener más accesos, etc.

Con el comando `show exploits` podremos buscar todos los exploits que existen en la base de datos



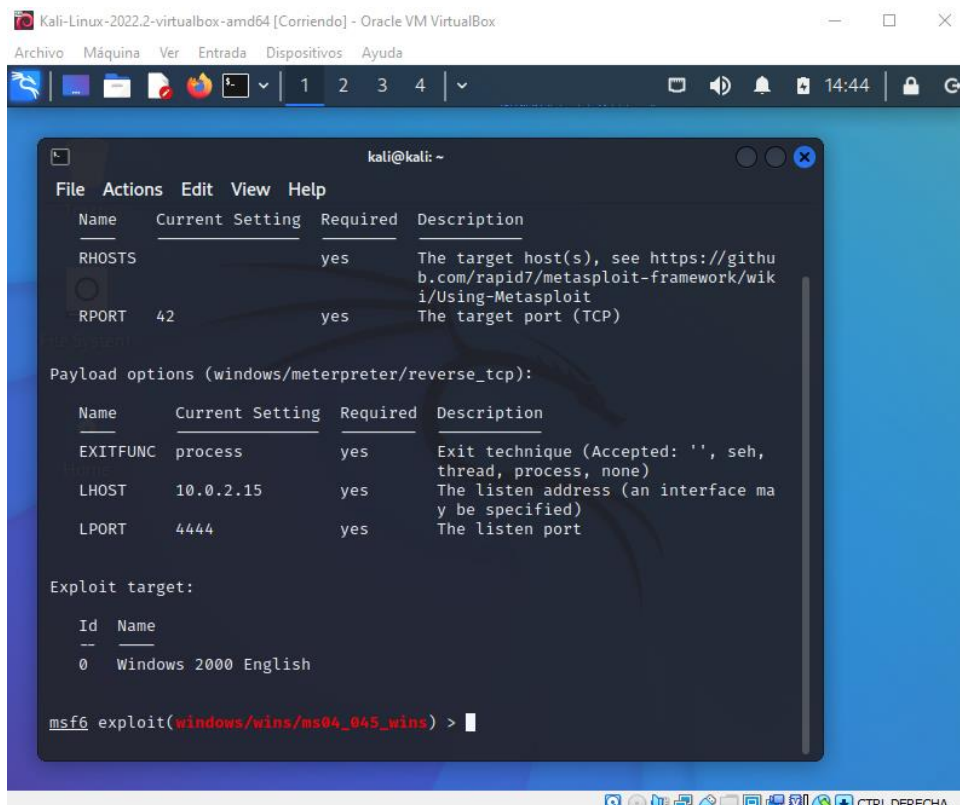
```

kali@kali: ~
File Actions Edit View Help
show exploits
2206 exploit/windows/unicenter/cam_log_security
      2005-08-22 great Yes CA CAM log_security() Stack
Buffer Overflow (Win32)
2207 exploit/windows/vnc/realvnc_client
      2001-01-29 normal No RealVNC 3.3.7 Client Buffer
Overflow
2208 exploit/windows/vnc/ultravnc_client
      2006-04-04 normal No UltraVNC 1.0.1 Client Buffer
r Overflow
2209 exploit/windows/vnc/ultravnc_viewer_bof
      2008-02-06 normal No UltraVNC 1.0.2 Client (vncv
viewer.exe) Buffer Overflow
2210 exploit/windows/vnc/winvnc_http_get
      2001-01-29 average No WinVNC Web Server GET Overf
low
2211 exploit/windows/vpn/safenet_ike_11
      2009-06-01 average No SafeNet SoftRemote IKE Serv
ice Buffer Overflow
2212 exploit/windows/winrm/winrm_script_exec
      2012-11-01 manual No WinRM Script Exec Remote Co
de Execution
2213 exploit/windows/wins/ms04_045_wins
      2004-12-14 great Yes MS04-045 Microsoft WINS Ser
vice Memory Overwrite
msf6 >

```

Una vez tengamos los exploits escogemos uno y utilizamos el comando `use`

Una vez usado el comando `use` utilizaremos el comando `options` para configurar el exploit y el payload (Si no aparece payload por defecto debemos buscar uno con `show payloads` e incluirlo).



Es importante tener persistencia para permanecer en el equipo atacado el mayor tiempo posible, para esto tenemos el backdoor

Se le domina como puerta trasera, cabe decir que se ejecuta un "Script" remoto a la máquina de la víctima con conexión puente al ordenador del atacante, para dejar al sistema vulnerable en escucha siempre.

El Backdoor persistente es compatible con todas las versiones de Windows.

Ejecutaremos el comando persistente meterpreter > run persistence

En python para pentesting he aprendido el uso de distintas librerías como Whois, DNS Python , Python Shodan para obtener información relevante

Aquí una práctica usando la librería whois y alguno de sus scripts predefinidos


```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ python  
Python 3.10.4 (main, Mar 24 2022, 13:07:27) [GCC 11.2.0] on linux  
Type "help", "copyright", "credits" or "license" for more information.  
>>> import whois  
>>> w = whois.whois('openwebinars.net')  
>>> w.expiration_date  
datetime.datetime(2023, 5, 24, 18, 9, 1)  
>>> w.text  
' Domain Name: OPENWEBINARS.NET\r\n Registry Domain ID: 1803645339_DOMAIN  
_NET-VRSN\r\n Registrar WHOIS Server: whois.namecheap.com\r\n Registrar U  
RL: http://www.namecheap.com\r\n Updated Date: 2022-04-24T07:29:41Z\r\n C  
reation Date: 2013-05-24T18:09:01Z\r\n Registry Expiry Date: 2023-05-24T18:  
09:01Z\r\n Registrar: NameCheap, Inc.\r\n Registrar IANA ID: 1068\r\n R  
egistrar Abuse Contact Email: abuse@namecheap.com\r\n Registrar Abuse Conta  
ct Phone: +1.6613102107\r\n Domain Status: clientTransferProhibited https://  
/icann.org/epp#clientTransferProhibited\r\n Name Server: EMMA.NS.CLOUDFLARE  
.COM\r\n Name Server: IVAN.NS.CLOUDFLARE.COM\r\n DNSSEC: unsigned\r\n U  
RL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/  
r\n>>> Last update of whois database: 2022-05-24T18:58:32Z <<<\r\n\r\nFor mor  
e information on Whois status codes, please visit https://icann.org/epp\r\n\r\n\nNOTICE: The expiration date displayed in this record is the date the\r\nreg  
istrar's sponsorship of the domain name registration in the registry is\r\nnc  
urrently set to expire. This date does not necessarily reflect the expiration  
\r\nndate of the domain name registrant's agreement with the sponsoring\r\nre  
gistrar. Users may consult the sponsoring registrar's Whois database to\r\nn  
view the registrar's reported date of expiration for this registration.\r\n\r\n'
```