

Curso introductorio de Ethical Hacking

Semana 03

Profesor: Randall Barnett Villalobos

Enumeración de servicios

Sesión 06

Etapa de Obtención de Acceso

Objetivo del módulo

- Poner en práctica temas vistos en semanas anteriores, como base para la introducción de nuevos temas de explotación de vulnerabilidades.
- Enumerar los servicios disponibles de la máquina virtual Mr Robot, para la verificación de cuáles son los más vulnerables.

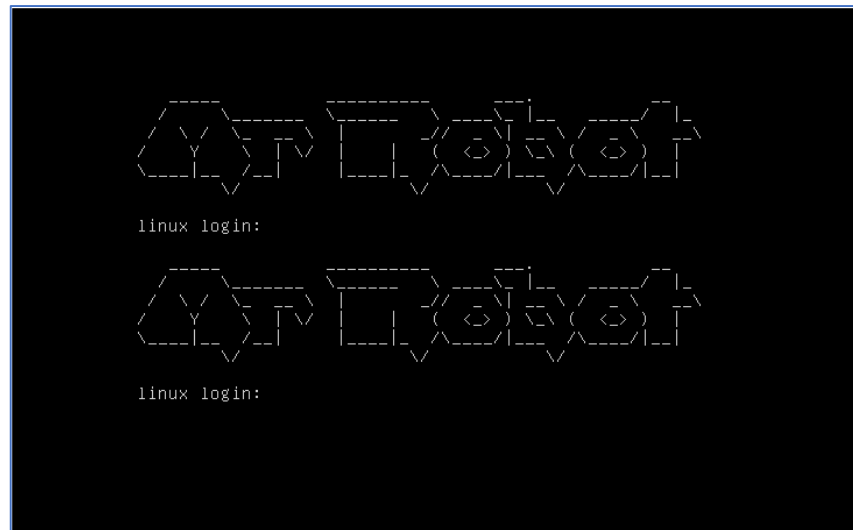


Proceso de enumeración de servicios

Uso de Nmap para enumerar los servicios disponibles.

Inicio de Mr. Robot

- El estudiante deberá iniciar la máquina virtual de Mr Robot.
- Una vez iniciada se encontrará con prompt como el siguiente:



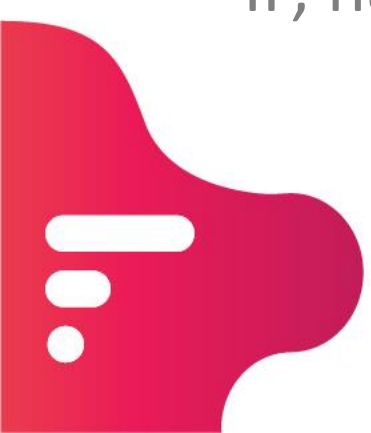
Inicio de Mr. Robot

- Puede notar que no hay pista evidente de un usuario o clave de acceso.
- Ni siquiera una pista del número de IP de la máquina virtual.
- Para obtener pistas, deberá iniciar su máquina virtual de Kali Linux.
- Y hacer un escaneo de la subred a la que pertenecen ambas máquinas. Para ello, debe realizar un ifconfig y luego con el dato de la IP, hacer el siguiente comando:



Inicio de Mr. Robot

- Puede notar que no hay pista evidente de un usuario o clave de acceso.
- Ni siquiera una pista del número de IP de la máquina virtual.
- Para obtener pistas, deberá iniciar su máquina virtual de Kali Linux.
- Y hacer un escaneo de la subred a la que pertenecen ambas máquinas. Para ello, debe realizar un ifconfig y luego con el dato de la IP, hacer el siguiente comando:



Enumeración de servicios

```
root@kali: ~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.22 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 fe80::20c:29ff:fe55:51d4 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:55:51:d4 txqueuelen 1000 (Ethernet)
    RX packets 142 bytes 13282 (12.9 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 178 bytes 15332 (14.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
```

xxx.xxx.xxx.0/24 ⇒ escanea el rango donde estamos.

-sS ⇒ ping TCP SYN

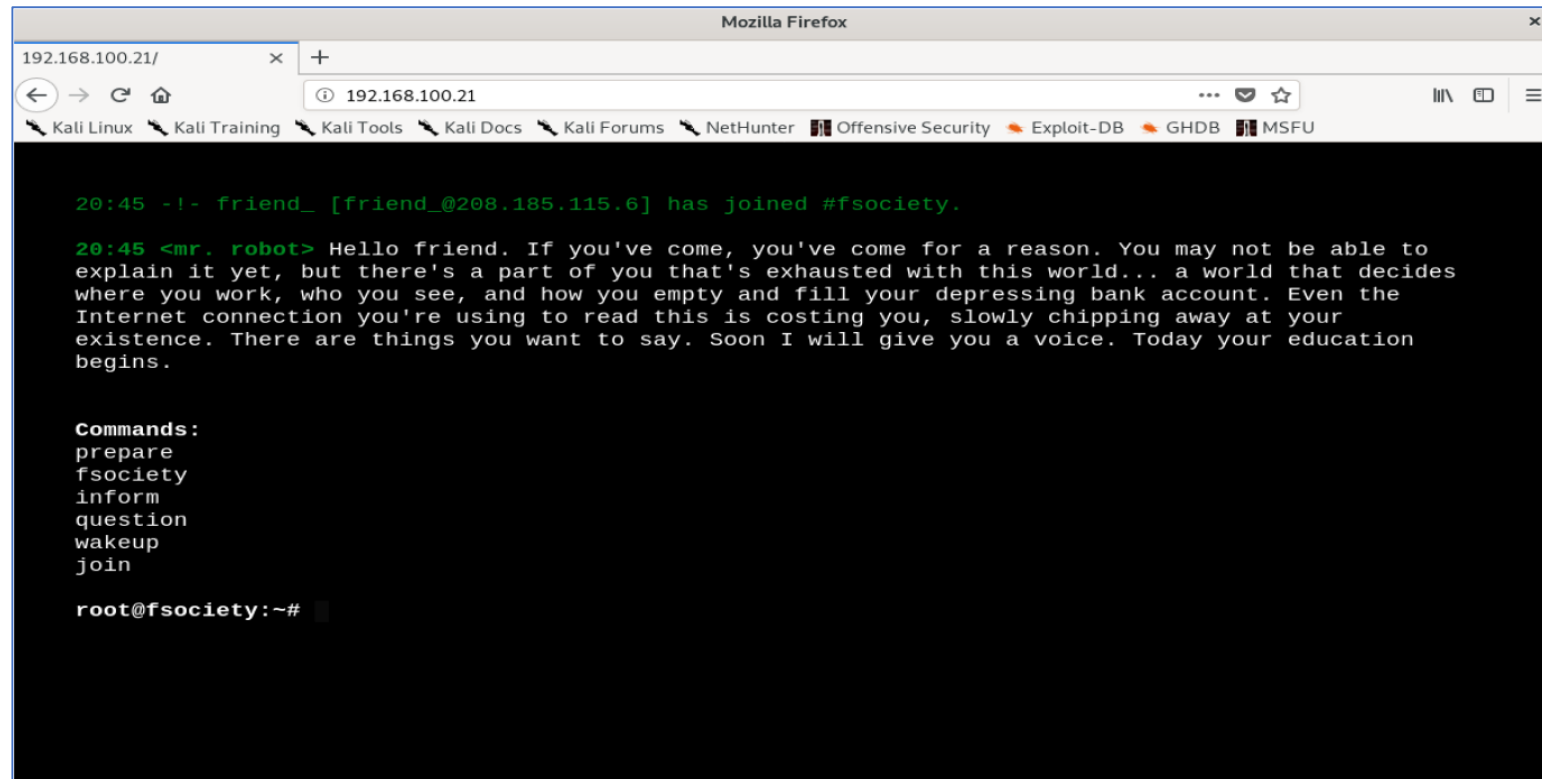
-T4 ⇒ velocidad del escaneo.

```
root@kali: ~# nmap -sS -T4 192.168.100.0/24
```

```
Nmap scan report for 192.168.100.21
Host is up (0.0014s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
22/tcp    closed ssh
80/tcp    open  http
443/tcp   open  https
MAC Address: 00:0C:29:E3:3B:6B (VMware)
```


Enumeración de servicios

- Dentro de los servicios descubiertos, se encuentra el HTTP.
- Por eso, trataremos de buscar alguna pista desde un browser:



The screenshot shows a Mozilla Firefox browser window with the address bar set to 192.168.100.21/. The browser's address bar and tabs show various links related to Kali Linux, Kali Training, Kali Tools, Kali Docs, Kali Forums, NetHunter, Offensive Security, Exploit-DB, GHDB, and MSFU. The main content area displays a terminal interface with a black background and green text. The terminal shows a message from a user named friend_ [friend_@208.185.115.6] who has joined the #fsociety channel. A message from a user named mr. robot follows, welcoming the user and explaining the purpose of the service. Below the message, a list of commands is displayed: prepare, fsociety, inform, question, wakeup, and join. The terminal prompt is root@fsociety:~#.

```
20:45 -!- friend_ [friend_@208.185.115.6] has joined #fsociety.

20:45 <mr. robot> Hello friend. If you've come, you've come for a reason. You may not be able to
explain it yet, but there's a part of you that's exhausted with this world... a world that decides
where you work, who you see, and how you empty and fill your depressing bank account. Even the
Internet connection you're using to read this is costing you, slowly chipping away at your
existence. There are things you want to say. Soon I will give you a voice. Today your education
begins.

Commands:
prepare
fsociety
inform
question
wakeup
join

root@fsociety:~#
```

Enumeración de servicios

- Una práctica muy común y útil, una vez descubierto un servicio de HTTP, es hacer una enumeración de directorios para buscar posibles contenidos en el sitio web provisto.
- Para lo anterior se puede utilizar la herramienta llamada: **dirb**
- El comando a utilizar sería el siguiente:
 - `dirb http://192.168.100.24`
- Recuerde que la IP dependerá de su propia red, lo anterior es solo un ejemplo.



```
root@kali:~# dirb http://192.168.100.24
```

```
-----  
DIRB v2.22  
By The Dark Raver  
-----
```

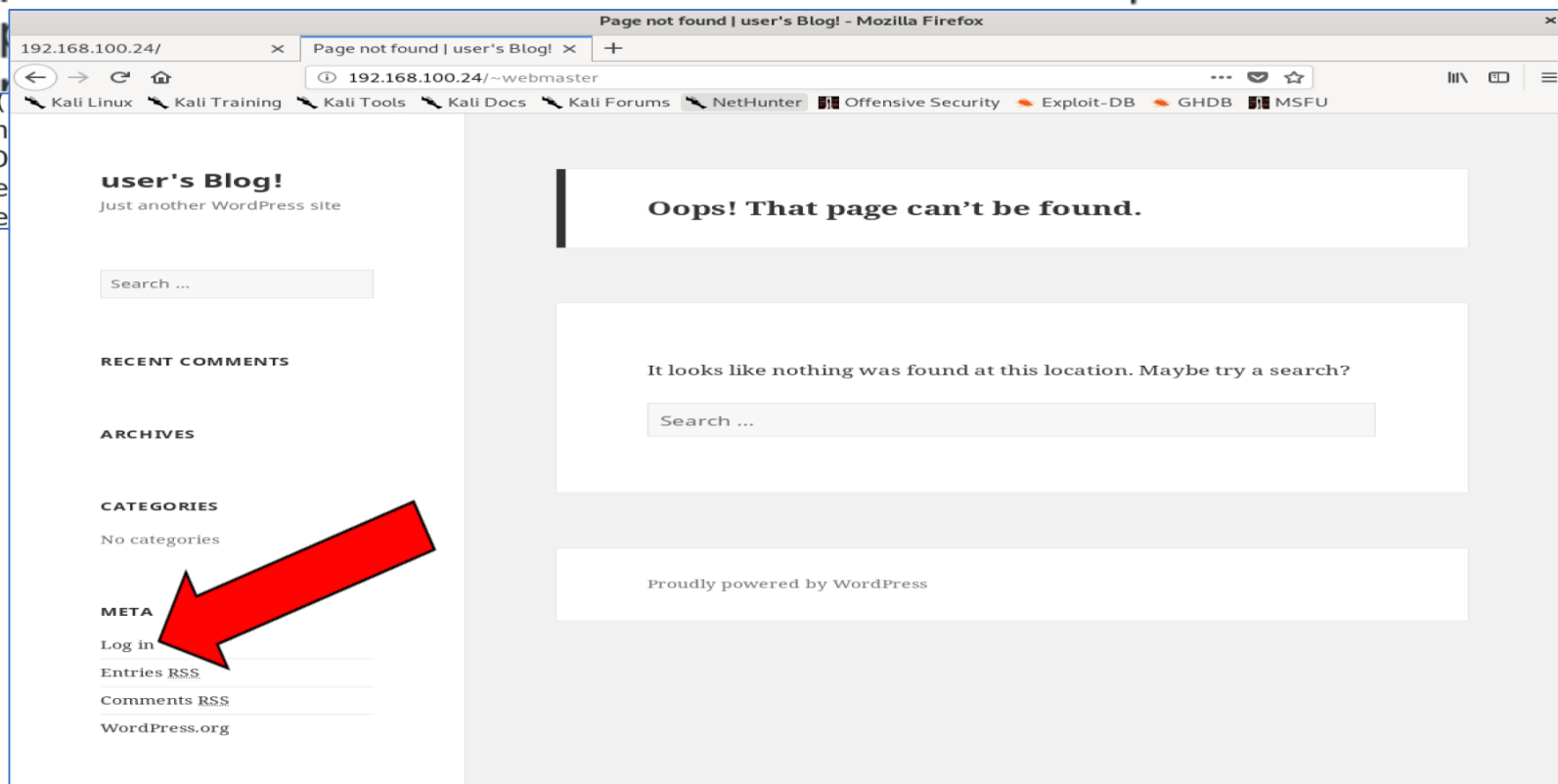
```
START_TIME: Tue Sep  1 13:54:24 2020  
URL_BASE: http://192.168.100.24/  
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
```

```
-----  
GENERATED WORDS: 4612
```

```
---- Scanning URL: ht
```

```
+ http://192.168.100.24/  
+ http://192.168.100.24/  
+ http://192.168.100.24/  
+ http://192.168.100.24/  
+ http://192.168.100.24/  
+ http://192.168.100.24/  
+ http://192.168.100.24/_media (  
+ http://192.168.100.24/_mem_bin  
+ http://192.168.100.24/_mm (COD  
+ http://192.168.100.24/_mmserve  
+ http://192.168.100.24/_mygalle
```

```
+ http://192.168.100.24/~tmp (CODE:503|SIZE:288)  
+ http://192.168.100.24/~user (CODE:503|SIZE:288)  
+ http://192.168.100.24/~webmaster (CODE:503|SIZE:288)  
+ http://192.168.100.24/~www (CODE:503|SIZE:288)  
+ http://192.168.100.24/~
```



Enumeración de servicios

- Como ya sabemos que es un sitio web montado en WordPress, podemos utilizar una herramienta adaptada para escanearlo: **WPScan**.
- Podemos ejecutar el siguiente comando y verificar el contenido del sitio:
 - `wpscan --url http://192.168.100.24/ --enumerate p`
- WPScan es un escáner de vulnerabilidades para WordPress, y es posible usarlo para situaciones de “caja negra” donde no sabemos los contenidos de los sitios.





WordPress Security Scanner by the WPScan Team
Version 3.8.4

Sponsored by Automattic - <https://automattic.com/>
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[+] URL: <http://192.168.100.24/> [192.168.100.24]

[+] Started: Tue Sep 1 20:24:29 2020

Interesting Finding(s):

[+] Headers

| Interesting Entries:

- | - Server: Apache
- | - X-Mod-Pagespeed: 1.9.32.3-4523

| Found By: Headers (Passive Detection)

| Confidence: 100%

[+] <http://192.168.100.24/robots.txt>

| Found By: Robots Txt (Aggressive Detection)

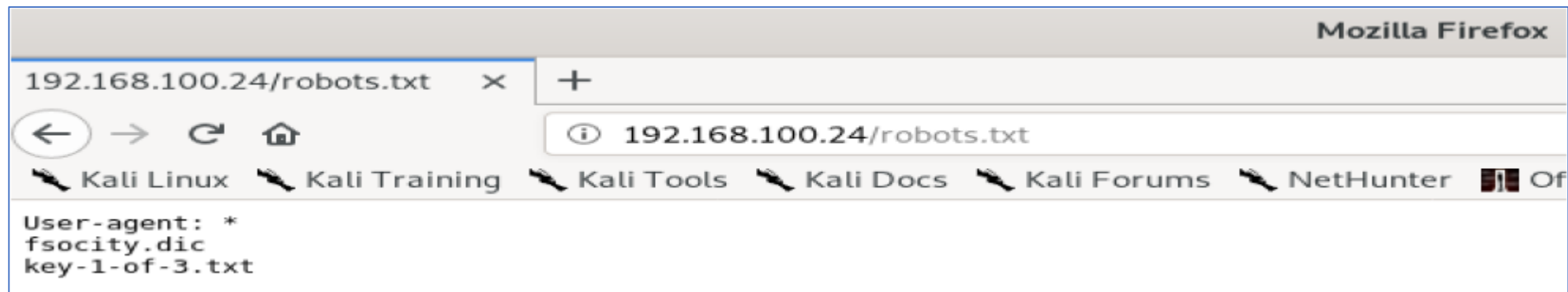
| Confidence: 100%

[+] XML-RPC seems to be enabled: <http://192.168.100.24/xmlrpc.php>

| Found By: Direct Access (Aggressive Detection)

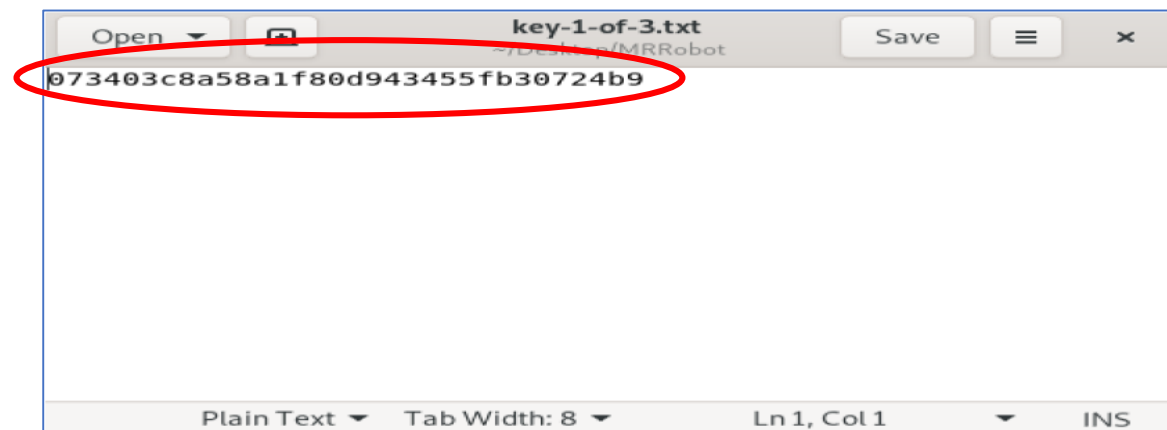
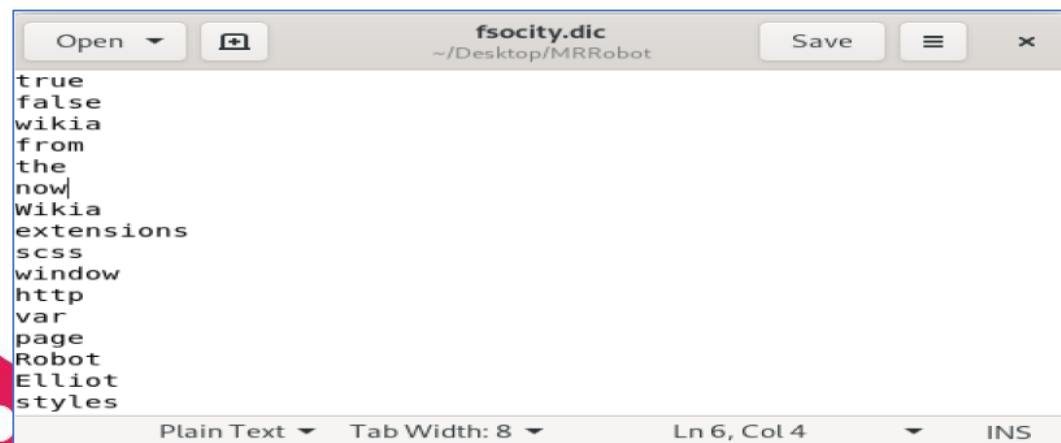
| Confidence: 100%

| References:



```
root@kali: ~/Desktop/MRRobot
root@kali:~/Desktop/MRRobot# wget 192.168.100.24/fsociety.dic
```

```
root@kali: ~/Desktop/MRRobot
root@kali:~/Desktop/MRRobot# wget 192.168.100.24/key-1-of-3.txt
```



Mira el video

Enumerar servicios.





Gracias