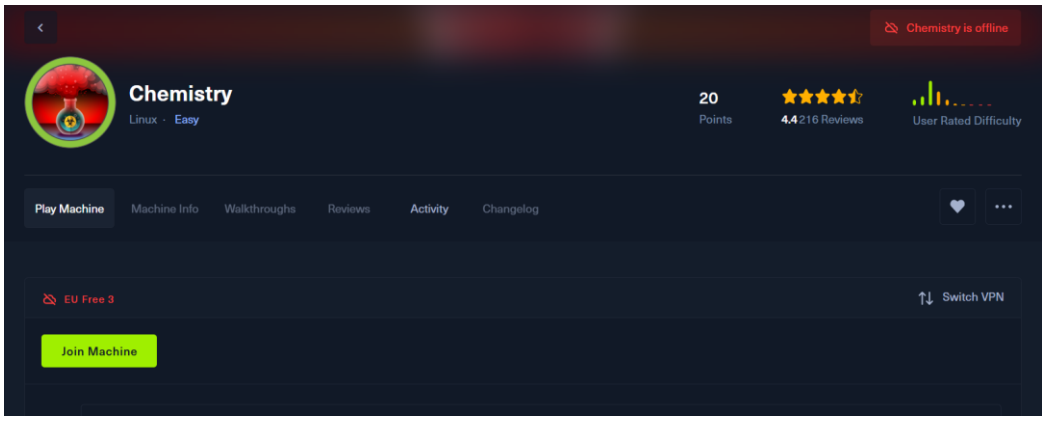
LAB 2 : Machine Chemistry (HTB)

Étape 1 : Mise en place de l'environnement de test d'intrusion

- 3 méthodes possibles pour mettre en place l'environnement :
  - Installer/Utiliser une machine Ubuntu et installer les outils
  - Installer/Utiliser une machine Kali linux et installer les outils
  - Installation et utilisation de **Exegol** (container contenant tous les outils de pentest)

Étape 2 : Démarrer la machine sur VirtualBox

- Créer un compte HackTheBox (https://app.hackthebox.com/login)
- Télécharger le fichier OpenVPN de HackTheBox (Bouton « connect to HTB » en haut)
  - Sur Windows : Installer OpenVPN et lancer le fichier .ovpn
  - Sur Linux : `sudo openvpn NAME.ovpn`
- Accéder à la machine **Chemistry** et cliquer sur « Join Machine » afin d'avoir l'adresse IP publique à travers laquelle vous allez se connecter à la machine (normalement c'est la 10.10.11.38).



Étape 3 : Reconnaissance

- Faire un scan **nmap** pour identifier les services et les ports ouverts
- Utiliser les options :
  - Script par défaut de nmap
  - Afficher la version des services
  - Faire un Scan **Syn**
  - Augmenter la rapidité du scan

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

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

ATTENTION. Quand vous listez les ports ouverts et que vous ne connaissez pas le protocole ou la technologie = Regardez sur internet ce que c'est et si une CVE (common Vulnerability Exposure) est associé à celle-ci.

Étape 4 : Recherche, identification et exploitation de la vulnérabilité

- Rechercher et exploiter **une** vulnérabilité sur la machine. Au moins 2 vulnérabilités existent sur cette machine.
- Détailler le processus suivi pour la recherche, l'identification et l'exploitation de la vulnérabilité dans le rapport.

  ATTENTION. Vous pouvez rencontrer des erreurs de version avec openjdk (**C'est normal !**), Changer la version et utiliser la version antérieure demandée.

BONUS.

Tenter d'identifier et d'exploiter la deuxième vulnérabilité. Détailler le processus suivi dans le rapport.