## **Machines du Lab**

Olivier LASNE - olivier@lasne.pro

Machines du Lab 2020-01-25

#### **Installation d'outils**

On va utiliser sshuttle pour se connecter en SSH depuis notre VM d'attaque.

```
1 sudo apt install sshuttle
```

Pour le lancer, on peut utiliser la commande

```
1 sudo sshuttle -r kali@137.74.90.91:22808 192.168.3.1/24
```

#### **Bonus:**

Vous pouvez utiliser sshfs pour monter un dossier du serveur distant en local.

```
1 sshfs -p 22808 kali@137.74.90.91:dossier_distant dossier_local
```

#### Machine 192,168,3,20

#### **Nmap**

On commence par un scan nmap:

```
1 # Nmap 7.91 scan initiated Mon Jan 25 22:03:06 2021 as: nmap -p- -sV -
      sC -oN 20/fullscan.nmap 192.168.3.20
2 Nmap scan report for 192.168.3.20
3 Host is up (0.000096s latency).
4 Not shown: 65529 closed ports
5 PORT STATE SERVICE VERSION
6 22/tcp open ssh
                           OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu
      Linux; protocol 2.0)
7 | ssh-hostkey:
       2048 db:45:cb:be:4a:8b:71:f8:e9:31:42:ae:ff:f8:45:e4 (RSA)
9
       256 09:b9:b9:1c:e0:bf:0e:1c:6f:7f:fe:8e:5f:20:1b:ce (ECDSA)
10 | 256 a5:68:2b:22:5f:98:4a:62:21:3d:a2:e2:c5:a9:f7:c2 (ED25519)
11 80/tcp open http Apache httpd 2.4.18 ((Ubuntu))
12 | http-server-header: Apache/2.4.18 (Ubuntu)
13 | _http-title: Site doesn't have a title (text/html).
14 139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
15 445/tcp open netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup:
      WORKGROUP)
16 8009/tcp open ajp13
                           Apache Jserv (Protocol v1.3)
   | ajp-methods:
18 |_ Supported methods: GET HEAD POST OPTIONS
19 8080/tcp open http
                           Apache Tomcat 9.0.7
20 | http-favicon: Apache Tomcat
21 | http-open-proxy: Proxy might be redirecting requests
```

Machines du Lab 2020-01-25

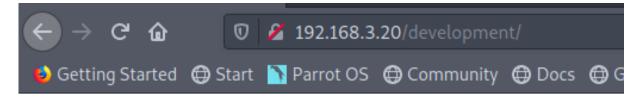
```
22 |_http-title: Apache Tomcat/9.0.7
23 Service Info: Host: BASIC2; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

### Énumération web

On lance un **gobuster** sur le site web pour découvrir du contenu supplémentaire sur le site.

```
1 $ gobuster dir -u http://192.168.3.20/ -w /usr/share/wordlists/
    dirbuster/directory-list-2.3-medium.txt -x txt,php -o gb_med.txt
2
3 -----
4 Gobuster v3.0.1
5 by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
[+] Url:
             http://192.168.3.20/
            10
/usr/share/wordlists/dirbuster/directory-list-2.3-
8 [+] Threads:
9 [+] Wordlist:
   medium.txt
10 [+] Status codes: 200,204,301,302,307,401,403
11 [+] User Agent: gobuster/3.0.1
12 [+] Extensions:
             txt,php
13 [+] Timeout:
             10s
15 2021/01/25 22:08:16 Starting gobuster
17 /development (Status: 301)
18 /server-status (Status: 403)
20 2021/01/25 22:08:59 Finished
```

Machines du Lab 2020-01-25



and an additional Cine December in the same

# Index of /development

<u>Name</u>	Last modified	Size Description
Parent Directory		-
dev.txt	2018-04-23 14:52	483
j.txt	2018-04-23 13:10	235

Apache/2.4.18 (Ubuntu) Server at 192.168.3.20 Port 80

FIG. 1: Dossier developement

#### **Partage SMB**

On utilise **smbmap** pour lister les partages SMB disponnibles :

python3 /usr/share/doc/python3-impacket/examples/smbclient.py 192.168.3.20