Rapport TP sur la mise en place

Table des matières

Rapport TP sur la mise en place **1**
Sommaire 1
Introduction 1
1. Mise en place 1
1.1 Configuration utilisateur et réseau 1
1.2 Configuration shh et vnc 3
Conclusion 5

Rapport TP sur la mise en place

By Clement ALLEGRE–COMMINGES and PETIT Lucien

Sommaire

— Introduction
— 1. Mise en place
  — 1.1 Configuration utilisateur et réseau
  — 1.2 Configuration shh et vnc
— Conclusion

Introduction

Dans cette première partie de TP nous avons effectué la mise en place de notre environnement sur un Raspberry PI400. Ce Raspberry Pi nous servira à héberger les services que nous tenterons d'attaquer durant l'ensemble de nos TPs d'attaque défense.

Nous avons donc configuré les paramètres utilisateurs et réseaux avant de configurer une connexion ssh via des clés privées.

1. Mise en place

1.1 Configuration utilisateur et réseau

Nous avons créé notre user en flashant un nouvel environnement (Raspberry Pi os bookworm) sur la carte SD du raspberry Pi.

— root :
  — username `root`

    - mot de passe : `password`
- user :
    - username : `user`
    - mot de passe : `password`

Nous avons choisi l'IP statique `192.168.1.200/24` avec `192.168.1.1` comme default gateway et `1.1.1.1` en DNS par défaut sur le réseau wifi TP_RESEAUX (pwd : PolytechTours37!). Nous avons aussi profité pour changer le nom de l'appareil pour `motivation`, notre nom d'équipe.

Pour vérifier que la configuration a bien été appliquée, nous avons utilisé la commande suivante :

```
user@motivation:~ $ id; who ; pwd $HOME
uid=1000(user) gid=1000(user) groups=1000(user),4(adm),20(dialout),24(cdrom),27(sudo),29(audio)
user                 2025-12-03 14:12
user     tty1        2025-12-03 14:12
user     pts/1       2025-12-03 14:14 (192.168.1.22)
user     pts/2       2025-12-03 14:15 (192.168.1.20)
/home/user
```

Nous retrouvons bien notre user standard en `tty1` ainsi que les 2 sessions ssh depuis wsl en `pts/1` et `pts/2` qui renvoie les IP de nos machines.

Pour vérifier que l'ip est bien statique et obtenir nous addresse MAC, on a utilisé `ip a` :

```
user@motivation:~ $ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group default qlen 10
    link/ether d8:3a:dd:36:0d:97 brd ff:ff:ff:ff:ff:ff
3: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default ql
    link/ether d8:3a:dd:36:0d:99 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.200/24 brd 192.168.1.255 scope global noprefixroute wlan0
       valid_lft forever preferred_lft forever
    inet 192.168.1.26/24 brd 192.168.1.255 scope global secondary dynamic noprefixroute wlan0
       valid_lft 86396sec preferred_lft 86396sec
    inet6 2a02:8440:b505:fda3:f1bc:8142:a4c9:e094/64 scope global dynamic noprefixroute
       valid_lft 294sec preferred_lft 114sec
    inet6 fe80::eeb0:a3cf:6761:8a59/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

On retrouve bien `192.168.1.200/24` en `forever` ce qui veut dire que notre Raspberry Pi a bien l'adresse IP statique que nous avions choisie. Nous avons pu aussi identifier l'adresse MAC de l'interface wifi du Raspberry Pi comme : `d8:3a:dd:36:0d:99`

Nous avons ensuite vérifié que nous pouvions pinguer notre `localhost`.

```
user@motivation:~ $ ping motivation.local
PING motivation.local (127.0.0.1) 56(84) bytes of data.
```

```
64 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.053 ms
64 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=64 time=0.087 ms
^C
--- motivation.local ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1010ms
rtt min/avg/max/mdev = 0.053/0.070/0.087/0.017 ms
```

Nous avons ensuite scanné le réseau avec `nmap` depuis un autre ordinateur pour vérifier la présence de notre Raspberry pi sur le réseau.

```
user@MSI:/mnt/c/Users/lucie/Documents/Cours/ISIE/5A/Attaque%20defense$ sudo nmap -n -sP 192.168
[sudo] password for user:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-03 14:54 CET
Nmap scan report for 192.168.1.1
Host is up (0.0079s latency).
Nmap scan report for 192.168.1.2
Host is up (0.054s latency).
            .
            .
            .
Host is up (0.15s latency).
Nmap scan report for 192.168.1.26
Host is up (0.15s latency).
Nmap scan report for 192.168.1.27
Host is up (0.13s latency).
Nmap scan report for 192.168.1.200
Host is up (0.014s latency).
Nmap done: 256 IP addresses (11 hosts up) scanned in 47.79 seconds
```

On retrouve bien 192.168.1.200 de connecté sur le réseau.

1.2 Configuration shh et vnc

Nous avons commencé par utiliser l'interface graphique pour activer les interfaces `ssh` et `vnc`. Cela nous permet d'utiliser la commande `ssh user@192.168.1.200` pour obtenir un terminal de contrôle et d'utiliser un client vnc (dans notre cas RealVnc) pour accéder à l'interface graphique.

Cependant, l'activation de ssh par défaut fonctionne avec une identification par mot de passe. Ce mode d'authentification n'est pas le plus sécurisé car il est vulnérable aux attaques par bruteforce et attaques par dictionnaires. Une des mitigations pour ce problème est d'utiliser une clé d'authentification unique pour faire cela, nous avons réalisé les étapes suivantes :

1. création d'une clé d'autentification

   ```
   user@MSI:/mnt/c/Users/lucie/Documents/Cours/ISIE/5A/Attaque defense$ ssh-keygen -f ~/.ssh
   Generating public/private ed25519 key pair.
   Enter passphrase for "/home/user/.ssh/id_rsa_RPI400" (empty for no passphrase):
   Enter same passphrase again:
   Your identification has been saved in /home/user/.ssh/id_rsa_RPI400
   Your public key has been saved in /home/user/.ssh/id_rsa_RPI400.pub
   ```

```
The key fingerprint is:
SHA256:+KuAv8wjW3Z9rtdXq88gM8bugYJ+4vREIhLK3gTKN1k user@MSI
The key's randomart image is:
+--[ED25519 256]--+
|                 |
|                 |
| o   E           |
|= o o  .         |
|o+ * ...S        |
|. =.o +o  o     .|
| ...+o.oo..O . ..|
|  .*++o..++ * +. |
|  .o*=+ooooo ooo |
+----[SHA256]-----+
```

2. On copie ensuite notre nouvelle clé vers le Raspberry avec ssh.

```
user@MSI:/mnt/c/Users/lucie/Documents/Cours/ISIE/5A/Attaque defense$ ssh-copy-id -i /home
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/user/.ssh/id_rsa_RPI
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any t
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it
user@192.168.1.200's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh -i /home/user/.ssh/id_rsa_RPI400 'user@192.1
and check to make sure that only the key(s) you wanted were added.
```

3. On a ensuite désactivé les accès par mots de passe et activé l'accès par clé en passant

   — `PasswordAuthentication` à `no`
   — `PubkeyAuthentication` à `yes`

   dans `/etc/ssh/sshd_config`

```
user@motivation:~ $ sudo nano /etc/ssh/sshd_config
```

4. On peut ensuite valider le fonctionnement de la connection `ssh`.

```
user@MSI:/mnt/c/Users/lucie/Documents/Cours/ISIE/5A/Attaque defense$ ssh -Y user@192.168
Warning: No xauth data; using fake authentication data for X11 forwarding.
Linux motivation 6.12.47+rpt-rpi-v8 #1 SMP PREEMPT Debian 1:6.12.47-1+rpt1~bookworm (202

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Dec  3 15:38:00 2025 from 192.168.1.20
user@motivation:~ $ exit
logout
Connection to 192.168.1.200 closed.
```

```
user@MSI:/mnt/c/Users/lucie/Documents/Cours/ISIE/5A/Attaque defense$ ssh 192.168.1.200
user@192.168.1.200: Permission denied (publickey).
```

On peut observer que les accès ssh par mot de passe sont bien désactivé et que les accès par clé sont fonctionnel.

Conclusion

À la fin de la mise en place, nous nous retrouvons avec un Raspberry opérationnel.