Betton Yaël
Sauvage Mathis

BUT 1-G2B

Compte rendu S.A.E S2.03

Sommaire :

Contexte de la S.A.E :

Pour cette Situation d'Apprentissage et d'Évaluation (SAÉ), nous devions concevoir et mettre en place une architecture réseau comportant plusieurs zones distinctes. L'objectif était de segmenter le réseau en différentes parties fonctionnelles afin d'assurer une organisation claire, une meilleure sécurité et une gestion efficace des flux. Ainsi, nous avons structuré notre réseau en trois zones principales : une zone personnelle destinée à l'administration et à la gestion interne, une zone client représentant les postes utilisateurs standards, et enfin une zone serveur, dédiée à l'hébergement de services comme SSH, FTP.

Dans ce contexte, une analyse réseau a été réalisée à l'aide de l'outil Wireshark pour observer en détail les échanges entre ces différentes zones, en particulier une tentative de connexion SSH entre une machine de la zone personnelle (ou client) et un serveur situé dans la zone serveur. La capture ci-jointe illustre le fonctionnement de cette communication ainsi que les différentes étapes protocolaires qui la composent.

1. Analyse du problème et choix de l'architecture :

A - Choix de l'architecture réseau

Dans un premier temps, nous avons analysé l'architecture du réseau en fonction des contraintes imposées. Nous devions assurer une répartition logique des adresses IP en fonction des différentes zones tout en optimisant les plages d'adresse disponibles.

Pour la zone Serveur m3 (au moins 140 machines) , nous devions avoir 450 machines, pour ce faire nous avons mis une plage d'adresse avec un CIDR de 23, ce qui permet d'avoir 512 adresses IP. Cette capacité permet de répondre largement aux besoins de cette zone. Nous avons choisi le réseau 192.168.1.0/23 afin de bien distinguer cette zone des zones Personnel et Client.

Dans la zone Personnel m1 , nous avions besoin de 289 adresses IP. Pour répondre à cette exigence, nous avons attribué le réseau 172.15.100.0/23 ce qui permet d'avoir 512 adresses possibles. La passerelle de la zone Personnel a été configurée sur l'adresse 172.15.101.254, attribuée au routeur R_P.

Concernant la zone Clients m2, nous devions pouvoir accueillir 700 machines, nous ne pouvions pas attribuer un CIDR en /23 car nous n'aurions pas eu suffisamment de machines (CIDR de 23 = 512 adresses). Nous avons alors opté pour un CIDR de 22 ce qui permet d'avoir 1024 adresses IP ce qui garantit une marge confortable d'adresses disponibles. L'interface R_C configurée sur l'adresse 172.15.99.254 jouera le rôle de routeur entre les différents réseaux. De plus, nous devons aussi créer un serveur DHCP pour allouer des adresses dynamiques, ce serveur doit pouvoir configurer 450 adresses IP. Nous avons décidé de lui donner la plage d'adresse de 172.15.96.1 à 172.15.97.254 .

Enfin, pour la zone Routeur, nous avons choisi d'utiliser le réseau 10.0.0.0/24, qui permet de lier les différents routeurs ensemble et par la même occasion les différentes zones entre elles y compris le routeur R. De plus, chaque routeur dispose d'interfaces connectées à des sous réseaux en /26, ce qui permet d'avoir 64 adresses IP. Ce séparation permet de distinguer le routage vers les différentes routes

et vers les différents réseaux , par exemple le routeur principal R dispose de trois interfaces, attribuées respectivement aux adresses 10.0.0.1/26 pour l'interface ETH0 (NET0), 10.0.0.65/26 pour l'interface ETH1 (NET1), et 10.0.0.129/26 pour l'interface ETH2 (NET2). Nous avons choisi de mettre un CIDR de 26(64 adresses disponible) car nous n'avons pas besoin de plus d'adresse pour ce réseau car il ne contenait que quelques routeurs.

2. Configuration sur Kathara :

A - Configuration des adresses IP et des routes :

Après avoir segmenté le réseau selon les consignes et contraintes qui nous avaient été imposées, nous avons commencé à attribuer les adresses IP de chaque machine et de chaque routeur , en nous appuyant sur le schéma réseau fourni (Annexe 1). Dans un premier temps, nous avons volontairement laissé les serveurs non configurés afin de nous concentrer sur la mise en place correcte du routage. L'objectif initial était de permettre à chaque machine d'atteindre Internet, notamment en réussissant un ping vers Google.

Voici un exemple typique d'une de nos configurations :

```
ip address add 10.0.0.1/26 dev eth0
ip link set dev eth0 up
ip address add 10.0.0.65/26 dev eth1
ip link set dev eth1 up
ip address add 10.0.0.129/26 dev eth2
ip link set dev eth2 up

ip route add 172.15.96.0/22 via 10.0.0.130
ip route add 172.15.100.0/24 via 10.0.0.66
ip route add 192.168.1.0/24 via 10.0.0.2
ip route add 192.168.2.0/24 via 10.0.0.2

iptables -t nat -A POSTROUTING -o eth3 -j MASQUERADE
echo "nameserver 8.8.8.8" > /etc/resolv.conf
```

Les deux dernières lignes de cette capture d'écran permettent d'établir la connexion entre la machine et internet. La première commande permet aux machines d'un réseau local d'accéder à Internet en passant par l'interface ETH3, grâce à la technique de masquerade .
La seconde commande définit un serveur DNS (ici 8.8.8.8 de Google) pour que la machine puisse résoudre les noms de domaine.

B - Configuration du serveur DHCP :

Un serveur DHCP (Dynamic Host Configuration Protocol) est un service réseau qui attribue automatiquement des adresses IP et d'autres paramètres réseau aux appareils connectés à un réseau.

Le serveur DHCP a été installé sur le routeur R_C, qui dispose de deux interfaces réseau :

- ETH0, connectée au réseau externe
- ETH1, connectée au réseau interne et chargée de distribuer les adresses IP aux clients

Voici les commandes utilisées pour l'installation :

```
apt update
apt upgrade -y
DEBIAN_FRONTEND=noninteractive apt-get install -y -o Dpkg::Options::="--force-confold" isc-dhcp-server

systemctl start isc-dhcp-server
```

Ces lignes permettent de mettre à jour les paquets, puis d'installer automatiquement le serveur DHCP.

Nous avons ensuite configuré le fichier /etc/dhcp/dhcpd.conf afin que le serveur puisse attribuer des adresses IP dans la plage 172.15.96.1 à 172.15.97.254, comme défini lors de la première phase de la S.A.E. Le routeur R_C a été défini comme passerelle par défaut (gateway) pour les clients, et un serveur DNS a également été spécifié. Enfin, les paramètres de durée de connexion ont été configurés pour gérer efficacement les connexions des différentes machines sur le réseau.

```
ddns-update-style none;

subnet 172.15.96.0 netmask 255.255.252.0 {
    range 172.15.96.1 172.15.97.254;
    option routers 172.15.99.254;
    option domain-name-servers 8.8.8.8;
    default-lease-time 7200;
    max-lease-time 43200;
}
```

Ensuite nous avons configuré le fichier /etc/default/isc-dhcp-server qui indique sur quelles interfaces réseau le serveur DHCP doit écouter et répondre aux demandes. On configure le serveur DHCP pour écouter et répondre uniquement à l'interface ETH1.

Enfin, nous finissons par configurer le fichier /etc/network/interfaces, il sert à définir la configuration réseau des interfaces sur la machine. Ce fichier est important car l'interface qui communique avec les clients doit avoir une adresse IP statique car elle sert de passerelle.

Maintenant nous devons faire en sorte que les machines PCC et PCD se connectent automatiquement au début de la configuration pour se faire nous utilisons cette commande :

```
while ! ip -4 addr show dev "eth0" | grep -q 'inet '; do
    dhclient "eth0"
    sleep 5
done
```

Ce code attend que ETH0 reçoit une adresse IPv4 via DHCP. Tant que ce n'est pas le cas, il lance dhclient eth0 toutes les 5 secondes, cette requête lance le client DHCP pour demander une adresse IP sur l'interface eth0.

C - Configuration du serveur SSH :

Un serveur SSH (Secure Shell) est un service qui permet d'établir une connexion sécurisée à distance entre un client et un ordinateur ou un serveur. Ce type de connexion est largement utilisé pour l'administration système, car il chiffre les échanges de données, assurant ainsi confidentialité et sécurité. Sur le serveur nommé sadmin, une configuration SSH a été mise en place pour permettre une gestion à distance sécurisée. Voici les différentes étapes réalisées pour cette configuration :

Mise à jour du système et installation du serveur SSH :

```
apt update && apt install -y openssh-server
```

Cette commande met à jour la liste des paquets disponibles, puis installe le paquet openssh-server, qui permet au système d'accepter des connexions SSH entrantes.

Création d'un utilisateur dédié à l'administration

```
useradd -m admin
```

Un nouvel utilisateur nommé admin a été créé avec un répertoire personnel (-m), dans le but de disposer d'un compte spécifique pour les tâches d'administration via SSH.

Définition du mot de passe pour le compte admin

```
echo "admin:admin" | chpasswd
su admin

systemctl start ssh
```

Cette commande initialise le mot de passe de l'utilisateur admin à "admin". Cela permet d'accéder rapidement au compte, notamment pour effectuer les premiers tests de connexion. Il est cependant recommandé de changer ce mot de passe par la suite pour renforcer la sécurité.

La commande su permet de basculer sur le compte admin, ce qui est utile pour valider les droits d'accès et procéder à d'éventuelles configurations supplémentaires.

Le service SSH est lancé, ce qui rend le serveur sadmin accessible à distance via une connexion SSH. Il devient ainsi possible d'administrer le système depuis un autre poste en toute sécurité.

D - Configuration du FTP

Sur le serveur nommé sf, un serveur FTP a été mis en place afin de permettre le partage de fichiers à distance à l'aide du protocole FTP (File Transfer Protocol). Ce service est souvent utilisé pour transférer des fichiers entre une machine locale et un serveur, notamment dans un contexte d'administration ou de gestion de contenu. Voici les étapes réalisées pour installer et configurer ce service :

Mise à jour du système et installation du serveur FTP

```
apt update && apt install -y vsftpd
```

Cette commande met à jour les paquets du système, puis installe vsftpd (*Very Secure FTP Daemon*). Ce serveur est fréquemment utilisé dans des environnements professionnels.

Création d'un utilisateur dédié au FTP avec la commande useradd. Un utilisateur nommé admin a été créé avec un répertoire personnel. Ce compte permet de centraliser les fichiers à partager et de garantir un espace isolé pour les transferts FTP.

Ensuite on initialise le mot de passe pour le compte admin avec la ligne de code : "echo "admin:admin" | chpasswd"

Le mot de passe de l'utilisateur admin a été défini à "admin". Cette étape permet une connexion immédiate au serveur FTP, notamment pour les premiers essais. Il est toutefois fortement conseillé de modifier ce mot de passe ultérieurement pour des raisons de sécurité.

Création d'un fichier de test dans le répertoire de l'utilisateur

```
su admin
mkdir -p /home/admin
touch /home/admin/file.txt
echo "Bonjour" >> /home/admin/file.txt
```

Après avoir basculé sur le compte admin, un fichier nommé file.txt a été créé dans son répertoire personnel. Le mot "Bonjour" y a été ajouté pour vérifier que le serveur FTP fonctionne correctement et que les fichiers peuvent être téléchargés via un client FTP.

```
systemctl start vsftpd
```

Le service vsftpd a été lancé, rendant le serveur sf accessible à distance via un client FTP. Les utilisateurs peuvent désormais se connecter en utilisant le compte admin pour télécharger ou déposer des fichiers sur le serveur.

3 - Test et Résultat :

A - Ping entre 2 machines et ping 8.8.8.8 :

Sur la capture d'écran ci-dessous, nous avons essayé de ping le PCC qui a reçu une adresse dynamique depuis S_demo. On peut constater que les différentes routes par lesquelles l'information passe sont fonctionnelles car nous atteignons bien le PCC. De plus, nous avons ensuite essayé de ping google pour vérifier que les ordinateurs qui obtiennent une adresse sont bien reliés au reste du réseau.

```
root@sdemo:/# ping 172.15.96.1
PING 172.15.96.1 (172.15.96.1) 56(84) bytes of data.
64 bytes from 172.15.96.1: icmp_seq=1 ttl=60 time=11.8 ms
64 bytes from 172.15.96.1: icmp_seq=2 ttl=60 time=5.27 ms
^C
--- 172.15.96.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 5.266/8.520/11.775/3.254 ms
root@sdemo:/# ping google.fr
PING google.fr (142.250.179.67) 56(84) bytes of data.
64 bytes from par21s19-in-f3.1e100.net (142.250.179.67): icmp_seq=1 ttl=251 time
=24.5 ms
64 bytes from par21s19-in-f3.1e100.net (142.250.179.67): icmp_seq=2 ttl=251 time
=20.9 ms
^C
--- google.fr ping statistics ---
```

On voit l'adresse de PCD obtenu dynamiquement dans la plage d'adresse spécifié

```
root@pcd:/# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t 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
25: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gro
up default qlen 1000
    link/ether d6:1b:43:7e:24:d7 brd ff:ff:ff:ff:ff:ff
    inet 172.15.96.2/22 brd 172.15.99.255 scope global dynamic eth0
       valid_lft 4306sec preferred_lft 4306sec
```

B - Vérification de l'activité des serveurs :

Nous pouvons vérifier si les différents services sont actifs grâce à la commande "systemctl status [nom du service]" .

```
vsftpd.service - vsftpd FTP server
    Loaded: loaded (/usr/lib/systemd/system/vsftpd.service, enabled)
    Active: active (running)
```

```
root@r_c:/# systemctl status isc-dhcp-server
isc-dhcp-server.service - Dynamic Host Configuration Protocol Server
    Loaded: loaded (/etc/init.d/isc-dhcp-server, disabled)
    Active: active (running)
```

```
root@sadmin:/# systemctl status ssh
ssh.service - OpenBSD Secure Shell server
    Loaded: loaded (/usr/lib/systemd/system/ssh.service, enabled)
    Active: active (running)
```

On observe sur la capture ci-dessous, comment se connecter au serveur ssh avec le mot de passe admin

Et voici la connexion au serveur ftp :

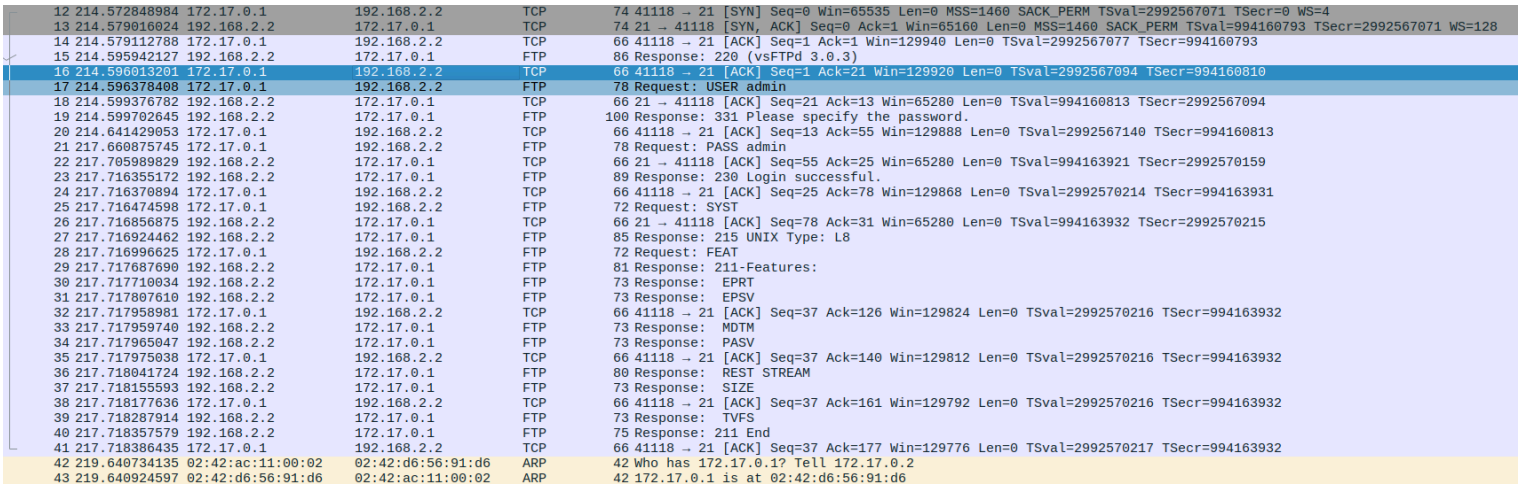
```
root@r_p:/# ssh admin@192.168.2.3
The authenticity of host '192.168.2.3 (192.168.2.3)' can't be established.
ED25519 key fingerprint is SHA256:nSjGSmTGGx4gj/fCqa16lNGw/RsnxPFThfQsdB42LNQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.2.3' (ED25519) to the list of known hosts.
admin@192.168.2.3's password:
Linux sadmin 6.11.0-17-generic #17~24.04.2-Ubuntu SMP PREEMPT_DYNAMIC Mon Jan 20
 22:48:29 UTC 2 x86_64

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.
$ pwd
/home/admin
```

```
root@pcd:/# ftp admin@192.168.2.2
Connected to 192.168.2.2.
220 (vsFTPd 3.0.3)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd /
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
lrwxrwxrwx    1 0        0               7 Jan 13 00:00 bin -> usr/bin
drwxr-xr-x    2 0        0            4096 Dec 31 10:25 boot
drwxr-xr-x    5 0        0             360 May 27 20:00 dev
drwxr-xr-x    1 0        0            4096 May 27 20:02 etc
drwxr-xr-x    1 0        0            4096 May 27 20:02 home
drwxr-xr-x    2 0        0            4096 May 27 20:00 hosthome
drwxrwxr-x    3 1000     982          4096 May 27 20:00 hostlab
lrwxrwxrwx    1 0        0               7 Jan 13 00:00 lib -> usr/lib
lrwxrwxrwx    1 0        0               9 Jan 13 00:00 lib64 -> usr/lib64
drwxr-xr-x    2 0        0            4096 Jan 13 00:00 media
drwxr-xr-x    2 0        0            4096 Jan 13 00:00 mnt
drwxr-xr-x    2 0        0            4096 Jan 13 00:00 opt
dr-xr-xr-x  507 0        0               0 May 27 20:00 proc
drwx------    1 0        0            4096 Jan 15 21:45 root
drwxr-xr-x    1 0        0            4096 May 27 20:02 run
lrwxrwxrwx    1 0        0               8 Jan 13 00:00 sbin -> usr/sbin
drwxrwxrwx    4 1000     1000         4096 May 24 09:40 shared
drwxr-xr-x    1 0        0            4096 May 27 20:02 srv
dr-xr-xr-x   13 0        0               0 May 27 20:00 sys
drwxrwxrwt    1 0        0            4096 May 27 20:02 tmp
drwxr-xr-x    1 0        0            4096 Jan 13 00:00 usr
drwxr-xr-x    1 0        0            4096 Jan 15 21:43 var
226 Directory send OK.
ftp>
```

C - Utilisation de Wireshark :



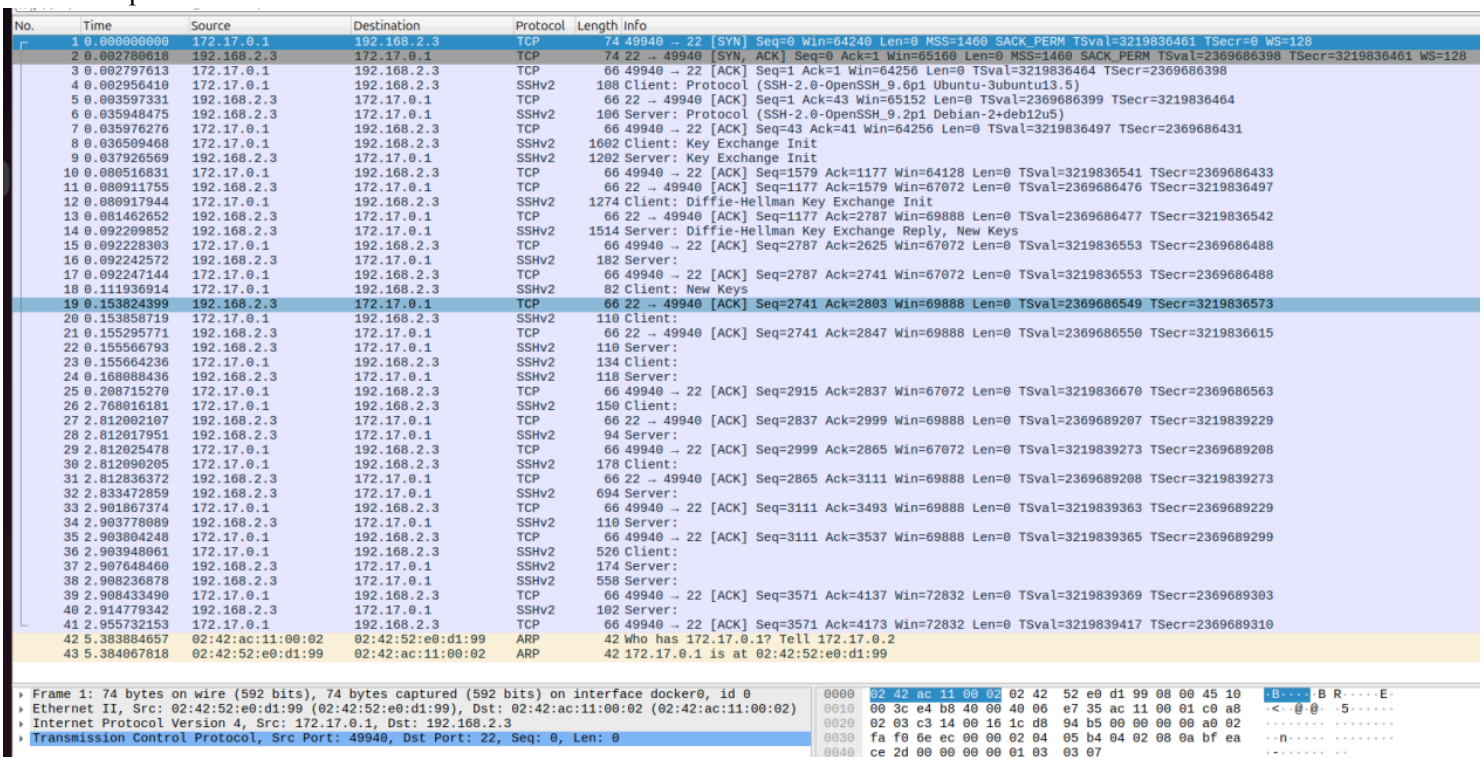
```
12 214.572848984 172.17.0.1      192.168.2.2      TCP      74 41118 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM TSval=2992567071 TSecr=0 WS=4
13 214.579016024 192.168.2.2     172.17.0.1       TCP      74 21 → 41118 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=994160793 TSecr=2992567071 WS=128
14 214.579112788 172.17.0.1      192.168.2.2      TCP      66 41118 → 21 [ACK] Seq=1 Ack=1 Win=129940 Len=0 TSval=2992567077 TSecr=994160793
15 214.595942127 192.168.2.2     172.17.0.1       FTP      86 Response: 220 (vsFTPd 3.0.3)
16 214.596013201 172.17.0.1      192.168.2.2      TCP      66 41118 → 21 [ACK] Seq=1 Ack=21 Win=129920 Len=0 TSval=2992567094 TSecr=994160810
17 214.596378408 172.17.0.1      192.168.2.2      FTP      78 Request: USER admin
18 214.599376782 192.168.2.2     172.17.0.1       TCP      66 21 → 41118 [ACK] Seq=21 Ack=13 Win=65280 Len=0 TSval=994160813 TSecr=2992567094
19 214.599702645 192.168.2.2     172.17.0.1       FTP     100 Response: 331 Please specify the password.
20 214.641429053 172.17.0.1      192.168.2.2      TCP      66 41118 → 21 [ACK] Seq=13 Ack=55 Win=129888 Len=0 TSval=2992567140 TSecr=994160813
21 217.660875745 172.17.0.1      192.168.2.2      FTP      78 Request: PASS admin
22 217.705989829 192.168.2.2     172.17.0.1       TCP      66 21 → 41118 [ACK] Seq=55 Ack=25 Win=65280 Len=0 TSval=994163921 TSecr=2992570159
23 217.716355172 192.168.2.2     172.17.0.1       FTP      89 Response: 230 Login successful.
24 217.716370894 172.17.0.1      192.168.2.2      TCP      66 41118 → 21 [ACK] Seq=25 Ack=78 Win=129868 Len=0 TSval=2992570214 TSecr=994163931
25 217.716474598 172.17.0.1      192.168.2.2      FTP      72 Request: SYST
26 217.716856875 192.168.2.2     172.17.0.1       TCP      66 21 → 41118 [ACK] Seq=78 Ack=31 Win=65280 Len=0 TSval=994163932 TSecr=2992570215
27 217.716924462 192.168.2.2     172.17.0.1       FTP      85 Response: 215 UNIX Type: L8
28 217.716996625 172.17.0.1      192.168.2.2      FTP      72 Request: FEAT
29 217.717687690 192.168.2.2     172.17.0.1       FTP      81 Response: 211-Features:
30 217.717710034 192.168.2.2     172.17.0.1       FTP      73 Response:  EPRT
31 217.717807610 192.168.2.2     172.17.0.1       FTP      73 Response:  EPSV
32 217.717958981 172.17.0.1      192.168.2.2      TCP      66 41118 → 21 [ACK] Seq=37 Ack=126 Win=129824 Len=0 TSval=2992570216 TSecr=994163932
33 217.717959740 192.168.2.2     172.17.0.1       FTP      73 Response:  MDTM
34 217.717965047 192.168.2.2     172.17.0.1       FTP      73 Response:  PASV
35 217.717975038 172.17.0.1      192.168.2.2      TCP      66 41118 → 21 [ACK] Seq=37 Ack=140 Win=129812 Len=0 TSval=2992570216 TSecr=994163932
36 217.718041724 192.168.2.2     172.17.0.1       FTP      80 Response:  REST STREAM
37 217.718155593 192.168.2.2     172.17.0.1       FTP      73 Response:  SIZE
38 217.718177636 172.17.0.1      192.168.2.2      TCP      66 41118 → 21 [ACK] Seq=37 Ack=161 Win=129792 Len=0 TSval=2992570216 TSecr=994163932
39 217.718287914 192.168.2.2     172.17.0.1       FTP      73 Response:  TVFS
40 217.718357579 192.168.2.2     172.17.0.1       FTP      75 Response: 211 End
41 217.718386435 172.17.0.1      192.168.2.2      TCP      66 41118 → 21 [ACK] Seq=37 Ack=177 Win=129776 Len=0 TSval=2992570217 TSecr=994163932
42 219.640734135 02:42:ac:11:00:02 02:42:d6:56:91:d6 ARP      42 Who has 172.17.0.1? Tell 172.17.0.2
43 219.640924597 02:42:d6:56:91:d6 02:42:ac:11:00:02 ARP      42 172.17.0.1 is at 02:42:d6:56:91:d6
```

La communication débute par l'établissement d'une connexion TCP entre le client et le serveur FTP. Ce processus suit le schéma classique du "3-way handshake" :

- La machine cliente envoie un paquet SYN pour initier la connexion sur le port 21.
- Le serveur FTP répond par un paquet SYN-ACK, indiquant qu'il accepte la connexion.
- Enfin, le client renvoie un ACK, confirmant l'ouverture du canal de communication. Une fois la connexion TCP établie, le protocole FTP prend le relais.

Le serveur envoie un message de bienvenue (220), signalant qu'il est prêt à recevoir des commandes. Le client s'authentifie alors en envoyant successivement les commandes USER et PASS, toutes deux transmises en clair.
Le serveur répond avec un 230 Login successful, confirmant la réussite de l'authentification. Ensuite, on observe plusieurs commandes FTP telles que PWD pour afficher le répertoire courant, TYPE I pour spécifier le transfert en mode binaire, puis PASV qui indique l'ouverture d'un canal de données

en mode passif. Le serveur retourne une adresse IP et un port dédiés à ce canal. Enfin, une nouvelle connexion TCP est établie sur ce port afin de permettre le transfert de fichiers. Ce fonctionnement met en évidence le découplage entre le canal de commande (port 21) et le canal de données dans le protocole FTP .



La communication débute par l'établissement d'une connexion TCP, indispensable au fonctionnement du protocole SSH. Ce processus suit le schéma :

- La machine 172.17.0.1 envoie un paquet SYN pour initier la connexion.

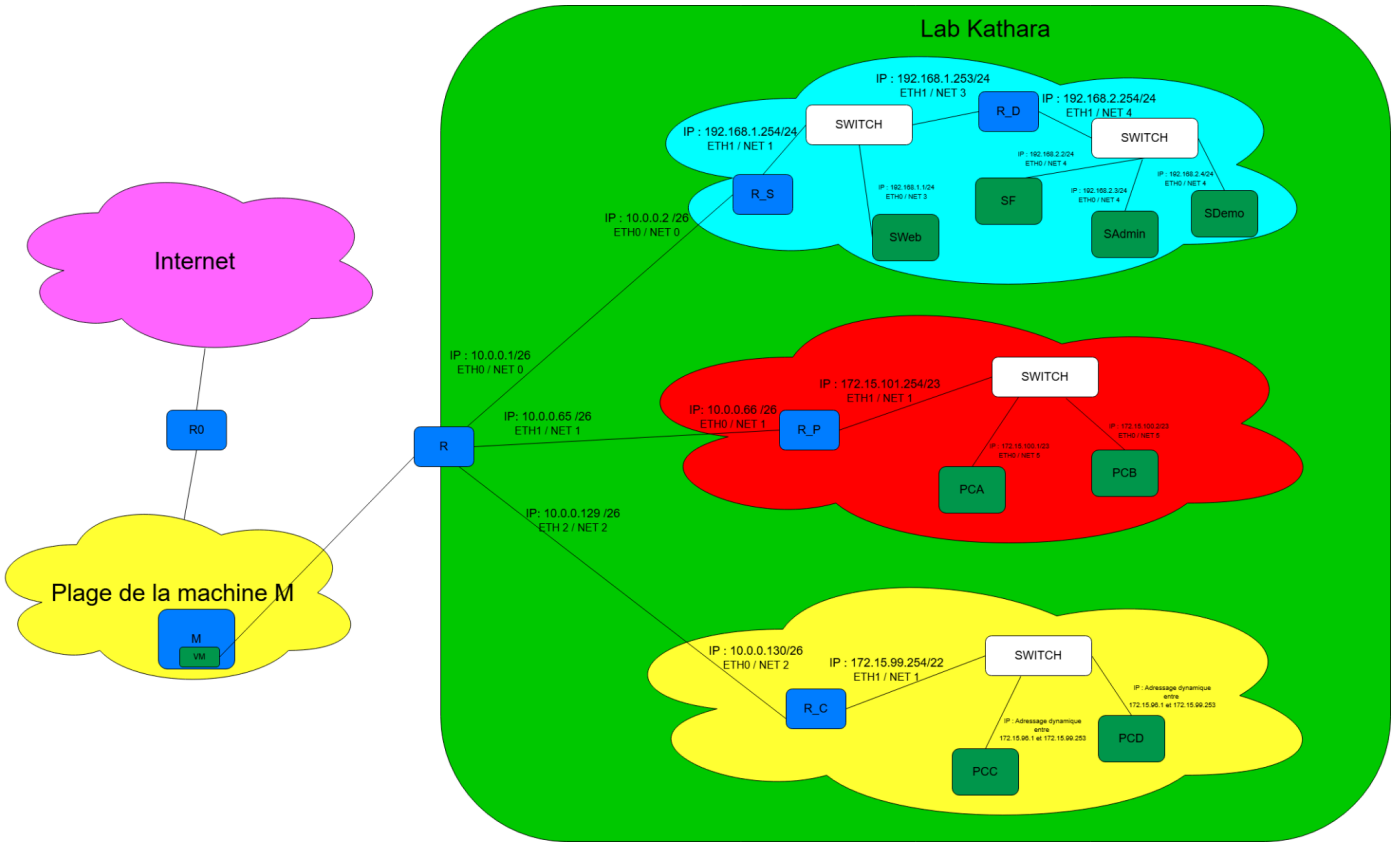
- La machine 192.168.2.3 répond par un paquet SYN-ACK, signalant qu'elle accepte la demande.

Enfin, le client renvoie un ACK pour confirmer l'établissement de la session TCP. À ce stade, la connexion est prête à accueillir un SSH sécurisé. Ensuite, dès que la connexion TCP est établie, le protocole SSH prend le relais. On observe l'échange des versions du protocole SSH utilisées par les deux machines. Le serveur annonce notamment la version OpenSSH_9.6p1 fonctionnant sous Debian. Ensuite, une phase de négociation cryptographique s'engage, incluant :

- L'échange des algorithmes de chiffrement et de hachage compatibles.
- La phase Diffie-Hellman permettant d'établir une clé secrète partagée de manière sécurisée
- L'échange des clés publiques et la mise en place du chiffrement de la session.

Ces étapes garantissent que la session SSH sera chiffrée et protégée contre toute interception. Enfin vers la fin de la capture, on remarque des paquets ARP. Ces paquets sont utilisés pour résoudre les adresses IP en adresses MAC, ce qui est indispensable pour la communication au niveau Ethernet. La machine 192.168.2.3 émet une requête ARP pour identifier l'adresse MAC correspondant à 172.17.0.1. Celle-ci répond avec succès, ce qui confirme que les deux machines sont capables de se retrouver sur le réseau local

Annexes :



NOM machine	ZONE	ip	ETH?	reseau	cidr	address reseau	address broadcast	Plage adresse serveur dhcp
R	PRIVE	10.0.0.1	ETH0	NET0	/26	10.0.0.0	10.0.0.63	
R	PRIVE	10.0.0.65	ETH1	NET1	/26	10.0.0.64	10.0.0.127	
R	PRIVE	10.0.0.129	ETH2	NET2	/26	10.0.0.128	10.0.0.191	
R_S	PRIVE	10.0.0.2	ETH0	NET0	/26	10.0.0.0	10.0.0.63	
R_S	SERVER	192.168.1.254	ETH1	NET1	/24	192.168.1.0	192.168.1.255	
R_P	PRIVE	10.0.0.66	ETH0	NET1	/26	10.0.0.64	10.0.0.127	
R_P	PERSONNEL	172.15.101.254	ETH1	NET1	/23	172.15.100.0	172.15.101.255	
R_C	PRIVE	10.0.0.130	ETH0	NET2	/26	10.0.0.128	10.0.0.191	
R_C	CLIENT	172.15.99.254	ETH1	NET1	/22	172.15.96.0	172.15.99.255	
R_D	SERVER	192.168.1.253	ETH0	NET3	/24	192.168.1.0	192.168.1.255	
R_D	SERVER	192.168.2.254	ETH1	NET4	/24	192.168.2.0	192.168.2.255	
Sweb	SERVER	192.168.1.1	ETH0	NET3	/24	192.168.1.0	192.168.1.255	
Sf	SERVER	192.168.2.2	ETH0	NET4	/24	192.168.2.0	192.168.2.255	
Sadmin	SERVER	192.168.2.3	ETH0	NET4	/24	192.168.2.0	192.168.2.255	
Sdemo	SERVER	192.168.2.4	ETH0	NET4	/24	192.168.2.0	192.168.2.255	
PCA	PERSONNEL	172.15.100.1	ETH0	NET5	/23	172.15.100.0	172.15.101.255	
PCB	PERSONNEL	172.15.100.2	ETH0	NET5	/23	172.15.100.0	172.15.101.255	
PCC	CLIENT	Adressage dynamique	ETH0	NET6	/22	172.15.96.0	172.15.99.255	
PCD	CLIENT	Adressage dynamique	ETH0	NET6	/22	172.15.96.0	172.15.99.255	
Sdhcp	CLIENT	172.15.99.254			/22	172.15.96.0	172.15.99.255	172.15.96.1 -> 172.15.97.254

Glossaire :

Adresse IP : Identifiant unique attribué à chaque machine sur un réseau pour permettre sa communication avec les autres équipements.

ARP (Address Resolution Protocol) : Protocole qui permet de connaître l'adresse physique (MAC) correspondant à une adresse IP dans un réseau local.

CIDR (Classless Inter-Domain Routing) : Méthode de notation permettant de définir efficacement des plages d'adresses IP et de gérer la taille des sous-réseaux.

DHCP (Dynamic Host Configuration Protocol) : Protocole réseau qui attribue automatiquement des adresses IP et d'autres paramètres réseau aux machines d'un réseau.

DNS (Domain Name System) : Système qui permet de traduire les noms de domaine (ex : www.google.com) en adresses IP compréhensibles par les machines.

FTP (File Transfer Protocol) : Protocole utilisé pour transférer des fichiers entre un ordinateur et un serveur via un réseau.

Gateway (Passerelle) : Dispositif (souvent un routeur) permettant à un réseau local d'accéder à d'autres réseaux, comme Internet.

Kathara : Outil de simulation de réseaux utilisé pour créer et tester des architectures réseau virtuelles, proche de GNS3 ou Netkit.

Masquerade (NAT) : Technique de traduction d'adresses utilisée pour permettre aux machines d'un réseau local privé d'accéder à Internet avec une seule adresse IP publique.

Ping : Commande utilisée pour tester la connectivité entre deux machines sur un réseau.

Routeur : Appareil réseau qui assure l'acheminement des données entre plusieurs réseaux.

SSH (Secure Shell) : Protocole permettant d'ouvrir une session à distance sécurisée sur une autre machine, souvent utilisé pour l'administration système.

Subnetting (Sous-réseautage) : Technique permettant de diviser un réseau IP en plusieurs sous-réseaux pour une meilleure organisation.

Wireshark : Outil d'analyse réseau permettant de capturer et d'interpréter les paquets de données échangés sur un réseau.

Bibliographie :

https://www.ionos.fr/digitalguide/serveur/configuration/serveur-ftp-ubuntu-installation-et-configuration/
https://www.it-connect.fr/chapitres/openssh-configuration-du-serveur-ssh/
https://www.onete.net/teaching/2021-2022/R2.04Reseaux1/IntroKathara.pdf