Attaque MITM d'un service SSH et mise en place de contre-Mesures

Q1.Pourquoi l'accès aux machines virtuelles par la console ou l'interface graphique n'est pas possible avec le super-administrateur root ?

Pour limiter les accès en cas d'attaque. Si un attaquant parvient à accéder au super admin, il aurait un accès complet sur la machine.

Correction :

Les bonnes pratiques en matière de cybersécurité recommande de désactiver les comptes administrateur sur les systM d'exploitations et de plutôt utiliser des comptes nominatifs afin d'avoir une **traçabilité**(on sait qui fait, quand…). Cela permet d'affiner le **niveau d'habilitation** attribué a chaque compte. Aussi, cela évitera des tentatives d'attaques par dictionnaire sur des cmptes admin.

Gras questions posées les années passées au bts

Q2.Expliquer à quoi sert la commande sudo et quels avantages a-t-elle sur l'utilisation de la commande su - ?

La commande sudo permet d'exécuter une commande en tant qu'administrateur et su – permet de passer en mode super admin. En utilisant sudo, one ne change pas de mode

Correction :

La cmd su sous linux permet de changer d'user ms aussi de basculer vers le cmpt super utilsateur cad root en utilisant su -. Si ts les admin utilisent le même compte root, cela pourrait entrainer les problème de traçabilité évoqué dans la Q1

La commande sudo permet via le fichier /etc/sudoers de donner des droits admins temporaires a un user afin qu'il puisse réaliser une cmd ou des opération nécessitant des privilèges plus important. Cette cmd sudo offre une meilleure traçabilité ms surtout de définir quelle cmd seront autorisées à être exécuter par un user restreint ; ce qui évite à un user d'acceder au cmpt root tel le cas su –

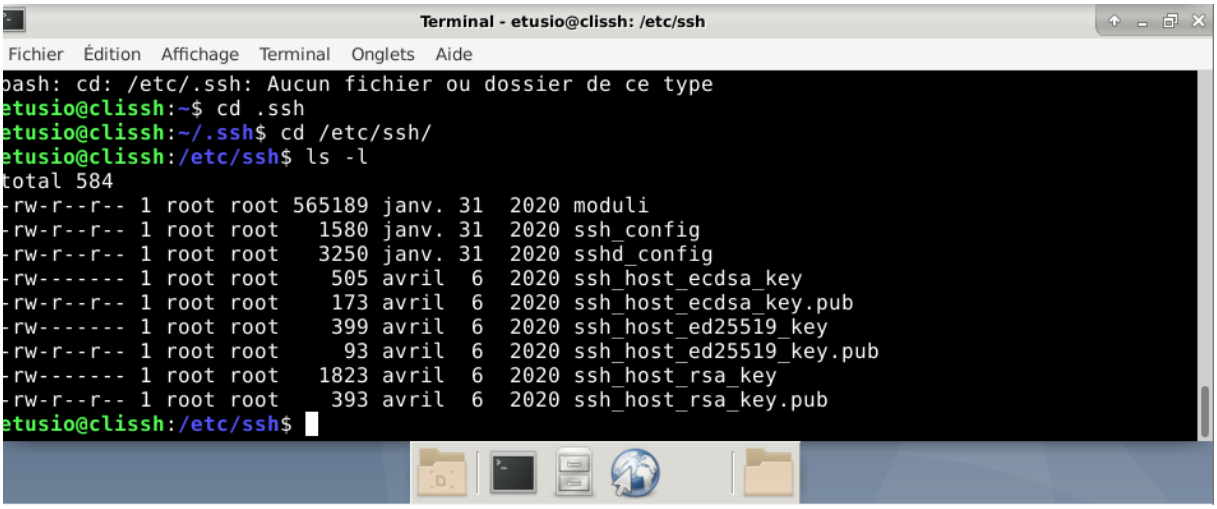
Rmq : les log d'autrehentification se trouve dans /var/log/auth.log sous debian et… Syslog fichier log du sytsM.

Q3. Quelles commandes permettent de savoir si le service OpenSSH (serveur) est déjà installé et démarré ?

Systemctl status ssh

Sudo dpkg -l | grep opensshserver

Q4. Dans le dossier .ssh clé publique stockés dans /.ssh/authorized_key ?



Rep config /etc/ssh. Avec fichier finnisasant par key ou oub clé pub et pri

Fichier moduli sert à l'échange de clé defihe

Ficjier config : sshd_config

Voir annexe p.23

Q5. L'alerte signifie que l'hote que le cherche à joindre n'est pas connu. Ce qui est normal donc on continue l'opération. L'alerte est spécifié comme message de sécurité.

Correction :

Cette alerte signifie que c'est la premier connexion sur cette machine avec le protocole ssh, ainsi l'identité de cette hote ne peut être vérifiée. Lors de cette première connexion on nous présente l'empreinte de la clé publique de la machine en question en nous demandant si nous voulons poursuivre la communication.

Rmq : nous devrions accepter de poursuivre uniquement si nous sommes en mesure de vérifier que l'empreinte de la clé présentés est bien celle de l'hôte sur lequel on souhaite se connecter.

Pour cela, nous auriont dû nécessairement recup cette empreinte au préalable sutr le serveur en questtion. Si nous ne sommes pas en mesures de vérifier cette empreintes, nous sommes dans l'incapcité de determiné l'identité de l'hote et nous nous exposons potentiellement à une attaque de type homme du milieu (mitm).

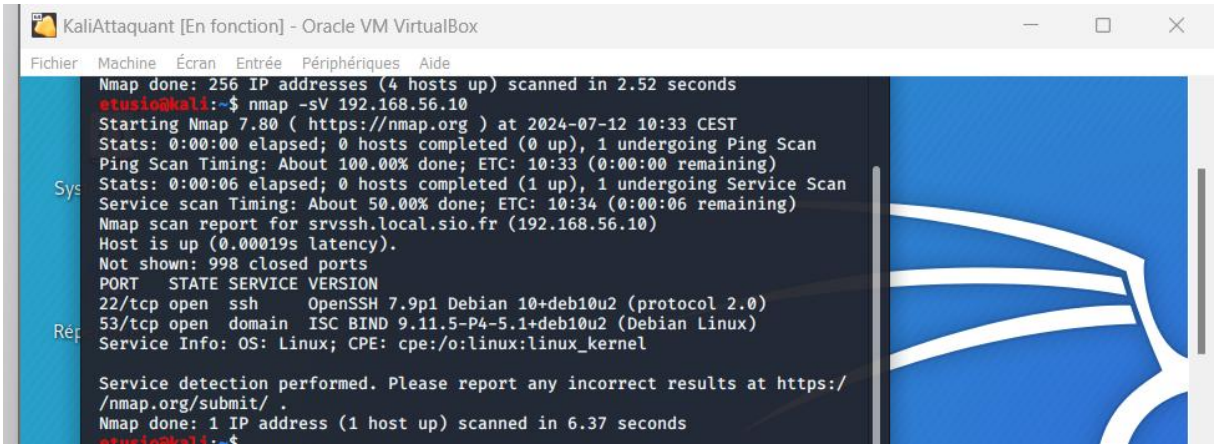
Q6. Non, car à présent l'hote est connu.

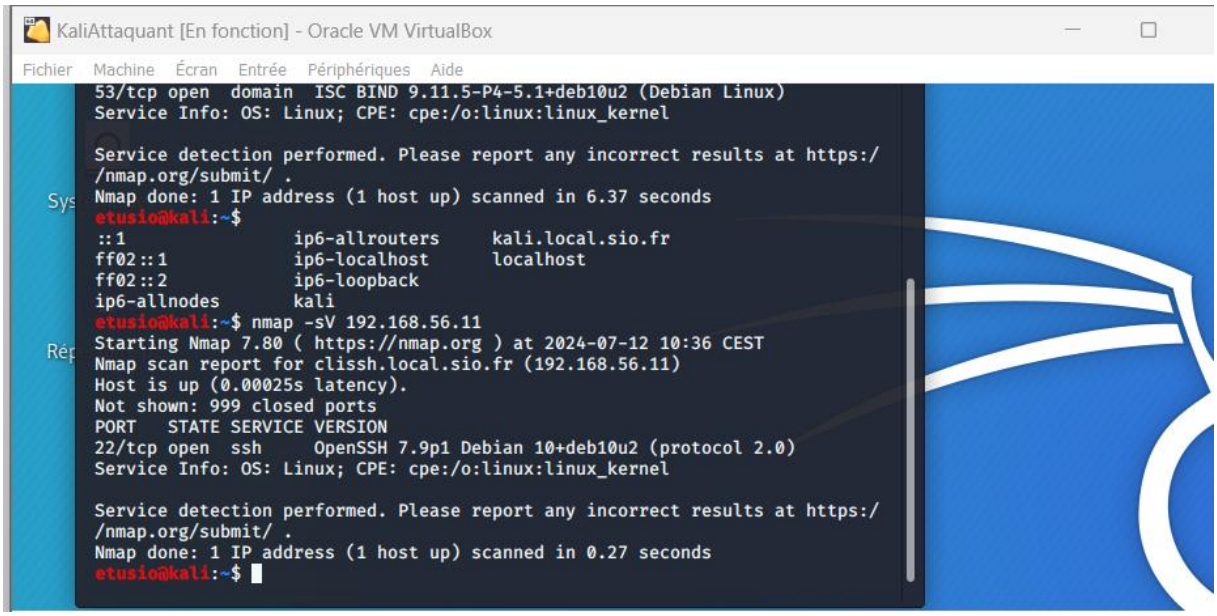
Si l'empreinte a été précedamment accepte, le,mssg n'apparait plus car ssh se base sur le principe « trust on the first use »

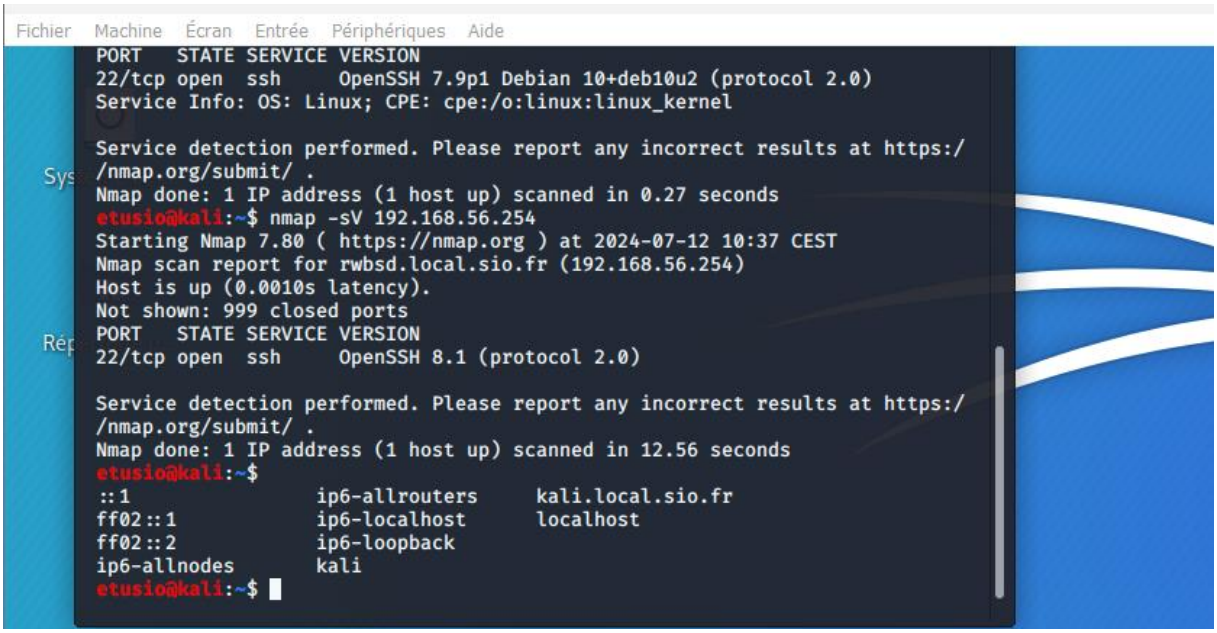
Lors de la premiere connexion il est demandé s'il on connait l'empreinte de la clé publique du serveur. Si l'on valide cette identité, le clissh enregistre la correspondance entre cette empreinte et le nom de domaine ou l'@ ip du serveur

Le fichier de correspondance présent de l'user etusio sur la machine client est /home/etusio/.ssh/know_hosts

Q7. Il permet de répertorier les hôtes connu pour éviter le message de sécu.







Q8. L'attaquant peut connaître le nombre d'hotes présent sur le réseau, leur addresses ip et les ports ouverts sur les machines. En connaissant les ports ouverts, l'attanquant connait la faille qu'il peut exploiter.

Correction :

Nmap réalise un scan sur les differente @ip selec puis affiche les port ouvert ainsi que les version des services à l'écoute sur ses ports

Q9. L'attaquant se place entre le client et le serveur afin d'intercepeter les commandes.

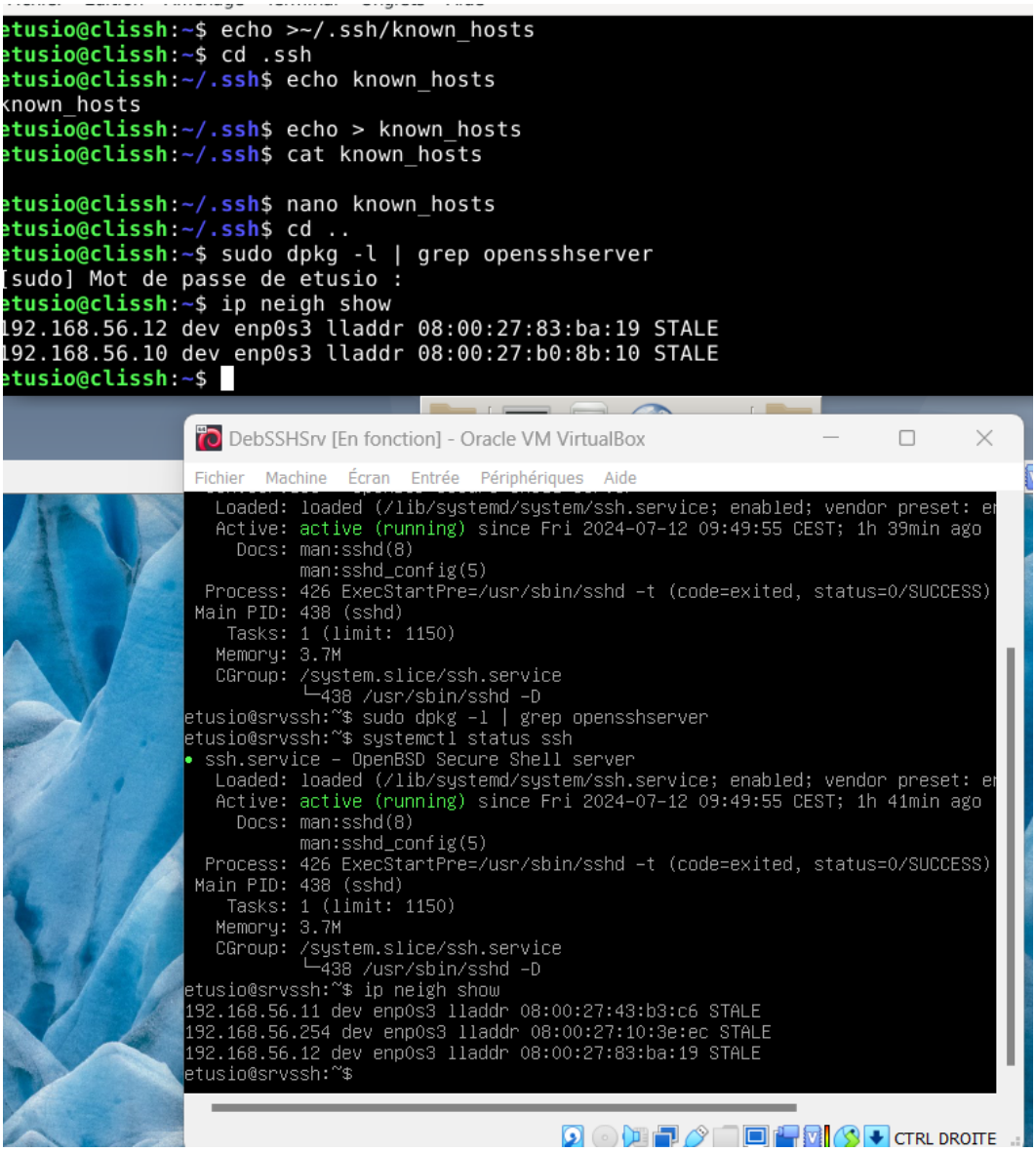
Voir/chercher def précise

Une attaque de l(homme du milieu consiste pour un attaquant à recup le trafic circulant entre deux hôtes sur le reseau sans quil ne s'en rendent compte.

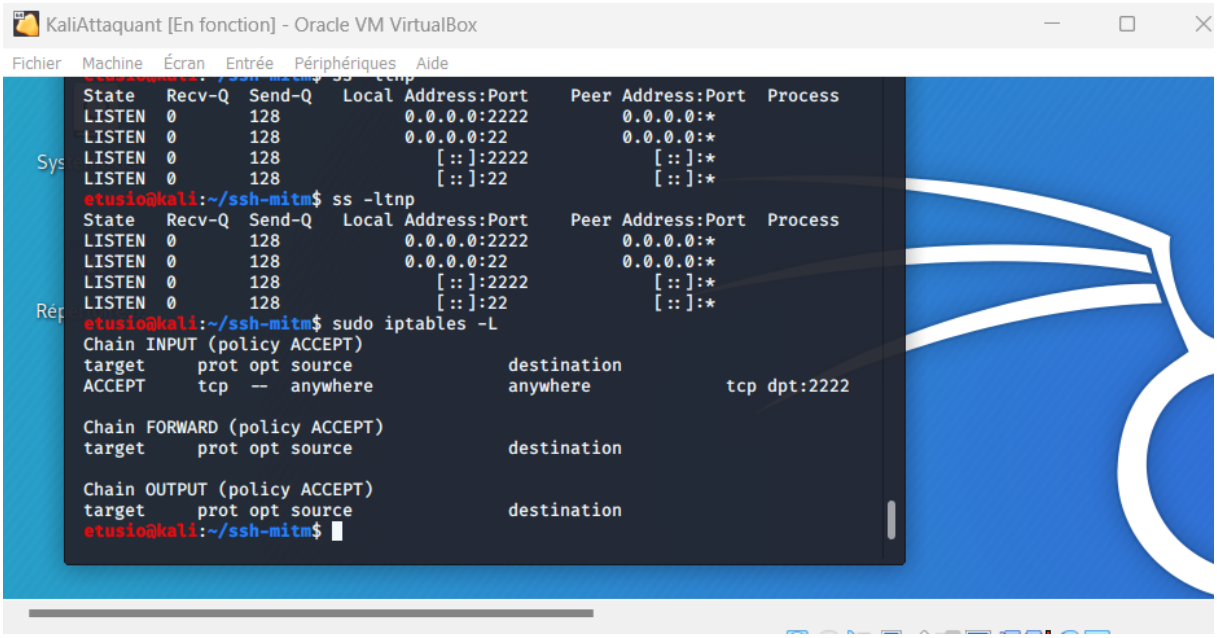
Si l'attaqua,t réalise une **attaque passive** son but est d'ecouter ce quil se passe afin de récupérer des infos et dans ce cas on porte atteinte à la confidentialité des échanges.

Dans le cas ou l'attaque es **active**, il peut dans ce cas modifier le contenu des d=échanges, il porte ainsi a la **confidentialité et l'intégrité** des échanges

Q10. Adresses cohérente car


etusio@clissh:~$ echo >~/.ssh/known_hosts
etusio@clissh:~$ cd .ssh
etusio@clissh:~/.ssh$ echo known_hosts
known_hosts
etusio@clissh:~/.ssh$ echo > known_hosts
etusio@clissh:~/.ssh$ cat known_hosts
etusio@clissh:~/.ssh$ nano known_hosts
etusio@clissh:~/.ssh$ cd ..
etusio@clissh:~$ sudo dpkg -l | grep opensshserver
[sudo] Mot de passe de etusio :
etusio@clissh:~$ ip neigh show
192.168.56.12 dev enp0s3 lladdr 08:00:27:83:ba:19 STALE
192.168.56.10 dev enp0s3 lladdr 08:00:27:b0:8b:10 STALE
etusio@clissh:~$
DebSSHSrv [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: en
Active: active (running) since Fri 2024-07-12 09:49:55 CEST; 1h 39min ago
Docs: man:sshd(8)
man:sshd_config(5)
Process: 426 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
Main PID: 438 (sshd)
Tasks: 1 (limit: 1150)
Memory: 3.7M
CGroup: /system.slice/ssh.service
└438 /usr/sbin/sshd -D
etusio@srvssh:~$ sudo dpkg -l | grep opensshserver
etusio@srvssh:~$ systemctl status ssh
• ssh.service - OpenBSD Secure Shell server
Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: en
Active: active (running) since Fri 2024-07-12 09:49:55 CEST; 1h 41min ago
Docs: man:sshd(8)
man:sshd_config(5)
Process: 426 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
Main PID: 438 (sshd)
Tasks: 1 (limit: 1150)
Memory: 3.7M
CGroup: /system.slice/ssh.service
└438 /usr/sbin/sshd -D
etusio@srvssh:~$ ip neigh show
192.168.56.11 dev enp0s3 lladdr 08:00:27:43:b3:c6 STALE
192.168.56.254 dev enp0s3 lladdr 08:00:27:10:3e:ec STALE
192.168.56.12 dev enp0s3 lladdr 08:00:27:83:ba:19 STALE
etusio@srvssh:~$
CTRL DROITE

Q11.



Q11.

Q12.

Q13. Attaque Arp spoofing : L'attaquant intercepte des données en détournant la communication des appareils entre eux, connectés sur un réseau LAN.

Le pirate s'étant placer entre le client et le serveur, ce type d'attaque lui permettra d'obtenir des informations suppléméntaire sur la cible.

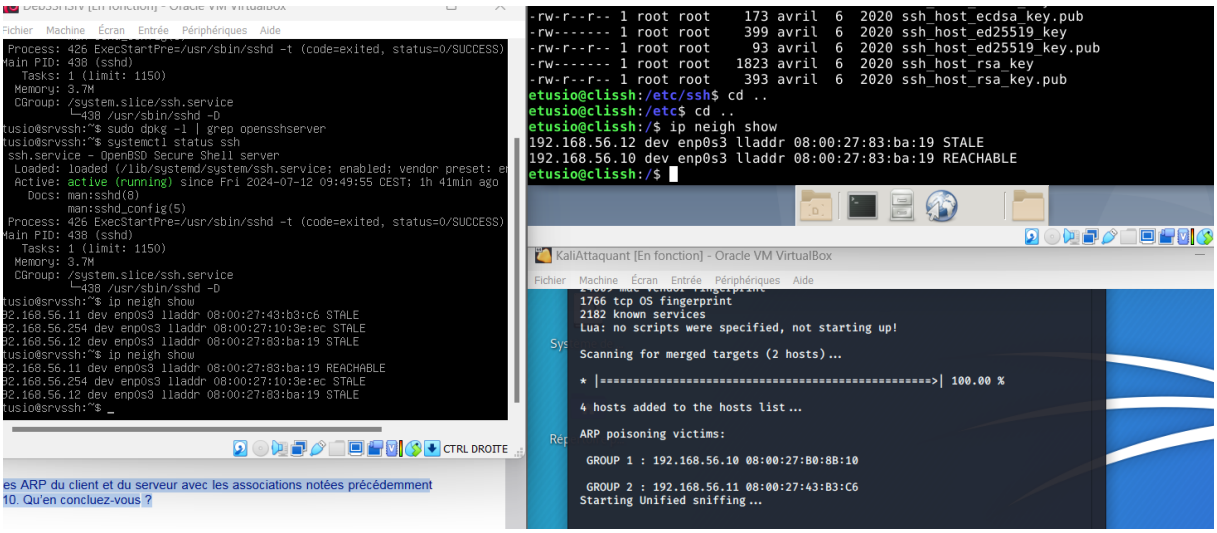
L'attaquant se place entre le client et le serveur. Ainsi les victimes vont sans le savoir lui transmettre leur écfhanges et suite à l'attaque arp spoofing, l'emmeteur enverra sa requête encapsuler dans une trame ethernet à destination de l'adresse mac de l'attaquant.

Pour que cette requête soit transmise au destinateur légitime, l'attaquant va desencapsuler la trame ethernet pour ananlyser l'entete ip qui copntienne (cette entte na pas été modifié) sans l'activation du routage sur kali, cette dernière ne sera pas zen mesure … ver le sdest légitime.

Q14.Comparer les caches ARP du client et du serveur avec les associations notées précédemment

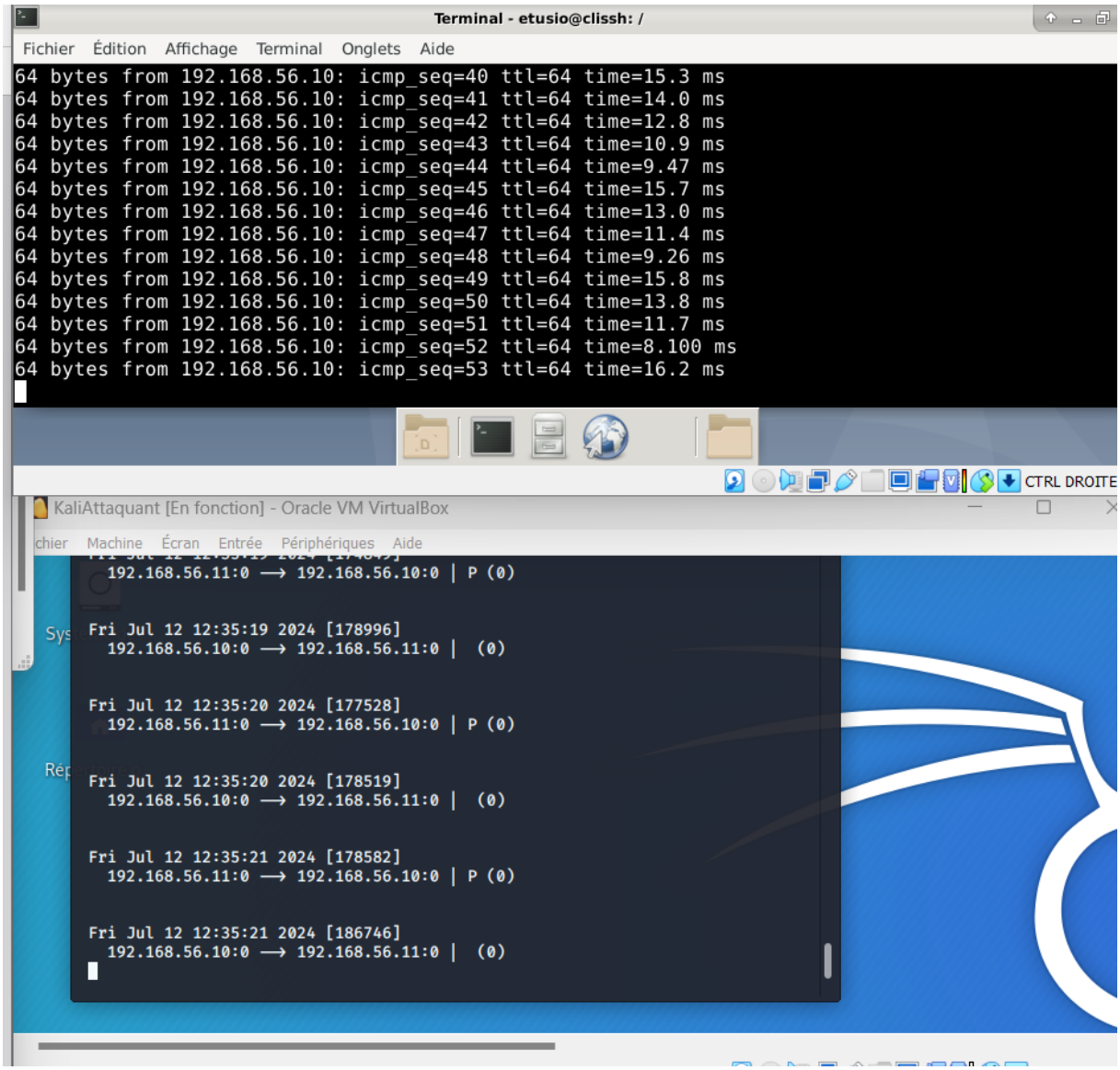
lors de la question 10. Qu'en concluez-vous ?

A présent .10 et .11 so,t reachable.

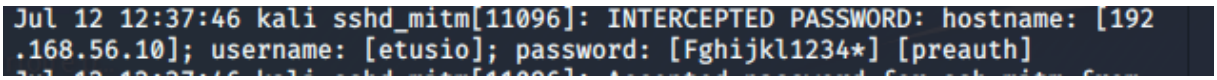


Q15.À partir de ces différentes observations, expliquer en détails comment fonctionne une attaque ARP Spoofing

16.Envoyer une requête ping (icmp-écho) depuis le client vers le serveur (192.168.56.10). Puis vérifier à l'aide d'une capture de trame sur la machine Kali Linux que ces dernières passent effectivement bien par l'attaquant. Quels éléments démontrent que l'attaque se déroule correctement ?



Q17.



Q18. Le fichier contient l'ensemble des cmdes effectués sur le clissh

Q19. Avec l'attaque, la table Arp a change. Le message d'erreur indique que la clé privée a étét changé. Et pas sécurité l'accès ssh est interdit.

Q20. Il faut effacer les clefs enregistrer dans le fichier .ssh/known_hosts

Modification du fichier sshd_config sur le serveur ssh

```
PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
AuthorizedKeysFile      .ssh/authorized_keys .ssh/authorized_keys2
```

Génération de la clef publique et privée pour l'authentification sur le client

```
etusio@clissh:~$ ssh-keygen -b 256 -t ecdsa
Generating public/private ecdsa key pair.
Enter file in which to save the key (/home/etusio/.ssh/id_ecdsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/etusio/.ssh/id_ecdsa.
Your public key has been saved in /home/etusio/.ssh/id_ecdsa.pub.
The key fingerprint is:
SHA256:3F7S472bySaF82F6wRNdBJO5KEtCtIWmX6F9+K579o0 etusio@clissh
The key's randomart image is:
+---[ECDSA 256]---+
|        ....   o=.|
|         +o.   o..|
|       +.o o . o.|
|      ..o.*.o o .|
|       .S+o=+o . |
|        ...++oB  |
|           ...*.+ |
|             *.+* |
|          o= =E..|
+----[SHA256]-----+
```

Q21. Car il est plus robuste

Q22. Pour que personne à part la personne qui l'a créé y ait accès

Q23.

```
etusio@clissh:~$ ls -a .ssh/
.  ..  id_ecdsa  id_ecdsa.pub  known_hosts
```

```
etusio@clissh:~$ cat .ssh/id_ecdsa.pub
ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBOp
Dnw35ar8gRmpoYsHMg6iMbtUHt1mSQRcQjv7nNXa5mMMsKAyhWHyf9uqDDGb8HtJWoHIYp/6Ss2
gwQnzyB9c= etusio@clissh
```

Q24. Le client nous empêche de nous connecter car il faut que les droits pour la clé privée soient seulement en lecture écriture pour l'utilisateur

Q25.

```
etusio@srvssh:~$ ls -al .ssh/authorized_keys
-rw------- 1 etusio etusio 175 sept. 13 12:59 .ssh/authorized_keys
```

Q26. La passphrase n’est plus demandé, c’est le mdp de l’utilisateur du serveur qui est demandé. sz

Q27. Le client ne peut pas se connecter au serveur ssh car la clé publique a été changé et a été détecté

Q29. Cela permet d’être sur de la machine sur laquelle on va se connecter et éviter de se connecter à une machine pirate

Q30.

1. **Vérification des permissions des clés privées de chiffrement**

Vérification des permissions

ls -l /etc/ssh/ssh_host_*key

Modification des permissions si nécessaire

sudo chown root:root /etc/ssh/ssh_host_*key

sudo chmod 600 /etc/ssh/ssh_host_*key

2. **S’assurer que c’est bien la version 2 du protocole SSH qui est utilisée ;**

Modification du fichier de configuration SSH

sudo nano /etc/ssh/sshd_config

Assure-toi que cette ligne est présente

Protocol 2

3. **Le serveur SSH doit dorénavant écouter sur le port 222/TCP ;**

Dans /etc/ssh/sshd_config, modifie cette ligne

Port 222

Redémarre le service SSH pour prendre en compte les modifications

sudo systemctl restart sshd

4. **Vérifier que les droits sur les fichiers sont appliqués de manière stricte par SSH ;**

Vérification des permissions sur /etc/ssh

sudo ls -l /etc/ssh/

Vérifie que seuls root a les permissions nécessaires et ajuste si besoin

sudo chmod -R go-rwx /etc/ssh/*

5. **L’accès SSH par l’utilisateur root doit être interdite ;**

Dans /etc/ssh/sshd_config, assure-toi que cette ligne est présente

PermitRootLogin no

6. **Mettre en œuvre une séparation des privilèges à l’aide d’un bac à sable (sandbox) ;**

Dans /etc/ssh/sshd_config, ajoute ou vérifie la ligne suivante

UsePrivilegeSeparation sandbox

7. **L’accès à distance par des comptes ne disposant pas de mot de passe doit être interdit ;**

Dans /etc/ssh/sshd_config

PermitEmptyPasswords no

8. **Autoriser 3 tentatives de connexion successives en cas d’erreur dans le mot de passe ;**

Dans /etc/ssh/sshd_config

MaxAuthTries 3

9. **Le service doit afficher les informations de dernière connexion à l’utilisateur quand il se connecte ;**

Dans /etc/ssh/sshd_config, assure-toi que la ligne suivante est activée

PrintLastLog yes

10. **N’autoriser que l’utilisateur etusio à se connecter sur le serveur.**

Dans /etc/ssh/sshd_config

AllowUsers etusio