

Activité 1 – attaque MITM d’un service SSH et mise en place de contre-mesures

Partie 1 – Attaque MITM d’un service SSH :

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

L’accès est restreint pour le super-administrateur root pour des raisons de sécurité. Un utilisateur ou un processus doit avoir uniquement les privilèges nécessaires pour effectuer sa tâche. Donner un accès complet à root peut compromettre la sécurité du système en permettant à un utilisateur d’exécuter des actions potentiellement dangereuses sans restrictions. Il est préférable d’utiliser des comptes d’utilisateurs ordinaires avec des privilèges limités pour effectuer des tâches courantes et de réserver l’accès au compte super-utilisateur (root) pour des opérations spécifiques qui exigent ces privilèges élevés.

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

La commande « sudo » est un outil de gestion des droits d’accès sur les systèmes Unix et Linux. Elle permet à un utilisateur de bénéficier temporairement des privilèges d’un autre utilisateur, souvent le super-utilisateur (root), afin d’exécuter des commandes qui nécessitent des autorisations spécifiques.

Au lieu de donner à un utilisateur un accès complet en tant que super-utilisateur, **sudo** permet de spécifier précisément quelles commandes ou quelles opérations un utilisateur est autorisé à exécuter en tant que super-utilisateur. Administration déléguée (Plusieurs utilisateurs avec des permissions définies.)

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

\$ sudo systemctl status ssh

Q4. Indiquer le répertoire où sont stockées les clés publique et privée créées ainsi que le positionnement des permissions appliquées sur les fichiers correspondants. Puis indiquer quel est le fichier de configuration du service SSH.

Clé publique : `home/etusio/.ssh/id_rsa` et pour les permissions : 644 (le propriétaire peut lire et écrire dans le fichier tandis que les autres utilisateurs peuvent seulement le lire.)

Clé privée : `~/ssh/id_rsa` et pour les permissions : 600 (seul le propriétaire de la clé peut lire et écrire dans ce fichier)

Le fichier de configuration est situé dans ‘`/etc/ssh/ssh_config`’

Q5. Que signifie cette alerte qui est affichée à l'écran ? Devez-vous continuer l'opération ? Pourquoi ?

Le certificat n'est pas valide, mais on peut continuer l'opération et ainsi être ajouté à la liste 'known hosts' et demander le mot de passe sur serveur ssh.

Q6. Lors d'une prochaine connexion depuis le même client sur ce serveur, ce message apparaîtra-t-il à nouveau ? Pourquoi ?

Non car on se trouve toujours dans la liste des serveurs host connus et nous demandons de se connecter directement.

Q7. Sur la machine virtuelle cliente, expliquer à quoi sert le fichier /home/etudio/.ssh/known_hosts.

Ils stockent les clés publiques des serveurs auxquels l'utilisateur s'est connecté et garantissent l'authenticité des serveurs SSH et ainsi préviennent l'utilisateur en cas de changement dans la clé publique de serveur, ce qui peut indiquer un problème de sécurité.

Q8. Indiquer quelles sont les informations que peut obtenir un attaquant grâce à ces commandes ?

`nmap -sP 192.168.56.0/24` = Scanne le réseau et liste les hôtes actifs sur le réseau.

`nmap -sV 192.168.56.10` → Liste des ports ouverts et services associés à l'hôte.

Q9. Expliquer les principes généraux d'une attaque de l'homme du milieu (Man in the Middle).

Une attaque de l'homme du milieu (Man-in-the-Middle ou MITM) est une technique d'attaque dans laquelle un attaquant intercepte et éventuellement modifie les communications entre deux parties sans que ni l'une ni l'autre ne le sache. L'attaquant se place littéralement entre les deux parties, agissant comme un intermédiaire trompeur :

1. **Interception des communications**
2. **Interférence avec les communications**
3. **Maintien de la discrétion**
4. **Collecte d'informations sensibles**

Passive → confidentialité compromise

Q10. Noter les associations adresse IP / adresse MAC présentes sur les deux machines. Sont-elles cohérentes ?

192.168.56.10 08:00:27:71:8C:66

192.168.56.11 08:00:27:03:48:CD

192.168.56.12 08:00:27:96:0A:7D

192.168.56.254 08:00:27:71:3B:1E

c'est bien la bonne association @ IP/MAC

Q11. Pourquoi l'activation du routage sur la machine de l'attaquant est indispensable au bon fonctionnement de l'attaque MITM ?

Il doit être en mesure de router les paquets le temps de l'attaque pour que le script start.sh puisse s'exécuter. Il doit décapsuler les trames venant de la machine cible pour obtenir les @IP destination pour ensuite l'encapsuler et l'envoie au destinataire de la trame avec l'@MAC de la machine cible.

Q12. Pourquoi cette redirection de ports est indispensable au succès de l'attaque de l'homme du milieu ?

La redirection de ports est indispensable car il y a une règle de filtrage sur le port 2222 qui accepte les connexion tcp. Sans cela, impossible de rediriger les flux de la machine cible vers le serveurs ssh.

Q13. Indiquer en quoi une attaque de type ARP Spoofing peut être utile ici au pirate ?

L'usurpation du protocole ARP est une attaque consistant à utiliser un protocole de résolution d'adresse sur un réseau local (LAN). Un protocole de résolution d'adresse est un protocole de communication qui connecte une adresse IP (Internet Protocol, ou protocole Internet) dynamique à l'adresse d'une machine physique, ou adresse MAC (Media Access Control). Le protocole ARP dirige la communication vers le réseau local.

On parle d'usurpation du protocole ARP lorsqu'un cyberattaquant ayant accès au réseau local se fait passer pour l'hôte B. Le cyberpirate envoie des messages à l'hôte A dans le but de leurrer ce dernier et de lui faire enregistrer son adresse comme étant celle de l'hôte B. De ce fait, l'hôte A enverra les communications destinées à l'hôte B directement au cyberattaquant. Dans ce type d'attaque appelé « man-in-the-middle », toute communication de l'hôte A vers l'hôte B est d'abord interceptée par le cyberattaquant avant de parvenir au destinataire prévu, l'hôte B servant généralement de passerelle par défaut, ou de routeur.

Q14. Comparer les caches ARP du client et du serveur avec les associations notées précédemment lors de la question 10. Qu'en concluez-vous ?

Sur le client, les @ip de la machine 192.168.56.10 ainsi que 192.168.56.12 ont la meme @MAC : 08:00:27:96:0A:7D(@MAC de la machine attaquant.)

```
etusio@clissh:~$ ip neigh show
192.168.56.12 dev enp0s3 lladdr 08:00:27:96:0a:7d STALE
192.168.56.10 dev enp0s3 lladdr 08:00:27:96:0a:7d REACHABLE
```

```
etusio@srvssh:~$ ip neigh show
192.168.56.12 dev enp0s3 lladdr 08:00:27:96:0a:7d STALE
192.168.56.11 dev enp0s3 lladdr 08:00:27:03:48:dc REACHABLE
192.168.56.254 dev enp0s3 lladdr 08:00:27:71:3b:1e STALE
```

AVANT/APRES sur le serveur ssh :

```
etusio@srvssh:~$ ip neigh show
192.168.56.12 dev enp0s3 lladdr 08:00:27:96:0a:7d STALE
192.168.56.11 dev enp0s3 lladdr 08:00:27:96:0a:7d REACHABLE
192.168.56.254 dev enp0s3 lladdr 08:00:27:71:3b:1e STALE
```

```

▼ Address Resolution Protocol (reply)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: reply (2)
  Sender MAC address: PcsCompu_96:0a:7d (08:00:27:96:0a:7d)
  Sender IP address: 192.168.56.10
  Target MAC address: PcsCompu_03:48:dc (08:00:27:03:48:dc)
  Target IP address: 192.168.56.11

```

Lors de la capture depuis la machine client, on peut apercevoir que la machine client 192.169.56.11 reçoit en permanence des requêtes ARP de la part du soit-disant serveur ayant l'@IP 192.168.56.10 mais elle possède l'@MAC de la machine pirate. Donc la machine cible ne se doute pas qu'une machine pirate est en train de détourner le flux du trafic entre la machine cible et le serveur. Pensant que le serveur lui envoie des requêtes ARP pour inondé la table ARP de la machine cible.

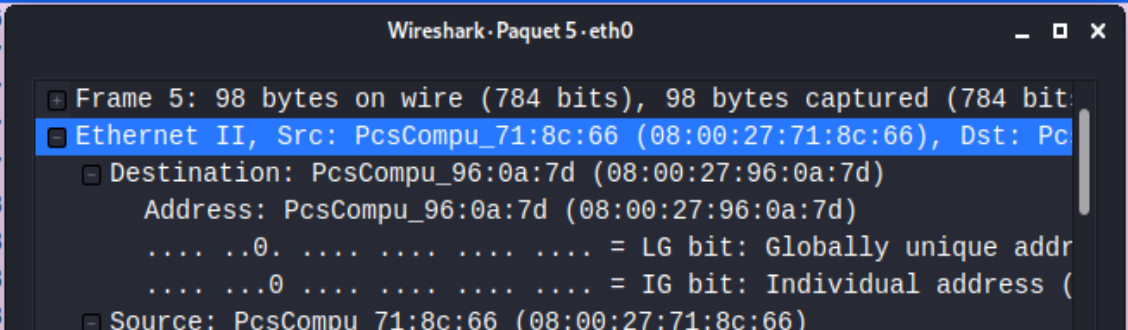
Q15.À partir de ces différentes observations, expliquer en détails comment fonctionne une attaque ARP Spoofing.

c'est une technique utilisée en informatique pour attaquer tout réseau local utilisant le protocole de résolution d'adresse ARP, les cas les plus répandus étant les réseaux Ethernet et Wi-Fi. Cette technique permet à l'attaquant de détourner des flux de communications transitant entre une machine cible et un hôte sur le réseau : ordinateur, routeur, box, etc. L'attaquant peut ensuite écouter, modifier ou encore bloquer les paquets réseaux.

1) Être dans le même réseau IP que la machine cible -----> repérer les associations des @IP et @MAC respectif des machines présent sur le réseau grâce à **ip neigh show** -----> polluer le cache ARP des machine cible pour faire attribuer une « fausse »@MAC à la cible

Q16. 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 ?

1	0.000...	PcsCompu_96:0a:7d	PcsCompu_71:8c:66	ARP	42	192.168.56.11	is at	08:00:27:96:0a:7d
2	0.000...	PcsCompu_96:0a:7d	PcsCompu_03:48:dc	ARP	42	192.168.56.10	is at	08:00:27:96:0a:7d
3	6.405...	192.168.56.11	192.168.56.10	ICMP	98	Echo (ping) request	id=	192.168.56.10
4	6.407...	192.168.56.11	192.168.56.10	ICMP	98	Echo (ping) request	id=	192.168.56.10
5	6.408...	192.168.56.10	192.168.56.11	ICMP	98	Echo (ping) reply	id=	192.168.56.11



Wireshark - Paquet 5 - eth0

Frame 5: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface eth0

Ethernet II, Src: PcsCompu_71:8c:66 (08:00:27:71:8c:66), Dst: PcsCompu_96:0a:7d (08:00:27:96:0a:7d)

Destination: PcsCompu_96:0a:7d (08:00:27:96:0a:7d)

Address: PcsCompu_96:0a:7d (08:00:27:96:0a:7d)

.....0..... = LG bit: Globally unique address (标准要求)

.....0..... = IG bit: Individual address (标准要求)

Source: PcsCompu_71:8c:66 (08:00:27:71:8c:66)

On peut voir les échanges ICMP entre le client et le serveur mais la particularité est que le serveur répond vers l'@MAC 08:00:27:96:0A:7D qui est dans son cache ARP l'@MAC de la machine cible ET attaquant.

Q17. Recopier la ligne qui contient le login et le mot de passe capturés dans le fichier `/var/log/auth.log`.

```
Oct 3 13:55:02 kali CRON[1263]: pam_unix(cron:session): session closed for user root
Oct 3 14:05:01 kali CRON[1270]: pam_unix(cron:session): session opened for user root by (uid=0)
Oct 3 14:05:01 kali CRON[1270]: pam_unix(cron:session): session closed for user root
Oct 3 14:14:57 kali sshd_mitm[1276]: INTERCEPTED PASSWORD: hostname: [192.168.56.10]; username: [etusio]; password: [Fghijkl1234*] [preauth]
Oct 3 14:14:57 kali sshd_mitm[1276]: Accepted password for ssh-mitm from 192.168.56.11 port 59458 ssh2
Oct 3 14:15:01 kali CRON[1281]: pam_unix(cron:session): session opened for user root by (uid=0)
Oct 3 14:15:01 kali CRON[1281]: pam_unix(cron:session): session closed for user root
Oct 3 14:17:01 kali CRON[1284]: pam_unix(cron:session): session opened for user root by (uid=0)
Oct 3 14:17:01 kali CRON[1284]: pam_unix(cron:session): session closed for user root
Oct 3 14:17:58 kali sudo: root : TTY=pts/0 ; PWD=/home/etusio/ssh-mitm ; USER=root ; COMMAND=./stop.sh
Oct 3 14:17:58 kali sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Oct 3 14:17:58 kali sshd_mitm[1018]: Received signal 15; terminating.
Oct 3 14:17:59 kali sudo: pam_unix(sudo:session): session closed for user root
root@kali:/home/etusio/ssh-mitm# cat /var/log/auth.log
```

Q18. Que contient le fichier `/home/ssh-mitm/shell_session_0.txt` présent sur Kali Linux ?

```
root@kali:/home/ssh-mitm# ls
bin client.log empty etc run.sh shell_session_0.txt tmp
root@kali:/home/ssh-mitm# cat shell_session_0.txt
Time: 2024-10-03 12:14:57 GMT
Server: 192.168.56.10:22
Client: 192.168.56.11:59458
Username: etusio
Password: Fghijkl1234*
-----
Linux srvssh 4.19.0-8-amd64 #1 SMP Debian 4.19.98-1+deb10u1 (2020-04-27) 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.
Last login: Thu Oct 3 13:20:38 2024
etusio@srvssh:~$ ssuuddoo ccaatt //eett c//sshh aaddooww
[sudo] Mot de passe de etusio : Fghijkl1234*
root:!:18350:0:99999:7:::
daemon:!:18350:0:99999:7:::
bin:!:18350:0:99999:7:::
sys:!:18350:0:99999:7:::
sync:!:18350:0:99999:7:::
games:!:18350:0:99999:7:::
```

Dans le fichier, on y retrouve les informations principale de l'attaque précédente avec la date et l'heure exacte, l'@IP/port du serveur et du client, y compris le login et mot de passe du serveur ainsi que des informations sur le serveur cible.

Q19. Expliquer pourquoi ce message d'erreur apparaît ?

La clé d'identification de l'hôte distant a changé dans le fichier `Known_host`. Cela est du à l'attaque man-in-the-middle qui détourner le flux du trafic et qui a utilisé la clé d'hôte.

Q20. Proposer une solution afin de pouvoir à nouveau se connecter au service SSH depuis le client.

#ssh-keygen -R 192.168.56.11 puis se reconnecter au serveur SSH et accepter la nouvelle clé ssh.