Sécurité

Quelques failles

Quelques failles

- Le clickjacking
- Le phishing
- Attaque par force brute
- Les malwares
- Le sniffing
- L'usurpation d'adresse IP - IP Spoofing
- Man-in-the-Middle - ARP Poisoning
- MAC FLOODING
- DNS Spoofing
- Déni de service – DoS

Sécurité
Quelques failles

Le clickjacking

Le Clickjacking vise à pousser un internaute à fournir des informations confidentielles ou à prendre le contrôle de son ordinateur en le poussant à cliquer sur des pages sûres

Sécurité
Quelques failles

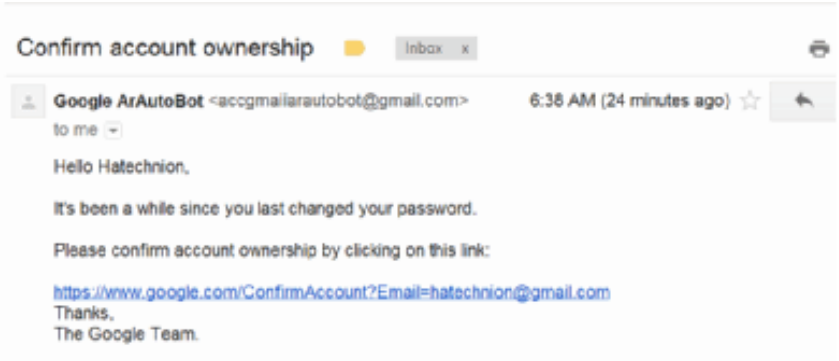
KEY LOGGER

Enregistre de façon indétectable la totalité des touches saisies sur votre clavier.

Sécurité
Quelques failles

Le phishing

Le phishing ou « hameçonnage » désigne une action malveillante opérée par un pirate informatique qui vise à soutirer une information confidentielle : informations bancaires, mots de passe, données relevant de votre vie privée.


Confirm account ownership Inbox x

Google ArAutoBot <acgmailarautobot@gmail.com> 6:38 AM (24 minutes ago)

to me

Hello Hatechnion,

It's been a while since you last changed your password.

Please confirm account ownership by clicking on this link:

https://www.google.com/ConfirmAccount?Email=hatechnion@gmail.com
Thanks,
The Google Team.

Sécurité
Quelques failles

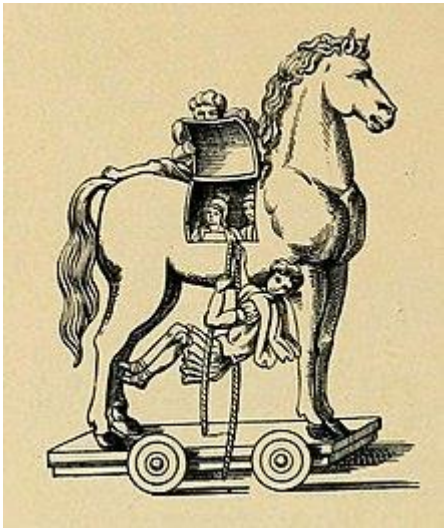
Attaque par force brute

L'attaque par force brute est une méthode utilisée pour trouver un mot de passe. Il s'agit de tester, une à une, toutes les combinaisons possibles.

Sécurité
Quelques failles

Les malwares

Ce sont les logiciels malveillants comme trojans, vers, spywares, adwares, virus qui peuvent d'une façon diffuser ou détruire l'information qui existe sur votre ordinateur.

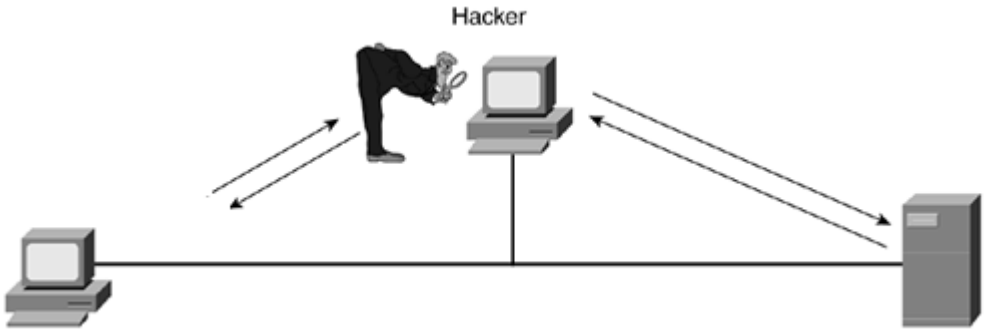


Sécurité
Quelques failles

Le sniffing

Consiste à écouter le réseau

Outil: sniffit



Sécurité
Quelques failles

L'usurpation d'adresse IP - IP Spoofing

L'attaque par usurpation d'adresse IP consiste à générer des paquets IP que semblent pour la cible provenir d'un poste accrédité

Outil: arpspoof

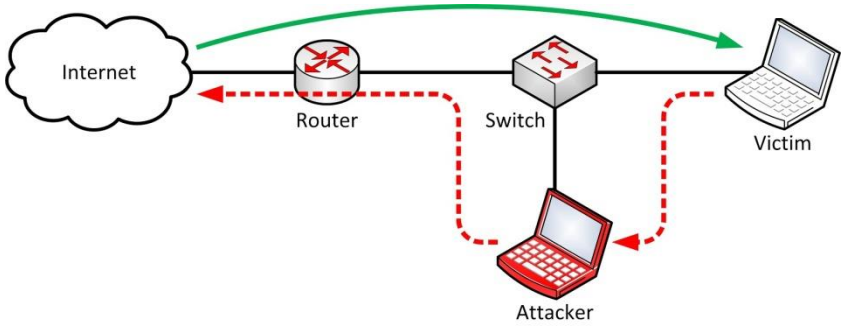
Sécurité
Quelques failles

Man-in-the-Middle - ARP Poisoning

C'est une forme d'IP Spoofing. Le pirate joue l'intermédiaire entre le client et un serveur (ou la passerelle de sortie vers Internet).

Il est le serveur vis-à-vis du client et il est le client vis-à-vis du serveur.

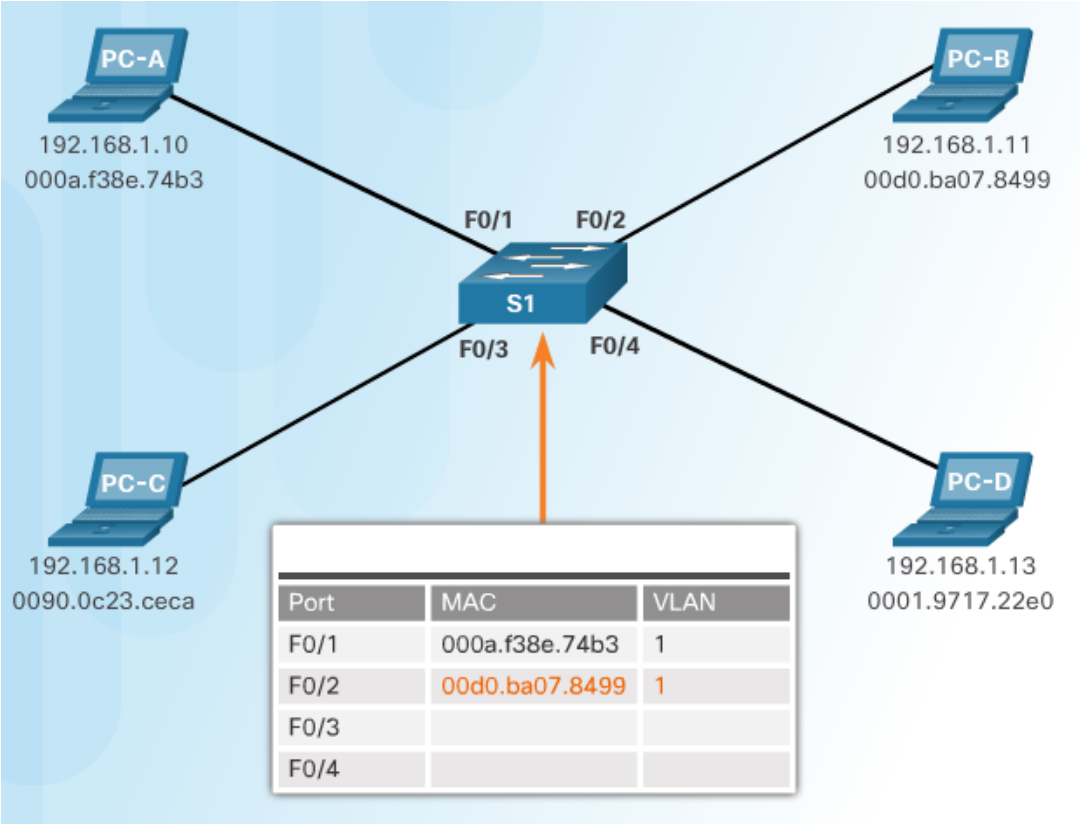
Il peut ainsi récolter des informations de confidentielles étant que tout le dialogue passe par sa machine



Sécurité
Quelques failles

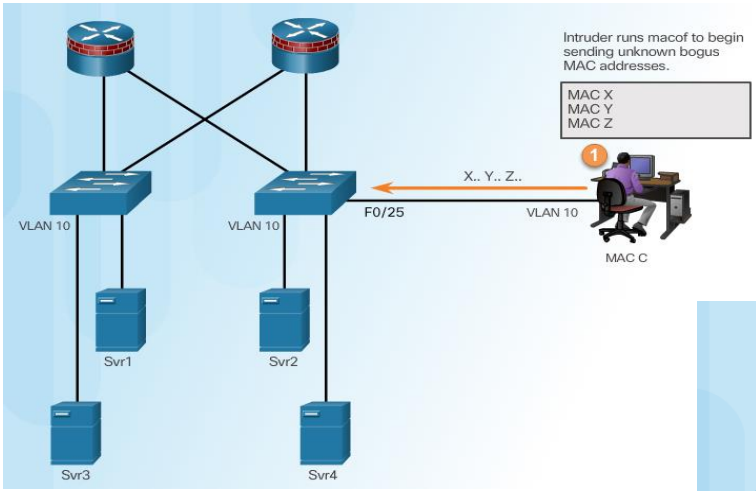
Attaque de type MAC FLOODING

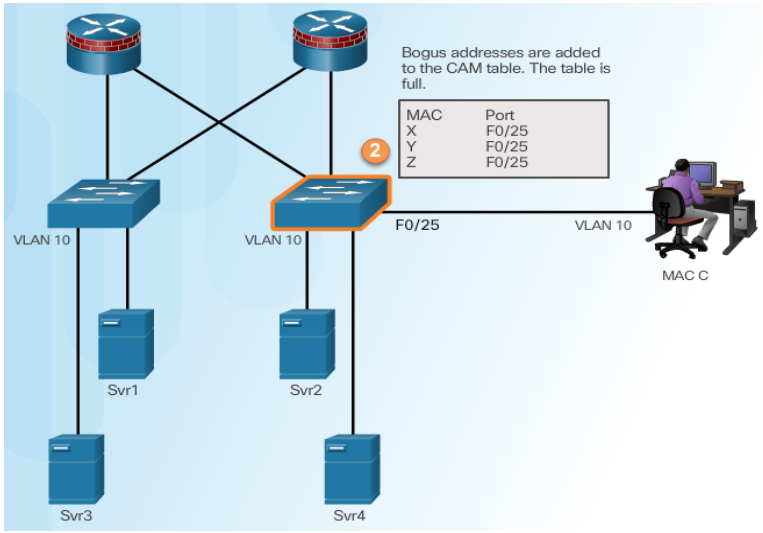
Table ARP d'un switch



Sécurité
Quelques failles

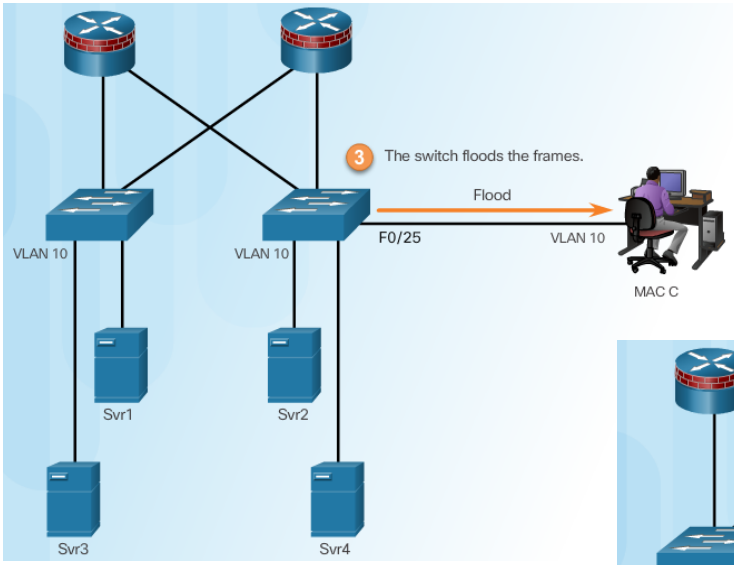
Attaque de type MAC FLOODING

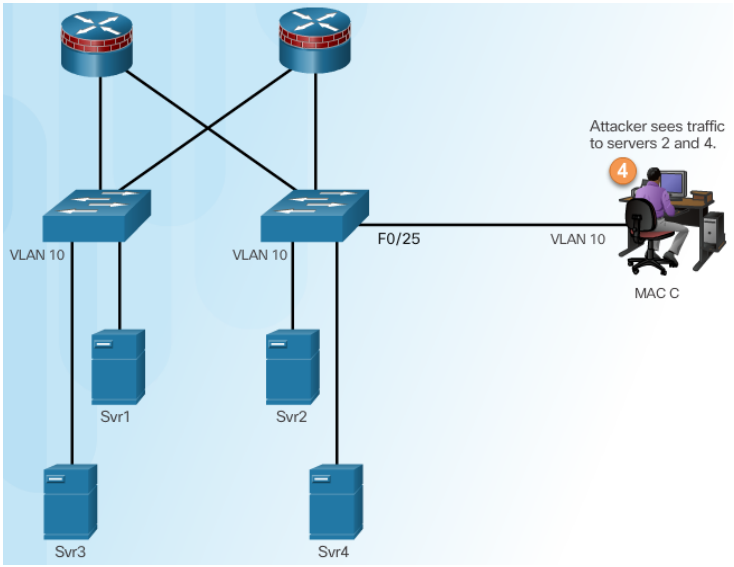




Sécurité
Quelques failles

Attaque de type MAC FLOODING





Sécurité
Quelques failles

DNS Spoofing

Cette attaque redirige, à leur insu, des Internautes vers des sites pirates.

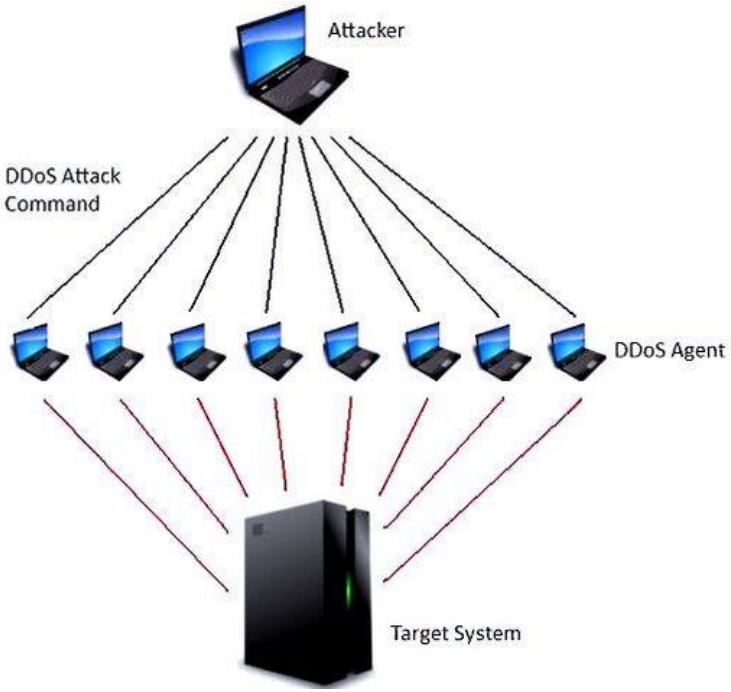
Le pirate fait correspondre nom réel et valide d'une machine publique à une adresse IP d'une machine qu'il contrôle.

Sécurité
Quelques failles

Déni de service – DoS

Cette attaque consiste à rendre inutilisable le système cible.

Soit en le surchargeant de requête, soit en le faisant « planter »



Sécurité
Quelques failles

Déni de service – DoS

TP avec les applications de DSNIFF:

- sniffing: sniffit
- usurpation d'adresse IP: arpspoof
- Mac flooding: macof
- Man-in-the-Middle : arpspoof
- DNS Spoofing: dnsspoof

Attention: Ce TP est uniquement à des fins éducatifs à faire dans le LAN prévu pour le TP.

Sécurité

Solution: Les utilisateurs, l'authentification

Linux est un système multi- utilisateur:

- Base de comptes utilisateurs et de comptes groupes
- Un fichier appartient à un utilisateur et à un groupe
- Les applications sont associées à des comptes utilisateurs et comptes groupes
- La connexion d'un utilisateur est associé à compte utilisateur et à un compte groupe

Sécurité

Solution: Les utilisateurs, l'authentification

Caractéristique d'un compte utilisateur

man 5 passwd

- Login
- Mot de passse
- UID
- GID
- Commentaire
- Répertoire de connexion
- Shell

Base de données locale des comptes utilisateurs: /etc/passwd

Sécurité

Solution: Les utilisateurs, l'authentification

Caractéristique d'un compte groupe

- Nom du groupe
- GID
- Mot de passe
- Liste des membres

- Base de données locale des comptes groupes: /etc/group

Sécurité

Solution: Les utilisateurs, l'authentification

Les mot de passe

Ce qu'il ne faut pas faire:

- Changer le mot de passe par défaut
- Utiliser un mot de passe en rapport avec vous,
- Des mots du dictionnaire,
- Un mot à l'envers,
- …
- Tout ce qui peut être deviné

Sécurité

Solution: Les utilisateurs, l'authentification

Les mot de passe

Ce qu'il faut faire:

- Le mot de passe doit être long (minimum 8 caractères)
- Utiliser les minuscules et des majuscules
- Utiliser des chiffres et des caractères spéciaux
- ….
- Le taper rapidement
- Changer régulièrement son mot de passe
- Ne pas transmettre le login et le mot de passe via le même canal

Sécurité

Solution: Les utilisateurs, l'authentification

Les mot de passe

Politique de l'administrateur:

- Imposer les utilisateur à respecter les règles de sécurité: /etc/login.defs

  PASS_MIN_LEN

- Fixer une durée d'expiration d'un mot de passe: chage

  chage -M 90 sysadmin
  chage -l sysadmin

Sécurité

Solution: Les utilisateurs, l'authentification

Les mot de passe

Politique de l'administrateur:

- Limiter la durée de via de certains comptes: chage

  chage -E 2019-12-31 prestataire02

- Verrouiller les comptes suspects: passwd -l ou usermod -L

  passwd -l sysadmin

Sécurité

Solution: Les utilisateurs, l'authentification

TP:

- **Attaque au dictionnaire avec John The Ripper**

  sudo cat /etc/shadow > passwordASR

  john --wordlist:fichier.dico passwordASR

  john --show passwordASR

Ou apt-get install wfrench

john -wordlist:/usr/share/dict/french passwordASR

- **Password aging**

- **Génération de mot de passe aléatoires**

  openssl rand -base64 16

  strings /dev/urandom | grep -o "[[:alnum:]]" | head -20 | tr -d "\n"

Sécurité

Contrôle d'accès au réseau : port-security

Solution contre certaines attaques

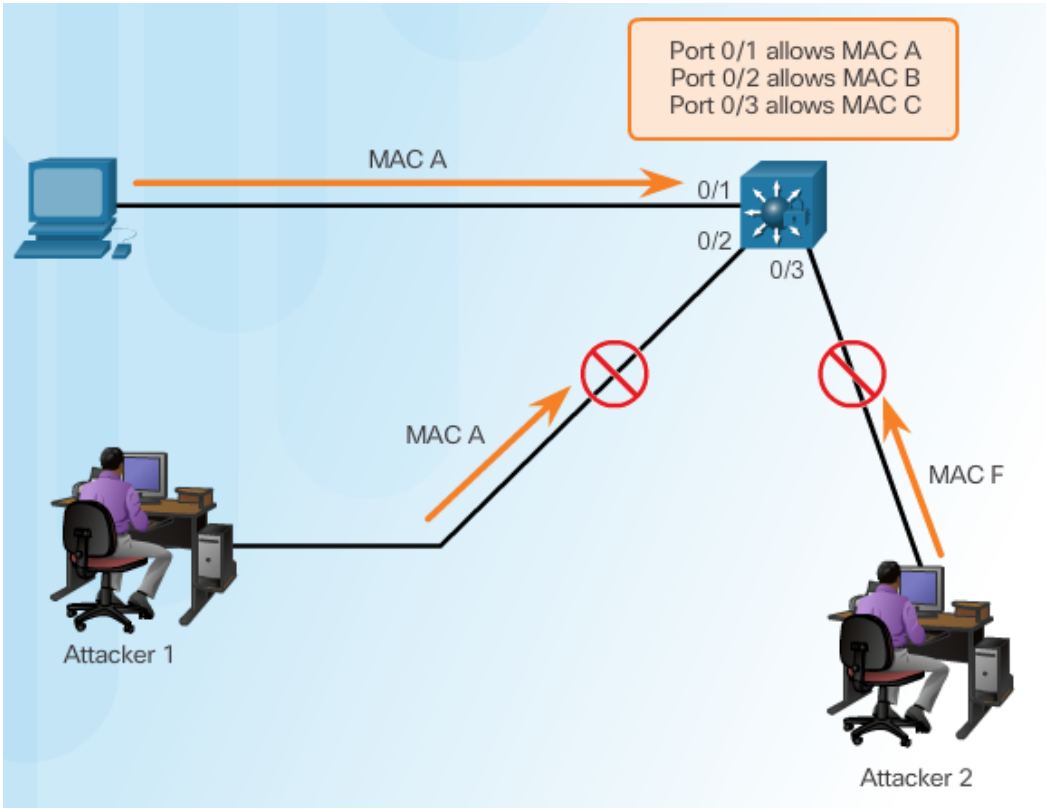
Sur le machine Linux, ajouter les adresses MAC dans le fichier /etc/ethers

```
root@srv-diokh:~# cat /etc/ethers
6C:71:D9:50:58:0C 192.168.43.1
root@srv-diokh:~#
```

Sécurité

Contrôle d'accès au réseau : port-security

Solution contre certaines attaques



Sécurité

Contrôle d'accès au réseau : port-security

PORT-SECURITY: activation, vérification et options

```
S1(config)# interface f0/1
S1(config-if)# switchport port-security
Command rejected: FastEthernet0/1 is a dynamic port.
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# end
S1#
```

Activation de la fonctionnalité de port security

Vérification de la fonctionnalité de port security

```
S1# show port-security interface f0/1
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
S1#
```

Les options

```
S1(config)# interface f0/1
S1(config-if)# switchport port-security ?
  aging         Port-security aging commands
  mac-address   Secure mac address
  maximum       Max secure addresses
  violation     Security violation mode
  <cr>

S1(config-if)# switchport port-security
```

Sécurité

Contrôle d'accès au réseau : port-security

PORT-SECURITY: gestion des adresses MAC

Définir le maximum d'adresse MAC

```
Switch(config-if)
switchport port-security maximum value
```

Définir manuellement l'adresse MAC

```
Switch(config-if)
switchport port-security mac-address mac-address {vlan | {access | voice}}
```

Enregistrement dynamique de l'adresse MAC

```
Switch(config-if)
switchport port-security mac-address sticky
```

Sécurité

Contrôle d'accès au réseau : port-security

PORT-SECURITY: les actions en cas de violation

Mode de violation:

- Protect
- Restrict
- Shutdown

Security Violation Modes

Violation Mode	Forwards Traffic	Sends Syslog Message	Increases Violation Counter	Shuts Down Port
Protect	No	No	No	No
Restrict	No	Yes	Yes	No
Shutdown	No	Yes	Yes	Yes

Sécurité

Contrôle d'accès au réseau : port-security

PORT-SECURITY: exemple


```
S1(config)# interface f0/1
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# switchport port-security maximum 3
S1(config-if)# switchport port-security violation shutdown
S1(config-if)# switchport port-security aging time 120
S1(config-if)#
```

Sécurité

Contrôle d’accès au réseau : port-security

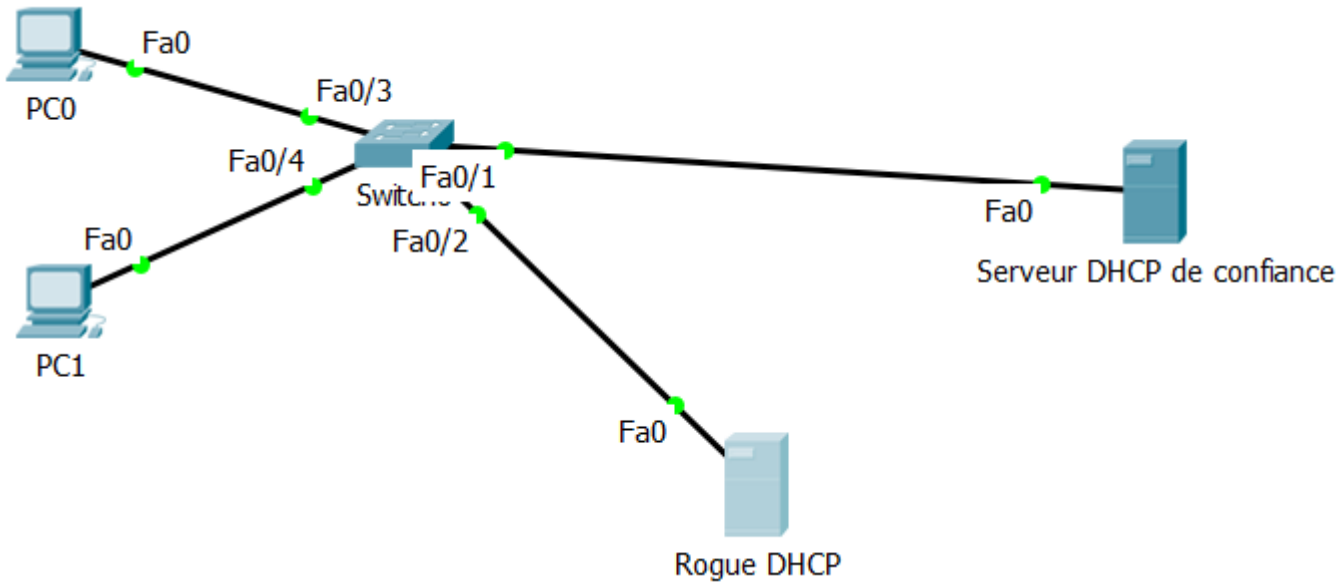
PORT-SECURITY: TP

TP sur Packet Tracer

Sécurité

Contrôle d'accès au réseau : DHCP SNOOPING

TP sur Packet Tracer




```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan 1
Switch(config)#int fa0/1
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#ip dhcp snooping limit rate 100
Switch(config-if)#
```