Guastamacchia
14/10/2024
Livio
SIO1

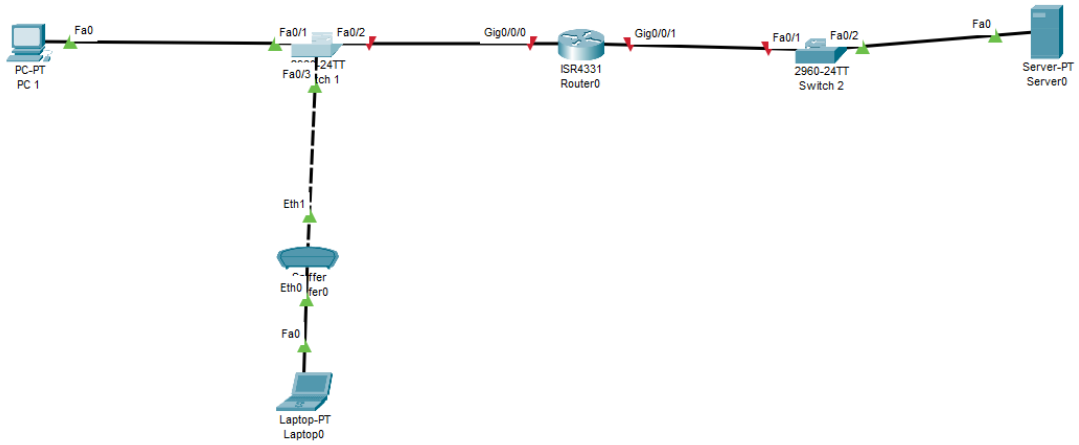
TP Cisco packet Tracer :

Introduction :

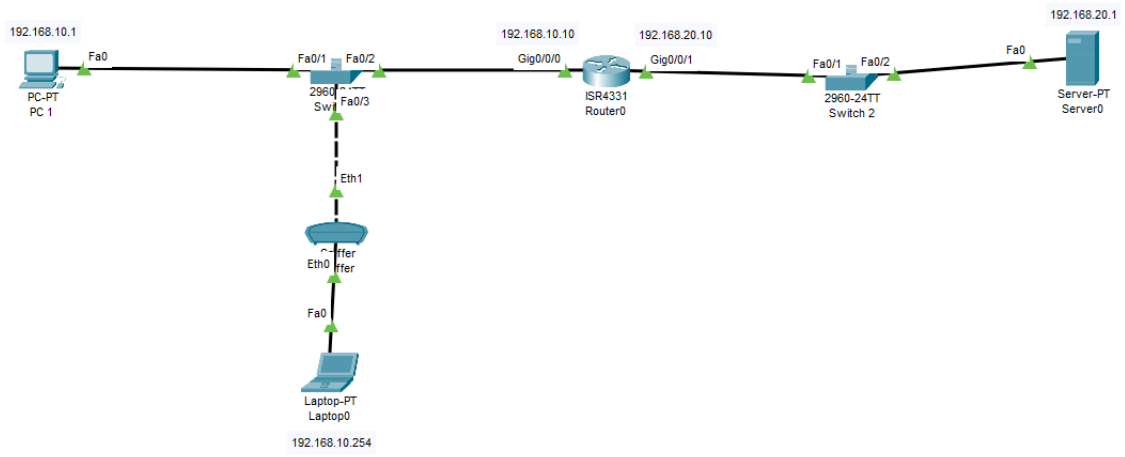
Dans ce TP nous allons représenter une attaque d'ARP Poisoning sur Packet Tracer puis par la suite nous devrons mettre en place des moyens de sécurisation pour protéger notre réseaux d 'une attaque similaire.

TP :

Pour commencer ce Tp nous allons déjà nous rendre dans le logiciel Cisco packet tracer et nous constituer une petit réseaux composer de : un pc, deux switch, un routeur, un pc portable, un sniffer et un server. Ce réseaux sera représenter comme ci-dessous.



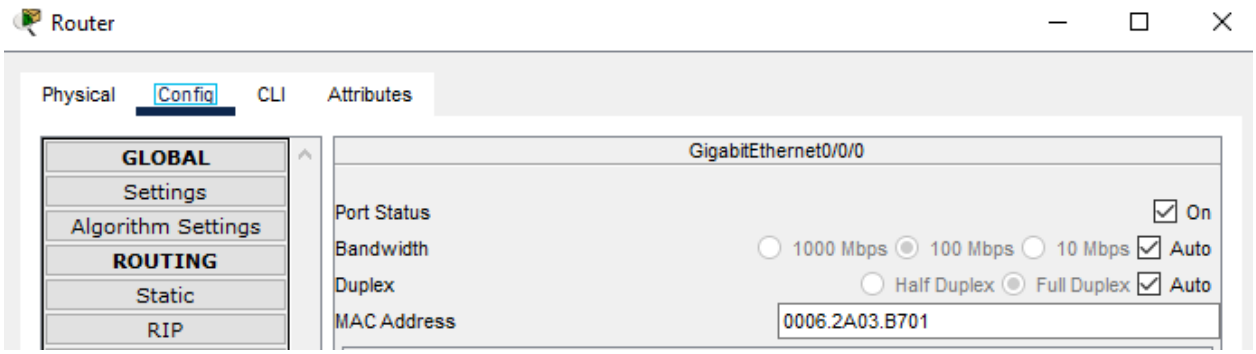
Pour que notre réseaux sois fonctionnel nous devons lui ajouter les adresses IP afin qu'ils puissent communiqué ensemble.



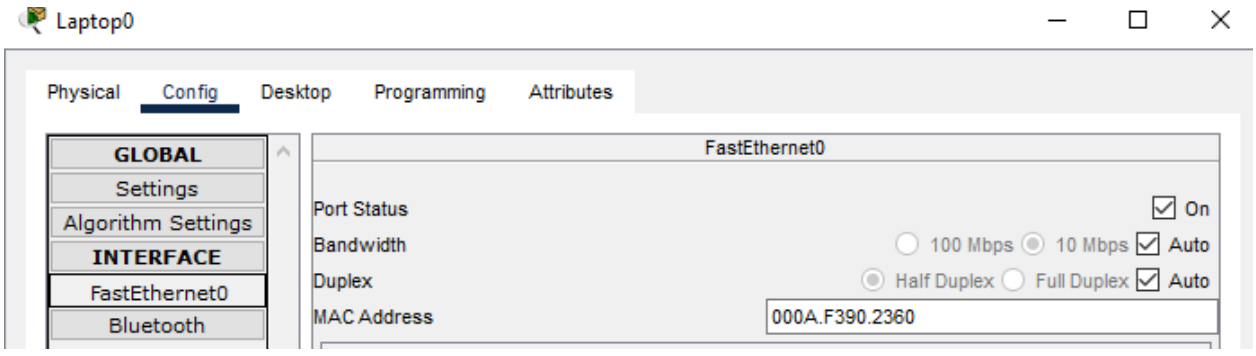
Afin de faire notre attaque nous allons faire en sorte que notre pc attaquant obtienne l'adresse mac du routeur.

Pour cela vue que nous somme sur Packet Tracer nous allons juste copier/coller l'adresse mac du routeur dans celui du pc attanquant

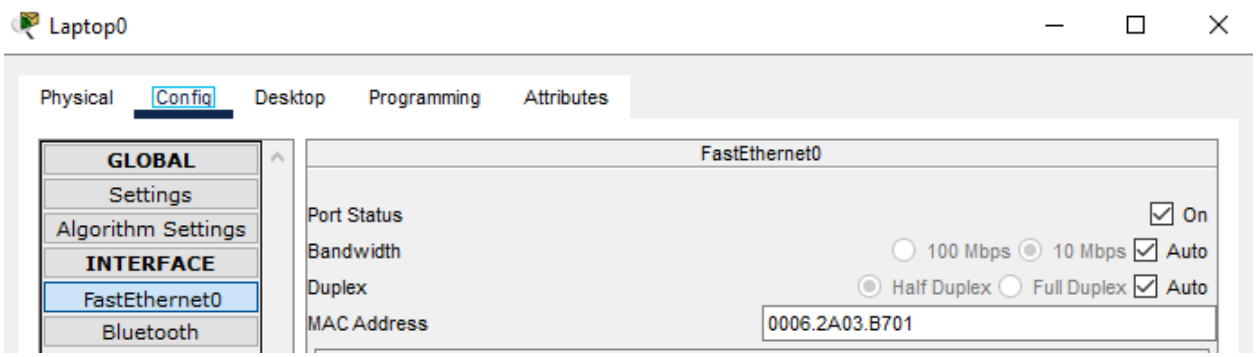
Mac adress du routeur :



Mac adress du pc attaquant :



Mac adress du pc attaquant modifier par celle du routeur :



Maintenant que nous avons falsifier l'adresse mac du pc attaquant, lorsque nous allons faire un ping du pc attaquant vers le pc client nous allons voir que le switch a actualiser sa table arp et considère notre pc attaquant comme le routeur.

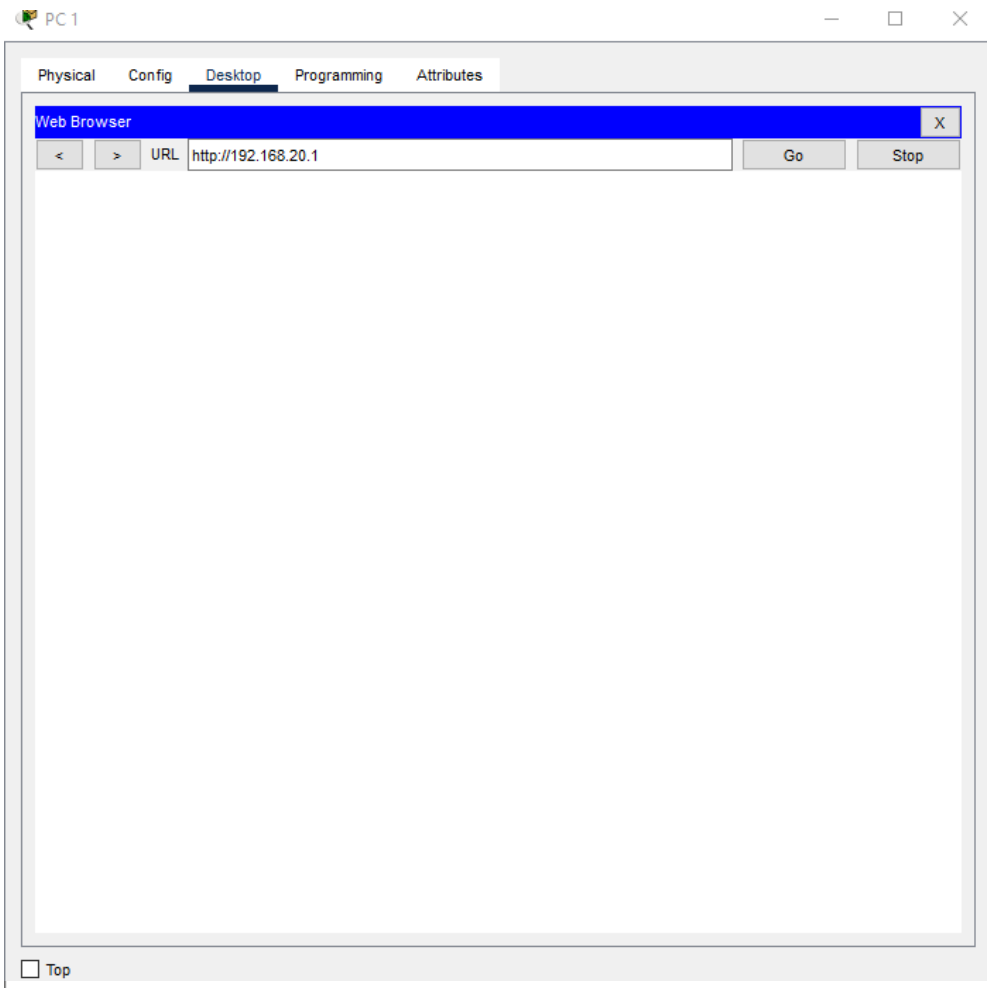
Nous allons faire un ping continu « ping -t » afin que le switch garde tous le temps le pc attaquant comme redirection

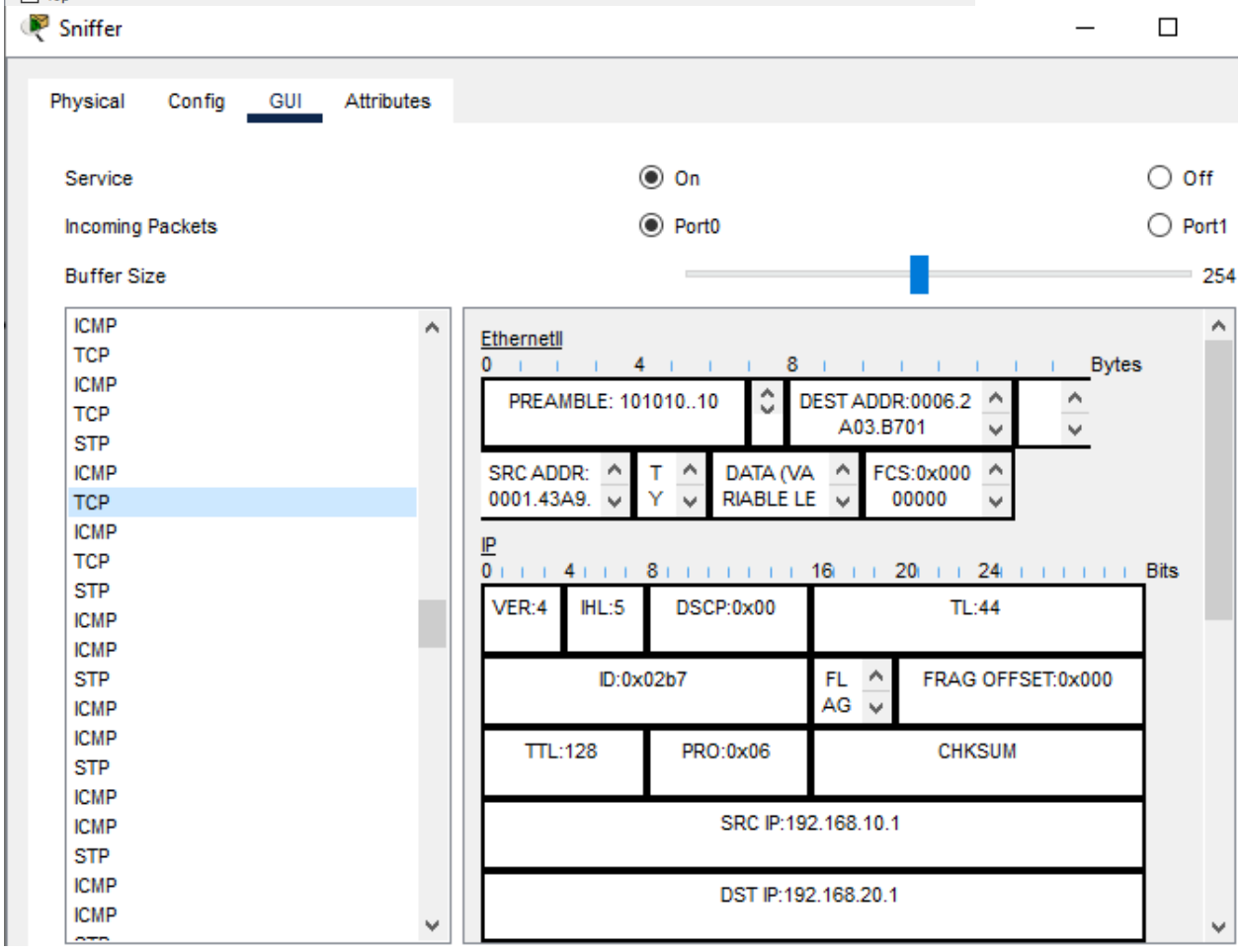
```
C:\>ping -t 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time<1ms TTL=128
Reply from 192.168.10.1: bytes=32 time=1ms TTL=128
Reply from 192.168.10.1: bytes=32 time<1ms TTL=128
Reply from 192.168.10.1: bytes=32 time<1ms TTL=128
Reply from 192.168.10.1: bytes=32 time<1ms TTL=128
Reply from 192.168.10.1: bytes=32 time=1ms TTL=128
Reply from 192.168.10.1: bytes=32 time<1ms TTL=128
Reply from 192.168.10.1: bytes=32 time=1ms TTL=128
```

```
show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.43a9.e09d    DYNAMIC     Fa0/1
   1    0006.2a03.b701    DYNAMIC     Fa0/3
Switch>
```

Nous allons le mettre en oeuvre maintenant avec le serveur.

Lorsque nous faisons un requête vers le serveur web nous voyons que la page ne charge pas et si nous allons voir du coter du sniffeur nous observons bien que le sniffer a recupérer les packet TCP destiner au serveur.


PC 1
Physical
Config
Desktop
Programming
Attributes
Web Browser
X
<
>
URL
http://192.168.20.1
Go
Stop
Top


Sniffer
Physical
Config
GUI
Attributes
Service
On
Off
Incoming Packets
Port0
Port1
Buffer Size
254
ICMP
TCP
ICMP
TCP
STP
ICMP
TCP
ICMP
TCP
STP
ICMP
ICMP
STP
ICMP
ICMP
STP
ICMP
ICMP
STP
ICMP
ICMP
EthernetII
0
4
8
Bytes
PREAMBLE: 101010..10
DEST ADDR:0006.2
A03.B701
SRC ADDR:
0001.43A9.
T
Y
DATA (VA
RIABLE LE
FCS:0x000
00000
IP
0
4
8
16
20
24
Bits
VER:4
IHL:5
DSCP:0x00
TL:44
ID:0x02b7
FL
AG
FRAG OFFSET:0x000
TTL:128
PRO:0x06
CHKSUM
SRC IP:192.168.10.1
DST IP:192.168.20.1

Conclusion :

Pour conclure ce TP nous avons pu voir comment se dérouler une attaque d'ARP Poisoning via Cisco Packet Tracer.
Pour pouvoir contrer ce type d'attaque il y a plusieur solution que l'on a pas tester dans ce tp mais que je vais cité ci-dessous :

- DHCP Screening
- Désactiver DTP
- Changer le VLAN natif aléatoire sur votre port trunk
- Activer la limite d'adresse MAC par port à 50
- Sauvegarder la configuration de votre switch paramétrée