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.

## <u>TP :</u>

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 :

🤻 Router		- 🗆 X
Physical Config CLI	Attributes	
GLOBAL	^	GigabitEthernet0/0/0
Settings		
Algorithm Settings	Port Status	
ROUTING	Bandwidth	🔵 1000 Mbps 🔍 100 Mbps 🔵 10 Mbps 🗹 Auto
Static	Duplex	🕖 Half Duplex 💿 Full Duplex 🗹 Auto
RIP	MAC Address	0006.2A03.B701

Mac adress du pc attaquant :

🍭 Laptop0						_	×
Physical Config D	eskt	op Programming	Attributes				
GLOBAL	^			FastEthernet0			
Settings		Port Status					0.0
Algorithm Settings		Bandwidth			0 100 Mbps (	0 10 Mb	uto
INTERFACE		Dunley			Half Dupley	Full Durd	uto
FastEthernet0 Bluetooth		MAC Address		000A.F390.2	360		

Mac adress du pc attaquant modifier par celle du routeur :

R	Laptop0							_		$\times$
P	hysical Config	Desł	ktop Programm	ing	Attributes					
	GLOBAL	^				FastEthernet0				
	Settings		Doct Status							0
	Algorithm Settings		Port Status							
	INTERFACE		Bandwidth			C	) 100 Mbps	10 M	bps 🗹 A	uto
	FastEthernet0	1	Duplex			• H	alf Duplex 🤇	) Full Dup	olex 🗹 A	uto
	Bluetooth		MAC Address			0006.2A03.B70				

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 ma	c-address-table Mac Address Tab	- le	
	N 111		
Vian	Mac Address	Туре	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.

	$ \Box$ $\times$	
Physical Confio Desktop Programming Attribu	utes	
Web Browser	X	
< > ORL http://192.108.20.1	Go Stop	
		_
Shifter		= 🗆
Divisional Constin Olli Attributes		
Physical Config GUI Attributes		
Physical Config <u>GUI</u> Attributes		0.04
Physical Config <u>GUI</u> Attributes Service	• On	⊖ off
Physical Config <u>GUI</u> Attributes Service Incoming Packets	<ul><li>On</li><li>Port0</li></ul>	○ Off ○ Port1
Physical Config <u>GUI</u> Attributes Service Incoming Packets Buffer Size	<ul> <li>On</li> <li>Port0</li> </ul>	<ul> <li>Off</li> <li>Port1</li> <li>254</li> </ul>
Physical Config <u>GUI</u> Attributes Service Incoming Packets Buffer Size	<ul> <li>On</li> <li>Port0</li> </ul>	<ul> <li>Off</li> <li>Port1</li> <li>254</li> </ul>
Physical Config <u>GUI</u> Attributes Service Incoming Packets Buffer Size	On     Port0     Ethernetll	<ul> <li>Off</li> <li>Port1</li> <li>254</li> </ul>
Physical Config <u>GUI</u> Attributes Service Incoming Packets Buffer Size	On     Port0 <u>Ethernetil</u> 0	<ul> <li>Off</li> <li>Port1</li> <li>254</li> <li>Bytes</li> </ul>
Physical Config GUI Attributes Service Incoming Packets Buffer Size ICMP TCP ICMP TCP	On     Port0 <u>Ethernetll     0 + 4 + 8 + 1 + 1     PREAMBLE: 10101010     DESTADDR:0006.2   </u>	Off Port1 254
Physical Config GUI Attributes Service Incoming Packets Buffer Size ICMP TCP ICMP TCP ICMP TCP STP	On     Port0      EthernetII     O	Off Port1 254
Physical Config GUI Attributes Service Incoming Packets Buffer Size ICMP TCP ICMP TCP STP ICMP ICMP ICMP ICMP	On     Port0      Ethernetil     0 + + 4 + + 8 + + + + + + + + + + + + + +	Off Port1 254
Physical Config GUI Attributes Service Incoming Packets Buffer Size ICMP TCP ICMP TCP STP ICMP TCP CMP TCP STP ICMP TCP	On     Port0      PreamBle: 10101010     PreamBle: 10100000     PreamBle: 10100000     PreamBle: 101000000     Pre	Off Port1 254
Physical Config GUI Attributes Service Incoming Packets Buffer Size ICMP TCP ICMP TCP STP ICMP TCP ICMP TCP ICMP TCP ICMP TCP ICMP	On     Port0      Ethernetil     O + 4 + 8 + 4 + 8      PREAMBLE: 10101010     DEST ADDR:0006.2 ^     A03.B701     SRC ADDR: ^ T ^ DATA (VA ^ FCS:0x000 ^     0001.43A9. × Y × RIABLE LE × 00000 ×      IP	Off Port1 254
Physical Config GUI Attributes Service Incoming Packets Buffer Size ICMP TCP ICMP TCP ICMP TCP ICMP TCP ICMP TCP ICMP TCP ICMP	On     Port0      Ethernetil     PREAMBLE: 10101010     DEST ADDR:0006.2     A03.B701     SRC ADDR: ^ T ^ DATA (VA ^ FCS:0x000 ^     0001.43A9.    Y    Y    RIABLE LE	Off Port1 254
Physical Config GUI Attributes Service Incoming Packets Buffer Size ICMP TCP ICMP	On     On     Port0      Ethernetil     0 + 4 + 8 + 4 + 8      PREAMBLE: 10101010     DEST ADDR:0006.2 ^     A03.B701 *      SRC ADDR: ^ T ^ DATA (VA ^ FCS:0x000 ^     0001.43A9. * Y * RIABLE LE * FCS:0x000 ^     00000 *      IP     0 + 4 + 8 + 4 + 16 + 20 + 24 +      VER:4 HL:5 DSCP:0x00 TL:44	Off Port1 254
Physical Config GUI Attributes Service Incoming Packets Buffer Size ICMP TCP ICMP TCP STP ICMP TCP ICMP TCP ICMP TCP ICMP TCP ICMP ICMP ICMP ICMP ICMP	On     Port0      Ethernetil     O + 4 + 8 + 4 + 8 + 4 + 4 + 4 + 4 + 4 + 4	Off Port1 254 • Bytes • Bits
Physical       Config       GUI       Attributes         Service       Incoming Packets       Incoming Packets         Buffer Size       ICMP       Incoming Packets         ICMP       ICMP       Incoming Packets         ICMP       ICMP       Incoming Packets         ICMP       ICMP       Incoming Packets         ICMP       Incoming Packets       Incoming Packets      <	On     Port0      EthernetII     O + 4 + 8 + 4 + 8      PREAMBLE: 10101010     DEST ADDR:0006.2 ^     A03.B701     SRC ADDR: ^ T ^ DATA (VA ^ FCS:0x000 ^     O001.43A9. * Y * RIABLE LE * 000000 *      IP     O + 4 + 8 + 4 + 16 + 20 + 24      VER:4 IHL:5 DSCP:0x00 TL:44      D:0x02b7 FL ^ FL ^ FRAG OFF	Off Port1 254 • Bits • Bits • Bits
Physical       Config       GUI       Attributes         Service       Incoming Packets       Incoming Packets         Buffer Size       ICMP       Incoming Packets         ICMP       Incoming Packets       Incoming Packets <td>On     Port0      Ethernetil     O + 4 + 8 + 4 + 8 + 4 + 4      PREAMBLE: 10101010     DEST ADDR:0006.2 ^     A03.B701         DEST ADDR:0006.2 ^     A03.B701         SRC ADDR: ^ T ^ DATA (VA ^ FCS:0x000 ^     0001.43A9.</td> <td>Off Port1 254</td>	On     Port0      Ethernetil     O + 4 + 8 + 4 + 8 + 4 + 4      PREAMBLE: 10101010     DEST ADDR:0006.2 ^     A03.B701         DEST ADDR:0006.2 ^     A03.B701         SRC ADDR: ^ T ^ DATA (VA ^ FCS:0x000 ^     0001.43A9.	Off Port1 254
Physical       Config       GUI       Attributes         Service       Incoming Packets       Incoming Packets         Buffer Size       ICMP       Incoming Packets         ICMP       Incoming Packets       Incoming Packets <td>On     Port0      Ethernetil     O + 4 + 8 + 4 + 8 + 4 + 4      PREAMBLE: 10101010     DEST ADDR:0006.2 ^     A03.B701 *      PREAMBLE: 10101010     DEST ADDR:0006.2 ^     A03.B701 *      SRC ADDR: ^ T ^ DATA (VA ^ FCS:0x000 ^     00000 *      PREAMBLE: 10101010     DEST ADDR:0000 *      PREAMBLE: 10101010     DEST ADDR:0006.2 ^      PREAMBLE: 10101010     PREAMBLE:</td> <td>Off Port1 254</td>	On     Port0      Ethernetil     O + 4 + 8 + 4 + 8 + 4 + 4      PREAMBLE: 10101010     DEST ADDR:0006.2 ^     A03.B701 *      PREAMBLE: 10101010     DEST ADDR:0006.2 ^     A03.B701 *      SRC ADDR: ^ T ^ DATA (VA ^ FCS:0x000 ^     00000 *      PREAMBLE: 10101010     DEST ADDR:0000 *      PREAMBLE: 10101010     DEST ADDR:0006.2 ^      PREAMBLE: 10101010     PREAMBLE:	Off Port1 254
Physical       Config       GUI       Attributes         Service       Incoming Packets       Incoming Packets         Buffer Size       ICMP       Incoming Packets         ICMP       ICMP       Incoming Packets         ICMP       ICMP       Incoming Packets         ICMP       ICMP       Incoming Packets         ICMP       Incoming Packets       Incoming Packets      <	On     Port0      Preamble: 10101010     Preamble: 10101010     DEST ADDR:0006.2 ^     A03.B701     SRC ADDR: ^ T ^ DATA (VA ^ FCS:0x000 ^     O001.43A9. * Y * RIABLE LE * 000000 *      P     Out 4 + 8 + 16 + 20 + 24 +      VER:4 HL:5 DSCP:0x00 TL:44      D:0x02b7 FL ^ FL ^ FRAG OFFS     AG * FRAG OFFS     TTL:128 PRO:0x06 CHKSUM	○ Off ○ Port1 254
Physical       Config       GUI       Attributes         Service       Incoming Packets       Incoming Packets         Buffer Size       ICMP       Incoming Packets         ICMP       Incoming Packets       Incoming Packets <t< th=""><td>On     On     Port0      Ethernetil     O + 4 + 8 + 4 + 8 + 4 + 4      PREAMBLE: 10101010     DEST ADDR:0006.2 ^     A03.B701     SRC ADDR: ^ T ^ DATA (VA ^ FCS:0x000 ^     O001.43A9. * Y * RIABLE LE * 00000 *      IP     O + 4 + 8 + 4 + 16 + 20 + 24 +      VER:4 HL:5 DSCP:0x00 TL:44      ID:0x02b7 FL ^ FL ^ FRAG OFFS     AG * FRAG OFFS     TTL:128 PR0:0x06 CHKSUM</td><td>O Off Port1 254 Bytes Bits SET:0x000</td></t<>	On     On     Port0      Ethernetil     O + 4 + 8 + 4 + 8 + 4 + 4      PREAMBLE: 10101010     DEST ADDR:0006.2 ^     A03.B701     SRC ADDR: ^ T ^ DATA (VA ^ FCS:0x000 ^     O001.43A9. * Y * RIABLE LE * 00000 *      IP     O + 4 + 8 + 4 + 16 + 20 + 24 +      VER:4 HL:5 DSCP:0x00 TL:44      ID:0x02b7 FL ^ FL ^ FRAG OFFS     AG * FRAG OFFS     TTL:128 PR0:0x06 CHKSUM	O Off Port1 254 Bytes Bits SET:0x000
Physical       Config       GUI       Attributes         Service       Incoming Packets       Incoming Packets         Buffer Size       ICMP       Incoming Packets         ICMP       Incoming Packets       Incoming Packets         ICMP	On     On     Port0      Ethernetil     O + 4 + 8 + 4 + 8 + 4 + 4     PREAMBLE: 10101010     DEST ADDR:0006.2 ^     A03.B701     V     SRC ADDR: ^ T ^ DATA (VA ^ FCS:0x000 ^     0001.43A9. v Y v RIABLE LE v 000000 v      P     O + 4 + 8 + 4 + 16 + 20 + 24 +     VER:4 HL:5 DSCP:0x00 TL:44      D:0x02b7     FL ^ FRAG OFF3     AG v FRAG OFF3     SRC IP:192.168.10.1	Off Port1 254
Physical       Config       GUI       Attributes         Service       Incoming Packets       Incoming Packets         Buffer Size       ICMP       Incoming Packets         ICMP       Incoming Packets       Incoming Packets         ICMP       In	On     On     Port0      Ethernetil     O + 4 + 8 + 4 + 8 + 4 + 4      PREAMBLE: 10101010     DEST ADDR:0006.2      A03.B701     A03.B701     V      SRC ADDR: ^ T ^ DATA (VA ^ FCS:0x000 ^     O0000 ^      P     O + 4 + 8 + 4 + 16 + 20 + 24 +      VER:4 HL:5 DSCP:0x00     TL:44      D:0x02b7     FL ^ FL ^ FRAG OFFS     AG ^ FRAG OFFS     SRC IP:192.168.10.1	Off Port1 254
Physical       Config       GUI       Attributes         Service       Incoming Packets       Incoming Packets         Buffer Size       ICMP       Incoming Packets         ICMP       Incoming Packets       Incoming Packets         ICMP       Incoming Packets       Incoming Packets         ICMP       Incoming Packets       Incoming Packets         ICMP       Incomin	On     Port0      Ethernetil     O + 4 + 8 + 4 + 8 + 4 + 4 + 4 + 8 + 4 + 4	○ Off ○ Port1 254

## **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 cidessous :

- 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