**TP Sécurité Informatique**

1. **Topologie 1**

Ajout switch sw1 et 2 VPCS (PC1, PC2) Définissions IP statiques de PC1 et PC2:

* On ouvre un Shell PuTTY et on met les commandes
  + **ip 10.3.1.2 255.255.255.0**
  + **ip 10.3.1.1 255.255.255**
  + Sauvegarde de la configuration : « **save** »

Ping de PC1 vers PC2: dans shell sur PC1: **ping 10.3.1.2**, et l'autre sens aussi de PC2 vers PC1. Dans notre cas les paquets sont bien envoyés et reçus de l’un vers l’autre.

Dans Shell de sw1: **show mac address-table** pour voir la CAM table.

On vérifie les MAC address : **show IP** à rentrer sur un Shell sur les 2 pc

1. **VLAN**

Ajout de la 3ème machine PC3 Shell : **IP 10.3.1.3 255.255.255.0**

Sur chacune des machines, on teste de ping les 2 autres PC Pour créer vlan dans Shell sw1:

* **vlan 10** => **name vlan10** => **exit**
* **vlan 20** => **name vlan20** => **exit**

dans Shell sw1:

* **conf t**
  + **interface Ethernet0/0 (on peut lister les interface avec show interface)**
  + **switchport mode access**
  + **switchport access vlan 10**
  + **exit**
  + **interface Ethernet0/1**
  + **switchport mode access**
  + **switchport access vlan 10**
  + **exit**
  + **interface Ethernet0/2**
  + **switchport mode access**
  + **switchport access vlan 20**
  + **exit**
  + **show interface**

**On n’oublie pas de sauvegarder la configuration des Switchs avec la commande écrite sur le TP.**

On teste les pings, ça fonctionne entre **PC1 <=> PC2** mais **PC3** devient unreachabled et ne peut plus ping. Cela est normal puisqu’il n’appartient pas au VLAN10.

1. **Rocky**

D’abord aller sur internet afin de télécharger l’iso de Rocky.

Install Rocky : **cat /etc/selinux/config**

**set selinux=permissive**

**TP II)**

**Tout d’abord la mise en place de la topologie :**

* Install des VPCS
* Mise en place de la VM (serveur dhcp)
* Configuration routeur pour accéder à internet avec le NAT

network:

version: 2

renderer: NetworkManager

ethernets:

enp0s8:

dhcp4: no

addresses:

**- 10.2.1.11/24**

routes:

- to: default

via: **10.2.1.254**

- sudo nano /etc/dhcp/dhcpd.conf (on ajoute):

**subnet 10.2.1.0 netmask 255.255.255.0 {**

**range 10.2.1.100 10.2.1.200**

**option subnet-mask 255.255.255.0**

**option domain-name-servers 1.1.1.1**

**option routers 10.2.1.254;**

}

- **sudo nano /etc/default/isc-dhcp-server:**

INTERFACESv4="enp0s8"

**3) Accès Internet Routeur :**

Sur le routeur, pour avoir accès à internet:

- conf t

- interface FastEthernet1/0

- ip address dhcp

- no shutdown

- exit; exit

- show ip interface brief

- ping 8.8.8.8 🡪 OK

**Configuration de l'adresse ip de l'interface LAN sur le routeur:**

- conf t

- interface FastEthernet0/0

- ip address 10.2.1.254 255.255.255.0

- no shutdown

**On active la NAT pour router les paquets depuis le LAN vers internet:**

- show ip int br

- conf t

- interface FastEthernet0/0

- ip nat inside

- interface FastEthernet1/0

- ip nat outside

- exit

- access-list 1 permit any

- ip nat inside source list 1 interface FastEthernet1/0 overload

- exit

- copy running-config startup-config

**Ping depuis PC3 vers 8.8.8.8 🡪 OK**

Une fois fais quand on prend un VPCS et qu’on entre la commande : **dhcp** il est écrit **DORA.**

Ce qui prouve que le fonctionnement est bon.

Proof !

**PC4> dhcp**

**DORA IP 10.2.1.102/24 GW 10.2.1.254**

**PC4> ping 10.2.1.51**

84 bytes from 10.2.1.51 icmp\_seq=1 ttl=64 time=3.041 ms

84 bytes from 10.2.1.51 icmp\_seq=2 ttl=64 time=1.229 ms

84 bytes from 10.2.1.51 icmp\_seq=3 ttl=64 time=1.992 ms

84 bytes from 10.2.1.51 icmp\_seq=4 ttl=64 time=1.806 ms

84 bytes from 10.2.1.51 icmp\_seq=5 ttl=64 time=1.681 ms

P**C4> ping 8.8.8.8**

84 bytes from 8.8.8.8 icmp\_seq=1 ttl=114 time=40.391 ms

84 bytes from 8.8.8.8 icmp\_seq=2 ttl=114 time=36.481 ms

84 bytes from 8.8.8.8 icmp\_seq=3 ttl=114 time=37.653 ms

84 bytes from 8.8.8.8 icmp\_seq=4 ttl=114 time=52.866 ms

84 bytes from 8.8.8.8 icmp\_seq=5 ttl=114 time=44.632 ms

ARP (AT 1)

**Poisoning**

**PC1> arp**

08:00:27:ad:25:87 10.2.1.114 expires in 90 seconds

aa:bb:cc:dd:ee:ff 10.2.1.14 expires in 113 seconds

**Spoofing**

**PC1> arp**

08:00:27:ad:25:87 10.2.1.114 expires in 48 seconds

08:00:27:ad:25:87 10.2.1.52 expires in 120 seconds

PC1> ping 10.2.1.52

84 bytes from 10.2.1.52 icmp\_seq=1 ttl=63 time=9.679 ms

84 bytes from 10.2.1.52 icmp\_seq=2 ttl=63 time=6.372 ms

84 bytes from 10.2.1.52 icmp\_seq=3 ttl=63 time=6.688 ms

84 bytes from 10.2.1.52 icmp\_seq=4 ttl=63 time=7.906 ms

84 bytes from 10.2.1.52 icmp\_seq=5 ttl=63 time=7.871 ms

**Man in the Middle**

**PC1> arp**

08:00:27:ad:25:87 10.2.1.114 expires in 31 seconds

08:00:27:ad:25:87 10.2.1.254 expires in 120 seconds

**R1#show arp**

Protocol Address Age (min) Hardware Addr Type Interface

Internet 10.2.1.11 25 0800.2789.6765 ARPA FastEthernet1/0

Internet 192.168.122.1 0 5254.00d1.e503 ARPA FastEthernet0/0

Internet 10.2.1.51 0 0800.27ad.2587 ARPA FastEthernet1/0

Internet 192.168.122.81 - ca01.0534.0000 ARPA FastEthernet0/0

Internet 10.2.1.114 1 0800.27ad.2587 ARPA FastEthernet1/0

Internet 10.2.1.254 - ca01.0534.001c ARPA FastEthernet1/0

**Remediation**

**Fixez les adresses IP et MAC importantes (passerelle, serveurs critiques) directement dans les tables ARP des machines**

* sudo arp -s <ip\_address> <mac\_address>

**Activer Dynamic ARP Inspection (DAI)**

Configurez cette fonctionnalité sur les switches gérés :

Exemple Cisco :

* ip arp inspection vlan <vlan\_id>
* ip dhcp snooping

**Utiliser HTTPS et SSL/TLS**

Chiffrez les communications réseau pour empêcher le vol d'informations sensibles, même en cas d'interception :

* Implémentez HTTPS pour les sites web et HSTS pour forcer son utilisation.
* Assurez-vous que les connexions à distance utilisent SSH, VPN ou TLS.

ICMP (AT2)

**sudo python icmp\_basic\_exfiltr.py 127.0.0.1 'hello data'**

[sudo] password for kali:

[\*] Envoi de la chaîne 'hello data' dans des pings vers 127.0.0.1

[\*] Paquet envoyé : hello data

**sudo python icmp\_basic\_receiver.py**

[\*] En attente de messages ICMP contenant des données...

Message reçu : Hello, ICMP exfiltration

Message reçu : Hello, ICMP exfiltration

**Remediation**

* Filtrer les paquets ICMP : Configurez un pare-feu pour bloquer ou limiter les paquets ICMP sortants contenant des charges utiles inhabituelles.
* Surveiller le trafic réseau : Implémentez des outils comme IDS/IPS (ex. : Snort) ou Wireshark pour détecter les paquets ICMP contenant des charges utiles suspectes ou des flux inhabituels. Activez des alertes pour tout trafic ICMP anormal.

STP (AT3)

**Remediation**

* Activer BPDU Guard sur les ports des utilisateurs : Cette fonctionnalité désactive automatiquement un port recevant des trames BPDU inattendues, empêchant ainsi les périphériques non autorisés de perturber la topologie STP.

Remediation (notes prises en cours) :

* DHCP : DHCP Spoofing on définit des interfaces en trusted et les autres on ferme les ports
* ARP : port security force le switch à prendre une mac part port , DAI,
* DNS SPOOFING : Faire le DHCP et l’ARP + chiffrer le DNS.
* TCP : On ne peut pas se prémunir de cette attaque vulnérable
* STP : BDPDU gard
* Exifilter : DPI ( deep packet inspection ).