Rapport - tâche 9 : Contre-mesures contre des attaques MiM

Les attaques Man In The Middle (MITM) consistent à s'insérer entre deux communications cibles. Diverses méthodes ou techniques permettent de réaliser ce type d'attaques. **Les attaquants ont souvent pour but d'usurper l'identité des serveurs ou d'une passerelle**. Ce qui leur permet d'écouter tous les échanges entre un client et ces machines centrales. Les réseaux locaux sont souvent des cibles idéales. Dans un réseau local, l'action principale consiste à **empoisonner la table des adresses MAC des cibles**. Cet empoisonnement se base sur la configuration des machines et du protocole ARP. En effet, le protocole ARP associe une adresse IP (qui peut changer) à une adresse MAC (fixe en théorie).
L'objectif de cette tâche est de mettre en place des sécurités pour éliminer le risque des attaques MITM dans notre réseau local.

1. **Description des solutions**

Les solutions ont été installées en fonction de l'attaque réalisée à savoir l'empoisonnement ARP (ARP spoofing). Les solutions choisies : **commande port-security**, **ARP gratuitous**, **entrée statique ARP**, **arpwatch.**

- **Commande port-security**

Avec les Switch Cisco, il est possible de faire un contrôle sur les ports en limitant l'accès à certaines adresses MAC, cela permet de sécuriser l'accès : **port-security.** Cette commande limite l'accès à un port en filtrant les adresses MAC sources. Si une adresse MAC n'est pas autorisée explicitement, la connexion sera refusée.
La gestion des adresses MAC peut se faire de trois façons :

- **mode statique :** configuration manuelle des adresses MAC
- **mode dynamique :** configuration dynamique des adresses MAC sans enregistrement
- **mode sticky :** configuration dynamique des adresses MAC et enregistrement dans running-config.

Si la sécurité en place n'est pas respectée, le switch peut agir de l'un des trois modes suivants :

- **mode protect :** les paquets concernant la machine « hors limite » ne passent plus. Il n'y a pas de message d'avertissement.
- **mode restrict :** les paquets concernant la machine « hors limite » ne passent plus. Par contre, le switch envoie un message syslog, un trap snmp et le compteur d'erreur est incrémenté.
- **mode shutdown :** les paquets concernant la machine « hors limite » ne passent plus. Les messages d'alerte sont envoyés et le port est coupé (**état err-disabled**). C'est le comportement par défaut.

- **ARP gratuitous**

Le protocole ARP comme mentionné en amont, fait le lien entre une adresse IP et une adresse MAC. L'ensemble des liens répertoriés constitue la table de mappage IP à MAC d'une machine. **Les ARP gratuitous sont des paquets de réponse ARP non déclenchés par une requête ARP**. Une machine peut les envoyer à des fins de mise à jour de la table de mappage, d'annonce ou de redondance.

- **ARP statique**

Les enregistrements associant une adresse IP à une adresse MAC peuvent se faire de façon statique.Autrement dit, par un administrateur qui le fait à l'aide d'une commande. Cette pratique se fait essentiellement pour les principaux appareils du réseau (passerelle par défaut, serveurs, etc.)

- **Arpwatch**

Arpwatch est un outil d'administration réseau permettant de surveiller l'activité du protocole ARP dans un réseau. **Il entretient une base de données des associations adresse MAC - adresse IP vues sur le réseau**. Ainsi, il peut alerter un administrateur lors d'éventuels changements comme **une nouvelle station ou activité, d'anciennes adresses échangées ou utilisées.** Ces alertes peuvent être envoyées à une adresse électronique.

2. **Mise en place des solutions**

Les solutions ont été mises en place sur le switch et le serveur.

- **Commande port-security**

Avant d'activer cette commande, il faut s'assurer que le port est soit en mode access soit en mode trunk.

J'ai utilisé cette commande afin de limiter à **1**, le nombre d'adresses MAC autorisées sur un port. Ensuite j'ai configuré le **mode sticky** pour la gestion des adresses MAC source. Grâce à ce mode, le switch réalise un **apprentissage dynamique de la MAC** puis l'enregistre dans le fichier **running-config** et cela me permet après vérification de sauvegarder la configuration.

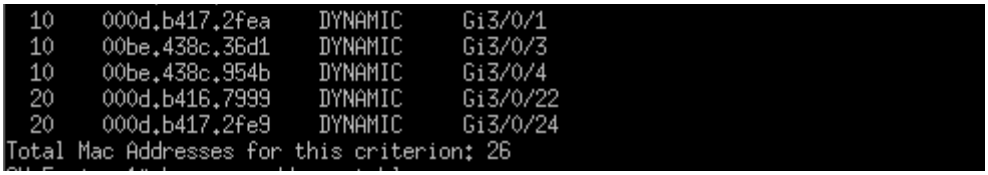
Par défaut, lors de la violation de cette sécurité, le port du switch est **"shutdown"**. Afin d'activer une **remontée automatique** du port stoppé, je mets un intervalle de **200 secondes** pour l'état **"psecure-violation"**.

Enfin, j'ai également désactivé les **ARP gratuitous** sur le switch.

Commandes essentielles tapées :

```
SW_Equipe_1#show mac address-table
SW_Equipe_1(config)#int gi3/0/3
SW_Equipe_1(config-if)#switchport port-security maximum 1
SW_Equipe_1(config-if)#switchport port-security mac-address sticky
SW_Equipe_1#sh port-security
SW_Equipe_1(config)#errdisable recovery cause psecure-violation
SW_Equipe_1(config)#errdisable recovery interval 200
SW_Equipe_1(config)#ip arp gratuitous none
SW_Equipe_1#sh mac address-table
SW_Equipe_1#sh run
```

Table de mappage MAC



```
SW_Equipe_1(config)#int gigabitEthernet 3/0/3
SW_Equipe_1(config-if)#swi
SW_Equipe_1(config-if)#switchport port-sec
SW_Equipe_1(config-if)#switchport port-security
SW_Equipe_1(config-if)#switchport port-security max
SW_Equipe_1(config-if)#switchport port-security maximum 1
```

```
SW_Equipe_1(config-if)#switchport port-security mac-address sticky
SW_Equipe_1(config-if)#end
```

```
SW_Equipe_1#sh port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
               (Count)       (Count)          (Count)
-----------------------------------------------------------------------------
    Gi3/0/3            1           1                  0         Shutdown
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 32768
```

```
SW_Equipe_1(config)#errdisable recovery cause psecure-violation
SW_Equipe_1(config)#end
```

```
SW_Equipe_1(config)#errdisable recovery interval 200
```

```
SW_Equipe_1(config)#ip arp gratuitous none
```

Nouvelle table de mappage MAC (passer à STATIC)

```
  10    000d.b417.2fea    DYNAMIC     Gi3/0/1
  10    00be.438c.36d1    STATIC      Gi3/0/3
  10    00be.438c.954b    DYNAMIC     Gi3/0/4
  20    000d.b416.7999    DYNAMIC     Gi3/0/22
  20    000d.b417.2fe9    DYNAMIC     Gi3/0/24
Total Mac Addresses for this criterion: 26
```

Errdisable status

```
SW_Equipe_1#sh errdisable recovery
ErrDisable Reason            Timer Status
-----------------            --------------
arp-inspection               Disabled
bpduguard                    Disabled
channel-misconfig (STP)      Disabled
dhcp-rate-limit              Disabled
dtp-flap                     Disabled
gbic-invalid                 Disabled
inline-power                 Disabled
l2ptguard                    Disabled
link-flap                    Disabled
mac-limit                    Disabled
loopback                     Disabled
loopdetect                   Disabled
pagp-flap                    Disabled
port-mode-failure            Disabled
pppoe-ia-rate-limit          Disabled
psecure-violation            Enabled
security-violation           Disabled
sfp-config-mismatch          Disabled
small-frame                  Disabled
```

Fichier de configuration

```
SW_Equipe_1#sh ru
Mar 29 16:45:35.164: %SYS-5-CONFIG_I: Configured from console by consolen
Building configuration...

Current configuration : 2796 bytes
!
! Last configuration change at 16:45:35 UTC Fri Mar 29 2024
! NVRAM config last updated at 16:23:31 UTC Fri Mar 29 2024
!
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SW_Equipe_1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
switch 3 provision ws-c2960x-24pd-l
!
!
!
!
ip arp gratuitous none
!
```

```
interface GigabitEthernet3/0/3
 description Server_WEB_FTP_A
 switchport access vlan 10
 switchport mode access
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 00be.438c.36d1
 switchport port-security
```

- **ARP gratuitous et entrée statique**

Ces méthodes se configurent assez facilement avec des commandes shell. Elles sont tapées sur le serveur.

désactivation arp gratuitous : sudo ip link set dev eth0 arp off

sudo echo 1 > /proc/sys/net/ipv4/conf/all/drop_gratuitous_arp #abandon des arp gratuits

sudo echo 0 > /proc/sys/net/ipv4/conf/all/arp_accept #refus des arp

Plusieurs façons de bloquer les ARP gratuitous

entrée statique dans la table ARP : sudo arp -s 192.168.1.254 00:0d:b4:17:2f:ea

Abandon des ARP gratuits

```
tp@rt: ~
Fichier  Editer  Affichage  Rechercher  Terminal  Aide
tp@rt:~$ sudo cat /proc/sys/net/ipv4/conf/all/drop_gratuitous_arp
0
tp@rt:~$ sudo nano /proc/sys/net/ipv4/conf/all/drop_gratuitous_arp
tp@rt:~$ sudo cat /proc/sys/net/ipv4/conf/all/drop_gratuitous_arp
1
tp@rt:~$
```

```
tp@rt:~$ sudo arp -s 10.0.0.254 00:0d:b4:17:2f:ea
tp@rt:~$ sudo arp -aevn
Adresse                  TypeMap AdresseMat          Indicateurs           Iface
10.0.0.100               ether   30:23:03:8b:f5:b4   C                     eth0
10.0.0.254               ether   00:0d:b4:17:2f:ea   CM                    eth0
10.0.0.2                 ether   00:be:43:8c:95:4b   C                     eth0
Entrées: 3      Ignorées: 0     Trouvées: 3
```

- **Arpwatch**

L'outil arpwatch a un paquet sous le dépôt Debian **"arpwatch"**. Donc j'ai réalisé une installation en ligne de commande **sudo apt-get install arpwatch**. Cet outil ne nécessite pas de fichier de configuration, il est assez pratique. Sa mise en place se comprend en lisant le fichier **README** dans **/etc/arpwatch** une fois l'installation faite. On peut créer si on le souhaite un fichier du type **IFNAME.iface** pour **appliquer des options supplémentaires** à celles indiquées dans le fichier par défaut **/etc/default/arpwatch**. Sinon, on peut **juste ajouter** ces options à la variable **ARGS** dans le fichier par défaut. Il ne reste plus qu'à activer le service sur une interface **sudo systemctl enable arpwatch@eth0** puis le lancer **sudo systemctl start arpwatch@eth0**.
On regarde alors les alertes dans les fichiers : **/var/log/syslog, /var/log/messages et /var/lib/arpwatch/eth0.dat (base de données générée).**

Base de données générée

```
tp@rt: ~
Fichier  Editer  Affichage  Rechercher  Terminal  Aide
  GNU nano 3.2                  /var/lib/arpwatch/eth0.dat

00:be:43:8c:36:d1       10.0.0.1        1712056781              eth0
00:0d:b4:17:2f:ea       10.0.0.254      1712056781              eth0
30:23:03:8b:f5:b4       10.0.0.100      1712050151              eth0
7c:8a:e1:98:dd:f8       10.0.0.10       1712055256              eth0
```

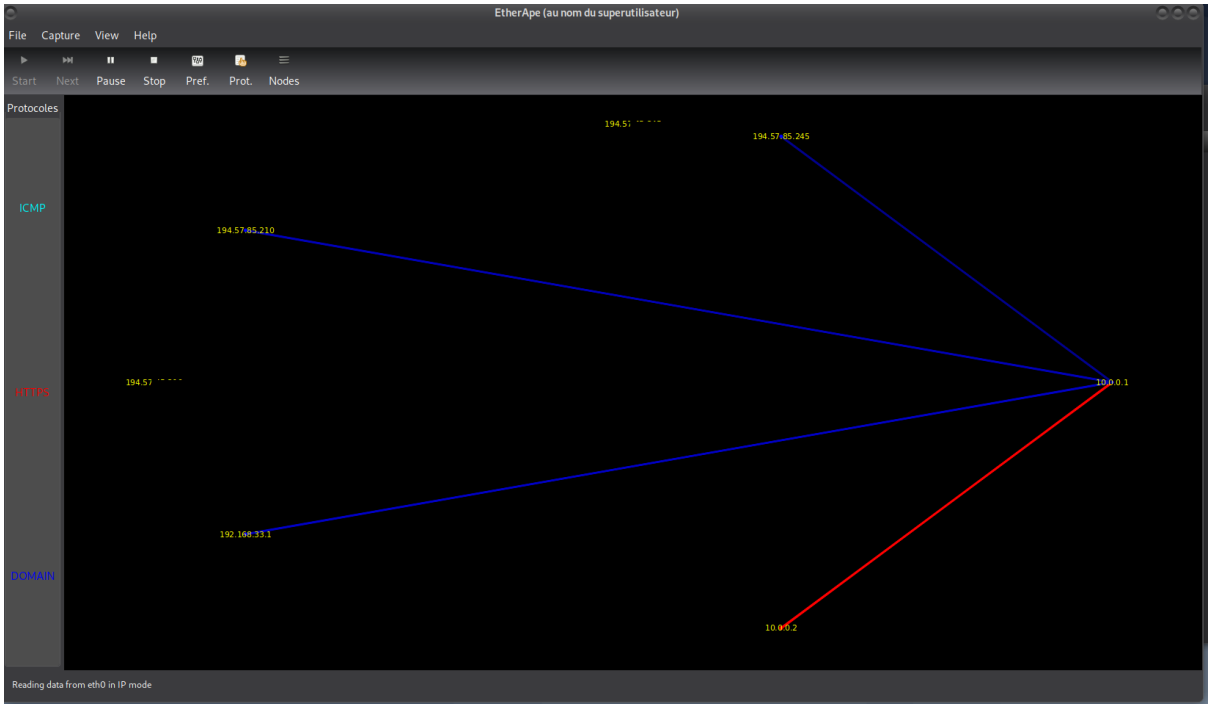
Tous les événements dans les journaux

```
Apr  2 11:09:38 rt ntpd[898]: error resolving pool 2.debian.pool.ntp.org: Temporary failure in nam$
Apr  2 11:10:34 rt ntpd[898]: error resolving pool 1.debian.pool.ntp.org: Temporary failure in nam$
Apr  2 11:11:30 rt ntpd[898]: error resolving pool 3.debian.pool.ntp.org: Temporary failure in nam$
Apr  2 11:12:17 rt arpwatch: new station 10.0.0.2 00:be:43:8c:95:4b eth0
Apr  2 11:12:26 rt ntpd[898]: error resolving pool 0.debian.pool.ntp.org: Temporary failure in nam$
Apr  2 11:12:45 rt arpwatch: new station 10.0.0.3 00:be:43:8c:95:4b eth0
Apr  2 11:12:45 rt arpwatch: execl: /usr/lib/sendmail: No such file or directory
Apr  2 11:12:45 rt arpwatch: reaper: pid 4621, exit status 1
Apr  2 11:13:13 rt arpwatch: new station 10.0.0.4 00:be:43:8c:95:4b eth0
Apr  2 11:13:13 rt arpwatch: execl: /usr/lib/sendmail: No such file or directory
Apr  2 11:13:13 rt arpwatch: reaper: pid 4622, exit status 1
Apr  2 11:13:23 rt ntpd[898]: error resolving pool 1.debian.pool.ntp.org: Temporary failure in nam$
Apr  2 11:13:41 rt arpwatch: new station 10.0.0.5 00:be:43:8c:95:4b eth0
Apr  2 11:13:41 rt arpwatch: execl: /usr/lib/sendmail: No such file or directory
Apr  2 11:13:41 rt arpwatch: reaper: pid 4636, exit status 1
Apr  2 11:14:09 rt arpwatch: new station 10.0.0.6 00:be:43:8c:95:4b eth0
Apr  2 11:14:09 rt arpwatch: execl: /usr/lib/sendmail: No such file or directory
Apr  2 11:14:09 rt arpwatch: reaper: pid 4642, exit status 1
Apr  2 11:14:19 rt ntpd[898]: error resolving pool 3.debian.pool.ntp.org: Temporary failure in nam$
Apr  2 11:14:37 rt arpwatch: new station 10.0.0.7 00:be:43:8c:95:4b eth0
```

Petits plus :

- **Etherape**

EtherApe est un logiciel libre qui permet de surveiller un réseau informatique. Ce logiciel est muni d'une interface graphique qui permet de visualiser ce qui se passe sur un réseau. Chaque transfert de donnée est représenté par un trait ainsi qu'un disque de couleur au point d'origine.
Cela ne nous permet malheureusement pas de détecter un empoisonnement ARP mais reste pratique pour le monitoring du réseau car on suit l'activité du réseau et l'importance (trait de plus en plus grand) du trafic entre des liens. On peut aussi enregistrer les activités du réseau pour évaluer l'utilisation du réseau ou les étudier par exemple.



- **Hôte ssh à se connecter**

J'ai bloqué toute connexion SSH entrante sauf celle venant du Stormshield (192.168.1.254). Cela peut être une forme de protection.

```
Fichier  Editer  Affichage  Rechercher  Terminal  Aide
tp@rt:~$ ssh tp@10.0.0.1
^C
tp@rt:~$ ssh admin@10.0.0.254
Password:
Last login: Fri Mar 29 11:49:22 2024 from 10.0.0.1
SN210W17C2190A7: FW SN210W (S / EUROPE)
Firewall software version 3.7.20

port       name       NS-BSD   state  addressIPv4         addressIPv6
   1        out       mvxpe2      up  80.80.80.1/24
   2         in       mvxpe1      up  192.168.0.254/24
   3       dmz1       mvxpe0      up  10.0.0.254/24

SN210W17C2190A7>ss
ssh        ssh-keygen sshd       sslinit
SN210W17C2190A7>ss
ssh        ssh-keygen sshd       sslinit
SN210W17C2190A7>ssh tp@10.0.0.1
The authenticity of host '10.0.0.1 (10.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:9z8fqEmeNiue4m3GNI6DcxAhYa6zu5MT8b1wRNlcD4E.
No matching host key fingerprint found in DNS.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.0.1' (ECDSA) to the list of known hosts.
tp@10.0.0.1's password:
Linux rt 5.10.0-0.deb10.28-amd64 #1 SMP Debian 5.10.209-2~deb10u1 (2024-02-15) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Mar 10 15:31:07 2022 from 172.20.40.90
tp@rt:~$
```

Conclusion

Au vu des solutions installées sur le réseau, les machines sur le réseau peuvent prétendre se protéger contre l'empoisonnement ARP. Aussi, avec les alertes de l'outil Arpwatch, une détection précoce permet d'anticiper et de désamorcer les tentatives de ARP poisoning.