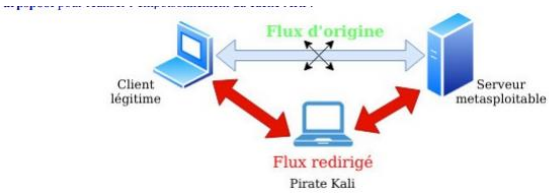
YALCIN LORENZO BTSSIO

COMPTE RENDU KALI LINUX

Avant de débuter le tp installer les machines suivantes :



TRAVAIL 1 :

Q1) Nous allons commencer par activer le routage de la machine Kali afin que la machine du pirate joue le rôle du routeur : nano /*etc/*sysctl.conf (et enlever le commentaire) :

```
# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1

# Uncomment the next line to enable packet forwarding for IPv6
#  Enabling this option disables Stateless Address Autoconfiguration
#  based on Router Advertisements for this host
#net.ipv6.conf.all.forwarding=1
```

Puis faire un sysctl -p pour recharger les paramètres système

Ensuite configurer le fichier nano /*etc*/network/interfaces en mettant une adresses ip manuel (la mienne du vlan20) :

```
  GNU nano 4.9.1                                  /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
        address 172.17.10.15 /24
        gateway 172.17.10.1
        # dns-* options are implemented by the resolvconf package, if installed
        dns-nameservers 8.8.8.8 8.8.4.4
#       dns-search local.sio.fr
```

Q2) Le protocole ARP (Address Resolution Protocol) permet de faire correspondre une adresse IP à une adresse MAC sur un réseau local, les ordinateurs et périphériques communiquent avec des adresses IP (logiques), mais pour envoyer un paquet sur un réseau local, ils ont besoin de l'adresse MAC (physique) de la machine cible.
ARP permet donc de traduire une IP en MAC automatiquement.

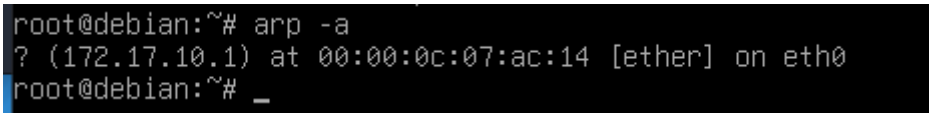
- arp -n :
Affiche la table ARP avec les adresses IP et MAC

- arp -a :
Affiche toutes les entrées ARP.arp -d <IP> :
Supprime une entrée ARP.

- ip neigh show (Linux moderne) :
Affiche la table de voisins ARP (équivalent de arp -a).

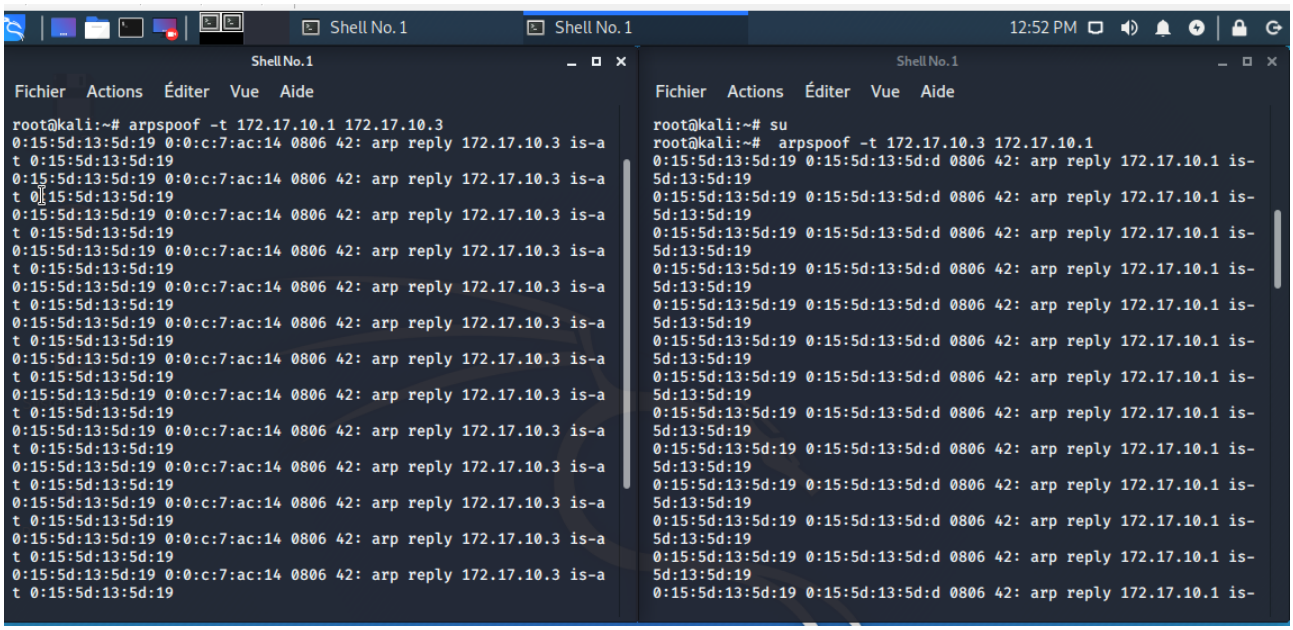
L'ip de la machine client est 172

Q3) Relever le cache ARP de la machine cliente légitime avant de réaliser l'attaque :

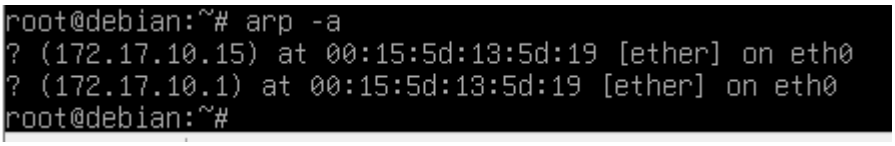


Q4) L'adresse MAC nous permet identifié l'appareil physiquement sur le réseau local, tandis que l'IP identifie l'appareil logiquement sur l'ensemble d'Internet.

Q5) Ensuite sur la machine kali je vais réaliser une attaque de type empoisonnement de cache ARP ciblant le client légitime en ouvrant 2 terminals et en utilisant le commande :
- arpspoof -p ipvictime ippasserelle (sur le premier terminal)
- arpspoof -p ippasserelle ipvictime (sur le deuxième terminal)



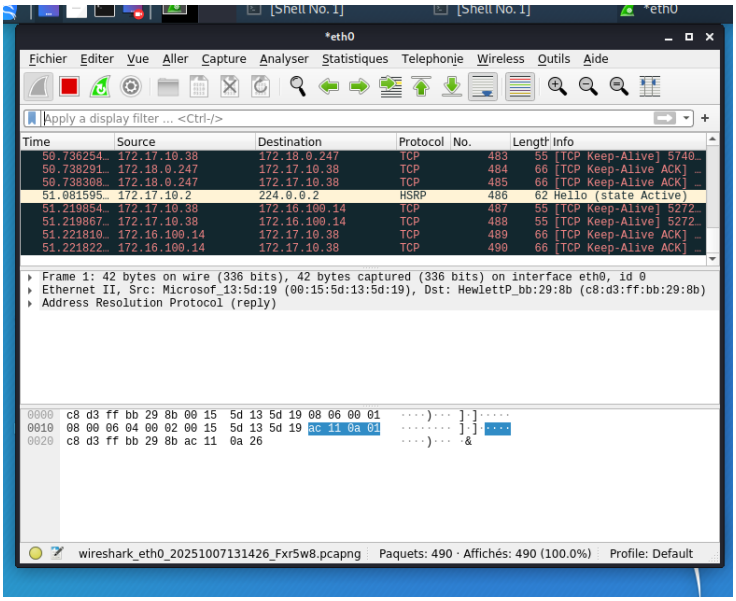
Q6) Voici le nouveau cache arp du client victime :



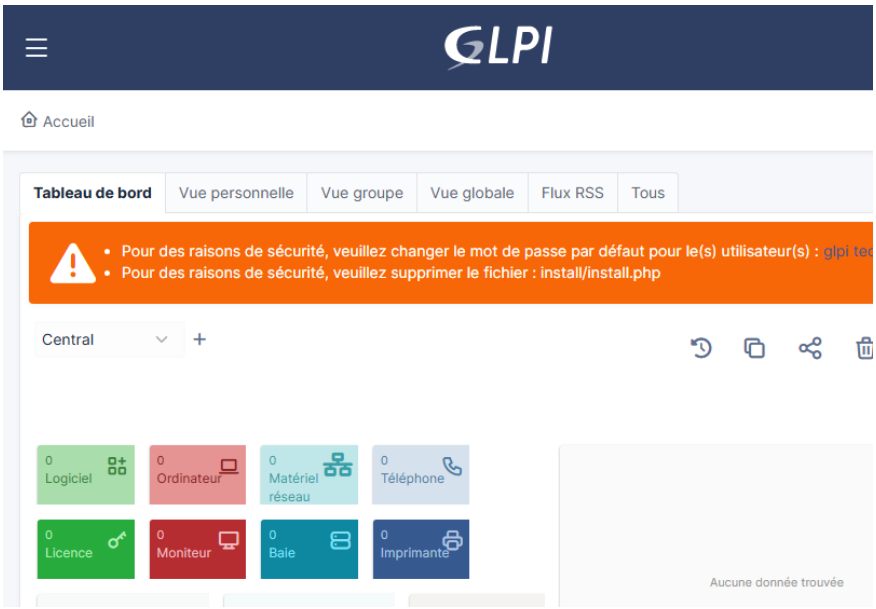
On remarque que l'attaque a bien été effectué la machine ARP de la victime montre que deux adresses IP différentes (172.17.10.15 et 172.17.10.1) pointent vers la même adresse MAC (00:15:5d:13:5d:19) , celle de notre machine attaquante. La victime croit maintenant que nous sommes à la fois la passerelle et l'autre hôte.

TRAVAIL 2 :

Q1)



Q2)



Q3) Oui, si la connexion n'est pas chiffré donc en http, donc avec un analyseur de paquet par exemple wireshark sur kali le pirate peut capturer le nom d'utilisateur, le mot de passe et toutes les données transmises afin d'éviter cela il faut utiliser HTTPS pour chiffrer la communication.

Q4) En utilisant Wireshark sur Kali Linux, le pirate peut capturer le trafic réseau HTTP non chiffré et visualiser directement le mot de passe en clair dans les requêtes

TRAVAIL 3 :

Q2. Expliquer le code noté dans le fichier default-ssl et les 2 commandes a2enmod ssl, a2ensite default-ssl

Le fichier default-ssl configure Apache pour utiliser HTTPS sur le port 443 en activant le chiffrement SSL et en définissant l'emplacement des certificats de sécurité. La commande "a2enmod ssl" active le module SSL nécessaire au chiffrement alors que "a2ensite default-ssl" active cette configuration HTTPS sur le serveur.

Après un redémarrage d'Apache, le serveur GLPI devient accessible en HTTPS ce qui chiffre toutes les communications et protège les mots de passe contre Wireshark.

Q3. En configurant un site en HTTPS, l'empoisonnement de cache ARP est-il toujours possible ? Peut-on encore capturer le mot de passe en clair ?

Oui on peut toujours capturer une trame réseau même si la connexion est en HTTPS, mais les mots de passe et noms d'utilisateur ne sont pas lisibles en clair dans ces trames.
L'attaquant voit seulement des données non chiffrées (adresses IP, ports, tailles des paquets) et le reste sera chiffrées ce qui garanti une certaine sécurité,

Q4. Conclure sur l'intérêt du chiffrement dans le contexte du client BOXTOBED.

Le chiffrement est important pour le client BOXTOBED car il protège les échanges entre le client et le serveur ca veut dire que même si quelqu'un intercepte le trafic, les données de type identifiants ou mots de passe restent illisibles ce qui garantit la sécurité et la confidentialité des informations.

Q5. Expliquer pourquoi il peut être important de surveiller les caches ARP de son routeur

Surveiller le cache ARP du routeur est important car cela permet de détecter rapidement des entrées anormales ou des changements d'association IP↔MAC qui sont signes d'un empoisonnement ARP et ainsi prévenir l'interception ou la redirection du trafic (MITM), les interruptions de service et d'autres compromissions de la sécurité du réseau.