POLYTECHNIQUE MONTRÉAL

LE GÉNIE EN PREMIÈRE CLASSE

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

TP1 : Outils de sécurité

Analyse d'informations par Wireshark et introduction à ASA

1.1 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 20 septembre 2024 - avant 23h55
Pondération	10 %
Directives particulières	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. **2. Capture d'écran de vos manipulations sont obligatoires pour chaque question.** 3. Soumission du rapport (en format PDF ou Word) par moodle uniquement (https://moodle.polymtl.ca). 4. Chaque heure de retard sera pénalisée de 3 points. 5. Avant de débuter votre séance de laboratoire, notez et inscrivez sur le rapport le nom inscrit sur votre station de travail
Chargé de laboratoire	Bilal Itani (bilal.itani@polymtl.ca)
Version originale	Bilal Itani, Mehdi Kadi
Révision	Bilal Itani

1.2 Connaissances préalables

- Familles de protocoles TELNET, FTP, DNS, ARP http, HTTPS.
- Format des messages (RFC 5322 [RFC 2822, RFC 822], RFC 6532)
- Notions de base en réseaux informatiques.

1.3 Objectifs du laboratoire

L'objectif de ce laboratoire est de montrer quelques-unes des fonctionnalités de l'analyseur de protocole Wireshark et de mettre en lumière l'une des limitations de sécurité de la famille des protocoles non chiffrés. Ce laboratoire consiste aussi en une introduction à l'équipement de protection réseau ASA (Adaptive Security Appliance ou unité de sécurité adaptative) à l'étudiant et de découvrir quelques solutions à des vulnérabilités en termes de sécurité informatique.

De manière spécifique, au terme de ce laboratoire, il s'agira pour l'étudiant de comprendre le composant « format de message » de la famille des protocoles ICMP, FTP, SFTP et de comprendre le processus d'analyse et de traçage de messages.

Les réseaux d'aujourd'hui présentent des environnements de plus en plus complexes au niveau des protocoles impliqués. Tout bon administrateur ou concepteur qui est impliqué dans des environnements réseautiques doit bien connaître les faiblesses des réseaux afin de bien protéger ceux-ci. L'analyseur de protocoles est l'outil essentiel qui permet de localiser en isolant une problématique (panne) dans un réseau. Il permet aussi d'analyser ce qui se passe sur le réseau et de découvrir comment une attaque est exécutée.

L'analyseur de protocole place l'interface réseau dans un mode appelé promiscuous ou banalisé. Dans un tel mode, toute trame reçue sur la carte réseau est remontée à l'analyseur de protocoles et affichée à l'intérieur de celui-ci. Ce qui n'est pas le cas en temps régulier où la carte réseau rejette toute trame qui n'est pas conforme à l'adresse MAC et IP du poste.
Ce laboratoire se veut avant tout une familiarisation avec l'environnement du laboratoire. Ceci consiste en l'utilisation de l'analyseur de protocole, l'analyse de quelques trames (processus d'encapsulation des données dans la pile TCP/IP du modèle) et utilisation d'images virtuelles. Les informations obtenues touchent des possibilités de faille de sécurité et les outils utilisés le seront à nouveau dans les laboratoires subséquents.

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 de 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 gérance de l'environnement.

1.4 [AU BESOIN] Accès à distance au laboratoires 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 L4708.

3. Saisir vos identifiants : gigl\{VOTRE_NOM_D'UTILISATEUR_POLY} et le mot de passe.

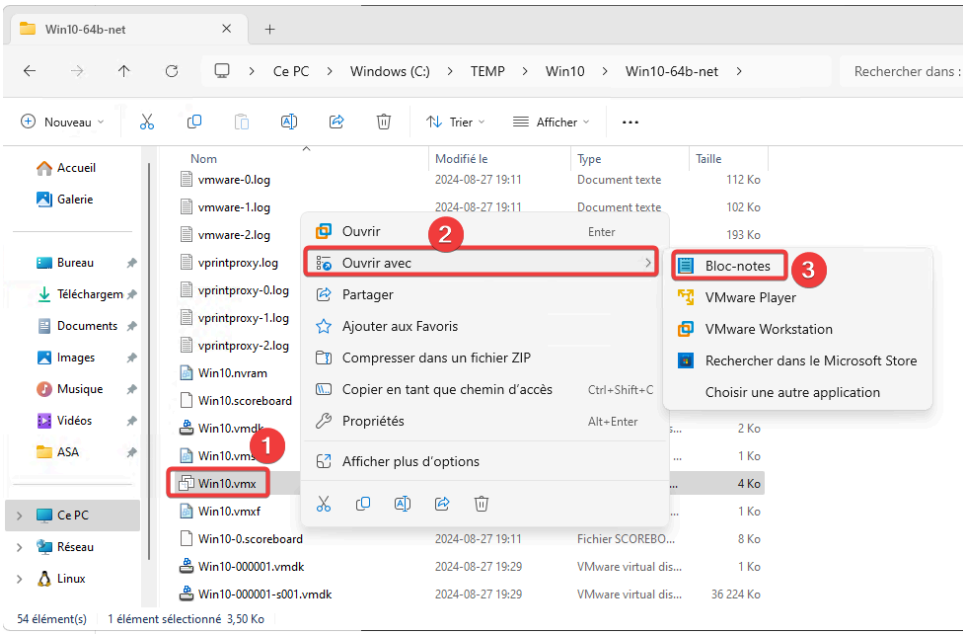
2.1 Partie A - Rappel et description avec ipconfig /all (10 points)

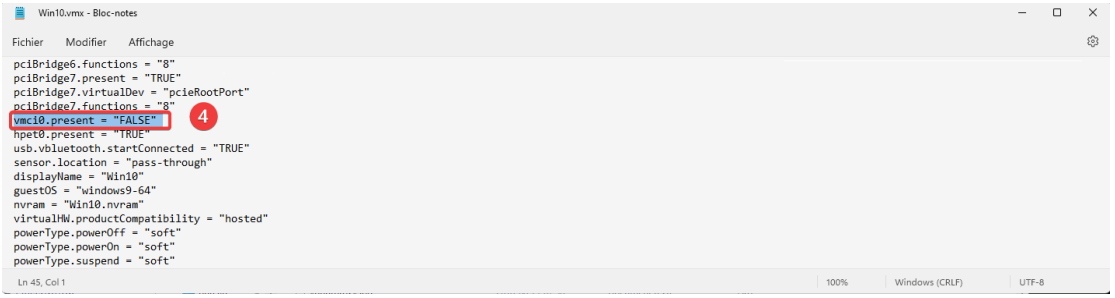
2.1.1 Configuration de votre environnement

Copiez les images virtuelles suivantes :

NB : Pour des questions de vitesses et d'espace, si vous devez copier ou cloner une VM, ne le faites pas sur votre espace personnel (X) mais dans le dossier C:\TEMP. À noter que le **répertoire C:\TEMP est supprimé automatiquement après chaque redémarrage de la machine et toutes les nuits ! SAUVEGARDER VOS FICHIERS** ailleurs à la fin de chaque séance !

- Copiez ou clonez les machines virtuelles C:\VM\INF8402\Windows10, C:\VM\INF8402\Kali_linux_2018.2 et C:\VM\INF8402\Metasploit2.0.
- **Ajuster les fichiers Win10.vmx, Kali-Linux-2018.2-vm-amd64.vmx et Metasploitable.vmx en les ouvrants avec le bloc-notes et s'assurer que le paramètre vmci0.present = "FALSE"**





- Vérifiez que les machines **Metasploit, Windows 10** et **Kali** sont sur le **VMnet8 (NAT)** et démarrez les systèmes d'exploitation.

- Dans Kali-linux, entrez dans le menu « *Power off / Settings* », changez la résolution d'écran à 1280x768

NB : Pour vous connecter aux machines, utilisez les bons identifiants parmi les suivants :

PC/Server	**User**	**Password**
Kali Linux	root	toor
Metasploit	msfadmin	msfadmin
ASA	polymtl	cisco

Tableau 1 : Identifiants pour les machines virtuelles

2.2.2 Exploration de votre environnement (5 points)

Sur votre **machine physique windows 11**, ouvrez une fenêtre terminale (fenêtre de commande DOS) et effectuez la commande **ipconfig /all**.

Q1) Combien d'interfaces réseau avez-vous (physique et logique) ? Accordez une attention particulière à la configuration réseau de ces interfaces (Ipv4, serveur DHCP, serveur DNS, serveur WINS, etc) (1 point)

Pour la carte la carte Intel 82578 DC :

Remarque : la carte Intel I217-V est la carte réseau de la carte maîtresse et elle est sur le réseau de l'école. La carte Intel Pro 1000 est une carte physique additionnelle ajoutée dans le PC afin de raccorder les images virtuelles sur le commutateur en avant de la classe. De plus, sachez que l'adresse physique MAC (OSI niveau 2) est souvent utilisée par les pirates informatiques qui tentent d'utiliser cette adresse parfois pour des attaques.

Q2) Quels sont les paramètre réseau de la carte Intel I217-V : (0.5 point)

a) Avec les 3 premiers octets de l'adresse MAC (OUI Organisation Unique Identifier) de quelle entreprise s'agit-il pour la fabrication de cette carte réseau.
(http://standards.ieee.org/develop/regauth/oui/oui.txt) :
b) Adresse IPv4 (peut être utilisé par des pirates informatiques, DoS ou autre) :
c) Masque réseau (y a-t-il sous réseautage ?) :
d) Comment cette adresse a été obtenue (note : ce peut être un trou de sécurité) :
e) Adresse IPv6 :
f) Serveur DHCP :
g) Serveur DNS :
h) Server Wins :

Q3) Qu'est-ce qu'un serveur WINS ? Quelle est la différence entre un serveur DNS et un serveur WINS ? (2 points)

N.B : Les services offerts par les 3 serveurs précédents sont des cibles potentielles d'attaque.

Sur les **machines virtuelles windows 10, Kali et Metasploit**, effectuez la commande **ipconfig /all** et la commande **ifconfig** afin d'afficher les paramètres réseaux configurés de vos machines virtuelles.

Q4) Vérifiez que tous les ordinateurs sont dans le même réseau (domaine de diffusion). Faites des tests de connectivité (ping) entre eux, dès que ces tests fonctionnent, écrivez les adresses IP de chaque machine. L'adresse IP de Metasploit est à l'écran. Vous devez inclure des captures d'écran de vos tests de connectivité (0.25 point)

Q5) Si vous trouvez qu'il n'existe pas de connectivité (ping) entre certains ordinateurs, il faudra **expliquer la raison de ce comportement**, **proposer une solution** et finalement **appliquer la solution**. Justifiez votre réponse à l'aide de captures d'écran. (0.25 point)

Q6) Incluez un diagramme de la configuration du réseau (VM + hôte) en précisant les adresses Ipv4 et les masques de sous-réseau de la machine physique ainsi que des machines virtuelles. (1 point)

2.3 TCP/UDP (1 point)

- **Dans la machine Windows 11 physique**, ouvrez un terminal, faites un *ping* avec l'option –t (ping en continu) au Metasploit et vérifiez la connectivité réseau.
- Conservez la fenêtre dos ouverte.
- **Dans Kali-linux** ouvrir l'application Wireshark menu : « *Applications/Sniffing & Spoofing/wireshark* »
- Accepter l'avis de Wireshark qui est en train de travailler comme root.
- Choisissez *Capture interface list*
- Vérifiez l'interface ou il y a déjà du trafic (généralement eth0)
- Choisissez le bouton *start* et choisissez *capture stop* ou l'icône carré rouge qui stop l'échantillonnage.
- Dans le champ *filtre* inscrire *icmp* ou choisir icmp dans le menu déroulant et appliquez le filtre avec le choix *Apply*. Vous obtenez alors les trames *icmp* (ping).

Q7) Pourquoi pouvez-vous voir cette connexion si la machine n'est ni l'origine ni la destination de la connexion ?

Q8) En sélectionnant un paquet dans Wireshark, identifiez les différentes couches du modèle OSI. Quelles sont les informations affichées, consultez l'annexe A ?

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.

2.4 **FTP** (2 points)

- **Assurer d'avoir désactivé le pare-feu Metasploit (sudo ufw disable)**

- Sur **la machine Kali-linux** ouvrir l'application Wireshark (si n'est pas déjà ouvert)
- Cliquez dans menu « *capture / Interfaces* ». Après, sélectionnez l'interface *eth0* et dans la boîte de filtre mettre « Ip.addr == ip Metasploit »
- Ouvrez le client Filezilla sur **la machine Windows 10** et connectez-vous à **la machine Metasploit** avec le même utilisateur et mot de passe.
- Sur Wireshark, placez-vous sur le premier type de paquets FTP, faites un clic droit sur le paquet et sélectionnez « *Follow → TCP stream* ».

Q9) Discutez, d'un point de vue sécurité, du protocole FTP. (1 point)

- Fermez l'analyseur de flux et effacez le filtre.
- Vous devez transmettre une image *.jpg* via FTP vers un autre site. Choisissez n'importe quelle image de démo.
- Placez-vous sur le premier type de paquets *ftp-data* et en utilisant l'analyseur de flux obtenez l'information de l'image, cliquez sur « Enregistrement » et stockez le fichier en mode *raw* sur le bureau avec n'importe quel nom et l'extension de fichier « .jpg ».

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

Q10) Pouvez-vous voir cette image ? Intercepter l'image. Justifiez votre réponse à l'aide d'une capture d'écran de vos étapes. (1 point)

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 Wireshark. 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.

2.5 SFTP (2 points)

- Ouvrez le client Filezilla sur la **machine virtuelle Windows 10** et connectez-vous à la machine Metasploit avec le même utilisateur et mot de passe en utilisant le port 22

Q11) Que signifie l'empreinte digitale affichée lors de la connexion ? (0.5 point)

Q12) Quelle est l'information que vous pouvez trouver de cette connexion dans Wireshark ? (0.5 point)

Q13) Comment utiliseriez-vous Wireshark pour analyser la sécurité d'une entreprise ? (0.5 point)

- Transmettez une image .jpg à nouveau telle que réalisée précédemment.

Q14) Est-il possible d'intercepter l'image ? Justifiez votre réponse (0.5 point)

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.

3.1 Partie B - ASA *Adaptive Security Appliance* (10 points)

Un ASA est une unité d'équipement réseau (telle qu'illustrée sur la figure 1) qui permet d'améliorer la sécurité des réseaux des entreprises. Une configuration de base d'un ASA consiste principalement en 3 zones distinctes étant normalement chacune associées à un réseau (VLAN) différent.

Fig. 1 - Cisco ASA 5520

Normalement, une des zones (interfaces du ASA) est raccordée au réseau Internet, on appelle cette zone OUTSIDE (0) pour représenter l'environnement extérieur de l'entreprise. Une seconde zone appelée INSIDE (100) représente les postes informatiques à l'intérieur de l'entreprise. Normalement, ces postes internes sont sécurisés et l'accès est limité de l'extérieur de l'entreprise (accès VPN, quelques ports spécifiques ouverts, …).

Une troisième zone moins restrictive (ouverte sur l'extérieur de l'entreprise), permet aux utilisateurs externes de l'entreprise d'accéder à des ressources informatiques de l'entreprise (serveur web, base de

données publicitaire ou autres, …). Les données non confidentielles de l'entreprise qui sont disponibles aux clients ou autres utilisateurs s'y retrouvent et cette zone se nomme DMZ (50) pour démilitarisée (delimitarized).

3.1.1 (Partie 2) Préparation de l'environnement

Interface ASA	IP	Commutateur VMware	Machine virtuelle
INSIDE (GigabitEthernet0)	192.168.199.5/24	VMnet 1	Windows 10
DMZ (GigabitEthernet1)	192.168.126.5/24	VMnet 2	Metasploit
OUTSIDE (Internet, GigabitEthernet2)	192.168.11.5/24	VMnet 8 (NAT)	Kali-Linux

Tableau 2 - Configuration réseau pour la deuxième partie du laboratoire

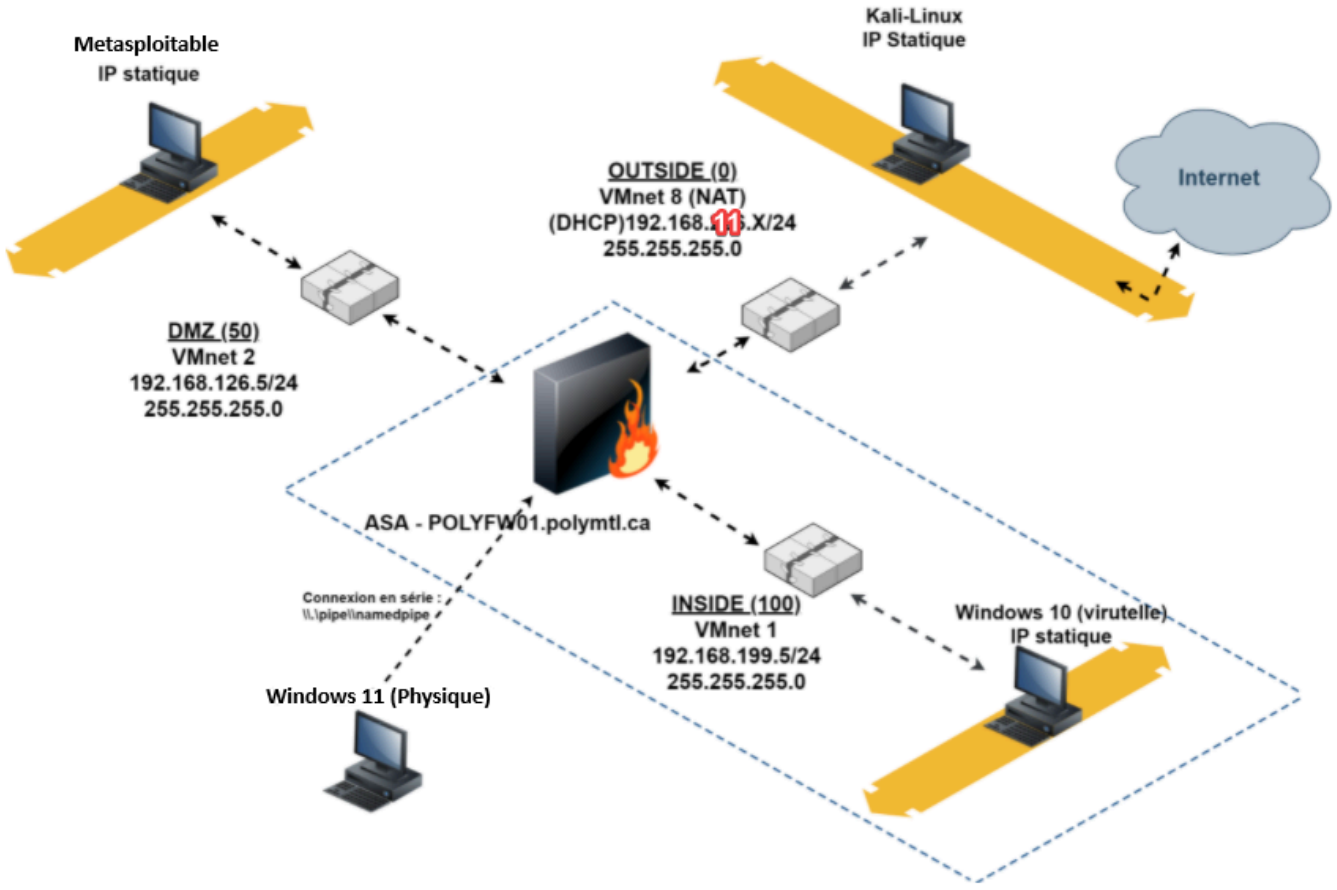
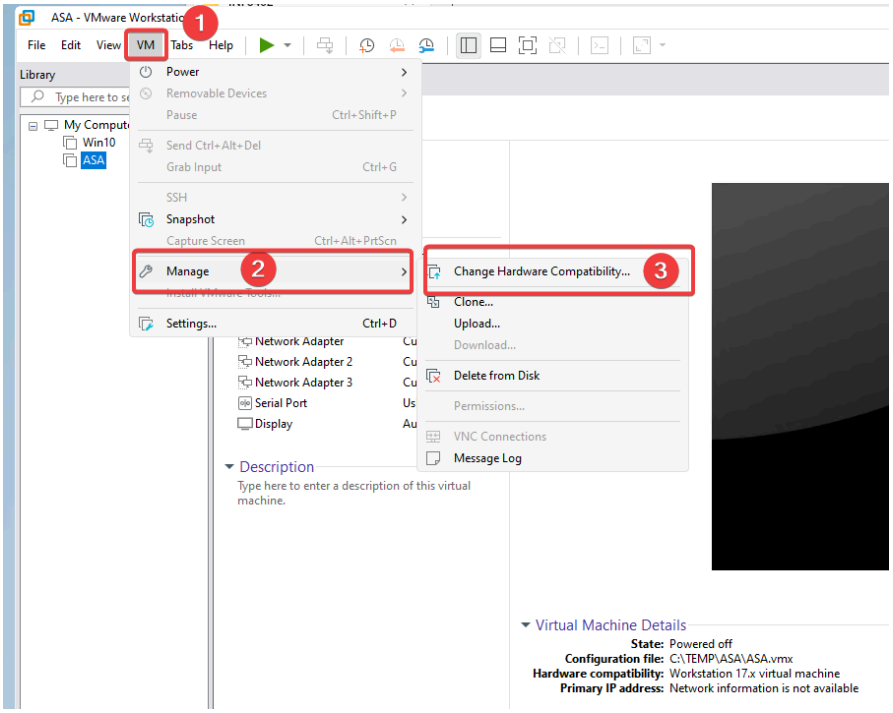
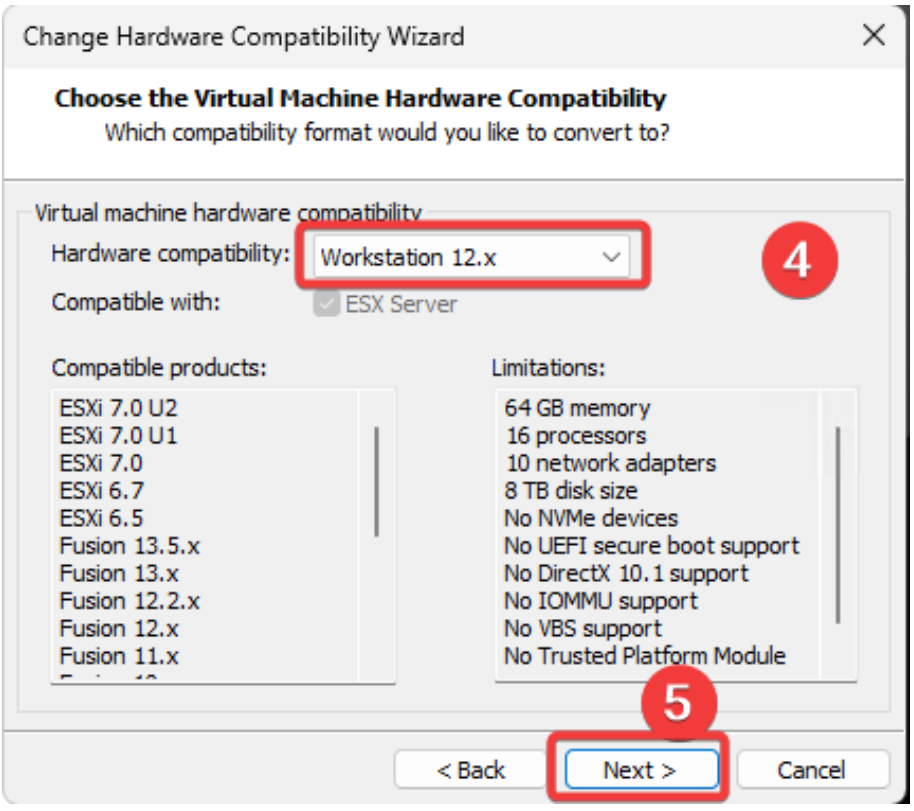
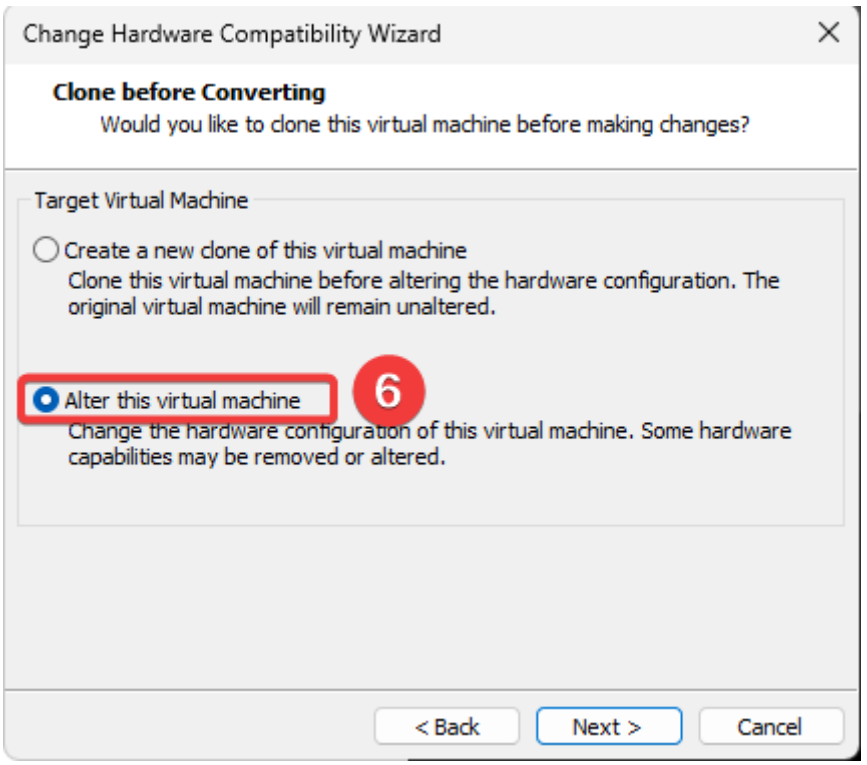


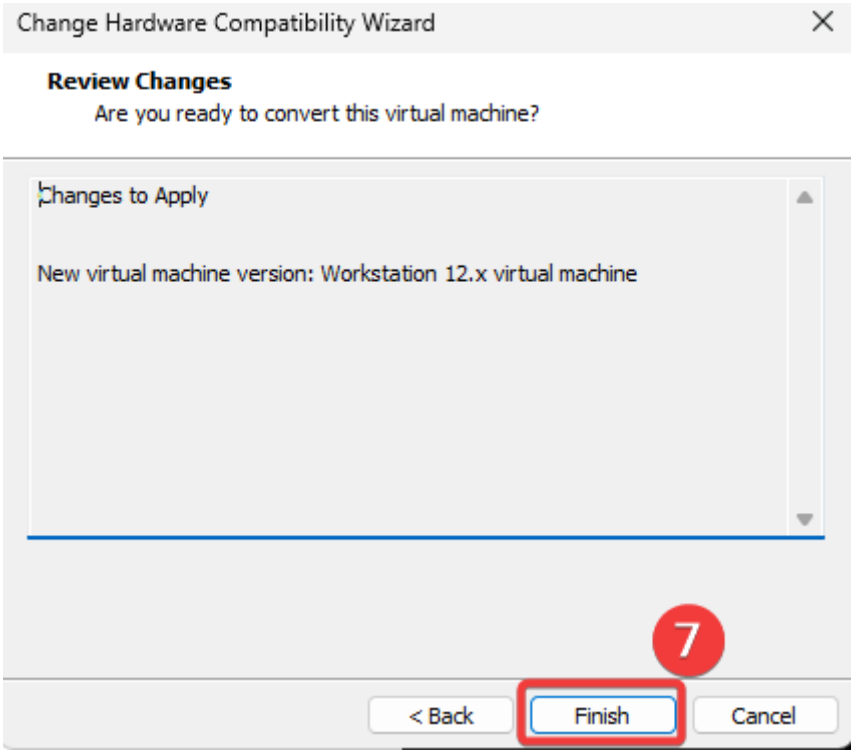
Fig.2 - Configuration requise pour la deuxième partie du laboratoire

- Éteignez les machines virtuelles.
- Copiez ou clonez la machine virtuelle C:\VM\INF8402\ASA
- **Ajuster le fichier ASA.vmx en l'ouvrant avec bloc-notes et s'assurer que le paramètre vmci0.present = "FALSE". Faire de même pour les autres machines virtuelles.**
- **Ajuster la compatibilité hardware de la machine ASA à Workstation 12.x comme suit:**









- Lorsque le répertoire est copié, ouvrez les VMs **Windows 10**, **Metasploit**, **Kali-linux** et **ASA** dans VMware. Configurez les cartes réseau virtuelles de ces machines afin que les images soient dans le réseau VMnet correspondant. (Tableau 2 et Figure 2).
- Démarrez les machines virtuelles et prenez le contrôle (ownership) des images virtuelles.
- Pour l'image d'**ASA**, ouvrez et démarrez la machine virtuelle ASA. Lors de l'affichage de la fenêtre de commande, appuyez sur la touche "*enter*". (cela ne donne pas une console directe sur le bureau !)

- Utilisez les touches CTRL-ALT afin de naviguer d'une image virtuelle à l'autre et au besoin retournez à votre système d'exploitation de base (machine Windows 11 physique).

3.1.2 Configuration de la machine ASA (accès au mode console)

- Sur votre **machine Windows 11 physique**, exécutez l'application PuTTY soit l'exécutable C:\Program Files (x86)\PuTTY\putty.exe. Dans la fenêtre Putty configuration, sélectionnez *serial* et entrez : « \\.\pipe\\namedpipe » et ensuite open. Tapez « *enter* » dans la fenêtre de la console ouverte.
- Accédez à ASA en mode console avec la touche *enter* (aucun mot de passe).
- Exécutez la commande « *login* » puis inscrire « *polymtl* » comme nom d'utilisateur et « *cisco* » comme mot de passe.
- Exécutez la commande « *show running-config* » et « *show ip* », prenez note de la configuration des interfaces GigabitEthernet(0/1/2).

Exécuter ces commandes sur votre console :

- configure terminal
- http 192.168.199.0 255.255.255.0 INSIDE (.199 désigne l'interface VMnet 1)
- int GigabitEthernet0
- ip address 192.168.199.5 255.255.255.0 (.199 désigne l'interface VMnet 1)

Exécutez à nouveau les commandes « *show running-config* » et « *show ip* » et confirmez que votre interface INSIDE est configurée sur l'interface VMnet 1)

3.1.3 Configuration du réseau des machines virtuelles Windows 10 et Metasploit

- Sur **la machine virtuelle Windows 10**, cliquez sur « *Start* » et recherchez « *Control Panel* ». Cliquez sur « *Network and sharing center* ». Dans la nouvelle fenêtre, cliquez sur « *Ethernet0* », à côté de « *Connections* ». Dans la nouvelle fenêtre, appuyez sur « *Properties* ». Faites un double-clic sur « *Internet Protocol Version 4 (TCP/IPv4)* » et configurez de manière statique la machine virtuelle Windows 10 avec l'adresse IP "192.168.199.100", le masque "255.255.255.0" et la route par default (*default gateway*) "192.168.199.5". Configurez aussi les DNS pour "8.8.8.8" et "8.8.4.4".

- Sur **la machine virtuelle Metasploit**, modifiez le fichier */etc/network/interfaces* pour remplacer la dernière ligne (*iface eth0 inet dhcp*) par :

  iface eth0 inet static

  address 192.168.126.100

  netmask 255.255.255.0

  gateway 192.168.126.5

  Redémarrez Metasploit après les modifications afin de les appliquer.

- Sur **la machine virtuelle Kali**, modifier de façon manuelle l'adresse IP pour qu'elle soit statique:

  Flèche du bas à côté du bouton power > Wired Connected > Wired Settings > Icone engrenage Wired > Onglet IPv4 :

Address	192.168.11.100
Netmask	255.255.255.0
Gateway	192.168.11.5
Dns	8.8.8.8, 8.8.4.4

3.2 Informations générales et tableau de bord des ASA (1.5 points)

- Démarrez l'application *asdm-launcher* qui est sur le bureau de votre **machine virtuelle windows 10**.
- Connectez-vous à l'interface GigabitEthernet0 d'ASA avec l'adresse Ipv4 configurée précédemment en utilisant le compte « polymtl » et le mot de passe « cisco »

Q15) Quel modèle d'ASA virtuel avez-vous ? Quelle est la version IOS de cet ASA ? Type de License ? (0.5 point)

Q16) Quelle est l'utilité d'un système ASA? Aidez-vous en consultant les informations disponibles dans le tableau de bord de l'ASA. (0.5 point)

Q17) Combien d'interfaces et de zones sont actuellement configurées (précisez-leur nom dans votre rapport) sur le ASA et combien peuvent être créés dans cet ASA virtuel ? (0.5 point)

3.3 Assistants (Wizards) (2.5 points)

Entrez et familiarisez-vous avec le menu de l'assistant de démarrage (*Wizard → Start-up wizard*).

Configurez les interfaces DMZ et OUTSIDE avec les adresses IP statiques correspondantes dans le tableau 2.

Q18) Quelle est la signification du niveau de sécurité de l'interface d'ASA ? Configurez le niveau de sécurité de l'interface **INSIDE à 100** et **DMZ à 50**, et ajoutez une capture d'écran. (2.5 points)

3.4 Règles de NAT, L4 pour pare-feu ASA (6 points)

Q19) Si un pare-feu n'a pas de règles, est-ce que les paquets sont réacheminés ou jetés ?
(0.25 point)
Q20) Quelle est la différence entre NAT et PAT ? (0.25 point)
Q21) Pourquoi existe-t-il des règles pare-feu (*Access Rules*), des règles NAT (*NAT Rules*) et des règles de services politiques (*Service Policy Rules*). (0.5 point)
Q22) Créez un NAT pour permettre à tous les utilisateurs des réseaux « INSIDE » et « DMZ » d'aller vers internet (ajoutez une capture d'écran à chaque étape). Vérifiez que la **machine virtuelle Windows 10** peut aller sur internet. Expliquer aussi ce qu'est une route statique (1.5 points)

- Si c'est nécessaire, ajoutez une route statique. Routing → Static Routes → Interface « OUTSIDE », IP Address « 0.0.0.0 » (Any), Netmask « 0.0.0.0 », Gateway IP « serveur WINS de l'interface VMnet8 »

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

Q23) Effectuez les mêmes étapes afin de donner accès à Internet à la **machine virtuelle Metasploit** présente sur le VMnet 2. (1.5 points)
Q24) Ajoutez les règles de pare-feu, soit des règles d'accès (*Access Rules*), permettant à **la machine Windows 10 (INSIDE)** d'effectuer un ping sur **la machine Metasploit (DMZ)** sans que **la machine Kali linux (OUTSIDE)**, située à l'extérieur du réseau, puisse le faire. (2 points)

Annexe A

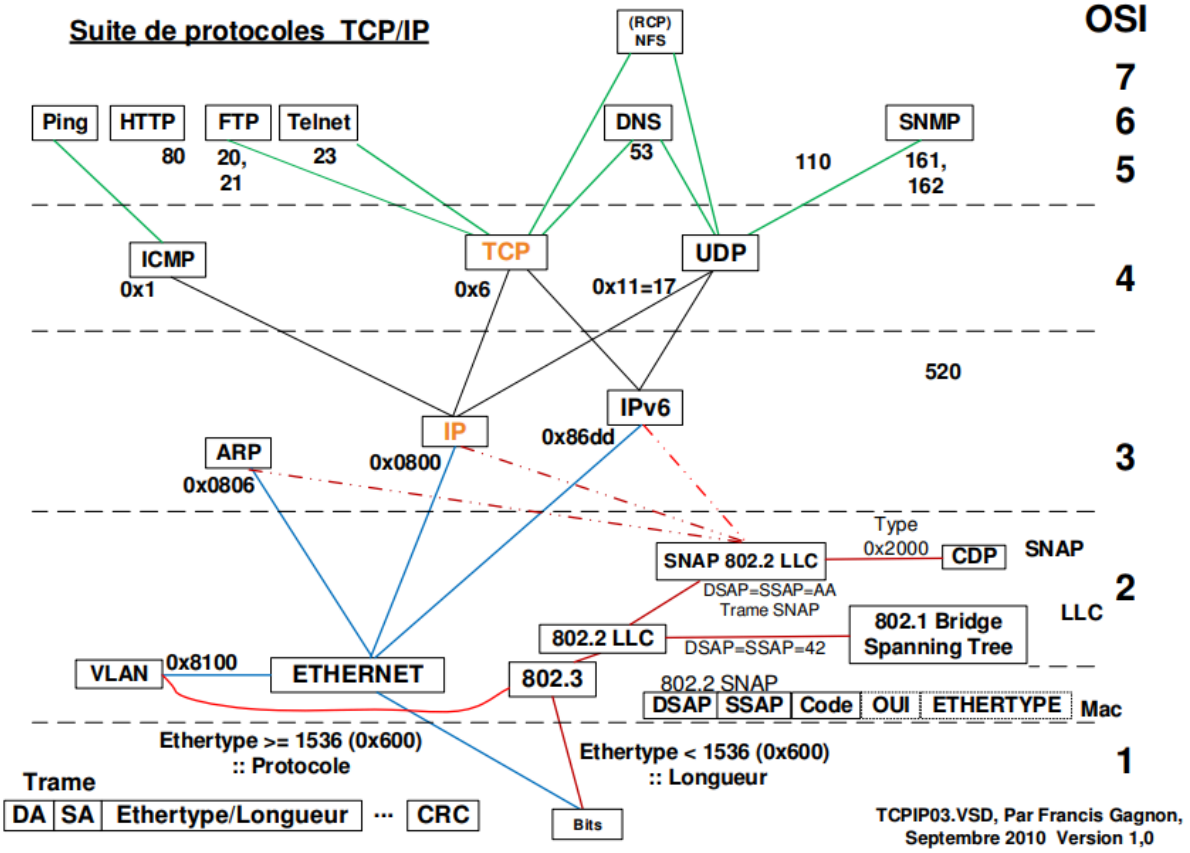


Fig.3 - Modèle OSI

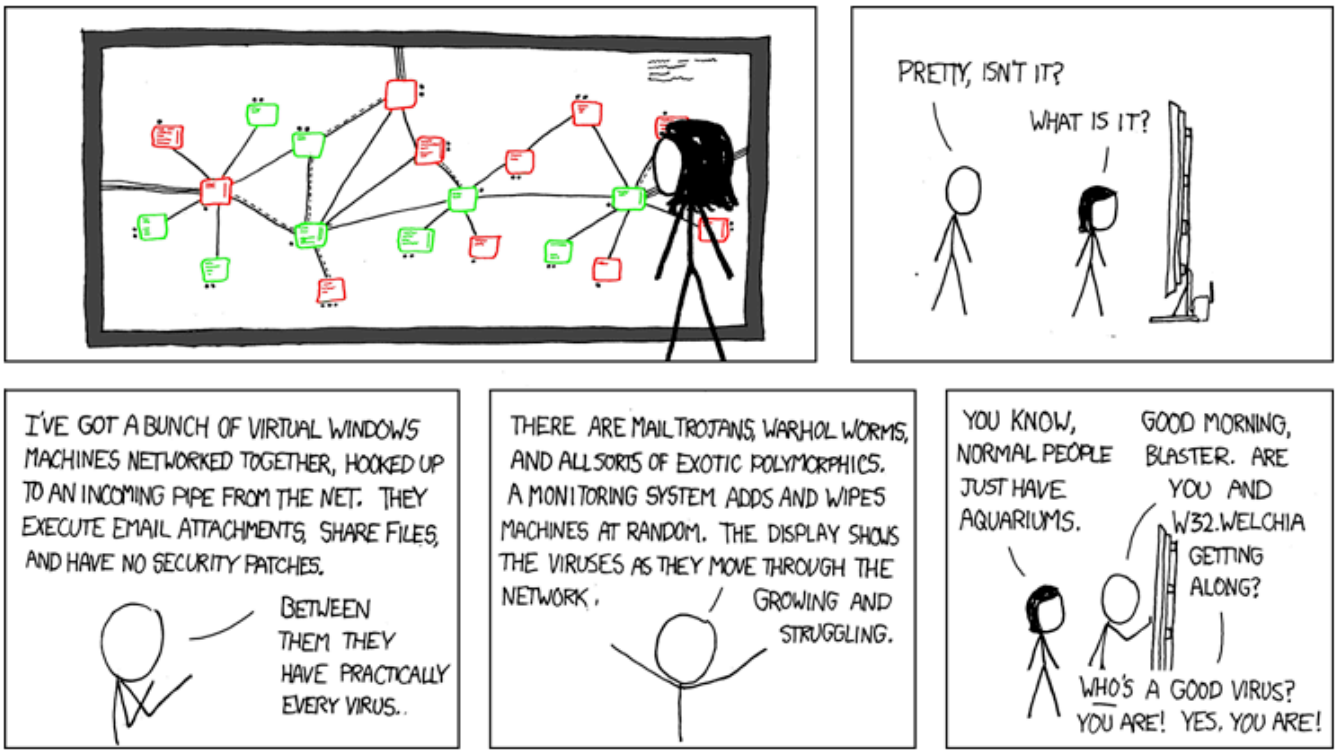


Fig.4 - Network, source : xkdc, https://xkcd.com/350/