POLYTECHNIQUE MONTRÉAL

LE GÉNIE EN PREMIÈRE CLASSE

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

TP3 : ASA - Configuration par ligne de commande

1.1 Informations générales

Session	Automne 2024
Public cible	Étudiants du cours INF8402
Taille de l'équipe	3 étudiants
Date et lieu de réalisation	À distance
Date de remise	22 Novembre 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 questions** 3. Soumission du rapport (en format PDF) par moodle uniquement (https://moodle.polymtl.ca). 4. Chaque heure de retard sera pénalisée de 3 points.
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 DNS, ARP http, HTTPS;
- Notions de base en réseaux informatiques;
- Notions configuration Pare-feux;
- Notions utiles par l'exploitation de vulnérabilités de sécurité.

1.3 Objectifs du laboratoire

L'objectif de ce laboratoire est d'impliquer l'étudiant dans un environnement virtuel similaire aux situations qu'il peut rencontrer en entreprise, avec un problème réel où il peut démontrer toutes les connaissances acquises aux laboratoires antérieurs.

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 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.

1.4 ASA *Adaptive Security Appliance (Mise en situation)*

Le premier laboratoire vous a permis de travailler avec l'application *asdm-launcher* (Cisco Adaptive Security Device Manager), mais votre licence payante va expirer et votre budget serré ne vous permet pas d'en acheter une nouvelle pour l'année prochaine. Vous vous êtes donc fixé comme objectif d'apprendre à configurer ASA sans avoir à utiliser Cisco ASDM. En effet, vous vous rappelez que avez utilisé un terminal lors du premier laboratoire afin de configurer par ligne de commande une interface d'ASA.

Afin de vous familiariser avec les commandes vous serez portés, lors de ce dernier laboratoire, à reproduire certaines étapes que vous avez effectuées lors du premier laboratoire, mais cette fois-ci en utilisant un terminal putty donnant accès à une console permettant de configurer ASA.

Pour ce laboratoire nous souhaitons configurer la zone appelée INSIDE qui a un niveau de sécurité de (100) et qui 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, …). Il faut configurer aussi , lors de ce laboratoire, une zone (interfaces du ASA) qui est raccordée au réseau Internet, et qui s'appelle zone OUTSIDE (0) pour représenter l'environnement extérieur de l'entreprise.

1.4.1 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)	192.168.226.5/24	VMnet 8 (NAT)	Kali

Tableau 1 - Configuration réseau de la machine utilisée

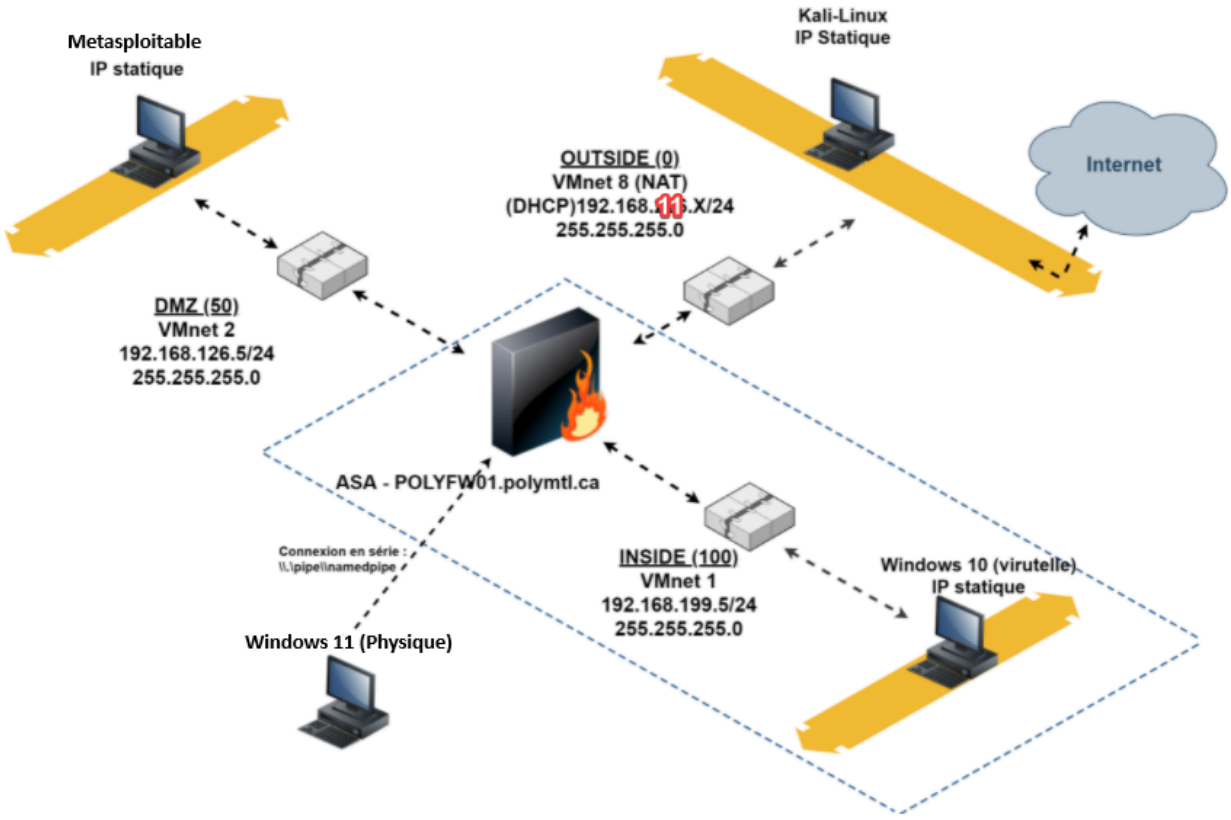
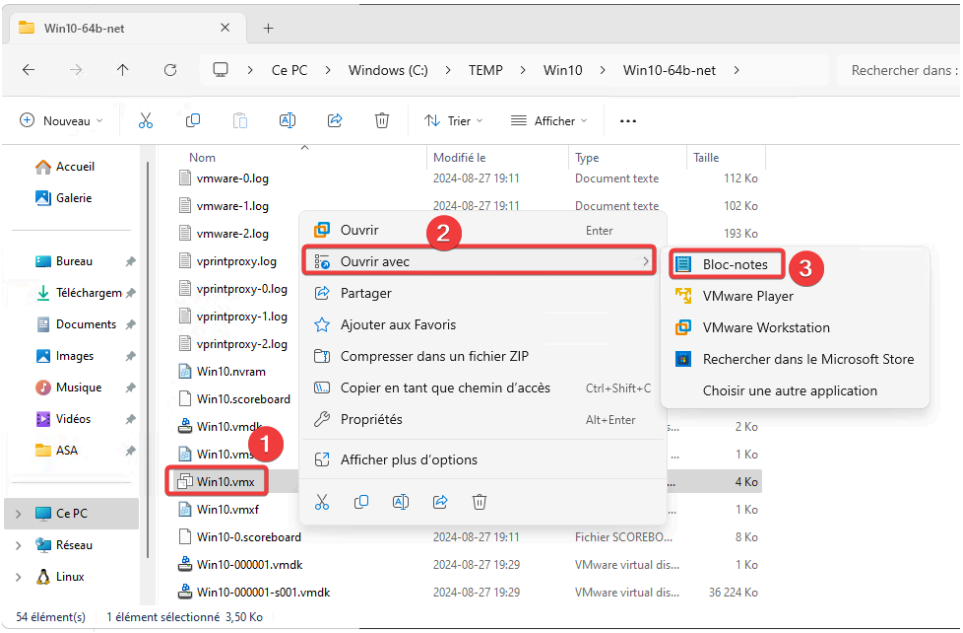
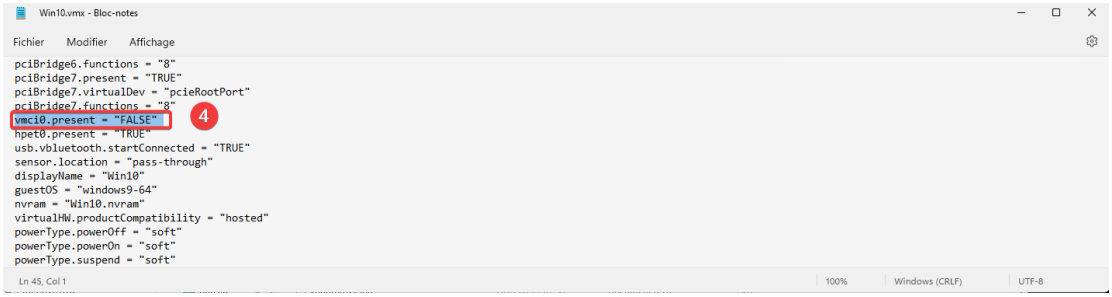


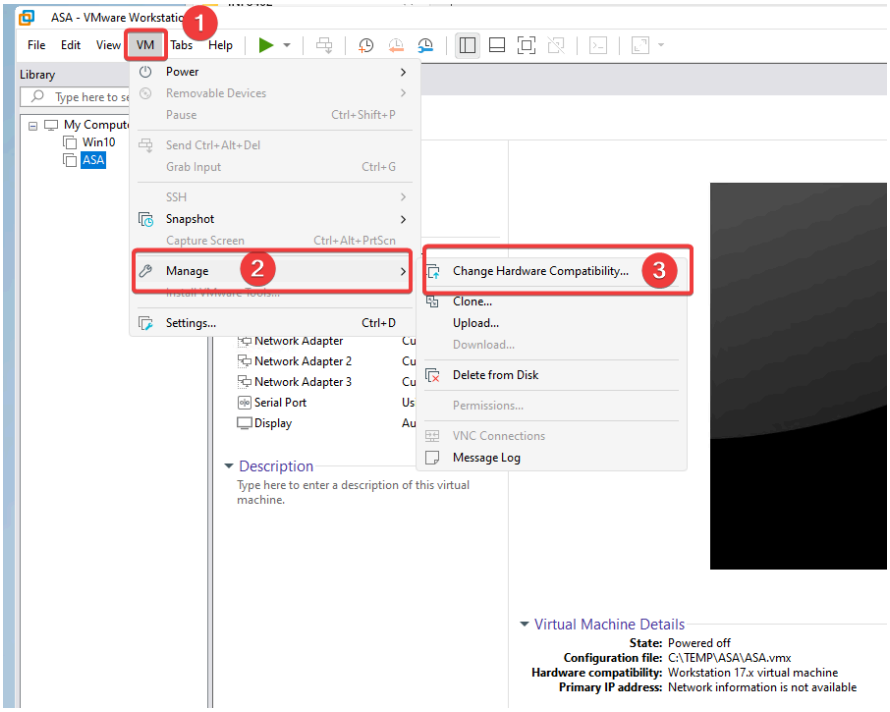
Fig.1 - Configuration requise pour la deuxième partie du laboratoire

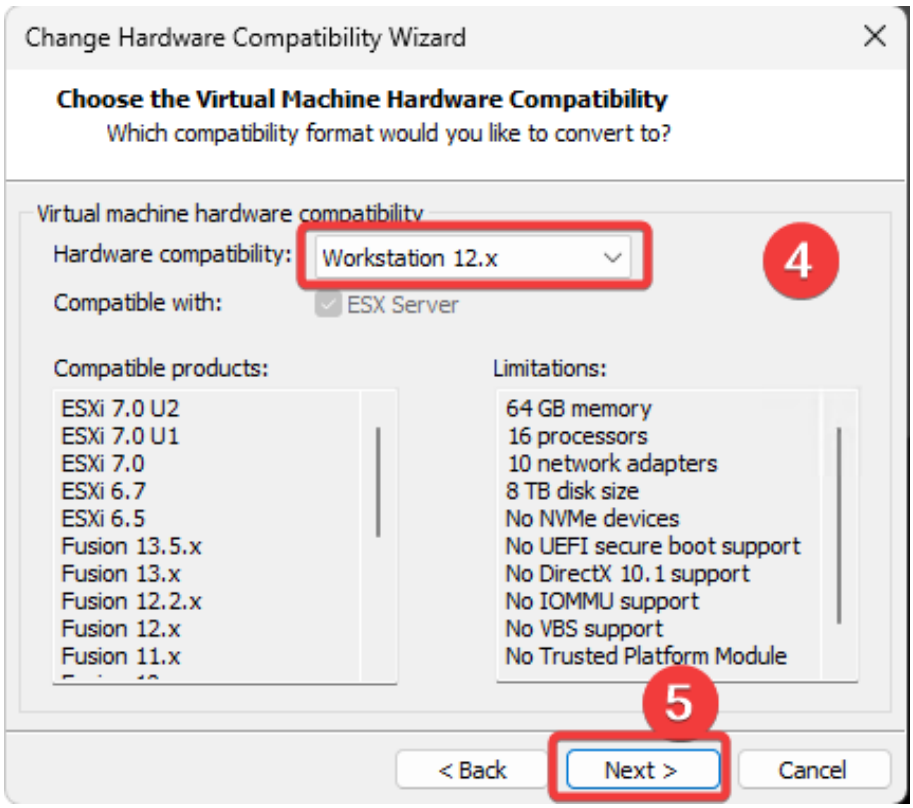
- Rendez-vous au répertoire C:\VM\INF8402\.
- Copiez ou clonez la machine virtuelle **ASA** dans C:\TEMP\.
- Copiez ou clonez la machine virtuelle **Windows 10** dans C:\TEMP\
- Copiez ou clonez la machine virtuelle **Metasploit** dans C:\TEMP\.
- Copiez ou clonez la machine virtuelle **Kali** dans C:\TEMP\.
- **Ajuster les fichiers Win10.vmx, Kali-Linux-2018.2-vm-amd64.vmx, Metasploitable.vmx et ASA.vmx en les ouvrants avec le bloc-notes et s'assurer que le paramètre vmci0.present = "FALSE"**

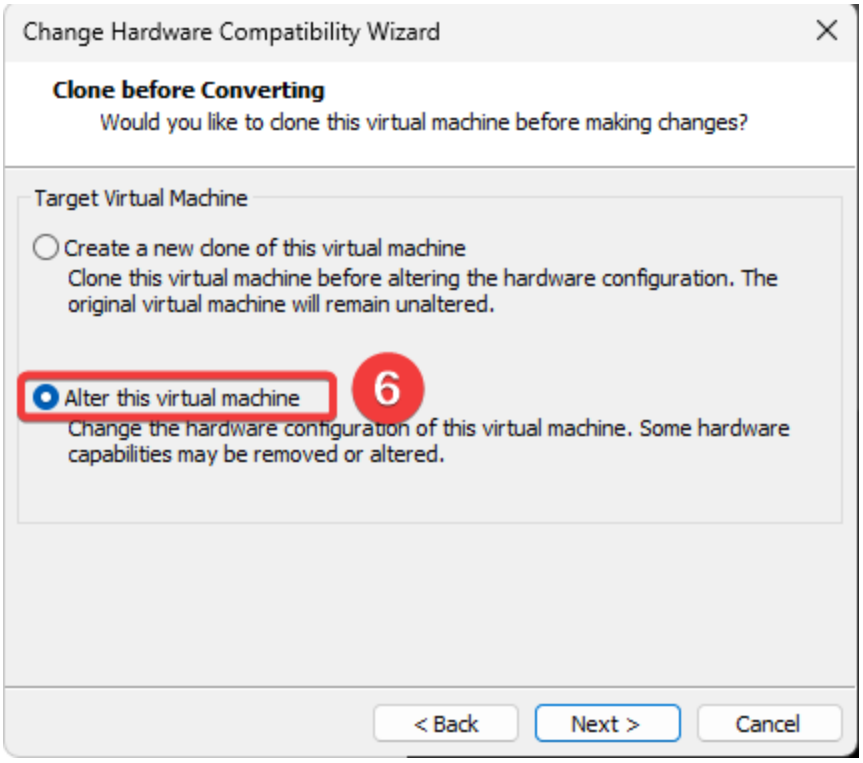

Win10-64b-net
Ce PC
Windows (C:)
TEMP
Win10
Win10-64b-net
Rechercher dans :
Nouveau
Trier
Afficher
Accueil
Galerie
Bureau
Téléchargem
Documents
Images
Musique
Vidéos
ASA
Ce PC
Réseau
Linux
Nom
Modifié le
Type
Taille
vmware-0.log
vmware-1.log
vmware-2.log
vprintproxy.log
vprintproxy-0.log
vprintproxy-1.log
vprintproxy-2.log
Win10.nvram
Win10.scoreboard
Win10.vmdk
Win10.vmx
Win10.vmxf
Win10-0.scoreboard
Win10-000001.vmdk
Win10-000001-s001.vmdk
2024-08-27 19:11
Document texte
112 Ko
102 Ko
193 Ko
2024-08-27 19:11
Fichier SCOREBO...
8 Ko
2024-08-27 19:29
VMware virtual dis...
1 Ko
36 224 Ko
4 Ko
54 élément(s)
1 élément sélectionné 3,50 Ko
Ouvrir
Enter
Ouvrir avec
Partager
Ajouter aux Favoris
Compresser dans un fichier ZIP
Copier en tant que chemin d'accès
Ctrl+Shift+C
Propriétés
Alt+Enter
Afficher plus d'options
Bloc-notes
VMware Player
VMware Workstation
Rechercher dans le Microsoft Store
Choisir une autre application
1
2
3

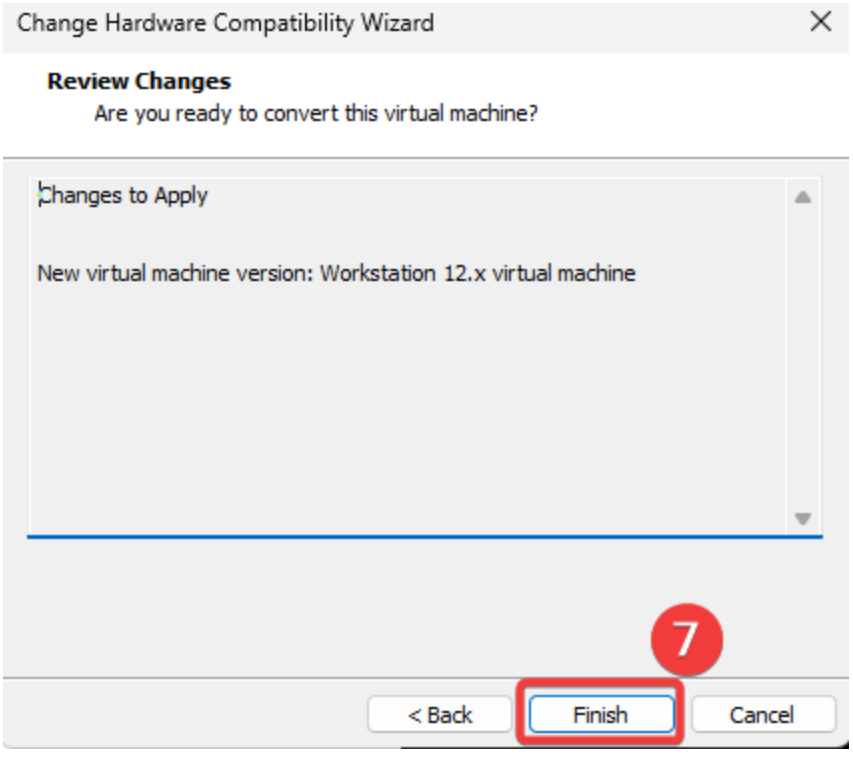

Win10.vmx - Bloc-notes
Fichier
Modifier
Affichage
pciBridge6.functions = "8"
pciBridge7.present = "TRUE"
pciBridge7.virtualDev = "pcieRootPort"
pciBridge7.functions = "8"
vmci0.present = "FALSE"
hpet0.present = "TRUE"
usb.vbluetooth.startConnected = "TRUE"
sensor.location = "pass-through"
displayName = "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
4

- **Ajuster la compatibilité hardware de la machine ASA à Workstation 12.x comme suit:**









- Configurez la carte réseau virtuelle de la machine **Windows 10** afin que l'image soit dans le réseau VMnet correspondant. (Tableau 1 et Figure 1).

- 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 10 physique).

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

- Sur votre **machine Windows 10 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). Il se peut que GigabitEthernet 1 et 2 n'apparaissent pas.

1.4.3 Configuration du réseau des machines virtuelles Windows 10

- 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 défault (*default gateway*) "192.168.199.5". Configurez aussi les DNS pour "8.8.8.8" et "8.8.4.4".

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

Tout d'abord, configurez l'interface INSIDE de manière statique en exécutant les commandes suivantes sur votre console putty:

- 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)

Vous pouvez exécuter à nouveau les commandes « *show running-config* » et « *show ip* » afin de confirmer que votre interface INSIDE est bien configurée sur l'interface VMnet 1.

Remarque : Vous pouvez à présent démarrez l'application asdm-launcher qui est sur le bureau de votre machine virtuelle Windows 10 en vous connectant à l'interface GigabitEthernet0 d'ASA avec l'adresse Ipv4 configurée précédemment en utilisant le compte « polymtl » et le mot de passe « cisco ».

Important : Vous devez répondre aux questions suivantes sur votre rapport et exécuter ces commandes sur la console putty. À chaque question, vous devez joindre une capture d'écran de l'interface ASDM afin de démontrer l'impact de chaque commande sur la configuration d'ASA. Vous pouvez consulter le guide de configuration du Cisco ASA de série 5500[1] afin de vous familiariser avec les commandes disponibles.

[1] https://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config.html

Format obligatoire pour votre rapport:

1. Écrivez vos réponses en identifiant à quelles questions vous répondez (toutes vos réponses devraient se retrouver dans la première page du rapport).
2. Ajoutez une annexe à votre rapport qui regroupe toutes les captures d'écrans nécessaires pour répondre aux questions.

Q1) Quelle est la commande qui permet de fixer le niveau de sécurité de l'interface INSIDE à 100? **(1 point)**

Q2) Quelle(s) commande(s) permet(tent) de configurer l'interface GigabitEthernet2 telles que présentée dans le tableau 1? **(2 points)**

Q3) Il est possible de constater que l'interface GigabitEthernet2 ne possède pas de nom. Quelle commande permet de nommer l'interface GigabitEthernet2 à OUTSIDE? **(1.5 points)**

Q4) Encore sur ASDM, il est possible de constater que l'interface GigabitEthernet2 n'est pas activée. Quelle commande permet d'activer cette interface? **(2 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.

Q5) Quelle(s) commande(s) permet(tent) de créer un NAT pour permettre à tous les utilisateurs des réseaux « INSIDE » d'aller vers internet. **(2 points)**

Q6) Quelle commande permet d'ajouter une route statique? **(1.5 points)**

N'oubliez pas de préciser ces paramètres dans votre commande : « OUTSIDE », IP Address « 0.0.0.0 » (Any), Netmask « 0.0.0.0 », Gateway IP « serveur WINS de l'interface VMnet8 ».

Q7) À ce stade, vous devriez avoir internet sur la machine window 10. De la même façon, donnez accès à internet à la machine Metasploit. Vous devez expliciter toutes les commandes à l'aide de captures d'écran. Montrez que vous avez accès à Internet en utilisant l'outil curl.

a) Quelle configuration statique avez-vous utilisé? Vous pouvez présenter la configuration que vous avez utilisez dans le fichier /etc/network/interfaces **(2 points)**
b) Quelle commande NAT permet à tous les utilisateurs du réseau « DMZ» d'aller vers internet? **(2 points)**

Q8) Quelle(s) commande(s) permet(tent) à Kali Linux d'accéder à Internet?

a) Quelle configuration statique avez-vous utilisé? Vous pouvez présenter la configuration que vous avez utilisez dans le fichier /etc/network/interfaces **(2 points)**
b) Quelle commande NAT permet à tous les utilisateurs du réseau « OUTSIDE » d'aller vers internet? **(2 points)**
c) Quelle commande permet d'activer la communication entre deux hôtes d'une même interface afin qu'ils puissent communiquer entre eux? **(2 points)**

Dans le Pare-feu ASA exécutez la commande « *show running-config* , et récupérez la configuration de l'ASA en ajoutant des captures d'écrans à votre rapport.

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