TD 2 – Protection

1 ère partie : Antivirus

Avast, Norton, AVG AntiVirus FREE, Kapersky , MacAfee, Comodo, Zone Alarm, ...
Mais aussi Windows Defender (depuis Windows 8) plus anciennement Microsoft Security Essentials (jusqu'à Windows 7) sont des anti-virus disponibles.

Exercice 1

Regardez le paramétrage de l'antivirus sur votre machine. S'il n'y en a pas , il est recommandé d'en télécharger un et s'il n'est pas activé il est recommandé de l'activer.

Lancer votre anti-virus et identifier tous les logiciels malveillants sur la machine (en principe il ne devrait pas y en avoir). S'il y en a, faites le nécessaire pour les éliminer.

Opération facultative et dangereuse : désactiver votre AntiVirus , aller surfer sur le web et télécharger quelles petites applications. Réactivez votre antivirus et lancer l'analyse. Est-ce que tout va bien ?

Exercice 2

Un grand débat a toujours lieu, lorsqu'on parle d'antivirus : gratuit ou payant ?
Regardez les offres commerciales des antivirus évoqués plus haut : Avast, Norton, AVG AntiVirus FREE, Kapersky , MacAfee, Comodo, Zone Alarm, ...
Faites un comparatif entre ces offres. A votre avis, qui est le meilleur ?
Les versions payantes sont-elles meilleures que les gratuites ? Pourquoi ?

2 ème partie : Pare feu

Exercice 1

1 - Qu'est ce qu'un pare-feu ?
2 - Quel est le principe de fonctionnement d'un pare-feu ?
3 - Le tableau ci-dessous donne des exemples de règles pour un pare-feu :

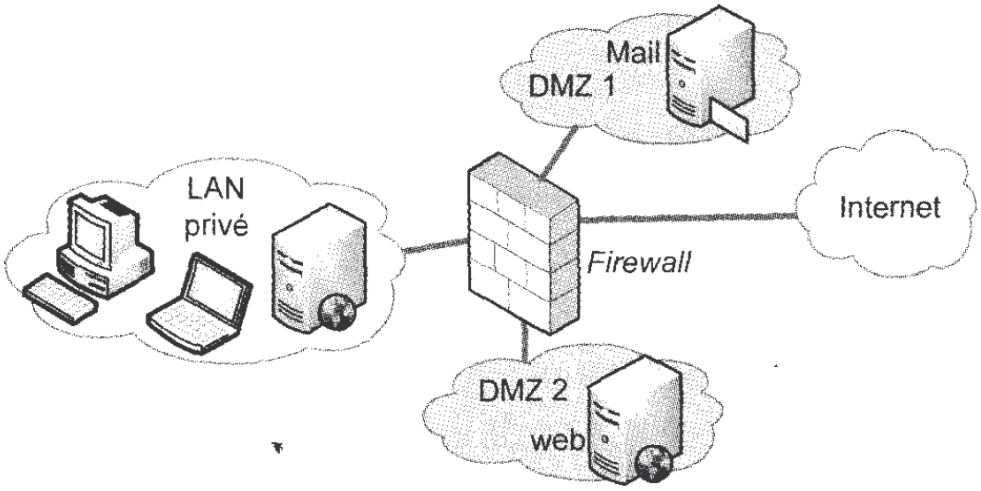
Règle	IP source	IP dest	Protocol	Port source	Port dest	Action
1	192.168.10.20	194.193.192.1	Tcp	tous	25	Autorisé
2	Tous	192.168.10.3	Tcp	tous	80	Autorisé
3	192.168.10.0/24	any	Tcp	tous	80	Autorisé
4	Tous	tous	tous	tous	tous	Interdit

A - Expliquez le rôle de chaque colonne.
B - Précisez la protection mise en place.

4 - Quelles sont les limites d'un pare-feu ?

Exercice 2

Ci-dessous, la règle A du firewall permet aux machines du LAN privé d'accéder à DMZ 2 alors que la règle C devait l'interdire. Comment remédier à cela ?



Règle	@ src	@ dest.	Protocole	Port source	Port dest.	Action
A	Toutes	DMZ 2	TCP	Tous	80	Autorisé
B	LAN	DMZ 1	TCP	Tous	25	Autorisé
C	LAN	Toutes	TCP	Tous	Tous	Refusé
E	Tous	Tous	Tous	Tous	Tous	Refusé

Exercice 3 : Protection contre les intrusions sous linux : pare-feu (iptables)

La commande iptables est un outil efficace pour protéger votre machine contre les attaques depuis ou vers le Web. Il s'agit en fait d'un pare-feu intégré dans la système Linux.

Comme pour tous les pare-feu, le principe est de contrôler (en bloquant ou en autorisant) le trafic réseau.
Le contrôle peut se faire à plusieurs niveaux :

- global de la machine
- des protocoles
- des adresses ip
- des ports
- ...

Selon le cas plusieurs syntaxes sont utilisées :

1 - Pour autoriser ou bloquer tout le trafic
iptables -P INPUT|OUTPUT DROP|ACCEPT

2 - Pour autoriser ou bloquer un protocole particulier
ip tables iptables -A INPUT|OUTPUT -p udp|tcp -j DROP|ACCEPT

3 - Pour autoriser ou bloquer une adresse particulière
ip tables iptables -A INPUT -p udp|tcp -s @ip -j DROP|ACCEPT
ip tables iptables -A OUTPUT -p udp|tcp -d @ip -j DROP|ACCEPT

4 - Pour voir l'état de la protection ou réinitialiser les protections
iptables -L // Etat de la protection
iptables -X // Suppression de toutes les protections
iptables -F

ATTENTION : la commande iptables doit s'exécuter en mode administrateur.

Travail à faire :

1 - Executer les commandes ci-dessous
ping www.google.fr
sudo iptables -P INPUT DROP
ping www.google.fr
sudo iptables -P INPUT ACCEPT
ping www.google.fr
sudo iptables -P OUTPUT DROP
ping www.google.fr
sudo iptables -P OUTPOUT ACCEPT
ping www.google.fr

Qu'observez-vous ? Pouvez-vous expliquer ce qui s'est passé ?

2 - Même question que précédemment avec les séquences de commandes ci-dessous

Séquence 1
sudo iptables -A INPUT -p tcp -j DROP
sudo iptables -A OUTPUT -p tcp -j DROP
ping www.google.fr
sudo iptables -X
sudo iptables -F

Séquence 2
sudo iptables -A OUTPUT -p udp -j DROP
ping www.google.fr
sudo iptables -X
sudo iptables -F
sudo iptables -A INPUT -p udp -j DROP
ping www.google.fr
sudo iptables -X
sudo iptables -F

3 - A vous de jouer !
Avec la commande nslookup récupérer l'adresse IP d'un site que vous connaissez puis modifier la protection de votre machine pour que :

a - Tous les sites sauf le votre soient autorisés
b - Aucun site sauf le votre soient autorisés

Exercice 4 : Pare-feu windows

A - Pare feu Windows

Pour accéder au pare-feu windows aller dans le menu démarrer --> panneau de configuration --> Pare feu Windows

Plusieurs options sont possibles sur le pare-feu :

- Autoriser les programmes à communiquer à travers le pare-feu
- Activer ou désactiver le pare feu
- Paramètres avancées
- Dépanner mon réseau

1 - Autoriser les programmes à communiquer à travers le pare-feu
Quels sont les programmes autorisés sur votre machine ?
Peut-on modifier cette liste ? Comment ?

2 - Activer ou désactiver le pare feu
Quelles sont les options possibles ?
Amusez-vous à modifier les options, type : bloquer toutes les connexions entrantes. Que se passe-t-il ?

3 - Paramètres avancées
Quelles sont les règles de trafic actives ?
Peut-on modifier ces règles ? Comment ?

4 - Dépanner mon réseau
Cette option vous offre la possibilité de tester l'état de plusieurs composants de votre machine et réseau.
Quels types de tests sont prévus ? Essayez toutes les options ...

B - Installation d'un pare feu

Le pare-feu intégré à Windows – tout comme celui de votre box internet – est souvent insuffisant car il ne permet pas de bloquer automatiquement les connexions sortantes. Il est donc indispensable d'installer un pare-feu personnel.
Il existe plusieurs pare-feu gratuits : Comodo , ZoneAlarm , Windows Firewall Control, ...

Sur le site : https://www.zonealarm.com/fr/software/free-firewall/, vous pouvez télécharger zone alarm, en principe, sans risque. Procédez à son installation et à sa configuration. Puis tester les fonctionnalités.