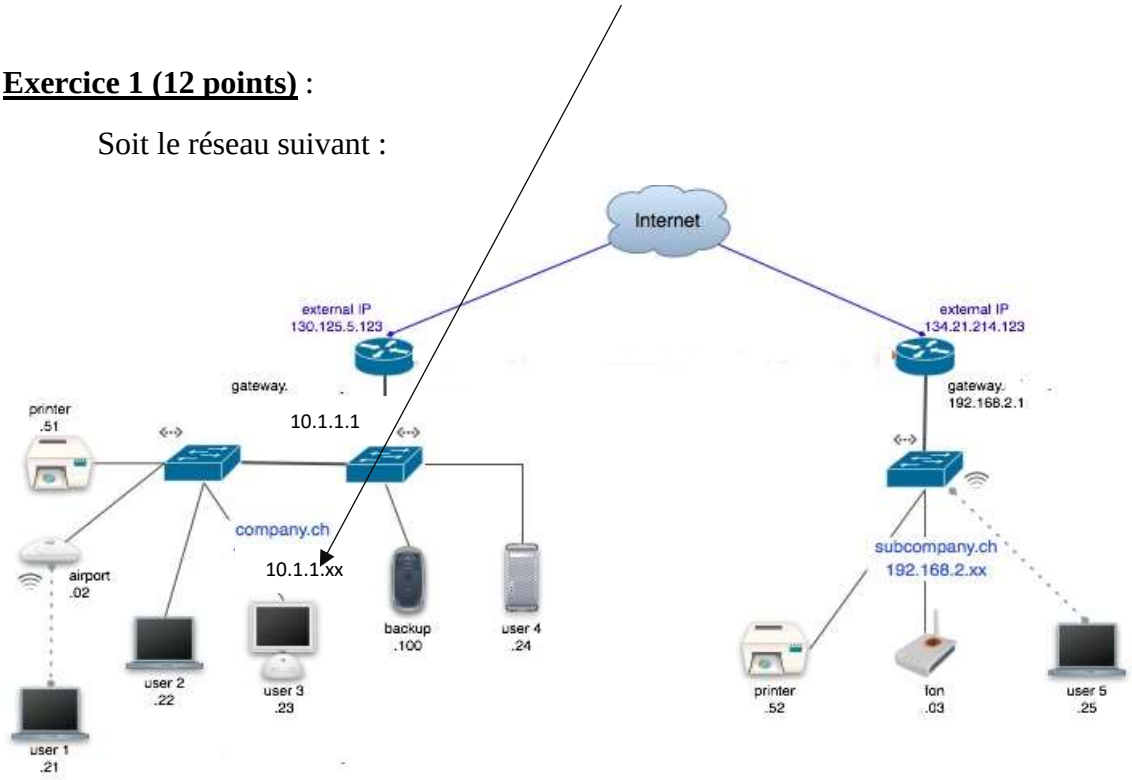
Faculté des Sciences, Département d'Informatique
ETLD du Module : Sécurité des SI,
2017/2018, Durée 1h15 Min
MA. RIAHLA

Sujet 2

Exercice 1 (12 points) :

Soit le réseau suivant :



1. Le point d'accès wifi 'airport' est branché directement au switch du réseau local, quel est le danger ?
   Le réseau wifi est dans le même réseau local que le réseau câblé de l'entreprise, donc un pirate avec sa tablette ou smartphone peut s'introduire au réseau de l'entreprise via wifi (1 point)
   Proposez une solution.
   Mettre un routeur (avec firewall c'est mieux) entre le switch et le point d'accès wifi. (1 point)

2. On souhaite connecter (en sécurisé) les deux réseaux du schéma, quelles sont les différentes solutions possibles ?
   SSH et VPN (1 point)
   Quel sont les protocoles réseaux qui interviennent dans chaque solution ?
   SSH, VPN (AH, ESP, IPCOMP, IKE) (0.5)
   Expliquez leur fonctionnement.
   Principe de fonctionnement : cryptographie hybride=symétrique + asymétrique (0.5)

3. Quel est l'intérêt pour un pirate de savoir que le port 25 de la machine user 1 est ouvert ?
   Port 25 ouvert donc l'existence d'un serveur mail -> le pirate peut envoyer des mails au serveur contenant des pièces jointe infectée, ou envoyer des spam (1.5 points)
   D'autres réponses logiques sont correctes

Quelle est son étape suivante ?
Installer des cheveux de Troie, porte dérobées, spam…etc (0.5)
D'autres réponses logiques sont correctes

4. Proposez une table NAT pour la passerelle 10.1.1.1 sachant que les machines user1, user 2, user 3 et user 4 sont respectivement un serveur Mail, un serveur HTTP, un serveur FTP et un deuxième serveur WEB. **(2 points)**

Table de translation NAT							
Interne				Externe			
source	port	dest	port	source	port	dest	port
10.1.1.21	25 (ou mail)	Peu import	Peu import	130.125.5.123	25 (ou mail)	Peu import	Peu import
10.1.1.22	80 (ou http)	Peu import	Peu import	130.125.5.123	80 (ou http)	Peu import	Peu import
10.1.1.23	21 (ou ftp)	Peu import	Peu import	130.125.5.123	21 (ou ftp)	Peu import	Peu import
10.1.1.24	80 (ou http)	Peu import	Peu import	?	80 (ou http)	Peu import	Peu import

5. L'administrateur réseau souhaite mettre en place un firewall au niveau de la passerelle 10.1.1.1, Quels sont les types de filtrage qu'il peut utiliser ? expliquez un exemple d'attaque évité par chaque type. **(2 points)**
Filtrage par : IP source ou destination : bloquer les adresses IP des pirates.
Filtrage par : Protocoles (TCP, UDP, ICMP,etc) : interdire smurf ICMP par exemple
Filtres Applicatifs (proxy HTTP, FTP, SMTP,…etc) : Dos, DDos, CSS/XSS, virus sur des fichiers..etc

6. Proposez une table de filtrage pour le réseau 10.0.0.0 au niveau de la passerelle 10.1.1.1. **(2 points)**

IP source	IP destination	Port source	Port destination	Paquet SYN	Action
any	10.1.1.21 ou pub	any	25 (ou mail)	Ok	Permis
any	10.1.1.22 ou pub	any	80 (ou http)	Ok	Permis
any	10.1.1.23 ou pub	any	21 (ou ftp)	Ok	Permis
any	10.1.1.24	any	80 (ou http)	Ok	Permis
any	any	any	any	any	Interdit (deny)

Exercice 2 (8 points) :

1. Quel type d'attaque peut révéler un fichier log d'un Firewall ? expliquez
(Deux réponses suffisent)
Dos ou ddos: explication (1 point)
Smurf (1 point)
Ip spoofing
D'autres réponses logiques sont correctes

2. Donnez un exemple d'une attaque DNS spoofing locale. **(2 points)**

Mettre dans le fichier hosts local d'une machine ou un serveur DNS local la correspondance : IP Victime->site pirate

D'autres réponses logiques sont correctes

3. Expliquez l'impact de l'ingénierie sociale sur la sécurité des systèmes d'information des entreprises. **(2 points)**

   Un pirate peut se faire des amis avec les employés de l'entreprise ou les bluffer (savoir parler) pour récupérer des informations confidentielles de l'entreprise.

D'autres réponses logiques sont correctes

4. Quelles sont les techniques de détection utilisées par les antivirus ?

Signature, Analyse du code ou intelligence artificielle (statique et dynamique) et contrôle d'intégrité (1 point)

Expliquez comment utiliser les trois méthodes conjointement. **(1 point)**

Pour les virus détectés par l'analyse du code, il n'est pas nécessaire de les mette dans les signatures.

Pour les virus de démarrage ou furtif par exemple : contrôle d'intégrité.

Utiliser les signatures justes quand c'est nécessaire pour ne pas encombrer la base de données des signatures.

D'autres réponses logiques sont correctes