IUT1, Département Réseaux & Télécommunications
Licence professionnelle RIMS 2016/2017

Sécurité des infrastructures (M33)

N.B. : Tous documents autorisés
Soin, propreté et clarté seront appréciés par le correcteur.
Barême ***indicatif :*** *1 : 5 pts - 2 : 5 pts - 3 : 6 pts - 4 : 4 pts*

NOM :

PRENOM :

Ex 1 : Analyse de risque

Dans le domaine de l'analyse de risques, avec une vision « réseaux et systèmes d'information », il est possible d'envisager la sécurité en quatre grands domaines :
- Sécurité physique
- Sécurité de l'exploitation
- Sécurité logique
- Sécurité applicative

Pouvez-vous en quelques mots expliquer ce que recouvrent ces quatre domaines de la sécurité et en quoi ces quatre grands domaines impactent la partie « réseaux et systèmes d'information » ?

Ex 2 : Système de détection d'intrusion (IDS) et logiciels utilisables lors des audits de sécurité

2.1 Quelles sont les différences entre un IDS réseau (Network-IDS) et un IDS hôte (Host-IDS) ? Expliquez l'intérêt de ces deux mécanismes ?

2.2 Lors d'un audit de sécurité, des logiciels spécifiques peuvent être utilisés pour faire des analyses, pouvez-vous citer deux ou trois logiciels de ce type et à quoi servent-ils ?

2.1

2.2

Ex 3 : <u>Attaques</u>

Vous êtes l'administrateur système et réseau d'une entreprise et avez en charge la sécurité informatique. A votre arrivée, le réseau se compose d'un serveur de messagerie (IMAP et SMTP) et d'un serveur hébergeant le site web de la société avec notamment son organisation. Ces deux serveurs utilisent le système d'exploitation Linux Centos et sont placés dans une DMZ. Le réseau comporte les postes clients (~10 sous Microsoft Windows) ainsi qu'un serveur Active Directory qui sert également de serveur de fichiers et DHCP. Un autocom IP est également présent pour les postes téléphoniques IP de la société.

1) Pour chaque ressource informatique (serveur, autocom, poste client) précisez quelles vulnérabilités pourraient être exploitées ?
2) Pour chaque serveur (serveur, autocom, poste client) précisez à quelles menaces ils sont potentiellement exposés ?
3) Pour chaque serveur (serveur, autocom, poste client) précisez à quelles attaques ils pourraient être confrontés.

Ex 4 : Virus

Vous trouverez ci-dessous deux définitions de programmes malveillants pour lesquels vous devrez déterminer les caractéristiques en les reportant dans le tableau présent au bas de l'exercice. Dans les deux cas il conviendra d'expliquer vos choix.

Nom	Bombe logique	Cheval de Troie	Virus d'exécutable	Virus de document	Virus de démarrage	Virus comportementaux	Vers simples	Macro vers
Cryptolocker								
Mydoom.A								

Cryptolocker : se propage par email et via un botnet préexistant. Quand il est activé, il chiffre plusieurs fichiers présents sur la machine via un chiffrement à clef publique et privée. La clé permettant de déverrouiller l'ensemble est alors uniquement stockée sur les serveurs hébergeant le malware. Le programme affiche alors un message disant que pour décrypter les informations, il faudra envoyer un paiement. La somme demandée est valable jusqu'à une certaine date puis augmente si le paiement n'a pas été fait en temps et en heure. Le système de chiffrement vise certaines extensions de fichiers en particulier, notamment celles des fichiers Microsoft Office, Open Document, AutoCAD, mais aussi les images. Il s'attaque aux disques durs, aux disques partagés sur les réseaux, aux clés USB, et parfois aux fichiers synchronisés dans le cloud.

Mydoom.A : se propage par les courriels ou le service P2P de Kazaa. Il affecte le système d'exploitation Microsoft Windows. Une fois l'ordinateur infecté, il s'envoie automatiquement à tout le carnet d'adresses sous de fausses identités, avec des objets aléatoires (Hi, Test, Mailer Daemon failure, etc.) et installe une *backdoor* dans le dossier système. Ce programme ne scrute pas uniquement le carnet d'adresses, mais il effectue également un *scan* du disque dur à la recherche d'adresses de courriel. Il va également inventer des adresses vers un domaine (<adresse bidon>@mondomaine.com) et multiplier ainsi les infections lorsque l'on redirige par défaut toutes les <adresses bidon>@mondomaine.com vers une adresse unique.