Partie 1 : QCM

1) Citer les trois notions de base de la sécurité des systèmes d'information
   a. Authentification, Autorisation, Intégrité
   b. Confidentialité, Intégrité, Disponibilité
   c. Confidentialité, Intégrité, Authentification
   d. Disponibilité, traçabilité,

2) Une DMZ est :
   a. Une salle spécialisée pour les serveurs critiques
   b. Un système de détection des intrusions
   c. Un réseau séparé du LAN dans lequel on met les serveurs publics
   d. Une technique d'accélération présente dans la plupart des firewalls modernes

3) Une attaque de type déni de service consiste à
   a. Refuser l'accès d'un client à un serveur en se faisant passer pour ce dernier
   b. Empêcher aux utilisateurs légitimes l'accès à un système
   c. Utiliser une erreur de programmation dans un système donné pour le compromettre
   d. Casser la clef de chiffrement des réseaux WIFI

4) Laquelle ne fait pas partie des recommandations de base pour la conception d'architectures firewalls :
   a. Interdire par défaut, autoriser au cas par cas
   b. Ouvrir seulement depuis l'interne vers l'externe
   c. Mettre en place une DMZ
   d. Avoir systématiquement une imprimante connectée au firewall

5) Une PKI permet de résoudre
   a. Le problème de distribution des mots de passe
   b. Le problème de distribution des clefs publiques
   c. Le problème de gestion des firewalls
   d. Le problème de la gestion des mots de passe sur un réseau

6) La biométrie est un dispositif :
   a. D'authentification
   b. D'autorisation
   c. De confidentialité
   d. D'intégrité

7) Un certificat cryptographique est essentiellement
   a. Un fichier contenant les mots de passe d'accès à un système, sous forme chiffrée
   b. Un trousseau contenant les clefs des contacts d'une personne
   c. Une clef publique et les informations associées à son propriétaire
   d. Une carte à puce contenant un processeur dédié à la cryptographie

8) Quel est le vecteur d'infections virales le plus fréquent
   a. Les disquettes
   b. Les messages e-mail
   c. Les sites web pirates
   d. Les clefs USB

9) L'avantage majeur des proxys applicatifs est
   a. Leur rapidité
   b. La possibilité d'utiliser SOCKS
   c. La possibilité d'analyser le flux applicatif
   d. Ils n'ont aucun avantage notable

10) Une des mesures prises par Microsoft pour sécuriser leur récent système d'exploitation Windows 2003 a été de le livrer sans activer par défaut les services Web, email, FTP, ... Pourquoi ?
   a. Afin de ne pas saturer la mémoire des serveurs avec des applications inutiles
   b. Ces services ne chiffrent pas les données et sont donc interceptables, ce qui pose problème aux utilisateurs de ces systèmes
   c. Afin de pouvoir facturer l'activation des différents services
   d. Car sinon, beaucoup d'utilisateurs les laisseraient ouverts, offrant autant de portes d'entrées potentielles sur leurs machines

11) MD5 et SHA sont
   a. Des algorithmes de cryptographie symétrique
   b. Des fonctions de hashage
   c. Des algorithmes de cryptographie asymétrique
   d. Des PKI usuelles

12) Le rôle de la sécurité en entreprise est de
   a. Réduire les risques à un niveau acceptable
   b. Prévenir tout risque
   c. Empêcher les utilisateurs de travailler librement
   d. Surveiller le bon fonctionnement des systèmes

13) Un switch offre pour un réseau un degré de sécurité supérieur à celui offert par un hub
   a. Vrai, il limite la possibilité de scanner
   b. Vrai, il limite la possibilité de « sniffer » (intercepter)
   c. Vrai, il limite la possibilité d'effectuer des dénis de services
   d. Faux

14) Quelle méthode pourrait être utilisée pour assurer la confidentialité de connexions entre un poste client et un serveur au travers d'Internet
   a. IPSEC en mode tunnel
   b. IPSEC en mode transport
   c. L2TP
   d. HTTPS

15) Une solution très économique pour permettre aux commerciaux de consulter leur boîte email lors de déplacements serait de
   a. Mettre en place une solution d'accès distant au travers des infrastructures d'un opérateur télécom par L2TP
   b. Mettre en place des modems sur chaque continent
   c. Mettre en place un accès par modem au réseau interne
   d. Mettre en place un Webmail consultable depuis Internet

16) L'application des patchs de sécurité permet de déjouer
   a. L'utilisation par les pirates de programmes d'attaques (« exploits ») sur nos machines
   b. Le scan des ports de nos machines
   c. Les virus véhiculés par disquettes
   d. L'incompétence des utilisateurs

17) La législation sur la criminalité informatique en France est
   a. Existante et éprouvée
   b. Existante mais jamais vraiment mise en application
   c. Présentant des lacunes la rendant peu favorable
   d. Inexistante

18) Les raisons qui justifient de mettre en place de la sécurité dans une organisation sont principalement :

a. La protection du patrimoine de l'entreprise
b. Certaines contraintes légales
c. La protection des données nominatives (CNIL)
d. Toutes les raisons précédentes

19) L2TP permet

a. De rendre plus économiques les appels modems
b. De constituer des VPN
c. De faire du tunnel de protocole niveau 2 au travers de réseaux IP
d. D'appliquer automatiquement les patchs sur tous les postes de l'entreprise

20) L'une des vulnérabilités principales sur les systèmes d'information d'entreprises

a. L'inexpérience et le risque lié aux utilisateurs
b. La présence de ports USB sur la plupart des machines
c. L'utilisation des mots de passe au lieu de méthodes plus sûres
d. Les connexions à Internet