Faculté des Nouvelles Technologies de l'Information et de la Communication
Département d'Informatique et Technologie de l'Information

1iére Master Informatique industrielle
Examen du module Sécurité informatique

Nom : Prénoms :

1. **Veuillez indiquer à quel protocole appartient chaque mécanisme ou sous protocole**

Record protocol	Alarm protocol
Security Association	Internet Key Exchange
Key Distribution Center	Ticket Granting System
Hanshake protocol	Change Cipher Spec protocol
Authentification Header	Encapsulating Security Payload
Authentication Server	Security Association Database
Internet Security Association Key Management Protocol	

2. **Veuillez citer les trois types standards d'utilisation des VPN (Réseaux privés virtuels) :**

   a) ……
   b) ……
   c) ……

3. **Veuillez répondre aux questions suivantes :**

- Quel mécanisme permet de partager une adresse IP routable entre plusieurs machines.

  ……
- Quel mécanisme permet d'associer une adresse IP publique à une IP privée interne au réseau.

  ……
- Quel mécanisme fait fonction d'intermédiaire entre les ordinateurs d'un réseau local et Internet.

  ……
- Quelle technique crée une zone isolée hébergeant des applications mises à disposition du public.

  ……

4. Veuillez indiquer si ces affirmations sont correctes ou fausses (Remplir le tableau):

1. Dans un cryptosystème symétrique les clés existent par paires (bi-clés)
2. L'intranet VPN permet aux entreprises de communiquer avec ses clients et ses partenaires.
3. Le VPN d'accès est utilisé pour relier au moins deux intranets entre eux
4. L'intranet VPN est utilisé pour permettre à des utilisateurs itinérants d'accéder au réseau privé.
5. Les Network-based intrusion prevention system permettent de surveiller les postes de travail
6. Les host-based IPS détectent les tentatives d'intrusion au niveau du noyau
7. Le filtrage dynamique permet de filtrer les communications application par application.
8. Le filtrage applicatif opère au niveau 4 du modèle OSI.
9. Le filtrage simple de paquets est basé sur l'inspection des couches 3 et 4 du modèle OSI.
10. La méthode de scanning consiste à analyser le comportement des applications
11. L'attaque ARP consiste à intercepter des paquets de données et à les rejouer
12. L'attaque par downgrade exploite le mécanisme de poignée de mains du protocole TCP.
13. La substitution homophonique utilise une suite de chiffres monoalphabétique périodiquement
14. La substitution polygrammes remplace chaque lettre du message par une lettre de l'alphabet
15. Dans une attaque sur texte chiffré choisi, le cryptanalyste choisir différents textes à déchiffrer
16. Le hachage permet de vérifier que l'empreinte correspond bien au message reçu
17. Un firewall effectuant un filtrage applicatif est appelé généralement un proxy
18. Les Intrusion Detection System écoutant le trafic réseau de manière furtive
19. L'extranet VPN permet à l'entreprise d'ouvrir son réseau local à ces partenaires
20. Les Network-based intrusion prevention system permettent de surveiller le trafic réseau

1		**5**		**9**		**13**		**17**	
2		**6**		**10**		**14**		**18**	
3		**7**		**11**		**15**		**19**	
4		**8**		**12**		**16**		**20**	

Bon courage