Republique Algerienne Democratique et Populaire
Ministere de l'Enseignement Superieur et de la Recherche Scientifique
Etablissement : ENP d'Oran
Département : Génie des Systèmes

Module : Sécurité des systèmes d'information 2018 /2019 **Durée** : 1h45

Examen Final

Partie 01 : (10 Points)

1. Quel type de virus utilisé pour accéder aux postes de travail sur internet ?
2. A quels niveaux du modèle OSI travaillent un firewall stateless ?
3. Quel est le but d'un DNS spoofing ?
4. Comment construire la signature digitale ?
5. Classer les actions suivantes en attaque, faille, vulnérabilité et menace

   a. Bugs logiciel
   b. Divulgation des mots de passe
   c. Mot de passe stocké en clair dans la BDD
   d. Erreurs humaines vulnérabilité

6. Que signifie « Machine du pirate en tant que **hijacker** ». intermédiaire.
7. **ACL**, à quoi cela sert-il ?
8. Expliquer l'attaque par inondation de ping : **ICMP**
9. Expliquer la différence entre le chiffrement par flux et chiffrement par bloc avec des exemples.
10. Quels sont les inconvénients de la cryptographie asymétrique ?
11. Quel objectif de la sécurité qui a été compromis dans les cas suivants :

    - Un employeur modifie son salaire dans le PC de comptable
    - Bob modifie les valeurs d'un attribut dans une base de données Intégrité
    - Un virus supprime les fichiers dans un flash disque et les remplace par des raccourcis

Virus Ransomware

12. Etablir les règles correspondantes à la politique de sécurité suivante :

    - Autoriser l'accès à un service (DNS, MAIL, HTTP, FTP) a partir de votre machine.
    - Interdire à l'hôte d'initier un dialogue avec l'extérieur.

13. Que signifie les règles suivantes :

    - Iptables -A INPUT -i lo –j ACCEPT
    - Iptables -A FORWARD -i eth0 -s 20.0.2.0/24 –p UDP - -dport 23 – m state - - state ESTABLISHED –j ACCEPT

Partie 02: (10 Points)

Exercice 1 :

1. Chiffrer le message suivant avec la méthode de vigéner,
   - Le Texte : « Le type de telle attaque est de paralyser un service ou un réseau ».
   - la clé employée est « ALSVRSSTBL ».
- Crypter le résultat obtenu par la méthode de « **Substitution monoalphabétique** » , utilisant la substitution suivante :

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
L	O	A	X	Z	N	M	F	W	Q	P	C	B	V	H	T	D	E	U	R	G	Y	I	S	K	J

2. Soient le cryptogramme suivant :
   « ULDTNLEEFEDRIQEFRUUAEIXCWPIEAENS »
   - Quelles sont les clés (ligne, colonne) possibles pour déchiffrer ce message ?
   - Quelle est la clé qui convient à déchiffrer ce message ?

39

Exercice 2 :

Bob utilise le protocole RSA et publie sa clé publique N=187 et e=3

3. Encoder le message m= 15 avec la clé publique de Bob
4. En utilisant $\Phi(n) = 160$, retrouver la factorisation de N, puis la clé privée de Bob.
5. Supposons q'Alice et Bob possèdent le même nombre N utilisé dans le RSA supposons que leurs exposants respectifs e_A et e_B sont premiers entre eux Charles désire envoyer le message m à Alice et à Bob ; donc il le chiffre et obtient c_A et c_B . montrez q'Eve peut trouver m si elle arrive à intercepter c_A et c_B

F.Kabli

Bon courage