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 2019-2020 **Durée : 1h**

Examen Final

Partie 01 :

1. Quel objectif de la sécurité compromis dans les cas suivants :
   - Un employeur modifie son salaire dans le PC de comptable
   - Mohamed modifie les valeurs d'un attribut dans une base de données
   - Un virus supprime les fichiers dans un flash disque et les remplace par des raccourcis
2. Classer les actions suivantes en : attaque, faille, vulnérabilité, menace
   a. Bugs logiciel
   b. Mot de passe stocké en clair dans la BDD
   c. Erreurs humaines Vulnérabilité
   d. Divulgation des mots de passe
3. Quels sont les avantages de la cryptographie à clé secrète partagée ? clé cypte + message cypté sécurité Rapide
4. Que signifie les règles suivantes :
   - Iptables -A OUTPUT -i lo –j ACCEPT
   - Iptables -A FORWARD -i eth1 -s 20.0.2.0/24 –p UDP - -dport 23 – m state - - state ESTABLISHED –j DROP
5. Etablir les règles suivantes :
   - La politique par défaut est de n'autoriser aucun trafic entrant et sortant à la machine 30.0.0.5
   - Considérer juste les connexions entrantes suivantes :
     a. Connexion SSH (HTTP : 88) depuis les machines du réseau interne
     b. Connexion TELNET (TCP : 23) depuis locales.

Partie 02:

Exercice 1 : Considérez le système de chiffrement RSA avec p=43 et q=7 :

1. Calculer n et son indicateur d'Euclide Φ(n).
2. Calculer l'exposant d associé à e= 11 et coder le message m=15.
1. Bob utilise le protocole RSA et publie sa clé publique, N=187 et e=3, En utilisant Φ(n) = 160, retrouver la factorisation de N, puis la clé privée de Bob.

Exercice 2 : Utiliser le chiffrement de Vigenére pour Chiffrer le texte suivant, avec le mot-clé « SYSTEM » :

LE COVID AFFECTE LES INDIVIDUS DE DIFFERENTES MANIERES

F.Kabli
Bon courage