Université de khenchela

Faculté des sciences et Technologies L3 ISIL

Sécurité informatique

TD 1 : Introduction à la sécurité informatique

1 Exercice

Q1. La confidentialité permet :

A) La non-modification de l'information

B) De rendre l'information inintelligible à d'autres personnes

C) Seulement aux acteurs de la transaction d'accéder aux données

D) de s'assurer de l'identité d'un utilisateur,

Q2. Un type d'attaque visant à rendre indisponible pendant un temps indéterminé les services ou ressources d'une organisation est :

A) DoS

B) Spoofing IP

C) Déni de service

D) Phishing

Q3. Attaque par rejeu :

A) consiste à intercepter des paquets de données et à les rejouer

B) exige la connaissance des algorithmes de décryptage adéquat

C) se base sur l'exploitation d'un dictionnaire

D) exploite un dispositif permettant d'écouter le trafic d'un réseau

Q4. Pour l'attaque « man in the middle » :

A) Le pirate falsifie les échanges afin de se faire passer pour l'une des parties.

B) Elle consiste à intercepter des paquets de données et à les rejouer.

C) Elle intervient dans le cryptage asymétrique.

D) Un type d'attaque visant à rendre indisponible le système pendant un temps indéterminé.

E) Elle intervient dans le cryptage symétrique.

Q5. Le dispositif « Sniffer » :

A) Permet d'écouter le trafic d'un réseau.

B) Est uniquement un type d'attaque.

C) Il peut également servir à une personne malveillante de collecter des informations.

D) Consiste à la réception d'un e-mail semblant provenir d'une entreprise de confiance.

E) Est à la fois un moyen de protection et un type d'attaque.

Q6.Selon le mode de la manipulation, il peut être un outil d'attaque ou de protection :

A) Analyseur de trafic

B) Spam

C) Hoax

D) Sniffer

E) Worm

2 Exercice

Dans le tableau ci-dessous, nous avons plusieurs scénarios d'incidents.

A) Identifier le service de sécurité violé.

B) Proposer un mécanisme de défense.

N	Sénario	Service ciblé	Méthode de défense
1	Alice envoie un mail électronique au nom de Bob à Eve.	?	?
2	Bob se connecte à un serveur sur lequel il n'a pas le droit d'accès.	?	?
3	Alice envoie un grand nombre de ping à l'ordinateur d'un collègue.	?	?
4	Alice se met entre le point d ?accès sans fil et l ?ordinateur portable de Bob. Toutes les trames envoyées par Bob sont reçues et retransmises par l ?ordinateur portable d ?Alice.	?	?
5	Bob modifie le montant d'une facture électronique d'Eve de 2230 DA à 90000 DA.	?	?
6	Un attaquant a réussi à consulter un fichier transitant sur le réseau. Il arrive à voir son contenu mais il n'arrive pas à le décrypter.	?	?
7	La base de données d'aire Algérie a été attaquée et toutes les places disponibles sur le vol Londres ont été réservées au nom de "L3 ISIL".	?	?
8	Un pirate utilise une adresse IP volée pour convaincre un système qu'il est un client fiable et connu.	?	?
9	Un attaquant a réussi à consulter un fichier transitant sur le réseau. Il arrive à voir son contenu et arrive à le décrypter et le lire.	?	?
10	Un utilisateur supprime accidentellement un fichier et pour ne pas être sanctionné il arrive à cacher cet acte.	?	?
11	Un pirate bombarde un serveur de BD par des requêtes sans arrêt.	?	?
12	Un pirate réussi à utiliser la carte bancaire d'un individu et se fait payer un IPhone sur le site d'Apple.	?	?
13	Les pirates injectent du contenu dans une page qui corrompt le navigateur de la cible. Il peut ainsi modifier la page web selon ses envies.	?	?

3 Exercice

Classer les événements suivants en vulnérabilités et menaces, puis les menaces en accidentelles et intentionnelles, enfin les menaces intentionnelles en passives et actives :

Défaut de conception dans l'architecture réseau	Panne de disque (disk failure)
Faibles mots de passe	Sabotage
Interception d'émissions	Coupure d'électricité (power loss)
Réseau ouvert (sans authentification)	Effacement de la mémoire
Panne du matériel (hardware failure)	Corruptions des données (data curruption)
Envoi d'un script malveillant attaché à une page web	Absence de contrôle d'accès
Défaillance du logiciel (software crash)	Données inexactes (inaccurate data)
Action malveillante intérieure (malicious inside action)	Prise de contrôle d'un site web
Erreur d'opérateur (operator error)	Accès non autorisé (unauthorized access)
Absence de sauvegarde (backup)	Écoute réseau
Logiciel malveillant (malware)"	Communications défaillantes ou corrompues
Espionnage	Inondation de messages
Ports non standards ouverts	Réseau wifi mal configuré
Incendie, explosion, inondation, séisme (fire, explosion, flood, earthquake)	Absence de redondance (des serveurs,des systèmes de communications, ...)

4 Exercice

Le risque en sécurité informatique peut être exprimé par la formule suivante :

$$Risque = \frac{(Menace \times Vulnerabilite)}{(Contre\_mesures)}$$

- Donner une définition de chacun de ces concepts à savoir :
  1. Risque,
  2. Menace,
  3. Vulnérabilité, et
  4. Contre mesures.

5 Exercice

A) Identifiez les objectifs fondamentaux en sécurité informatique. Puis, expliquez la différence entre eux.

B) Donnez deux classifications standard (vu au cours) pour les attaques. Expliquer chaque classe en donnant des exemples.