TD 1 – Initiation à la Sécurité Informatique

Exercice 1 :

1. Quels sont les différents types de sécurité étudiés au cours ?
2. Identifiez les exigences fondamentales en sécurité informatique. Puis, expliquez la différence entre eux.
3. Présentez les mécanismes de sécurité définis dans X.800.
4. Aujourd'hui, les chercheurs en sécurité informatique s'intéressent davantage au "Privacy" ? Est-ce que peut-on la classifier comme une exigence de sécurité ?
5. Quels sont les services offerts par le contrôle d'accès ?

Exercice 2 :

1. On a vu au cours que l'authentification est un moyen pour vérifier ou pour prouver l'identité d'un utilisateur. Cependant, l'utilisateur doit il présenter quelles informations pour prouver son identité ?
2. Quel est la différence entre authentification, authentification à deux facteurs, et authentification à trois facteurs ? Donnez des exemples.
3. Présentez le schéma "*Authentification vs. Autorisation*" vu au cours.
4. Quels sont les différents types d'intégrité.
5. Dessinez une matrice semblable au tableau 1.3 (vu au chapitre 1) qui montre la relation entre les services de sécurité et les attaques.
6. Dessinez une matrice semblable au tableau 1.3 (vu au chapitre 1) qui montre la relation entre les mécanismes de sécurité et les attaques.

TD 2 – Les attaques Informatique

Exercice 1 :

1. Classifiez les attaquants par compétence, puis par objectif.
2. Donnez deux classifications standard (vu au cours) pour les attaques. Cependant, vous pouvez proposer une nouvelle classification et cela n'est possible qu'à après l'étude de tous les attaques.
3. Nous avons vu au cours les attaques réseaux (les plus fréquentes) publié par McAfee Labs en 2016. Donnez quatre attaques les plus fréquentes.
4. Basé sur l'application du map développée par kaspersky (https://cybermap.kaspersky.com/), on a pu voir au cours les attaques en temps réel. Comment sont-elles détectées en temps réel ?
5. Donnez quatre scénarios pour lancer une attaque physique.
6. Donnez trois scénarios pour lancer une attaque en réseau.
7. Donnez un scénario pour lancer une attaque DoS en réseau.

Exercice 2 :

1. Quelle est la différence entre les menaces de sécurité passives et actives?
2. Listez et définissez brièvement les catégories d'attaques de sécurité passives et actives.
3. En classe, nous avons fait la distinction entre une attaque de porte d'entrée et une attaque de porte arrière (front-door attack and a back-door attack). Expliquez comment ils sont différents et donnent un exemple de chacun.
4. Donnez des exemples de ce que le malware tente d'accomplir.
5. Décrivez les façons dont les pirates blancs (white-hat hackers) tentent de rendre les systèmes informatiques plus sûrs.
6. Accédez au site Symmantec Security Response à l'adresse suivante:
   Http://securityresponse.symantec.com/
   Voir la liste des dernières menaces de virus. Quels sont les noms des cinq premiers?

TD 3– Malware

Exercice 1 :

1. Les attaques nouvelles sur Internet et qu'elles n'ont pas encore été classées, sont appelées «attaques de jour zéro, zero-day attacks». Faire des recherches sur Internet sur les attaques de jour zéro. Qu'as-tu appris?
2. Quelle est la différence entre un virus et un ver ?
3. Dans quelle mesure les vers sont-ils plus dangereux que les virus ?
4. Certains vers qui se propagent sur Internet ne provoquent aucun dommage sur les machines atteintes. Pourquoi sont-ils cependant nuisibles ?
5. Pour désinfecter un ordinateur, il est recommandé de le redémarrer depuis un CD-ROM ou une clef USB; pourquoi ?

Exercice 2 :

1. Qu'est-ce qu'une porte dérobée (backdoor) ?
2. Comment un attaquant peut-il procéder pour en installer une ?
3. Qu'est-ce qu'un cheval de Troie ?
4. Comment un attaquant peut-il procéder pour en installer un ?

Exercice 3 :

Il arrive régulièrement que des codes malveillants réussissent à persister sur une machine sans être détectés par les antivirus installés par la victime de l'infection. Décrire deux techniques différentes qui permettent à un code malveillant de ne pas être détecté par les logiciels antivirus.

Exercice 4 :

Quelle(s) technique(s) utilise un antivirus pour détecter les programmes malveillants ?

TD 4 : Le chiffrement RSA

1 Codage et décodage RSA.

On considère la clef publique RSA (11, 319), c'est-à-dire pour $n = 319$ et $e = 11$.
Note : on pourra utiliser les résultats suivants :

- $319 = 11 \times 29$; $10^{11} = 263 \pmod{319}$; $263^2 = 216 \times 319 + 265$;
- $133^3 = 12 \pmod{319}$; $133^{25} = 133 \pmod{319}$;
- $11^2 = 121 \pmod{280}$; $11^4 = 81 \pmod{280}$; $11^8 = 121 \pmod{280}$; $11^{16} = 81 \pmod{280}$;
- $95 = 64 + 31$; $81.11 = 51 \pmod{280}$; $81.121 = 1 \pmod{280}$.

1. Quel est le message correspondant au codage avec cette clé du message $M = 100$?
2. Calculer d la clé privée correspondant à la clé publique e.
3. Décoder le message $M' = 133$.
4. Le message codé 625 peut-il résulter d'un codage avec la clé publique ? Même question avec la clé privée.

2 Cryptographie RSA et authentification

Un professeur envoie ses notes au secrétariat de l'École par mail. La clef publique du professeur est (3,55); celle du secrétariat est (3,33).

1. Vérifier que la clef privée du professeur (supposée connue de lui seul) est 27; et que celle du secrétariat est 7.

2. Pour assurer la confidentialité de ses messages, le professeur chiffre les notes avec la clef RSA du secrétariat. Quel message chiffré correspond à la note 12 ?

3. Pour assurer l'authenticité des messages contenant les notes, le professeur signe ses messages pour le secrétariat aprés les avoir chiffrés. Le secrétariat reçoit le message 23. Quelle est la note correspondante ?

TD 5. L'analyse des protocoles de sécurité

Pour chaque description ci-dessous, indiquez le terme (<4 mots) qui la décrit le mieux.

Question 1. Cela garantit que les données ne peuvent être lues que par le récepteur prévu.

Question 2. Cela garantit que toute modification des données est détectée par le récepteur prévu.

Question 3. Cela garantit que les données reçues ont été envoyées par l'expéditeur spécifié.

Question 4. Cela garantit qu'un tiers peut vérifier que les données ont été envoyées par l'expéditeur spécifié.

Question 5. Ce type de crypto utilise différentes clés pour le cryptage et le décryptage.

Question 6. The attack model in which the attacker has access to an encryption oracle but not a decryption oracle.

Question 7. Ce chiffrement par blocs symétriques prend en charge une seule taille de clé.

Question 8. Ce chiffrement par blocs symétriques prend en charge plusieurs tailles de clé.

Question 9. Propriété d'une fonction de hachage qui rend difficile la recherche d'un message m haché sur un nombre donné.

Question 10. C'est l'ensemble des entiers en 1; ...; n - 1 qui sont relativement premiers à n.

Question 11. C'est le nombre d'entiers dans 1; ...; n - 1 qui sont relativement premiers à n.

Question 12. Une attaque qui passe par un ensemble de mots de passe candidats.

Question 13. Cela signifie qu'après qu'une clé de session a été oubliée par les principaux qui l'ont utilisée, personne ne peut déchiffrer les données chiffrées avec cette clé.

Question 14. Alice a un compte sur un serveur. Le serveur lui fait changer son mot de passe tous les quelques mois, auquel Alice incrémente simplement un nombre dans son mot de passe, par exemple, pwd1, pwd2,. Pourquoi le serveur ne se plaint-il pas que le nouveau mot de passe ressemble beaucoup à son ancien?

Question 15. Soit $[e;\ n]$ être la clé publique RSA d'un serveur. Supposons que quelqu'un vous donne les facteurs premiers de n, disons p et q. Pouvez-vous obtenir la clé privée $[d;\ n]$? Sinon, expliquez brièvement. Si oui, indiquez brièvement les étapes.

Question 16. Une fonction de hachage H () génère un hachage de 256 bits. Combien de messages aléatoires en moyenne faudrait-il hacher avant de trouver deux messages distincts hachés à la même valeur.

Question 17. Un mot de passe fort est nettement meilleur qu'un mot de passe faible contre une attaque par dictionnaire en ligne. Expliquer brièvement

Question 18. Un mot de passe fort est nettement meilleur qu'un mot de passe faible contre une attaque par dictionnaire hors ligne. Expliquer brièvement.

Question 19. Protocoles d'authentification

$[sk_A; pk_A]$ Alice's public-key pair. Bob has pk_A.
$[sk_B; pk_B]$ Bob's public-key pair. Alice has pk_B.
$E_P(pk; x)$ public-key encryption of x with public key pk
Sgn(sk; x) public-key signing of x with secret key sk
E(s; x) symmetric-key encryption of x in CBC mode using AES with key s
D(s; x) symmetric-key deryption of x in CBC mode using AES with key s
MAC(s; x) symmetric-key MAC (ECBC) of x using key s
H(x) SHA-256 hash function of x
HMAC(k; x) HMAC of x using key k and H

Alice	Bob
A: generate a new symmetric key s send $[E_P(pk_B; s); E(s;m);Sgn(sk_A;H(m))]$	
	B: receive message extract m

- Analysez la confidentialité, l'intégrité, l'authenticité et la non-répudiation.