

SupNum RSS320: Introduction à la Sécurité Informatique

Examen de la session principale

Durée 1h30

Sidi BIHA

02/2025

Exercice 1 (12 points)

1. Expliquez pourquoi la sécurité informatique constitue un compromis entre plusieurs facteurs. Quels sont ces facteurs ?
2. Définissez ce qu'est l'ingénierie sociale et donnez un exemple concret de techniques utilisées par les attaquants.
3. Comparez un virus, un ver et un cheval de Troie en précisant leurs modes de propagation et leurs objectifs principaux.
4. Expliquez la différence entre un NIDS et HIDS.
5. Qu'est-ce qu'un pare-feu (firewall) et quelle est sa principale fonction dans la sécurisation d'un réseau ?
6. Quels sont les différents types de pare-feu ?
7. Quel est le rôle d'une DMZ dans l'architecture réseau d'une entreprise.
8. Différenciez le chiffrement symétrique du chiffrement asymétrique.
9. Quel est le rôle d'un certificat numérique dans la sécurisation des communications sur Internet ?
10. Qu'est-ce qu'une attaque de type man-in-the-middle ?
11. Quels sont les avantages et les inconvénients du chiffrement symétrique en termes de performance et de sécurité par rapport au chiffrement asymétrique ?
12. Comment les fonctions de hachage assurent-elles l'intégrité des données ?

Exercice 2 (8 points)

1. Quelle option de nmap a généré le résultat suivant ?

```
Nmap scan report for presidency.mr (82.151.65.210)
Host is up, received syn-ack ttl 57 (0.0077s latency).
Scanned at 2025-02-10 22:02:11 UTC for 39s
```

PORT	STATE	SERVICE	REASON	VERSION
21/tcp	filtered	ftp	no-response	
22/tcp	filtered	ssh	no-response	
80/tcp	open	http	syn-ack ttl 58	Apache httpd
443/tcp	open	ssl/http	syn-ack ttl 57	Apache httpd

```
Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 40.20 seconds
Raw packets sent: 10 (416B) | Rcvd: 3 (132B)
```

2. Quelle option de nmap a généré le résultat suivant ?

```
Starting Nmap 7.91 ( https://nmap.org ) at 2025-02-10 10:00 UTC
Initiating Ping Scan at 10:00
Scanning 4 hosts [2 ports/host]
Completed Ping Scan at 10:00, 0.65s elapsed (8 hosts)
Nmap scan report for 192.168.100.10
Host is up, received echo-reply ttl 64 (0.035s latency).
Nmap scan report for 192.168.100.11 [host down, received no-response]
Nmap scan report for 192.168.100.112
Host is up, received echo-reply ttl 64 (0.034s latency).
Nmap scan report for 192.168.100.113 [host down, received no-response]
Nmap done: 4 IP addresses (2 hosts up) scanned in 0.90 seconds
```

3. Donnez deux exemples d'outils utiles pour l'énumération des noms de domaines.
4. Pour chacun des outils suivants, décrivez brièvement sa fonction principale ainsi qu'un exemple d'utilisation :

- (a) hydra
- (b) john
- (c) cmseek
- (d) sqlmap