Année universitaire : 2023-2024

Centre Universitaire Abdalhafid Boussouf-Mila
Institut de Mathématiques et Informatique
3ème Année informatique
Module : Sécurité informatique

Corrigé interrogation

Exercice 1 :

1. Défaut de conception dans l'architecture réseau	2. Panne de disque (disk failure)
3. Faibles mots de passe	4. Sabotage
5. Interception d'émissions	6. Réseau ouvert (sans authentification)
7. Effacement de la mémoire	8. Corruptions des données (data curruption)
9. Panne du matériel (hardware failure)	10. Envoi d'un script malveillant attaché à une page web
11. Absence de contrôle d'accès	12. Défaillance du logiciel
13. Données inexactes	14. Action malveillante intérieure
15. Prise de contrôle d'un site web	16. Erreur d'opérateur
17. Accès non autorisé	18. Absence de sauvegarde (backup)
19. Écoute réseau	20. Logiciel malveillant (malware)
21. Communications défaillantes ou corrompues	22. Inondation de messages
23. Ports non standards ouverts	24. Réseau wifi mal configuré
25. Incendie, explosion, inondation, séisme	26. Absence de redondance (des serveurs, des systèmes de communications, ...)
27. Coupure d'électricité	28. Espionnage

1. Vulnérabilité :

(1) Défaut de conception dans l'architecture réseau (3)Faible mots de passe, (6)Réseau ouvert (sans authentification) (11)Absence de contrôle d'accès , (13)Données inexactes (18)Absence de sauvegarde (backup), (23)Ports non standards ouverts, (24)Réseau wifi mal configuré (26)Absence de redondance,

2. Menaces

(a) Accidentelles : (2)Panne de disque, (8) Corruptions des données (data curruption) (9)Panne du matériel, (12)Défaillance du logiciel, (16)Erreur d'opérateur, (21) Communications défaillantes ou corrompues (25) Incendie, explosion, inondation, séisme, (27)Coupure d'électricité.

(b) Intentionnelles :

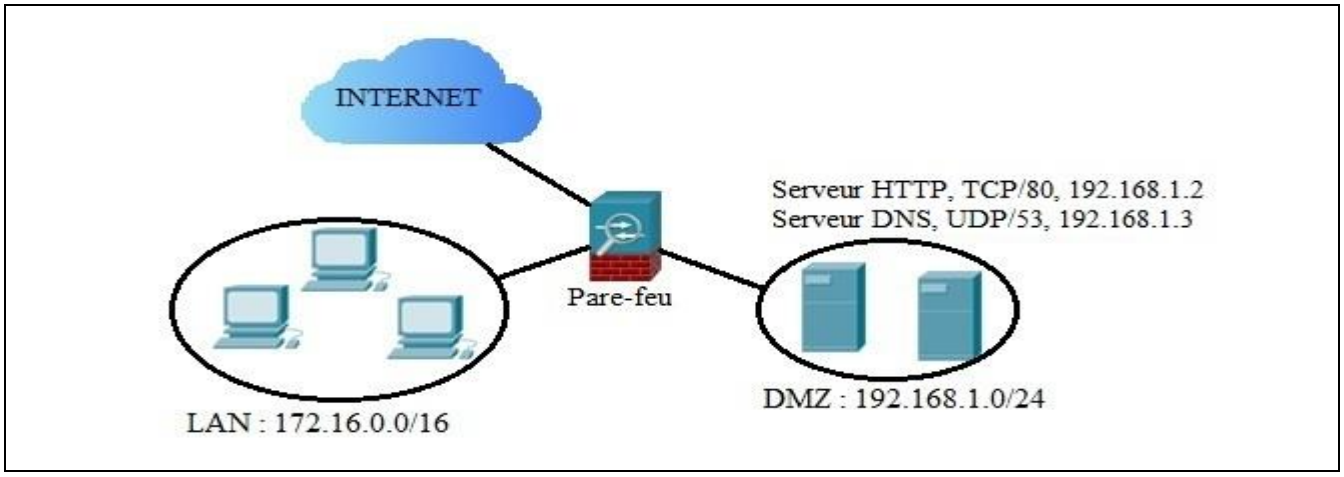
i. Passive : (5)Interception d'émission, (10)Envoi d'un script malveillant attaché à une page web, (17) Accès non autorisé(19)Écoute réseau, (22)Inondation de messages, (28)Espionnage,

ii. Active : (4)Sabotage, (7)Effacement de la mémoire (14)Action malveillante intérieure, (15)Prise de contrôle d'un site web, (20)Logiciel malveillant (malware)

Exercice 3 :

Une entreprise dispose d'un pare-feu pour limiter l'accès depuis et vers les machines de son réseau interne. L'architecture du réseau de l'entreprise comprend également une zone démilitarisée (DMZ) pour le déploiement des serveurs Web et DNS propres à l'entreprise.

- Le réseau de l'entreprise est représenté par le schéma ci-dessus.
- La politique de sécurité appliquée par le pare-feu est décrite par le tableau ci-dessus.



- La politique de sécurité appliquée par le pare-feu est décrite par le tableau suivant :

N°	IP Source	IP Dest.	Protocole	Port Source	Port Dest.	Action
1	172.16.0.0	192.168.1.2	TCP	>1024	80	Accepter
2	192.168.1.2	172.16.0.0	TCP	80	>1024	Accepter
3	172.16.0.0	192.168.1.3	UDP	>1024	53	Accepter
4	192.168.1.3	172.16.0.0	UDP	53	>1024	Accepter
5	*	192.168.1.2	TCP	>1024	80	Accepter
6	192.168.1.2	*	TCP	80	>1024	Accepter
7	172.16.0.0	*	TCP	>1024	53	Accepter
8	*	172.16.0.0	TCP	53	>1024	Accepter
9	*	*	*	*	*	Refuser

1. Donner la politique correspondante à chaque paire de règles (1-2), (3-4), (5-6) et (7-8).

Règle	Politique
(1-2)	Permettre aux utilisateurs du réseau local d'accéder au serveur HTTP local
(3-4)	Permettre aux utilisateurs du réseau local d'accéder au serveur DNS local
(5-6)	Permettre aux utilisateurs externes d'accéder au serveur HTTP local
(7-8)	Permettre aux utilisateurs du réseau local d'accéder au serveur DNS sur internet

2. Préciser la règle qui vérifiera chacun des paquets suivants et dites si le paquet sera accepté ou refusé :

- **p1-** IP src. : 172.16.0.30 IP Dest. : 12.230.24.45 Protocole : TCP Port src. :1045Portdest. : 443
- **p2-** IP src. : 172.16.10.5 IP Dest : 192.168.1.3Protocole: UDP Port src. :6810 Port dest. : 53
- **p3-** IP src. : 140.10.2.1 IP Dest : 192.168.1.2Protocole: TCP Port src. :8000 Port dest. : 80
- **p4-** IP src. : 17.14.3.3 IP Dest : 192.168.1.3Protocole: UDP Port sce:6000 Port dest. : 53
- **p5-** IP src. : 192.168.1.2 IP Dest : 1.2.3.4 Protocole: TCP Port sce:80Port dest. : 9999

paquet	**N° de la règle à appliquer**	**action**
P1	9	refusé
P2	3	accepté
P3	5	accepté
P4	9	refusé
P5	6	accepté