Université de Tlemcen Année Universitaire 2020-2021 Faculté des Sciences Département Informatique	Module Sécurité Informatique L3

TD3 Contre-mesures

Exercice 1

Donnez pour chaque service de sécurité l'attaque (les attaques) qui lui correspond et les contre-mesures permettant de lui réaliser

Service de sécurité	***Attaques***	***Contre-mesure***
- Authentification	- Usurpation d'identité	- Systèmes d'authentification, Login/mot de passe, certificat électronique, filtrage - Ajout du code d'authentification de message (MAC) - Chiffrement (contrôle d'accès) - Contrôle d'accès, IDS/IPS - Signature électronique
- Intégrité	- Modification	
- Confidentialité	- Accès (interception)	
- Disponibilité	- Déni de service	
- Non répudiation	- Répudiation	

Exercice 2

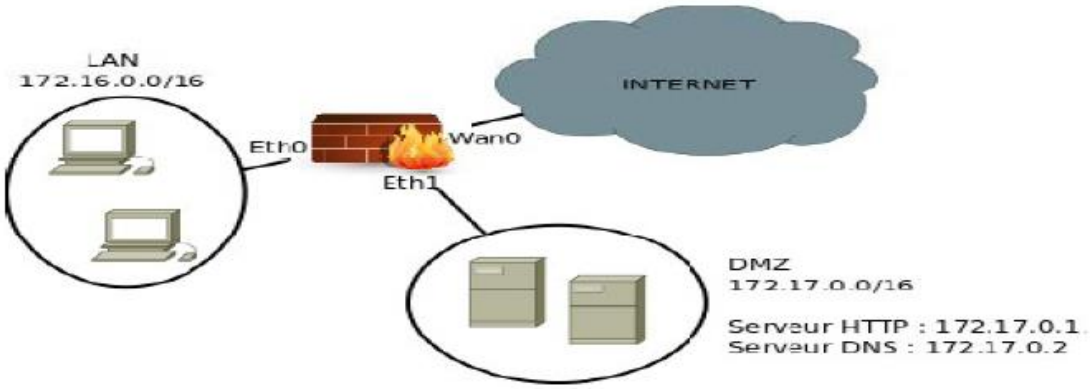
Qu'est-ce qu'un pare-feu ? Quels sont ses rôles et fonctions ?
- Entité matérielle ou logicielle qui permet de filtrer les entrées indésirables
- Protéger les environnements informatiques en les masquant, séparant, créant un périmètre de sécurité

Un pare-feu est un outil de sécurité nécessaire mais pas suffisant, pourquoi ?
- Il ne peut réaliser à lui seul l'ensemble des fonctions de sécurité identifiées dans une politique de sécurité
- Par exemple, il n'assure ni la cryptographie ni la vérification d'intégrité
- Permet de définir des zones dans lesquelles les accès sont contrôlés

Définissez le concept de sécurité périmétrique (zone démilitarisée)
- Périmètre de sécurité dans lequel on isole les serveurs (web) ouverts au public
- Les serveurs privés ne sont pas visibles ou atteignables depuis internet

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. La politique de sécurité appliquée par le pare-feu est décrite par le tableau ci-dessous.



N°	Interface entrée	Interface sortie	Adr IP source	Adr IP destination	Protocole	Port source	Port dest	Action
1	Eth0	Eth1	172.16.0.0	172.17.0.1	TCP	> 1024	80	Accepter
2	Eth1	Eth0	172.17.0.1	172.16.0.0	TCP	80	> 1024	Accepter
3	Eth0	Eth1	172.16.0.0	172.17.0.2	UDP	> 1024	53	Accepter
4	Eth1	Eth0	172.17.0. 2	172.16.0.0	UDP	53	> 1024	Accepter
5	Wan0	Eth1	*	172.17.0.1	TCP	> 1024	80	Accepter
6	Eth1	Wan0	172.17.0.1	*	TCP	80	> 1024	Accepter
7	Eth0	Wan0	172.16.0.0	*	TCP	> 1024	80	Accepter
8	Wan0	Eth0	*	172.16.0.0	TCP	80	> 1024	Accepter
9	*	*	*	*	*	*	*	Refuser

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

(1-2) autoriser le flux TCP entre le réseau LAN et la zone DMZ
(3-4) autoriser le flux UDP entre le réseau LAN et la zone DMZ
(5-6) autoriser le flux TCP entre le réseau WAN et la zone DMZ
(7-8) autoriser le flux TCP entre le réseau LAN et le réseau WAN

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

p1-	IP sce : 172.16.0.30	IP Dest : 12.230.24.45	Prot : TCP	Port sce :1045	Port dest : 443
p2-	IP sce : 172.16.10.5	IP Dest : 172.17.0.2	Prot : UDP	Port sce :6810	Port dest : 53
p3-	IP sce : 140.10.2.1	IP Dest : 172.17.0.1	Prot : TCP	Port sce :8000	Port dest : 80
p4-	IP sce : 17.14.3.3	IP Dest : 172.17.0.2	Prot : UDP	Port sce :6000	Port dest : 53
p5-	IP sce : 172.17.0.1	IP Dest : 1.2.3.4	Prot : TCP	Port sce :80	Port dest : 9999