Examen de réseaux

19 décembre 2013

Documents et calculatrices non autorisés
Durée de l'épreuve : 2h

Les exercices qui suivent sont indépendants et peuvent être traités dans le désordre.

Exercice 1 (2 points)**.** Représenter côte à côte les couches des modèles OSI et TCP/IP. Y placer les protocoles suivants et préciser leur rôle : DNS, Ethernet, HTTP, ICMP, IMAP, IP, RIP, SMTP, TCP, UDP.

Exercice 2 (4 points)**.** Pour chacun des réseaux suivants, indiquer le masque de sous-réseau, l'adresse de broadcast, le nombre d'adresses disponibles et préciser la première et la dernière adresse de la plage d'adresses :

1. `194.167.0.0/16`
2. `10.13.37.0/24`
3. `217.194.224.0/20`
4. `192.168.0.0/30`

Exercice 3 (4 points)**.** Rappeler le principe du routage à état de liens. Le routeur A a reçu l'information synthétisée sur la table 1. Reconstruire la topologie du réseau à partir de cette information. À l'aide de l'algorithme de Dijkstra, dessiner des arbres collecteurs pour les routeurs A, B et C. En déduire les tables de routage de chacun de ces trois routeurs.

Exercice 4 (6 points)**.** Un routeur `rt` est relié par une interface réseau à une machine `pc1` et par une seconde interface réseau à une machine `pc2`. Une fois les interfaces et tables de routage configurées, une commande est tapé sur `pc1`. En écoutant sur ses deux interfaces, `rt` a capturé les trames de la table 2. Ces trames sont présentées dans le désordre.

1. Identifier les paires d'adresses (MAC, IP) pour chacune des 4 interfaces réseau.
2. Représenter le réseau sur un schéma en prenant soin de préciser de nommer les interfaces et de donner les adresses MAC et IP correspondantes.
3. Donner les tables de routage de chacune des 3 machines.
4. Retrouver l'ordre d'émission des trames et le sous-réseau sur lequel chacune circule.
5. En supposant que les sous-réseaux sont de type `/24`, retrouver les commandes tapées sur chacune des 3 machines, configuration comprise.

Exercice 5 (4 points)**.** Après avoir rappelé le principe du protocole du *bit alterné*, dessiner le chronogramme des échanges du scénario suivant. L'émetteur A envoie successivement 3 segments au destinataire B. Les segments 1 et 3 sont transmis correctement, le segment 2 est perdu.

Exercice 6 (4 points)**.** Une attaque distribuée par déni de service (DDoS) consiste pour un attaquant à détourner les ressources et protocoles de l'internet pour rendre indisponibles des services réseau mis en œuvre sur un hôte victime. Une telle attaque par réflexion consiste à forger des requêtes à destinations de réflecteurs qui vont amplifier les requêtes afin de saturer la victime et/ou son réseau.

1. L'attaque *smurf* repose sur l'existence de réseaux mal configurés dont les routeurs transmettent les paquets IP *broadcast* et dont les machines répondent aux messages *ping* (ICMP echo request) reçus en *broadcast*. En supposant qu'un attaquant possède l'adresse IP `6.6.6.6`, sa victime l'adresse `8.8.8.8` et que le réseau `101.101.0.0/16` soit mal configuré, préciser le paquet IP forgé par l'attaquant et expliquer le déroulement de l'attaque. Quel est l'intérêt de ce type de réflecteur ?
2. L'attaque par amplification DNS repose sur l'existence de serveurs DNS récursifs ouverts. En supposant qu'un attaquant possède l'adresse IP `6.6.6.6`, sa victime l'adresse `8.8.8.8` et que le serveur DNS `101.101.101.101` soit ouvert, préciser le paquet IP forgé par l'attaquant et expliquer le déroulement de l'attaque. Quel est l'intérêt de ce type de réflecteur ?
3. Un tel type d'attaque par réflexion peut-il utiliser facilement le protocole TCP ?

— A : (B, 7), (D, 7), (E, 1) ;

— B : (A, 7), (C, 9), (D, 8), (E, 1) ;

— C : (B, 9), (D, 10) ;

— D : (A, 7), (B, 8), (C, 10), (E, 6) ;

— E : (A, 1), (B, 1), (D, 6) ;

TABLE 1 – Scénario algorithme LS

#	MAC source	MAC destination	IP source	IP destination	Prot.	Résumé du contenu
a	2a:0f:37:30:8b:18	6e:5f:98:37:0c:07			ARP	10.13.37.1 is at 2a:0f:37:30:8b:18
b	2a:0f:37:30:8b:18	6e:5f:98:37:0c:07			ARP	Who has 10.13.37.10? Tell 10.13.37.1
c	2a:0f:37:30:8b:18	6e:5f:98:37:0c:07	192.168.54.54	10.13.37.10	ICMP	Echo (ping) reply id=0x0202, seq=1/256, ttl=63
d	2e:18:cc:d4:8c:e7	8a:83:e9:a1:10:85			ARP	192.168.54.54 is at 2e:18:cc:d4:8c:e7
e	2e:18:cc:d4:8c:e7	8a:83:e9:a1:10:85			ARP	Who has 192.168.54.1? Tell 192.168.54.54
f	2e:18:cc:d4:8c:e7	8a:83:e9:a1:10:85	192.168.54.54	10.13.37.10	ICMP	Echo (ping) reply id=0x0202, seq=1/256, ttl=64
g	6e:5f:98:37:0c:07	2a:0f:37:30:8b:18			ARP	10.13.37.10 is at 6e:5f:98:37:0c:07
h	6e:5f:98:37:0c:07	ff:ff:ff:ff:ff:ff			ARP	Who has 10.13.37.1? Tell 10.13.37.10
i	6e:5f:98:37:0c:07	2a:0f:37:30:8b:18	10.13.37.10	192.168.54.54	ICMP	Echo (ping) request id=0x0202, seq=1/256, ttl=64
j	8a:83:e9:a1:10:85	2e:18:cc:d4:8c:e7			ARP	192.168.54.1 is at 8a:83:e9:a1:10:85
k	8a:83:e9:a1:10:85	ff:ff:ff:ff:ff:ff			ARP	Who has 192.168.54.54? Tell 192.168.54.1
l	8a:83:e9:a1:10:85	2e:18:cc:d4:8c:e7	10.13.37.10	192.168.54.54	ICMP	Echo (ping) request id=0x0202, seq=1/256, ttl=63

TABLE 2 – trames capturées, dans le désordre