M1 ISRE

Janvier 2008

Nom et prénom

Durée 1 heure 30

Exercice 1 TCP et UDP

Dans le répertoire Capture Base, Si ce n'est déjà fait ouvrir le fichier : **USERPASS**.cap

1 TCP/UDP

1.1 TRAMES 37, 38 ET 39.

Q10-1: quel est le processus en cours ? Précisez pour chaque trame : les indicateurs (flag) qui les caractèrisent, les numéros de séquences relatifs actifs, les numéros de séquence en acquittement et l'évolution de ces numéros.

.....

.....

.....

.....

.....

.....

.....

Q5-1 pour chacune des ces trames, vous indiquerez la taille de l'entête, la taille des données TCP, la présence d'options et le nom des options présentes quand il y a en a.

Q3-1 donnez les numéros de séquences initiaux absolus.

1.2 TRAMES 39 ET 40 :

Q5-2 Comparez les numéros de séquences des trames 39 et 40. Expliquez.

1.3 EXAMINEZ LA TRAME 18

Q1-1 Va-t-elle être transmise immédiatement et pourquoi ?

……

Q3-2 Quel est son N° de séquence et sur quoi pointe-t-il ?

……

Q3-3Quel est le N° de séquence Acquitté et sur quoi pointe-t-il ?

……

1.4 Examinez les trames 29, 30 et 31.

Q5-3: pour chacune d'elle, préciser : l'objet de la trame, l'indicateur qui la caractérise, le numéro de séquence actif, le numéro de ack. Expliquez le processus en cours en indiquand le rôle joué par chaque trame.

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

.....

.....

.....

.....

Q5-4 Combien d'octets de données WIN95 a-t-il émis depuis l'ouverture de cette session ? vous devez détailler votre calcul.

.....

.....

.....

.....

1.5 On s'intéresse à la trame 57 du fichier ftp-transfert.cap.

Q5-5 Après l'envoi de cette trame, combien d'octets la machine destinationpeut-elle recevoir avant d'être en débordement de buffer de réception ?

.....
.....
.....
.....
.....
.....
.....
.....

1.6

Q10-2On considère l'échange suivant

No trame	Source	destination	No seq relatif	No ack	flag	taille fenêtre	taille données
1	M1/P1	M2/P2		X	SYN	X	
2	M2P2	M1/P1			SYN/ACK	X	
3	M1/P1	M2/P2			ACK	X	
4	M1/P1	M2/P2	1	1	ack	4096	
5	M2/P2	M1/P1	1		ack	4096	0
6	M1/P1	M2/P2	2001		ack	4096	1000
7	M1/P1	M2/P2		1	ack	4096	1000
8	M1/P1	M2/P2			ack	4096	1000
9	M2/P2	M1/P1		3001	ack	4096	0
10	M1/P1	M2/P2					

- indiquez les valeurs correctes dans les cases vides
- quelle quantité totale de données la machine M1/P1 peut-elle envoyer sans recevoir de ack dans les trames 10 et suivantes ?

Exercice2 Adressage IP

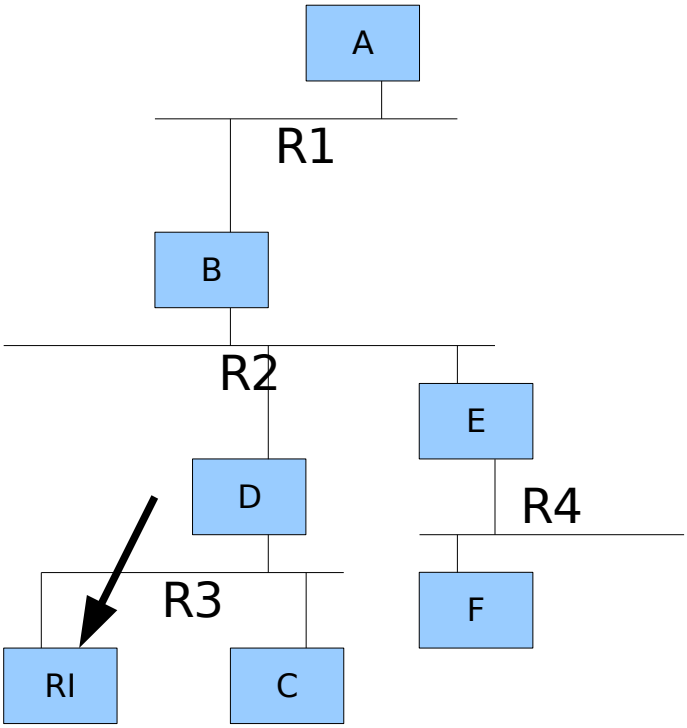
Q10-3 donnez les masques de sous-réseau, les plages d'adresses appartenant à chaque réseau, l'adresse de diffusion pour chacun des réseaux suivants :

- 192.168.10.0/24
- 192.168.0.0/24
- 192.168.23.0/26
- 192.168.23.128/26
- 192.168.192.0/23
- 10.0.0.0/7

Exercice 3 routage

Q10-4 On considère le réseau décrit sur la maquette 3. La machine RI (routeur internet) n'est pas géré par vous. On la supposera correctement configurée. Le routeur par défaut de la machine D vous est imposé: c'est RI.

Votre travail consiste à définir 1) les routeurs par défaut des machines A, B, C, E et F, d'éventuelles routes statiques de façon à ce que tout le monde réussisse à communiquer avec tout le monde et avec internet.



R1: 192.168.10.0/24, R2:192.168.20.0/24, ..., R4:192.168.40.0/24

dernier octet de l'adresse de A: 1, de B: 2, de C: 3, de D: 4, de E: 5, de F 6 et de RI: 249.

Machine A:

- routeur par défaut:
- route statique:
- route statique:
- route statique:
- route statique:
- route statique:

Machine B:

- routeur par défaut:
- route statique:
- route statique:
- route statique:
- route statique:
- route statique:

Machine C:

- routeur par défaut:
- route statique:
- route statique:
- route statique:
- route statique:
- route statique:

Machine D:

- routeur par défaut: 192.168.30.249 (imposé)
- route statique:
- route statique:
- route statique:
- route statique:
- route statique:

Machine E:

- routeur par défaut:
- route statique:
- route statique:
- route statique:
- route statique:
- route statique:

Machine F:

- routeur par défaut:
- route statique:
- route statique:
- route statique:
- route statique:
- route statique:

Exercice 4 WiFi

On travaille avec le fichier « Armada Boot.cap » situé dans le dossier « Airmagnet Captures ».

On s'intéresse à la trame 1 :

- Q3-4Quel est le type de cette trame ?

  .....

- Q3-5 Que vaut le champ timestamp ? A quoi sert-il ?

  .....

- Q3-6Quelle est la sourcedu paquet ? quelle est sa destination ?

  .....

- Q1-2 combien de temps la sépare de la trame suivantes du même type ? Comment aurait-on pu le prévoir ?

  .....

- Q3-7 Est-on en mode ad hoc ou en mode infrastructure ? Expliquez la différence entre les deux modes.

  .....

- Q3-8 donnez les valeurs et expliquez ce que représentent les champs BBSID et ESSID ?

  .....

Probe et association:

- Q10-5 citez les méthodes de découvertes des réseaux par un hôte. vous expliquerez brièvement dans chaque le processus. Vous citerez un exemple de trames du fichier « Armada Boot.cap » correspondant à l'un des cas.

  .....
  .....
  .....
  .....
  .....
  .....
  .....
  .....
  .....
  .....
  .....
  .....
  .....

SIFS, DIFS, PIFS

- Q3-9 à quoi correspondent ces 3 termes ?

Ouvrez le fichier Ann-2.cap. On s'intéresse aux trames 288 et 289:

- Q3-10 décrivez le processus en jeu

.....
.....
.....
.....

- Q1-3que valent les champs Duration de ces trames ?

.....
.....
.....

- Q3-11 Que représentent le contenu de ces champs ?

.....
.....
.....
.....
.....
.....
.....

- Q5-6 Quel impact aura la réception du RTS par une station non concernée par l'échange ?

.....
.....
.....
.....
.....
.....

- Q3-12 indiquez la façon dont se décompose la valeur du champ Duration de la trâme RTS. (on veut la durée des phases incluses dans le temps contenu dans Duration)

.....
.....
.....
.....
.....
.....
.....
.....

- Q3-13 sachant que SIFS = 10µs, dites quelle est la durée d'émission du RTS.

.....
.....
.....
.....
.....
.....
.....
.....