

Durée : 1h30 — Tous documents autorisés

■ ■ ■ Programmation Python avec Scapy — 5 points

1– Une entreprise veut découvrir la présence de tunnel d'évasion utilisant ICMP dans son réseau.

5pts Questions :

- Donnez deux méthodes différentes permettant de détecter la présence d'un tunnel exploitant ICMP ; (1pt)
- Écrire le programme python utilisant la bibliothèque Scapy réalisant la détection de tunnel basé ICMP suivant une des deux méthodes proposées. (4pts)

Pour chaque tunnel détecté, vous afficherez l'adresse IP source avec son adresse MAC et l'adresse IP destination.

■ ■ ■ Analyse de trame — 7 points

2– Analysez les trames suivantes :

7pts

0000	33	33	FF	D9	4E	F8	F0	18	98	E8	88	73	86	DD	60	00	33	..N.....s..`.
0010	00	00	00	20	3A	FF	FE	80	00	00	00	00	00	00	14	E4	...	:.....
0020	09	E2	86	B4	82	8C	FF	02	00	00	00	00	00	00	00	00	00
0030	00	01	FF	D9	4E	F8	87	00	97	F0	00	00	00	00	FE	80	...	N.....
0040	00	00	00	00	00	00	CA	54	4B	FF	FE	D9	4E	F8	01	01	TK...N...
0050	F0	18	98	E8	88	73											s

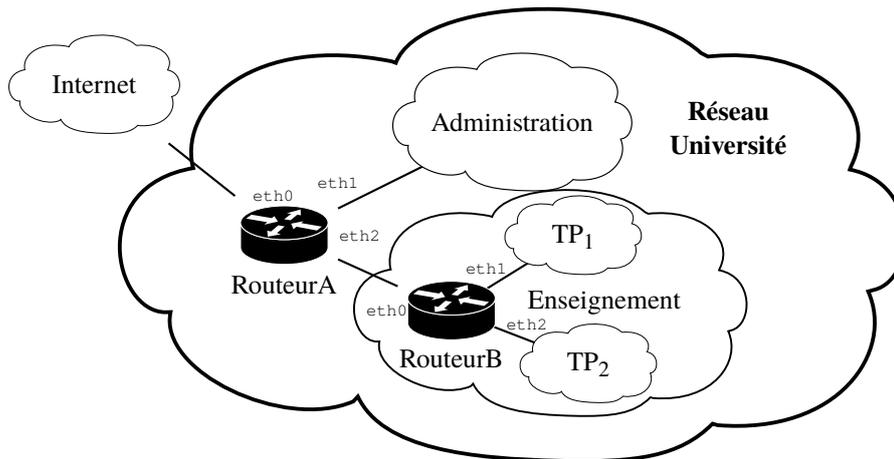
0000	C8	54	4B	D9	4E	F8	F0	18	98	E8	88	73	86	DD	60	05	.	TK.N.....s..`.
0010	06	00	00	10	3A	40	20	01	41	D0	FE	0B	85	00	01	55	@ .A.....U
0020	19	A1	25	E9	A7	0D	26	07	53	00	00	60	00	5C	00	00	..%	...&.S..`.\..
0030	00	00	00	00	00	01	80	00	6D	2E	82	50	00	00	66	40	m..P..f@
0040	5C	78	39	30	5C	78	39	65	5C	78	30	30	5C	78	30	30	\x90\x9e\x00\x00	
0050	52	5C	78	63	38												R\xc8	

- Que contient les trames ? (2pts)
Vous donnerez une description pertinente.
- Sont-elles passées par un routeur ? (1pt)
Est-ce que ce sont des paquets « forgés » ? Pourquoi ?
- Est-ce que les adresses IPv6 ont été obtenues par « auto-configuration » ? (2pts)
Analysez ces adresses et justifiez votre réponse.
- Y-a-t-il un rapport entre les deux trames ? (2pts)
Vous détaillerez et justifierez vos explications.



Planification réseaux — 8 points

- 3-
8pts
- Le service responsable du système d'information d'une université vous demande de lui proposer une configuration en IPv6 de son réseau de formation utilisant des salles de TPs informatiques.



L'université dispose de l'adresse IPv6 suivante : `2003:fac:1234::/48`.

Le responsable du système d'information vous fournit la description suivante :

- * il existe 3 réseaux différents : Administration, TP₁, et TP₂ ;
- * une salle servant à l'infrastructure réseau contenant les routeurs A et B.

Les différents usages des matériels et personnes utilisant ces réseaux :

{Enseignants et Etudiants pour les salles informatiques TP₁ et TP₂, Administratifs pour le réseau Administration, Techniciens pour la salle Infrastructure}.

Questions :

- Le réseau étant équipé de deux routeurs et constitué de deux réseaux principaux, quel découpage allez-vous utiliser pour définir les locations ? (1pt)
Vous discuterez et justifierez votre réponse.
- Décomposez en nombre de bits, l'adresse IPv6 fournie, en tenant compte des « Usages » & « Location » et d'une « écriture simplifiée » pour les adresses IPv6 à utiliser. (1pt)
- Donnez un plan d'adressage en IPv6 pour ce réseau, en favorisant la localisation. (2pts)
Vous donnerez :
 - * pour chaque réseau utilisé l'adresse IPv6 qui lui correspond ;
 - * la table de routage de chaque routeur.
- Comment doit être configuré un poste Enseignant ? un poste Étudiant ? (1pt)
- Le responsable du système d'information vous demande si les VLANs, qu'il a l'habitude d'utiliser, sont compatibles avec l'utilisation IPv6 et s'ils sont toujours intéressants à utiliser. (1pt)
Vous rédigerez une explication.
- On veut mettre en place une protection à l'aide du firewall NetFilter en utilisant la Policy « ACCEPT » par défaut. (2pts)
Donnez les règles du firewall NetFilter en policy ACCEPT, permettant de
 - bloquer les requêtes Web en provenance des différentes « salles informatiques » vers Internet pour les postes étudiants ;
 - bloquer les accès SSH des salles de TPs vers le réseau Administration.*Vous indiquerez sur quel routeur vous placerez vos règles.*