Intitulé de l'épreuve : RESEAUX ET TELECOMMUNICATIONS

Nombre de copies : 3

Numérotez chaque page (dans le cadre en bas de la page) et placez les feuilles dans le bon sens.

EXERCICE 5

① Les sept couches du modèle OSI sont :

couche 7	Application
couche 6	Présentation
couche 5	Session
couche 4	Transport
couche 3	Réseau
couche 2	Liaison
couche 1	Physique

②

IP =	couche 3 (Réseau)
Parité =	couche 1 (Physique)
ADSL =	couche 1 (Physique)
Switch =	couche 2 (Liaison)
RJ45 =	couche 1 (Physique)
Trame =	couche 2 (Liaison)
Masque =	couche 3 (Réseau)
CRC =	couche 7 (Application)

③ Les informations ajoutées par la couche liaison aux données reçues de la couche réseau avant d'être transmises à la couche physique sont les modifications des addresses MAC source et destination, ainsi que l'en-tête de contrôle d'erreur.

[redacted]

④ Le réseau dont l'addresse IP du PC1 est 193.55.42.72 appartient à la classe C.

⑤ L'adresse du modem-routeur est donnée par l'information de passerelle, soit 193.55.42.65

⑥ Il y a 30 hôtes dans ce réseau (PC1 à PC30), cependant il faut inclure le modem-routeur qui est la passerelle de ce réseau; soit au total 31 adresses IP.

⑦ La plus grande valeur attribuable au quatrième octet du masque correspond au masque nécessaire pour servir 31 IPs, soit un masque de /26 (notation cidr) donc 255.255.255.192

⑧ a. adresse de sous-réseau : 193.55.42.64
b. adresse de diffusion : 193.55.42.127
c. adresse IP la plus basse : 193.55.42.65 (attribuable à un hôte)
d. adresse IP la plus haute : 193.55.42.126 (attribuable à un hôte)

N° 2 19

EXERCICE 4

① Les règles définies sur les 3 routeurs indiquent que :
- quelque soit l'origine (adresse IP), des LAN ou d'Internet, le protocole SMTP (Simple Mail Transport Protocol) est autorisé
- et de la même manière quelque soit la destination, le SMTP est autorisé

Cela signifie que l'ensemble des machines des différents réseaux peuvent réceptionner des paquets SMTP sans filtre.
Ainsi, un attaquant peut, de n'importe où, y compris Internet :
- lancer des attaques de type DOS denial of service
- faire du SMTP spoofing (se simuler en tant que relais SMTP pour collecter l'ensemble des emails)
- utiliser toutes les failles connues par ce protocole sur l'ensemble des machines.

② voir report tableau page suivante

num règle	interface arrivée	@IP source	port source	@IP dest	port dest	protocole	nom règle	action
~~4~~	~~193.95.33.3~~	~~193.95.33.65~~				~~UDP/7~~	~~ECHO~~	
2								
3								
4								

N° 3.19

Routeur 1 =

Num règle	interface arrivée	@ IP source	Port src	@ IP dst	Port dst	Protocole	Nom règle	Action
1	193.95.33.3	193.95.33.65			UDP/7	ECHO	ADM65 ECHOOK	Autoriser
2	195.95.38.4	103.95.11.11				ICMP	EXTPING	Autoriser
3					UDP/7	ECHO	NO ECHO	Interdire
4							DEFAULT NO	Interdire

Routeur 2 =

num règle	interface arrivée	@ IP src	Port src	@ IP dst	Port dst	Protocole	nom règle	Action
1	193.95.33.80	193.95.33.65			UDP/7	ECHO	ADM65 ECHOOK	Autoriser
2					TCP/*			Autoriser
3	193.95.33.2	103.95.11.11				ICMP		Autoriser
4					UDP/7	ECHO	NO ECHO	Interdire
5					TCP/21	FTP	NO FTP	Interdire
6							DEFAULT NO	Interdire

Routeur 3 =

num règle	interface arrivée	@ IP src	Port src	@ IP dst	Port dst	Protocole	nom règle	Action
1	193.95.33.1	193.95.33.65			UDP/7	ECHO	ADM65 ECHOOK	Autoriser
2	193.95.33.1	103.95.11.11				ICMP		Autoriser
3					UDP/7	ECHO	NO ECHO	Interdire
4							DEFAULT NO	Interdire

N° 4.1.9

Intitulé de l'épreuve : RESEAUX ET TELECOMMUNICATIONS

Nombre de copies : 3

Numérotez chaque page (dans le cadre en bas de la page) et placez les feuilles dans le bon sens.

EXERCICE 3

(1)

Adresse destination dans la requête ping	
IP Destination	192.168.1.2
MAC Destination	00:00:00:00:00:02

(2)

Adresse destination dans la requête ping	
IP destination	128.178.33.38
MAC destination	00:00:00:00:00:03

En effet, la station 1 ne connaît pas 128.178.33.38, donc l'échange type dans le LAN serait :

192.168.1.1 envoie [ARP who-has? 128.178.33.38] au LAN
192.168.1.3 répond [ARP is-at 00:00:00:00:00:03] à 00:00:00:00:00:01
192.168.1.1 envoie le paquet ping 128.178.33.38

La passerelle disposant sur son interface externe de la possibilité de faire des requêtes vers l'extérieur, alors il indique à la station 1 de passer par lui pour pouvoir router sa requête ping.

N° ... 5 1 5 ...

[redacted]

③ Les différents échanges sont :

- 192.168.1.1 envoie un requête Ping vers "www.site.fr", mais IP non connue
- 192.168.1.1 [DNS who-is? www.site.fr] vers 128.178.33.38 (connu par question précédente)
- 128.178.33.38 [DNS is-at? 195.25.238.132] vers 192.168.1.1
- 192.168.1.1 [ARP who-has? 195.25.238.132] vers tout le LAN
- 192.168.1.3 [ARP is-at ? 00:00:00:00:00:03] vers 00:00:00:00:00:01
- 192.168.1.1 envoie donc la requête ping à 192.25.238.132

Adresse Destination dans le paquet DNS	
IP Destination	128.178.33.38
MAC Destination	00:00:00:00:00:03

Adresse Destination dans le paquet ping	
IP Destination	195.25.238.132
MAC Destination	00:00:00:00:00:03

④ Le protocole ARP est simpliste et ne remet pas en cause la provenance ou la véracité de l'information. Ainsi, la mise à jour de la table ARP nécessite simplement la réception d'un paquet de ce type :

192.168.1.2 [ARP is-at ? 00:00:00:00:00:02] vers la MAC adresse de la station 1

la station 2 peut donc également forger un paquet de ce type :
128.178.33.38 [ARP is-at? 00:00:00:00:00:02] vers station 1.

la station 1 ne remet pas en cause l'information et met à jour sa table ARP :

l'IP 128.178.33.38 se trouve à 00:00:00:00:00:02

qui pourtant correspond à la MAC Adresse de la station 2.

Ainsi, l'IP du serveur DNS n'est plus à l'adresse MAC du routeur

N° 6.1.3

(5) Adresse destination dans le paquet ping

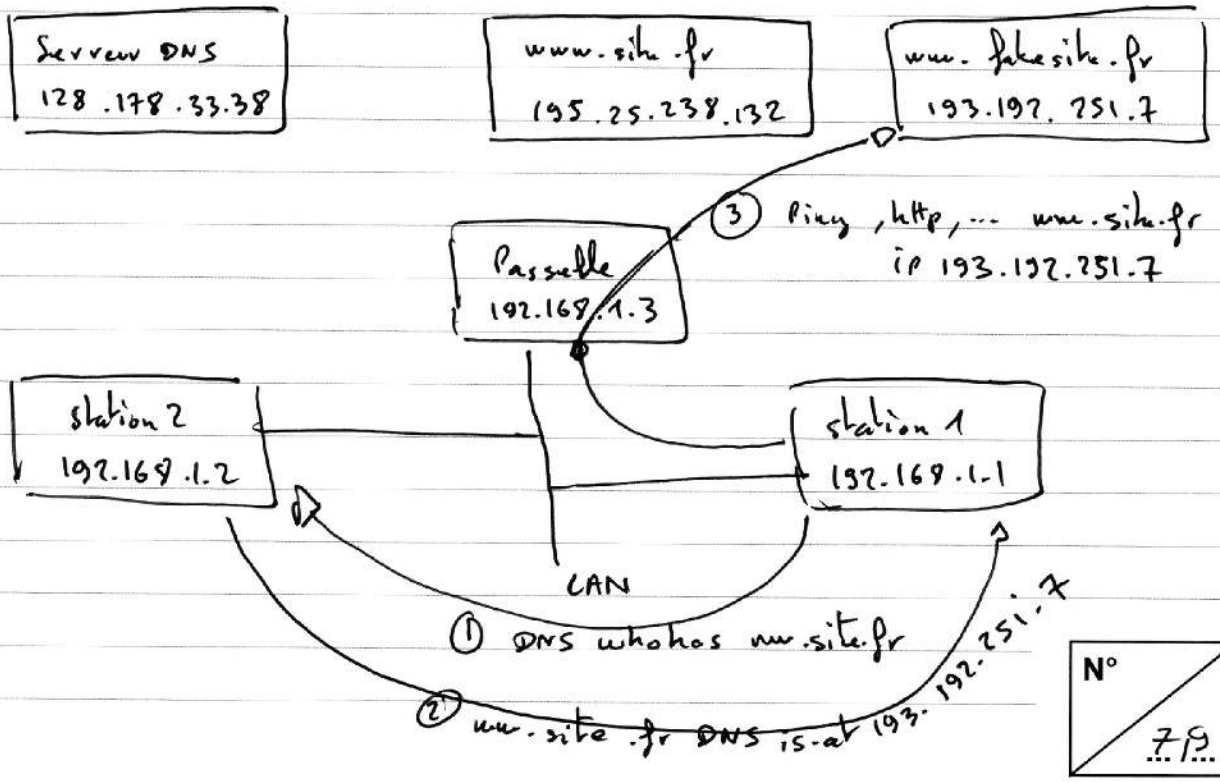
	sans attaque	avec attaque
IP destination	128.178.33.38	128.178.33.38
MAC destination	00:00:00:00:00:03	00:00:00:00:00:02

(6) Dès lors que la station 2 a usurpé le rôle de la passerelle en envoyant une requête ARP à la station 1 indiquant que l'IP de la passerelle correspond à son adresse MAC (00:00:00:00:00:02 et non 00...03), alors tous les paquets à destination des réseaux externes au LAN ~~transmis~~ iront à la station 2.

Ainsi la station 2 peut répondre à la station 1 de fausses informations dans les différentes requêtes, mais aussi de pouvoir donc faire une résolution du site "www.site.fr" par l'IP du site "www.fakesite.fr", qui est 193.192.251.7.

La station 1 tentera donc d'accéder à "www.site.fr" mais avec l'IP de "www.fakesite.fr" sans s'en apercevoir.

(7)



EXERCICE 2

① Le fait d'utiliser une IP dans le même réseau local permet de s'affranchir du routage via une passerelle. Ainsi toute résolution ARP ou RARP se fait localement. De plus il est possible d'utiliser l'adresse de diffusion du réseau pour connaître l'ensemble des hôtes de ce réseau local. Se faire passer pour une autre machine est donc simple en diffusant ou envoyant une requête ARP forgée à l'hôte cible directement. ARP est agnostique et ne vérifie pas l'information. En usurpant l'IP source, les cibles continuent de valider et approuver l'authenticité des requêtes émises.

② La première étape consiste à envoyer une requête ARP indiquant un couple IP : MAC de l'ordinateur malveillant à l'ordinateur cible. L'adresse IP source est donc déjà approuvée. La seconde étape est de recevoir et traiter les requêtes de la machine cible.
La troisième permet dans la réponse d'insérer les données voulues.
Ici dans le cas présent, une commande malveillante.

③ Si l'attaquant s'était trouvé sur le même réseau local mais sans usurper l'IP cible, alors il aurait fallu ajouter du spoofing de MAC Address également. En effet il faut que les machines cibles puissent vérifier la IP source.

④ Un vol de session permet de récupérer l'ensemble des échanges de cette session. Ainsi il peut y avoir les noms d'utilisateurs, mots de passe, token, et toutes les données échangées.
Il est tout à fait possible d'envisager de l'exfiltration de données, ou de la malveillance à l'encontre d'un utilisateur etc...

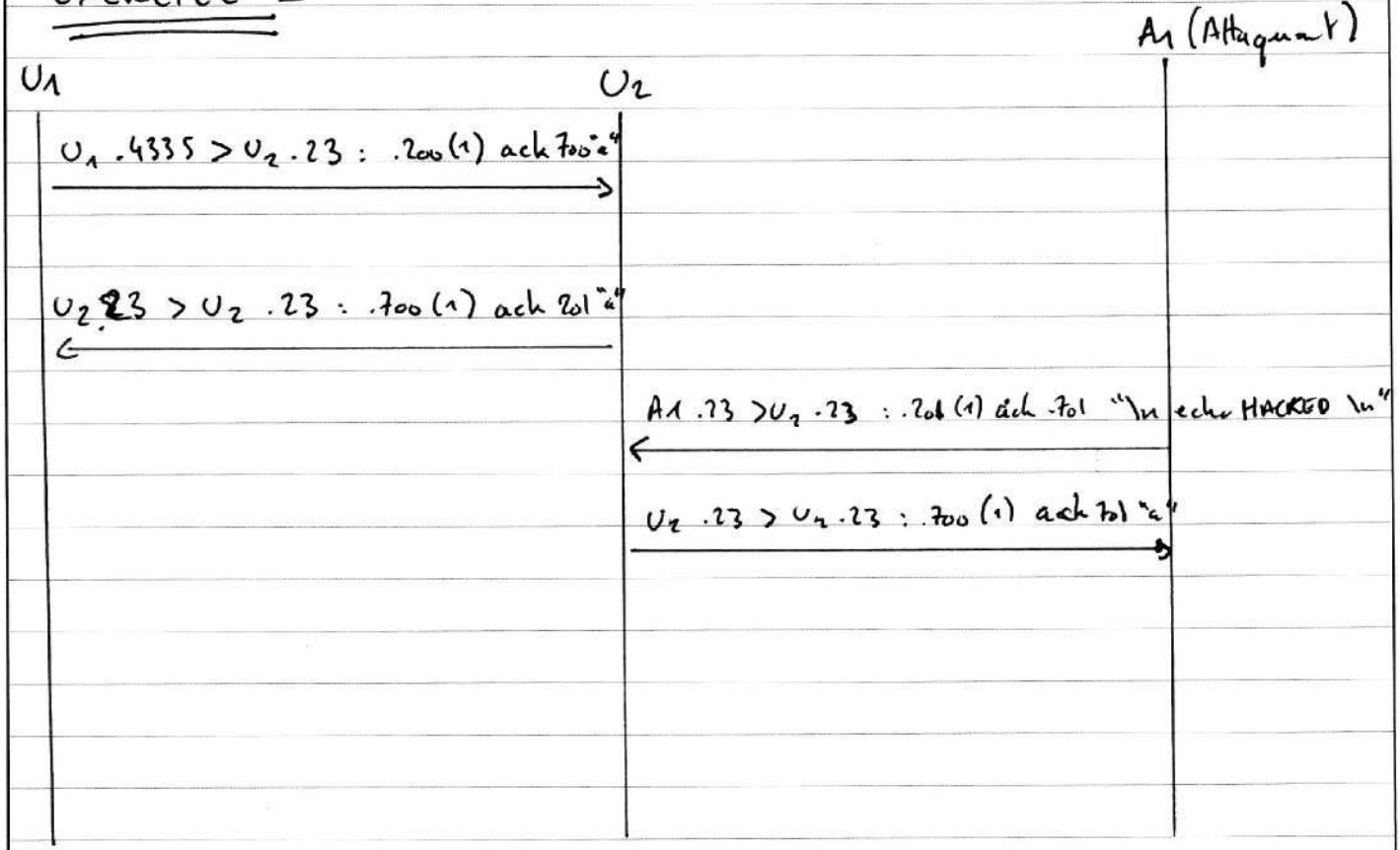
N° ... 8 19

Intitulé de l'épreuve : RÉSEAUX ET TELECOMMUNICATIONS

Nombre de copies : 3

Numérotez chaque page (dans le cadre en bas de la page) et placez les feuilles dans le bon sens.

EXERCICE 1



N°

... /...

N°

... /...

N°

... /...