MINISTÈRE
DE L'EUROPE
ET DES AFFAIRES
ÉTRANGÈRES

Liberté
Égalité
Fraternité

DIRECTION GENERALE DE L'ADMINISTRATION
ET DE LA MODERNISATION
———
DIRECTION DES RESSOURCES HUMAINES
———
SOUS-DIRECTION DE LA POLITIQUE DES RESSOURCES HUMAINES
———
BUREAU DES CONCOURS ET EXAMENS PROFESSIONNELS

CONCOURS INTERNE ET EXTERNE POUR L'ACCÈS À L'EMPLOI D'ATTACHÉ DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION AU TITRE DE L'ANNÉE 2023

ÉPREUVES ÉCRITES D'ADMISSIBILITÉ

JEUDI 16 FEVRIER 2023

ÉPREUVE TECHNIQUE PORTANT SUR L'OPTION CHOISIE PAR LE CANDIDAT LORS DE L'INSCRIPTION

OPTION : RÉSEAUX ET TÉLÉCOMMUNICATIONS

Durée de l'épreuve : 4 heures
Coefficient : 5
Toute note inférieure à 8 sur 20 est éliminatoire

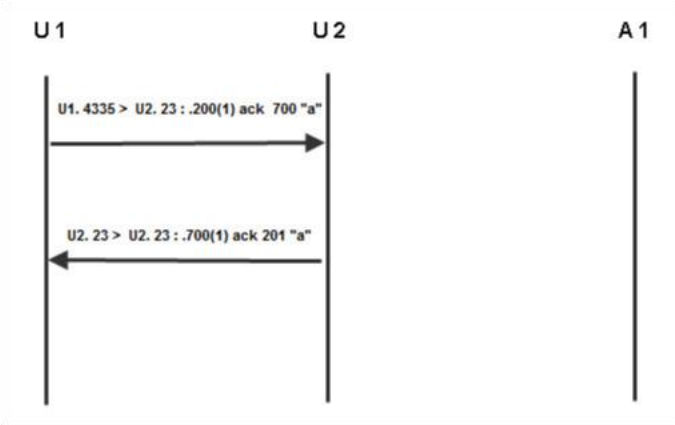
SUJET

Voir pages suivantes.

Ce dossier comporte 7 pages (page de garde non comprise).

Exercice 1

Un attaquant A1 espionne une connexion Telnet entre U1 et U2. Il forge un paquet TCP pour insérer la commande **\n echo HACKED \n** dans le flux de données. Le dernier échange de paquets avant l'insertion est illustré ci-dessous. Reporter le schéma sur votre copie avec le paquet inséré et les paquets suivants.



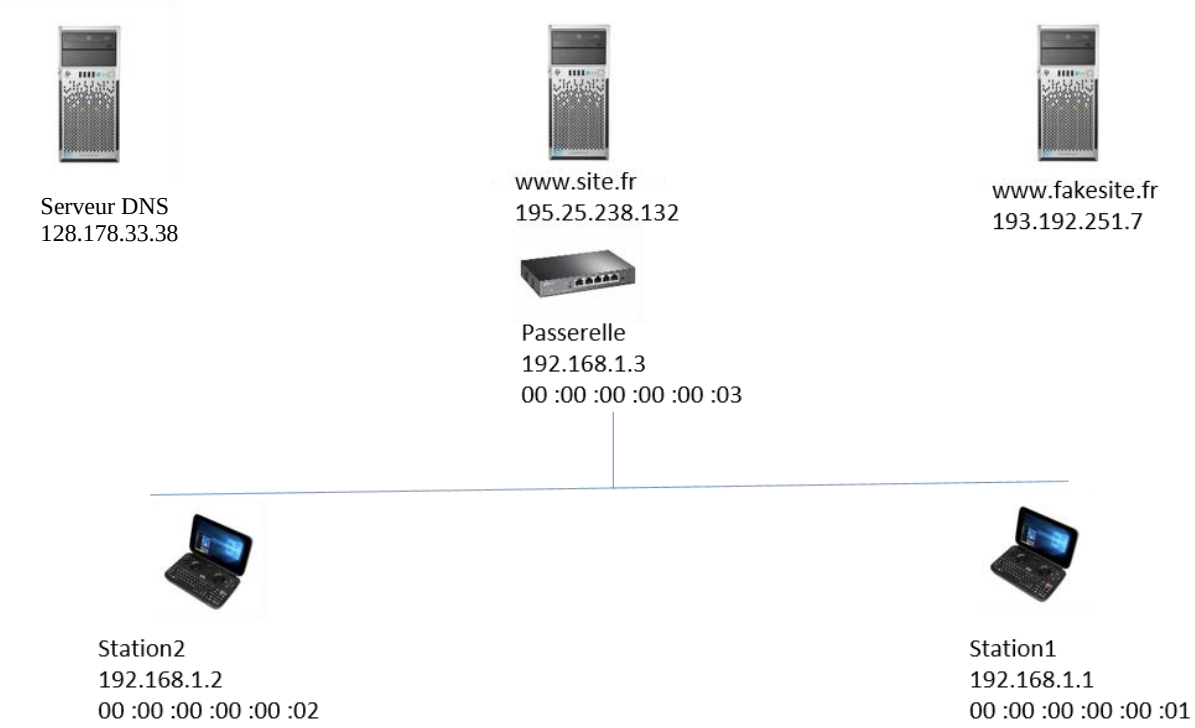
Exercice 2

Une attaque de type « IP spoofing » consiste à se faire passer pour une autre machine en utilisant son adresse IP comme adresse source. L'attaque de Mitnick contre Shimomura avait pour but de faire exécuter une commande malveillante sur la machine cible en se faisant passer pour une autre se trouvant dans le même réseau local.

1. Pourquoi l'attaquant a-t-il utilisé l'adresse IP d'une machine au lieu d'en choisir une au hasard ?
2. Quelles sont les trois étapes principales de cette attaque ?
3. Si l'attaquant s'était trouvé sur le même réseau local, en quoi l'attaque aurait-elle été différente ?
4. Quel est typiquement le but d'un attaquant qui effectue une attaque de vol de session ?

Exercice 3

On considère un réseau local (LAN) composé de deux stations de travail et séparé de l'extérieur par un router (passerelle). Les stations de travail sont configurées pour utiliser un serveur DNS **128.178.33.38** extérieur au LAN et n'utilisant pas de cache DNS interne. On considère enfin deux serveurs HTTP extérieurs au LAN, **www.site.fr** et **www.fakesite.fr**. Les différents éléments sont représentés sur la figure ci-dessous. L'objectif de l'exercice est de proposer une attaque fondée sur le DNS spoofing, telle que lorsque l'utilisateur de station1 (victime) tentera d'accéder au site www.site.fr, il aboutira de manière transparente sur le site www.fakesite.fr. L'attaque sera effectuée à partir de station2.



Lorsqu'une station souhaite communiquer avec l'extérieur du LAN, elle utilise, comme adresse MAC de destination, l'adresse MAC de la passerelle. La passerelle reçoit le paquet et le transmet en direction de sa destination (qui se trouve en dehors du LAN) ; l'adresse destination dans le paquet IP reste inchangée. On suppose pour l'instant qu'aucune des machines du LAN (y compris la passerelle) ne connaît les adresses MAC des autres machines et que le protocole ARP est utilisé pour obtenir des adresses MAC.

1. L'utilisateur de la machine station1 exécute la commande **ping 192.168.1.2.** Ci-dessous figurent les messages échangés sur le LAN jusqu'à l'envoi du ping ainsi que les adresses contenues dans le paquet ping.
   - 192.168.1.1 envoie [ARP who-has ? 192.168.1.2] à l'ensemble du LAN.
   - 192.168.1.2 répond [ARP is-at 00:00:00:00:00:02] à 00:00:00:00:00:01
   - 192.168.1.1 envoie le paquet ping 192.168.1.2

Reporter le tableau ci-dessous sur votre copie et compléter :

Adresse destination dans la requête ping	
IP Destination	
MAC Destination	

2. L'utilisateur de la machine station1 exécute la commande ping **128.178.33.38**. Indiquer les messages échangés sur le LAN jusqu'à l'envoi du ping puis reporter le tableau ci-dessous sur votre copie et compléter :

Adresse destination dans la requête ping	
IP Destination	
MAC Destination	

3. L'utilisateur de station1 exécute la commande **ping www.site.fr**. Indiquer tous les messages échangés sur le LAN jusqu'à l'envoi du ping, puis reporter les tableaux suivants sur votre copie et compléter. Bien que les protocoles DNS et ARP soient fondés sur des principes radicalement différents, leur objectif est le même : éviter à l'utilisateur la mémorisation d'adresses. Le protocole DNS effectue la conversation entre les noms de domaine, en général faciles à retenir, et les adresses IP. On notera [DNS who-is? <Domain name>] une requête DNS et [DNS is-at? <IP address>] une réponse DNS.

Adresse destination dans le paquet DNS	
IP Destination	
MAC Destination	

Adresse destination dans le paquet ping	
IP Destination	
MAC Destination	

4. On suppose maintenant que les machines conservent en mémoire les adresses MAC récemment utilisées. Sachant que de nombreux systèmes d'exploitation acceptent les réponses ARP même s'ils n'ont jamais formulé de requêtes ARP, décrire comment station2 peut se faire passer pour la passerelle auprès de la station1.

5. L'utilisateur de la machine station1 exécute la commande **ping 128.178.33.38**. Reporter le tableau ci-dessous sur votre copie et compléter avec les informations qui seront contenues dans le paquet ping, dans le cas où il n'y a pas d'attaque et dans le cas où l'attaque a lieu.

Adresse destination dans le paquet ping		
	Sans attaque	Avec attaque
IP Destination		
MAC Destination		

6. On suppose que **station2** réussit à se faire passer pour la passerelle auprès de **station1**. Expliquer comment utiliser cette faille pour réaliser l'attaque initialement souhaitée : lorsque l'utilisateur de station1 tentera d'accéder au site **www.site.fr**, il aboutira de manière transparente sur le site **www.fakesite.fr**. Il est important de noter que l'attaque doit rester transparente pour **station1**.

7. On suppose que station2 a mis son attaque en œuvre. Reporter sur votre copie le schéma ci-après (sans les icônes) et dessiner les chemins pris par les paquets transitant sur la LAN lorsque station1 exécute la commande www.site.fr (on ne dessinera pas les requêtes et réponses ARP).

Serveur DNS
128.178.33.38

www.site.fr
195.25.238.132

www.fakesite.fr
193.192.251.7

Passerelle
192.168.1.3
00 :00 :00 :00 :00 :03

Station2
192.168.1.2
00 :00 :00 :00 :00 :02

Station1
192.168.1.1
00 :00 :00 :00 :00 :01

Exercice 4

Pour des raisons de sécurité et d'organisation, l'architecture du réseau a été conçue comme indiqué dans la figure 1.

- Le réseau LAN-1 est le réseau des serveurs accessibles depuis l'extérieur et depuis l'intérieur de l'entreprise.
- Le réseau LAN-2 est le réseau de la direction générale.
- Le réseau LAN-3 est le réseau du personnel.

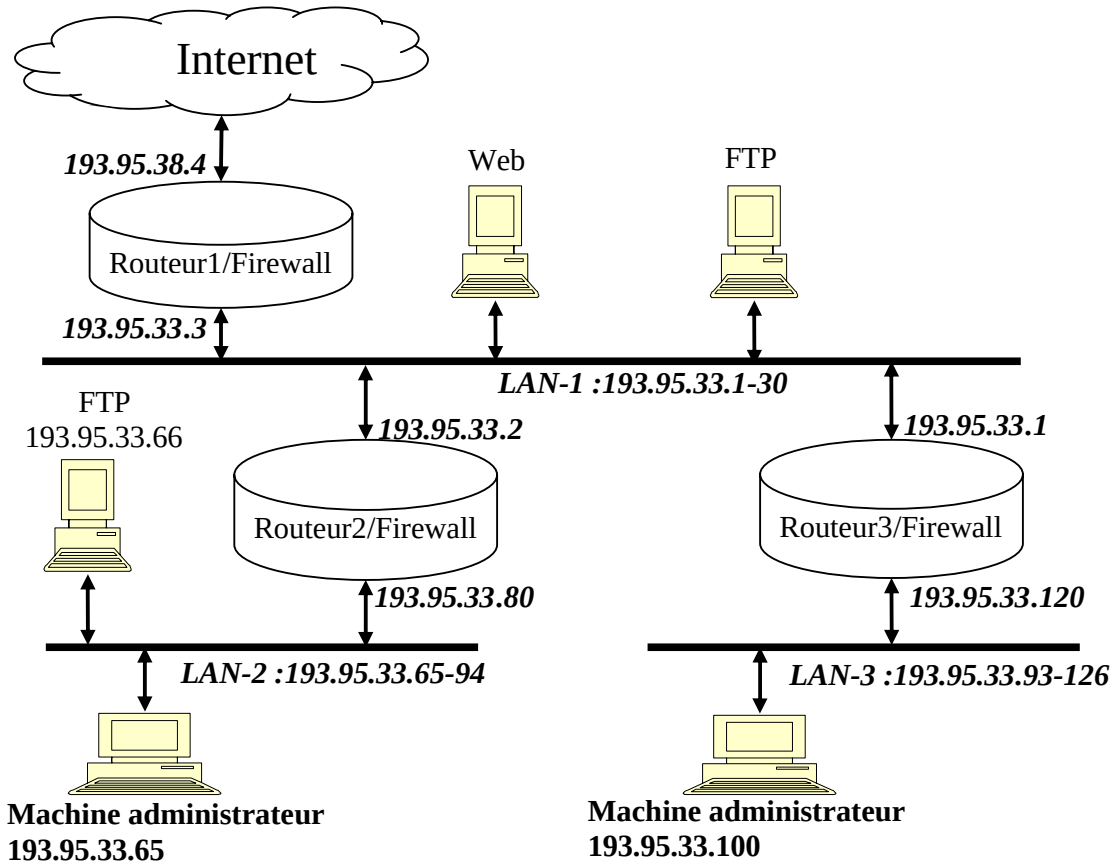


Figure 1 : architecture du réseau

1. Pour permettre aux utilisateurs des réseaux LAN-1, LAN-2 et LAN-3 de dialoguer avec des serveurs SMTP externes, les règles suivantes ont été définies au niveau des trois routeurs du réseau. Expliquer pourquoi ces règles peuvent permettre à un acteur malveillant de lancer des attaques sur ces réseaux.

Routeur 1, 2 et 3	IP source	IP destination	Protocole et port source	Protocole et port destination	Action
Paquet entrant	**Toutes**	**Toutes**	**TCP/25**	**Toutes**	**Autoriser**
Paquet entrant	**Toutes**	**Toutes**	**Toutes**	**TCP/25**	**Autoriser**

2. **Indiquer et ordonner** les règles de filtrage sur chaque routeur permettant de répondre à la politique de sécurité suivante (présentée par les règles A, B, C et D) :
   A. Autoriser uniquement la machine administrateur 193.95.33.65 à lancer la commande **echo** (port 7 UDP) sur toutes les machines du réseau. Toutes les tentatives pour lancer cette commande à partir de l'extérieur seront bloquées.
   B. Permettre l'échange de trafic TCP entre le LAN-1 et le LAN-2.

C. Permettre uniquement à la machine externe dont l'adresse est 103.95.11.11 d'envoyer un trafic ICMP (1) sur les machines du LAN1, LAN-2, LAN-3.
D. Interdire l'échange de trafic FTP (port 21, TCP) entre le LAN-1 et le LAN-2

N.B :

- Reporter les tableaux ci-dessous sur votre copie et compléter en se limitant aux champs présentés.
- Une case vide signifie que cette dernière peut prendre n'importe quelle valeur.

Routeur 1

N°de la règle	Interface d'arrivée	@IP source	Port source	@IP dest	Port dest	Nom ou N° du protocole	Nom de la règle	Action

Routeur 2

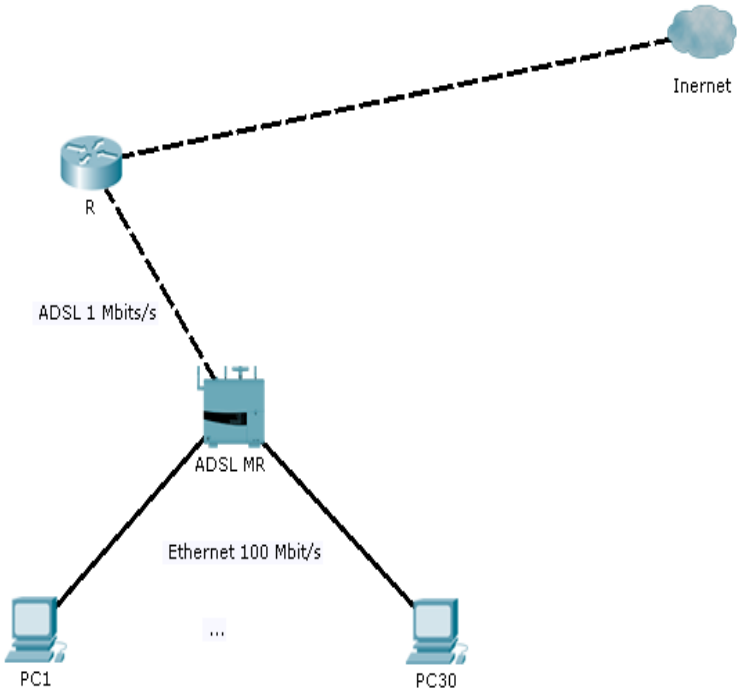
N° de la règle	Interface d'arrivée	@IP source	Port source	@IP dest	Port dest	Nom ou N° du protocole	Nom de la règle	Action

Routeur 3

N° de la règle	Interface d'arrivée	@IP source	Port source	@IP dest	Port dest	Nom ou N° du protocole	Nom de la règle	Action

Exercice 5

Soit le réseau représenté dans la figure suivante :



Le modem routeur "ADSL MR" relie les 30 postes, de PC1 à PC30, par des câbles RJ45 avec un débit de 100 Mbits/s. Le modem est aussi relié au routeur R du FAI par une liaison téléphonique d'un débit de 1 Mbits/s.

1. Citer les sept couches du modèles OSI.
2. Donner pour chacun des termes suivants la couche à laquelle il appartient : **IP**, **Parité**, **ADSL**, **Switch**, **RJ45**, **Trame**, **Masque**, **CRC**.
3. Quels sont les informations ajoutées par la couche liaison aux données reçues de la couche réseau avant d'être transmises à la couche physique.

La configuration IP du poste PC1 est donnée comme suit :

Adresse IP : 193.55.42.72

Masque : 255.255.255. ?

Passerelle : 193.55.42.65

Serveur DNS : 193.55.42.65

4. Préciser à quelle classe appartient ce réseau.
5. Donner l'adresse du modem-routeur.
6. Combien d'adresses IP faut-il utiliser pour adresser toutes les machines de ce réseau ?
7. Quelle est donc la plus grande valeur qu'on peut attribuer au quatrième octet du masque (marqué par ?) ? Donner alors la valeur complète du masque.
8. En utilisant le masque précédent, donner :
   a) L'adresse de sous-réseau.
   b) L'adresse de diffusion dans le réseau.
   c) L'adresse IP la plus basse.
   d) L'adresse IP la plus haute.