Examen
Administration et sécurité des réseaux
Classes: 3SIL

Exercice 1 [7pts]: Soit l'architecture du réseau indiqué dans la figure 1.

- Le réseau LAN-1 est le réseau des serveurs accessibles de l'extérieur et de 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

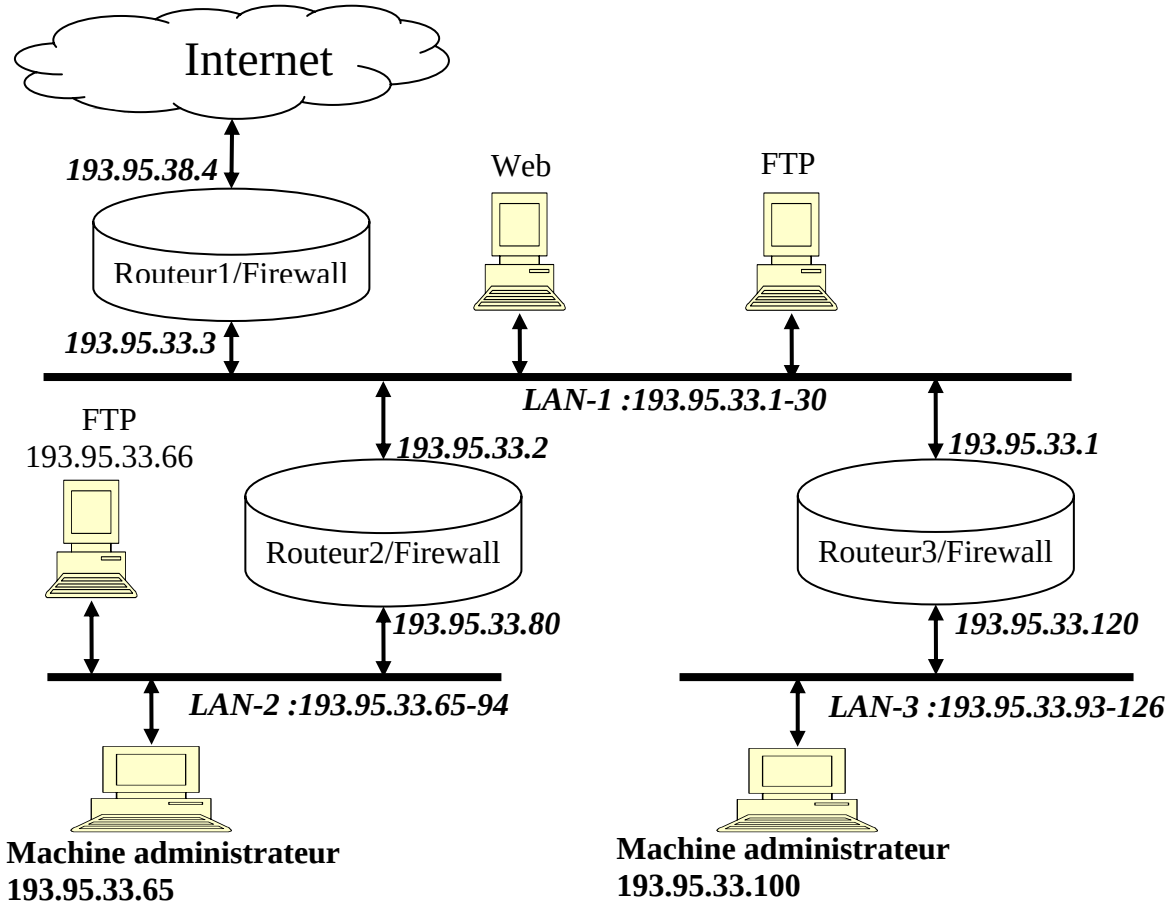

Figure 1 : architecture du réseau

Question1 : Pour permettre aux utilisateurs des réseaux LAN-1, LAN-2 et LAN-3 à dialoguer avec des serveurs **SMTP externe**, les règles suivantes ont été définies au niveau des trois routeurs du réseau de l'entreprise. Expliquer pourquoi ces règles peuvent permettre à un agresseur de lancer des attaques sur les réseaux de l'entreprise? Proposer une solution : de nouvelles règles de filtrage.

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 sortant	Toutes	Toutes	Toutes	TCP/25	**Autoriser**

⇨ Un attaquant externe (client) peut utiliser le port 25 comme port source et se connecte à des serveurs internes

⇨ Solution : considérer aussi le bit ACK (puisque SMTP fonctionne au dessus de TCP) et utiliser des numéros de port clients >1023

R1, R2 et R3	@IP source	@IP dest	Port source	port dest	protocole	ACK=1	Action
Entrant	toutes	toutes	25	>1023	TCP	oui	Accepter
Sortant	toutes	toutes	>1023	25	TCP	*	Accepter

Question2 : Donner 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) en se limitant aux champs suivants:

N° de la règle	Routeur	Interface d'arrivée	@IP source	Port source	@IP dest	port dest	Nom ou N°du protocole	Nom de la règle	Action
1	R2	.33.80	193.95.33.65	>1023	LAN1 LAN3	23	TCP	A	Accepter
2	R2	.33.2	LAN1 LAN3	23	.65	>1023	TCP	A	Accepter
3	R3	.33.1	.65	>1023	LAN3	23	TCP	A	Accepter
4	R3	.120	LAN3	23	.65	>1023	TCP	A	Accepter
5	R1	.38.4	*	>1023	LAN1 LAN2 LAN3	23	TCP	A	Bloquer
10	R2	.80	LAN2	>1023	LAN1	*	TCP	B	Accepter
11	R2	.2	LAN1	*	LAN2	>1023	TCP	B	Accepter
12	R2	.80	LAN2	*	LAN1	>1023	TCP	B	Accepter
13	R2	.2	LAN1	>1023	LAN2	*	TCP	B	Accepter
6	R1	.38.4	.11	N.A	LAN1	N.A	ICMP	C	Accepter
7	R1	.3	LAN1	N.A	.11	N.A	ICMP	C	Accepter
8	R2	.80	Lan2	>1023	LAN1	21	TCP	D	Bloquer
9	R2	.2	LAN1	>1023	LAN2	21	TCP	D	Bloquer

N.A : non applicable

A. Autoriser **uniquement** la machine administrateur 193.95.33.65 à lancer la commande **telnet (**port 23 TCP (6)) sur toutes les machines de l'entreprise. Toutes les tentatives de lancer cette commande à partir de l'extérieur seront bloquées.

B. Permettre l'échange de trafic TCP (6) entre le LAN-1 et le LAN-2.

C. Permettre uniquement à la machine externe d'adresse 103.95.11.11 d'envoyer un trafic ICMP (1) sur **uniquement** les machines du LAN1.

D. Interdire l'échange de trafic FTP (port 21, TCP(6)) entre le LAN-1 et le LAN-2

Exercice 2[6pts]:

1. Donner l'utilité d'un DNS cache ?

⇨ Accélérer la résolution de nom (minimiser le temps de réponse)

2. Un DNS secondaire peut-il contenir plus d'information de résolution de noms que son DNS primaire

⇨ Non s'il joue seulement le rôle de DNS secondaire pour la zone géré par son maître
⇨ Pas forcément dans le cas contraire

3. Une zone peut-elle être gérée par un seul serveur DNS?

⇨ Oui s'il est primaire

4. Soient les deux messages DNS suivants représentant une requête et sa réponse :

```
⊟ Domain Name System (response)
    Transaction ID: 0x0002
  ⊟ Flags: 0x8180 (Standard query response, No error)
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .0.. .... .... = Authoritative: Server is not an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
      .... .... .... 0000 = Reply code: No error (0)
    Questions: [redacted]
    Answer RRs: [redacted]
    Authority RRs: [redacted]
    Additional RRs: [redacted]
  ⊞ Queries
  ⊟ Answers
    ⊞ www.ibm.com: type A, class inet, addr 129.42.16.99
    ⊞ www.ibm.com: type A, class inet, addr 129.42.17.99
    ⊞ www.ibm.com: type A, class inet, addr 129.42.18.99

  ⊟ Authoritative nameservers
    ⊞ ibm.com: type NS, class inet, ns NS.AUSTIN.ibm.com
    ⊞ ibm.com: type NS, class inet, ns NS.WATSON.ibm.com
```

```
⊟ Domain Name System (query)
    Transaction ID: 0x0002
  ⊟ Flags: 0x0100 (Standard query)
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... ...0 .... = Non-authenticated data OK: Non-authenticated data is unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ www.ibm.com: type A, class inet
        Name: www.ibm.com
        Type: Host address
        Class: inet
```

   a. Compléter les quatre champs manquants dans le premier message

⇨ Dans l'ordre **(1,3,2,0)**

   b. S'agit-il d'une requête standard ou inverse? Expliquer

⇨ Champs opcode = 0 donc standard query

   c. Le message réponse provient-il d'un serveur DNS primaire? Expliquer

⇨ Champs authoritative= 0 donc la réponse ne provient pas d'un serveur primaire

Exercice 3 [7pts]:

Une technique de chiffrement simple consiste à effectuer le "ou exclusif ⊕" du message **m** à chiffrer avec une clé **k** qui est aussi longue que le message à protéger. On note **m⊕k** le message **m chiffré avec k**, si m[i] est le i^{ème} bit du message m et k[i] est le i^{ème} bit de la clé k, alors le i^{ème} bit de m⊕k est égal à (m[i] ⊕ k[i]).

1- Qu'appelle-t-on technique de chiffrement symétrique?

⇨ Technique où le chiffrement et le déchiffrement se font en utilisant la même clé (symétrique)

2- Montrez que le "ou exclusif ⊕ " est une technique de chiffrement symétrique.

⇨ m ⊕K ⊕K= m ⊕(K ⊕K)= M ⊕0=M donc le "ou exclusif ⊕ " est une technique de chiffrement symétrique

3- Cette technique est difficilement applicable car le fait de stocker des clés secrètes aussi longues que les messages n'est pas très pratique. En revanche, il est possible de générer un message aléatoire N de la même taille que le message à chiffrer. Dans le premier protocole, c'est le service S qui génère N et l'envoie à X et Y, dans le second protocole c'est X qui génère N_X et Y qui génère N_Y.

Protocole 1

- S --> X, Y: N
- X --> Y : m ⊕ N

Protocole 2

- X --> Y: m ⊕ N_X
- Y --> X : m ⊕ N_X ⊕ N_Y
- X --> Y: m ⊕ N_Y

Analysez les 2 protocoles du point de vue de X, Y et de Z un participant malveillant qui peut écouter tous les messages échangés, en expliquant les messages transférés entre X et Y.

⇨ Protocole 1 : N (la clé symétrique) est envoyé par S à X et à Y et peut être écouté par Z. Y reçoit m⊕N et calcule m = m⊕N⊕N

⇨ Protocole 2 : soit w= m ⊕ N_X ⊕ N_Y le message reçu à la deuxième étape par X. Ce dernier calcule w⊕ N_X= m ⊕ N_Y et l'envoie à Y qui retrouve m= m ⊕ N_Y ⊕ N_Y

Est-ce que ces protocoles permettent à X et Y d'échanger de façon confidentielle le message m? Expliquer?

⇨ Protocole 1: non car N peut être écouté

⇨ Protocole 2: non car un « ou exclusif » entre les trois messages échangés donne m.

Rappel : Quelques propriétés mathématiques

$$A \oplus B = \bar{A}.B + A.\bar{B}$$

$$\overline{A \oplus B} = A.B + \bar{A}.\bar{B}$$

$$A \oplus A = 0$$

$$A \oplus 0 = A$$

$$A \oplus 1 = \bar{A}$$

$$A \oplus \bar{A} = 1$$