Résolution du devoir de cryptographie

**PARTIE 1 :**  Prérequis et calcul

1. Le masque de sous-réseau en /28 est : 255.255.255.240
2. Les nombres de bits alloués sont :

* Pour la partie réseau : 28 bits
* Pour la partie hôte : 4 bits

1. Pour le nombre total d’adresses IP on a : 2n avec n = 4 donc on a 16 adresses IP par sous-réseau.
2. Pour le nombre maximal d’hôte par sous-réseau on a : 2n -2 avec n = 4 donc on a 14 hôtes par sous-réseau.
3. Présentons les informations sous forme de tableau

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sous-réseau** | **Adresse du réseau** | **Première adresse utilisable** | **Dernière adresse utilisable** | **Adresse du**  **broadcast** |
| SR 1 | 192.178.12.0 | 192.178.12.1 | 192.178.12.14 | 192.178.12.15 |
| SR 2 | 192.178.12.16 | 192.178.12.17 | 192.178.12.30 | 192.178.12.31 |
| SR 3 | 192.178.12.32 | 192.178.12.33 | 192.178.12.46 | 192.178.12.47 |
| SR 4 | 192.178.12.48 | 192.178.12.49 | 192.178.12.62 | 192.178.12.63 |

**Partie 2 :** Conception et implémentation du réseau

1. **Topologie réseau**

* Simulation du réseau avec tous les équipements cités en se servant du logiciel Cisco Packet Tracer
* Indications des connexions entre les appareils
* Liaisons entre le switch2 et les trois desktops (2 ; 3 ; 4) ainsi que l’imprimante10
* Liaison entre le switch2 et un point d’accès
* Liaisons entre le point d’accès et les trois laptops (1 ; 5 ; 9)
* Liaison entre le switch2 et le switch3
* Liaisons entre le switch3 et les deux serveurs (Serveur A et Serveur B)
* Liaison entre le switch3 et un routeur (Routeur0)
* Liaison entre le routeur et le switch0
* Liaison entre le switch3 et l’imprimante6

1. **Plan d’adressage IP**

|  |  |  |  |
| --- | --- | --- | --- |
| N° | Type de machine | Adresse IP | Masque SR |
| 01 | Laptop | 192.178.12.2 | /28 |
| 02 | Desktop | 192.178.12.1 | /28 |
| 03 | Desktop | 192.178.12.3 | /28 |
| 04 | Desktop | 192.178.12.6 | /28 |
| 05 | Laptop | 192.178.12.12 | /28 |
| 06 | Imprimante | 192.178.12.17 | /28 |
| 07 | Serveur | 192.178.12.13 | /28 |
| 08 | Serveur | 192.178.12.11 | /28 |
| 09 | Laptop | 192.178.12.14 | /28 |
| 10 | Imprimante | 192.178.12.10 | /28 |

Légendes :

: Adresse inchangée

: :Adresse IP modifié en raison de validité

: Intrus

1. **Tests de connectivité**

Test de connectivité entre les machines (voir page suivante : image du réseau simulé)

1. **Détection et sécurité**

* **Détection des erreurs de configuration**
* 192.178.12.0 : Adresse du réseau attribué au Laptop1 alors remplacement de l’adresse IP du Laptop1 par **192.178.12.2**
* 192.178.12.11 : Adresse IP appartenant au Laptop5 et au serveur B alors conservation de l’adresse pour le serveur B et remplacement de l’adresse IP du Laptop5 par **192.178.12.12**
* **Finalisation du réseau**
* La machine ne se trouvant pas dans le bon réseau est l’imprimante6
* Cette machine appartient au sous-réseau 2 dont l’adresse est **192.178.12.16** et l’adresse de broadcast est **192.178.12.31**
* **Image du réseau simulé**

**TP Cryptographie**

1. **Mise au point des indices donnés**

* Cryptage asymétrique
* Mode d’opération CBC en 256
* Clé : Le dernier octet en binaire de l’adresse broadcast de la machine infiltré du réseau avec **le préfix des deux premières lettres de l’adresse mac de l’ordinateur ayant pour adresse IP 182.216.58.64** du fichier de capture de wireshark transmis
* 31 en binaire donne : **00011111**
* Adresse MAC de l’ordinateur : **5c : 8c : 30 : 5e :77 : bc**
* La clé est donc : **5c00011111**

1. **Décryptage du fichier**

* Importation du fichier crypté de la machine hôte vers la machine virtuelle
* Décryptage du fichier et obtention du message caché.

**Partie 3 :** Questions stratégiques et analyse

1. ***Le sous-réseau à choisir :***

L’entreprise à décider d’ajoute un nouveau département avec 20 hôtes uniques.

Alors pour accueillir les **20 hôtes**, on aura besoin d’un sous-réseau qui peut contenir au minim 20 adresses IP utilisables.

Un sous-réseau avec un /27 (c’est-à-dire un masque 255.255.255.224) offre :**2^ {32-27} - 2 =** **32 - 2 = 30 adresses utilisables.** Donc au final un /27 est parfaitement adapté pour un département de 20 hôtes car :

* + Il y a assez d’adresses (30) pour 20 machines.
  + Il évite le gaspillage d’adresses comparé à un /26 ou /24.

Utilisé plutôt ceux-là **/27 (255.255.255.224).**

1. ***L’adresse de réseau et l’adresse de diffusion :***

Avec comme adresse principale : **192.178.0.2/24** et avec un masque **/24 (255.255.255.0)**,

On a :

* + **Adresse de réseau :** la première adresse de la plage **192.178.0.0**
  + **Adresse de diffusion :** la dernière adresse **192.178.0.255**

Tout simplement car le masque /24 signifie que les 24 premiers bits sont réservés pour l’identifiant réseau, on garde les 8 derniers bits pour les hôtes : **(Tous à 0 → réseau → 192.178.0.0 ; tous à 1 → broadcast → 192.178.0.255)**

1. ***Pourquoi l’adresse de diffusion ne peut-elle pas être assignée à un hôte ?***

L’adresse de diffusion est réservée pour envoyer un message à tous les hôtes du réseau. Elle est réservée exclusivement aux communications de diffusion.

1. ***Pourquoi est-il important de ne pas divulguer l’adresse de diffusion dans un contexte de sécurité ?***

Parce que l’adresse de diffusion peut être utilisée pour :

* + Lancer des attaques de type broadcast Storm (inonder le réseau de messages inutiles).
  + Lancer des attaques DDoS (par amplification via le broadcast).
  + Découvrir tous les hôtes actifs du réseau facilement.

Donc, masquer ou protéger cette adresse est essentiel pour :

* + Réduire les surfaces d’attaque.
  + Protéger les hôtes contre les intrusions.
  + Maintenir une meilleure confidentialité du plan d’adressage.

***5. PC1 et PC2 dans le même sous-réseau ne se pinguent pas :***

Raisons possibles :

* **Pare-feu activé sur l’un des deux PC**

• Empêche les paquets ICMP (ping).

• ping PC2 depuis PC1 et inversement.

• Désactiver temporairement le pare-feu ou autoriser ICMP.

* **Adresse IP ou masque mal configuré**

• Si PC1 ou PC2 a une mauvaise IP ou un masque incorrect, ils ne se verront pas.

• Taper ipconfig (Windows) ou if config / ip a (Linux).

• Vérifier qu’ils ont la même adresse réseau et le même masque.