TP Cryptographie - Analyse et Traitement de l'Énoncé

Partie 1 : Pré-requis et Calculs

Adresse réseau principale : 192.178.12.0/24

Masque de sous-réseau utilisé : /28

1. Calculs Initiaux pour un Sous-Réseau /28 :

a. Masque en notation décimale pointée : 255.255.255.240

b. Bits alloués - Réseau : 28 bits, Hôtes : 4 bits

c. Nombre total d'adresses IP par sous-réseau : 16

d. Nombre maximal d'hôtes utilisables par sous-réseau : 14

2. Plages d'Adresses IP des 4 premiers sous-réseaux /28 :

Sous-réseau	Adresse Réseau	Première IP	Dernière IP	Adresse de Broadcast
1	192.178.12.0	192.178.12.1	192.178.12.14	192.178.12.15
2	192.178.12.16	192.178.12.17	192.178.12.30	192.178.12.31
3	192.178.12.32	192.178.12.33	192.178.12.46	192.178.12.47
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 :

- Le réseau contient : 3 Laptops, 3 Desktops, 2 Serveurs, 2 Imprimantes.

- Chaque machine doit être connectée dans le même LAN (même sous-réseau /28).

- Utiliser un switch ou routeur central pour relier toutes les machines.

2. Plan d'adressage IP (Exemple à partir de 192.178.12.0/28) :

Laptop 01 : 192.178.12.1

Desktop 02 : 192.178.12.2

Desktop 03 : 192.178.12.3

Desktop 04 : 192.178.12.6

Laptop 05 : 192.178.12.11

Serveur 06 : 192.178.12.13

Serveur 07 : 192.178.12.11 (Erreur de duplication !)

Laptop 08 : 192.178.12.14

Imprimante 09 : 192.178.12.15

3. Tests de Connectivité :

- Vérifier la réponse au ping entre chaque machine.

- Identifier toute machine sans connectivité correcte.

4. Détection et sécurité :

- Erreur : IP 192.178.12.11 est attribuée à deux machines (Laptop 05 et Serveur 07).

- Cela cause un conflit d'adresse.

- De plus, l'adresse 192.178.12.17 (Imprimante 06) n'est pas dans le même sous-réseau /28 (elle appartie

- Adresse réseau de l'imprimante 06 : 192.178.12.16

PARTIE3 :

EXPLOITATION DES INDICES FOUURNIS

Le chiffrement utilisé est un cryptage asymétrique ayant un mode d'opération CBC avec une clé de 256bits.

La clé de déchiffrement est construite à partir du dernier octet en binaire de l'adresse broadcast de la machine infiltrée dans le réseau et des deux premiers octets de l'adresse MAC de l'ordinateu r dont l'IP est 183.216.58.64 selon les données du fichier de capture wireshark transmis :

Le dernier octet de l'adresse est 31, soit 000011111 en binaire, l'adresse MAC de la machine cibl e est 5C :8C :30 :5E :77 : BC.

Donc la clé se forme comme suit : 5C8C00011111 ou CC00011111 (pour anonymiser les vraies v aleurs).

DECHIFFREMENT DU FICHIER

Pour déchiffrer le fichier, nous avons tout d'abord importé le fichier depuis la machine hôte vers la machine virtuelle, ensuite nous avons déchiffré le fichier à l'aide de la clé obtenue pour pouvoir extraire et lire le message caché.