SAE 21
Durée : 3 heures
TP2 – TCP UDP Scapy

Nom :
Groupe :
Date :

Objectifs du TP

- ➔ Observer les connexions TCP
- ➔ Créer un paquet TCP de demande de connexion
- ➔ Réaliser un outil de scan de ports

Vous disposez de deux PC avec un dual boot **Windows / Linux Debian**. Nous utiliserons **Linux Debian** pour ce TP

I – Connexion TCP et analyse

Rappeler les étapes de l'établissement d'une connexion TCP en précisant les éléments principaux (échanges, adresses, drapeaux, numéros de séquences, ports…)

Sur une des machines Linux installez le serveur FTP vsftpd et créez un compte utilisateur, sur l'autre machine installez le client FTP Filezilla.

Etablir une connexion FTP à partir du client vers le serveur, en s'authentifiant avec le compte créé précédemment. Capturez cette phase de connexion avec Wireshark et donnez les détails des échanges en rapport avec la première question (attention aux numéros de séquence relatifs ou raw).

Question bonus : en observant les données échangées lors de la phase d'authentification de l'utilisateur, quelle remarque pouvez-vous faire sur la sécurité de votre serveur FTP ?

Interrompre la connexion au serveur et relever sur Wireshark les échanges relatifs à cette déconnexion.

II – Création d'un paquet de connexion TCP avec Scapy

Installez Scapy sur le PC client.

Créer un paquet de demande de connexion FTP vers le PC serveur. Remplissez le maximum de champs (adresses MAC, adresse IP, protocoles, ports, drapeaux…). Le port source sera généré aléatoirement.

Lancez une capture Wireshark et envoyez ce paquet sur le réseau. Commentez le résultat capturé.

III – Scan de ports avec Scapy

Sur le PC client, créez un deuxième paquet de connexion TCP vers le serveur mais cette fois en utilisant en port destination le port du service http.

Lancez une capture Wireshark et envoyez ce paquet sur le réseau. Commentez le résultat capturé.

En comparant les résultats obtenus à la question précédente et au II, comment faire pour découvrir si un service est ouvert sur une machine ?

Créer un script avec Scapy pour tester un ensemble de ports et afficher leur état.

IV – Attaque SYN Flood

Le SYN Flood est une attaque de type déni de service (DDoS : DDoS (distributed denial of service) qui consiste à envoyer massivement des paquets de connexion TCP sur un serveur. Comment peut-on réaliser une telle attaque avec scapy ? Faites un script qui permettrait d'attaquer le serveur FTP mis en place précédemment.

Exécutez le script, qu'observez-vous avec Wireshark (sur la machine cible) au niveau des paquets TCP ?

L'attaque lancée ne doit pas empêcher l'accès à votre serveur FTP. Ceci est dû à des éléments configurés par défaut sur le système d'exploitation. Cherchez quels sont les paramètres sur votre machine Debian qui permettent d'empêcher le déni de service par SYNFlood?