Guide de la semaine 2

Principaux concepts en réseau et sécurité

- **Bases de HTTP**
  - Composants de la communication HTTP (en-têtes, chemins, méthodes, etc.).
  - Codes de statut HTTP courants et leur signification (par exemple, `200 OK`, `404 Not Found`).
  - Envoi de données avec `curl` (formulaire, JSON, cookies, redirections).
- **Protocoles**
  - **HTTP/FTP/SMTP/SSH** : Utilisation dans la communication et le transfert de fichiers/emails.
  - **TCP/IP** : Rôles à travers ses couches (Lien, Internet, Transport, Application).
  - **Protocole de résolution d'adresse (ARP)** : Résout les adresses IP en adresses MAC dans les réseaux locaux.
- **Outils d'interception**
  - Outils pour l'analyse du trafic : `tcpdump`, Wireshark, `capinfos`.
  - Commandes pour gérer les routes et les interfaces : `ip route`, `ip addr`, `ifconfig`.
  - Outils pour analyser les données binaires : `strings`, `xxd`.

Handshake TCP et transmission

1. **Handshake :**
   - Processus en 3 étapes : `SYN`, `SYN–ACK`, `ACK`.
   - Établit une connexion entre les hôtes.
2. **Transmission des données :**
   - L'hôte A envoie des données (par exemple, "Hello World").
   - L'hôte B accuse réception avec des numéros de séquence.
   - Se termine avec des paquets `FIN` pour fermer la connexion.

Outils réseau en ligne de commande

- **`nc` (Netcat) :**
  - Se connecter à des hôtes distants ou écouter sur des ports spécifiques.
- **`nmap` :**
  - Scanner les réseaux pour trouver des ports ouverts et des hôtes.

- `tcpdump` :
  - Surveiller le trafic sur des interfaces et ports spécifiés.

Structure des paquets

- **Paquet Ethernet :** Inclut les adresses MAC, le type, et plus.
- **Paquet TCP :** Ports source/destination, numéros de séquence, indicateurs, et plus.

Scapy pour la création de paquets

- **Classes spécifiques aux couches :**
  - `Ether` **(Couche 2) :** Crée des trames Ethernet.
  - `IP` **(Couche 3) :** Ajoute des données de la couche IP (adresse de destination, type de protocole).
  - `TCP` **(Couche 4) :** Définit la communication TCP (ports, séquence, indicateurs).
- **Envoi de paquets :**
  Syntaxe : `sendp(packet, iface='nom_interface')`

Applications pratiques

- Analyser et créer des paquets avec Scapy pour les tests ou le débogage.
- Surveiller et manipuler le trafic pour les tests de pénétration ou l'analyse de sécurité.
- Utiliser `curl`, `nmap` et `tcpdump` pour interagir avec les réseaux et observer leur comportement.