**Réseaux**:

* Scan
  + Simple : 3-handshake TCP complet (facilement détectable et loggable).
  + Scan SYN : uniquement SYN ACK (pas d’ACK de fin).
  + Scan XMAS, NULL et FIN : moins fiable mais plus furtif.
  + Scan passif : analyse des en-têtes des trames qui passent.
* IP Spoofing : usurpation de l’adresse source.
* ARP spoofing : redirection de trafic vers soi.
* DNS spoofing : permet de redirigé un traffic (MITM…)
* Fragment attack : attaque dissimulé dans un paquet IP fragmenté.
* TCP hijiacking : redirection d’un flux TCP une fois l’auth réalisée.
* DOS/DDOS (Choisir des bonnes IPs avant de DOS)
  + IP spoofing et broadcast ICMP.
  + SYN flooding
  + UDP flooding
* Ping of death
* Nestea attack
* Teardrop

**Applicatives :**

* Buffer overflow.
* Injection SQL.
* Injection cmd shell
* Cross site scripting : XSS, CSS : lien comportant des instructions javascript.
* Attaques dans acrobat reader

**OS**

* Rootkit

**Sociales**

* Phishing

**Sécurité :**

* Checker TTL, windows size et MSS et IDs sur TCP et regarder si variation significatives = probablement un programme de scan d eports.