1. Obtention d’informations :
   1. Obtention ports ouverts + version de l’OS

* Scan : **Nmap**
  + 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 : la victime envoie RST si port fermé, et rien si ouvert ou configuré de tel sorte qu’il ne réponde pas.
  + Scan passif : analyse des en-têtes des trames qui passent.

Si le scan ne marche pas (ports filtrés), on passe au firewalking.

**Protection : Configuration firewall pour bloquer les scans.**

* 1. Obtention des versions des logiciels en écoute :
* **Telnet** : on peut aussi telnet sur un autre port pour glaner des infos mais ne marche pas avec tous les services.
* **Netcat** : Envoie de données sur un port en TCP/UDP.

**Protection : configurer les services pour être le moins bavard possible.**

* 1. Social ingeniering :
* Phishing

1. Attaques réseaux :
2. Attaques applicatives :

* DOS applicatif : utilisation d’un bogue.
* Exploitation d’un bogue : DOS applicatif…
* Buffer overflow

**Protection : patchs, versions à jour et veille sécurité.**

1. Attaques sociales :

* Phishing :
  + Attaque homographe et punnycode
* IP Spoofing : usurpation de l’adresse source.
* ARP spoofing : redirection de trafic vers soi.
* DNS spoofing : permet de redirigé un trafic (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 :**

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

**OS**

* Rootkit

**Sécurité réseau :**

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

**Sécurisation Debian**

* Désactiver boot sur CDROM et disquette : voir Trinux et le fait d’accéder à une partition depuis une disquette et Knoppix pour CDROM.
* Pas d’option failsafe au démarrage dans les options de lilo : Accès root sinon sans mdp.
* Mdp dans BIOS et cadenas histoire d’éviter d’enlever la pile du BIOS qui va rst mdp.
* Fermeture des services (et donc des ports) inutiles au système.
* Configurer pare-feu pour empêcher les scans de ports.
* Configurer les users/groupes et définir les bons droits en fonction des fichiers/commandes sensibles.
* Limiter les programmes s’exécutants en mode root.
* Paramétrer un firewall