Groupe 1

Attaque réseau : Scan de ports (Port Scanning)

- Découverte des services ouverts sur une machine

Attaque logiciel : Brute force login

- Tentative répétée de mots de passe sur un formulaire ou service

Groupe 2

Attaque réseau : SYN Flood

- Saturation d'un serveur via requêtes de connexion TCP

Attaque logiciel : SQL Injection (SQLi)

- Injection de requêtes dans une base de données via une application web

Groupe 3

Attaque réseau : ARP Spoofing

- Interception du trafic sur un réseau local

Attaque logiciel : Cross-Site Scripting (XSS)

- Injection de script dans une page web

Groupe 4

Attaque réseau : DNS Spoofing

- Redirection d'un utilisateur vers un faux site

Attaque logiciel : CSRF (Cross-Site Request Forgery)

- Forcer un utilisateur connecté à exécuter une action non voulue

Groupe 5

Attaque réseau : ICMP Flood (Ping Flood)

- Saturation réseau via envoi massif de pings

Attaque logiciel : Directory Traversal

- Accès non autorisé à des fichiers système via une application web

Groupe 6

Attaque réseau : Wi-Fi Deauthentication Attack

- Déconnexion forcée des utilisateurs d'un réseau Wi-Fi

Attaque logiciel : Authentication Bypass

- Contournement de la page de login d'une application