💣🛡 Cours : Attaques et Défenses en Cybersécurité

📘 1. Introduction

L'objectif de ce module est de comprendre les **types d'attaques** informatiques courantes, leur **fonctionnement**, et les **mécanismes de défense** permettant de les détecter, prévenir ou atténuer. Il s'inscrit dans une démarche **offensive (red team)** et **défensive (blue team)**.

□ 2. Types d'attaques (catégorisées)

🔎 A. Attaques sur le réseau

Attaque	Description
Sniffing	Interception des paquets réseau (Wireshark, tcpdump)
Spoofing	Usurpation d'identité (ARP, DNS, IP)
MITM	Attaque de l'homme du milieu, interception des communications
DoS / DDoS	Saturation d'un service

🌐 B. Attaques sur le Web

Attaque	Exemple/Description
SQL Injection	`OR 1=1 --` dans un champ de login
XSS (Cross-Site Scripting)	Injection de script dans une page web
CSRF	Exploite la session de l'utilisateur pour forcer des actions
Directory Traversal	Accès à des fichiers sensibles (`../../../etc/passwd`)

🔐 C. Attaques sur les systèmes

Attaque	Description
Privilege Escalation	Élever ses droits d'utilisateur
Exploitation de failles	CVE (ex: Log4Shell, EternalBlue)
Rootkits / Malware	Logiciels cachés pour espionner ou manipuler le système

□ D. Attaques sociales

Type	Description
Phishing	Faux mails/pièges pour voler des infos
Pretexting	Attaque basée sur un scénario crédible
Baiting	Attirer avec des ressources (USB infecté)

□ 3. Outils utilisés par les attaquants

Outil	Fonction
Nmap	Scan de ports et services
Metasploit	Cadre d'exploitation de failles
Burp Suite	Tests d'intrusion Web
Hydra/John	Brute force de mots de passe
Aircrack-ng	Attaques sur Wi-Fi
Social-Engineer Toolkit (SET)	Ingénierie sociale

🛡 4. Défenses et contre-mesures

🔐 A. Contre les attaques réseau

- Segmentation VLAN
- Filtrage IP/MAC
- IDS/IPS (Snort, Suricata)
- Chiffrement (SSL, VPN)

🌍 B. Contre les attaques web

- Validation des entrées (backend + frontend)
- Utilisation de ORM pour éviter les injections
- CSP (Content Security Policy) contre XSS
- Jetons anti-CSRF

□ C. Contre les attaques système

- Mise à jour régulière (patch management)
- Antivirus/EDR
- Moindre privilège (principe du *least privilege*)
- Journaux et SIEM (analyse d'incidents)

📧 D. Contre les attaques sociales

- Sensibilisation à la cybersécurité
- Simulations de phishing
- Authentification multifacteur (2FA)
- Politique de mot de passe stricte

🔄 5. Méthodologie d'une attaque (Kill Chain)

```
1. Reconnaissance (passive/active)
2. Scanning & énumération
3. Gaining Access (exploitation)
4. Maintaining Access (backdoor, RAT)
5. Escalation de privilèges
6. Covering Tracks (effacer logs, rootkits)
```

🛡 6. Défense en profondeur (Defense in Depth)

C'est une approche multi-couches :

- **Pare-feu réseau**
- **Antivirus/EDR**
- **Monitoring système**
- **Sécurité applicative**
- **Formation des utilisateurs**
- **Politiques de sécurité**

🎓 7. Exemple de scénario

Attaque :

- Scanning avec `nmap`
- Exploitation d'une faille `CVE` via Metasploit
- Escalade de privilèges
- Installation d'un reverse shell (Maintien de l'accès)

Défense :

- IDS détecte le scan
- Pare-feu bloque le port

- Journal système alerte une élévation de privilèges
- SIEM envoie une alerte en temps réel

📄 8. Conclusion

Comprendre les **techniques d’attaque** est indispensable pour mieux les **contrer**. Un bon ethical hacker doit penser comme un attaquant tout en se comportant comme un défenseur.
