Formation Tests d’intrusion

Jour 1 : Introduction à la Cybersécurité et aux Tests d’Intrusion

Matin :

- Introduction à la cybersécurité : enjeux et menaces
- Principes de base des attaques informatiques (phishing, malware, ransomware)
- Présentation des méthodologies de tests d’intrusion (PTES, OWASP)

Après-midi :

- Reconnaissance et collecte d’informations (OSINT)
- Scan de vulnérabilités et cartographie du réseau
- Introduction aux outils de tests d’intrusion (Nmap, Metasploit, Burp Suite)

Jour 2 : Exploitation et Protection des Systèmes

Matin :

- Exploitation des vulnérabilités courantes (failles web, réseau, système)
- Attaques par injection SQL et XSS
- Techniques de contournement des protections

Après-midi :

- Bonnes pratiques de sécurisation (pare-feu, segmentation réseau, durcissement des systèmes)
- Étude de cas et mise en pratique sur un environnement simulé
- Conclusion et recommandations pour aller plus loin