

CyberSécurité

Sécurité offensive - Pentesting/Malware (72 heures)

26_27_4IRC_08_CYBER_UE9_090_MAJ

ACQUIS

- Appliquer les étapes clés d'un test d'intrusion complet, de la reconnaissance à l'exploitation.
- Maîtriser les méthodologies et outils de tests d'intrusion (pentesting) tels que Metasploit, Burp Suite et Nmap.
- Identifier, exploiter et documenter les vulnérabilités dans des environnements sécurisés.
- Explorer et simuler des scénarios réels d'attaques pour mieux comprendre les vulnérabilités.
- Analyser le cycle de vie des malwares, incluant leurs techniques d'infection et d'obfuscation.
- Étudier les techniques de reconnaissance, d'exfiltration et d'obfuscation des malwares.
- Détecter, neutraliser et comprendre les mécanismes des logiciels malveillants.
- Rédiger des rapports post-pentest détaillés avec recommandations adaptées.
- Maîtriser la rédaction de rapports de sécurité clairs et exploitables.

CONTENU

- Introduction au pentesting et à la sécurité offensive
- Comprendre les définitions, objectifs, et portée des tests d'intrusion.
- Respecter la réglementation et les principes éthiques en sécurité offensive.
- Adopter des méthodologies reconnues (OWASP, PTES).
- Reconnaissance et collecte d'informations
- Appliquer des techniques passives et actives de reconnaissance.
- Exploiter des outils comme Nmap, Shodan et OSINT pour collecter des données.
- Analyser les surfaces d'attaque pour identifier les points faibles.
- Scanning et énumération
- Effectuer l'analyse des ports et services ouverts.
- Identifier les vulnérabilités à l'aide d'outils tels que Nessus et OpenVAS.
- Réaliser l'énumération des systèmes, réseaux, et applications.
- Exploitation des vulnérabilités
- Utiliser des outils comme Metasploit pour exploiter des failles de sécurité.
- Mettre en oeuvre des techniques courantes : Buffer Overflow, SQL Injection, XSS.
- Appliquer des méthodes d'escalade de privilèges et de maintien d'accès (persistance).
- Introduction aux malwares
- Identifier les différents types de malwares : virus, trojans, ransomwares, rootkits.
- Étudier les techniques de dissimulation, comme l'obfuscation et les packers.
- Réaliser des analyses dynamiques et statiques de logiciels malveillants.
- Reporting et remédiation
- Rédiger des rapports post-pentest détaillés et exploitables.

- Proposer des recommandations et des bonnes pratiques de remédiation.
- Communiquer efficacement les résultats aux parties prenantes.
- Exercices pratiques et études de cas
- Simuler des scénarios d'attaque sur des environnements virtuels.
- Analyser un malware réel dans un environnement isolé.
- Mener un test d'intrusion complet, suivi de la rédaction et de la présentation d'un rapport.

PRÉREQUIS

- Maîtrise des concepts fondamentaux de la sécurité réseau.
- Connaissances de base en cryptographie et en sécurité des systèmes d'exploitation (Windows/Linux).
- Familiarité avec les langages de script tels que Python ou Bash.
- Expérience pratique avec des environnements virtualisés et des plateformes cloud.

PÉDAGOGIE

ÉVALUATION

BIBLIOGRAPHIE