RANDORISEC

Formation aux tests d'intrusion

Descriptif :

Avec l'évolution et l'augmentation de la menace cyber les tests d'intrusion se démocratisent et rares sont les entreprises ayant des activités sensibles qui n'en bénéficient pas aujourd'hui.
Cette activité, très spécialisée, ne s'improvise pas et demande une bonne connaissance de la démarche et des outils et techniques d'attaques.
La théorie sera rapidement abordée mais c'est surtout de nombreuses astuces et techniques, ayant été acquises sur le terrain, au cours de centaines de tests d'intrusions, qui seront transmises.
Comme nous pensons que le moyen le plus efficace d'apprendre à réaliser un test d'intrusion passe principalement par la pratique la majeure partie de la formation repose sur des LABS (exercices pratiques) et des épreuves qui permettent aux élèves de réaliser eux-mêmes les attaques.
A l'issue de cette formation vous serez capables de réaliser vous-mêmes des tests d'intrusion simples aussi bien sur des infrastructures que sur des applications et des sites web.
Vous pourrez aussi mieux comprendre les rapports d'audits et de tests d'intrusion rédigés par d'autres ou encore vérifier la bonne correction de vulnérabilités.
Cette formation vous apportera aussi un éclairage nouveau si vous réalisez des investigations numériques.

Public visé :

Auditeurs ou consultants en sécurité
Ingénieurs, techniciens, administrateurs systèmes / réseaux
Responsables ou architectes sécurité

Prérequis:

Les participants doivent être à l'aise avec les systèmes d'exploitation Windows et Unix/Linux (ex : savoir changer son adresse IP). Une bonne connaissance des protocoles TCP/IP, des langages de script et du développement d'application Web sont un plus mais ne sont pas indispensables.

Un environnement complet comprenant plusieurs machines virtuelles personnelles (une machine d'attaque, une machine vulnérable et une machine pour le développement d'exploit) sera mis à disposition par le formateur pour les LABS.
Pour installer les VM chaque participant doit apporter sa propre machine avec les prérequis suivants :

- Droits d'administration ou « root » pour pouvoir modifier la configuration réseau et installer VM Player
- Environ 30Go d'espace disque libre

RANDORISEC

Planning :

JOUR 1
Reconnaissance et attaques de mots de passe

Objectif: savoir identifier des vulnérabilités et casser des mots de passe

1. Introduction (déroulement du pentest, outillage, mindset)
2. Reconnaissance passive
    - Externe: whois, shodan, google - LAB
    - Interne: docs, sites d'équipe, écoute sur le réseau - LAB
3. Reconnaissance active
    - Classique (nmap) - LAB
    - Personnalisé (zmap, netcat, scapy) - LAB
4. Cartographie des vulnérabilités
    - Rapide (scripts NSE) - LAB
    - Classique (Nessus) - LAB
5. Attaques des mots de passe
    - Guess (hydra) - LAB
    - Brute-force (JtR, hashcat) - LAB
    - Rainbow tables (rcracki) - LAB
    - Pass The Hash (metasploit, mimikatz) – LAB

JOUR 2
Exploitation

Objectif: savoir exploiter des vulnérabilités de l'infrastructure

1. Exploitation d'un « buffer overflow » 101 (comment détecter puis exploiter un débordement de tampon de A à Z) - LAB
2. Frameworks d'exploitation (CoreImpact / Canvas / MSF)
3. Metasploit - LAB
4. Server side (compromettre un serveur à l'écoute) - LAB
5. Client side (compromettre un poste de travail) - LAB
6. Post exploitation – LAB

RANDORISEC

JOUR 3
Pentest applicatif

Objectif: savoir identifier et exploiter des vulnérabilités applicatives

1. Méthodologie
2. Outillage (BurpSuite, Nikto, SQLMap, Acunetix WVS)
3. Reconnaissance
4. Gestion des accès
    - Authentification
    - Autorisations
    - Sessions
5. Gestion des entrées utilisateur
    - Injections: SQL, Commandes système, Path traversal, SSRF, etc...
    - Données réfléchies: XSS, Redirections, En-têtes
6. Logique de l'application
7. Hébergement de l'application
8. Autres tests
9. LAB