

Formation Test d'intrusion et développement d'exploitations

Présentation

Cette formation en test d'intrusion couvre les bases du pentesting, y compris les méthodologies, la reconnaissance et la collecte d'informations, ainsi que l'analyse et l'exploitation des vulnérabilités. Les participants apprendront à développer des exploits, effectuer des tests sur les applications web et réseaux, et rédiger des rapports détaillés. Des labs pratiques permettent de mettre en œuvre les compétences acquises dans des environnements réalistes.

Durée : 35,00 heures (5 jours)

Tarif INTRA : Nous consulter

Objectifs de la formation

- Acquérir les bases du test d'intrusion : comprendre les méthodologies de test d'intrusion (OSSTMM, PTES, NIST) et identifier les vulnérabilités courantes dans les systèmes, réseaux et applications.
- Maîtriser les outils de pentesting : utiliser des outils tels que Metasploit, Nmap, Burp Suite et Wireshark et automatiser les tests à l'aide de scripts et de frameworks.
- Apprendre à développer des exploits : comprendre les vulnérabilités courantes (débordement de mémoire, injection SQL, XSS, etc.) et créer des exploits personnalisés pour des failles spécifiques.
- Mettre en pratique les connaissances : appliquer les techniques dans des environnements de test sécurisés et rédiger des rapports de test d'intrusion professionnels.

Prérequis

- Connaissances de base en réseaux et systèmes d'exploitation.
- Familiarité avec Linux et la ligne de commande.
- Notions de programmation (Python, Bash).



Public

- Pentesters débutants ou intermédiaires.
- Développeurs souhaitant comprendre les vulnérabilités logicielles.
- Administrateurs système et réseau souhaitant renforcer la sécurité de leurs infrastructures.
- Professionnels de la cybersécurité souhaitant se spécialiser dans le test d'intrusion.

Programme de la formation

1/ Introduction au Test d'Intrusion

- Définition et objectifs du pentesting.
- Cadre légal et éthique.
- Méthodologies de test d'intrusion (OSSTMM, PTES, NIST).

2/ Reconnaissance et Collecte d'Informations

- Techniques de reconnaissance passive et active.
- Utilisation d'outils comme Nmap, Recon-ng, Shodan et Maltego.
- Cartographie des réseaux et identification des cibles.

3/ Analyse des Vulnérabilités

- Détection des vulnérabilités avec Nessus, OpenVAS et Nikto.
- Étude des failles courantes (OWASP Top 10, CVE).
- Exploitation des vulnérabilités connues.

4/ Développement d'Exploits

- Principes de base de l'exploitation de vulnérabilités.
- Techniques d'exploitation : débordement de mémoire, injection SQL, XSS, CSRF, etc.
- Utilisation de Metasploit pour créer et déployer des exploits.
- Écriture d'exploits personnalisés en Python, Ruby ou Bash.

5/ Post-Exploitation

- Maintien de l'accès aux systèmes compromis.
- Escalade de privilèges et pivotement dans le réseau.
- Techniques de dissimulation d'activité (rootkits, backdoors).

6/ Tests sur Applications Web

- Identification des vulnérabilités web (OWASP Top 10).
- Utilisation de Burp Suite et ZAP pour les tests.
- Exploitation des failles XSS, SQLi et CSRF.

7/ Tests sur Réseaux et Systèmes

- Exploitation des vulnérabilités réseau (attaque de l'homme du milieu, usurpation ARP).
- Tests sur les systèmes Windows et Linux.
- Exploitation des services vulnérables (SMB, FTP, SSH).

8/ Rédaction de Rapports

- Structuration d'un rapport de test d'intrusion.
- Présentation des résultats et recommandations.
- Bonnes pratiques pour communiquer avec les parties prenantes.

9/ Labs Pratiques

- Environnements virtuels pour la pratique (HTB, VulnHub, TryHackMe).
- Scénarios réalistes de test d'intrusion.
- Développement et test d'exploits dans des conditions contrôlées.

Organisation

Formateur

Les formateurs de Docaposte Institute sont des experts de leur domaine, disposant d'une expérience terrain qu'ils enrichissent continuellement. Leurs connaissances techniques et pédagogiques sont rigoureusement validées en amont par nos référents internes. Riches de leur expérience sur le sujet, ils sauront accompagner vos collaborateurs dans leur montée en compétences.

Moyens pédagogiques et techniques

- Alternance d'apports théoriques et de mises en pratique contextualisées.
- Progression pédagogique structurée, de la compréhension à la mise en œuvre opérationnelle.
- Pédagogie immersive favorisant une mise en application immédiate des compétences.
- Formation interactive et participative s'appuyant sur des ateliers pratiques, études de cas et échanges collectifs (+ 60 % du temps de formation.)
- Séquences pédagogiques rythmées et évaluations formatives régulières pour renforcer l'ancrage des apprentissages.
- Supports de cours, ressources documentaires et références mis à disposition par le formateur

Dispositif de suivi de l'exécution et de l'évaluation des résultats de la formation

En amont de la formation *(évaluation en ligne dans l'extranet apprenant)*

- Recueil des besoins et des attentes des participants.
- Auto-positionnement permettant d'évaluer le niveau initial des apprenants.

Tout au long de la formation

- Évaluations continues réalisées par le formateur à travers des questions orales, exercices, QCM, études de cas et mises en situation pratiques.

À l'issue de la formation *(évaluations en ligne dans l'extranet apprenant)*

- Auto-positionnement afin de mesurer l'acquisition des compétences visées.
- Validation de l'acquisition des compétences par le formateur
- Questionnaire de satisfaction « à chaud » à l'issue de la formation
- Questionnaire de satisfaction "à froid", 45 jours après la formation afin d'évaluer l'ancrage des acquis et leur mise en application en situation professionnelle.

Accessibilité

Nos formations peuvent être adaptées à certaines conditions de handicap. Nous contacter pour toute information et demande spécifique.