DOCAPOSTE Institute

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

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE
Tél : Variable non renseignée - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

- 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.

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE
Tél : Variable non renseignée - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

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

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE
Tél : Variable non renseignée - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

internes. Riches de leur expérience sur le sujet, ils sauront accompagner vos collaborateurs dans leur montée en compétences.

Moyens pédagogiques et techniques

- Apports des connaissances communes.
- Mises en situation sur le thème de la formation et des cas concrets.
- Méthodologie d'apprentissage attractive, interactive et participative.
- Equilibre théorie / pratique : 60 % / 40 %.
- Supports de cours fournis au format papier et/ou numérique.
- Ressources documentaires en ligne et références mises à disposition par le formateur.
- Pour les formations en présentiel dans les locaux mis à disposition, les apprenants sont accueillis dans une salle de cours équipée d'un réseau Wi-Fi, d'un tableau blanc ou paperboard. Un ordinateur avec les logiciels appropriés est mis à disposition (le cas échéant).

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

En amont de la formation :

- Recueil des besoins des apprenants afin de disposer des informations essentielles au bon déroulé de la formation (profil, niveau, attentes particulières...).
- Auto-positionnement des apprenants afin de mesurer le niveau de départ.

Tout au long de la formation :

- Évaluation continue des acquis avec des questions orales, des exercices, des QCM, des cas pratiques ou mises en situation...

A la fin de la formation :

- Auto-positionnement des apprenants afin de mesurer l'acquisition des compétences.
- Evaluation par le formateur des compétences acquises par les apprenants.
- Questionnaire de satisfaction à chaud afin de recueillir la satisfaction des apprenants à l'issue de la formation.
- Questionnaire de satisfaction à froid afin d'évaluer les apports ancrés de la formation et leurs mises en application au quotidien.

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE
Tél : Variable non renseignée - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

Accessibilité

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

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE
Tél : Variable non renseignée - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France