Maitrisez les techniques avancées du hacking et de la sécurité informatique

Date et durée

Code formation : HACK-001-FR
Durée : 5 jours
Nombre d'heures : 35 heures

Description

Les techniques de piratage et de sécurité informatique (cybersécurité) sont des activités en constante évolution, dans lesquelles **les attaquants et les défenseurs sont engagés dans une course sans fin**. En effet, les hackers explorent sans cesse de nouvelles vulnérabilités, développent des outils sophistiqués et des tactiques toujours plus ingénieuses pour compromettre les systèmes d'information. Dans le même temps, les professionnels en cybersécurité s'efforcent de renforcer les défenses, de **détecter les menaces de manière proactive** et de réagir efficacement en cas d'incident.

Cette formation intensive vise à vous apporter une réelle compréhension du monde de la cybersécurité, en abordant à la fois **les techniques offensives et défensives**. Ainsi, vous pourrez approfondir votre analyse des mécanismes d'une cyberattaque, des outils utilisés par les attaquants et des **bonnes pratiques en matière de sécurisation des SI**. Au-delà des aspects théoriques, de nombreux labs vous permettront de mettre en œuvre ces connaissances et de développer des compétences opérationnelles.

Dédié aux **professionnels de l'informatique ou de la cybersécurité** qui ont déjà une bonne expérience dans ces domaines. En suivant ces cours, vous serez en mesure de renforcer la sécurité de vos systèmes d'information, de détecter et de répondre efficacement aux cyberattaques, et de **faire face aux défis croissants de la cybersécurité**.

Objectifs

À l'issue de cette formation en cybersécurité, vous atteindrez les objectifs suivants :

- comprendre en profondeur les mécanismes des cyberattaques pour mieux les prévenir et y répondre ;
- acquérir les compétences nécessaires pour protéger les systèmes d'information contre les menaces actuelles et futures ;
- développer une expertise dans l'utilisation d'outils offensifs et défensifs de pointe ;
- optimiser la détection et la réponse aux incidents de sécurité pour minimiser les impacts sur l'organisation.

Points forts

• **Une formation immersive et complète**, encadrée par un expert de terrain qui vous permettra de comprendre les enjeux réels de la cybersécurité.
• **Des cours théoriques et pratiques** qui vous permettront de mettre en œuvre des techniques d'attaque, de défense, et d'acquérir une compréhension approfondie des mécanismes de sécurité.
• **Un examen final basé sur une simulation d'attaque et de réponse** et un accompagnement personnalisé tout au long de votre parcours.

Modalités d'évaluation

Travaux Pratiques

Pré-requis

Suivre cette formation nécessite les prérequis suivants :

- des connaissances de base en réseau et système, ainsi qu'une compréhension des concepts fondamentaux de la sécurité informatique ;
- Une première expérience en cybersécurité est un atout, mais n’est pas obligatoire.

Public

Cette formation s'adresse aux publics suivants :

- les analystes en sécurité informatique ;
- les ingénieurs en sécurité informatique ;
- les architectes en sécurité informatique ;
- les consultants en sécurité informatique ;
- les développeurs ;
- les administrateurs systèmes et réseaux.

Programme

Jour 1 : Introduction à la cybersécurité et à l'approche Red Team

- Présentation de la cybersécurité :
    - Définition du hacking, de la cybersécurité et de leurs enjeux.
    - Présentation du panorama des menaces actuelles et émergentes.
    - les référentiels de sécurité (ANSSI, ENISA, CLUSIF, Cybermalveillance.gouv, etc.)
    - Les types de hackers (hacktivistes, cybercriminels, insiders, etc.).
    - Les types d'attaques (phishing, malware, ransomware, attaques par déni de service, etc.).
    - Les outils et les techniques utilisés par les hackers (reconnaissance, scan de ports, exploitation de vulnérabilités, etc.).
    - Le cycle de vie d'une cyberattaque (reconnaissance, exploitation, maintien d'accès, escalade de privilèges, exfiltration de données, etc.).
- Mise en place d'une Red Team :
    - L'approche offensive avec des simulations d'attaques réelles pour identifier les vulnérabilités.
    - La reconnaissance et l'exploration (scan de réseau, exploration des services ouverts et identification des failles).
    - L'exploitation des vulnérabilités et les techniques d'élévation de privilèges.
    - La mise en place d’une backdoor (exfiltration d’informations, création de dictionnaires et attaque par force brute).

Jour 2 : Compréhension de la sécurité côté défense

- Mise en place d'une Blue Team :
    - La défense proactive contre les cyberattaques (détection, prévention et réponse).
    - Les piliers de la sécurité (confidentialité, intégrité, disponibilité et traçabilité).
    - La mise en œuvre de stratégies de défense en profondeur.
    - La sécurité des réseaux et des systèmes (réseaux internes, VLAN, DMZ, pare-feu, etc.).
- Durcissement des systèmes et des applications
    - Le hardening sur Linux et Windows (processus de sécurisation d'un SI).
    - La sécurisation des services réseau (SSH, DHCP, VLAN, etc.).

    - La mise en place de mesures de sécurité pour les services critiques (IDS/IPS et gestion des logs).
    - La supervision et la gestion des incidents de sécurité via des outils comme SOC et SIEM.
- Réponse aux incidents :
    - La mise en place d'une réponse structurée aux incidents (analyse des logs et identification des traces d'attaque).
    - L'utilisation d'outils comme Wireshark et ELK pour la détection d'intrusions.
    - Les approches de la gestion des incidents (identification, isolation et remédiation).

Jour 3 : Concepts avancés et durcissement approfondi

- Principes avancés de la sécurité :
    - Le fonctionnement de l'IAAA (Identification, Authentification, Autorisation et Audit).
    - Les principes de sécurité (Need to Know, Least Privilege, Non-répudiation, etc.).
    - La sécurisation de l'accès aux systèmes critiques (gestion des privilèges, segmentation des réseaux et contrôle des accès).
- Sécurité des infrastructures réseau :
    - La couche 2 du modèle OSI (VLANs, Port Security et prévention des attaques ARP MITM).
    - La couche 3 du modèle OSI (IPsec et filtrage des routeurs).
    - La couche 4 du modèle OSI (utilisation de passerelles et de pare-feu et configuration d'IDS/IPS).
    - La couche 5 du modèle OSI (Proxy et filtrage des communications sortantes).
- Surveillance et gestion de la sécurité
    - Présentation des outils SOC et SIEM pour la détection et la gestion des menaces.
    - La mise en place d'un système de gestion des logs avec ELK.

Jour 4 : Labs pratiques (AD, Linux et App Web)

- Exploitation d'Active Directory :
    - Le fonctionnement d'une architecture AD (gestion des identités et des permissions).
    - Les techniques d'attaque sur Active Directory (injection LDAP, attaque Kerberos et escalade de privilèges via des attaques pass-the-hash).
    - L'escalade de privilèges, la manipulation des groupes et des politiques de sécurité.
- Exploitation de systémes Linux :
    - L'élévation de privilèges et l'exploitation des services vulnérables.
    - Les techniques de backdoor et l'exfiltration de données.
    - Le durcissement et la mise en place de protections.
- Exploitation d'applications web :
    - Les attaques courantes (injection SQL, XSS, CSRF, etc.).
    - L'utilisation d'outils comme Burp Suite pour l'exploitation des vulnérabilités.
    - Le durcissement des applications Web (sécurisation des points d'entrée et des bases de données).

Jour 5 : Labs pratiques (attaques et défenses)

- Simulation d'attaques réelle :
    - L'attaque complète depuis la reconnaissance jusqu'à l'exfiltration de données.
    - L'utilisation d'outils de la Red Team (Metasploit, Nmap, Burp Suite,etc.).
    - Les techniques de Pivoting et d'escalade dans des environnements multi-composants (AD, Linux, WebApps).
- Réponse aux incidents et analyse de logs :
    - La collecte et l'analyse des logs sur différents systèmes et environnements.
    - L'investigation avec des outils comme Wireshark, ELK, et Splunk.
    - La réponse aux incidents (identification des actions à prendre pour contenir et éliminer les attaques).
- Bilan et bonnes pratiques
    - Retour sur les principales failles découvertes pendant les labs.
    - Les bonnes pratiques de sécurité à adopter pour renforcer la défense des systèmes.
    - Discussion sur la mise en place d'une politique de sécurité pérenne et efficace.