Formation Hacking éthique et sécurité, Niveau 1

Présentation

Cette formation technique réunit la sécurité des infrastructures et la sécurité des applications web dans un cours conçu pour enseigner les bases du piratage informatique et répondre au besoin du marché d'une véritable expérience pratique du piratage et des contremesures associées pour identifier, contrôler et prévenir les menaces organisationnelles.

Cette formation vous permettra de découvrir les approches adoptées par les attaquants lorsqu'ils ciblent des organisations, de mener des essais de pénétration étape par étape, d'utiliser des outils open source et accessibles pour accéder aux systèmes vulnérables et de comprendre comment exploiter votre propre réseau avant les attaquants.

Durée : 35,00 heures (5 jours)
Tarif INTRA : Nous consulter

Objectifs de la formation

- Découvrir et obtenir des informations sur les systèmes d'exploitation et les services disponibles au sein de votre infrastructure
- Découvrir et exploiter les systèmes d'exploitation Windows et Linux grâce à une série de vulnérabilités bien connues
- Mener des attaques par force brute sur les mots de passe pour compromettre les services et accéder à un hôte
- Découvrir les techniques de piratage des serveurs d'application et des systèmes de gestion de contenu pour accéder aux données des clients
- Mener des attaques côté client et exécuter du code sur la machine d'une victime
- Identifier les vulnérabilités communes des applications web et introduire de manière pratique la sécurité dans le cycle de vie de leur développement logiciel

Prérequis

- Connaissance de base des systèmes Windows et Linux, par exemple comment visualiser l'adresse IP d'un système, installer des logiciels, gérer des fichiers

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE - 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

- Compréhension des principes fondamentaux du réseau, par exemple l'adressage IP, connaissance des protocoles tels que ICMP, HTTP et DNS
- Compréhension de base des principes fondamentaux du protocole HTTP, par exemple la structure d'une requête HTTP, les verbes de méthode HTTP, les codes de réponse HTTP

Public

- Décideurs
- Responsables DSI
- Responsables sécurité du SI
- Chefs de projets IT

Programme de la formation

1/ Forcer l'accès par Sniffing, Brute-forcing et Metasploit

- Les bases du TCP/IP
- L'art du scan de ports
- Dénombrement des cibles
- Exercice - ARP Scan (Dénombrement)
- Exercice - Scanner des ports (recensement des services)
- Brute-Forcing
- Exercice - SNMP (Brute Force Attack)
- Exercice - SSH
- Exercice - Postgres
- Les bases Metasploit
- Exercice - Les bases Metasploit

2/ Forcer l'accès aux mots de passes, à Unix et ses services et à un CMS

- Craquage de mots de passe
- Exercice - Craquage de mots de passe
- Piratage des systèmes Unix
- Exercice - Heartbleed
- Piratage de serveurs d'applications sur Unix
- Exercice - Piratage de serveurs d'applications (Tomcat)

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE - 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

- Exercice - Piratage des serveurs d'application (Jenkins)
- Piratage d'un logiciel CMS tiers
- Exercice - Exploit : sérialisation PHP
- Exercice - Exploit WordPress

3/ Forcer l'accès à Windows, ses logiciels et domaines

- Énumération Windows
- Exercice - Énumération des hôtes Windows
- Attaques côté client
- Exercice - Piratage de logiciels tiers
- Piratage de serveurs d'applications sous Windows
- Exercice - Piratage de serveurs d'applications sous Windows
- La post-exploitation
- Exercice - Piratage de Windows - Extraction de mot de passe
- Piratage de domaines Windows
- Exercice - Piratage de domaines Windows

4/ Forcer l'accès aux applications web (niveau 1)

- Comprendre le protocole HTTP
- Exercice - Démonstration de Burp
- Exercice - Manipulation des en-têtes (Headers)
- Collecte d'informations
- Exercice - Collecte d'informations
- Dénombrement des noms d'utilisateur et réinitialisation des mots de passe erronés
- Exercice - Dénombrement des noms d'utilisateur
- Exercice - Attaque du mot de passe par force brute
- Exercice - Fonctionnalité du mot de passe oublié
- Vulnérabilités liées au SSL/TLS
- Exercice - TLS
- Contournement des autorisations
- Exercice - Contournement d'autorisation par manipulation de paramètres
- Exercice - Contournement de l'autorisation
- Exercice - Téléchargement de fichiers arbitraires

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE - 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

DOCAPOSTE Institute

5/ Forcer l'accès aux applications web (niveau 2)

- Cross Site Scripting (XSS)
- Exercice - XSS (réfléchi)
- Exercice - Détournement de session XSS
- Exercice - XSS stocké
- Cross Site Request Forgery (CSRF)
- Exercice - CSRF (Démo)
- Injection SQL
- Exercice - SQLite
- Attaques d'entités externes XML (XXE)
- Exercice - XXE
- Téléchargement de fichiers non sécurisés
- Exercice - Téléchargement de fichiers non sécurisés

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 compétence.

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.

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE - 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

- 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 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.

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE - 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