Formation « Tests d'intrusion des serveurs et des applications Web»

Réf : PENTESTWEB

L'infrastructure Web expose directement votre société aux menaces externe. Renforcez vos défenses en sécurisant efficacement tous les vecteurs exploités par les attaquants !

Objectifs

- Anticiper les besoins des tests d'intrusion
- Comprendre les principales vulnérabilités du web
- Analyser les risques encourus
- Détecter les failles de sécurité
- Exploiter les vulnérabilités pour prendre le contrôle de l'infrastructure

Durée & horaires

- 5 jours soit 35 heures
- Le lundi : de 9h30 à 12h et de 13h30 à 17h30/18h00.
- Du mardi au vendredi : de 09h00 à 12h et de 13h30 à 17h00/17h30.

Nombre de participant

- Minimum 8 participants – Maximum 24 participants

Public visé

- Quiconque souhaite comprendre et pratiquer les techniques utilisées par les attaquants pour compromettre un système d'information depuis Internet :
  - Pentesters
  - RSSI
  - Chefs de projets
  - Développeurs
  - Architectes
  - Administrateurs systèmes

Pré-requis

- Aucun prérequis
- Des notions d'utilisation d'une distribution Linux est un plus

Méthode pédagogique

- Cours magistral avec travaux pratiques et échanges interactifs. La formation est proposée en mode présentiel et accessible en mode distanciel via ZOOM pour ceux qui ne veulent pas se déplacer

Supports

- Support de cours numérique en Français projeté
- Support de cours en Français imprimé en présentiel / au format numérique en distanciel après signature du règlement intérieur
- Cahier d'exercices
- Cahier de corrections
- Ordinateur portable prêté pour la réalisation des exercices

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**
- **Evaluation de pré-formation envoyée avant le début de la formation**
- **Evaluation de mi-formation effectuée en session par le formateur au moyen de QCM et de travaux pratiques**
- **Examen final à la fin de la formation (cf certification)**
- **Ces évaluations ont pour but de valider les compétences acquises.**

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification PENTESTWEB par HS2.**

Programme

Le test d'intrusion
- Méthodologie et type de tests
- Équipement et outils
- Législation
- Déroulement de l'audit
- Gestion des informations et des notes
- Clôture de l'audit
- Pour aller plus loin

Le proxy applicatif
- Usages
- Burpsuite, Zap...

Les mécanismes du Web
- Le protocole HTTP (méthodes, entêtes, codes de retours, encodage...)
- Les risques du modèle client/serveur

La sécurité du client
- La SOP
- Les communications "cross-domain"
- Contournements CORS
- Contournements CSP
- Open Redirect

Cryptographie
- SSL/TLS
- Les suites cryptographiques
- Renegociation non sécurisée
- Audits et contrôles
- La PKI
- Le cassage de condensats

Reconnaissance et fuite d'informations
- Introduction et objectifs
- Découverte passive
  - Résolutions DNS et registres
  - Détournement de sous-domaine
  - OSINT
  - Les Googles Dorks
  - Les fuites
- Découverte active
  - Le transfert de zone
  - Le balayage de ports
  - Découverte de serveurs web
  - Prévisualisation des applications
  - Crawling et Spidering
  - Le WAF
- Le scan de vulnérabilités

Les processus d'authentification
- Gestion de l'identité
- Les attaques sur l'authentification
  - XML Signature Wrapping
  - Détournement d'Oauth

La gestion des sessions
- Les jetons de session
- Les cookies
- Jetons JWT
- Forge de requêtes inter-sites (CSRF)
- Fixation de session
- Forge de jetons de session
- Le cloisonnement des sessions
- Référence directe à des objets non sécurisés (IDOR)

Les injections
- Les injections coté client
  - L'injection XSS
- Les injections côté serveur
  - L'attaque CRLF (et response splitting)
  - Les injections de commandes
  - L'injection XXE
  - L'injection SQL

- Quelques injections moins fréquentes (XPath, LDAP, NoSQL)
- Les injections via sérialisation/dé-sérialisation
- Forge de requête côté client (SSRF)

Les injections de fichiers

- Le téléversement de fichiers
- Les inclusions de fichiers locaux et distants

Les Webservices et API

- Le fonctionnement des Webservices (XML-RPC, SOAP, REST)
- Les websockets
- Méthodologie d'intrusion
- Les applications mobiles

Le Cloud

- Méthodologies et spécificités
- Quelques outils
- Vulnérabilités

Les vulnérabilités plus complexes

- Tour d'horizon (Buffer Overflow...)
- Méthodologie d'exploitation

Tout au long de la semaine, vous pratiquerez les attaques présentées durant le cours sur notre infrastructure web réaliste simulé : de simple visiteur sur un site web, terminez root d'un serveur ! (Tous les outils utilisés durant les exercices sont accessibles gratuitement en dehors de la formation)