Formation « Tests d'intrusion »

Réf : PENTEST1

Réaliser des tests d'intrusion est la méthode la plus efficace pour mettre en évidence les vulnérabilités qui seront exploitées par vos adversaires.

Découvrez ces vulnérabilités par vous-même avant que celles-ci soient exploitées par d'autres !

Objectifs

- Préparer un test d'intrusion réussi
- Maîtriser toutes les phases d'un test d'intrusion (de la découverte à la post exploitation)
  - Découvrir facilement et rapidement le réseau cible
  - Exploiter en toute sécurité les vulnérabilités identifiées
  - Élever ses privilèges pour piller les ressources critiques
  - Rebondir sur le réseau compromis
- Comprendre les vulnérabilités exposées par les réseaux externes et internes
- Utiliser efficacement la trousse à outils du pentester

Durée & horaires

- 5 jours soit 35 heures
- Du lundi au jeudi : de 9h30 à 12h et de 13h30 à 17h30/18h00.
- Le vendredi : de 09h30 à 12h et de 13h30 à 16h00/16h30.

Nombre de participant

- Minimum 8 participants – Maximum 24 participants

Public visé

- Pentesters
- Consultants SSI
- RSSI
- Architectes

Pré-requis

- Des notions en IT et/ou SSI
- Des notions d'utilisation d'une distribution Linux est un plus

Méthode pédagogique

- Cours magistral avec travaux pratiques et échanges interactifs
- Les concepts essentiels développés dans la formation sont illustrés au travers de mises en pratique sur PC permettant d'acquérir des compétences concrètes applicables en tests d'intrusions
- Un réseau vulnérable fidèle à la réalité sert de plateforme pour les tests
- Tous les outils utilisés sont issus du monde libre et peuvent être réutilisés lors des missions
- Les techniques et outils classiques ainsi que modernes sont utilisés tout au long de la formation

Supports

- Support de cours numérique en Français projeté
- Support de cours en Français imprimé
- 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 PENTEST1 par HS2.**

Programme

Introduction aux tests d'intrusion

- Organisation de l'audit
- Équipement et outils
- Méthodologie des tests d'intrusion
- Déroulement de l'audit
- Gestion des informations et des notes
- Réunion de clôture, rapport d'audit et restitution
- Clôture de l'audit
- Pour aller plus loin

Metasploit

- Introduction
- La base de données
- Les modules
- Les payloads
- La post exploitation
- Pivoter/Rebondir
- Fonctionnalités avancées
- Quelques conseils

Découverte d'informations

- Introduction
- Découverte passive
  - Écoute passive
- Découverte active
  - Cartographie du réseau
  - Balayage de ports
- Scan de vulnérabilités

Exploitation Réseau

- Contournement 802.1x
- Usurpation d'ARP

Exploitation Web

- Introduction à l'exploitation Web
  - Méthodologie d'intrusion Web
  - Le proxy applicatif
  - Recherche de vulnérabilités automatisée
- Compromission de l'applicatif web
  - Accès direct aux ressources non sécurisées
  - Injection de commandes
  - Téléversement de fichiers malveillants

- Les inclusions de fichiers locaux et distants
- Les consoles d'administration

- Compromission de la base de données
  - Injection SQL (SQLI)

Exploitation des services

- Découverte de crédentiels
- Service de partage de fichiers NFS
- Service de partage de ressources SMB
- Services de nommage Netbios, LLMNR
- Service SNMP
- Services d'administration distants CLI Telnet et SSH
- Services d'administration avec affichage déporté RDP, VNC, X11
- Service de partage de fichiers FTP
- Services de bases de données
  - MSSQL
  - Oracle
- Les autres services

Post-exploitation

- Généralités
- Élévation de privilèges
- Fiabiliser l'accès
- Pillage
- Rebond
- Contournement d'antivirus
- Cassage des empreintes

Post-exploitation : Linux

- Collecte d'informations
- Les droits
- Sudo
- Applications et services
- Tâches planifiées
- Les utilisateurs
- Le réseau
- Les exploits

Post-exploitation : Windows

- Collecte d'informations
- Mots de passe en clair
- Tâches planifiées
- Services
- DLL
- GPP
- SAM
- Secrets LSA
- Les exploits

Post-exploitation : Active Directory

- Active Directory
- LDAP
- Password Spraying
- Pass-the-hash

- Collecte des partages réseaux
- Coercition
- Kerberos
- Over-Pass-The-Hash
- Kerberoasting
- Forge de tickets
- Dump NTDS
- Recherche de chemins d'attaque