MAJ 20/02/2023

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

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

- Équipement et outils
- Organisation de l'audit
- Méthodologie des tests d'intrusion
- Gestion des informations et des notes
- Exemple de bon rapport d'audit
- Les meilleurs pratiques : PASSI

Rappels et bases

- Les shells Unix *sh
- Les shells Windows cmd & powershell
- Rappels sur les réseaux tcp/ip
- Rappels du protocole HTTP
- Introduction à Metasploit
  - Exploits et Payloads
  - Fonctionnalités utiles
  - Base de données
  - Modules
  - Customisation
- Mises en pratique

Découverte d'information

- Reconnaissance de la cible
  - Open Source Intelligence
- Découverte passive du SI
  - Écoute réseau
- Scans réseau
  - Cartographie du réseau
  - Découverte de services
  - Identification des Systèmes d'exploitation
- Scanners de vulnérabilités
  - Scanner Open Source Openvas
- Mises en pratique

Mots de passe

- Attaques en ligne
  - Brute force en ligne
  - Outils Open Source
- Attaques hors ligne
  - Analyse d'empreintes
  - Méthodologies de cassage
  - Les Raibow Tables
  - Outils Open Source
- Mises en pratique

Exploitation

- Identification des vulnérabilités
  - Contexte des vulnérabilités

- Étude de divers types de vulnérabilités
- Méthodologie d'exploitation
  - Identifier le bon exploit ou le bon outil
  - Éviter les problèmes
  - Configurer son exploit
- Exploitations à distance
- Exploitations des clients
- Mises en pratique

Post-exploitation

- Le shell Meterpreter et ses addons
- Élévation de privilèges
- Fiabiliser l'accès
- Pillage
  - Vol de données
  - Vol d'identifiants
- Rebond
  - Pivoter sur le réseau
  - Découvrir et exploiter de nouvelles cibles
- Mises en pratique

Intrusion web

- Méthodologie d'intrusion WEB
- Utilisation d'un proxy WEB
  - Proxy Open Source ZAP
- Usurpation de privilèges
  - CSRF
- Les injections de code
  - Côté client : XSS
  - Côté serveur : SQL
- Compromission des bases de données
- Autres types d'injections
- Les inclusions de fichiers
  - Locales
  - A distance
- Les webshells
  - Précautions d'emploi
- Mises en pratique

Intrusion Windows

- Méthodologie d'intrusion Windows
- Découverte d'informations
  - Identification de vulnérabilités
  - Techniques de vols d'identifiants
- Réutilisation des empreintes
  - Technique de "Pass The Hash"
- Élévation de privilèges
  - Locaux
  - Sur le domaine : BloodHound
- Échapper aux anti-virus
  - Techniques diverses
  - Outil Open Source Veil
- Outillage powershell
  - Framework Open Source PowerShell Empire

- Mises en pratique

Intrusion Unix/Linux

- Méthodologie d'intrusion Linux
  - Rappels sur la sécurité Unix
- Découverte d'informations
  - Identifications de vulnérabilités
- Élévation de privilèges
  - Abus de privilèges
  - Exploitation de vulnérabilités complexes
- Mises en pratique

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

Rappels et bases
==========
Les différents shells
Les réseaux TCP/IP
    Couches réseau, transport et applicatives
Introduction à Metasploit
    Console vs. GUI
    Méthodologie Générale
    La base de données
    Les exploits
    Les payloads
    Les autre modules
    Meterpreter
    Quelques conseils

Découverte d'informations
==========
Passive
    OSINT
    Ecoute réseau
Active
    Cartographie du réseau
    Cartographie des services

Exploitation Réseau
==========
Couche Liaison
- Inondation de table MAC
- Usurpation de STP
- Usurpation d'ARP

Couche Internet
- Usurpation DHCP
- Usurpation et empoisonnement DNS

Couche Transport
- Détournement de session TCP

Exploitation Web
==========
Introduction à l'exploitation Web
- Méthodologie d'intrusion Web
- Le proxy applicatif
- Rappels du protocole HTTP
- Identification des cibles
- Recherche d'informations
- Recherche de vulnérabilités automatisée

Compromission de l'utilisateur
- Fixation de session
- Cross Site Request Forgery (CSRF)
- Cross Site Scripting (XSS)

Compromission de l'applicatif web
- Accès direct aux ressources non sécurisées
- Défaut de cloisonnement
- Injection de commandes
- Injection XML eXternal Entity (XXE)
- Server Side Request Forgery (SSRF)
- Téléversement de fichiers malveillants
- Les inclusions de fichiers locaux et distants
- Les consoles d'administration

Compromission de la base de données
- Injection SQL (SQLi) (directe, aveugle, booléenne, temporelle)
- Autres injections (LDAP, XPATH)

Exploitation des services
==========
Découverte de crédentiels
Exploitation des services
- Service de partage de fichiers NFS
- Service de partage de ressources SMB
- Services de nommage Netbios, LLMNR
- Services d'administration distants CLI SSH, Telnet, R*-utils
- Services d'administration avec affichage déporté RDP, VNC, X11
- Service de partage de fichiers FTP
- Services de courrier SMTP

Les autres services

Post Exploitation

==========