Ref : DNDAPENTEST1	**Durée :** 5 jours	**Tarif :** 3 €HT

Formation Tests d'intrusion 1

Objectifs de la formation Tests d'intrusion niveau 1:

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.

Programme de la formation Tests d'intrusion niveau 1:

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 Payloadso
- Fonctionnalités utiles
- Base de données
- Modulles
- 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

Public

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.

Méthodes pédagogiques

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