Cybersécurité – Sensibilisation aux techniques d’intrusion

Programme *(Mis à jour le 22/10/2025)*

Introduction

- Objectifs d’un test d’intrusion
- Schéma d’une attaque
- Etapes d’un audit

Méthodologies issues de l’état de l’art

- PTES (Penetration Testing Execution Standard)
- OWASP (web) – Checklist
- Bilan sur les méthodologies

Phase 1 – Enumération du réseau et des services

- Outils d’énumération réseau et des services
- Enumération des équipements actifs (OSI L2 et L3)
- Enumération des ports (OSI L4)
- Identification des services (OSI L5+)
- Classification des équipements identifiés (infra., métier, postes, …)

Phase 2 – Analyse des vulnérabilités

- Outils d’analyse des vulnérabilités
- Bases de données des vulnérabilités logicielles
- Exemple : Systèmes exploitation non mis à jour
- Exemple : Logiciels non mis à jour
- Exemple : Faiblesses dans la politique de mots de passe
- Exemple : Vulnérabilités protocolaires
- Exemple : Faiblesses dans la gestion des droits et des accès
- Exemple : Vulnérabilités web

Phase 3 – Exploitation des vulnérabilités

- Outils d’exploitation des vulnérabilités
- Exploitation des vulnérabilités
- Exemple : Systèmes exploitation non mis à jour
- Exemple : Logiciels non mis à jour
- Exemple : Faiblesses dans la politique de mots de passe
- Exemple : Vulnérabilités protocolaires (design)
- Exemple : Faiblesses dans la gestion des droits et des accès
- Exemple : Vulnérabilités web

Phase 4 – Escalade de privilèges

- Windows – Escalade de privilèges
- Linux – Escalade de privilèges

Phase 5 – Post-exploitation et mouvement latéral

- Récupération des credentials
- Password spraying, Pass the hash
- Tunneling et pivoting
- Enumération d’un domaine Active Directory

Référence

THIS3635

Durée

3 jours / 21 heures

Prix HT / stagiaire

2475€

Objectifs pédagogiques

- Appréhender les techniques actuelles de durcissement de la sécurité informatique et réseau dans un réseau local ou longue distance
- Être sensibilisé aux grandes techniques de tentatives d’intrusions système ou réseau
- Connaître les contremesures à déployer dans le système pour s’en prémunir.

Niveau requis

- Une connaissance de base en réseaux IP est requise.

Public concerné

- Responsables sécurité, administrateurs systèmes et réseaux, mais également toute personne impliquée dans l’organisation de la sécurité de son entreprise.

Formateur

Les formateurs intervenants pour Themanis sont qualifiés par notre Responsable Technique Olivier Astre pour les formations informatiques et bureautiques et par Didier Payen pour les formations management.

Conditions d’accès à la formation

Délai : 3 mois à 1 semaine avant le démarrage de la formation dans la limite des effectifs indiqués

Moyens pédagogiques et techniques

Salles de formation (les personnes en situation de handicap peuvent avoir des besoins spécifiques pour suivre la formation. N’hésitez pas à nous contacter pour en discuter) équipée d’un ordinateur de dernière génération par stagiaire, réseau haut débit et vidéo-projection UHD
Documents supports de formation projetés
Apports théoriques, étude de cas concrets et exercices
Mise à disposition en ligne de documents supports à la suite de la formation

Dispositif de suivi de l'éxécution de l'évaluation des résultats de la formation

Feuilles d’émargement (signature électronique privilégiée)
Evaluations formatives et des acquis sous forme de questions orales et/ou écrites (QCM) et/ou mises en situation
Questionnaires de satisfaction (enquête électronique privilégiée)

Exemples d’attaques

- Exploitation de vulnérabilités critiques : MS08-67, MS14-068, MS17-010
- Exploitation de vulnérabilités critiques : dirtycow, mempodipper
- Empoisonnement LLMNR, NetBIOS, WPAD
- Empoisonnement et relais des challenges Net-NTLM
- Enumération Active Directory
- Phishing : mails, répertoires partagés
- Kerberoasting

Dans la vraie vie

- Contrôles d’accès NAC – 802.1X
- Sondes IDP / IPS
- Anti-Virus
- Windows – AMSI
- Windows – AppLocker
- Windows – Powershell Constrained Mode