

# Audit de sécurité interne - Outillage et test d'intrusion

UIMM

PÔLE FORMATION

UIMM

LA FABRIQUE DE L'AVENIR

Cybersécurité - Systèmes Numériques

03/05/2026

## Public et prérequis

Bases informatiques nécessaires en administration système

Métiers de l'informatique

## Les objectifs

Elaborer un audit interne de PENTEST

## Les méthodes pédagogiques et d'encadrement

Pédagogie active basée sur des exemples, des démonstrations, des partages d'expériences, des cas pratiques et une évaluation des acquis tout au long de la formation

## Validation et certification

Attestation de fin de formation

## Contenu de la formation

### Introduction

- Contexte et objectifs du module

### Rappels et bases Active Directory

- Workgroup vs AD
- Arbres, Forêts & Relations d'approbation
- Objets AD
- SYSVOL & GPO
- Kerberos et modes d'authentification (NTLM, Net-NTLMv2...)

### Préambule à l'audit

- Contexte et périmètre d'un test d'intrusion
- Méthode et mentalité d'auditeur
- Outillage de l'auditeur
- Types d'audit

### Test d'intrusion en boîte noire

- Découverte de l'environnement
- Connexion, interrogations DNS & scans
- Cartographie
- Recherche de vulnérabilités
- Domaine - Accès anonyme
- Domaine - Politique de mots de passe
- Domaine - Commentaires AD

### CENTRES DE FORMATION

**Nancy-Maxéville, Thaon-les-Vosges, Bar-le-Duc, Saint-Dié-des-Vosges, Yutz, Henriville, Bouxières-sous-Froidmont, Epinal**

### DURÉE DE LA FORMATION

**2 jours**

### ACCUEIL PSH

**Formation ouverte aux personnes en situation de handicap. Moyens de compensation à étudier avec le référent handicap du centre concerné.**

## Les + du pôle formation

- 2000 jeunes formés par an
- 500 demandeurs d'emploi formés par an
- 3000 entreprises partenaires
- Accompagnement individualisé
- Diplômes reconnus par l'Etat
- Savoir-être, management, sécurité
- Pédagogie innovante (par projets, en îlots, projet Voltaire, Olympiades des métiers)
- Equipement en machines modernes qui préparent aux métiers de demain

- Domaine - Comptes triviaux
- Domaine - Partages SYSVOL et GPPs
- Domaine - Principe de moindre privilège
- Domaine - Comptes de service (KERBERoasting)
- Domaine - Pré-authentication Kerberos (ASREPRoasting)
- Domaine/Réseau - Fuites de données via LLMNR/NBT-NS
- Système - Systèmes obsolètes
- Système - EternalBlue (MS17-010)
- Système - BlueKeep (CVE-2019-0708)
- Système - Zerologon (CVE-2020-1472)
- Local - "Password reuse" et propagation latérale
- Local - RID 500
- Services - SSH
- Services - FTP
- Services - Bases de données
- Services - RTSP
- Services - VNC
- Services - SMTP
- Services - SNMP
- Services - WEB
- Propagation / Compromission / Post-exploitation
- Propagation latérale et verticale
- "Mimikatz"
- Exemple de post exploitation : Exfiltration NTDS

### Notions d'audit en boîte grise

- Collecte et analyse de données
- Système
- Réseau
- Utilisateurs
- Correctifs
- Chiffrement
- Processus
- Tâches planifiées
- Vulnérabilités courantes
- Chiffrement
- Protection BIOS
- Mise à jour
- Utilisation de VNC ou autres

### Travaux Pratiques

- Réalisation d'un audit / test d'intrusion interne sur une infrastructure simulée, réaliste, embarquant un environnement Active Directory ainsi que des services tiers.

### Recommandations et Remédiations

- Analyse des vulnérabilités présentées
- Proposition de recommandations et remédiations

## Modalités d'évaluation

Evaluation en cours de formation

## Coût et financement

Sur demande et transmis dans le devis

## Modalités d'inscription

A réception du bulletin d'inscription et du devis signé, transmission à l'entreprise de la convention et des documents d'entrée en formation (convocation, règlement intérieur, ...)

## Personne en situation de handicap

Pour un accompagnement personnalisé lié à un handicap, merci de nous contacter pour une mise en relation avec notre référent handicap

## Délai d'accès

5 jours

## Organisation de la formation

7 heures / jour