# USCB17 - Audit de sécurité technique

Mis à jour le 22-04-2022

**Code : USCB17**

Unité spécifique de type mixte

4 crédits

**Responsabilité nationale :**
EPN05 - Informatique / 1

**Contact national :**

Cnam Centre Régional de Bretagne

Zoopôle Les Croix
2 rue Camille Guérin
22440 Ploufragan
0 972 311 312
Isabelle Guée
bzh_master_cybersecurite@lecnam.

## Présentation

### Objectifs pédagogiques

*Description :*

Le test d'intrusion ou Pentest, est un des audits techniques permettant d'évaluer « in vivo » la sécurité d'un système d'information ou d'un réseau informatique. La méthode consiste à analyser les risques d'un SI dus à une mauvaise configuration ou à une vulnérabilité, à prouver leur exploitation, puis à proposer un plan d'action de remédiation.

*Objectifs pédagogiques :*

Cette formation aborde les fondamentaux théoriques et pratiques de l'audit de PenTest. Cette formation sera structurée autour de mises en situation avec des jeux de machines virtuelles.

### Compétences

*Compétences acquises :*

- Savoir organiser une procédure d'audit de sécurité « Test de pénétration » dans un SI
- Définir et négocier un mandat d'audit pour un SI
- Mettre en application les compétences techniques de recherche de vulnérabilité et de pénétration d'un SI
- Rédiger et présenter un rapport d'audit

*Savoirs :*

- Identifier des vulnérabilités exploitables permettant de pénétrer un système, rendre compte et proposer un plan de remédiation

## Programme

### Contenu

- Introduction aux audits techniques
- Le Test de pénétration
  - Aspects Réglementaire (responsabilité, législation, contraintes et précautions),
  - Objectifs, avantages et limites
  - Cycles du Pen Test
  - Types d'audits : boîte blanche, noire ou grise
  - Définition et négociation du mandat de l'audit (Moyens, objectifs hypothèses de départ et d'arrêt)
- Méthodologies et outils
  - Préparation de l'audit
  - Déroulement (Phase de reconnaissance, analyse de vulnérabilité, exploitation, gain et maintien d'accès)
  - Les meilleurs pratiques : PASSI
  - Compte-rendu et fin des tests
- Rappels des bases techniques
  - Shell Linux et Windows, réseaux TCP/IP, etc.
  - Introduction à Metasploit (exploits et payload, modules, bases de données, customisation, pivoting)
- Reconnaissance de la cible (passive, active)
  - Scanners de vulnérabilités
  - Recherche de mots de passe (on-line/off-line, méthodologie de cassage d'empreinte, etc.)
- Intrusion Web
  - Méthodologie d'intrusion Web
  - Burp
  - Usurpation de privilèges (technique Cross-Site Request Forgery)
  - Injections de code (côté client XSS, côté serveur SQL)

    - Compromission des bases de données
    - Les WebShells
- Intrusion Windows
    - Méthodologie d’intrusion Windows
    - Découverte d’informations
    - Techniques de vols d’identifiants (Pass The Hash)
    - Cartographie de l’Active Directory avec BloodHound
- Intrusion Linux
    - Rappels sur la sécurité Unix
    - Découverte d’information, identification de vulnérabilités
    - Elévation de privilèges
- Exploitation
    - Recherche et identification des vulnérabilités
    - Méthodologies d’exploitation (identifier le bon exploit et le bon outil)
    - Exploitation à distance
    - Technique d’évasion aux anti-virus (outil Veil)
- Post-Exploitation
    - Shell Meterpreter et framework PowerShell Empire
    - Fiabiliser l’accès
    - Rebond et déplacement latéral (pivoter sur le réseau, découvrir et exploiter de nouvelles cibles)
    - Pillage (Vol de données, vol d’identifiant, exfiltration d’information)
- Eléments de rédaction d’un rapport
    - Analyse globale de la sécurité du système
    - Description des vulnérabilités trouvées
    - Définition des recommandations de sécurité
    - Précautions nécessaires à la transmission du rapport

## Modalités de validation

- Examen final

## Description des modalités de validation

Examen sur un cas pratique de mise en situation d’audit sur des machines virtuelles.