SEC106 - Analyses de sécurité : vulnérabilités et attaques

Mis à jour le 04-12-2024

Code : SEC106

Unité d'enseignement de type cours

6 crédits

Volume horaire de référence (+/- 10%) : **50 heures**

Responsabilité nationale : EPN05 - Informatique / 1

Contact national :

EPN05-Informatique

2 rue Conté
33.1.10A
75003 Paris

Marlène DEFFON
marlene.deffon@lecnam.net

Présentation

Prérequis

Bac+2 informatique,

Objectifs pédagogiques

- Application des principes de management des vulnérabilités face aux exigences organisationnelles,
- Modélisation et analyse de la surface d'exposition d'un système d'exploitation, d'un réseau et d'un système d'information (face à la confidentialité, l'intégrité, la disponibilité, l'authentification, la non-répudiation).
- État de l'art des outils d'analyse de vulnérabilités de l'entreprise et mise en place,
- Analyse de l'exploitabilité d'une vulnérabilité vis-à-vis de l'efficacité des contrôles de sécurité en place,
- Conception et configuration d'une preuve de concept de vulnérabilités,
- Les métiers dans le processus d'analyse de vulnérabilités, principes de management d'une équipe d'analystes,
- Formalisation des résultats de l'analyse sous forme de rapports d'analyse.

Compétences

- Savoir mener l'analyse de vulnérabilités d'un système d'exploitation, d'un réseau, d'une infrastructure et d'un parc informatique,
- Assurer la surveillance rapprochée des vulnérabilités,
- Évaluer l'exploitabilité et l'efficacité des contrôles de sécurité en place,
- Analyser et contextualiser les vulnérabilités afin de les prioriser (scans de vulnérabilités, plan de recommandations suite aux vulnérabilités remontées , suivi des mesures correctives),
- Réaliser des POC des vulnérabilités en maquette,
- Manager une équipe de techniciens et d'ingénieurs SOC,
- Rédiger et communiquer des rapports d'analyse orientés risques : le présenter et proposer des contre-mesures,
- Savoir mettre en place les outils de diagnostics de l'entreprise.

Programme

Contenu

Vulnérabilités des systèmes :

- classification des vulnérabilités (CVE)
- analyse de vulnérabilités de sécurité : système et applications et injections, canaux cachés, replay

Attaques des systèmes :

- classification des attaques
- analyse des attaques simples et complexes et ciblées

Outils de diagnostic et des vulnérabilités pour l'audit

- tests de robustesse des composants
- audit de la donnée et de l'IT

Modalités de validation

- Projet(s)

- Mémoire
- Examen final

Description des modalités de validation

Examen final sur table

Contrôle continu avec un dossier d'analyse de vulnérabilité

Bibliographie

Titre	Auteur(s)
Sécurité informatique - Ethical Hacking: Apprendre l'attaque pour mieux se défendre	Par ACISSI.
Sites de l’ANSSI et du CLUSIR	ANSSI