SEC102 - Menaces informatiques et codes malveillants : analyse et lutte

Mis à jour le 20-03-2025

Code : SEC102

Unité d'enseignement de type cours

6 crédits

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

Responsabilité nationale : EPN05 - Informatique / Véronique LEGRAND

Contact national :

EPN05-Informatique

2 rue Conté
33.1.10A
75003 Paris

Marlène DEFFON
marlene.deffon@lecnam.net

Présentation

Prérequis

Bac+ 2 en scientifique, technique ou informatique

Sous ces conditions, les informaticiens en poste dans les entreprises mais aussi publics en recherche d'une double compétence ou en reconversion.

Une expérience professionnelle significative dans les métiers de l'informatique

Objectifs pédagogiques

- Comprendre le processus d'investigation numérique, les normes et éthiques à prendre en compte,
- Comprendre et pratiquer les différents méthodes d'analyse : réseaux, mémoires, OS,données et disques,
- Comprendre les méthodes d'analyse de code : source, binaire, extraction mémoire,
- Connaitre les différents tests de sécurité et établir les critères selon le contexte d'application,
- Comprendre les principes d'une revue de codes, d'un test des vulnérabilités connues.

Compétences

- Pratiquer une analyse de journaux (systèmes ou applicatifs);
- Pratiquer une analyse de codes malveillants;
- Connaitre et paramétrer les outils et méthodes d'investigation ciblées sur des systèmes informatiques;
- Savoir identifier les techniques d'attaques et exploits par code malveillant par leurs effets aux différents stades du déploiements du code;
- Savoir identifier les vulnérabilités principales
- Savoir minimiser, stopper ou réduire l'impact du code malveillant.

Programme

Contenu

Syllabus détaillé :

- -------
- TEMPS 1
- -------

- Le processus de l'investigation numérique : référentiel ISO/IEC 27043:2015, autres normes.
- Le cycle de vie de la lutte contre le code malveillant en 3 phases : veille, alertes, réponse,
- Phase de veille : modes d'action pour prévoir les effets,
- Phase d'alerte : effets des codes malveillants, détection des effets des codes, identification de la menace,
- Phase de réponse : minimiser, stopper ou réduire l'impact du code malveillant Les contenus :

Les principes éthiques seront enseignés tout au long de cet enseignement.

- -------
- TEMPS 2
- -------

- Principe des codes malveillants et de la rétro-conception
- Étude des modes d'actions, typologies des codes et de leurs effets ("virus", “worm”, “botnet”, etc.)
- Effets d'un code malveillant : caractérisation, analyse des impacts techniques, économiques, fonctionnels à partir d'un exemple réel,
- Méthodologie de réponse à incidents : anatomies d'attaque-type à partir d'exemples réels,
- Bases de connaissance sur les codes malveillants ("threat intelligence"),
- Typologie d'un rapport d'investigation numérique adapté à différents niveaux d’interlocuteurs.

- -------
- TEMPS 3
- -------

Les différentes formes d'analyse :

- Analyse statique (avant exécution, code source)
- Faux positifs et faux négatifs
- Analyse dynamique (exécution de programme, profilage)
- Analyse de teinte
- Performances, avantages et inconvénients
- Analyse énergétique

- -------
- TEMPS 4
- -------
- Analyse post-mortem (forensique) et principes de lutte : réduction des effets, limitation des impacts techniques et fonctionnels,
- Outils logiciels pour l'investigation de codes malveillants : “volatility”, …

- -------
- TEMPS 5
- -------
- Traitement d'un cas d'étude

Modalités de validation

- Contrôle continu
- Examen final

Description des modalités de validation

2 modalités suivies :

1. Continue : TP et mémoire portant sur un sujet lié aux codes malveillants (modélisation, anatomie, rétro-conception d'un malware...)
2. Finale : Examen sur table : Cas ou QCM.

L'examen final est validé par le responsable national chaque année de façon systématique avant la mise en place de l'examen.