Diplôme d'établissement ENSEIRB-MATMECA – Bordeaux INP
« Expert Cybersécurité des Infrastrucures Numériques - ECIN »

Description détaillée du programme :

UE1 : Gouvernance, gestion des risques et conformité

Module 1 : Ecosystème français et européen de la cybersécurité (3j)

- Objectifs : comprendre l'organisation du marché français de la cybersécurité et le cadre réglementaire français et européen dont l'ANSSI
- Plan du cours : ANSSI, qualifications, dispositifs nationaux et européens, Campus, GDPR, LPM, etc. la terminologie cyber est aussi introduite :
- Compétences développées : gouvernance, réglementaire, organisation du marché
- Volume horaire : 24h

Module 2 : Gouvernance, gestion des risques et conformité (3j)

- Objectifs : Maîtriser les concepts de la GRC, basés sur les normes, méthodologies et réglementations
- Plan du cours : ISO 27001 et 27002, SMSI, NIS, LPM, EBIOS, etc…
- Compétences développées : gouvernance de la sécurité, organisation, pilotage, maîtrise des risques, conformité réglementaire
- Volume horaire : 24h

UE2 : Audit de sécurité technique

Module 3 : Intrusion sur les applications Web (3j)

- Objectifs : ce module s'adresse à des personnes disposant de connaissances techniques et souhaitant parfaire leurs connaissances des vulnérabilités sévères modernes. Le module a pour but de présenter, en s'appuyant sur de nombreux cas pratiques, les différentes réflexions et observations permettant de guider l'expert dans sa découverte de vulnérabilités.
- Plan du cours :
    - Introduction (déroulement d'une intrusion, méthodologie et concepts généraux, démarches et ressources)
    - BurpSuite (utilisation de BurpSuite dans le cadre d'une intrusion en boite noire, possibilités et limites de BurpSuite, raccourcis et mécanismes d'automatisation, Extensions)
    - Reconnaissance (surface d'attaque, outillage)
    - Méthodologies et démarche (caractère itératif du processus,

vulnérabilités logiques, gestion de mécanismes communs : authentification, contrôle d'accès, entrées utilisateurs, identification des technologies côté client et côté serveur)
    - Etude et exploitation des vulnérabilités avancées (Tour d'horizon des vulnérabilités applicatives : XXE, SSRF, injections, SSTI, Prototype, pollution, attaques cryptographiques, attaques des mécanismes d'authentification, GraphQL, vulnérabilités spécifiques au cloud)
    - Etude et exploitation de vulnérabilités spécifiques (Java, PHP, Python/Django, Perl)
- Compétences développées : Capacité d'identification et d'exploitation des vulnérabilités Web. Capacité de faire des recommandations de correction et de remédiation sur les vulnérabilités Web. Capacité de réaliser des développements sécurisés.
- Volume horaire : 24h

Module 4 : Intrusion sur les systèmes Linux (3j)

- Objectifs : l'objectif de ce module est de réaliser des instructions sur les d'infrastructures de type Linux à travers l'exploitation de plusieurs vulnérabilités. Ce module comprend des cas d'utilisations pratiques et réalistes pour réaliser des intrusions discrètes à travers l'exploitation de systèmes et l'élévation de privilèges. Au cours de ce module, la méthodologie et les techniques utilisées seront exposées et détaillées.
- Plan du cours :
    - Fonctionnement d'un environnement Linux (déroulement d'une intrusion, mécanismes d'administration, fonctionnement, authentification, hiérarchie des comptes, mécanismes de sécurité)
    - Intrusion en mode anonyme (reconnaissance et méthodologie de cartographie, exploitation, vulnérabilités applicatives, interceptions réseau, cas d'un accès physique à un poste de travail)
    - Intrusion en mode authentifié (reconnaissance locale sur un système, élévation de privilèges, rejeu d'informations d'authentification, exploitation de configurations : sudo, tâches planifiées, permissions, etc., exploitation de vulnérabilités publiques, contournement de restrictions logicielles : Sandboxing, Linux Security Module, persistance, gestion de l'empreinte sur le système)
    - Exploitation de droits administrateur local (manipulation des ressources locales, extraction des secrets d'authentification, dissection de la mémoire Linux, exploitation d'éléments système live, compromission en profondeur, empoisonnement de services systèmes, empoisonnement de binaires, mise en place de mécanismes de persistance avancés : rootkits utilisateur, rootkits noyau, portes dérobées, gestion de l'empreinte sur le système, méthodologie de rebond.
- Compétences développées : Capacité d'identification et d'exploitation des vulnérabilités Linux. Capacité de faire des recommandations de correction et de remédiation sur les vulnérabilités Linux. Capacité de réaliser des développements sécurisés sur Linux.
- Volume horaire : 24h

Module 5 : Intrusion sur les systèmes Windows (3j)

Objectifs : ce module aborde différentes notions de sécurité dans un environnement Windows et Active Directory pour la réalisation de test d'intrusion. Différents travaux pratiques seront abordés pour comprendre les protocoles d'authentification, la gestion des autorisations et les différents moyens d'élévation de privilèges.

- Plan du cours :
  - Bases théoriques des différents éléments de sécurité de Windows (stockage des mots de passe, protocoles d'authentification, protocoles de résolution de noms)
  - Élévation de privilèges locaux (contournement de compte utilisateur, Récupération d'informations, extension de la compromission)
  - Élévation de privilèges au sein d'un domaine (Rebond, Chemins de contrôle, extraction d'information d'authentification, contournement de restrictions logiciels)
  - Élévation de privilèges inter-domaines
- Compétences développées : Capacité d'identification et d'exploitation des vulnérabilités Windows. Capacité de faire des recommandations de correction et de remédiation sur les vulnérabilités Windows. Capacité de réaliser des développements sécurisés sur windows.
- Volume horaire : 12h

UE3 : Entrainement de cybersécurité

Module 6 : Entrainement technique – CTF (1,5j)

- Objectifs : Apprendre les techniques d'intrusion et d'investigation sur la base d'un scénario défini à l'avance
- Plan du cours : Participer et résoudre un CTF
- Compétences développées : Capacité d'intrusion sur les systèmes, hacking Ethique, challenge technique.
- Volume horaire : 12h

Module 7 : Entrainement organisationnel – Gestion de crise (1,5j)

- Objectifs : comprendre et participer à un exercice de gestion de crise sur la base d'un scénario défini à l'avance
- Plan du cours : exercice de crise, gestion de la crise, communication, collaboration, mesures de contournement
- Compétences développées : communication de crise, gestion du stress et des équipes, transversalité, gestion de l'urgence et des priorités.
- Volume horaire : 12h