Projet Ethical Hacking (associé Cybersécurité)

Niveau d'étude
BAC +5

Composante
Polytech Dijon
(Ex-ESIREM)

Présentation

Description

Un réseau d'entreprise classique comporte plusieurs points d'accès à d'autres réseaux, à la fois publics et privés. Le défi consiste à garantir la sécurité des réseaux tout en les gardant ouverts à leurs clients (QoS).

Le projet commun pour double objectif la formation à la garantie de la propriété numérique et à la sécurisation des moyens de production. Le projet est mené par 2 groupes d'étudiants au sein de l'atelier flexible (ligne 4.0 localisée à Dijon et déjà utilisée en projet de 3A). Les groupes seront alternativement conduit à cartographier, attaquer et défendre la ligne situé à l'intérieur de locaux sécurisés. Les attaquants et défendeurs auront plusieurs niveaux d'intervention à réaliser successivement. Tout d'abord à distance : Pour le groupe issu de la spécialisation Cybersécurité, il s'agit d'opérer sans accès aux locaux mais dans le rayon du réseau sans fil ; Pour le groupe issu de la spécialisation IoT, il s'agit de détourner/sécuriser le contrôle d'accès.

La phase suivante permet aux 2 groupes d'avoir un contrôle physique de certains éléments de la ligne (d'autres éléments étant toujours inaccessibles, fermés à clé ou protégé par mot de passe). L'objectif commun des attaquants étant d'intercepter les données de production. Soit directement depuis les capteurs (IoT) soit au niveau par accès serveur (Cyber) en utilisant les failles informatiques et humaines prévues à cet effet. Le dernier niveau d'attaque consiste à laisser une ligne de production apparemment nominale mais dont certaines données font l'objet d'un piratage.

Le groupe en charge de la protection devra repérer l'intrusion et définir des stratégies de défense (comparaison de chaînes, chiffrement et contrôle statistique).

Objectifs

* Appréhender le paramétrage des matériels en accord avec les règles de cybersécurité
* Appréhender l'analyse de topologies de réseaux et les tests d'intrusion
* Appréhender les conséquences d'exploitation malveillante de failles sur une ligne de production
* Recommander des contre-mesures préventives et correctives pour atténuer les risques de cyberattaque (pour la spécialité Cybersécurité)
* Recommander l'architecture physique et informatique pour l'archivage massif de données et le traitement décentralisé (*Big Data* et *Edge Computing*, pour la Spécialité IoT)

Heures d'enseignement

En/Su	Encadrement / Suivi	80h

Pré-requis obligatoires

* Base de l'Internet des Objets (UE7 du semestre 6)
* Transmission et Traitement de l'information (UE2 du semestre 7)
* Sécurité des protocoles réseaux (UE7 du semestre 8 pour la spécialité Cyber)
* Capteurs pour l'industrie 4.0 (UE7 du semestre 8 pour la spécialité IoT)
* Mathématiques de la cryptographie

Modalités de contrôle des connaissances

Session 1 ou session unique - Contrôle des connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Nombre	Coefficient	Remarques
Cours Magistral	CC (contrôle continu)	Ecrit sur table				
Travaux Pratiques	CC (contrôle continu)	Production écrite				

Session 2 - Contrôle des connaissances

Nature de l'enseignement	Modalité	Nature	Durée (min.)	Nombre	Coefficient	Remarques
Cours Magistral	CC (contrôle continu) 2nde chance	Ecrit sur table				
Travaux Pratiques	CC (contrôle continu) 2nde chance	Production écrite				