PROPOSITION DE SUJET
PROJET TECHNIQUE DE FIN DE E3
2ème SEMESTRE 2019/2020

Fiche à transmettre par mail à **l'un des enseignants** responsables de l'organisation des projets de fin d'année, suivant la teneur du projet :

D. Bureau (Informatique) denis.bureau@esiee.fr
C. Delabie (Ingénierie des Systèmes Intelligents) christophe.delabie@esiee.fr
P. Poulichet (Santé, Energie et Environnement) patrick.poulichet@esiee.fr

NOMS DES ÉLÈVES (4 minimum obligatoirement) :

1. BONANDRINI Vassia
2. BRETON Yann
3. LEGEAY Tom
4. BENGRICHE Saïd

TITRE DU PROJET :

Mise en place et configuration d'une plateforme de détection d'intrusion basée sur Security Onion pour une utilisation personnelle

MOTS-CLÉS :

Cyberdéfense, IDS, IPS, analyse du trafic, sécurité réseaux.

DESCRIPTION DU PROJET :

Security Onion est une distribution Linux (basée sur Ubuntu) spécialisée dans la sécurité et dont les ressources matérielles nécessaires pour l'installation sont relativement importantes. Elle inclut:

- La capture et sauvegarde de trafic,
- La journalisation d'événements,
- Des outils d'analyse et rapports,
- Surveiller un accès Internet résidentiel/d'une petite entreprise.

Notre projet consiste à pouvoir installer et configurer Security Onion sur un PC basique voire Raspberry.

TRAVAIL À RÉALISER :

Nous allons voir comment les différents logiciels inclus dans Security Onion fonctionnent et réaliser des guides d'installation et de configuration. De plus, nous allons choisir quels logiciels nous inclurons dans notre solution pour que notre plateforme puisse fonctionner sur un PC basique. Nous allons ensuite simuler des attaques pour voir si la solution fonctionne bien.

OUTILS MATÉRIELS / LOGICIELS SUPPORT :

PC, Virtualbox, Raspberry
Outils d'analyseur d'alertes : Snorby, Squert, Sguil, ELK, ELSA, NIDS (Snort/Suricata)

Accord du responsable de projet de fin d'année du département :

Le / / 2020