**Sujet de projet pour l’UV5.4**

Résumé

**Titre : Simulation de système d’information et interception d’évènements applicatifs**

**Mots-Clefs : Hynesim, écoute d’application**

**Compétences développées par l’élève :**

Utilisation de la plateforme de simulation de réseau Hynesim

Monitoring d’application

**Acronyme : SnifHynesim**

Encadrement du projet

**Encadrant(s)** (Nom, Prénom, Organisme, Email, Tél.) :

**Ciprian.teodorov@ensta-bretagne.fr**

**Joel.champeau@ensta-bretagne.fr**

Outils envisagés

**Matériel :**

**Logiciel :**

**Hynesim**

Références

**URLs :**

https://www.hynesim.org/

**Ouvrages :**

**Articles :**

Budget nécessaire

**Type de dépense :**

**Montant :**

Description du sujet

Le domaine de la cybersécurité cherche développer des simulateurs pour analyser ou reproduire des systèmes d’information afin notamment de tester des scénarios d’attaques sur des systèmes reproduits à l’identique.

Des simulateurs de système d’information comme Hynesim utilisent les technologies de virtualisation de machine pour offrir une capacité de simulation d’un réseau de machines intégrant tout type de support (ordinateurs, routeurs, switchs) et d’OS (windows, Linux,…). Une fois le réseau virtualisé, nous pouvons exécuter toutes les applications possibles sur chacune des machines et ainsi dérouler tous les scénarios d’attaques possibles.

Si nous voulons monitorer le fonctionnement des applications s’exécutant dans les différentes machines virtuelles, nous pouvons développer des sondes dédiées aux applications dans le simulateur de système d’information Hynesim.

Pour se faire, nous allons nous baser sur des applications du web qui possèdent des API REST ouvertes (comme Facebook par exemple : <https://developers.facebook.com/docs/graph-api>) et écrire des points de monitoring de ces API dans Hynesim.

Si les points de monitoring fonctionnent, nous serons amenés à définir de scripts de génération automatique de code pour ces points de monitoring.

Nombre d’élèves visé

1 élève