TD2 : Sécurité et monitoring
V2.0.0

Document en ligne : mickael.martin.nevot.free.fr

Travail : **groupe de demi-promotion**

1 Sujet

Il est demandé de participer à un jeu d'entreprise (ou simulation) dans un monde fictif inspiré du réel.

Le travail est effectué en deux équipes. La première équipe endossera le rôle de l'entreprise, la seconde celle du groupe de *black hats*.

L'**animation** du jeu d'entreprise sera effectuée par l'enseignant. Il décide également des **conséquences** des **actions** effectuées.

2 Équipes

2.1 Entreprise

Vous recevez la charge de la sécurité informatique et du monitoring d'une entreprise de jeux offrant au moins une partie de ces fonctionnalités en ligne et n'ayant, initialement, aucune politique sécuritaire.

Votre **objectif** est de défendre du mieux que possible votre entreprise face à l'attaque des *black hats.*

2.2 Groupe de *black hats*

Vous êtes un groupe de *black hats.*

Votre **objectif** est de pirater le plus en profondeur possible l'entreprise.

3 Déroulement du jeu :

Le jeu est découpé en **cinq phases.**

À chaque phase, vous devrez choisir un certain nombre d'**actions** (respectivement défensives ou offensives) en vous aidant du cours. Elles doivent être gardées secrètes.

À la fin de chaque phase, les **actions offensives ou défensives détectées** et leurs **conséquences** vous seront communiqués par l'animateur.

3.1 Phase 0 (30 minutes)

Présentation du jeu par l'enseignant, constitution des **groupes** d'étudiants.

3.2 Phase 1 (50 minutes)

Le groupe de l'entreprise doit choisir **six actions défensives** préventives comme base de la sécurité informatique de l'ensemble de son réseau.

Le groupe de *black hats* doit choisir **six actions offensives** pour tenter de pirater l'ensemble du réseau de l'entreprise.

3.3 Phases 2 à 5 (10 minutes)

Le groupe de l'entreprise doit choisir **deux actions défensives** préventives **supplémentaire** pour la sécurité informatique de l'ensemble de son réseau.

Le groupe de *black hats* doit choisir **deux actions offensives supplémentaires** pour continuer de tenter de pirater l'ensemble du réseau de l'entreprise.