

## Création d'un jeu de carte

Objectif : combiner les éléments de protection des réseaux avec leur rôle fonctionnel afin de mettre en œuvre des situations d'attaque afin de forcer les participants à bloquer ou contourner une attaque. Le jeu de carte doit comprendre les éléments fixes suivants :

- Une base qui sera la voie d'entrée du réseau (modem)
- Une liste de point d'attaque possible pouvant être :
  - Un serveur de base de données
  - Un serveur de sauvegarde des données
  - Un poste de travail

Les éléments de construction (ou sécurisation du réseau) pourront être les suivants :

- pare-feu
- tunnel vpn
- routeur
- hub
- proxy
- IDS/IPS

### Les règles du jeu

Dès le début du jeu les joueurs placent la voie d'entrée (modem) et piochent au hasard une voie de sortie de leur infrastructure. Ensuite ils piocheront 5 cartes dans les deux piles respectives suivantes :

- Route de connexion (voir si l'on insère plusieurs types en fonction des technologies ou si les routes sont considérées comme universelles quelque soient les éléments qu'elles interconnectent).
- Éléments de construction du réseau (présents dans la liste précédente)

### L'enchaînement

À chaque tour un joueur devra tirer une carte de la pile événement. Ces événements pourront être les suivants :

survenance d'une attaque dont voici les types : DOS, Brute force, DDOS, MITM, SQL Dump, IP Spoofing, ARP Poisoning

soit une modification d'un élément de construction dont voici les types : dotation d'un protocole, modification des droits d'accès, changement de port, définition d'une règle de routage

Un joueur aura le droit de poser une attaque par tour sur le réseau adverse ou une modification par tour sur son réseau. La carte d'attaque cible un élément du réseau ou l'élément de sortie. Pour la désactiver le joueur subissant l'attaque devra utiliser une carte de modification qui lui permettra de lever l'attaque (ex : DOS / définition d'une règle de bannissement sur scope d'adresse IP...).

Enfin le joueur pourra à la fin du tour se défausser d'une carte pour ensuite piocher une autre afin de changer un élément de construction du réseau en sa possession. Les cartes « route de connexion » seront illimitées et utilisables à volonté par l'ensemble des joueurs.

### Les conditions de fin de jeu

La règle du jeu est que le premier joueur à avoir posé tous les éléments de réseaux en sa possession en début de partie et qui ne possède plus d'attaque en cours sur son système d'information aura gagné la partie.

La structure des types de cartes

Les éléments de constructions et les voies d'entrées et de sortie seront composés des éléments suivants :

Nom

Type d'OS

Version de l'OS

Protocole activé

Port activé

Les cartes d'attaques auront les propriétés suivantes

Nom de l'attaque

Cible de l'attaque

Effet de l'attaque

Les cartes de modification auront les propriétés suivantes

Nom de la modification

Matériel pouvant être ciblé par la modification

Effet de la modification