TD - Attaque par Déni de Service (DoS)

Exercice 1 :

Afin de mettre en œuvre l'attaque DoS Flood classique, l'attaquant doit générer un nombre suffisamment important de paquets pour dépasser la capacité de la liaison vers l'organisation cible. Considérons une attaque utilisant des paquets ICMP echo request (ping) d'une taille de 500 octets (en ignorant les entêtes de trames). Combien de paquets par seconde l'attaquant doit-il envoyer pour inonder une organisation cible à l'aide d'une liaison à 0,5 Mbps? Combien de paquets par seconde si l'attaquant utilise une liaison 2 Mbps? Ou une liaison 10 Mbps?

Exercice 2 :

À l'aide d'une attaque TCP SYN spoofing, l'attaquant vise à inonder la table de demandes de connexion TCP sur un système afin qu'il ne puisse pas répondre aux demandes de connexion légitimes. Prenons un système serveur avec une table pour 256 demandes de connexion. Ce système réessayera d'envoyer le paquet SYN-ACK cinq fois s'il ne reçoit pas de paquet ACK en réponse, à un intervalle total de 30 secondes pour les cinq ACKs, avant de purger la demande de sa table. Supposons qu'aucune contre-mesure supplémentaire n'est utilisée contre cette attaque et que l'attaquant a rempli cette table avec un flot initial de demandes de connexion. À quel rythme l'attaquant doit-il continuer à envoyer des demandes de connexion TCP à ce système afin de s'assurer que la table reste pleine? En supposant que le paquet TCP SYN a une taille de 40 octets (en ignorant les entêtes de trames), combien de bande passante l'attaquant consomme-t-il pour poursuivre cette attaque?

Exercice 3 :

Considérons une variante distribuée de l'attaque que nous avons expliquée dans l'exercice 1. Supposons que l'attaquant a compromis un certain nombre de PCs à utiliser comme systèmes zombies. Supposons également que chacun de ces systèmes a une bande passante moyenne de 128 kbps.

1. Quel est le nombre maximal de paquets ICMP echo request (ping) de 500 octets qu'un seul PC zombie peut envoyer par seconde?
2. De combien de systèmes zombies l'attaquant aurait-il besoin pour inonder une organisation cible en utilisant
   a. Une liaison à 0,5 Mbps?
   b. Une liaison à 2 Mbps? Ou
   c. Une liaison 10 Mbps?
3. Compte tenu qu'un botnet est composé de plusieurs milliers de systèmes zombies, que pouvez-vous conclure sur la capacité de leur contrôleur à lancer simultanément des attaques DDoS sur plusieurs organisations? Ou sur une grande organisation avec plusieurs liaisons réseau beaucoup plus importantes que celles que nous avons envisagées dans ces problèmes?