Eloïse STEIN
Arthur RAUCH

Mini-projet en sécurité avancée

Détection de scan

1) Le but d'un scan vertical étant de détecter rapidement les ports ouverts d'une machine distante, celui-ci se caractérise par une succession rapide de requête de la part d'une même machine sur un grand nombre de ports connus, ces requêtes n'aboutissant généralement pas à une connection. On peut donc détecter une telle attaque en analysant le trafic afin de localiser cette caractéristique.
2) Les structures de données utilisées sont les structures de données des header Ethernet, IP et TCP afin de récupérer les IP et ports des host.
3) Si un host a tenté au moins 50 requêtes sur des ports différents avec un intervalle d'émission inférieur à 10ms, on considère que l'host effectue un scan.
   Notre algorithme est composé d'un tableau dynamique associant chaque ip host à un compteur stockant le nombre de requêtes de ports différents émises avec un intervalle de temps de moins de 10ms. Le programme parcourt la liste de paquets stockés dans un fichier de capture pcap afin de remplir ce tableau.
4) Voir projet.
5) Voir projet.