TD-Projet : Mise en pratique d'implémentation de protocole en python via Scapy (6 heures)

23 octobre 2023

L'objectif de ce Projet est de changer de perspective, d'utilisateur de protocole nous allons passer au statut de développeur / implémenteur. Vous aurez plusieurs sujets à choisir parmi ceux proposés sur moodle et chacun abordera un aspect "sécurité". En choisissant votre groupe, vous choisissez le projet qui vous intéresse.
Les programmes devront être réalisés en Python avec la librairie Scapy, vous trouverez des ressources sur moodle pour créer un protocole.

1 Liste des sujets proposés

Voici la liste des sujets proposés pour 2023 - 2024 :

- Sujet 1 - Exfiltration DNS (2 personnes) : C'est pas le tout de trouver des données dans un réseau, il faut également les faire sortir.
- Sujet 2 - Command and control (2 personnes) : Je commande et tu obéis, what else ?
- Sujet 3 - Exfiltration ICMP (2 personnes) : Un ping ça ne sert qu'à tester les équipements, vraiment ?
- Sujet 4 - Attaque par rebond (4 personnes) : Quatre type d'attaque par rebond à implémenter, ça c'est du challenge !
- Sujet 5 - Attaque DNS et DHCP (2 personnes) : Tu oses attaquer mon DNS ? Tu as eu une bonne idée de te mettre en DHCP !
- Sujet 6 - Anonymous conversation (4 personnes) : Pourrait-on vraiment être anonyme sous le regard bienveillant de Big Brother.
- Sujet 7 - Le choc des titans (3 personnes) : Un scénario épique entre des artistes du protocole ARP. Il ne pourra en rester qu'un mais, lequel ?

Attention, les scénarios ne sont acceptés qu'avec l'accord de chacun et ne devront, en aucun cas, avoir lieu sur le réseau de l'UBS. Le but est de comprendre comment certaines vulnérabilités des protocoles peuvent être exploitées. Les participants sont invités à utiliser un partage de connexion en 4G ou bien à aller sur l'environnement virtuel du module de système d'exploitation.

Dans le cas où, certains seraient choqués par les sujets proposés, n'hésitez pas à vous manifester, des menus enfants peuvent être proposés pour des groupes allant de deux à trois personnes (bataille navale, pierre / feuille / ciseau, flipper protocol, trouve le numéro auquel je pense, action ou vérité, robobrol).

2 Rendu

Pour un démonstrateur, le système de rendu choisi est la courte capsule vidéo (5 minutes maximums). Dans cette capsule vous devrez indiquer :

- Le noms des membres du groupe
- Une brève explication de ce que fait votre programme
- Une démonstration montrant également les commandes de lancement des programmes. Il va de soit que tout doit être mis en oeuvre pour prouver le comportement attendu du programme. Si ce dernier doit envoyer un ping, il faut qu'on puisse le voir, par exemple via Wireshark.
- Le niveau fonctionnel de vos programmes (ça peut être sous forme de tableau synthétique s'il y en a plusieurs) :
  - Niveau 5 : Fonctionne parfaitement, testé sur plus de 50 paquets à suivre.
  - Niveau 4 : Fonctionne parfaitement sur les 2 tests que j'ai pu faire.
  - Niveau 3 : Fonctionne partiellement
  - Niveau 2 : Non Fonctionnel
  - Niveau 1 : Non commencé, rien fait

Vous pourrez utiliser "kdenlive" pour faire le montage vidéo au besoin (application gratuite fonctionnant sur tous les systèmes d'exploitation).

Il y aura, pour chaque séance et comme pour le TP précédent un rapport d'activité synthétique à remplir (un par groupe suffira, de préférence toujours de la même personne, c'est plus simple à suivre lors de la correction).

Tous les programmes réalisés ainsi que la capsule devront être déposés sur Moodle pour le 01/12/2023 à 23h55 au plus tard. Prenez de l'avance pour faire le dépôt et déposez-le dès 22h au plus tard, **Dépôts par mail non acceptés**. Aucun délai supplémentaire ne pourra être accordé car la correction débutera directement après.