Description

Objectif et contexte

Cette SAE avait pour objectif de nous initier à l'analyse du trafic réseau en utilisant des outils comme Scapy et Wireshark. Pour observer, filtrer, décrypter et comprendre les échanges réseau.

Le projet comprenait une série de challenges pratiques portant sur différents protocoles (ICMP, FTP, TELNET, HTTP), et l'exploitation de captures réseau au format .pcap/.pcapng.

Cahier des charges

Nous devions :

- Maîtriser l'environnement Scapy en Python
- Lire et interpréter des captures réseau fournies
- Détecter et extraire des informations sensibles id, mots de passe, fichiers transférés
- Développer des scripts Python d'analyse réseau en temps réel
- Résoudre plusieurs challenges pratiques en lien avec des protocoles réseau réels FTP, TELNET, HTTP

Travaux et résultats obtenus

Organisation du travail

Le travail s'est fait en binôme, en autonomie chacun de son côté.

Travaux réalisés et résultats obtenus

- Découverte et configuration de Scapy
- Analyse de captures ICMP et ICMPv6, avec inspection des en-têtes et des trames échangées
- Extraction et analyse d'une session FTP : récupération du fichier transféré ftpdoc.odt et décryptage du message avec un script Python pour le code César avancé
- Écriture d'un sniffer FTP temps réel avec capable de capturer en clair les identifiants et mots de passe sur le port 21
- Analyse et sniffing d'une session TELNET : récupération des identifiants
- Analyse et sniffing d'une session HTTP

Partie réflexive

Les + et les - du projet

Les + :

- SAE très concrète, avec des résultats visibles et motivants
- Apprentissage de Scapy
- Aspect cybersécurité stimulant, notamment la récupération d'identifiants clairs ou chiffrés même si ce n'est pas mon domaine d'étude pour plus tard

Les - :

- Certaines parties sont complexes à débugger
- Bonne maîtrise de Python pour aller au bout des challenges
- Peu d'encadrement sur les techniques d'analyse