DOCUMENTATION PROJET - ANALYSE DDoS AVEC WIRESHARK

1. CONTEXTE DU PROJET

Test d'intrusion et analyse forensique d'une attaque DDoS de type SYN Flood en environnement contrôlé. L'objectif était de maîtriser l'analyse réseau.

2. MÉTHODOLOGIE

•Environnement : Laboratoire virtuel isolé avec Kali Linux et Metasploitable2
•Attaque : SYN Flood ciblant le service web Apache (port 80)
•Outil d'analyse : Wireshark pour la capture et l'analyse du trafic
•Durée : 1 journée complète

3. ÉTAPES RÉALISÉES

•Configuration de l'environnement de test sécurisé
•Exécution contrôlée de l'attaque DDoS avec hping3
•Capture complète du trafic réseau
•Analyse forensique des paquets malveillants
•Documentation des impacts et indicateurs de compromission

4. RÉSULTATS OBTENUS

•Identification claire du pattern d'attaque SYN Flood
•Mesure de l'impact sur la disponibilité du service (indisponibilité totale)
•Capture d'écran démontrant le pic de trafic anormal

5. COMPÉTENCES DÉMONTRÉES

•Analyse réseau avec Wireshark
•Méthodologie d'investigation forensique
•Gestion d'environnement de test sécurisé

6. CONCLUSION

Ce projet a validé la capacité à détecter et analyser des attaques DDos démontrant des compétences techniques en cybersécurité offensive et défensive.