FICHE DE RÉVISION – LAB 1 (PARTIE 2)

Analyse DNS – Exfiltration de données

Objectif
Identifier une exfiltration de données via DNS à partir des logs Security Onion / Kibana.

Pourquoi analyser le DNS ?
Le DNS est souvent autorisé par les pare-feux. Les attaquants l'utilisent pour exfiltrer discrètement des données encodées.

Étape 1 : Filtrer le trafic DNS
Dans Kibana, section *Zeek Hunting* → cliquer sur **DNS**.

Étape 2 : Examiner les entrées DNS
Observer les types de requêtes DNS : A, AAAA, PTR, NB.
Vérifier les codes de réponse DNS.

Étape 3 : Identifier clients et serveurs DNS
Repérer les IPs du DNS Client (machine infectée) et du DNS Server (serveur contacté).

Étape 4 : Détection d'anomalie
Observer les requêtes avec des sous-domaines anormalement longs vers **ns.example.com**.
Ces chaînes contiennent uniquement des caractères hexadécimaux (0-9, a-f).

Étape 5 : Export des requêtes
Cliquer sur *Export: Raw* pour télécharger les requêtes DNS en CSV.

Étape 6 : Nettoyage du fichier
Supprimer : guillemets, domaines, virgules.
Garder uniquement l'hexadécimal.

Étape 7 : Décodage
Commande :
xxd -r -p DNS-Queries.csv > secret.txt
Puis : *cat secret.txt*

Résultat
Le message décodé révèle un document confidentiel exfiltré.

Conclusion Examen
Les requêtes DNS contiennent des données encodées utilisées pour exfiltrer des informations sensibles. Ceci confirme une attaque avancée de type DNS tunneling.