Cours : Les Techniques d’Exploration en Ethical Hacking

🔎 1. Qu’est-ce que l’exploration ?

L’**exploration**, ou **reconnaissance**, est la première phase active du hacking éthique. Elle consiste à **collecter des informations sur une cible** (entreprise, site web, serveur, réseau) pour identifier les points faibles potentiels avant une attaque simulée.

Elle peut être **passive** (discrète, sans contact direct avec la cible) ou **active** (avec interaction directe).

□ 2. Objectifs de l’exploration

- Identifier les adresses IP, noms de domaine, sous-domaines
- Connaître les systèmes d’exploitation utilisés
- Découvrir les ports ouverts et services actifs
- Cartographier l’infrastructure réseau
- Recueillir des informations sur le personnel (ingénierie sociale)

□ 3. Types d’exploration

1. Exploration passive

- Aucune interaction directe avec la cible
- Utilise des sources publiques : moteurs de recherche, DNS, réseaux sociaux

2. Exploration active

- Interaction directe avec la cible (ex. ping, scan de ports)
- Risque d’être détecté

🛠 4. Techniques et outils d'exploration

🗃 A. Footprinting (Empreinte)

Collecte d'informations générales :

- Whois : Informations sur le nom de domaine
- DNS enumeration : sous-domaines, serveurs mail (avec `nslookup`, `dig`, etc.)
- Google hacking (dorks)
- Recherche sur les employés (LinkedIn, Facebook…)

🛠 Outils :

- `whois`, `theHarvester`, `Recon-ng`, Google Dorks

📡 B. Scanning réseau

- Identifier les hôtes actifs (live hosts)
- Repérer les ports ouverts
- Détecter les services et versions installées

🛠 Outils :

- `Nmap` : scan d'hôtes, de ports, détection OS
- `Masscan` : scan rapide
- `Netcat` : test de connectivité sur un port

Exemples de commandes :

```
nmap -sP 192.168.1.0/24        # Scan ping (live hosts)
nmap -sS -p- 192.168.1.1       # Scan TCP furtif sur tous les ports
nmap -A 192.168.1.1            # OS detection + version + script
```

□ C. Enumeration

Approfondir les infos sur les services détectés :

- Enumération des utilisateurs (FTP, SMB, LDAP…)
- Recherche de versions vulnérables

🛠 Outils :

- `enum4linux` (SMB/NetBIOS)
- `SNMPwalk`
- `Nikto` (serveurs web)
- `Gobuster`, `Dirb` (bruteforce de répertoires web)

🌐 D. OSINT (Open Source Intelligence)

Utilisation des sources ouvertes pour recueillir des infos :

- Fuites de données
- Emails exposés
- Fichiers sensibles

🛠 Outils :

- `Maltego`, `SpiderFoot`, `Shodan`, `Google Dorks`

---

5. Exemple de scénario d'exploration

Objectif : cartographier un site web d'entreprise

1. Utilisation de `whois` pour récupérer les informations du domaine.
2. `nslookup` et `dig` pour découvrir les sous-domaines.
3. Utilisation de `theHarvester` pour trouver des adresses email.
4. Scan réseau avec `nmap` pour découvrir les ports ouverts.
5. Analyse des services avec `nmap -A` pour trouver la version d'Apache.
6. Scan web avec `Nikto` et `Gobuster`.

⚠ 6. Précautions à prendre

- 🔒 Toujours obtenir l'autorisation avant de scanner une cible !
- Respecter la confidentialité des données découvertes
- 🌲 Utiliser des proxys ou VPN pour ne pas révéler votre adresse IP en testant des environnements autorisés

---

📚 7. Ressources complémentaires

- https://nmap.org
- https://shodan.io
- https://osintframework.com
- Livre : *Nmap Network Scanning* – Gordon Fyodor Lyon
