Kali linux sans internet

1. **Scan des réseaux WiFi**

- **Commande :** `airodump-ng`
- **Description :** Utilisez `airodump-ng` pour scanner les réseaux WiFi disponibles et capturer les paquets pour analyser les trames de données.
- **Exemple :**

```
airodump-ng wlan0
```

2. **Détection des clients connectés**

- **Commande :** `airodump-ng`
- **Description :** Vous pouvez utiliser `airodump-ng` pour détecter les clients connectés à un réseau WiFi spécifique.
- **Exemple :**

```
airodump-ng --bssid <BSSID> -c <channel> wlan0
```

3. **Capture des paquets de données**

- **Commande :** `airodump-ng`
- **Description :** Capturez les paquets de données pour analyser les trames de données et détecter les vulnérabilités.
- **Exemple :**

```
airodump-ng --bssid <BSSID> -c <channel> -w capture wlan0
```

4. **Déchiffrement des paquets WEP**

- **Commande :** `aircrack-ng`
- **Description :** Utilisez `aircrack-ng` pour déchiffrer les paquets WEP capturés.
- **Exemple :**

```
aircrack-ng -b <BSSID> -w <wordlist> capture-01.cap
```

5. **Attaque de type Deauthentication**

- **Commande :** `aireplay-ng`
- **Description :** Forcez les clients à se reconnecter pour capturer des paquets de données.
- **Exemple :**

```
aireplay-ng --deauth 10 -a <BSSID> wlan0
```

6. **Attaque de type WPA/WPA2 PSK**

- **Commande :** `aircrack-ng`
- **Description :** Utilisez `aircrack-ng` pour attaquer les réseaux WPA/WPA2 en utilisant une attaque par force brute.
- **Exemple :**

```
aircrack-ng -b <BSSID> -w <wordlist> capture-01.cap
```

7. **Analyse des vulnérabilités**

- **Commande :** `nmap`
- **Description :** Utilisez `nmap` pour scanner les ports ouverts et détecter les vulnérabilités sur les périphériques connectés.
- **Exemple :**

```
nmap -sV <target_ip>
```

8. **Exploitation des vulnérabilités**

- **Commande :** `metasploit`
- **Description :** Utilisez Metasploit pour exploiter les vulnérabilités détectées.
- **Exemple :**

```
msfconsole

use exploit/<path_to_exploit>

set RHOST <target_ip>
run
```

9. **Post-exploitation**

- **Commande :** `metasploit`
- **Description :** Après avoir exploité une vulnérabilité, vous pouvez utiliser Metasploit pour effectuer des actions post-exploitation, telles que l'installation de backdoors ou le vol de données.
- **Exemple :**

```
use post/windows/gather/credentials

set SESSION <session_id>
run
```

10. **Capture des paquets avec Wireshark**

- **Commande :** `wireshark`

- **Description :** Utilisez Wireshark pour capturer et analyser les paquets réseau en temps réel. Cela peut aider à identifier des vulnérabilités spécifiques et à comprendre le trafic réseau.
- **Exemple :**

```
wireshark
```

11. **Attaque de type Evil Twin**

- **Commande :** `hostapd`
- **Description :** Créez un faux point d'accès WiFi pour capturer les données des clients connectés.
- **Exemple :**

```
hostapd /etc/hostapd.conf
```

12. **Analyse des fichiers de configuration**

- **Commande :** `cat`
- **Description :** Examinez les fichiers de configuration des réseaux WiFi pour identifier des informations sensibles ou des vulnérabilités.
- **Exemple :**

```
cat /etc/hostapd.conf
```

13. **Utilisation de Kismet**

- **Commande :** `kismet`
- **Description :** Kismet est un outil de détection et d'analyse des réseaux sans fil. Il peut être utilisé pour scanner les réseaux WiFi et détecter les vulnérabilités.
- **Exemple :**

```
kismet
```

14. **Attaque de type Man-in-the-Middle (MitM)**

- **Commande :** `ettercap`
- **Description :** Utilisez Ettercap pour intercepter et manipuler le trafic réseau entre deux parties.
- **Exemple :**

```
ettercap -G
```

15. **Analyse des logs**

- **Commande :** `tail`
- **Description :** Examinez les logs des systèmes pour identifier des activités suspectes ou des vulnérabilités.

- **Exemple :**

```
tail -f /var/log/syslog
```

Revision #1
Created 2 April 2026 08:51:15 by Raphaël
Updated 2 April 2026 08:51:33 by Raphaël