Mission 9 — Tester les protections avec Kali

Objectif : Prouver que Port-Security, DHCP Snooping, Dynamic ARP Inspection, ACL/pare-feu, Wi-Fi résistent, et que tout est journalisé sur le serveur de logs.
Cas de test :

Port-Security

1. Brancher PC-A (MAC-1) → OK.
2. Remplacer par Kali (MAC-2) → violation attendue.
3. Vérifier :

```
show port-security interface GiX/Y
show logging
```

--> Sur rsyslog, il doit y avoir une alerte !!!

DHCP Snooping
Sur Kali :

```
sudo dhclient -v eth0
```

--> Tenter faux serveur (sur port non-trusted) --> Il doit échouer côté client

Vérifier dans Wireshark --> Filtrer "bootp" + logs switch.

DAI (ARP Inspection)
Observation de l'ARP :

```
sudo arp-scan --interface eth0 --localnet
```

Tenter ARP spoof (poste de test) --> DAI doit le bloquer

Pour le contrôler :

```
show ip arp inspection statistics
show logging
```

--> Faire une capture Wireshark filtre arp

ACL/Pare-feu routeur

Depuis Kali (VLAN test), scanner services admin routeur/NAS :

```
nmap -sS -p 22,23,80,443,161,514 (IP routeur)
```

Essais directs (doivent normalement échouer) :

```
ssh admin@172.16.0.1
curl -k https://172.16.0.1
```

→ Attendu : **inaccessible** (filtré). Logs côté routeur/rsyslog

Borne de test
Recon :

```
sudo airmon-ng start wlan0
airodump-ng wlan0mon
```

Traçabilité
Test

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

Heure (NTP) cohérent et avec des événements (routeur + switch).

BONUS (IL FAUT DEMANDER) :

- **Ettercap/Bettercap** (démonstration DAI)
- **John the Ripper** (hash fourni)

Pour effectuer un test de pénétration sur une borne WiFi en utilisant Kali Linux, vous pouvez suivre ces étapes et utiliser les commandes appropriées. Ces étapes simulent une attaque pour évaluer les vulnérabilités du réseau WiFi.

1. **Analyse du réseau WiFi**

Commande : `airodump-ng`

Description : Cette commande permet de scanner les réseaux WiFi disponibles et de 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
```

Ces commandes et étapes vous permettront de réaliser un test de pénétration complet sur une borne WiFi, en identifiant et exploitant les vulnérabilités potentielles.

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 vulnérabilités avec Nessus**

Commande : `nessus`
Description : Nessus est un outil de scan de vulnérabilités qui peut être utilisé pour identifier les failles de sécurité sur les réseaux WiFi.
Exemple :

```
nessus
```

16. **Exploitation des vulnérabilités avec Metasploit**

Commande : `metasploit`
Description : Utilisez Metasploit pour exploiter les vulnérabilités identifiées. Metasploit offre une large gamme d'exploits et de payloads pour différentes vulnérabilités.
Exemple :

```
msfconsole

use exploit/<path_to_exploit>

set RHOST <target_ip>
run
```

17. **Post-exploitation avec Metasploit**

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
```

18. **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
```

- **Commande :** `aircrack-ng`
- **Description :** Utilisez Aircrack-ng pour attaquer les réseaux WPA/WPA2 en utilisant une atta

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

Revision #6
Created 15 March 2026 22:12:46 by Raphaël
Updated 2 April 2026 08:05:32 by Raphaël

20. Utilisation de Wireshark pour la capture des paquets

Commande wireshark