Guide des Commandes

Cybersécurité - Détection de Scan de Ports

”

1 Installation (une seule fois)

Ces commandes sont à exécuter une seule fois au début du Lab pour préparer l'environnement.

1.1 Mise à jour du système

```
# Mettre a jour la liste des paquets
sudo apt update
```

1.2 Installation des outils nécessaires

```
# Installer Python, pip et Nmap
sudo apt install python3 python3-pip nmap -y
```

1.3 Installation de la bibliothèque Scapy

```
# Installer Scapy pour manipulation de paquets
pip3 install scapy
```

1.4 Configuration des permissions

```
# Donner les permissions de capture reseau a Python
sudo setcap cap_net_raw,cap_net_admin=eip $(which python3)
```

Important

Sans ces permissions, le script ne pourra pas capturer les paquets réseau et affichera une erreur ”Permission denied”.

2 Vérification de l'interface réseau

Avant de lancer le détecteur, vous devez identifier le nom de votre interface réseau.

2.1 Lister les interfaces disponibles

```
# Afficher toutes les interfaces reseau
ip addr show
```

2.2 Interfaces courantes

— `eth0` ou `enp0s3` : Connexion Ethernet câblée
— `wlan0` ou `wlp2s0` : Connexion Wi-Fi
— `lo` : Interface loopback (localhost)

✔ Astuce

Notez le nom exact de votre interface (par exemple : `eth0`). Vous en aurez besoin pour lancer le détecteur.

3 Lancement du détecteur

3.1 Démarrer le script (Terminal 1)

```
# Lancer le detecteur sur l'interface eth0
sudo python3 port_scan_detector.py eth0
```

Remplacez `eth0` par le nom de votre interface réseau identifiée précédemment.

3.2 Sortie attendue

Vous devriez voir s'afficher :

```
[+] Detecteur de scan de ports initialise
[+] Interface: eth0
[+] Seuil d'alerte: 10 ports en 60s
============================================================
[+] Demarrage de la surveillance...
[+] Appuyez sur Ctrl+C pour arreter
```

Le détecteur est maintenant actif et surveille le trafic réseau.

4 Génération de scans de ports

Ouvrez un **second terminal** pour générer des scans et déclencher les alertes.

4.1 Test 1 : Scan simple de 20 ports

```
# Scanner les ports 1 a 20 sur localhost
nmap -p 1-20 localhost
```

4.2 Test 2 : Scan rapide (100 ports courants)

```
# Scan rapide des ports les plus utilises
nmap -F localhost
```

4.3 Test 3 : Scan furtif (SYN scan)

```
# Scan furtif de 100 ports
nmap -sS -p 1-100 localhost
```

4.4 Test 4 : Scanner une autre machine

```
# Scanner une autre adresse IP (remplacez par une IP de votre reseau)
nmap -p 1-50 192.168.1.1
```

Avertissement

Ne scannez **JAMAIS** une machine qui ne vous appartient pas sans autorisation explicite. C'est illégal et peut être considéré comme une tentative d'intrusion.

5 Observation des alertes

5.1 Alerte en temps réel

Dans le terminal où tourne le détecteur, vous devriez voir apparaître :

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
ALERTE DE SECURITE - SCAN DE PORTS DETECTE
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Timestamp: 2024-11-03 14:23:45
IP Source: 127.0.0.1
Nombre de ports scannes: 15
Ports: [21, 22, 23, 25, 80, 443, 3306, ...]
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

5.2 Consulter le fichier de logs

Les alertes sont également enregistrées dans un fichier.

5.2.1 Afficher tout le contenu

```
# Voir toutes les alertes enregistrees
cat scan_alerts.log
```

5.2.2 Suivre les alertes en temps réel

```
# Suivre l'ajout de nouvelles alertes en direct
tail -f scan_alerts.log
```

5.3 Format du fichier log

Chaque ligne du fichier `scan_alerts.log` contient :

```
2024-11-03 14:23:45 | SCAN_DETECTED | 127.0.0.1 | 15 ports
```

Format : `Timestamp | Type | IP Source | Nombre de ports`

6 Arrêt du détecteur

6.1 Arrêt propre

Dans le terminal du détecteur, appuyez sur :

`Ctrl + C`

6.2 Statistiques finales

Le détecteur affichera automatiquement les statistiques avant de s'arrêter :

```
============================================================
STATISTIQUES
============================================================
IPs suspectes detectees: 1
  - 127.0.0.1: 15 ports scannes
============================================================
```

7 Fichiers du Lab

Fichier	Description
port_scan_detector.py	Script Python principal de détection
Lab_detection_scan.tex	Sujet du Lab au format LaTeX
scan_alerts.log	Fichier de logs (généré automatiquement)
guide_commandes.tex	Ce guide de commandes

TABLE 1 – Fichiers du projet

8 Dépannage

8.1 Erreur : "Permission denied"

Cause : Pas de permissions pour capturer les paquets.
Solution :

```
sudo setcap cap_net_raw,cap_net_admin=eip $(which python3)
# OU lancer avec sudo
sudo python3 port_scan_detector.py eth0
```

8.2 Erreur : "No module named 'scapy'"

Cause : Scapy n'est pas installé.
Solution :

```
pip3 install scapy
# OU avec sudo
sudo pip3 install scapy
```

8.3 Erreur : "Interface not found"

Cause : Nom d'interface incorrect.
Solution :

```
# Verifier le nom exact de votre interface
ip addr show
# Puis utiliser le bon nom
sudo python3 port_scan_detector.py <nom_interface>
```

8.4 Aucune alerte ne s'affiche

Cause : Seuil non atteint (moins de 10 ports scannés).
Solution :

```
# Scanner plus de ports
nmap -p 1-100 localhost
# OU utiliser un scan rapide
nmap -F localhost
```

9 Éléments à fournir

1. Le fichier `port_scan_detector.py` avec vos commentaires
2. Le fichier `scan_alerts.log` contenant au moins 3 détections
3. Captures d'écran montrant :
   — Le détecteur en cours d'exécution
   — Une alerte affichée
   — Le contenu du fichier de logs

Bon travail !