Scan Reseau avec Nmap

E-Nova - Securite et Audit Reseau

1. Contexte de la Mission

Dans le cadre de mon alternance chez E-Nova, j'utilise l'outil Nmap pour effectuer des scans reseau afin de garantir la securite de l'infrastructure. Ces scans permettent de detecter d'eventuels appareils inconnus sur le reseau et de verifier l'etat des machines en cours de reconditionnement.

2. Presentation de Nmap

Nmap (Network Mapper) est un outil open source d'exploration reseau et d'audit de securite. Il permet de decouvrir les hotes actifs sur un reseau, d'identifier les ports ouverts, de detecter les services en cours d'execution et de reperer d'eventuelles vulnerabilites.

Fonctionnalites principales :

- Decouverte des hotes actifs sur un reseau
- Scan des ports ouverts (TCP/UDP)
- Detection des services et versions
- Identification du systeme d'exploitation
- Detection de vulnerabilites avec des scripts NSE

3. Objectifs des Scans

Objectif 1 : Detecter les appareils inconnus

Verifier qu'aucun appareil non autorise n'est connecte au reseau de l'entreprise. Cela permet de detecter d'eventuelles intrusions ou des appareils oublies.

Objectif 2 : Verifier l'etat des PC en reconditionnement

Avant de livrer un appareil reconditionne, je verifie qu'il n'y a pas de services suspects actifs ou de ports inhabituels ouverts qui pourraient indiquer une infection.

Objectif 3 : Inventaire reseau

Maintenir une vue claire des equipements connectes au reseau de l'atelier.

4. Commandes Utilisees

Scan de decouverte du reseau (Ping Scan)

Cette commande permet de lister tous les appareils actifs sur le reseau sans scanner les ports :

```
nmap -sn 192.168.1.0/24
```

- **-sn** : Desactive le scan de ports, effectue uniquement un ping
- **192.168.1.0/24** : Plage d'adresses a scanner (254 hotes)

Scan des ports TCP courants

Pour verifier les ports ouverts sur une machine specifique :

```
nmap -sT 192.168.1.50
```

- **-sT** : Scan TCP Connect (connexion complete)

Scan de ports specifiques

Pour verifier si des ports sensibles sont ouverts :

```
nmap -p 22,80,443,3389,445 192.168.1.50
```

- **-p** : Specifie les ports a scanner (SSH, HTTP, HTTPS, RDP, SMB)

Detection du systeme d'exploitation

Pour identifier le systeme d'exploitation d'une machine :

```
nmap -O 192.168.1.50
```

- **-O** : Active la detection du systeme d'exploitation

5. Exemple de Resultat

```
Resultat d'un scan sur un PC en reconditionnement :

PORT STATE SERVICE
22/tcp open ssh
80/tcp closed http
443/tcp closed https
3389/tcp open ms-wbt-server (RDP)
445/tcp closed microsoft-ds

Interpretation : Le PC a SSH et RDP actifs (normal pour
l'administration), les autres ports sont fermes (bon signe).
```

6. Analyse et Actions

Ports normaux :

- Port 22 (SSH) : Administration a distance Linux/Mac
- Port 3389 (RDP) : Bureau a distance Windows
- Port 80/443 (HTTP/HTTPS) : Serveur web (si necessaire)

Ports suspects a investiguer :

- Ports inhabituels ouverts (ex: 4444, 5555, 6666...)
- Port 445 ouvert sans raison (risque ransomware)

- Ports de trojans connus

Actions en cas de detection suspecte :

1. Isoler immediatement la machine du reseau
2. Effectuer un scan antivirus complet
3. Verifier les processus en cours d'execution
4. Reinstaller le systeme si necessaire

7. Competences Mobilisees

Competence	Contexte
Audit reseau	Scan et analyse avec Nmap
Securite	Detection d'appareils non autorises
Analyse	Interpretation des resultats de scan
Ligne de commande	Utilisation de Nmap en CLI
Documentation	Rapport des scans effectues

8. Note Importante

Aspect legal : L'utilisation de Nmap est legale uniquement sur les reseaux dont on a l'autorisation. Chez E-Nova, j'effectue ces scans dans le cadre de mes missions et avec l'accord de mon tuteur. Scanner un reseau sans autorisation est illegal.