TCP, UDP, ICMP et diagnostic réseau

Formation : BTS SIO — Option SISR



1. Rôle et fonctionnement

TCP fournit un flux d'octets fiable et ordonné avec établissement de connexion. UDP transporte des datagrammes sans garantir leur livraison ni leur ordre. ICMP sert notamment aux messages de diagnostic ; il ne possède pas de ports TCP ou UDP.

Service	Transport habituel
DNS	UDP et TCP 53
SSH	TCP 22
HTTP / HTTPS	TCP 80 / 443 dans les exemples du laboratoire
NTP	UDP 123
RDP	TCP 3389, UDP possible
WAC de la maquette	TCP 10443

2. Méthode de diagnostic

Procéder du plus proche au plus éloigné : interface locale, VLAN, passerelle, route, filtrage, service, puis DNS. Tester par IP aide à isoler un problème de résolution de noms.

```
ip -br address
ip route
ping -c 4 192.168.3.126
ss -lntup
dig @192.168.3.10 example.org
curl -I http://192.168.3.10
```

La dernière commande n'est pertinente que si un serveur HTTP est attendu sur cette adresse. Pour tester un port précis depuis Windows :

```
Test-NetConnection -ComputerName 192.168.3.209 -Port 8443
tracert 192.168.3.209
```

3. Capture ciblée

```
sudo tcpdump -ni ens18 -c 30 'host 192.168.3.10 and port 53'
```

Une capture contient potentiellement des données sensibles ; choisir un filtre et une durée adaptés. Observer requête et réponse sur le bon lien avant de conclure.

4. Interpréter les résultats

Un ping bloqué ne prouve pas que le service est arrêté. Un port TCP accessible ne prouve pas que l'authentification fonctionne. Une recette doit préciser source, destination, protocole, résultat attendu et observation, avec un test autorisé et un test de refus.

5. Lire une capture : ARP, DNS puis HTTP

Pour un client 172.23.1.15 qui cherche www.debian.org, identifier d'abord sa passerelle et son résolveur. Dans l'exemple étudié, ils sont respectivement 172.23.1.1 et 172.23.1.253.

1. Si l'adresse MAC du résolveur local n'est pas en cache, le client la recherche par ARP.
2. Il interroge le résolveur pour obtenir l'adresse du site.
3. Si la destination se trouve hors du sous-réseau, il envoie les paquets à sa passerelle ; une résolution ARP peut être nécessaire pour cette dernière.
4. La connexion au serveur Web peut ensuite être examinée indépendamment de la résolution DNS.

ARP peut être absent d'une capture si le voisin est déjà connu. Relier les paquets à la chronologie observée plutôt que d'imposer une séquence théorique à toutes les traces.

6. Découverte d'hôtes avec Nmap

Exemples exécutés dans le laboratoire autorisé :

```
sudo nmap -sn 192.168.3.0/25
sudo nmap -sn 192.168.3.128/26
sudo nmap -sn 192.168.3.192/28
sudo nmap -sn 192.168.3.208/29
```

`-sn` effectue une découverte sans scan de ports. Les captures indiquent huit adresses signalées actives dans le premier bloc, puis quatre dans chacun des trois autres.

```
┌──(etudiant㉿kali)-[~]
└─$ sudo nmap -sn 192.168.3.0/25
[sudo] Mot de passe de etudiant :
Starting Nmap 7.99 ( https://nmap.org ) at 2026-10-15 17:25 +0200
Nmap scan report for 192.168.3.3
Host is up (0.0010s latency).
MAC Address: BC:24:11:2E:A4:B2 (Proxmox Server Solutions GmbH)
Nmap scan report for 192.168.3.6
Host is up (0.0013s latency).
MAC Address: BC:24:11:80:05:CF (Proxmox Server Solutions GmbH)
Nmap scan report for 192.168.3.11
Host is up (0.0011s latency).
MAC Address: BC:24:11:C9:EB:48 (Proxmox Server Solutions GmbH)
Nmap scan report for 192.168.3.100
Host is up (0.0054s latency).
MAC Address: 6C:1F:F7:6D:BE:6D (Ugreen Group Limited)
Nmap scan report for 192.168.3.110
Host is up (0.0017s latency).
MAC Address: 08:00:27:5A:87:BC (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.3.111
Host is up (0.0015s latency).
MAC Address: D8:43:AE:E3:C2:78 (Micro-Star Intl)
Nmap scan report for 192.168.3.126
Host is up (0.0023s latency).
MAC Address: A4:11:BB:DC:73:66 (Cisco Systems)
Nmap scan report for kali (192.168.3.125)
Host is up.
Nmap done: 128 IP addresses (8 hosts up) scanned in 2.27 seconds

┌──(etudiant㉿kali)-[~]
└─$
```

Découverte Nmap dans le sous-réseau Production.

```
┌──(etudiant㉿kali)-[~]
└─$ sudo nmap -sn 192.168.3.192/28
Starting Nmap 7.99 ( https://nmap.org ) at 2026-10-15 17:28 +0200
Nmap scan report for 192.168.3.192
Host is up (0.0012s latency).
Nmap scan report for 192.168.3.205
Host is up (0.0023s latency).
Nmap scan report for 192.168.3.206
Host is up (0.0020s latency).
Nmap scan report for 192.168.3.207
Host is up (0.0014s latency).
Nmap done: 16 IP addresses (4 hosts up) scanned in 2.97 seconds

┌──(etudiant㉿kali)-[~]
└─$
```

Résultat observé pour le sous-réseau Administration.

Certaines sorties signalent les adresses réseau ou broadcast comme actives. Ne pas transformer ces réponses en inventaire de machines sans vérification : le routage, les équipements intermédiaires et les réponses reçues peuvent influencer la détection.

7. Scan TCP SYN

```
sudo nmap -sS 192.168.3.126
```

```
┌──(etudiant㉿kali)-[~]
└─$ sudo nmap -sS 192.168.3.126
Starting Nmap 7.99 ( https://nmap.org ) at 2026-10-15 17:32 +0200
Nmap scan report for 192.168.3.126
Host is up (0.0074s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https
MAC Address: A4:11:BB:DC:73:66 (Cisco Systems)

Nmap done: 1 IP address (1 host up) scanned in 3.73 seconds
```

Ports TCP 22, 80 et 443 signalés ouverts sur 192.168.3.126.

La capture affiche 997 ports fermés parmi ceux testés et trois ouverts. Sans détection de version, les noms ssh, http et https correspondent aux associations de ports de Nmap ; ils ne constituent pas une identification complète du logiciel distant.

8. Références

- IETF — TCP
- IETF — UDP
- Debian — tcpdump

From:
https://wiki.ewengadonnaud.xyz/ - **Base de savoir réseaux/cyber/devops**

Permanent link:
https://wiki.ewengadonnaud.xyz/doku.php?id=reseau:diagnostic

Last update: **2026/10/18 01:23**