

---

# Cours : Sécurisation des Réseaux

---

## 1. Introduction

La **sécurité réseau** consiste à protéger l'intégrité, la confidentialité et la disponibilité des données transitant sur un réseau. Elle est essentielle pour empêcher les attaques comme le **sniffing**, le **spoofing**, les **DoS**, les **intrusions**, etc.

---

## ☐ 2. Les piliers de la sécurité réseau (CIA)

Pilier	Signification	Objectif principal
<b>Confidentialité</b>	Empêcher l'accès non autorisé	Chiffrement, pare-feu, VPN
<b>Intégrité</b>	Empêcher la modification des données	Hashing, signatures numériques
<b>Disponibilité</b>	Garantir l'accès légitime	Anti-DDoS, redondance, surveillance réseau

---

## 3. Principales menaces réseau

Type de menace	Description
<b>Sniffing</b>	Interception de trafic (Wireshark, tcpdump)
<b>Spoofing</b>	Usurpation d'identité (ARP, DNS, IP spoofing)
<b>DDoS</b>	Saturation d'un service ou d'un réseau
<b>Man-in-the-Middle</b>	Interception et altération des communications
<b>Malware/Ransomware</b>	Infection par des logiciels malveillants
<b>Intrusions externes</b>	Accès non autorisé via des failles

---

## ☐ 4. Outils de sécurité réseau

Objectif	Outils
Analyse du trafic	Wireshark, tcpdump

Objectif	Outils
Pare-feu/IDS/IPS	iptables, pfSense, Snort, Suricata
VPN	OpenVPN, WireGuard, IPSec
Détection d'intrusions	OSSEC, Zeek, Fail2ban
Scanners de ports	Nmap, Zenmap
Gestion des logs	Syslog, ELK, Graylog

---

## 5. Mesures de sécurisation réseau

### A. Contrôle des accès

- Filtrage par adresse IP et MAC
- Authentification forte (2FA)
- Segmentation réseau (VLAN)

### B. Pare-feu (Firewall)

- Blocage des ports inutiles
- Règles d'autorisation strictes
- Firewall applicatif (WAF pour les services web)

### C. Chiffrement

- Protocoles sécurisés : HTTPS, SSH, SFTP
- VPN pour les connexions distantes
- WPA3 pour les réseaux Wi-Fi

### D. Surveillance réseau

- Analyse en temps réel des paquets
- SIEM pour corrélation des logs
- Alertes automatiques en cas d'anomalie

### E. Hardenning

- Désactivation des services inutiles
  - Mise à jour régulière des équipements
  - Suppression des comptes par défaut
- 

## 6. Protocoles de sécurité réseau

Protocole	Usage sécurisé
<b>HTTPS</b>	Chiffrement des sites web (SSL/TLS)
<b>SSH</b>	Connexion distante sécurisée
<b>IPSec</b>	Sécurisation des communications IP
<b>WPA3</b>	Sécurisation du Wi-Fi
<b>TLS</b>	Chiffrement des données réseau

---

## 🏰 7. Architecture sécurisée d'un réseau

```

[ Internet ]
  |
[ Firewall ]
  |
[ IDS/IPS ]
  |
[ DMZ ] ----- [Serveur Web sécurisé]
  |
[ LAN sécurisé interne ]
  |
[ PC, Imprimantes, Serveur fichiers ]

```

🔒 **DMZ (Demilitarized Zone)** : zone tampon entre Internet et le LAN pour héberger les services accessibles publiquement.

---

## 🔧 8. Bonnes pratiques

- 🔄 Mises à jour régulières (firmwares, OS, antivirus)
  - ☐ Tests de pénétration réguliers
  - 🔒 Chiffrement des communications sensibles
  - 🔍 Surveillance continue du trafic
  - ☐ Plans de reprise après sinistre (PRA)
- 

## 🎓 9. Exemple d'exercice pratique

🔒 Mettre en place un pare-feu avec `iptables` :

```

# Bloquer tout par défaut
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT ACCEPT




```

```
# Autoriser SSH depuis IP spécifique
iptables -A INPUT -p tcp --dport 22 -s 192.168.1.100 -j ACCEPT

# Autoriser le trafic HTTP/HTTPS
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -p tcp --dport 443 -j ACCEPT
```

---

## 10. Ressources recommandées

-  <https://owasp.org>
  -  “Network Security Essentials” – William Stallings
  -  Plateformes : [TryHackMe - Network Security](#), [HackTheBox](#)
-