Outils Réseau & Sécurité

Nmap • Wireshark • Cisco Packet Tracer

Guide complet — Théorie & Pratique

VM dédiée : SECURITY-SAM — Ubuntu Desktop 24.04
Infrastructure : mvgroup.local — 10.0.0.0/16

Rédigé par : Samuel — Mai 2026

1. Introduction

Ce document présente trois outils essentiels pour les professionnels réseau et sécurité informatique. Ils sont installés sur la VM dédiée SECURITY-SAM (Ubuntu Desktop 24.04) afin de centraliser les outils d'audit et d'analyse réseau.

Outil	Type	Usage principal
Nmap	Scanner réseau	Découverte d'hôtes, scan de ports, détection de services
Wireshark	Analyseur de paquets	Capture et analyse du trafic réseau en temps réel
Cisco Packet Tracer	Simulateur réseau	Conception et simulation de topologies réseau

1.1 VM SECURITY-SAM

Paramètre	Valeur
Nom	SECURITY-SAM
OS	Ubuntu Desktop 24.04 LTS
Rôle	VM dédiée aux outils réseau et sécurité
Nmap	Version 7.94SVN
Wireshark	Version 4.2.2
Cisco Packet Tracer	Version 9.0

2. Nmap — Network Mapper

2.1 Présentation

Nmap (Network Mapper) est un outil open source de découverte réseau et d'audit de sécurité. Il permet de scanner des réseaux pour identifier les hôtes actifs, les ports ouverts, les services qui tournent et les systèmes d'exploitation. C'est l'un des outils les plus utilisés par les administrateurs réseau et les professionnels de la sécurité.

2.2 Installation

```
sudo apt-get update
sudo apt-get install -y nmap

# Vérifier la version
nmap --version
```

2.3 Syntaxe générale

```
nmap [options] [cible]
```

La cible peut être une IP, un nom d'hôte, une plage d'IPs ou un réseau en notation CIDR.

2.4 Types de scans

Option	Type de scan	Description
-sn	Ping scan	Découverte d'hôtes sans scan de ports (le plus rapide)
-sS	SYN scan (furtif)	Scan TCP SYN — ne complète pas la connexion (nécessite root)
-sT	TCP Connect scan	Scan TCP complet — moins furtif mais sans root
-sU	UDP scan	Scan des ports UDP (plus lent)
-sV	Version scan	Détecte les versions des services
-sC	Script scan	Exécute les scripts NSE par défaut

-O	OS detection	Détection du système d'exploitation
-A	Aggressive scan	Active OS, version, scripts et traceroute
-Pn	Skip host discovery	Considère tous les hôtes comme actifs

2.5 Commandes pratiques

Découverte réseau

```
# Scanner tous les hôtes actifs sur le réseau
nmap -sn 10.0.0.0/16

# Scanner un hôte spécifique
nmap 10.0.0.5

# Scanner une plage d'IPs
nmap 10.0.0.1-20
```

Scan de ports

```
# Scan des 1000 ports les plus courants (défaut)
nmap 10.0.0.5

# Scan de tous les ports (1-65535)
nmap -p- 10.0.0.5

# Scan de ports spécifiques
nmap -p 80,443,22,3389 10.0.0.5

# Scan avec détection de version des services
nmap -sV 10.0.0.5
```

Scan avancé

```
# Scan complet avec OS et services
nmap -A 10.0.0.5

# Scan d'un hôte qui bloque les pings (Windows DC)
nmap -Pn -sV 10.0.200.2
```

```
# Forcer la détection via ports TCP spécifiques
nmap -PS22,80,135,443,3389 10.0.200.2

# Scan furtif SYN
nmap -sS 10.0.0.5
```

Options de sortie

```
# Enregistrer le résultat dans un fichier texte
nmap -sV 10.0.0.0/16 -oN scan_réseau.txt

# Enregistrer en format XML
nmap -sV 10.0.0.0/16 -oX scan_réseau.xml

# Mode verbose (plus de détails)
nmap -v -sV 10.0.0.5
```

2.6 Résultats obtenus sur l'infrastructure mvgroup.local

Scan de découverte réseau — nmap -sn 10.0.0.0/16

IP	Hostname DNS	Rôle
10.0.0.1	_gateway	Passerelle / Routeur
10.0.0.5	glpi.mvgroup.local	Serveur GLPI
10.0.0.10	WAZUH-INDEXER-SAM.mvgroup.local	Wazuh Indexer
10.0.0.11	WAZUH-MANAGER-SAM.mvgroup.local	Wazuh Manager
10.0.0.12	WAZUH-DASHBOARD-SAM.mvgroup.local	Wazuh Dashboard

ℹ️ *Le DC 10.0.200.2 n'apparaît pas dans le scan -sn car le pare-feu Windows bloque les pings ICMP. Utiliser -PS135,445,3389 pour le détecter.*

Scan du contrôleur de domaine — nmap -PS22,80,135,443,3389 10.0.200.2

Port	Service	Rôle AD
53/tcp	domain	DNS
88/tcp	kerberos-sec	Authentification Kerberos

135/tcp	msrpc	RPC Windows
139/tcp	netbios-ssn	NetBIOS
389/tcp	ldap	Annuaire LDAP
445/tcp	microsoft-ds	SMB — Partage fichiers
464/tcp	kpasswd5	Changement MDP Kerberos
636/tcp	ldapssl	LDAP sécurisé
3268/tcp	globalcatLDAP	Global Catalog LDAP
3269/tcp	globalcatLDAPssl	Global Catalog LDAP SSL

2.7 Référence rapide des options

Option	Description
-sn	Ping scan — pas de scan de ports
-sV	Détection des versions de services
-sC	Scripts NSE par défaut
-A	Scan agressif (OS + version + scripts)
-O	Détection OS
-p-	Tous les ports (1-65535)
-p X,Y,Z	Ports spécifiques
-Pn	Pas de découverte d'hôtes
-PS<ports>	TCP SYN ping sur ports spécifiques
-oN fichier	Sortie en texte normal
-oX fichier	Sortie en XML
-v	Mode verbose
--open	Afficher uniquement les ports ouverts

3. Wireshark — Analyseur de paquets

3.1 Présentation

Wireshark est le plus célèbre analyseur de protocoles réseau (packet sniffer) au monde. Il permet de capturer et d'inspecter en temps réel les paquets qui transitent sur une interface réseau. C'est un outil indispensable pour le diagnostic réseau, la sécurité et la formation.

3.2 Installation sur Ubuntu

```
sudo apt-get install -y wireshark

# Autoriser les utilisateurs non-root à capturer
sudo usermod -aG wireshark $USER
sudo chmod +x /usr/bin/dumpcap

# Appliquer sans redémarrer
newgrp wireshark

# Lancer Wireshark
wireshark
```

⚠ *Wireshark ne peut pas être lancé en tant que root. Utilisez toujours un utilisateur normal avec les droits du groupe wireshark.*

3.3 Interface principale

Zone	Description
Liste des interfaces	Affiche les interfaces réseau disponibles pour la capture
Barre de filtres	Permet d'appliquer des filtres d'affichage en temps réel
Liste des paquets	Affiche tous les paquets capturés avec horodatage
Détails du paquet	Détaille les couches du modèle OSI du paquet sélectionné
Vue hexadécimale	Affiche le contenu brut du paquet en hexadécimal

3.4 Filtres d'affichage essentiels

Les filtres permettent d'isoler le trafic qui vous intéresse parmi des milliers de paquets.

Filtres par protocole

Filtre	Description
icmp	Afficher uniquement les paquets ICMP (ping)
dns	Afficher uniquement les requêtes/réponses DNS
http	Afficher le trafic HTTP
https ou tcp.port==443	Afficher le trafic HTTPS
ldap	Afficher le trafic LDAP
smb	Afficher le trafic SMB (partage fichiers Windows)
arp	Afficher les requêtes ARP
dhcp	Afficher le trafic DHCP

Filtres par IP

Filtre	Description
ip.addr == 10.0.0.5	Trafic vers ou depuis 10.0.0.5
ip.src == 10.0.0.5	Trafic provenant de 10.0.0.5
ip.dst == 10.0.0.5	Trafic destiné à 10.0.0.5
ip.addr == 10.0.200.2	Trafic vers ou depuis le DC
!(ip.addr == 10.0.0.1)	Exclure le trafic de la passerelle

Filtres par port

Filtre	Description
tcp.port == 80	Trafic HTTP
tcp.port == 443	Trafic HTTPS
tcp.port == 389	Trafic LDAP
tcp.port == 22	Trafic SSH
udp.port == 51820	Trafic WireGuard
tcp.port == 3389	Trafic RDP (Bureau à distance)

Filtres combinés

```
# Trafic DNS vers le DC
dns && ip.addr == 10.0.200.2

# Trafic HTTP ou HTTPS
http || tcp.port == 443

# ICMP entre deux hôtes spécifiques
icmp && ip.addr == 10.0.0.5 && ip.addr == 10.0.100.6

# Exclure le trafic broadcast
!broadcast && !multicast
```

3.5 Captures réalisées sur l'infrastructure

Capture ICMP — ping vers GLPI

Source	Destination	Protocole	Info
10.0.100.6	10.0.0.5	ICMP	Echo (ping) request
10.0.0.5	10.0.100.6	ICMP	Echo (ping) reply

Capture DNS — résolution de noms

Source	Destination	Protocole	Info
10.0.100.6	10.0.200.2	DNS	Standard query A glpi.mvgroup.local
10.0.200.2	10.0.100.6	DNS	Standard query response A glpi.mvgroup.local 10.0.0.5
10.0.100.6	10.0.200.2	DNS	Standard query A WAZUH-DASHBOARD-SAM.mvgroup.local
10.0.200.2	10.0.100.6	DNS	Standard query response A WAZUH-DASHBOARD-SAM.mvgroup.local 10.0.0.12

3.6 Fonctionnalités avancées

Fonctionnalité	Accès	Description

Follow TCP Stream	Clic droit → Follow → TCP Stream	Reconstitue une conversation TCP complète
Statistiques	Menu Statistiques	Graphiques de trafic, conversations, protocoles
Export	Fichier → Exporter	Exporter les paquets capturés
Colorisation	Vue → Règles de colorisation	Personnaliser les couleurs par protocole
Filtres de capture	Capture → Options	Filtrer avant la capture pour réduire le volume

4. Cisco Packet Tracer — Simulateur réseau

4.1 Présentation

Cisco Packet Tracer est un simulateur réseau développé par Cisco Systems et disponible gratuitement via la plateforme NetAcad. Il permet de concevoir, configurer et simuler des topologies réseau complètes sans matériel physique. C'est un outil idéal pour l'apprentissage, la documentation et la planification d'infrastructure.

4.2 Installation sur Ubuntu

1. Créer un compte gratuit sur https://www.netacad.com
2. Télécharger le fichier .deb depuis la section Lab Downloads
3. Installer le paquet :

```
sudo dpkg -i CiscoPacketTracer_900_Ubuntu_64bit.deb

# Si dépendances manquantes :
sudo apt-get install -f -y

# Lancer Packet Tracer (en utilisateur normal, pas root)
packettracer
# Ou depuis le menu Applications Ubuntu
```

⚠ *Packet Tracer ne peut pas être lancé en root. Lancez-le depuis le menu Applications ou en tant qu'utilisateur normal.*

4.3 Interface principale

Zone	Description
Zone de travail	Espace principal où on place et connecte les équipements
Barre d'équipements	En bas — sélection des appareils (routeurs, switches, PCs...)
Barre d'outils	En haut — outils de dessin, PDU, sélection
Mode temps réel / simulation	Bascule entre le mode normal et la simulation pas-à-pas
Panneau de simulation	Visible en mode simulation — affiche les paquets en transit

4.4 Équipements disponibles

Catégorie	Équipements	Usage
Routers	4331, 2911, ISR...	Routage entre réseaux
Switches	2960, 3650...	Commutation couche 2/3
End Devices	PC, Server, Laptop...	Hôtes clients et serveurs
Network Devices	Firewall, WLC...	Sécurité et gestion WiFi
Connections	Cuivre, Fibre, Série...	Câbles de connexion
WAN Emulation	Cloud, DSL Modem...	Simulation WAN/Internet

4.5 Topologie créée — Infrastructure mvgroup.local

La topologie suivante représente l'infrastructure réelle mise en place dans ce portfolio :

Équipement PT	Nom	IP configurée	Rôle
Router 4331	Gateway-10.0.0.1	10.0.0.1/16	Passerelle par défaut
Switch 2960	SW-CORE	—	Commutateur principal
Server	DC-SAM	10.0.200.2/16	Contrôleur de domaine AD
Server	GLPI-SAM	10.0.0.5/16	Serveur GLPI
Server	WAZUH-INDEXER-SAM	10.0.0.10/16	Wazuh Indexer
Server	WAZUH-MANAGER-SAM	10.0.0.11/16	Wazuh Manager
Server	WAZUH-DASHBOARD-SAM	10.0.0.12/16	Wazuh Dashboard
Server	WIREGUARD-SAM	10.0.0.20/16	Serveur VPN WireGuard
PC	W11-CLIENT1-SAM	10.0.100.1/16	Client Windows 11
PC	UBUNTU-CLIENT2-SAM	10.0.100.2/16	Client Ubuntu 24.04
PC	SECURITY-SAM	10.0.100.6/16	VM Sécurité/Audit

4.6 Configuration du routeur

```
enable
configure terminal
interface GigabitEthernet0/0/0
```

```
ip address 10.0.0.1 255.255.0.0
no shutdown
exit
write memory
```

4.7 Configuration IP des hôtes

Pour chaque PC/Serveur : Double-clic → Desktop → IP Configuration

Champ	Valeur exemple (GLPI-SAM)
IP Address	10.0.0.5
Subnet Mask	255.255.0.0
Default Gateway	10.0.0.1
DNS Server	10.0.200.2

4.8 Test de connectivité

Depuis un PC client (Desktop → Command Prompt) :

```
# Ping vers le serveur GLPI
ping 10.0.0.5

# Ping vers le DC
ping 10.0.200.2

# Ping vers Wazuh Dashboard
ping 10.0.0.12
```

✅ Tous les pings fonctionnent entre les équipements de la topologie.

4.9 Mode simulation

Le mode simulation permet de visualiser le cheminement des paquets étape par étape :

4. Cliquer sur le bouton Simulation (horloge en bas à droite)
5. Utiliser l'outil Add Simple PDU (enveloppe)
6. Cliquer sur la source puis sur la destination
7. Cliquer sur Play ou Forward pour avancer pas à pas
8. Observer le paquet traverser chaque équipement

5. Récapitulatif & Bonnes pratiques

5.1 Comparaison des outils

Critère	Nmap	Wireshark	Packet Tracer
Type	Scanner actif	Capture passive	Simulateur
Impact réseau	Génère du trafic	Aucun impact	Aucun (simulation)
Droits requis	Root pour SYN scan	Groupe wireshark	Utilisateur normal
Usage principal	Audit, découverte	Diagnostic, analyse	Formation, documentation
Environnement	Réseau réel	Réseau réel	Simulation

5.2 Bonnes pratiques

- Ne jamais scanner un réseau sans autorisation explicite — c'est illégal
- Toujours documenter les scans Nmap avec -oN pour garder une trace
- Utiliser Wireshark uniquement sur des réseaux dont vous êtes responsable
- Ne jamais lancer Wireshark ou Packet Tracer en root
- Sauvegarder régulièrement les topologies Packet Tracer (.pkt)
- Utiliser des filtres Wireshark pour ne capturer que le trafic nécessaire

5.3 Ressources utiles

- Nmap : https://nmap.org/docs.html
- Wireshark : https://www.wireshark.org/docs/
- Cisco Packet Tracer : https://www.netacad.com
- Nmap Cheat Sheet : https://nmap.org/cheatsheet.html
- Wireshark Display Filters : https://wiki.wireshark.org/DisplayFilters