Rapport d’Audit de Sécurité Réseau

Généré le : 18/06/2025 à 07:09

■■ Module : nmap - 2025-06-17 22:40:31

#	Résultat
1	➤ Paramètres : -p- 192.168.1.1
2	➤ Résultat :
3	Ports 22, 80, 443 ouverts.

■■ Module : openvas - 2025-06-17 22:40:31

#	Résultat
1	➤ Paramètres : --deep-scan
2	➤ Résultat :
3	Configuration Apache vulnérable.

■■ Module : metasploit - 2025-06-17 22:40:31

#	Résultat
1	➤ Paramètres : scanner/ssh/ssh_version
2	➤ Résultat :
3	OpenSSH 7.2 détecté.

■■ Module : zap - 2025-06-17 22:40:31

#	Résultat
1	➤ Paramètres : --spider http://demo.testfire.net
2	➤ Résultat :
3	Formulaires sans token CSRF trouvés.

■■ Module : hydra - 2025-06-17 22:40:31

#	Résultat
1	➤ Paramètres : -L users.txt -P passwords.txt ftp://192.168.1.1
2	➤ Résultat :
3	Aucun identifiant trouvé.

■■ Module : wireshark - 2025-06-17 22:40:31

#	**Résultat**
1	➤ Paramètres : capture2.pcap
2	➤ Résultat :
3	Tentative d'injection DNS repérée.

■■ Module : aircrack - 2025-06-17 22:40:31

#	Résultat
1	➤ Paramètres : -w rockyou.txt -b 00:11:22:33:44:55 capfile.cap
2	➤ Résultat :
3	Échec du craquage de clé WPA.

■■ Module : nikto - 2025-06-17 22:40:31

#	Résultat
1	➤ Paramètres : -h http://testsite.local
2	➤ Résultat :
3	Répertoire .git exposé.