






Types de Scans Réseau – Explications

Ce tableau présente les principaux types de scans réseau à utiliser dans les tests IPS FortiGate. Chaque ligne explique le but, le mécanisme, le contexte d'usage et la détection IPS attendue.

 Type de Scan	 Objectif	 Fonctionnement	 Utilisation Typique	 Détection IPS
TCP Connect Scan	Connexion complète à chaque port	Envoie SYN → Reçoit SYN/ACK → Envoie ACK (3-way handshake complet)	Méthode simple, utilisée sans privilèges administrateur	`TCP.Full.Connect`
Stealth SYN Scan	Détection discrète des ports ouverts	Envoie SYN → Reçoit SYN/ACK → Pas d'ACK final (pas de session complète)	Très utilisé par les attaquants (furtif)	`TCP.SYN.Scan`, `Port.Scan`
Scan Rapide / Massif	Balayage très rapide de ports ou d'adresses IP	Envoie un grand nombre de SYN à haute fréquence (ex: Masscan, Nmap -T5)	Botnets, scans automatisés sur Internet	`Masscan.Activity`, détection par volume
UDP Scan	Identifier les services UDP disponibles	Envoie datagrammes UDP vides → attend réponse ou ICMP "port unreachable"	Moins fréquent, utile pour DNS, SNMP, etc.	`UDP.Scan`, `ICMP.Port.Unreachable`
Ping Scan (Discovery)	Découvrir les hôtes actifs sans scanner les ports	Envoie des paquets ICMP Echo ou requêtes ARP	Cartographie réseau de base ; non intrusif	Faible détection sauf si ICMP surveillé
Version Detection Scan	Identifier la version du service derrière un port	Connexion au service → lecture bannière ou test léger	Reco ciblée ; utilisée avant exploitation	Détection de fingerprinting
OS Detection	Deviner le système d'exploitation	Analyse TCP/IP (TTL, taille de fenêtre, etc.)	Utilisé dans les attaques avancées	`OS.Fingerprint.Attempt`

		pour comparer à une base connue		
Scan Complet / Combiné	Réaliser un scan global (services, OS, scripts NSE)	Combine plusieurs modes : `sV`, `O`, `-- tracroute`	Audits, pentests, tests de vulnérabilité complets	Plusieurs signatures déclenchées