⚡ Nmap Hidden Tricks – Command Cheat Sheet (15)

Bugitrix.com

1️⃣ Scan All Ports (Smart Full Scan)

sudo nmap -p- --min-rate 1000 -T3 target.com

Finds services running on non-standard ports.

2️⃣ Scan Only High-Value Ports (Fast Recon)

nmap -p 21,22,25,53,80,443,3000,3306,5432,6379,8080,8443,9000 target.com

Targets ports most likely to expose bugs.

3️⃣ Scan the Origin IP (Bypass CDN)

nmap -p- <TARGET_IP>

Reveals services hidden behind Cloudflare/CDNs.

4️⃣ Increase Version Detection Accuracy

nmap -sV --version-all target.com

Improves service fingerprinting accuracy.

5️⃣ Verify Unknown Services Manually

nc target.com 9999

curl http://target.com:9999

Confirms real service behavior.

6️⃣ Fingerprint Services by Behavior

nmap -p 80,443 --script http-headers,http-methods target.com

Reveals frameworks and misconfigs.

7️⃣ Use NSE for Discovery (Not Vuln Spam)

nmap -p 80,443 --script http-enum target.com

Finds hidden paths and admin panels.

8️⃣ Run Targeted NSE Scripts

nmap -p 21 --script ftp-anon target.com

nmap -p 6379 --script redis-info target.com

Finds real misconfigurations.

9️⃣ Use Safe + Auth Script Categories

nmap --script "safe,auth" target.com

Low noise, high-value intelligence.

🔟 Fragment Packets (Firewall Evasion)

sudo nmap -f target.com

Bypasses weak packet filters.

11️⃣ Use Decoys (Attribution Noise)

sudo nmap -D RND:10 target.com

Blends scan traffic with fake IPs.

12️⃣ Compare Domain vs IP Scan (Cloud Recon)

nmap target.com

nmap <TARGET_IP>

Exposes origin-only services.

13️⃣ Internal Network Discovery

nmap -sn 10.0.0.0/24

nmap -sS 10.0.0.0/24

Finds internal hosts and services.

14️⃣ Save Output for Tool Chaining

nmap -oA recon target.com

Use output with FFUF, Burp, scripts.

15️⃣ Read Output Like a Hacker

nmap -sV -p 8080,8443 target.com

Look for services that **shouldn’t be public**.