**TEAM MEMBER : A**

**VIVEK KUMAR**

**🧷Vulnerability Scanning (Member A)**

**📌Objective:**

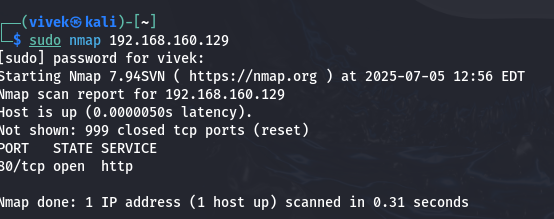
**🌟Nmap Commands for Scanning (Vulnerability)**

**Nmap**

Nmap is short for Network Mapper, an open-source tool used for port and IP scanning and app detection. Network and system administrators use it for network inventory, managing service upgrade schedules, and monitoring service uptime

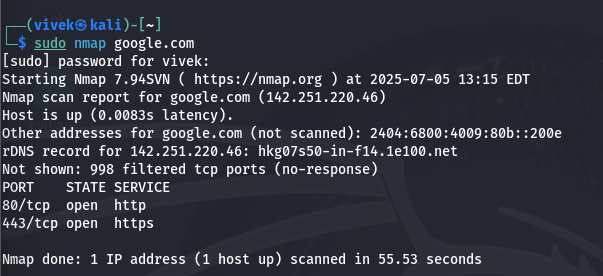
Admins use it for penetration testing, to check what devices are running on their network. Nmap also enables them to see what ports are open and discover potential vulnerabilities.

**Basic scan of a single IP or hostname.**



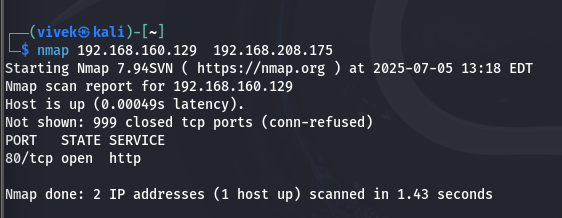
➡️*Scans the target IP for open ports.*

**Scan a domain**



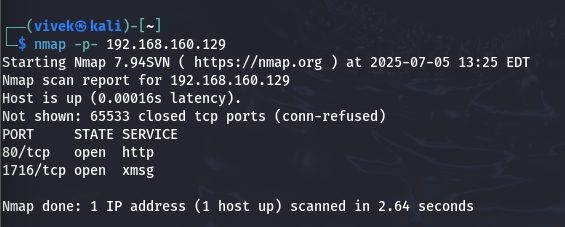
➡️ *Resolves the domain and scans the corresponding IP.*

**Scan multiple Ips**

****

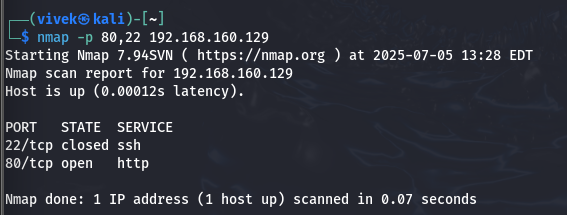
**➡️ *Scans multiple specified IPs.***

**Scan all ports**

****

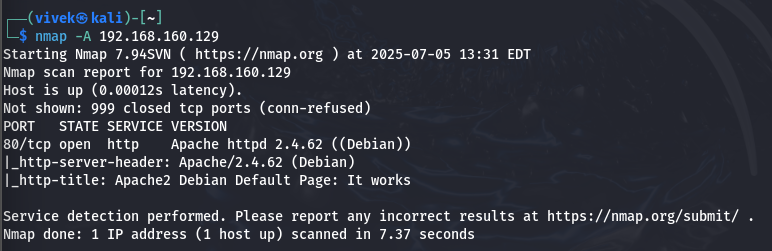
**➡️ Scans all TCP ports.**

**Scan specific ports**

****

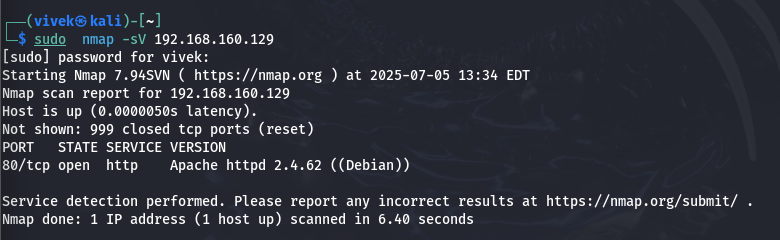
**➡️ Scans ports 22 (SSH), 80 (HTTP).**

**Aggressive scan**

****

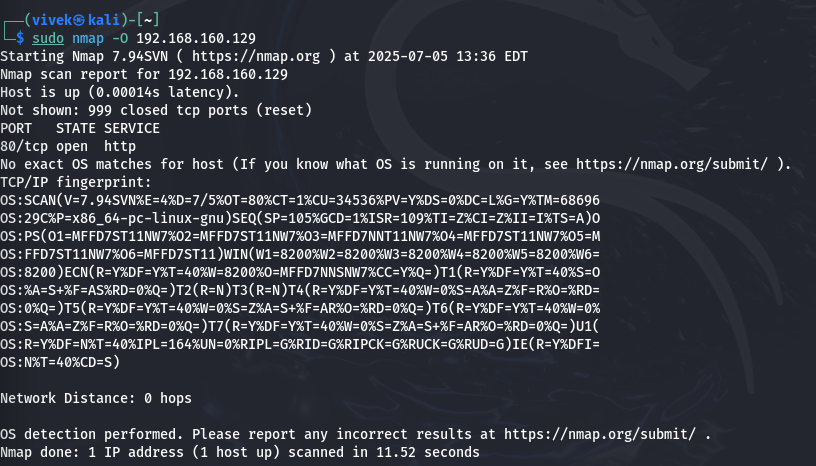
***➡️*** *Performs OS detection, version detection, script scanning, and traceroute.*

**Service and version detection**



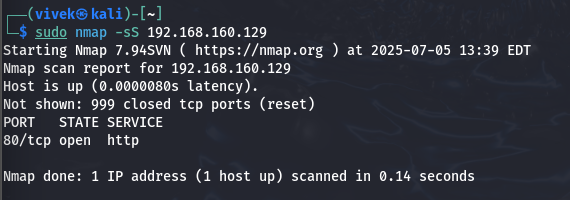
➡️ *Detects services running and their versions.*

**Operating system detection**



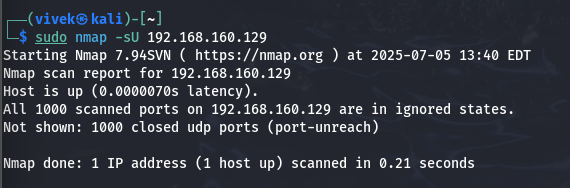
➡️ *Attempts to determine the OS of the host.*

**Stealth SYN Scan**



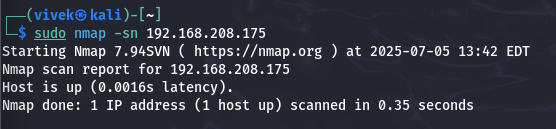
➡️ Sends SYN packets to detect open ports without completing the handshake.

**UDP Scan**

****

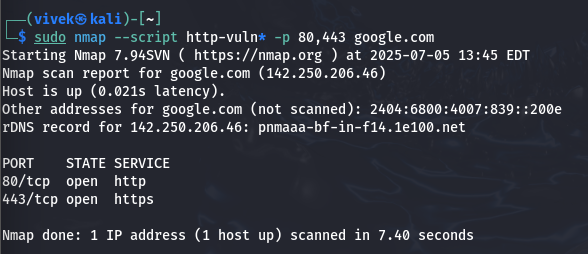
➡️ Scans for open UDP ports (slower than TCP)

**Detect firewall (ping scan)**

****

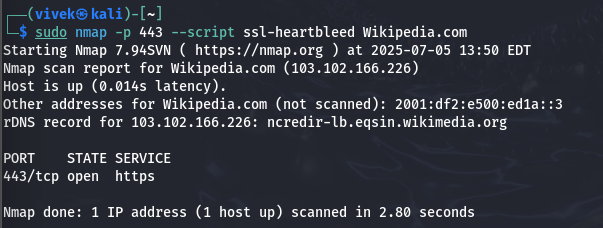
➡️*Pings the host to check if it is up without scanning ports.*

**Scan for HTTP vulnerabilities**

****

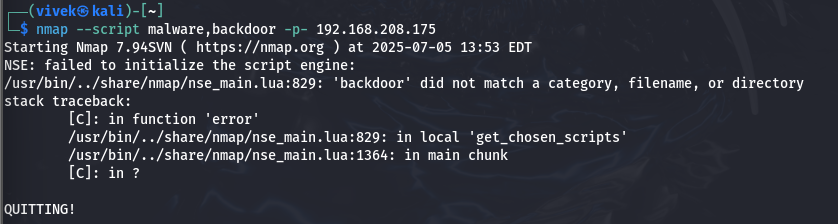
*➡️ Runs all vulnerability-related HTTP NSE scripts on ports 80/443*

**Scan for SSL/TLS vulnerabilities (like Heartbleed)**

****

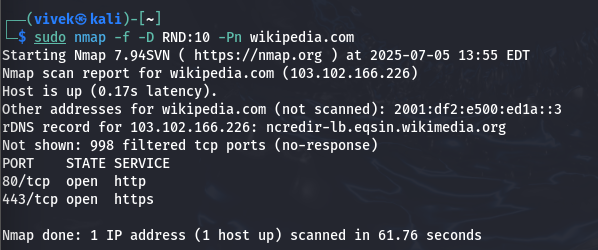
*➡️ Checks if the target is vulnerable to the Heartbleed bug.*

***Detect malware backdoors or trojans***



*➡️ Uses malware detection scripts on all ports*

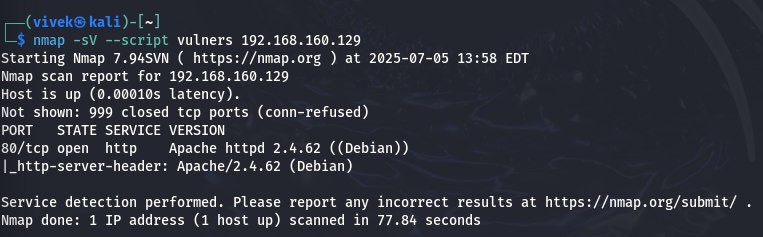
**Firewall/IDS Evasion**



✅ *Explanation:*

* *-f : Fragment packets to evade detection*
* *-D RND:10 : Use decoys to confuse IDS*
* *-Pn : Skip ping to avoid being blocked by ICMP filters*

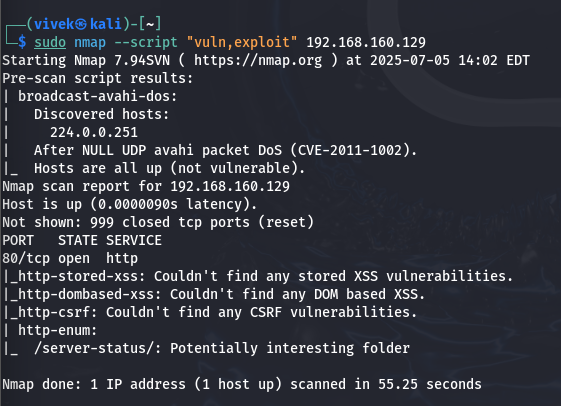
**Scan for outdated or vulnerable software versions**

****

**🛡️ Nmap Script Categories for Pentesting**

**You can run script categories like:**

* ***auth → authentication-related***
* ***vuln → known vulnerabilities***
* ***exploit → known exploits***
* ***brute → brute-force***
* ***malware → detect malicious activity***
* ***safe → safe for production testing***

***example :- ***