**PRACTICAL NO 4**

**AIM:** Port Scanning with NMap

* Use NMap to perform an ACK scan to determine if a port is filtered, unfiltered, or open.
* Perform SYN, FIN, NULL, and XMAS scans to identify open ports and their characteristics.
* Analyze the scan results to gather information about the target system's network services

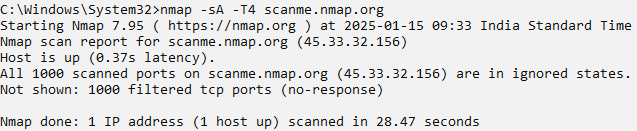
**SOLUTION:**

Download and install nmap from the website : https://nmap.org/download#windows

**1) ACK -sA (TCP ACK scan)**

It never determines open ports. It is used to map out firewall rulesets, determining which ports are filtered

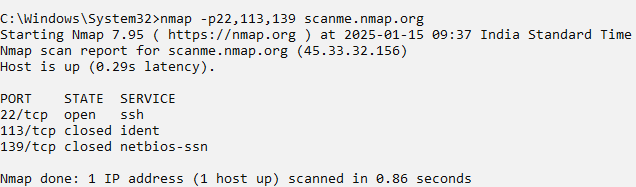
Command: nmap -sA -T4 scanme.nmap.org



**2) SYN (Stealth) Scan (-sS)**

SYN Scan is the default and most popular scan options for good reasons . It can be performed quickly , scanning thousands of ports per second on a fast network not hampered by intrusive firewalls

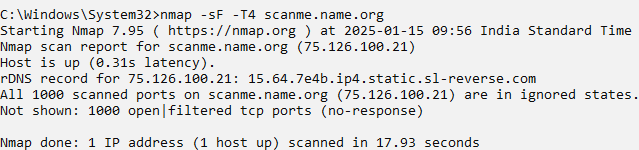
Command : nmap -p22,113,139 scanme.nmap.org



**3) FIN (-sF)**

Sets just the TCP FIN bit

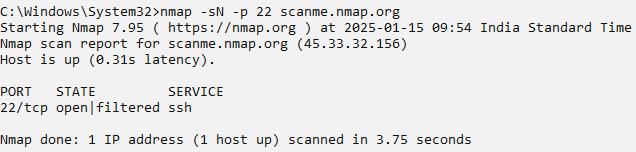
Command: nmap -sF -T4 scanme.name.org



**4) NULL Scan (-sN)**

Does not set any bits (TCP Flag Header is 0)

Command : nmap -sN -p 22 scanme.nmap.org



**5) XMAS Scan (-xS)**

Sets the FIN, PSH and URG flags, lightning the packet up like a Christmas tree

Command : nmap -sX -T4 scanme.nmap.org

