- **Title** : Use N-map for open port to provide a detail report of the services running on each device, service port and detecting the OS.

- **Objective** : To utilize the Nmap tool to perform open port detection, enumerate services running on each open port, and detect the operating system of the target machine.

- Mode used : Nmap

- Theory :
  - Nmap uses various scanning techniques, including TCP SYN, TCP connect, UDP, and others, to probe and discover information about the target network. It employs signature-based detection to identify the services running on open ports and employs fingerprinting techniques for OS detection.

- Different techniques using Nmap :

1. Open port Detection :- Nmap will list all open ports on the target machine, providing information about the State (open, closed, filtered) of each port.

2. Service Enumeration : Nmap will attempt to identify the services running on each open port and display details such as service name version, and other relevant information.

3. Os Detection : Nmap will analyze responses from the target to make an educated guess about the operating system running on the target machine.

4. Scripting Engine (NSE) : Nmap features a powerful Scripting Engine (NSE) that allows users to extend functionality beyond simple scanning. NSE scripts can be employed to perform advanced task such as vulnerability detection, information gathering, or specific protocol analysis

5. Timing and Performance options : Nmap provides options to control the timing and performance of the scan

6. Output Formats : Nmap offers various output formats, including human-readable text. XML and grepable formats.

7. Firewall Evasion Techniques : Nmap provides options for users to employ techniques for firewall evasion such as fragementation, decoy scanning, and idle scanning.

8. Comprehensive Documentation : Nmap is well-documented, and users can refer to the official Nmap documentation to understand the various options techniques and uses cases

○ Procedure :

- Set Up :-
  - Identify the target IP address or hostname.
  - Open a terminal or command prompt on your machine.
  - Execute the Nmap command with appropriate options to perform open port detection, service enumeration and OS detection.
  - Open Nmap and specify the target (IP of website)
- Observation :
  - Nmap will list all the open ports on the target machine, providing information about the state of each port.
  - It will attempt to identify the services running on each open port and display details such as service name, version and other relevant information.
  - It will analyze responses from the target to make an educated guess about the OS running on target machine.

○ Conclusion : Nmap provides valuable information about the target's network, helping security professionals asses potential vulnerabilities and weaknesses.