

Walchand College of Engineering, Sangli

Title & Use N-map for open port to provide a detail service port and detecting the os

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

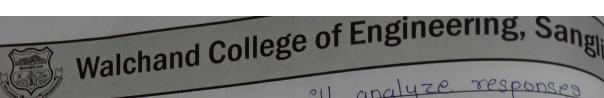
·Mode used & Nmap

o 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 fingerpointing techniques for 0s detection.

· Different techniques using Nmap?

- 1. Open port Detection: Nmap will list all open posts on the target machine, providing information about the state (open, closed, filtered) of each port.
- 2. Service Enumeration & Nmap will attempt open port and display details such as service name version, and other relevant information



- 8. 08 petertion? Nmap will analyze responses

 from the target to make an educated guess
 about the operating system running on the
 target machine.
- 4. Sempting Engine (NSE) & Nmap features a

 powerful Scripting Engine (NSE) that allows

 powerful Scripting Engine (NSE) that allows

 users to extend functionality beyond simple

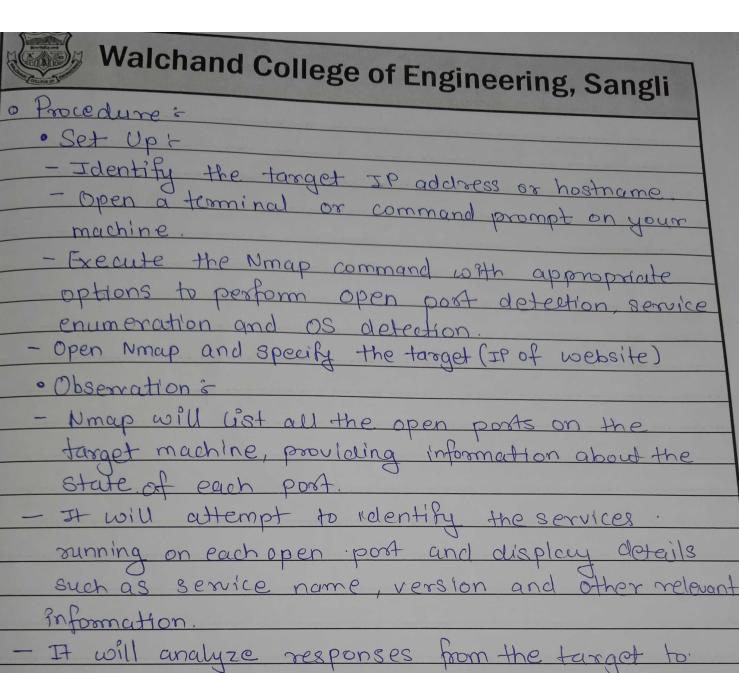
 users to extend functionality beyond simple

 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. Firmall Evasion Techniques? Nmap provides options for users to employ techniques for firewall evasion such as fragementation decay scanning and idle scanning.
- 8. Comprehensive Documentation & Nmap is welldocumented, and users can refer to the official Nmap documentation to understand the various options techniques and uses cases



- It will analyze responses from the target to make an educated guess about the OS running on target machine.

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