Assignment 2

Title: Find sweep IP ranges for live

Theory:

Introduction to Nmap
Its Need/Purpose
Advantages
Disadvantages

Demonstration:

Syntax :nmap <ip address>
Command: nmap 172.16.182.24
Purpose : Syntax for scanning a single IP.
Output:

Syntax : nmap www.domain.com
Command 2: nmap www.amazon.com
Purpose : Scanning Hostname
Output:

Syntax :nmap <ip address range>
Command 3:nmap 192.168.1.1-100
Purpose :Scanning an IP range
Output:

Syntax :nmap 192.168.1.1/24
Command 4: nmap 192.168.1.1/24
Purpose : Scanning a Subnet
Output:

Syntax : nmap -p <_port> <ip address>
Command 5: nmap -p 8080 192.168.1.1
Purpose :Use -p <_port> to scan for one specific port on the target
Output:

Syntax :nmap -F <ip address>
Command 6:nmap -F 192.168.1.1
Purpose :The -F tells Nmap to scan for the 100 most common ports that can be open on a target.
Output:

Syntax :nmap -p (range) <ip address
Command 7: nmap -p 80-100 172.16.182.54
Purpose :Scans a range of ports on the target
Output:

Syntax :sudo su
Enter your password
Command 8: sudo nmap -f 192.168.1.1
Purpose :command to provide access privileges:
Output:

T0 T5

Find sweep IP ranges for live host

1) **ARP scan: nmap -PR -sn 172.16.182.224/24**

2) **ICMP scan: nmap -PP -sn 172.16.182.224/24**

3) **TCP/UDP ping scan:**

-PA

-PU

Conclusion:

FAQs:

What does "tcpwrapped" mean?
Why does Nmap show some of my ports as "filtered"?
How should Nmap be capitalized?
What is Nmap's license?