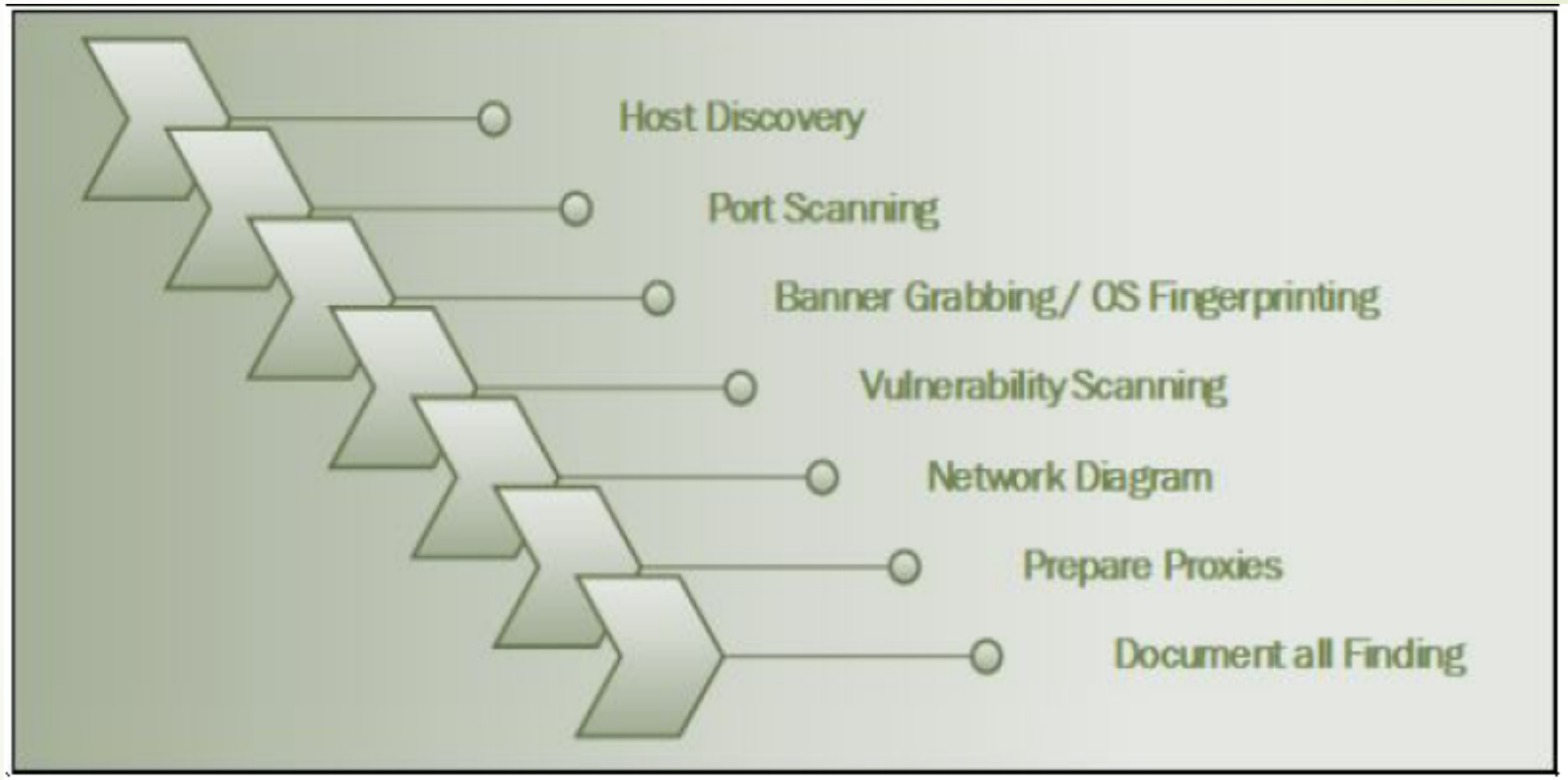
Scanning and Enumeration

Overview of Network Scanning

Scanning Methodology

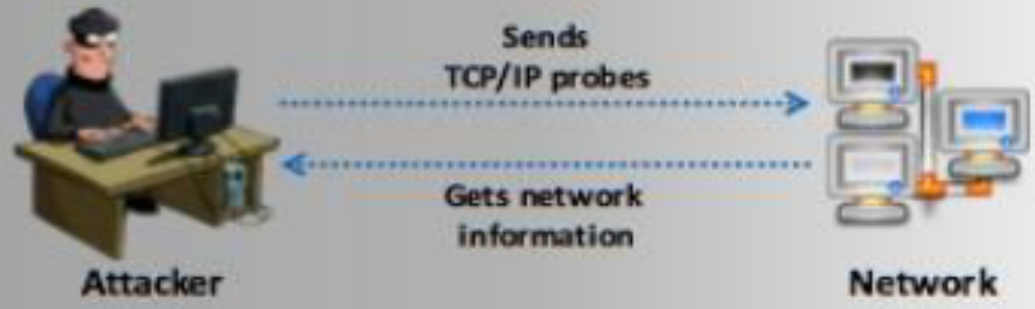
The Scanning Methodology includes the following step: -
Checking for live systems
Discovering open ports
Scanning beyond IDS
Banner grabbing
Scanning Vulnerabilities
Network Diagram
Proxies



Overview of Network Scanning

- Network scanning refers to a set of procedures used for identifying hosts, ports, and services in a network
- Network scanning is one of the components of intelligence gathering which can be used by an attacker to create a profile of the target organization

Network Scanning Process

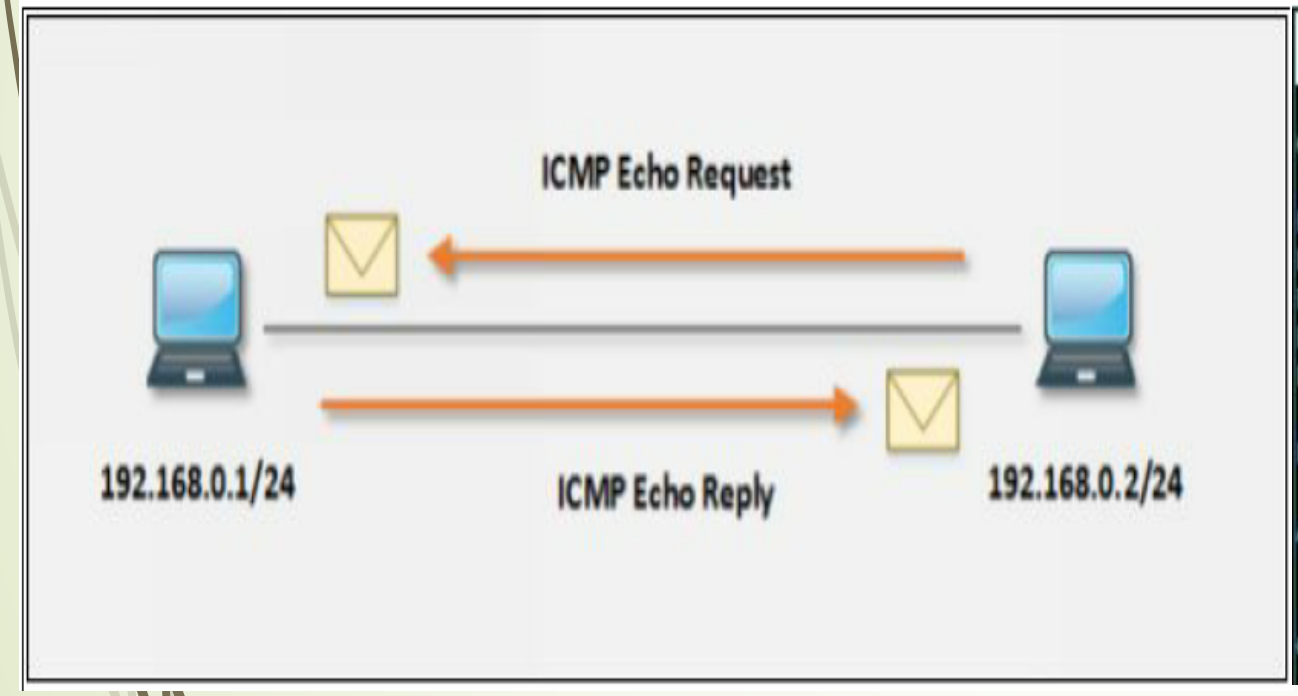


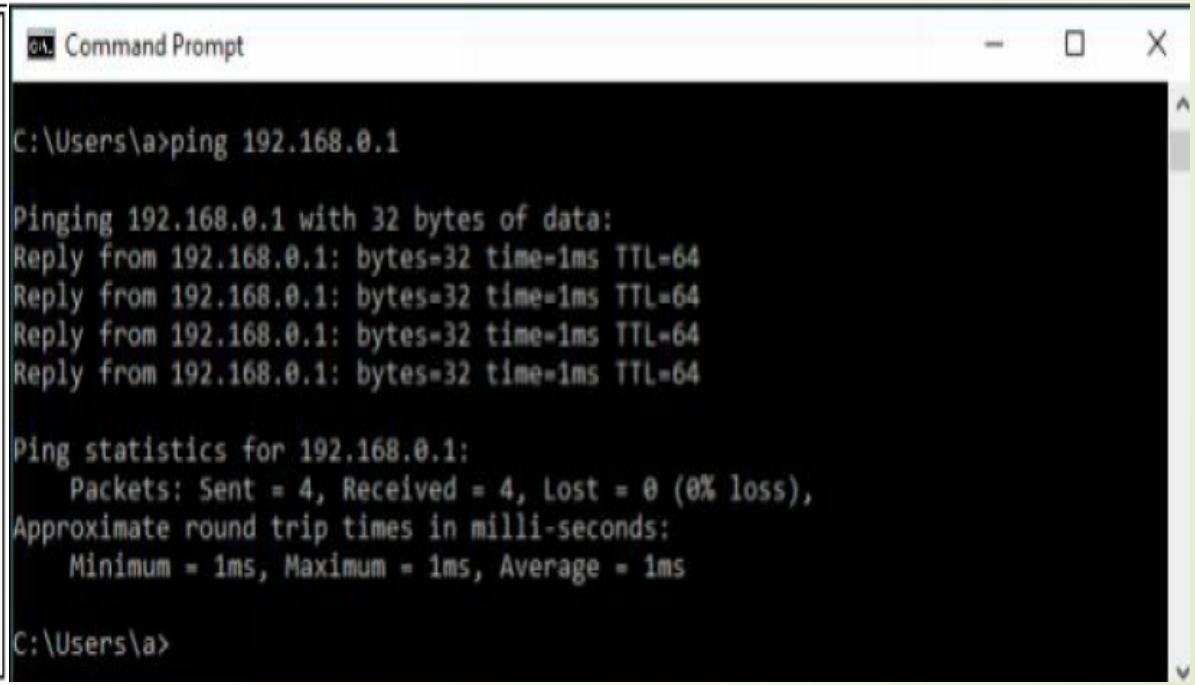
Objectives of Network Scanning

- To discover live hosts, IP address, and open ports of live hosts
- To discover operating systems and system architecture
- To discover services running on hosts
- To discover vulnerabilities in live hosts

Checking for Live Systems

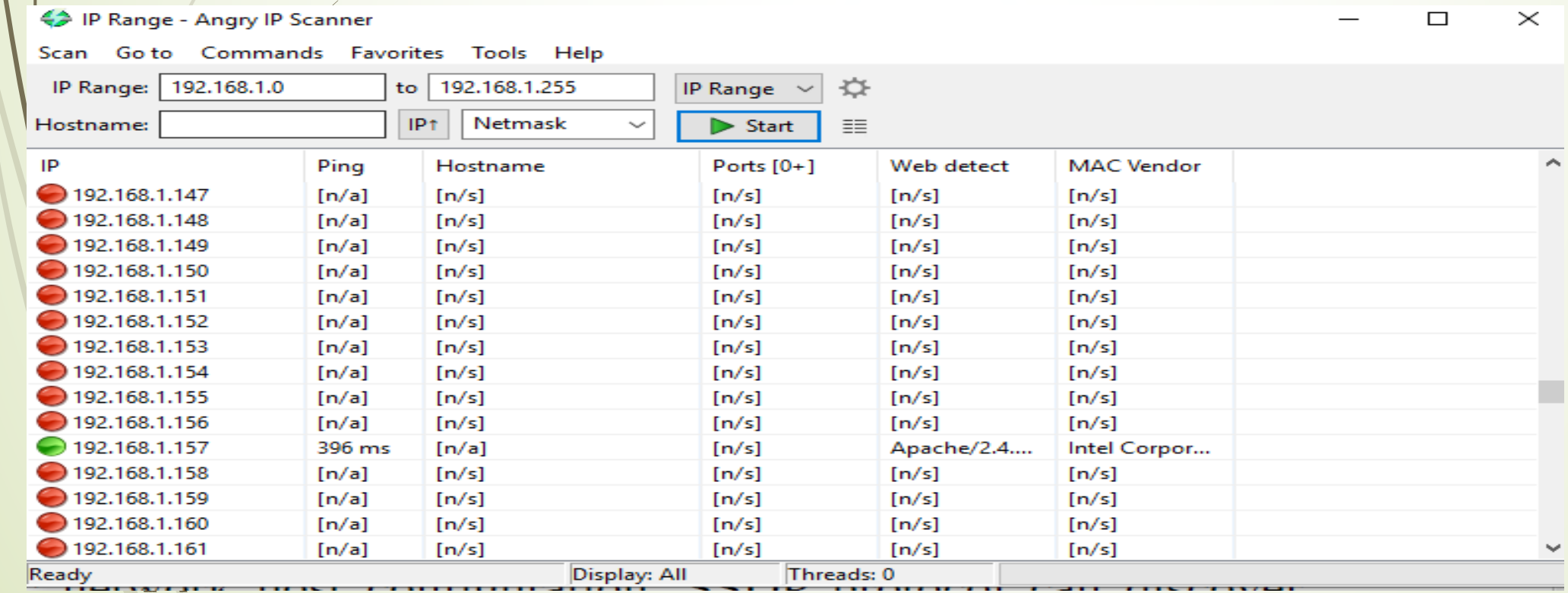
Initially, we must know about the hosts which are living in a targeted network. Finding live hosts in a network is done by ICMP Packets. The target replies ICMP Echo packets with ICMP echo reply. This response verifies that the host is live.





Ping Sweep (ICMP Scanning)

Ping Sweep determines live host on a large scale. Ping Sweep is a method of sending ICMP Echo Request packets to a range of IP addresses instead of sending one by one requests and observing the response. Live hosts respond with ICMP Echo Reply packets. Thus, instead of probing individually, we can probe a range of IPs using Ping Sweep. There are several tools available for Ping Sweep. Using these ping sweep tools such as SolarWinds, Ping Sweep tool or Angry IP Scanner, We can ping the range of IP addresses



Nmap Scan Techniques

Scan Techniques

Switch	Example	Description
-sS	nmap 192.168.1.1 -sS	TCP SYN port scan (Default)
-sT	nmap 192.168.1.1 -sT	TCP connect port scan (Default without root privilege)
-sU	nmap 192.168.1.1 -sU	UDP port scan
-sA	nmap 192.168.1.1 -sA	TCP ACK port scan
-sW	nmap 192.168.1.1 -sW	TCP Window port scan
-sM	nmap 192.168.1.1 -sM	TCP Maimon port scan

Host Discovery

Switch	Example	Description
-sL	nmap 192.168.1.1-3 -sL	No Scan. List targets only
-sn	nmap 192.168.1.1/24 -sn	Disable port scanning. Host discovery only.
-Pn	nmap 192.168.1.1-5 -Pn	Disable host discovery. Port scan only.
-PS	nmap 192.168.1.1-5 -PS22-25,80	TCP SYN discovery on port x. Port 80 by default
-PA	nmap 192.168.1.1-5 -PA22-25,80	TCP ACK discovery on port x. Port 80 by default
-PU	nmap 192.168.1.1-5 -PU53	UDP discovery on port x. Port 40125 by default
-PR	nmap 192.168.1.1-1/24 -PR	ARP discovery on local network
-n	nmap 192.168.1.1 -n	Never do DNS resolution

Nmap Scan Techniques

Service and Version Detection

Switch	Example	Description
-sV	nmap 192.168.1.1 -sV	Attempts to determine the version of the service running on port
-sV --version-intensity	nmap 192.168.1.1 -sV --version-intensity 8	Intensity level 0 to 9. Higher number increases possibility of correctness
-sV --version-light	nmap 192.168.1.1 -sV --version-light	Enable light mode. Lower possibility of correctness. Faster
-sV --version-all	nmap 192.168.1.1 -sV --version-all	Enable intensity level 9. Higher possibility of correctness. Slower
-A	nmap 192.168.1.1 -A	Enables OS detection, version detection, script scanning, and traceroute

Timing and Performance

Switch	Example	Description
-T0	nmap 192.168.1.1 -T0	Paranoid (0) Intrusion Detection System evasion
-T1	nmap 192.168.1.1 -T1	Sneaky (1) Intrusion Detection System evasion
-T2	nmap 192.168.1.1 -T2	Polite (2) slows down the scan to use less bandwidth and use less target machine resources
-T3	nmap 192.168.1.1 -T3	Normal (3) which is default speed
-T4	nmap 192.168.1.1 -T4	Aggressive (4) speeds scans; assumes you are on a reasonably fast and reliable network
-T5	nmap 192.168.1.1 -T5	Insane (5) speeds scan; assumes you are on an extraordinarily fast network

Enumeration Concepts

In the phase of Enumeration, An attacker initiates active connections with the target system. With this active connection, direct queries are generated to gain more information. These information helps to identify the system attack points. Once attacker discovers attack points, it can gain unauthorized access using this collected information to reach assets.

Information that is enumerated in this phase are: -

Routing Information
SNMP Information
DNS Information
Machine Name
User Information
Group Information
Application and Banners
Network Sharing Information
Network Resources

Services Enumeration using Nmap

Operating System & Version scanning on target host 10.10.10.12.