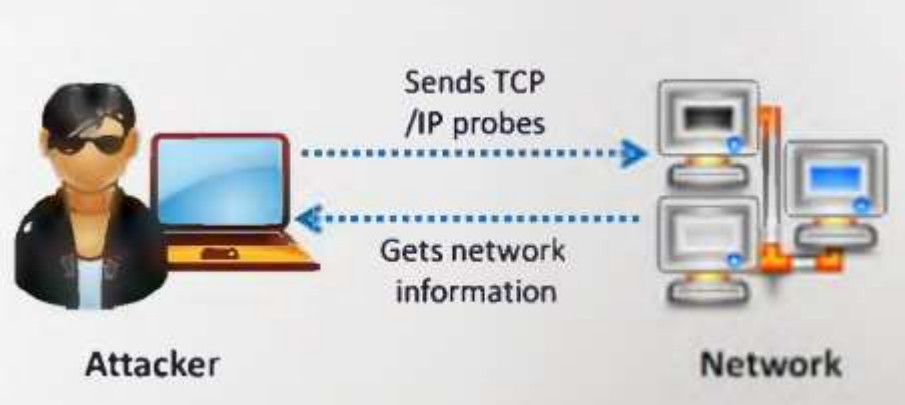
Scanning Networks

Contents

Introduction



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

(1) To discover live hosts, IP address, and open ports of live hosts

(2) To discover operating systems and system architecture

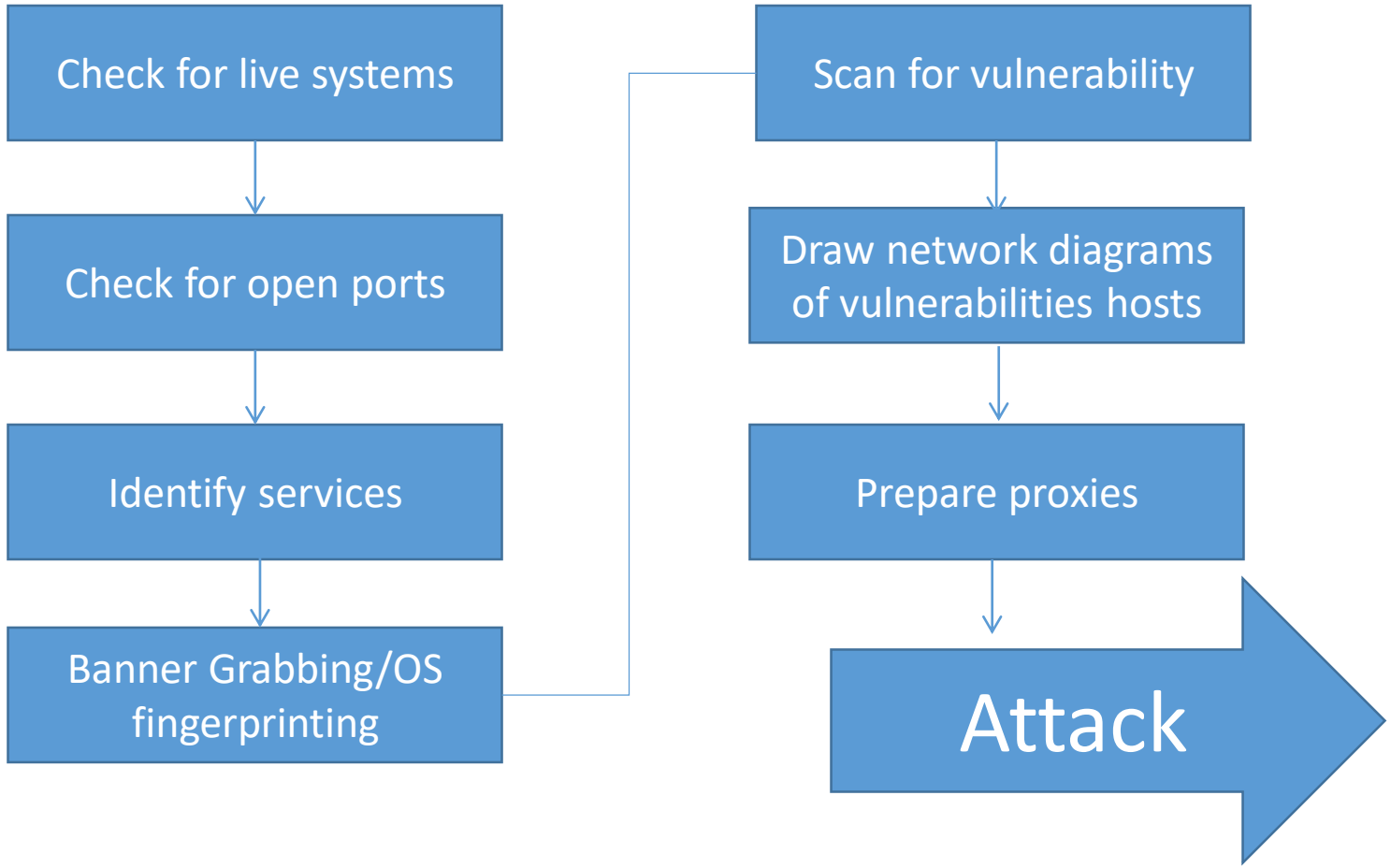
(3) To discover services running on hosts

(4) To discover vulnerabilities in live hosts

Objectives of network scanning

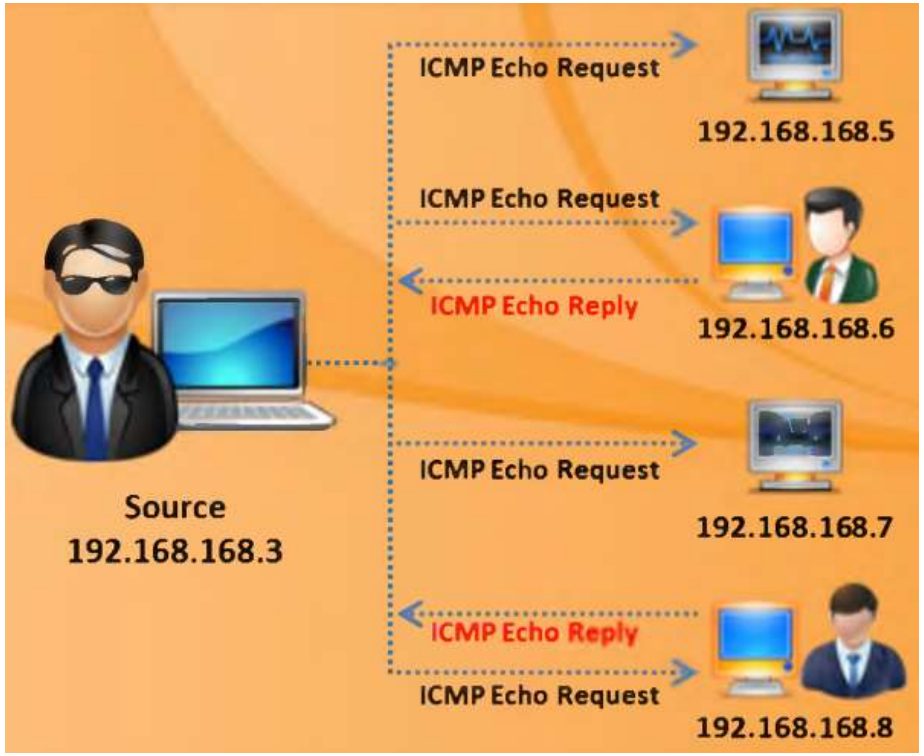
Scanning methodology

1) Check for **live systems**
2) Check for **open ports**
3) Scanning beyond IDS
4) Banner grabbing
5) Scanning for **vulnerabilities**
6) Draw network diagrams
7) Prepare proxies
8) Scanning Pen Testing



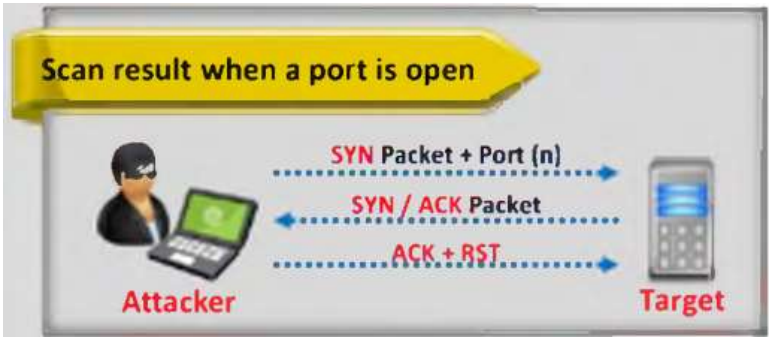
Check for live systems – ICMP Scanning

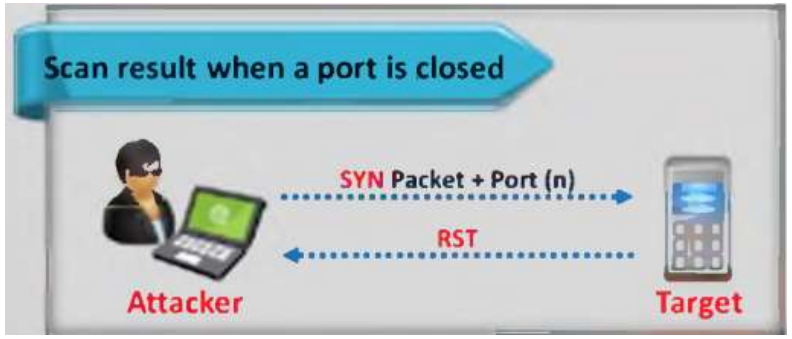
- Ping scan involves sending ICMP echo requests to a host. If the host is live, it will return an ICMP echo reply
- This scan is useful for locating active devices or determining if ICMP is passing through a firewall
- Tools: Nmap, Angry, IP Scanner, SolarWinds, Ping Scanning Pro,…

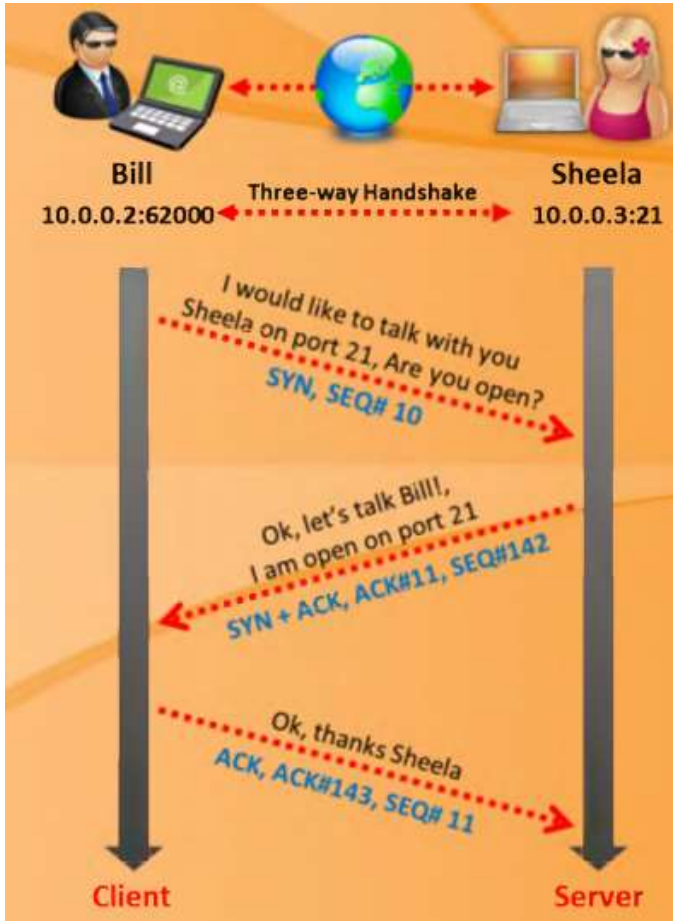


Check for open ports

- Three-way handshake: TCP uses a 3-way handshake to establish a connection between server and client
- TCP connect scan detects when a port is open by completing the 3-way handshake
- TCP connect scan establishes a full connection and tears it down by sending RST packet







Tools: Nmap, Hping

Check for open ports (cont.) – UDP Scanning

UDP Port Open

- There is no three-way TCP handshake for UDP scan
- The system does not respond with a message when the port is open

UDP Port Closed

- If a UDP packet is sent to closed port, the system responds with ICMP port unreachable message
- Spywares, Trojan horses, and other malicious applications use UDP ports

Tools: Nmap, NetScan Tools Pro, Advanced Port Scanner,…

Port Scanning Countermeasures

- Configure firewall, IDS rules: block unwanted ports
- Hide sensitive information from public view
- Ensure that mechanism used for routing & filtering at routers, firewalls cannot be bypassed

Scanning beyond IDS

IDS evasion techniques

- Use fragmented IP packets
- Use source routing
- Spoof IP address
- Proxy servers

Banner Grabbing

- Banner grabbing or OS fingerprinting is the method to determine the operating system running on a remote target system. There are two types of banner grabbing: active and passive
- Identifying the OS used on the target host allows an attacker to figure out the vulnerabilities the system poses and the exploits that might work on a system to further carry out additional attacks
- Tools: ID Serve, Netcraft, Netcat

Banner Grabbing Countermeasures

- Display false banners to misguide the attackers
- Turn off unnecessary services on the network host to limit the information disclosure

Vulnerability Scanning

- Vulnerability scanning identifies vulnerabilities and weaknesses of a system and network in order to determine how a system can be exploited
  - ✓Network topology and OS vulnerabilities
  - ✓Application and services vulnerabilities

✓Tools: SAINT, OpenVAS, Nexpose, Retina

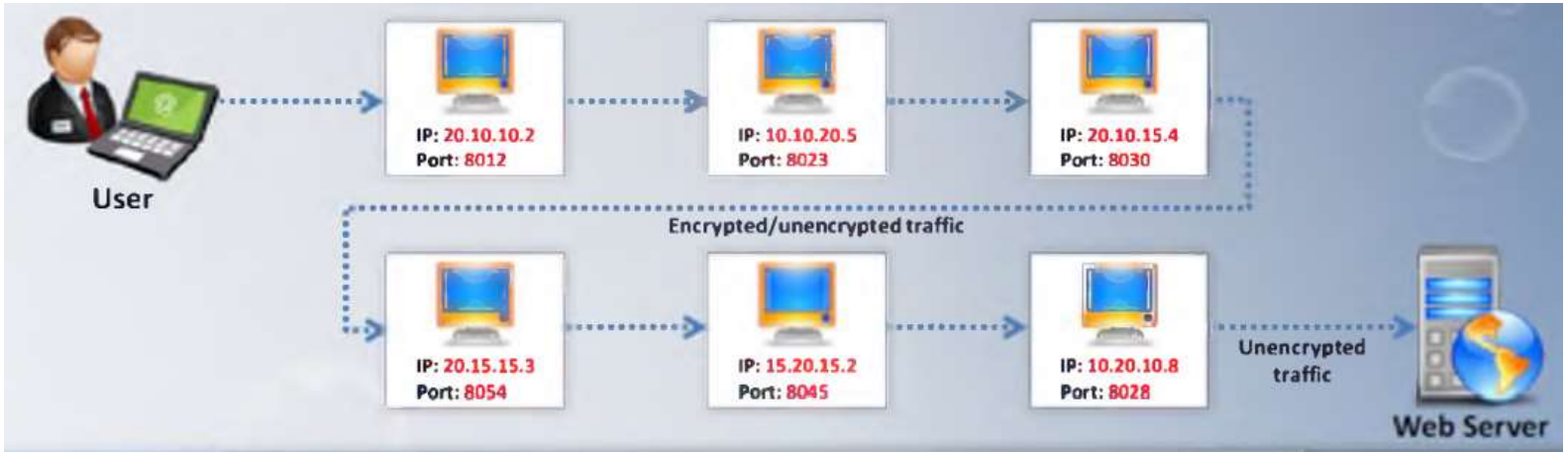
Draw network diagrams

- Drawing target's network diagram gives valuable information about the network and its architecture to an attacker
- Network diagram shows logical or physical path to a potential target
- Tools: Network View,…

Prepare proxies

- A proxy is a network computer that can serve as an intermediary for connecting with other computers

- Proxy chaining

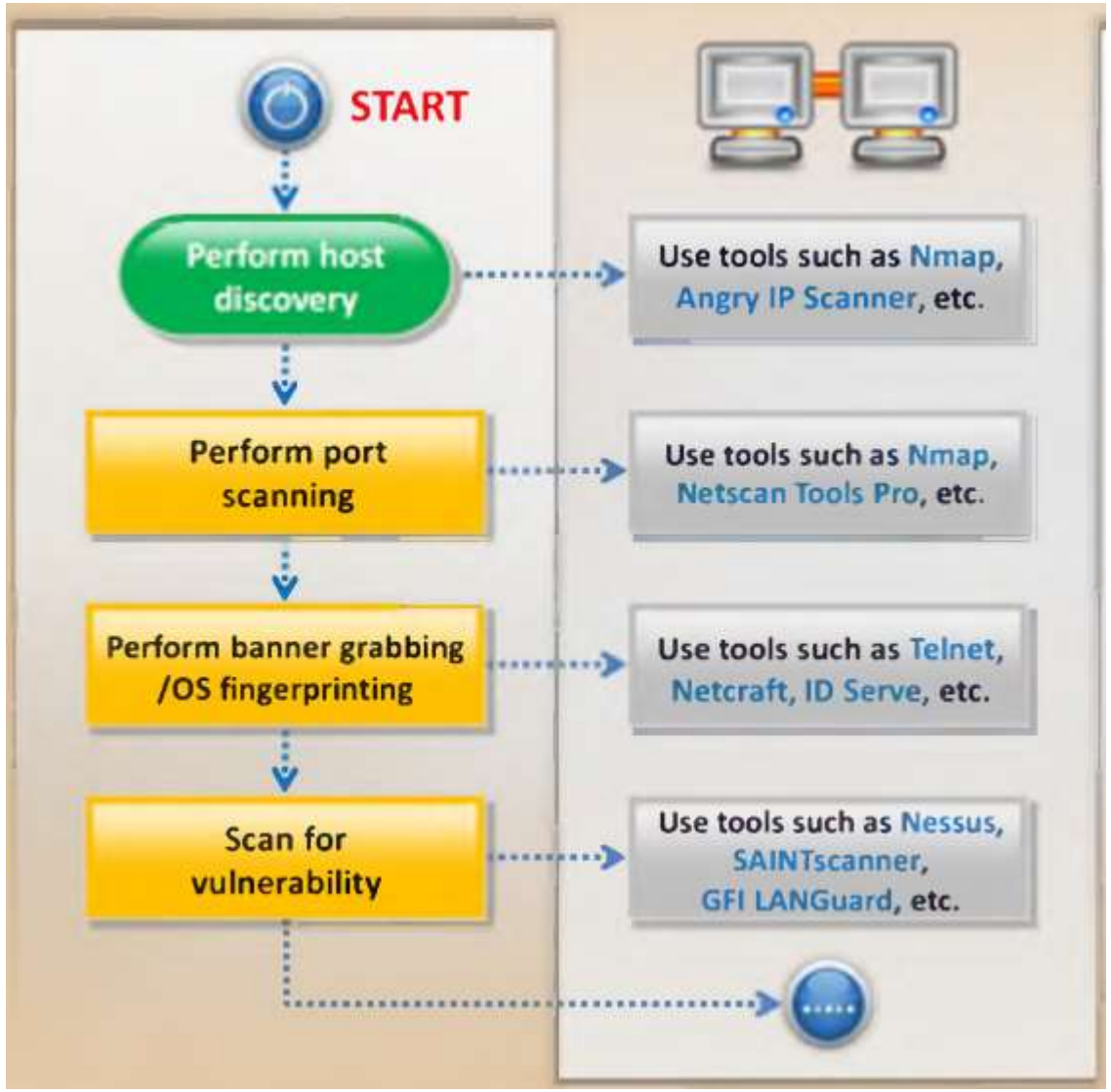


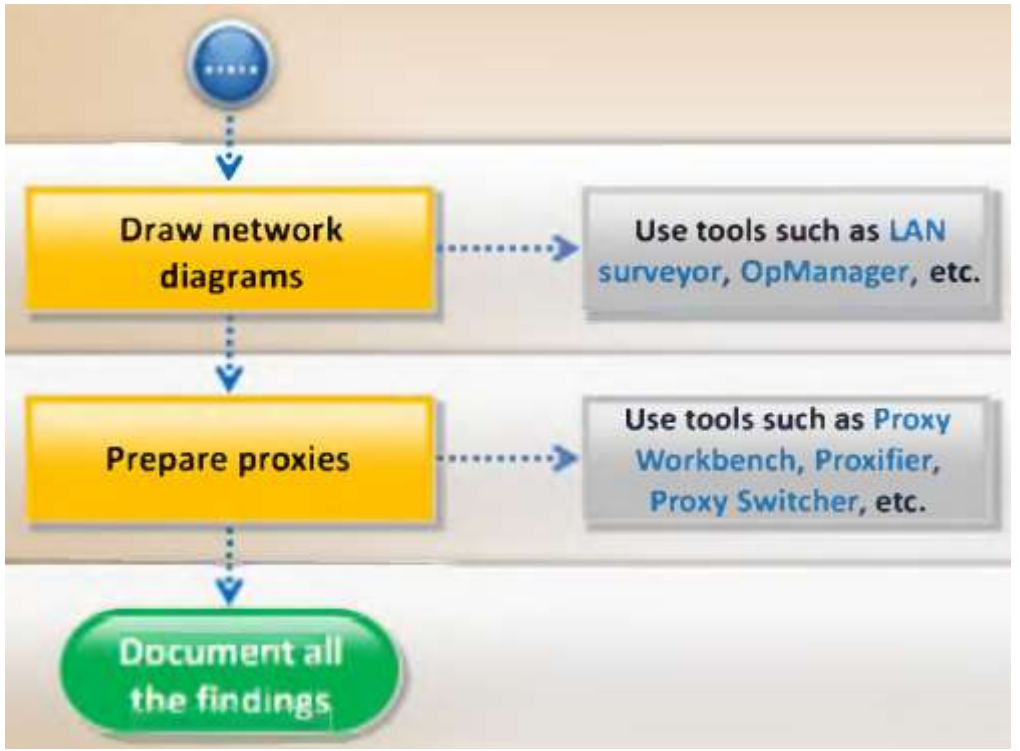
- Tools: ezProxy,…

Scanning Pen Testing

- Pen testing a network for scanning vulnerabilities determines the network's security posture by identifying live systems, discovering open ports, associating services and grabbing system banners to simulate a network hacking attempt
- The penetration testing report will help system administrators to:

Scanning Pen Testing





Summary

- **The objective of scanning** is to discover live systems, active/running ports, the operating systems, and the services running on the network
- Attacker determines the live hosts from a range of IP addresses by sending ICMP ECHO requests to multiple hosts
- Attackers use various scanning techniques to bypass firewall rules and logging mechanism, and hide them selves as usual network traffic
- Banner grabbing or OS finger printing is the method to determine the operating system running on a remote target system
- Drawing target's network diagram gives valuable in formation about the network and its architecture to an attacker
- Proxy is a network computer that can serve as an intermediary for connecting with other computers
- A chain of proxies can be created to evade a traceback to the attacker