Module 6
Scanning

Ansh Bhawnani

Basics of Scanning

Module 6

Basics of Scanning

- **“Knowing your enemy is winning half the war..”**
- 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.
- To hack the network, you will have to find a vulnerable point in the network that can be exploited. Network Scanning is used to find out such points in the network.

Basics of Scanning

- Scanning is done actively on the target.
- Network scanning can be done internally or from the Internet.

- **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

Scanning Methodology

Module 6

1. Checking for Live Systems

Module 6

Checking for Live Systems

- 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.

Checking for Live Systems

Ping Sweep:

- Used to determine the live hosts from a range of IP addresses by sending ICMP ECHO requests to multiple hosts.
- If a host is live, it will return an ICMP ECHO reply.
- Attackers calculate subnet masks using Subnet Mask Calculators to identify the number of hosts present in the subnet.
- Attackers then use ping sweep to create an inventory of live systems in the subnet.

2. TCP 3-Way Handshake

Module 6

TCP 3-Way Handshake

- **TCP Communication Flags:**
  - **URG** (Urgent): Data contained in the packet should be processed immediately
  - **FIN** (Finish): There will be no more transmissions
  - **RST** (Reset): Resets a connection
  - **PSH** (Push): Send all buffered data immediately
  - **ACK** (Acknowledgement): Acknowledges the receipt of a packet
  - **SYN** (Synchronize): Initiates a connection between hosts

TCP 3-Way Handshake

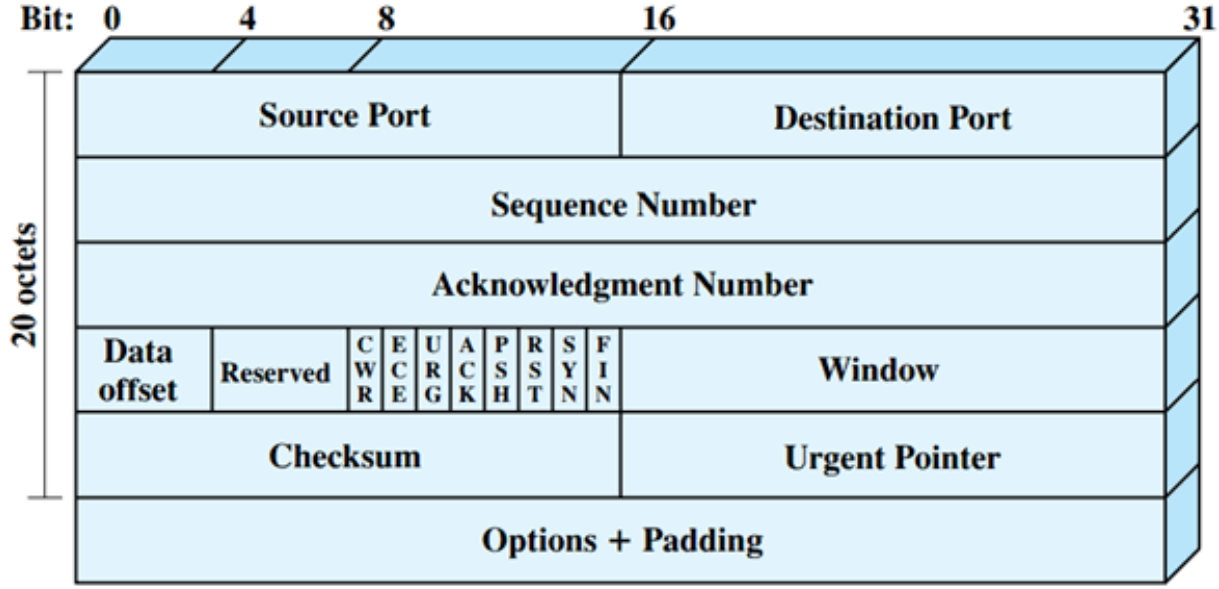
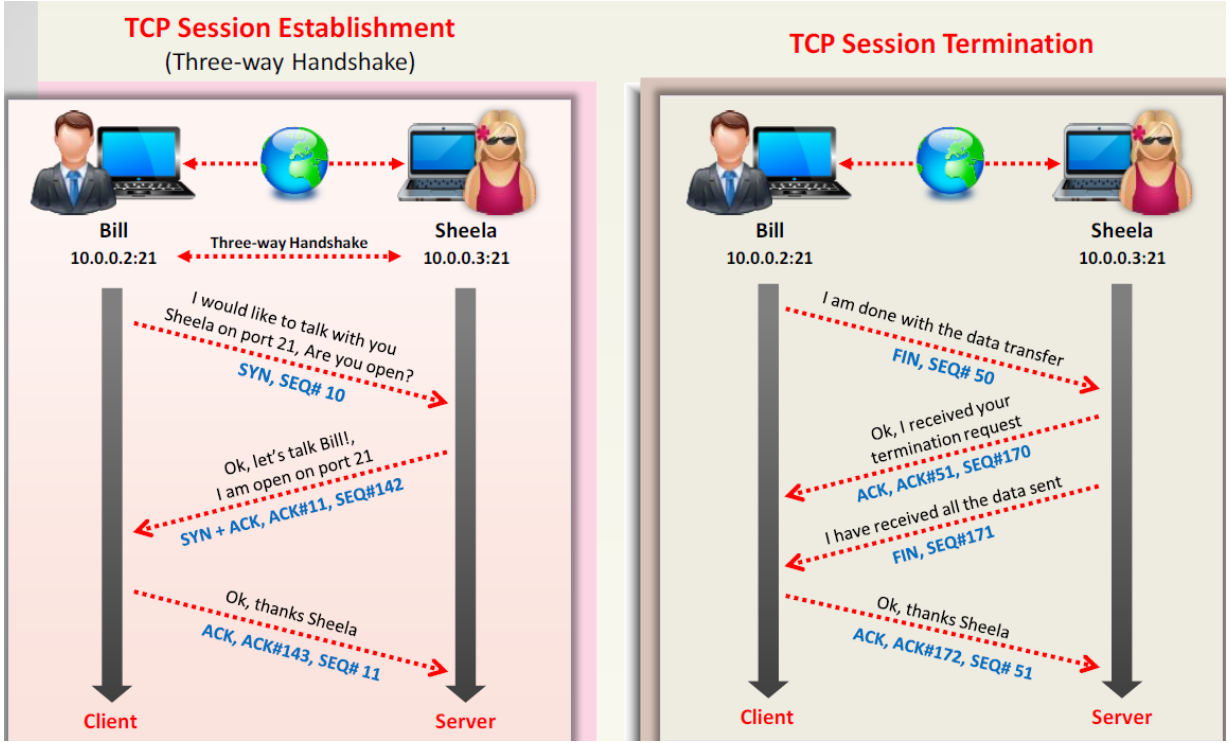


Figure TCP Header

TCP 3-Way Handshake



3. Check for open ports (Port Scanning)

Module 6

Port Scanning

- To run an exploit, an attacker needs a vulnerability.
- To find a vulnerability, the attacker needs to fingerprint all services which run on the machine (find out which protocol they use, which programs implement them and preferably the versions of those programs).
- To fingerprint a service, the attacker needs to know that there is one running on a publicly accessible port.
- To find out which publicly accessible ports run services, the attacker needs to run a port scan.

Port Scanning

- Port scanning is gathering attack surface for the victim against whom you want to launch attack or simply gathering loop holes of your own system (like network and system administrators)
- **States of ports:**
  - **Open:** Actively accepting TCP connections, UDP datagrams or SCTP associations
  - **Closed**: Accessible (it receives and responds to probe packets), but there is no application listening on it
  - **Filtered:** Packet filtering is enabled (firewall, router rules, etc.) and cannot determine open or closed

4. Port Scanning Methodology

Module 6

Port Scanning Methodology

Scanning Tool: Nmap

- Network administrators can use Nmap for network inventory, managing service upgrade schedules, and monitoring host or service uptime.
- Attacker uses Nmap to extract information such as live hosts on the network, services (application name and version), type of packet filters/firewalls, operating systems and OS versions.

Port Scanning Methodology

Scanning Tool: hping2/ hping3

- Command line network scanning and packet crafting tool for the TCP/IP protocol.
- It can be used for network security auditing, firewall testing, manual path MTU discovery, advanced traceroute, remote OS fingerprinting, remote uptime guessing, TCP/IP stacks auditing, etc..

Scanning Techniques

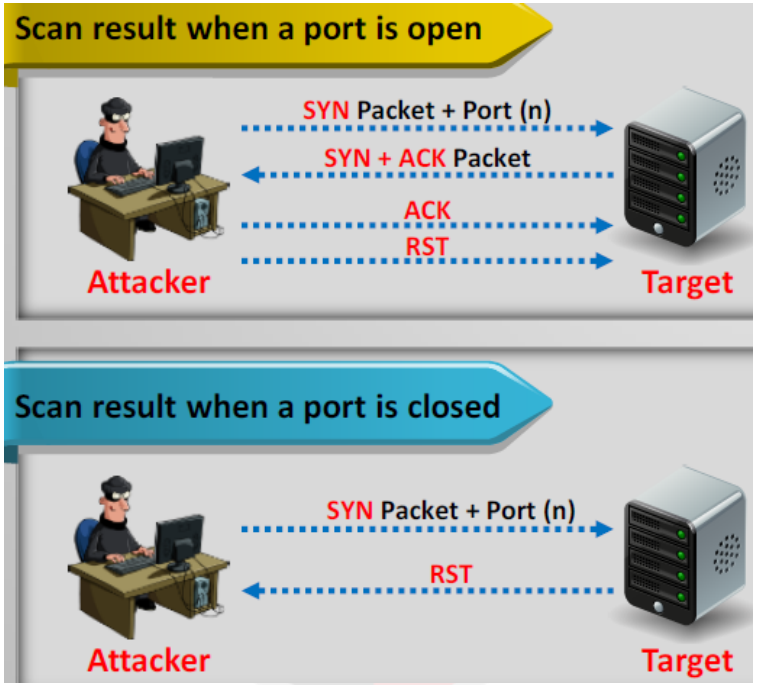
- **Scanning TCP Network Services**:
  - Open TCP Scanning Methods
    - TCP Connect / Full Open Scan
  - Stealth TCP Scanning Methods
    - Half-open Scan
    - Inverse TCP Flag Scanning
      - Xmas Scan
      - FIN Scan
      - NULL Scan
    - ACK Flag Probe Scanning
  - Third Party and Spoofed TCP Scanning Methods
    - IDLE / IP ID Header Scanning
- **Scanning UDP Network Services**:
  - UDP Scanning

Scanning Techniques

TCP Connect / Full Open Scan (-sT)

- TCP Connect scan detects when a port is open by completing the three-way handshake.
- TCP Connect scan establishes a full connection and tears it down by sending a RST packet.
- It does not require super user privileges.

Scanning Techniques

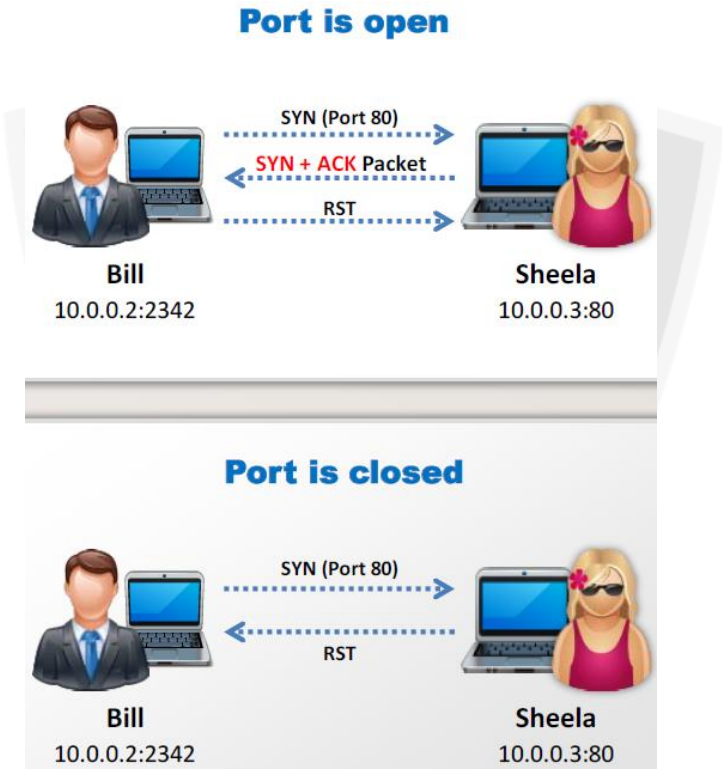


Scanning Techniques

Stealth Scan (Half-open Scan) (-sS)

- Resetting the TCP connection between client and server abruptly before completion of three-way handshake signals making the connection half open.
- Stealth Scan Process:
  - The client sends a single SYN packet to the server on the appropriate port.
  - If the port is open then the server responds with a SYN/ACK packet.
  - If the server responds with an RST packet, then the remote port is in the "closed" state.
  - The client sends the RST packet to close the initiation before a connection can ever be

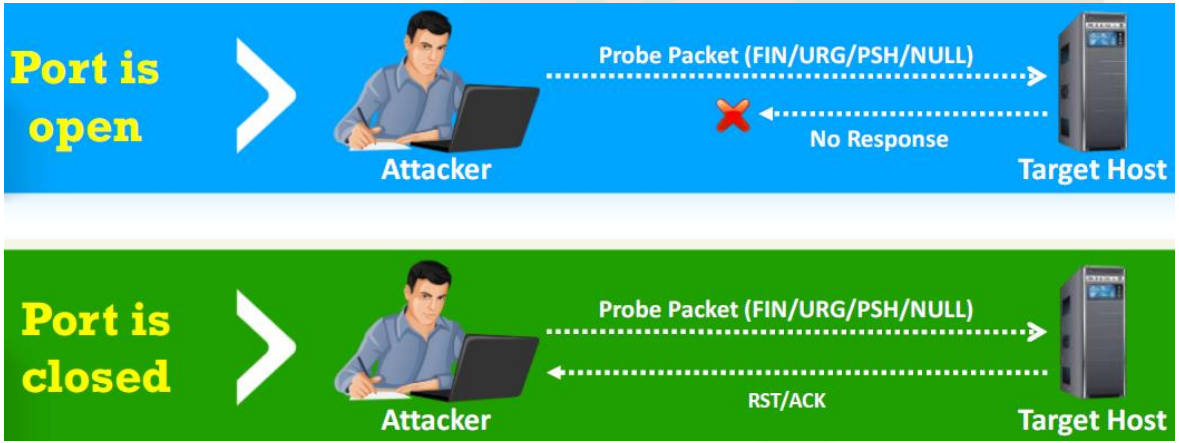
Scanning Techniques



Scanning Techniques

Inverse TCP Flag Scanning (-sF, -sN)

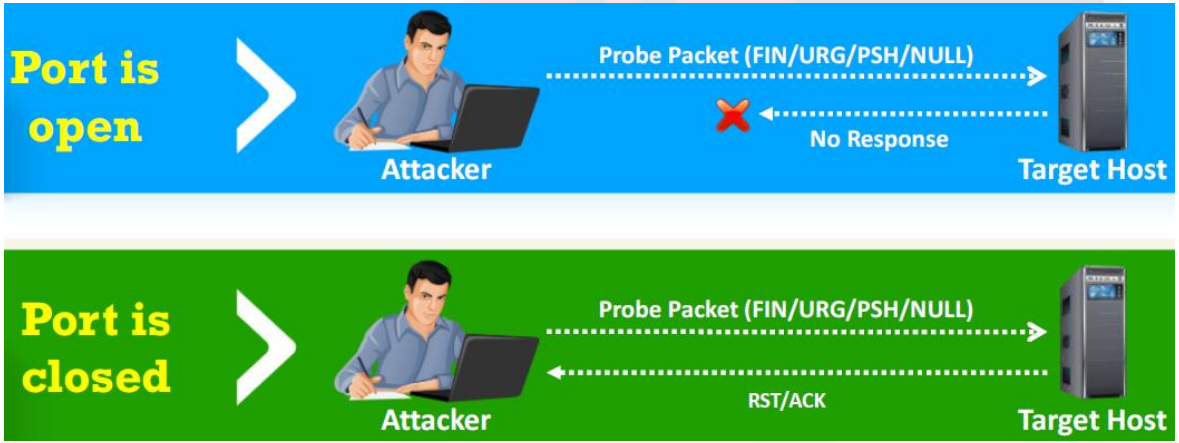
- TCP probe packets with a TCP flag (FIN, URG, PSH) set or with no flags, no response means port is open and RST means the port is closed.



Scanning Techniques

Xmas Scan (-sX)

- In Xmas scan, attackers send a TCP frame to a remote device with FIN, URG, and PUSH flags set.



Scanning Techniques

ACK Flag Probe Scanning (-sA)

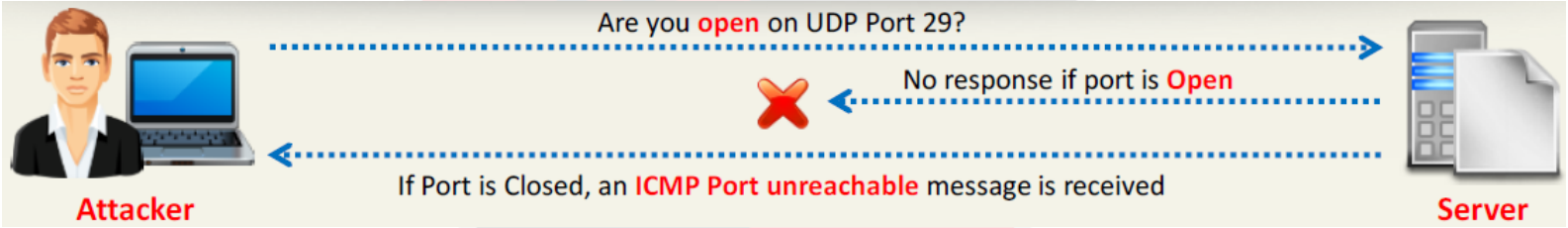
- Attackers send TCP probe packets with ACK flag set to a remote device and then analyzes the header information (TTL and WINDOW field) of received RST packets to find whether the port is open or closed.
- If the TTL value of RST packet on particular port is less than the boundary value of 64, then that port is open.
- If the WINDOW value of RST packet on particular port has non zero value, then that port is open.
- Attackers send an ACK probe packet with random sequence number, no response means port is filtered

Scanning Techniques

UDP Scanning (-sU)

- 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 (type 3, code 3).
  - Spywares, Trojan horses, and other malicious application use UDP ports.

Scanning Techniques



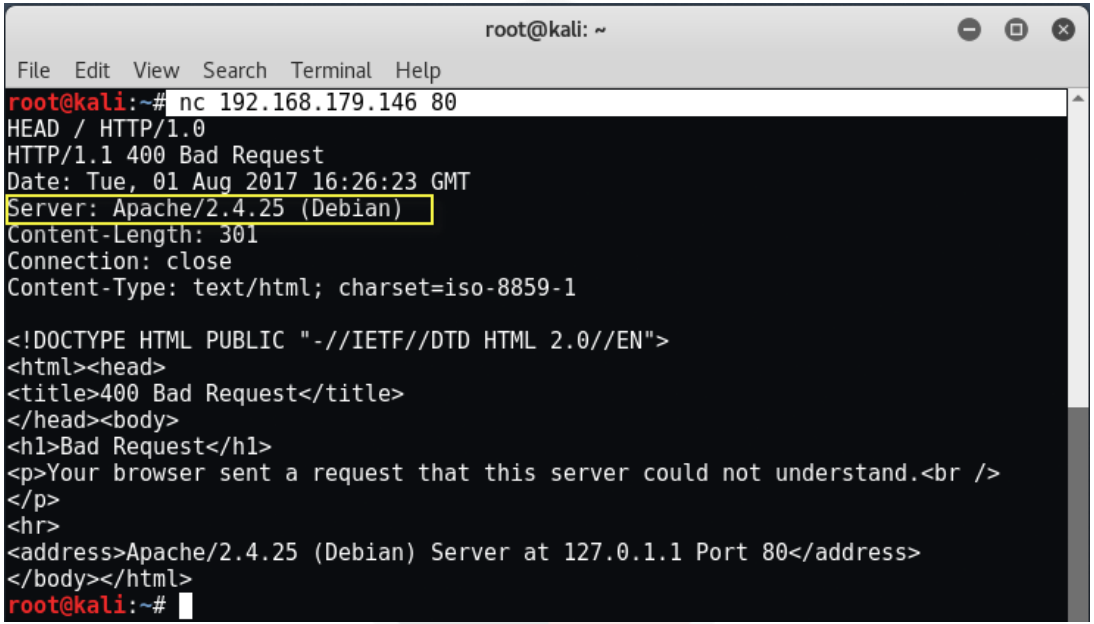
Banner Grabbing

Module 6

Banner Grabbing

- Banner grabbing or OS fingerprinting is the method to determine the operating system or software version 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 possesses and the exploits that might work on a system to further carry out additional attacks.

Banner Grabbing



Banner Grabbing

- **Active Banner Grabbing**:
  - Specially crafted packets are sent to remote OS and the responses are noted.
  - The responses are then compared with a database to determine the OS.
  - Response from different OSes varies due to differences in TCP/IP stack implementation.

Banner Grabbing

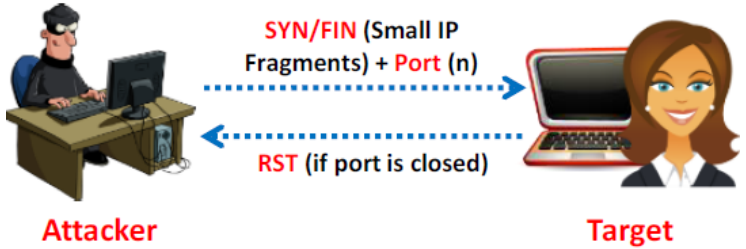
- **Passive Banner Grabbing**:
  - **Banner grabbing from error messages**: Error messages provide information such as type of server, type of OS, and SSL tool used by the target remote system.
  - **Sniffing the network traffic**: Capturing and analyzing packets from the target enables an attacker to determine OS used by the remote system.
  - **Banner grabbing from page extensions**: Looking for an extension in the URL may assist in determining the application version. Example: .aspx => IIS server and Windows platform.

Evading IDS, Firewalls

Module 6

Evading IDS, Firewalls

- Use fragmented IP packets.
- Spoof your IP address when launching attacks and sniff responses from server.
- Use source routing (if possible).
- Connect to proxy servers or compromised trojaned machine to launch attacks.



SYN/FIN Scanning

Scanning for Vulnerabilities

Module 6

Scanning for Vulnerabilities

- Vulnerability scanning identifies vulnerabilities and weaknesses of a system and network in order to determine how a system can be exploited.
  - **Network vulnerabilities**
  - **Open ports and running services**
  - **Application and services vulnerabilities**
  - **Application and services configuration errors**

Mapping Networks (Visual Mapping)

Module 6

Network Visual Mapping

- 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.

- **Network Discovery Tool**
  - LANSurveyor
  - Network Topology Mapper
  - OpManager
  - NetworkView

Countermeasures

Module 6

Countermeasures

Port Scanning Countermeasures

- Configure firewall and IDS rules to detect and block probes.
- Run the port scanning tools against hosts on the network to determine whether the firewall properly detects the port scanning activity.
- Ensure that mechanism used for routing and filtering at the routers and firewalls respectively cannot be bypassed using particular source ports or source-routing methods.
- Ensure that the anti scanning and anti spoofing rules are configured.

Countermeasures

Port Scanning Countermeasures

- Ensure that the router, IDS, and firewall firmware are updated to their latest releases.
- Use custom rule set to lock down the network and block unwanted ports at the firewall.
- Filter all ICMP messages (i.e. inbound ICMP message types and outbound ICMP type 3 unreachable messages) at the firewalls and routers.
- Perform TCP and UDP scanning along with ICMP probes against your organization's IP address space to check the network configuration and its available ports.

Countermeasures

Banner Grabbing Countermeasures

Disabling or Changing Banner

- Display false banners to misguide attackers.
- Turn off unnecessary services on the network host to limit the information disclosure.
- Use ServerMask tools to disable or change banner information.
- Use a directive in httpd.conf file to change banner information
- Alternatively, change the ServerSignature line to ServerSignature Off in httpd.conf file.

Countermeasures

Banner Grabbing Countermeasures

Hiding File Extensions from Web Pages

- File extensions reveal information about the underlying technology
- Hide file extensions to mask the web technology.
- Change application mappings such as .asp with .htm or .foo, etc. to disguise the identify of the servers.
- Apache users can use mod_negotiation directives.
- IIS users use tools such as PageXchanger to manage the file extensions.
- It is even better if the file extensions are not at all used.

HACKING

Is an art, practised through a creative mind.