IT3789 Cyber Security Attack & Defence

L8 – Vulnerability Identification (2)

WITH KNOWLEDGE COMES RESPONSIBILITY

Vulnerability Identification

Scanning

War Dialling

Network Mapping

Port Scanning

Vulnerability Scanning

Port Scanning

- Port Scanning Objectives:
  1. Verification of the existence of the system.
  2. Check for open ports that accept connection.
- Yields more information than ping sweep.
- Service identification is usually performed using the same tools as port scanning.
  - Open ports can be associated to services running in target system.

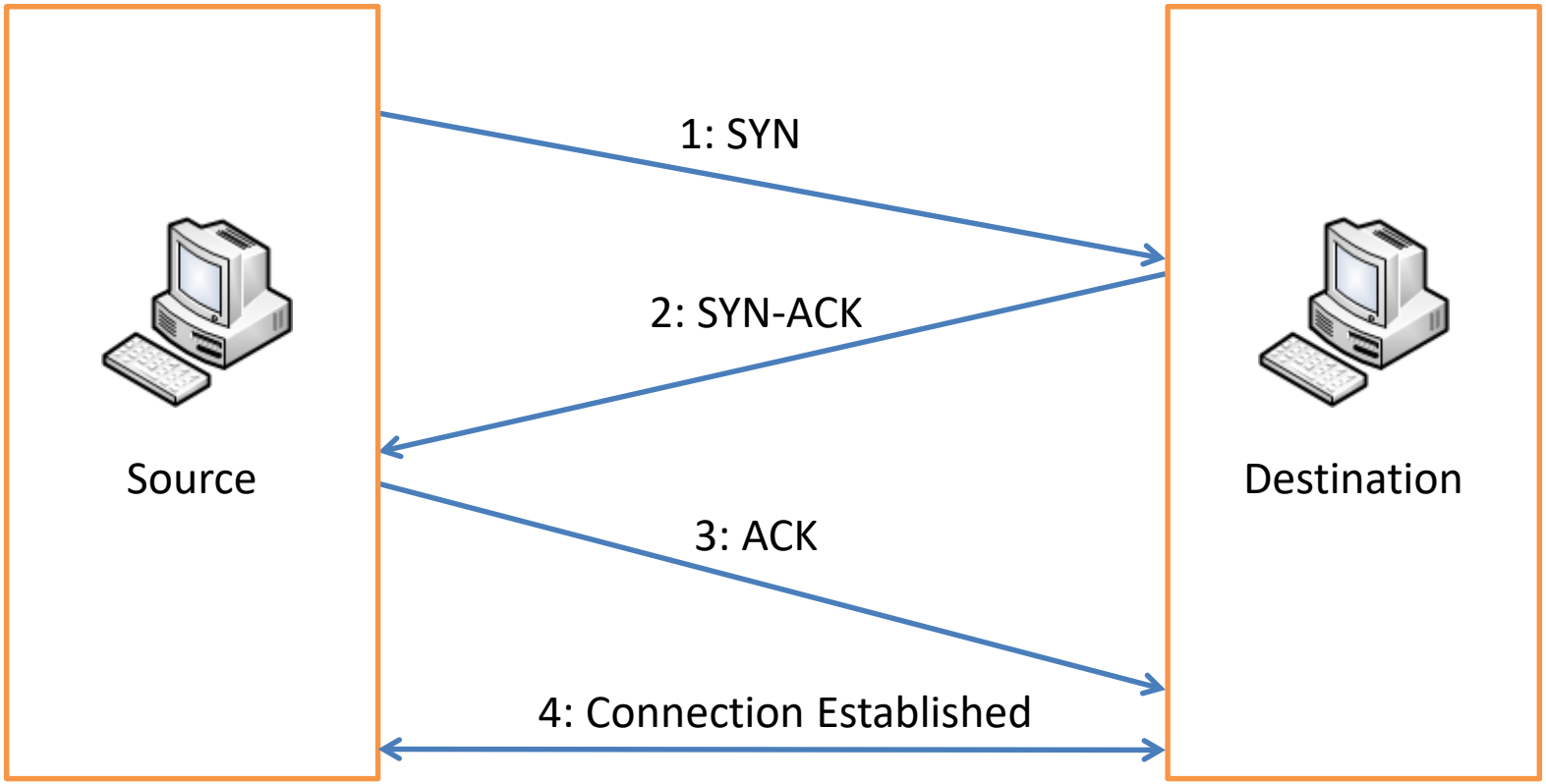
Port Scanning

- Scan for open ports using port scanners such as Nmap.
- When a server application or service is listening on a port, that port is open.
  - Can be a destination of IP traffic.
- Ports reveal what types of service are running.
  - Port assignments are listed at IANA web site
    - http://www.iana.org/assignments/port-numbers
  - A list of potential ways into the system.
    - http://www.bekkoame.ne.jp/~s_ita/port/

TCP Connection Basics

- Uses 6 TCP flags that are set in packets.
  - SYN: Initial request that is sent by the sender to establish connection.
  - ACK: Acknowledgement to the request
  - FIN: Finish request that is sent to end the connection.
  - URG: Urgent request signifies that the segment contains urgent data.
  - PSH: Push request indicates data to be send out and receive immediately.
  - RST: Reset indicates that receiver wants to abort the connection.
- Combination of these flags sets the control connection session at various times.

TCP Connection Basics



3-Way Handshake

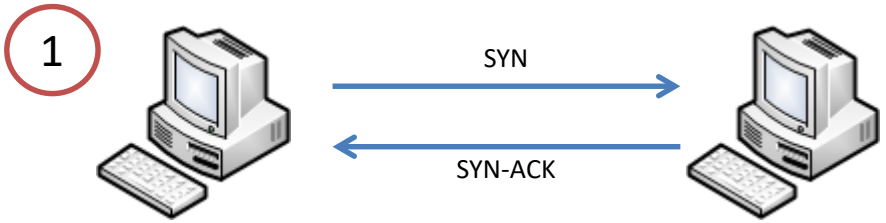
Nmap

- Nmap is an open source port scanning tool.
- Functionalities of Nmap
  - Port scanning
  - OS fingerprinting
  - Service fingerprinting
  - Vulnerability scanner (Nmap Scripting Engine - NSE)

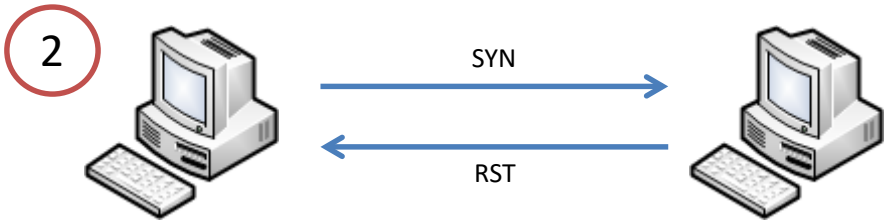
Reference: www.insecure.org, www.nmap.org

Scanning TCP Ports

- Attempts to establish a TCP connection with target port.

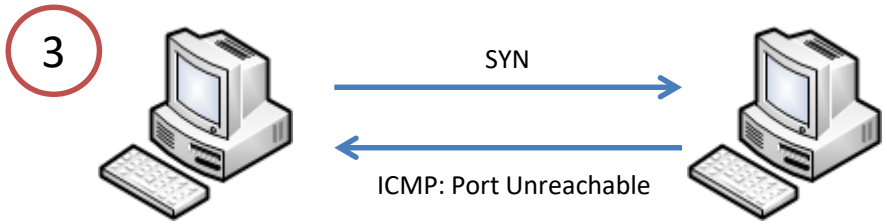


- If target responds with SYN-ACK, then port is opened.

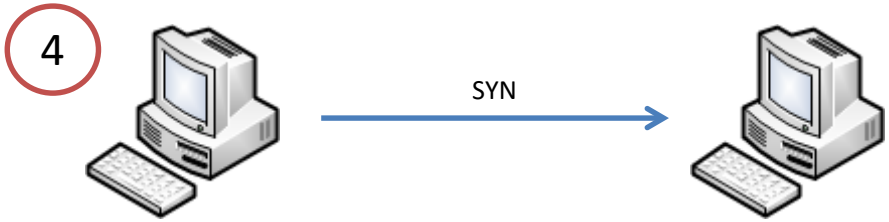


- If target responds with RST, then port is closed.

Scanning TCP Ports



- If target responds with ICMP port unreachable, then likely a firewall is blocking the traffic to the port.



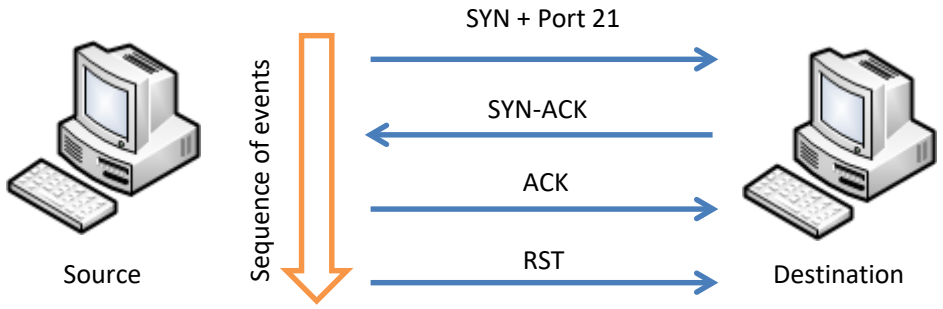
- If target does not respond, then likely a firewall is blocking the traffic to the port.

TCP Scan: TCP Connect Scan/Full Scan

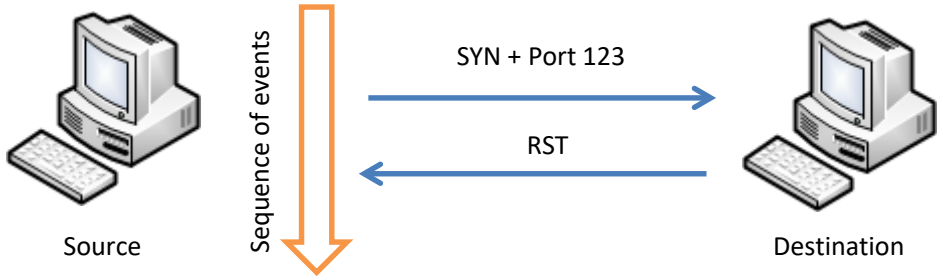
- Make a full TCP connection to the target system to determine if a port is available.
- Used when there is no other option.
- Advantage:
  - TCP-based methods that any user can employ, no additional rights or privileges are required.
- Disadvantages:
  - Takes longer and require more packets to obtain the same information.
  - Target machines are more likely to log the connection.

TCP Scan: TCP Connect Scan/Full Scan

- The target responses with SYN-ACK if port is opened.



- The target responses with RST if port is closed.

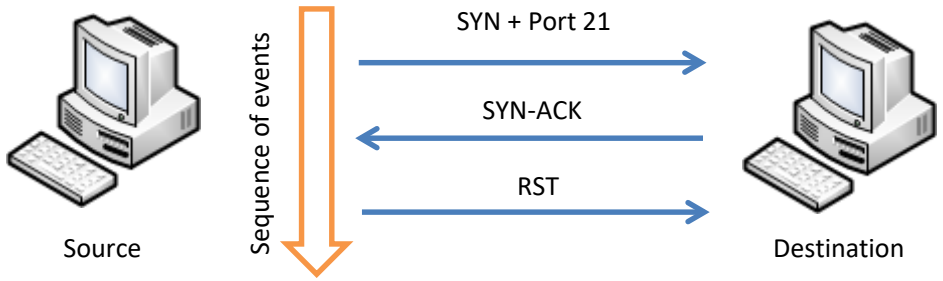


TCP Scan: Half Open Scan/SYN Stealth Scan

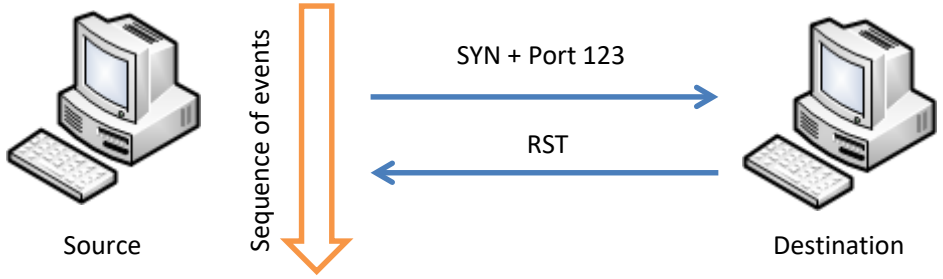
- Gather information about open port without completing the TCP handshake.
  - Less stressful to the application service.
  - Less visibility in the target system's application logs since no sessions are ever initiated.
- Common scan when looking for open ports on a remote device.
- Advantages:
  - Evading most IDS and firewalls as it seems like a standard TCP request.
  - Allows clear, reliable differentiation between the open, closed and filtered states.
  - Faster than connect scan.
- Disadvantages:
  - Root privileges are required to build raw packets necessary for the half-open connection process.

TCP Scan: Half Open Scan/SYN Stealth Scan

- The target responses with SYN-ACK if port is opened.



- The target responses with RST if port is closed.

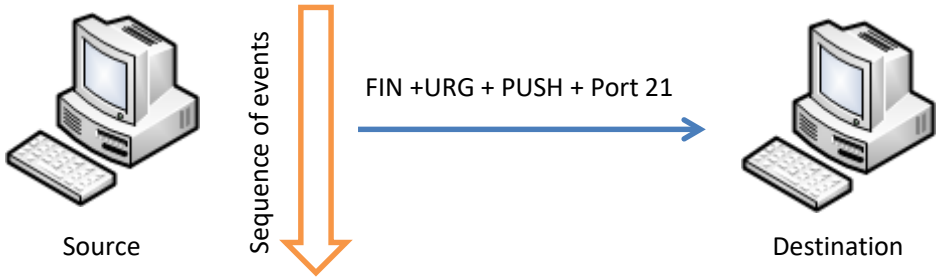


TCP Scan: XMAS/FIN/Null Scan

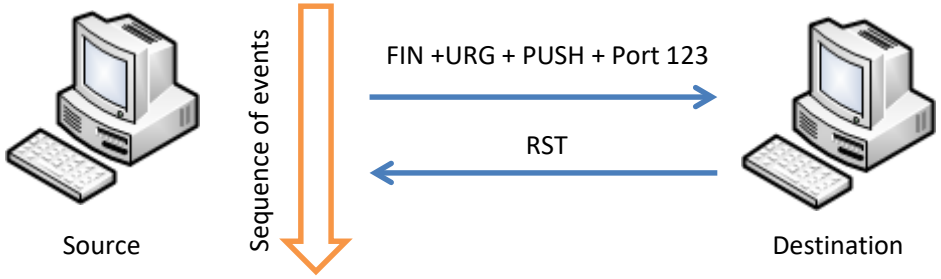
- XMAS Scan: By sending malformed packet with FIN, URG and PSH flags set.
- FIN Scan : By sending malformed packet with FIN flag set.
- Null Scan: By sending malformed packet with no flag set.
- Advantages:
  - Used to bypass some non-stateful firewalls as usually these firewalls only filter SYN packets.
  - No TCP sessions are created, therefore, nothing should appear in the application logs.
  - Very little network bandwidth is required.
- Disadvantages:
  - Works only on most Unix-based system (systems that follow RFC 793 implementation of TCP/IP).
  - Does not work against Microsoft Windows, many Cisco devices, BSDI, and IBM OS/400.
  - Cannot distinguish open ports from filtered ones.

TCP Scan: XMAS Scan

- If there is no response from the target, the port is either opened or the target is filtered behind a firewall.

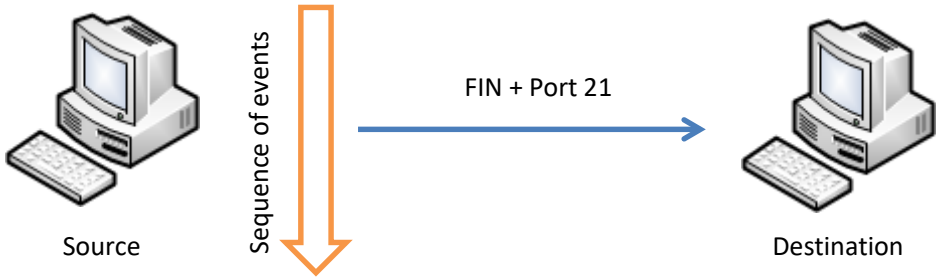


- The target responses with RST if port is closed.

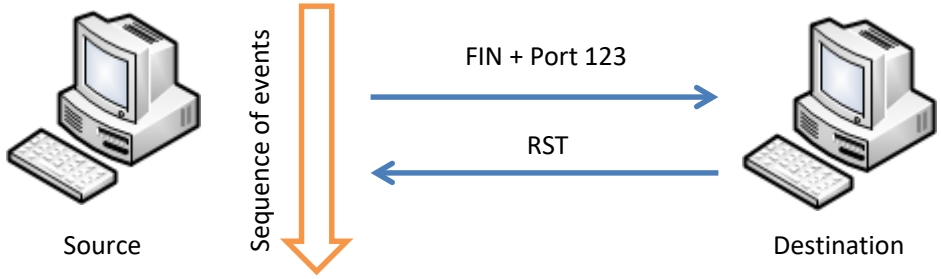


TCP Scan: FIN Scan

- If there is no response from the target, the port is either opened or the target is filtered behind a firewall.

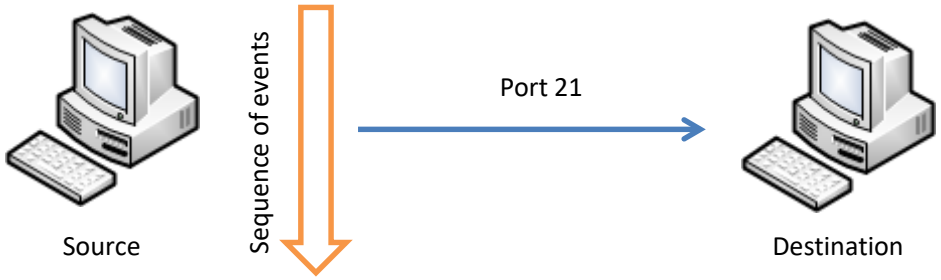


- The target responses with RST if port is closed.

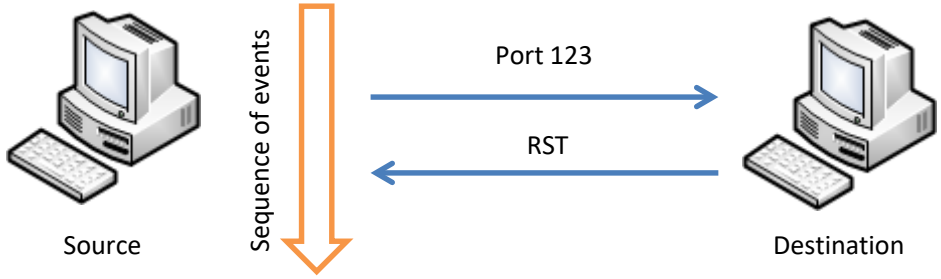


TCP Scan: Null Scan

- If there is no response from the target, the port is either opened or the target is filtered behind a firewall.



- The target responses with RST if port is closed.

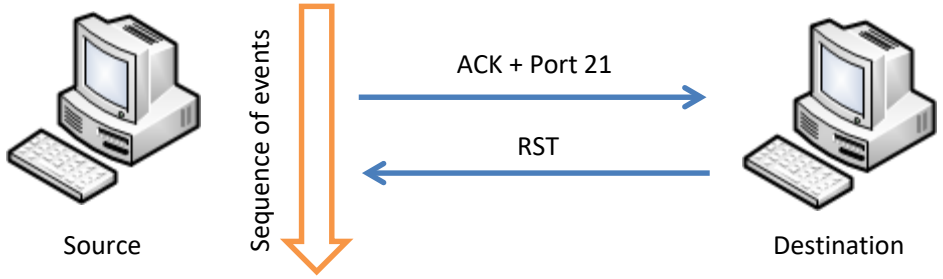


TCP Scan: ACK Scan

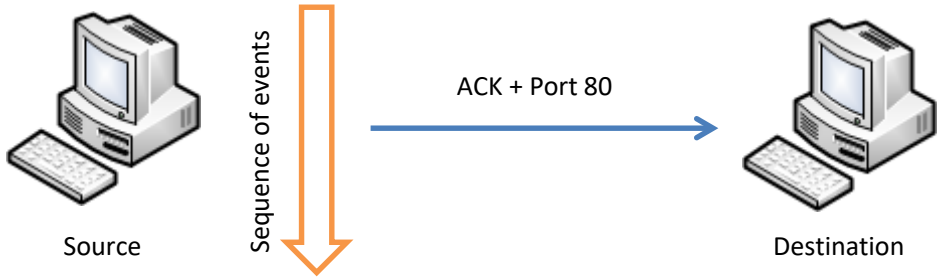
- Send an ACK packet to target.
- Used to map out firewall rules.
  - Determine whether firewalls are stateful or not.
  - Determine which ports are filtered or unfiltered.
  - Does not determine which ports are open or closed.
- Advantage:
  - Scan is unobtrusive and almost invisible when combined with the other network traffic.
- Disadvantage:
  - Can never identify an open port.

TCP Scan: ACK Scan

- The target responses with RST if port is opened or closed (unfiltered or no firewall is present).



- Port is filtered behind a stateful firewall if the target does not response **OR** an ICMP destination unreachable message is returned.

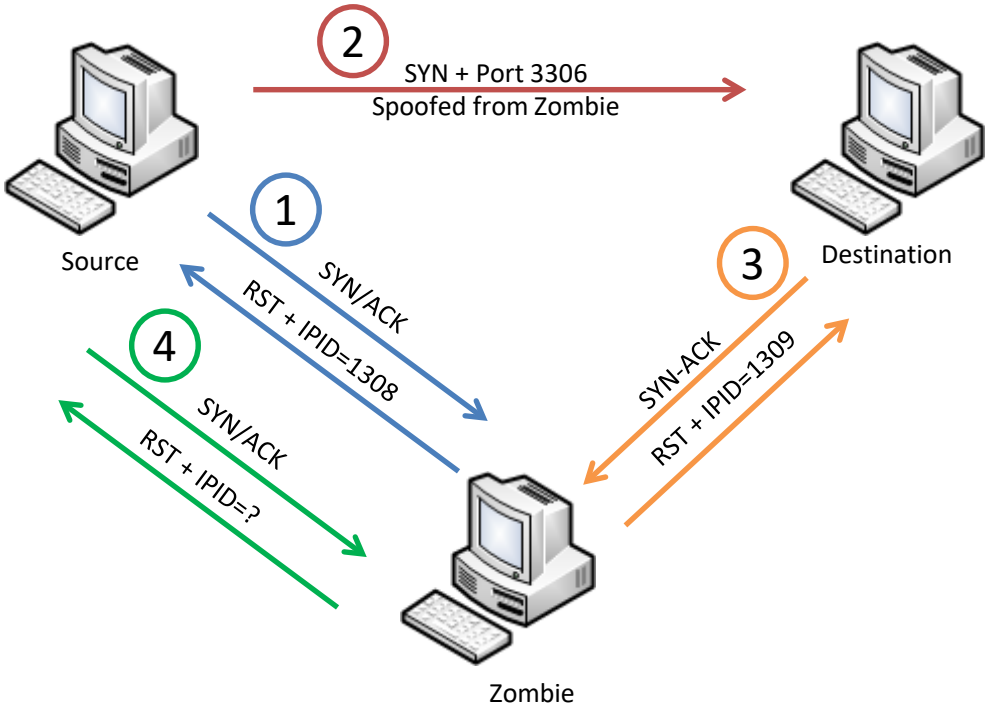


TCP Scan: IDLE Scan

- Uses a spoofed IP address to send SYN packet to a target.
  - Similar to ACK Scan
- Determine port scan response by monitoring IP header sequence numbers.
- Advantage:
  - The target will never see the IP address of the machine performing the scan.
- Disadvantage:
  - Can only locate ports.
    - OS fingerprinting and version detection cannot be performed.
  - The zombie must be an idle station.
  - There will be more network traffic than a normal port scan due to IDLE scan's bulk processing.

TCP Scan: IDLE Scan

- If the IPID has incremented (IPID=1310), then the port is opened on the destination.
- If the IPID has not incremented (IPID=1309), then the port is closed.

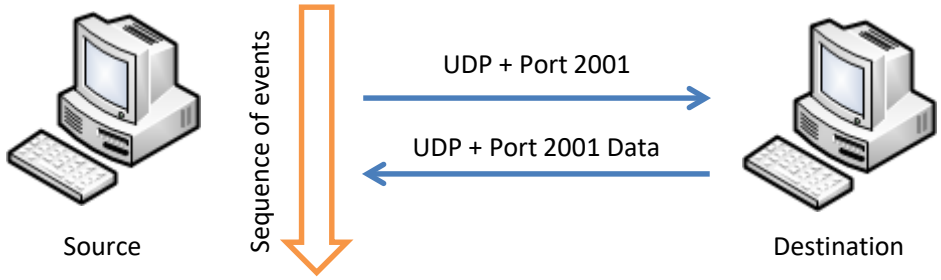


UDP Connection Basics

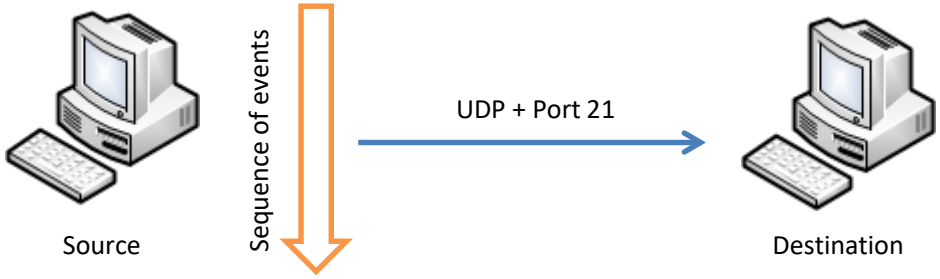
- UDP is a connectionless protocol and does not involve a 3 way handshake.
- UDP port scanning is often unreliable and slower.
- Less options as there is no control bits like in TCP.

UDP Scan

- The target responses with UDP data if port is opened.



- The target does not response if port is filtered or firewall blocked , the UDP packet can also be lost along the route.

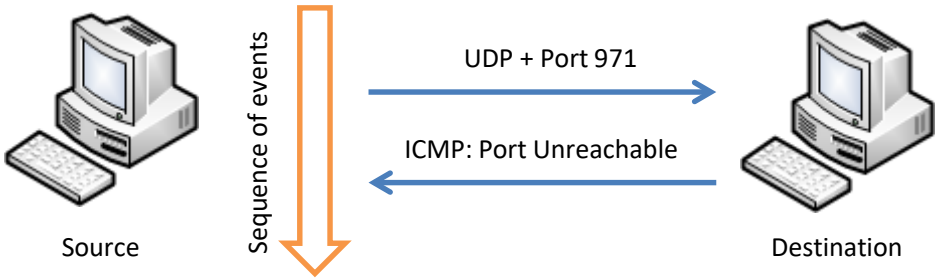


Possible Reasons:

1. Port is filtered.
2. Firewall is blocking inbound or outbound port.
3. Service on port ignores packet as it is looking for a specific payload.

UDP Scan

- Port is closed if an ICMP port unreachable message is returned.
  - If ICMP unreachable errors (type 3, code 3), the port is marked as closed.
  - If ICMP unreachable errors (type 3, codes 1, 2, 9, 10 or 13), the port is marked as filtered.



Stealth Scanning

- Varies time and frequency of scan to avoid detection by IDS.
  - Scan random ports until all have been covered.
  - Reduce the speed of the scan.
- Technique used in combination with other scans such as SYN Stealth Scan.
- Full connect scan can never be stealth.

Nmap Scan Summary

Nmap Scan	Command Syntax	Requires Privileged Access	Identifies TCP Ports	Identifies UDP Ports
TCP SYN Scan	`-sS`	YES	YES	NO
TCP connect() Scan	`-sT`	NO	YES	NO
FIN Scan	`-sF`	YES	YES	NO
Xmas Tree Scan	`-sX`	YES	YES	NO
Null Scan	`-sN`	YES	YES	NO
Ping Scan	`-sP`	NO	NO	NO
Version Detection	`-sV`	NO	NO	NO
UDP Scan	`-sU`	YES	NO	YES
IP Protocol Scan	`-sO`	YES	NO	NO
ACK Scan	`-sA`	YES	YES	NO
Window Scan	`-sW`	YES	YES	NO
RPC Scan	`-sR`	NO	NO	NO
List Scan	`-sL`	NO	NO	NO
Idlescan	`-sI`	YES	YES	NO
FTP Bounce Attack	`-b`	NO	YES	NO

Source: https://www.professormesser.com/nmap/optimizing-your-nmap-scan-nmap-scanning-methods/

Vulnerability Identification

Scanning

War Dialling

Network Mapping

Port Scanning

Vulnerability Scanning

Vulnerability Identification

1. Identified and verified applications running on target systems.
2. Search the Web to see if any exploits available for the applications or OS on target systems.
   - http://www.nvd.nist.gov
   - http://www.exploit-db.com
   - http://www.securityfocus.com

Vulnerability Scanning

- Scan for known vulnerabilities using tools such as Nessus and Core Impact.
- At this point, attacker knows which systems are available, how they are connected, and which ports are open.
- Vulnerability scanning tools look for holes on the target due to
  - Misconfigurations
  - Unpatched systems with known vulnerabilities
  - Other weaknesses
- By rapidly checking for thousands of known vulnerabilities, attacker can get in faster.

Vulnerability Identification (2)

Port Scanning

- TCP Connection Basics
- TCP Scan
- UDP Connection Basics
- UDP Scan
- Stealth Scanning
- Nmap Scan Summary

Vulnerability Identification

- Vulnerability Scanning