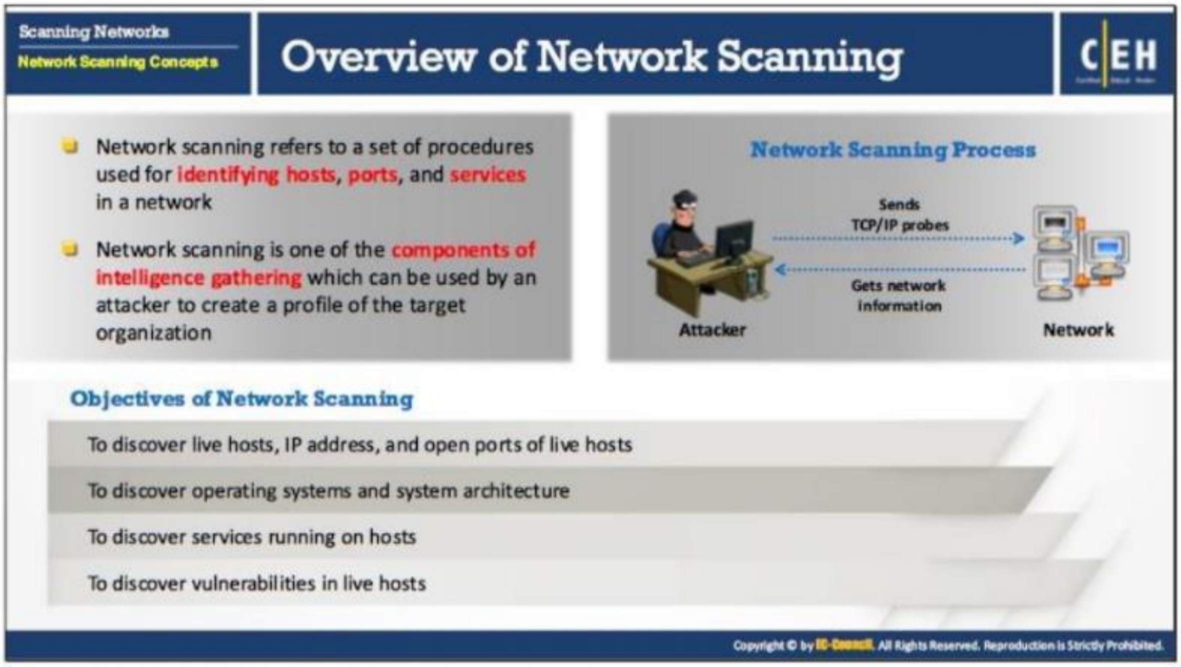


Scanning Networks

Network Scanning Concepts

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

Sends TCP/IP probes
Gets network information
Attacker
Network

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

Types of Scanning

- **Port Scanning** – Lists the open ports and services. Port scanning is the process of checking the services running on the target computer by sending a sequence of messages in an attempt to break in. Port scanning involves connecting to or probing TCP and UDP ports on the target system to determine if the services are running or are in a listening state.

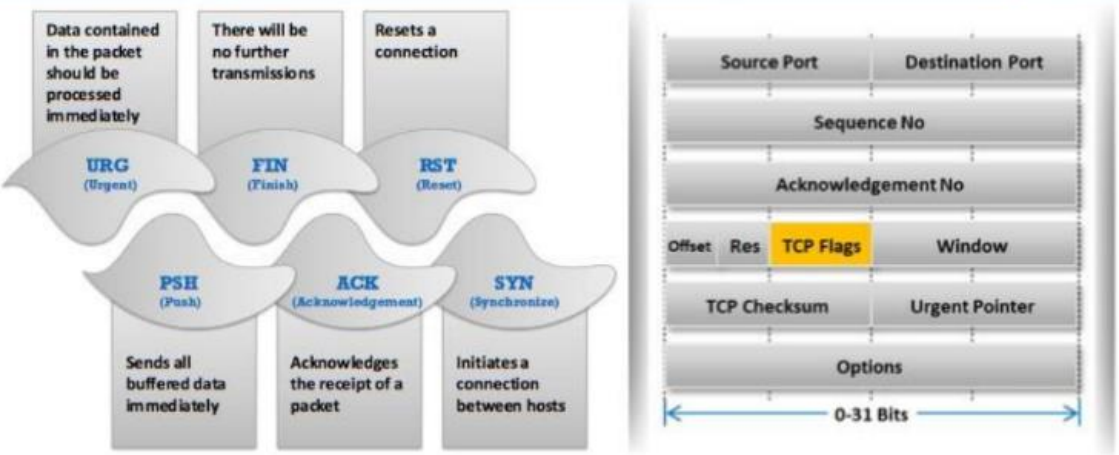
- **Network Scanning** – Lists IP addresses. Network scanning is a procedure for identifying active hosts on a network, either to attack them or to assess the security of the network.

- **Vulnerability Scanning** – Shows the presence of known weaknesses. Vulnerability scanning is a method used to check whether a system is exploitable by identifying its vulnerabilities. A vulnerability scanner consists of a scanning engine and a catalog. The

Scanning Networks

Network Scanning Concepts

TCP Communication Flags



Standard TCP communications are controlled by flags in the TCP packet header

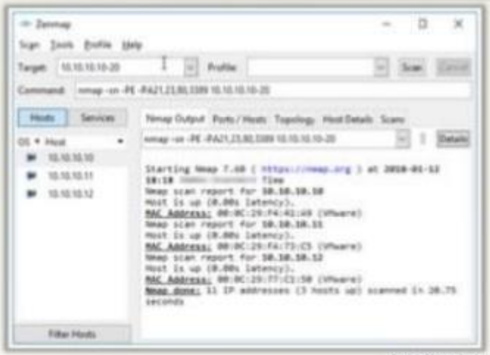
Scanning Networks

Scanning Techniques

Ping Sweep - Checking for Live Systems

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

The ping sweep output using Nmap



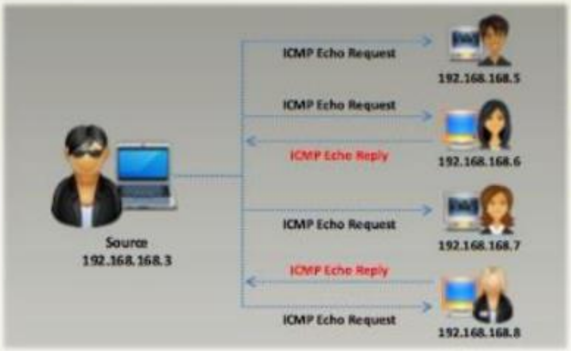
Target: 10.10.10.10-20

Command: nmap -sn -PE -PA21,23,80,3389 10.10.10.10-20

10.10.10.10
10.10.10.11
10.10.10.12

```
Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-12
10:10 [illegible] Time
Nmap scan report for 10.10.10.10
Host is up (0.00s latency).
MAC Address: 00:0C:29:F4:41:A9 (VMware)
Nmap scan report for 10.10.10.11
Host is up (0.00s latency).
MAC Address: 00:0C:29:F4:73:C5 (VMware)
Nmap scan report for 10.10.10.12
Host is up (0.00s latency).
MAC Address: 00:0C:29:77:C1:50 (VMware)
Nmap done: 11 IP addresses (3 hosts up) scanned in 20.75
seconds
```

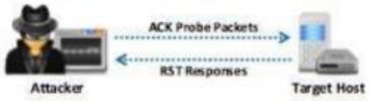
https://nmap.org

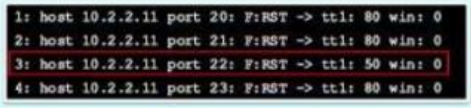


ACK Flag Probe Scanning

- 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 out if the **port is open or closed**

TTL based ACK flag probe scanning

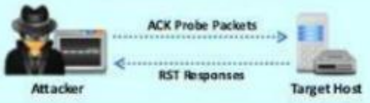


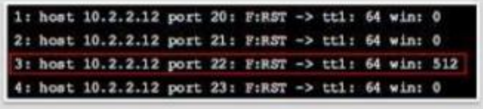


```
1: host 10.2.2.11 port 20: F:RST -> ttl: 80 win: 0
2: host 10.2.2.11 port 21: F:RST -> ttl: 80 win: 0
3: host 10.2.2.11 port 22: F:RST -> ttl: 50 win: 0
4: host 10.2.2.11 port 23: F:RST -> ttl: 80 win: 0
```

If the **TTL value of RST packet** on a particular port is less than the boundary value of **64**, then that **port is open**

WINDOW based ACK flag probe scanning

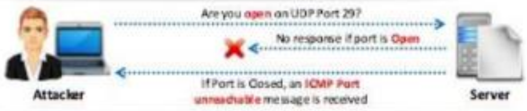




```
1: host 10.2.2.12 port 20: F:RST -> ttl: 64 win: 0
2: host 10.2.2.12 port 21: F:RST -> ttl: 64 win: 0
3: host 10.2.2.12 port 22: F:RST -> ttl: 64 win: 512
4: host 10.2.2.12 port 23: F:RST -> ttl: 64 win: 0
```

If the **WINDOW value of RST packet** on a particular port has a **non zero value**, then that **port is open**

UDP Scanning

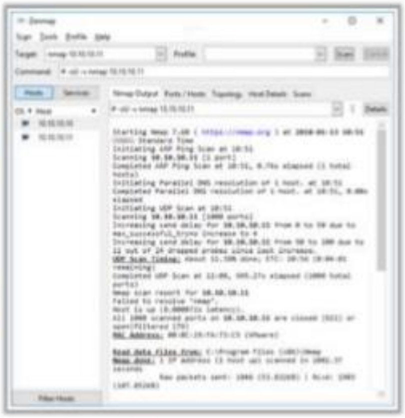

Are you open on UDP Port 29?
No response if port is Open
If Port is Closed, an ICMP Port unreachable message is received
Attacker
Server

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**

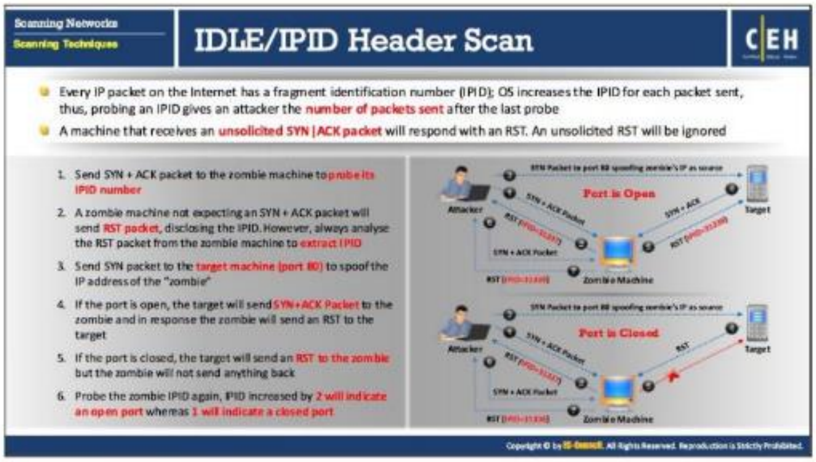
UDP Port Closed

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



```
Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-13 10:51
[illegible] Standard Time
Initiating ARP Ping Scan at 10:51
Scanning 10.10.10.11 [1 port]
Completed ARP Ping Scan at 10:51, 0.74s elapsed (1 total
hosts)
Initiating Parallel DNS resolution of 1 host. at 10:51
Completed Parallel DNS resolution of 1 host. at 10:51, 0.00s
elapsed
Initiating UDP Scan at 10:51
Scanning 10.10.10.11 [1000 ports]
Increasing send delay for 10.10.10.11 from 0 to 50 due to
max_successful_tryno increase to 4
Increasing send delay for 10.10.10.11 from 50 to 100 due to
11 out of 24 dropped probes since last increase.
UDP Scan Timing: About 11.10% done; ETC: 10:56 (0:04:01
remaining)
Completed UDP Scan at 11:05, 555.27s elapsed (1000 total
ports)
Nmap scan report for 10.10.10.11
Failed to resolve "nmap".
Host is up (0.00071s latency).
All 1000 scanned ports on 10.10.10.11 are closed (821) or
open|filtered (179)
MAC Address: 00:0C:29:FA:73:C5 (VMware)

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 1001.37
seconds
           Raw packets sent: 1846 (53.832KB) | Rcvd: 1003
(107.852KB)
```



Scanning Networks

Scanning Techniques

IDLE/IPID Header Scan

C|EH

- Every IP packet on the Internet has a fragment identification number (IPID); OS increases the IPID for each packet sent, thus, probing an IPID gives an attacker the number of packets sent after the last probe
- A machine that receives an unsolicited SYN|ACK packet will respond with an RST. An unsolicited RST will be ignored

1. Send SYN + ACK packet to the zombie machine to probe its IPID number
2. A zombie machine not expecting an SYN + ACK packet will send RST packet, disclosing the IPID. However, always analyse the RST packet from the zombie machine to extract IPID
3. Send SYN packet to the target machine (port 80) to spoof the IP address of the "zombie"
4. If the port is open, the target will send SYN+ACK Packet to the zombie and in response the zombie will send an RST to the target
5. If the port is closed, the target will send an RST to the zombie but the zombie will not send anything back
6. Probe the zombie IPID again, IPID increased by 2 will indicate an open port whereas 1 will indicate a closed port

IDLE/IPID Header Scan

The IDLE/IPID Header scan is a TCP port scan method that you can use to send a spoofed source address to a computer to find out what services are available. It offers complete blind scanning of a remote host. Most network servers listen on TCP ports, such as web servers on port 80 and mail servers on port 25. Port is considered "open" if an application is listening on the port. One way to determine whether a port is open is to send a "SYN" (session establishment) packet to the port. The target machine will send back a "SYN|ACK" (session request acknowledgment) packet if the port is open, and an "RST" (Reset) packet if the port is closed. A machine that receives an unsolicited SYN|ACK packet will respond with an RST. An unsolicited RST will be ignored. Every IP packet on the Internet has a "fragment identification" number (IPID). OS increases the IPID for each packet sent, thus probing an IPID gives an attacker the number of packets sent since the last probe.

SSDP and List Scanning

SSDP Scanning

- The Simple Service Discovery Protocol (SSDP) is a network protocol that works in conjunction with the UPnP to detect plug and play devices
- Vulnerabilities in UPnP may allow attackers to launch Buffer overflow or DoS attacks
- Attacker may use UPnP SSDP M-SEARCH information discovery tool to check if the machine is vulnerable to UPnP exploits or not

List Scanning

- This type of scan simply generates and prints a list of IPs/Names without actually pinging them
- A reverse DNS resolution is carried out to identify the host names

List Scanning

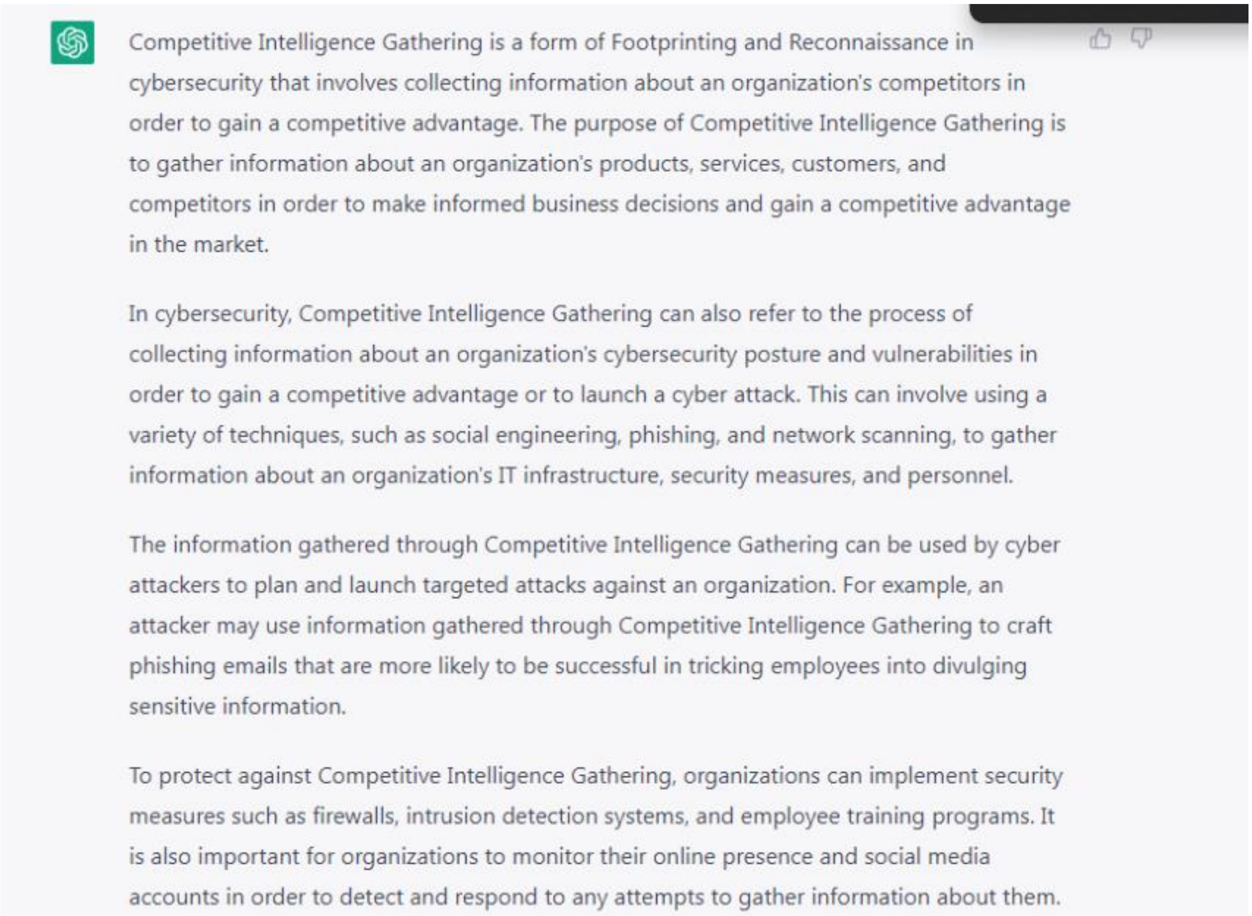
In a list scan, the discovery of the active network host is indirect. A list scan simply generates and prints a list of IPs/Names without actually pinging or scanning the hosts. As a result, the list scan shows all IP addresses as "not scanned" (0 hosts up). By default, a reverse DNS resolution is still carried out on each host by Nmap for learning their names.

Advantages:

- A list scan can perform a good sanity check.
- The list scan detects incorrectly defined IP addresses on the command line or in an option file. It primarily repairs the detected errors to run any "active" scan.

SSDP Scanning

SSDP (Simple Service Discovery Protocol) is a network protocol that generally communicates with machines when querying them with routable IPv4 or IPv6 multicast addresses. The SSDP service controls communication for the Universal Plug and Play (UPnP) feature. It generally works when the machine is not firewalled; however, it can sometimes work through a firewall. The SSDP service will respond to the query sent over IPv4 or IPv6 broadcast addresses. This response includes information about the Universal Plug and Play (UPnP) feature associated with it. The attacker uses SSDP scanning to detect UPnP vulnerabilities that may allow him/her to launch buffer overflow or DoS attacks.

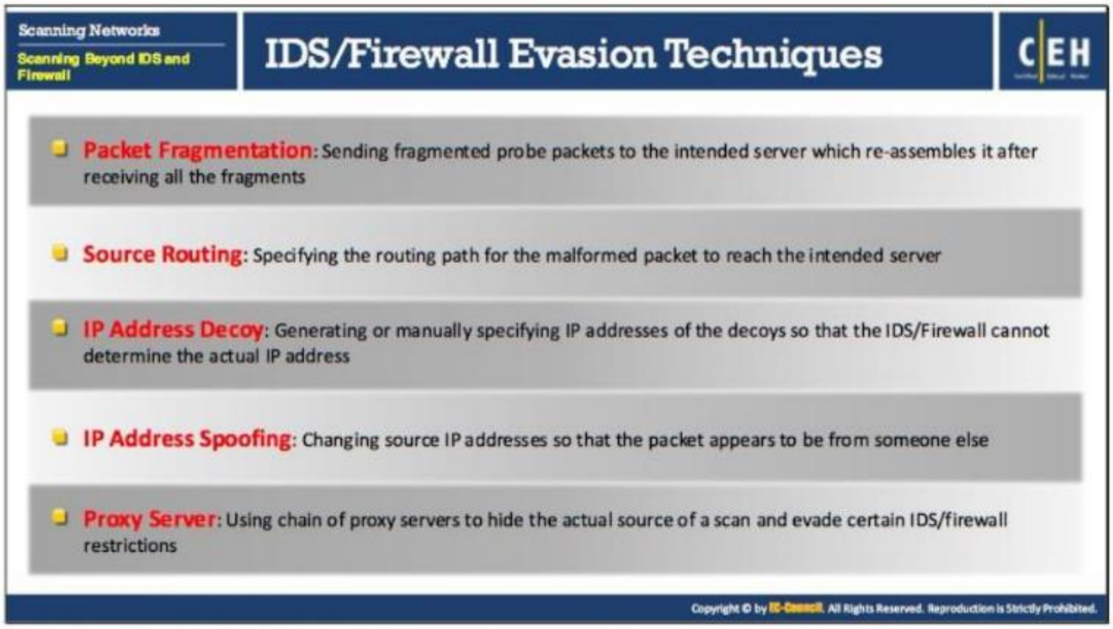


Competitive Intelligence Gathering is a form of Footprinting and Reconnaissance in cybersecurity that involves collecting information about an organization's competitors in order to gain a competitive advantage. The purpose of Competitive Intelligence Gathering is to gather information about an organization's products, services, customers, and competitors in order to make informed business decisions and gain a competitive advantage in the market.

In cybersecurity, Competitive Intelligence Gathering can also refer to the process of collecting information about an organization's cybersecurity posture and vulnerabilities in order to gain a competitive advantage or to launch a cyber attack. This can involve using a variety of techniques, such as social engineering, phishing, and network scanning, to gather information about an organization's IT infrastructure, security measures, and personnel.

The information gathered through Competitive Intelligence Gathering can be used by cyber attackers to plan and launch targeted attacks against an organization. For example, an attacker may use information gathered through Competitive Intelligence Gathering to craft phishing emails that are more likely to be successful in tricking employees into divulging sensitive information.

To protect against Competitive Intelligence Gathering, organizations can implement security measures such as firewalls, intrusion detection systems, and employee training programs. It is also important for organizations to monitor their online presence and social media accounts in order to detect and respond to any attempts to gather information about them.



Scanning Networks

Scanning Beyond IDS and Firewall

IDS/Firewall Evasion Techniques

- **Packet Fragmentation**: Sending fragmented probe packets to the intended server which re-assembles it after receiving all the fragments
- **Source Routing**: Specifying the routing path for the malformed packet to reach the intended server
- **IP Address Decoy**: Generating or manually specifying IP addresses of the decoys so that the IDS/Firewall cannot determine the actual IP address
- **IP Address Spoofing**: Changing source IP addresses so that the packet appears to be from someone else
- **Proxy Server**: Using chain of proxy servers to hide the actual source of a scan and evade certain IDS/firewall restrictions

IDS/Firewall Evasion Techniques

Though firewalls and IDSs avoid malicious traffic (packets) from entering a server, attackers manage to send intended packets to the destination server by implementing techniques such as:

- **Packet Fragmentation**: Here, the attacker sends fragmented probe packets to the intended server which re-assembles it after receiving all the fragments.
- **Source Routing**: The attacker specifies the routing path for the malformed packet to reach the intended server.
- **IP Address Decoy**: Generating or manually specifying IP addresses of the decoys so that the IDS/Firewall cannot determine the actual IP address.
- **IP Address Spoofing**: The attacker changes source IP addresses so that the attack appears to be coming in as someone else.
- **Proxy Server**: This is a process in which the attacker uses a chain of proxy servers to hide the actual source of a scan and evade certain IDS/firewall restrictions.