Unit-2 Network Security and Forensics

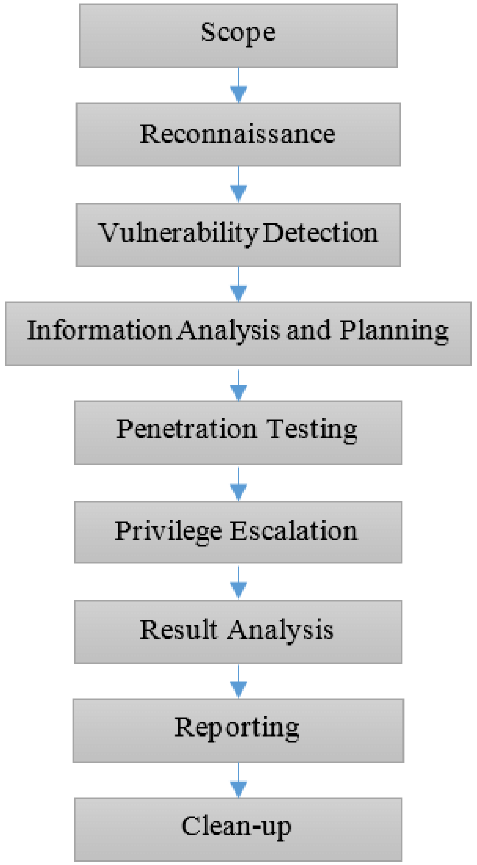
DR. VIJETA KHARE

Penetration Testing or Pen Test

- ✓ Practice of testing a computer system, Network or Web Application to find security vulnerabilities that could be exploited.
- ✓ Penetration testing can be automated with software applications or performed manually.
- ✓ Either way, the process involves gathering information about the target before the test, identifying possible entry points, attempting to break in and reporting back the findings.
- ✓ Objective of penetration testing is to identify security weaknesses.
- ✓ Penetration testing can also be used to test an organization's Security policy, its adherence to compliance requirements.
- ✓ Its employees' security awareness and the organization's ability to identify and respond to security incidents.

Penetration Testing Life Cycle- Phases

- ✓ Scoping
  - ✓ What systems, locations, techniques and tools can be used in a penetration test?
  - ✓ Helps to focus on system over which the org has control.
- ✓ SOW
  - ✓ Formal document defines entire scope of work involved in pen testing, methodology, liabilities & responsibilities, allowed & disallowed technologies, milestones, deliverables, cost and timeline.
- ✓ Passive Reconnaissance.
  - ✓ Reconnaissance- preparatory phase where an attacker seeks to gather as much information as possible about a target prior to launching an attack.
  - ✓ Passive Reconnaissance involves acquiring information without directly interacting with the target.
- ✓ Active Scan.
  - ✓ Scanning refers to the pre-attack phase when the attacker scans the network for specific information on the basis of information gathered during reconnaissance.



Enumeration

- ✓ Basically means counting.
- ✓ Pentester establishes an active connection to the target host.
- ✓ The vulnerabilities are then counted and assessed.
- ✓ It is done mainly to search for attacks and threats to the target system.
- ✓ Enumeration is used to collect usernames, hostnames, IP addresses, passwords, configurations, etc.

Vulnerability Identification

- ✓ It is a flaw that could lead to the compromise of the confidentiality, integrity or availability of an information system.
- ✓ Vulnerability identification involves the process of discovering vulnerabilities and documenting these into an inventory within the target environment.
- ✓ In order for vulnerabilities to be identified, they need to be accurately mapped. There are **vulnerability lists** that make this easy to do. Eg., CVE (Central Vulneribility Exposure), OWSP(Open Web Application Security Project) etc.

Vulnerability Exploit

- ✓ Vulnerability is a flaw in a system or in a software that could provide a way to bypass the security infrastructure.
- ✓ Exploiting is the act of trying to turn a vulnerability (a weakness) into an actual way to breach a system.
- ✓ A vulnerability can therefore be 'exploited' to turn it into viable method to attack a system.

Project Documentation

- ✓ Executive summary.
- ✓ Scope should be defined but precisely.
- ✓ Methodology followed for Pen Testing(OSSTMM, NIST, OWASP etc.)
- ✓ Results of penetration test & Findings.
- ✓ Weakness in general & counter measures that were not implemented that caused vulnerability.
- ✓ Analysis(overall risk that was detected based on finding).
- ✓ Recommendations with solutions.

Network Scanning with Nmap

Introduction

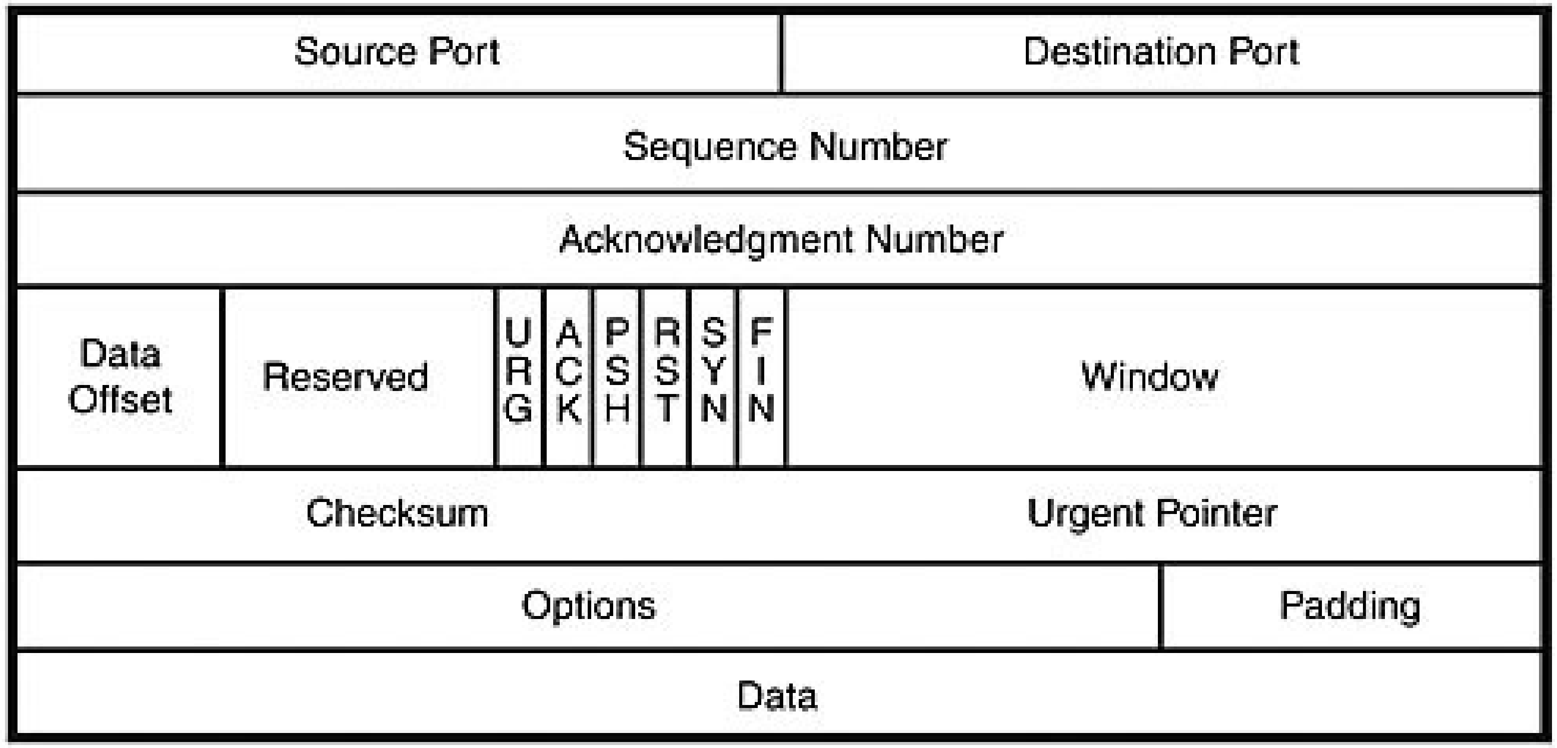
❶ **The first step is Information Gathering in Penetration Testing**

- Discover the services which are open or closed
- Version label
- Operation System and its types

Pre Study

SIZE OF H
20-60 BY

❶ **TCP Packet Header**



Source Port								Destination Port
Sequence Number								
Acknowledgment Number								
Data Offset	Reserved	URG	ACK	PSH	RST	SYN	FIN	Window
Checksum								Urgent Pointer
Options								Padding
Data								

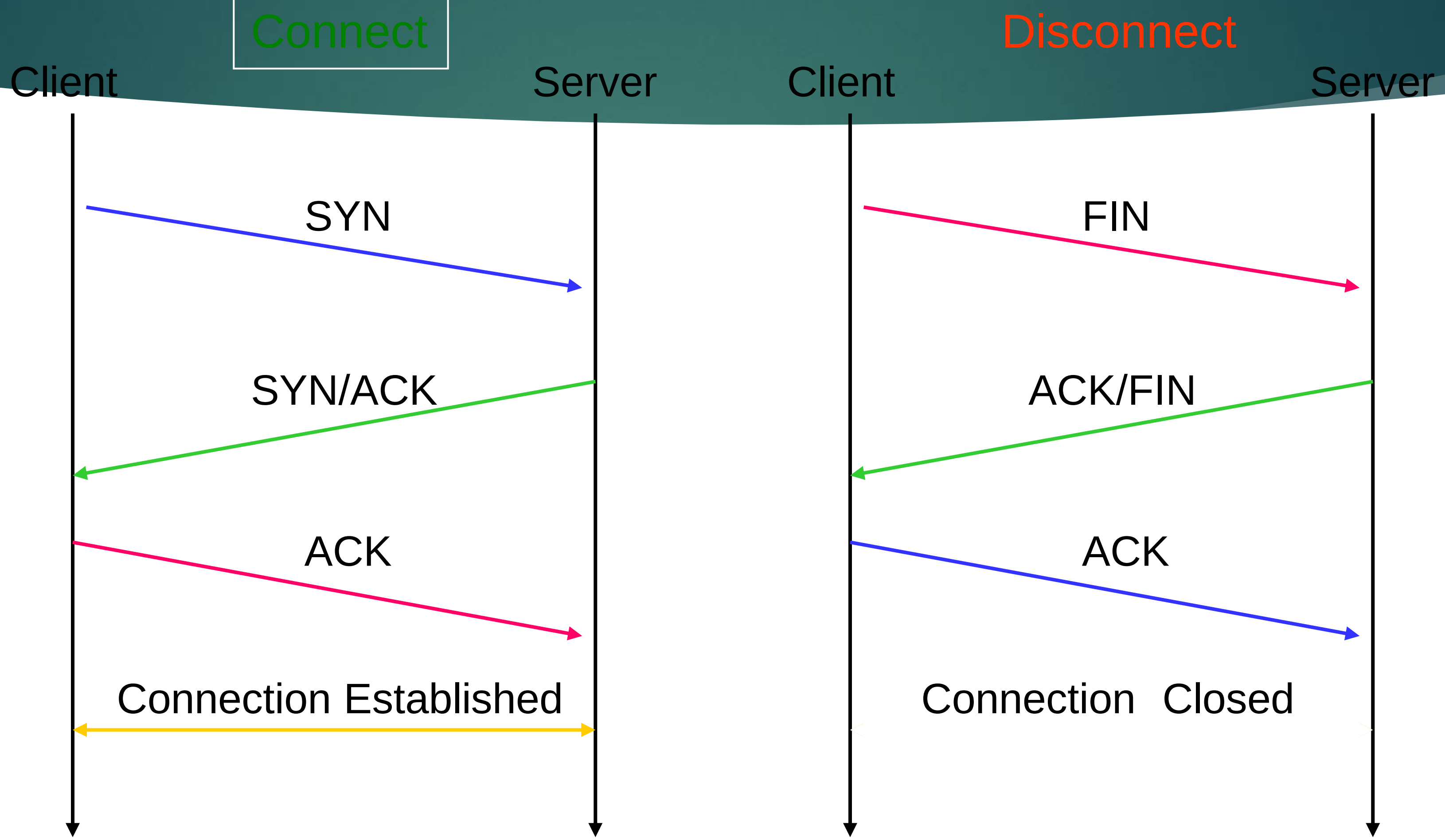
Cont..

- **Source and Destination Ports**
- **Sequence Number and Acknowledgment Number**
- **Data Offset ,Reserve , Control flag, Window**
- **Checksum, Urgent Pointer**
- **Options, Padding**
- **Data**

TCP Flag Definitions

Flag	
SYN	The beginning of a connection
ACK	Acknowledge receipt of a previous packet or transmission
FIN	Close a TCP connection
RST	Abort a TCP connection

TCP conversation



Three-way handshake

What is nmap?

- NMAP is a free and open source utility for network discovery and security auditing. Like there are too many devices connected to the network and a pentester or network administrators will gather a information like which type of devices, their services uptimes, live systems, which kind of services are running their with the help of this utility.

- ZENMAP :-GUI

Quick Start Cheat-sheet

Switch	Description	Example
-sS	TCP SYN port scan.	nmap -sS 192.168.1.1
-sT	TCP Connect port scan	nmap -sT 192.168.1.1
-sU	UDP port scan.	nmap -sU 192.168.1.1
-sA	TCP ACK port scan.	nmap -sA 192.168.1.1

Conti......

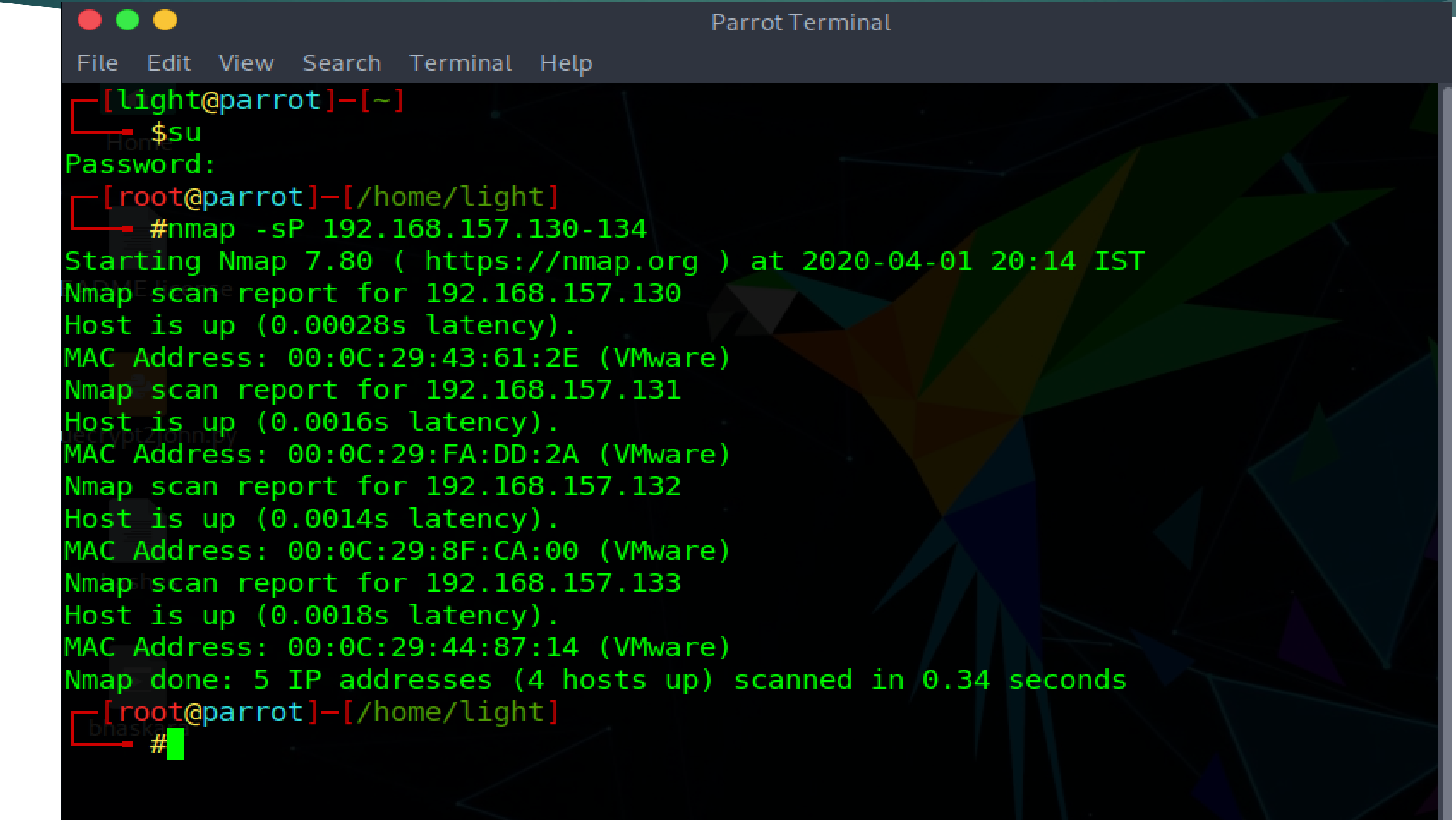
Switch	Description	Example
-Pn	Only port scan.	nmap -Pn 192.168.1.1
-sn	Only host discovery.	nmap -sn 192.168.1.1
-PR	ARP discovery	nmap -PR 192.168.1.1
-n	Disable DNS resolution.	nmap -n 192.168.1.1

HOST Scan

This Scan is used to find or identify active host in the network by sending ARP request packets to all system in that network. And in result it will show a message “Host is up” by Receiving MAC address from Each active host.

Syntax: - nmap -sP target_ip_range

```
nmap -sn target_ip_range
```



```
┌─[light@parrot]─[~]
└──╼ $su
Password:
┌─[root@parrot]─[/home/light]
└──╼ #nmap -sP 192.168.157.130-134
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-01 20:14 IST
Nmap scan report for 192.168.157.130
Host is up (0.00028s latency).
MAC Address: 00:0C:29:43:61:2E (VMware)
Nmap scan report for 192.168.157.131
Host is up (0.0016s latency).
MAC Address: 00:0C:29:FA:DD:2A (VMware)
Nmap scan report for 192.168.157.132
Host is up (0.0014s latency).
MAC Address: 00:0C:29:8F:CA:00 (VMware)
Nmap scan report for 192.168.157.133
Host is up (0.0018s latency).
MAC Address: 00:0C:29:44:87:14 (VMware)
Nmap done: 5 IP addresses (4 hosts up) scanned in 0.34 seconds
┌─[root@parrot]─[/home/light]
└──╼ #
```

Port Scan/TCP Scan/Stealth Scan

- With the help of this scan, User can Identify open or close state of a particular port on target machine.

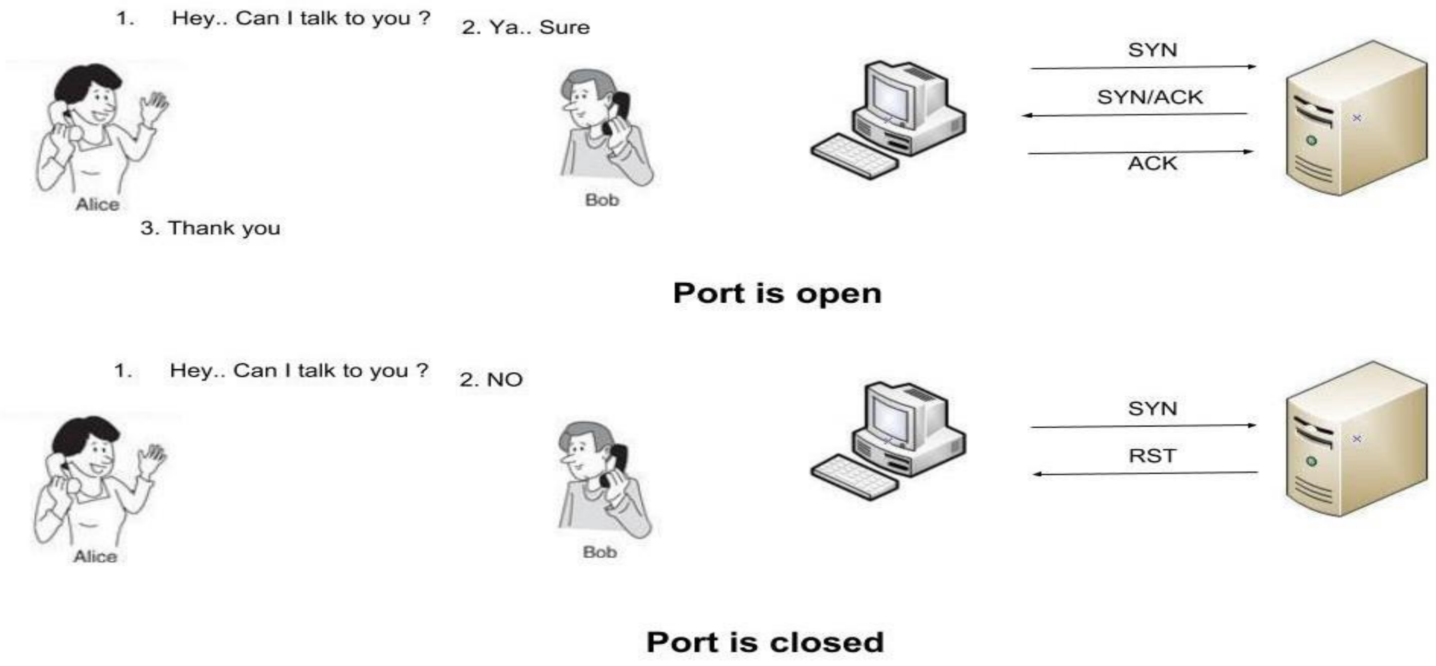
Six Types of Port status

- Open
- Closed
- Filtered
- Unfiltered
- Open/Filtered
- Closed/Filtered

- **Syntax** :-

nmap -p port_number or service_name target_IP_range

nmap -sT port_number target_IP_range



UDP Scan

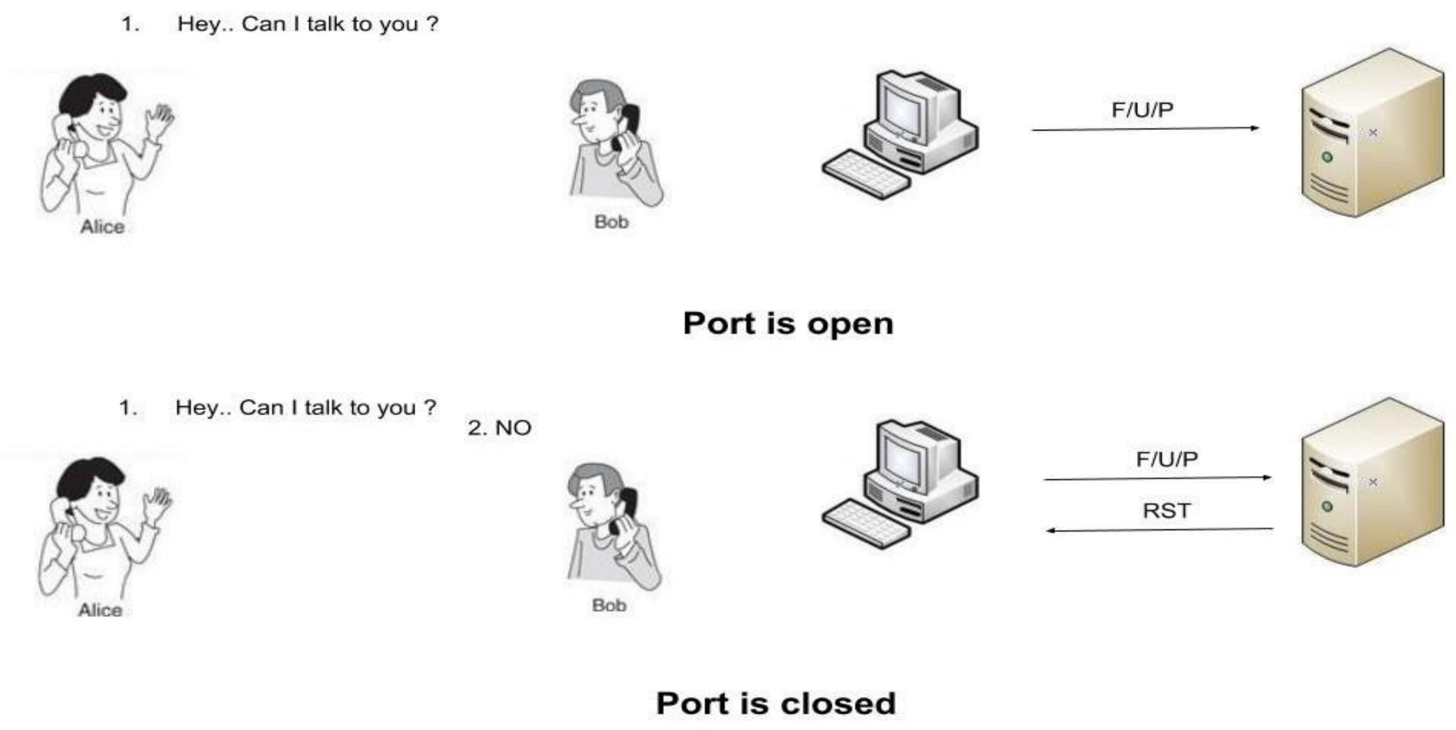
- This method is used to list all open UDP ports on a host.With the help of this scan penetration testers know that they often expose host essential information or can even be vulnerable moreover used to compromise a host.

- **Syntax**:- nmap -sU target_IP

XMAS SCAN

- This scan is accomplished by sending packets with the FIN, URG and PUSH flags, if the server sends RST’s regardless of the port state, then that is not vulnerable to this type of scan. If the client didn’t get any response, then the port is considered as open.
- Xmas Scan is only workable in Linux machines and does not work on the latest version of windows

Syntax :- nmap -sX target_IP



Port is open

Port is closed

NULL Scan

- Null scan sends a packet with no flags switched on, if the server sends RST'S regardless of the port state, them that is not vulnerable to this type of scan. If the client didn't get any response, them the port is considered as open.

- **Syntax :-** nmap -nS target_IP

FIN Scan

- A FIN packet is used to terminate the tcp connection between source and destination port typically after the data transfer is complete. In the place of SYN packet, Nmap starts a FIN scan by using a FIN packet. If the port is open then no response will come from destination port when FIN packet is send through source port.

- Syntax: - nmap -sF target_IP

OS Detection Scan

- Apart from open port enumeration nmap is quite useful in OS fingerprinting. This scan very helpful to penetration tester in order to conclude possible security vulnerabilities and determining the available system calls to set the specific exploit payloads.

  - **Device type**
  - **Running**
  - **OS CPE**
  - **OS details**

Cont..

- **Syntax**: nmap -O target_ip
- **Syntax:** nmap -O -p- –osscan-guess <target>
- **Syntax:** nmap -O –osscan-limit <target>

Whois?

- Whois is a widely used Internet record listing that identifies who owns a domain and how to get in contact with them. The Internet Corporation for Assigned Names and Numbers (ICANN) regulates domain name registration and ownership.
- A Whois record contains all of the contact information associated with the person, group, or company that registers a particular domain name.
- Typically, each Whois record will contain information such as the name and contact information of the Registrant (who owns the domain), the name and contact information of the registrar Registrar (the organization or commercial entity that registered the domain name), the registration dates, the name servers, the most recent update, and the expiration date.
- Whois records may also provide the administrative and technical contact information (which is often, but not always, the registrant).

****Complete nmap through practical's****