# Q1

## S22

**(a) Explain the terms : Datapipe, Fpipe and WinRelay. 03**

- Datapipes are pipes which are used to deliver data whether its streaming or singular, it tranfers data from network to validator and validator to user. Its used to redirect port. Uses TCP only
- Fpipe is a port redirection tool It will redirect from proxy port to required port. Uses UDP/TCP.
- WinRelay is a port redirection tool It will redirect from proxy port to required port. Uses UDP/TCP IPv4 & IPv6.

**(b) What do you mean by Vulnerability? Explain types of vulnerabilities in detail with its example.04**

- Vulnerability is a weakness which allows an attacker to reduce a system's security.
- **System vulnerability:**
  - **Hardware**
    - **Design Flaws:** Faulty design choices during the hardware development process can create vulnerabilities. These flaws may be difficult or impossible to patch due to the physical nature of the hardware.
    - **Manufacturing Defects:** Errors during the manufacturing process can introduce vulnerabilities into hardware components.
    - **Firmware Bugs:** Firmware is a type of software that controls hardware devices. Bugs in firmware can create vulnerabilities that can be exploited by attackers.
  - **Software**
    - **Programming Errors:** Human mistakes during the development process can introduce vulnerabilities into the code. Examples include buffer overflows.
    - **Outdated Software:** Software that hasn't been updated with the latest security patches remains vulnerable to known exploits.
- **Network vulnerability:**
  - **Unpatched Network Devices:** Like software, network devices such as routers and firewalls require regular updates to address security vulnerabilities. Failure to patch these devices leaves the network vulnerable to known exploits.
  - **Unsecured Wireless Networks:** Wireless networks without proper security measures, such as encryption, are easily accessible to attackers. .
  - **Misconfigured Firewalls:** Firewalls are critical security tools that control incoming and outgoing network traffic. Improperly configured firewalls can inadvertently allow unauthorized access to the network
- **Procedural Vulnerability:**
  For examples:
  - **Password procedure:** Password should follow the standard password policy.

- **Training procedure:** Employees must know which actions should be taken and what to do to handle the security. Employees must never be asked for user credentials online. Make the employees know social engineering and phishing threats.

**(c) What is Cybercrime? Explain the different categories of cybercrime in details.07**

- Cyber crime refers to harm someone or a group of individuals physically or mentally using modern technolgy

- **Cybercrime against individual :** Email Spoofing , Spamming , Cyber Harassment , Phishing.
- **Cybercrime against property :** Credit Card Fraud , Pirated Items.
- **Cybercrime against organization :** Computer Virus , Unauthorized Accessing of Computer.
- **Cybercrime against society :** Cyber Terrorism , Fraud documents.
- **Crimes originating from offensive newsgroup :** stolen data , sale of pornographic material.

# S23

**(a) Define System and Web Vulnerability. 03 RE**
**(b) Explain Metasploit and OpenVAS. 04**

- **Metasploit**
  - Metasploit is a tool hackers (and security pros) use to test if systems can be hacked.
  - It is used to exploid system. (attack)
  - It helps to:

    1. **Find weaknesses:** Check if something is insecure.
    1. **Test attacks:** Try hacking it.
    1. **Do more after hacking:** Like finding hidden stuff or taking control

- **OpenVAS**
  - OpenVAS is like a scanner that checks systems for security holes.
  - It is used to identify vulnerability. (defence)
  - It helps to:

    1. **Scans your system:** Finds problems, like old software or settings that can be abused.
    1. **Gives reports:** Shows what’s wrong and how to fix it.
    1. **Stays updated:** Knows the latest tricks hackers use.

**(c) Describe Nmap. Explain different functionality with its command in detail. 07**

- Nmap is a free and open-source network scanning tool used for network discovery, security auditing, and troubleshooting.
- It is used from Terminal because its command line based software.
- It helps identify hosts, open ports, running services, and their versions, along with OS detection.
  - **Agressive Scan:**
    - nmap -A 192.168.1.10
    - It will scan all data eg. version , os , ports etc
  - **Stealth Scan:**
    - nmap -sS 192.168.1.10
    - It will scan without alerting to any system (used to bypass firewalls)
  - **Service Version Detection**
    - nmap -sV 192.168.1.10
    - It will scan for versions running on ports
  - **Operating System Detection:**
    - nmap -O 192.168.1.10
    - It will scan on which os is system running on
  - **Ports Detection:**
    - nmap -p- 192.168.1.10
    - It will scan for all available ports

## W21

**(a) Explain Vulnerability Scanning. 03**

- Vulnerability scanning usually refers to the scanning of systems that are connected to the Internet.
- It can also refer to system scanning of internal networks that are not connected to the internet in order to assess the threat of malicious software.
- It is possible to know the basic security measures when managing network and websites. but it is not possible to catch all the vulnerabilities which are in the network and websites.
- The vulnerability scanners provide you the automate security scanning.
- The vulnerability scanners can scan your network and websites for up to thousands of different security risks.
- It produces a list of those vulnerabilities, and gives steps on how to overcome or reduce them.
- Types of Vulnerability Scanners:
  - Cloud-Based Vulnerability Scanners
  - Host-Based Vulnerability Scanners
  - Network-Based Vulnerability Scanners
  - Database-Based Vulnerability Scanners

**(b) Define the term in briefly: (i) Open Port Identification (ii) Banner Check 04**

- **Open Port Identification:** This process involves scanning a system or network to identify which ports are open and actively accepting connections. Open ports indicate running services or applications that could be potential points of entry for communication or security exploitation.
- **Banner Check:** Banner checking involves sending a request to a network service (like a web server or SSH) to capture and analyze its response, which often includes metadata about the service, version, or operating system. This information is useful for network diagnostics or vulnerability assessment.

**(c) Describe Network Sniffers and Injection Tool. Explain any two injection tools in brief. 07 RE**

# W22

**(a) Describe Reconnaissance and Probe 03**

- **Reconnaissance:**
  - Reconnaissance attack is a kind of information gathering on network system and services. This enable the attacker to discover vulnerabilities or weaknesses on the network.
  - Reconnaissance attack can be active or passive.
- **Probe:**
  - Probe is an attempt to gain access to a computer and its files through a known or probable weak point in the computer system.
  - A probe is an action taken in order to learning or collecting data about the state of the network.
  - For example, an empty message can be sent simply to see whether the destination actually exists.
  - Ping is a common utility for sending such a probe.

**(b) Explain Phishing and 3 ways it is done. 04**

- Its a cyberattck where people are tricked in order to gain sensitive information such as credit card , bank details , identity etc
- **Email Phishing:**
  - The attacker sends a fake email that looks like it's from a trusted source (e.g., a bank or service provider)
- **SMS Phishing:**
  - A more targeted form of phishing aimed at specific individuals or organizations.
- **Spear Phishing:**
  - Victims receive fake messages with malicious links or requests for personal information.
  - Spear Phishing is done in order to get sensitive imformation of collegues such as data which are highly censored by organization etc.

**(c) Explain Metasploit and Nmap 07 RE**

## W23

**(a) Describe Network Sniffers with suitable example. 03 RE**
**(b) What is Cyber Crime? Explain different types of Cyber Crimes in brief. 04 RE**

**(c) What do you mean by Password cracking and brute force tools? Explain any one in detail. 07**

- Password cracking is the process of recovering passwords from data that have been stored.
- A common approach (brute-force attack) is to try guesses repeatedly for the password and check them against correct password.
- Password cracking is an old technique that is successful mostly because humans are not very good random-sequence generators.
- Brute-force guessing techniques against password cracking takes advantage of hardware performance.
- **John the Ripper**
  - John the Ripper remains one of the fastest, most versatile, and most popular password crackers available
  - Currently available for many destros of Unix, Windows, DOS etc.
  - Auto detects password and includes a customizable cracker.
  - Its primary purpose is to detect weak Unix passwords.
  - After panetration it will generate report in binary formate in /run or /src directory.

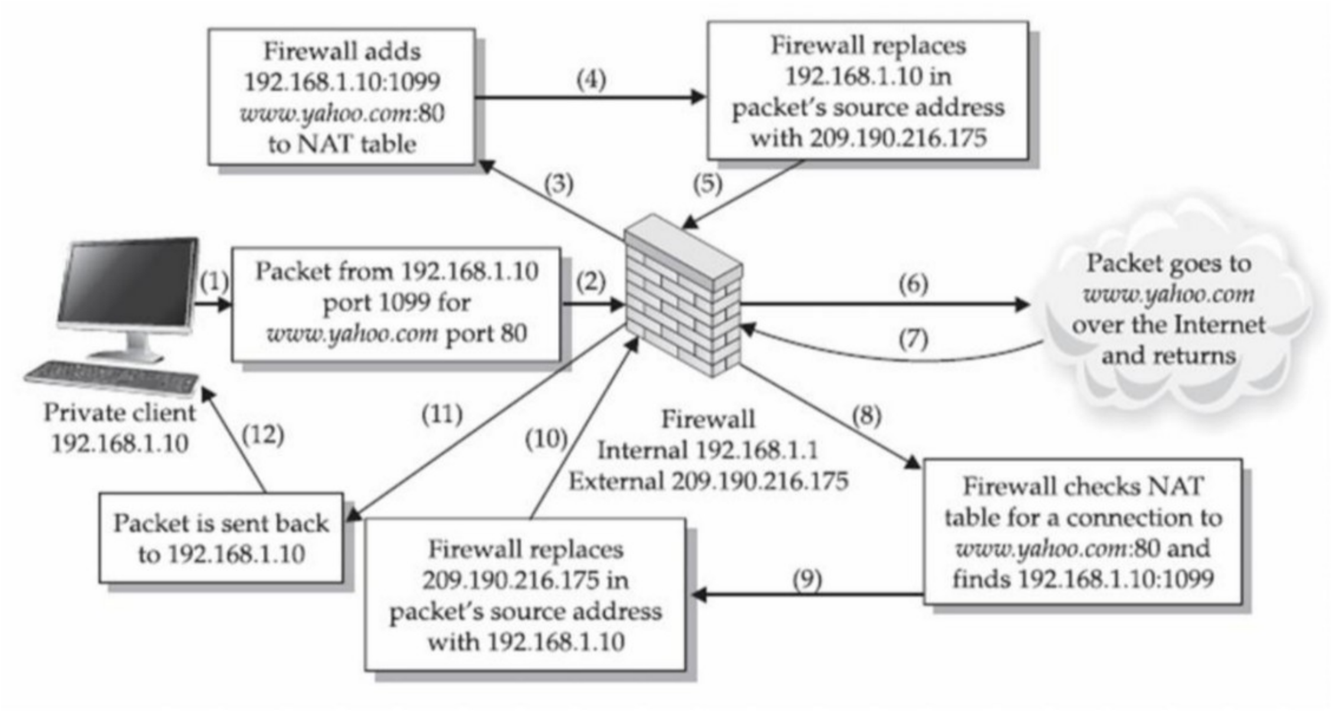
- **THC – Hydra**
  - It is multiple services supportive and network authentication cracker.
  - It uses network to crack remote systems passwords.
  - It can be used to crack passwords of different protocols including HTTPS, HTTP, FTP, SMTP.
  - It’s best when we use it in Linux environment.
  - Fast cracking speed.
  - Available for Windows, Linux etc.
  - New modules can be added easily to enhance features.

# Q2

## W21

**(a) Define Network Address Translation. 03**

- Network Address Translation (NAT) is designed for IP address conservation.
- Network Address Translation (NAT) is method of connecting multiple computers to the Internet using one IP address.
- It enables private IP networks that use unregistered IP addresses to connect to the Internet.
- NAT operates on a router, usually connecting two networks together, and translates the private addresses in the internal network into legal addresses, before packets are forwarded to another network.
- Here in below figure, we can easily understand flow of each step one by one.
- Here we see that Firewall that work as NAT device for IP converting and transfer packet to other network.
- Diagram:



**(b) What is Probe. Explain its different types. 04**

- Probe is an attempt to gain access to a computer and its files through a known or probable weak point in the computer system.
- A probe is an action taken in order to learning or collecting data about the state of the network.
- For example, an empty message can be sent simply to see whether the destination actually exists.
- Ping is a common utility for sending such a probe.

- There are two types: I) Traffic Porbe II) Vulnerability Porbe
- **I) Traffic Porbe:**
  - Some services declare information about themselves without receiving particular data from a client.
  - For example, a web service will not give response until it receives data from the client.
  - A valid HTTP request using the HEAD method will provide some useful information like web server information, information about installed server operating system etc.
  - Traffic probes try to use valid requests. Because valid protocol messages are less likely to crash or interrupt a service
- **II) Vulnerability Porbe:**
  - Some security bugs cannot be identified without sending a payload that exploits.
  - These types of probes are more accurate. They rely on direct observation not only on port numbers or service banners.
  - But they also carry more risk of interrupting the service, because the test payload must be trying to take advantage of an error in the service's code.
  - An attacker who exploits HTML injection vulnerability like this could steal data from the user or damage the web site.
  - Example: http:xyz.com/?q=%20 one can try to tweak this and exploid the server if its not well maintained and has bugs it will cause problem to service

**(c) Differentiate between Packet Filter and Firewall. 07**

| Aspect | Packet Filter | Firewall |
|---|---|---|
| **Definition** | A basic mechanism to filter network traffic based on static rules. | A comprehensive security system that monitors and controls traffic. |
| **Layers Operated On** | Operates at the **network** and **transport** layers (IP, TCP/UDP). | Operates at **network**, **transport**, and **application** layers. |
| **State Awareness** | **Stateless**: Does not track the state of connections. | Can be **stateful**: Tracks the state of connections and sessions. |
| **Filtering Criteria** | Filters based on IP addresses, port numbers, and protocols. | Filters based on IP, ports, protocols, and application-layer data. |
| **Advanced Features** | No advanced features; limited to static filtering. | Includes NAT, VPN, intrusion detection/prevention, and deep packet inspection. |
| **Security Level** | Provides **basic security**; vulnerable to spoofing and state-based attacks. | Provides **comprehensive security** against various attacks. |
| **Performance** | Lightweight, fast, and resource-efficient. | More resource-intensive due to advanced features. |
| **Configuration Complexity** | Simple to configure and manage. | Complex to configure and manage. |
| **Use Case** | Suitable for small or less complex networks requiring basic traffic control. | Ideal for large, complex networks needing advanced protection. |
| **Examples of Use** | Allowing/blocking specific IPs or ports. | Protecting against intrusion, malware, and application-level attacks. |

**OR(c) Differentiate between Stateless and Stateful Firewalls. 07**

| | **Stateless Packet Filtering Firewalls** | **Stateful Packet Filtering Firewalls** |
|---|---|---|
| **1.** | The stateless firewalls are designed to protect networks based on static information such as source and destination. | Stateful firewalls filter packets based on the full context of the connection. |
| **2.** | It uses some predefined packet filtering rules, the packets are judged based on that, if it conforms to the predefined rules then it is considered to be “safe” and allowed to pass through. If the conditions are not met, the packet is considered to be “unidentified” or “malicious” and it will be blocked. | It uses the concept of a state table where it stores the state of legitimate connections. Stateless firewall filters are only based on header information in a packet but stateful firewall filter inspects everything inside data packets, the characteristics of the data, and its channels of communication. |
| **3.** | Less secure than stateless firewalls. | Stateful firewalls are more secure. |
| **4.** | Cheaper or cost-efficient. | Expensive as compared to stateless firewall |
| **5.** | Faster than Stateful packet filtering firewall. | Slower in speed when compared to Stateless firewall. |
| **6.** | Treats every request as new session | Treats first request to the new server as new session than after recording the session it will maintain the session till its closed hence request afterwards will be servered in running session |
| **7.** | For small businesses, a stateless firewall could be a better option, as they face fewer threats and also have a limited budget in hand. | For larger enterprises, a stateful firewall would be a smarter option, as they have larger outgoing traffic that needs monitoring and enough money to afford it. Stateful firewalls offer dynamic packet filtering, so they can provide a thick security layer to mitigate attacks. |

## W22

**(a) Describe NAT with example 03 RE**
**(b) Differentiate between Stateful and Stateless firewalls. 04 RE**
**(c) Explain Injection tools like Tcpdump, Windump and Wireshark 07**

- **Tcpdump**
  - TCPdump is a network debugging tools runs under command line. It allows user to intercept and display TCP/IP and other packets being transmitted or received over a network.
  - It is frequently used to debug applications that generate or receive network traffic.
  - It is also used to testing whether security, firewalls, networking status and its configration are setup correctly or not.
  - It is unix based tool.
  - TCPdump can only be used by root user. It can decode and monitor the meta data of IP/TCP.
  - It can be used for intercepting and displaying the communications of another user or computer.
  - TCPdump and Windump has default output length of the size of datagram is 68 bytes.
  - TCPdump does not collect whole output for display.
  - It is used to analyse traffic on unix.
  - It can be used to troubleshoot unix based networking.
- **Windump**
  - It is a free version of TCPdump for windows. Windump comes in two parts.
  - Provides command-line packet analysis for Windows users.
  - Windump is program which uses set of libraries and drivers of WinPcap
  - Since its windows version of Tcpdump it allows all utilities of Tcpdump
  - It is used to analyse traffic on windows
  - It can be used to troubleshoot windows based networking
- **Wireshark**
  - Wireshark is a free and open source packet analyzer.
  - It is used for network troubleshooting and analysis.
  - It runs on Linux, UNIX, OSx, BSD, Solaris, and Microsoft windows.
  - User can see all traffic visible on that interface.
  - It supports, capture formats from several other commercial and open source network sniffers.

**OR(c) Explain Ettercap and Hping Kismet 07**

- **Ettercap**
  - Ettercap is a free and open source network security tool for man-in-the-middle attacks on LAN.
  - It can be used for computer network protocol analysis and security auditing.
  - It runs on various UNIX- like operating systems including Linux, mac, windows.
  - Ettercap works by putting the network interface into promiscuous mode and by poisoning the target’s machine.
  - Thereby it can act as a ‘man in the middle’ and unleash various attacks on the victims.
  - It can be used actively or passively.
  - Character injection into an established connection. Characters can be injected into a server or to a client while maintaining a live connection.

    - It supports sniffing of a password and username and even the data.
    - It can determine the OS of the victim host and its network adapter.
    - It can kill connections of choices from the connection-list.
    - It can hijack DNS requests.
- **Hping**
    - Hping is a free packet generator and analyzer for the TCP/IP protocol.
    - It is one of the tools for security auditing and testing of firewalls and networks.
    - The new version of hping, hping3, is scriptable.
    - It gives human readable description of TCP/IP packets as output.
    - Programmer can write scripts for packet manipulation and analysis in very short time.
    - Hping also has a listen mode.
    - Hping’s “listen” mode can be used for receiving data.
    - Determining a Host’s Status When Ping Doesn’t Work.
    - Testing Firewall Rules.
    - Stealth Port Scanning.
- **Kismet**
    - Kismet is a free software and it is network detector,packet sniffer and intrusion detection system for wireless LANs.
    - This runs under Linux,Windows.
    - Kismet works passively.
    - It is able to detect the presence of wireless client.
    - It has the ability to log all sniffed packets and save them.
    - Kismet also supports logging of the geographical coordinates of the network if the input from a GPS receiver is additionally available.
    - These are as follows:
        - A drone: it can be used to collect packets and then pass them on to a server for interpretation.
        - A server: it can be used to interpreting packet data and extrapolating wireless information and organizing it.
        - The client: it communicates with the server and displays the information the server collects.

## W23

**(a) Differentiate between Computer Viruses and Worms. 03**

| Attributes | Worms | Viruses |
|---|---|---|
| **Definition** | A Worm is a form of malware that replicates itself and can spread to different computers via a Network. | A Virus is a malicious executable code attached to another executable file that can be harmless or can modify or delete data. |
| **Objective** | The main objective of worms is to eat the system's resources. It consumes system resources such as memory and bandwidth and makes the system slow in speed to such an extent that it stops responding. | The main objective of viruses is to modify the information. |
| **Host** | It doesn't need a host to replicate from one computer to another. | It requires a host is needed for spreading. |
| **Harmful** | It is less harmful as compared. | It is more harmful. |
| **Detection and Protection** | Worms can be detected and removed by the antivirus and firewall. | Antivirus software is used for protection against viruses. |
| **Controlled by** | Worms can be controlled by remote. | Viruses can't be controlled by remote. |
| **Execution** | Worms are executed via weaknesses in the system. | Viruses are executed via executables. |
| **Symptoms** | 1. Hampering computer performance by slowing down it<br>2. Automatic opening and running of programs<br>3. Sending of emails without your knowledge | 1. Pop-up windows linking to malicious websites<br>2. Hampering computer performance by slowing down it<br>3. After booting, starting of unknown programs. |
| **Types** | Internet worms, Instant messaging worms, Email worms, File sharing worms, and Internet relay chat (IRC) worms are different types of worms. | Boot sector viruses, Direct Actionvirusess, Polymorphicvirusess, Macro viruses, Overwritevirusess, and File Infector viruses are different types of viruses |
| **Examples** | Examples of worms include Morris worm, storm worm, etc. | Examples of viruses include Creeper, Blaster, Slammer, etc. |
| **Interface** | It does not need human action to replicate. | It needs human action to replicate. |
| **Speed** | Its spreading speed is faster. | Its spreading speed is slower as compared to worms. |

**(b) What are the Cyber Crime Scenarios and explain its applicability for Legal Sections? 04 RE**
**(c) Explain attacks on wireless network. How do you protect Wireless Network? 07**

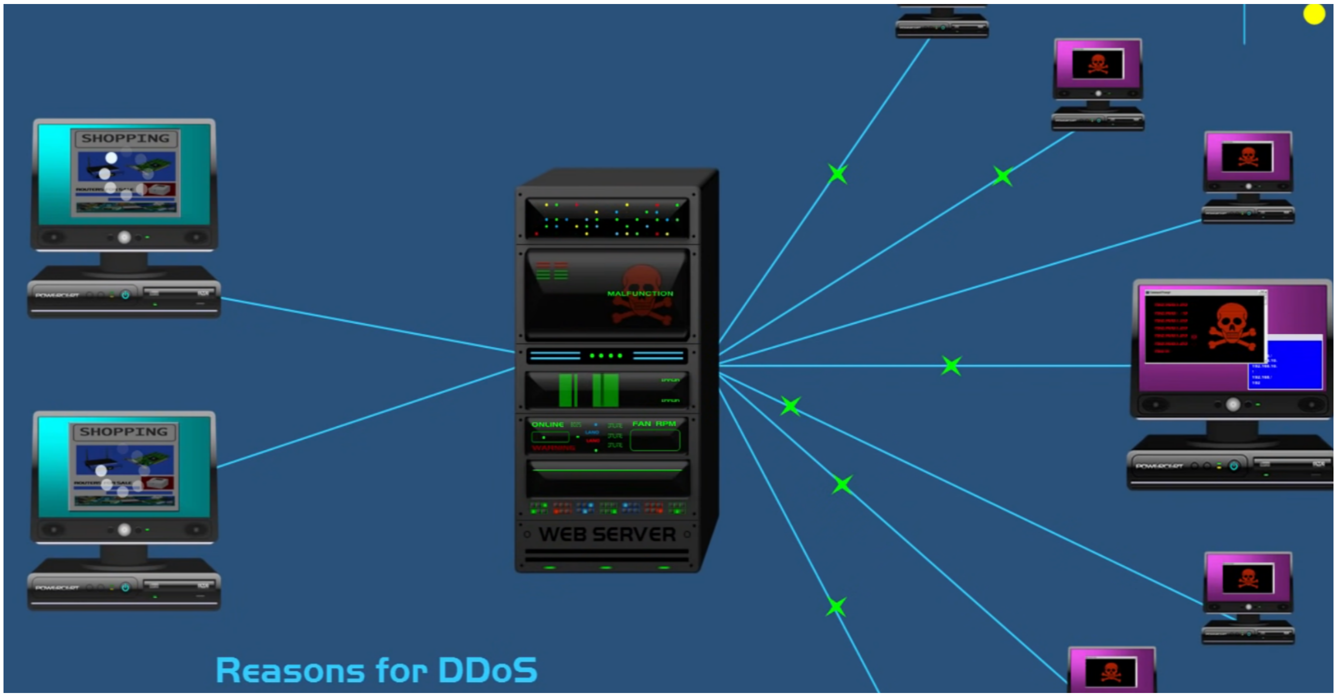
- Standard wireless communication occurs when the end user and the wireless access point are able to communication on a point-to-point basis without interruptions.
- There are many attack variations in existence against wireless networks that breaks the standard communication format.
- These attacks includes
  - Denial of Service (DoS)
  - Man-in-the-middle attacks
  - Encryption cracking
  - Spoofing
  - Sniffing
- Put up a firewall
  - Protect your wireless network with a firewall to keep intruders from sniffing your data.
  - While these components often come included within wireless routers, they work best in the form of standalone applications or as a feature of anti-virus software.
- Be careful where you roam
  - There is no need to share sensitive information from the Wi-Fi hotspot provided by the local library. Wait until you return to a trusted network to conduct such sensitivity activity.
  - Disable your wireless connection.
- Limit online communications to protected sites
  - "HTTPS" in the URL rather than "HTTP".
- Watch out for the Evil Twin
  - Malicious individuals often create Wi-Fi hotspots beside legitimate access points. When sitting down to make a connection, you may unknowingly select the evil twin from the list of available access points, giving the malicious individual access to anything you transmit.
- Encryption
  - Hacker will eventually try to latch onto your wireless signal. You can apply additional security by implementing encryption protocols to transform your sensitive data into characters that are only readable by intended receivers.

**OR(c) Define Denial-of-Service (DOS). How can we prevent DDOS attack? 07**

- A DoS attack is an attempt to make computer resources unavailable and deny to give service to its legitimate users.
- In this attack, the attacker floods the bandwidth of the victims' network by sending constant multiple request to the victims' server and make it busy for giving response of the multiple request.
- It is the actual reason for preventing access to a service to the genuine users.
- DoS attacks often last for days, weeks and even months at a time, making them extremely destructive to any online organization.
- They can cause loss of revenues, consumer trust, force businesses to suffer long-term reputation damage.

SHOPPING
SHOPPING
WEB SERVER
CPU
MEMORY
TEMP
ONLINE
FAN RPM

- A DDoS attack means Distributed DoS attack, DoS attacks from multiple computer for the same victim is Distributed DoS attack.
- A large numbers of zombie systems are synchronized to attack a particular system. The zombies are infected by the attackers and it is also victims in the DDoS attack.
- The zombie systems are called “Secondary Victims” and the main target is called “Primary Victim”.
- Malware carries the DDoS attack mechanisms.
- Botnet is the popular medium to lunch DdoS attack.
- It could be stopped using :
  - Firewalls
  - Rate Limiting
  - CAPTCHAs
  - Geofencing
  - Cloud services



# Q3

## W21

**(a) Define Snort. 03 RE**
**(b) What are the different usages of Network Sniffers? List out it. 04**

- Sniffers are the best tools for hackers to attack computers.
- Network administrators use sniffers for network troubleshooting and security analysis.
- Many sniffing and anti-sniffing packages available on the internet for download.
- Network sniffers tools are used to watch over networks as well as collect all kinds of information including diagnostic information.
- TCPDump,WinDump,WireShark are the examples of Network sniffing tools.
- Uses of Network Sniffers:
  - Identify the type of network application used.
  - Identify the hosts using network.
  - Identify the bottlenecks.
  - Capture data sniffing packages used for troubleshooting of network application.
  - Create network traffic logs.

**(c) List out various Application Inspection tools. Explain any two. 07 RE**
**OR(a) How do you protect Wireless Network? 03 RE**
**OR(b) What do you mean by Password cracking and brute force tools? Explain any one. 04 RE**
**OR(c) What are the kinds of Web Vulnerabilities Tools available? Explain any two. 07 RE**

**W22**

**(a) Explain Zed Attack Proxy. 03**

- Many web application attacks require a knowledge of HTML and no other tool than a browser's address bar.
- Zed Attack Proxy (ZAP) is example of an interactive proxy.
- An interactive proxy provides the means to inspect, alter, and manipulate web traffic in order to probe a web application for the presence of vulns.
- ZAP is written in Java, so your experience in using it doesn't noticeably change between systems.
- Note that you'll need to set up your environment correctly for building Java source code
- Since its built on java it required a JDK.

**(b) Differentiate between John Ripper and HTC-Hydra. 04**

| Aspect | John the Ripper | THC-Hydra |
|---|---|---|
| **Purpose** | Password cracking for **local files** (e.g., hashes). | Password cracking for **network services**. |
| **Target** | Cracks hashed passwords stored in files (e.g., /etc/shadow). | Targets authentication systems over networks. |
| **Attack Type** | Performs dictionary attacks, brute force, and hybrid attacks on password hashes. | Performs brute force and dictionary attacks over network protocols. |
| **Supported Protocols** | Not protocol-specific; works on files with password hashes from systems like Linux, Windows, or databases. | Supports network protocols like **HTTP, HTTPS, FTP, SSH, SMTP, SQL, Cisco, etc.** |
| **Speed** | Optimized for local cracking, but speed depends on the system's performance. | Extremely fast due to its optimization for network-based attacks. |
| **Ease of Use** | Slightly more complex due to configuration for hash formats. | Easier to use with simple command-line syntax for network testing. |
| **Best Suited For** | Cracking **offline password** (stored locally). | Cracking **online authentication systems**. |

**(c) Explain the web vulnerability tools like Nikto and W3af. 07**

- **Nikto**
  - Nikto is a Web server scanner that tests web servers for dangerous files, outdated server software and other problems.
  - It's also known as a web server assessment tool.
  - It is designed to find insecure files, configurations and programs on an type of web server.
  - Nikto is used for assessing the security of a web application's deployment.
  - It won't be as helpful for assessing the security of a custom web application.
  - It is written in perl.
  - It is supported by windows and unix.
  - Scan multiple ports on a server, or multiple servers

    - It is can be used using command lines
- **W3af**
    - w3af is an open-source web application security scanner.
    - The project provides a vulnerability scanner and exploitation tool for Web applications.
    - This cross-platform tool is available in all of the popular operating systems.
    - It is written in the Python programming language.
    - Users have the choice between a graphic user interface and a command-line interface.
    - It removes some of the headaches involved in Manual web application testing through its Fuzzy and Manual request generator feature.
    - Identify vulnerabilities like SQL Injection, Guessable credentials.
    - For linux its recommended to use Git reposetory of it.
    - It supporst most of the popular framework such as Wordpress etc. It doesn't support custom web frameworks.

**OR(a) Explain Curl, OpenSSL and Stunnel. 03**

- **Curl:**
    - Curl is an open source tool and library for transferring data with URL syntax.
    - Curl supports HTTP POST, HTTP PUT etc.
    - It normally displays a progress meter during operations, indicating the amount to transferred data, transfer speeds and estimated time left.
    - Curl is used in command lines or scripts to transfer data.
    - It is also used in routers, printers, mobile phones,tablets, set-top boxes, media players, etc.
    - It is available on Unix, Linux Mac OS X and Windows platforms.
    - Curl is default in most of the unix systems.
- **OpenSSL:**
    - OpenSSL is an open-source implementation of the SSL protocols.
    - The OpenSSL library is the most commonly used open source library for establishing encrypted connections.
    - The OpenSSL command is present by default on most Unix-based systems.
    - The core library, written in the C programming language.

- **Stunnel:**
    - Stunnel is open source multi platform program, used to provide universal tunnelling.
    - It can be used to provide secure encrypted connections for clients or servers.
    - You can also use stunnel to wrap SSL around any network service.
    - It runs on a various operating systems, including most Unix based systems and Windows.

**OR(b) Differentiate between packet filter and firewall. 04 RE**

**OR(c) Explain the network monitoring tool Snort. 07**

- Snort is an open source network Intrusion Prevention System
- It can perform real time traffic analysis and packet-logging on IP networks.
- Also perform protocol analysis, content searching/matching.
- It can be used to detect a variety of attacks, such as buffer overflows, stealth port scans and much more.
- Manage security of network is the very purpose of Snort.

- It has three modes
    - 1. To display all packages.
    - 2. To make a log files in local storage.
    - 3. To check and apply set of rules over packages in order to gain security.

## W23

**(a) What is Keyloggers? Explain different types of Keyloggers. 03**

- Keylogger is a piece of code that logs keystrokes.
- Keylogger captures the keystrokes typed on your keyboard and saves these keystrokes in a file, including the details like the usernames and passwords you entered, credit card details, websites you have visited, the applications you opened, and so on.
- The file may stores locally or periodically send it over the network to the owner of the program.
- There are two types software keyloggers and hardware keyloggers.
- The software keyloggers are installed on computer system by Trojan or Viruses without the knowledge of the user.
- Hardware keyloggers are small hardware devices connected to the PC or keyboard.
- It save every keystork into a file or in the memory of the hardware device.

**(b) Explain Wireshark and how do we use Wireshark to find a password in network? 04 RE**
**(c) What is Hacking? Explain types of Hackers. 07**

- hacker is an unauthorized user who attempts tor gains access tan information system.
- The term hacker was originally a term of respect for computer experts who knew all about computers, and could do cool things with them.
- The person who is able to discover weakness in a system and managed to exploit it to accomplish his goal referred as a Hacker, and the process is referred as Hacking.
- White hat - good
- Black hat - worst
- Grey hat - find vulnaribility without permission than reports it.
- Red hat - attcks on back hat before they do
- Blue hat - Professional
- Green hat - newbies

**OR(a) Difference between Stateless Vs Stateful Firewalls. 03 RE**
**OR(c) Explain in details: Network Address Translation (NAT) with suitable diagram. 07 RE**

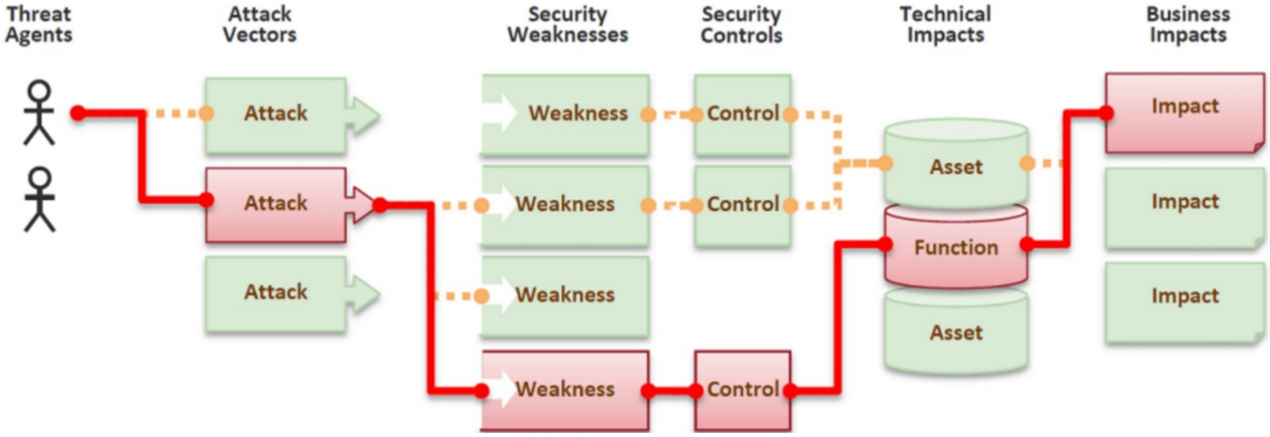
# Q4

## W21

**(a) Define Denial-of-Service. 03 RE**

**(b) Justify the attack vector. List out different types of attack vector. 04**

- An attack vector is a path or means by which a hacker (or cracker) can gain access to a computer or network server in order to deliver a payload or malicious outcome.
- They take advantage of known weak spots to gain entry. Many attack vectors take advantage of the human element in the system, because that's often the weakest link.



- Types of attack vector
- Email as an Attack Vector
  - Email attacks continue to advance in sophistication.
  - Millions of messages can be sent out in the hope that a large number of people will be duped.
- Attachments (and other files)
  - Malicious attachments install malicious computer code. Attachments attempt to install their payload as soon as you open them.
  - The code could be a Virus, Trojan horse or any other kind of malware.
- Attack by WebPages
  - Fake Web sites are used extract personal information, like your address, credit card number and expiration date from people.
  - The Fake websites look very much like the genuine websites they imitate.
- Viruses
  - These are malicious computer code that makes them a payload.
  - The main attack vector for viruses was originally infected USB drive, but now the vectors include email attachments, downloaded files, worms and more.
- Attacks of the worms
  - Most worms are delivered as attachments
  - These worms spread without the need for humans to open attachments.

**(c) What is Firewall (RE) and illustrate its different types. 07**

- Packet-Filter Firewall:
  - The firewall performs a simple check of the data packets coming through the router inspecting information such as the destination and origination IP address, packet type, port number, and other surface-level information without opening up the packet to inspect its contents.
  - This means they don’t have a huge impact on system performance and are relatively simple.
  - However, they’re also relatively easy to bypass compared to firewalls with more robust inspection capabilities.
- Circuit-Level Gateways:
  - Circuit-level gateways work by verifying the transmission control protocol (TCP) handshake.
  - This TCP handshake check is designed to make sure that the session the packet is from legitimate.
  - While extremely resource-efficient, these firewalls does not check the packet itself.
- Stateful Packet-Inspection (SPI):
  - These firewalls combine both packet inspection technology and TCP handshake verification to create a level of protection greater than either of the previous two architectures could provide alone.
  - However, these firewalls do put more of a strain on computing resources as well. This may slow down the transfer of legitimate packets compared to the other solutions.
- Application Gateways:
  - These firewalls operate at the application level.
  - It may also perform deep-layer packet inspections, checking the actual contents of the information packet to verify that it contains no malware.
- Next-Gen firewalls:
  - Some common features of next-generation firewall architectures include deep-packet inspection (checking the actual contents of the data packet), TCP handshake checks, and surface-level packet inspection.

- Software Firewall:
  - Software firewalls include any type of firewall that is installed on a local device rather than a separate piece of hardware.
  - The big benefit of a software firewall is that it's highly useful for creating defense in depth by isolating individual network endpoints from one another.

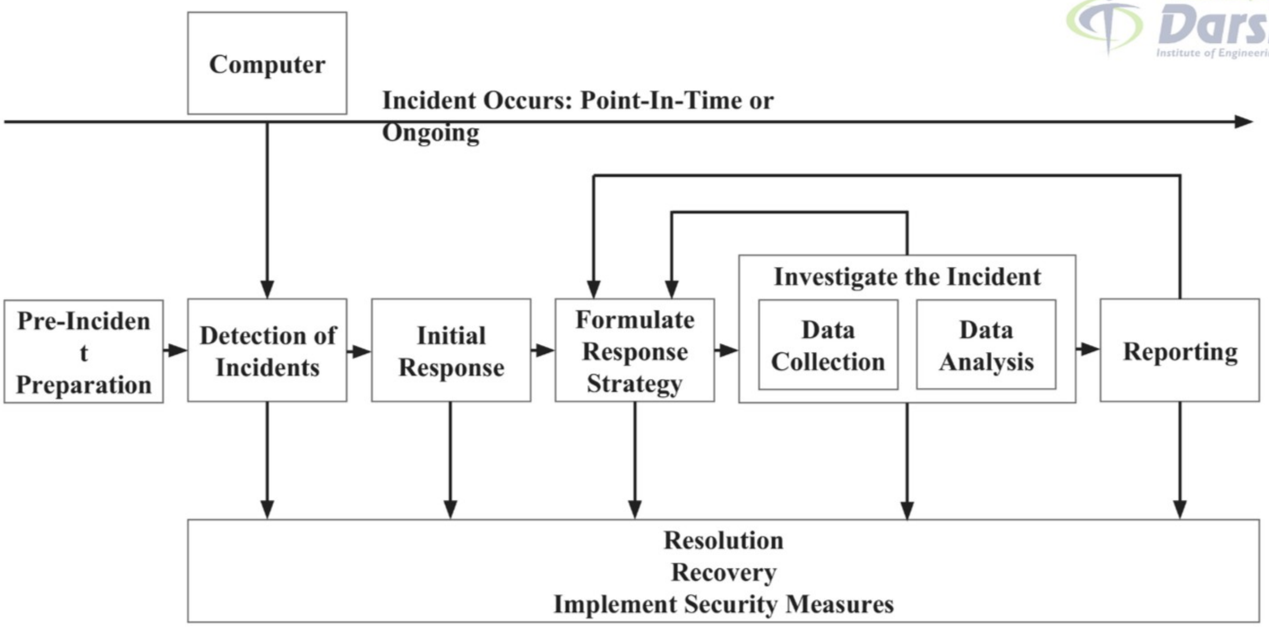
**OR(a) Illustrate the aim and objective of Indian IT ACT 2000. 03**

- The primary aim of the IT Act 2000 is to **legalize electronic transactions** and provide a framework for the **cybersecurity** of data and networks. It aims to **facilitate e-commerce**, **prevent cybercrimes**, and **regulate digital communication** in India.

**OR(b) List out different types of Traditional Problems Associated with Computer Crime. 04 RE**

**OR(c) What is Incident Response. Explain it process flow with appropriate diagram. 07**

- Incident response is the response to a computer crime, security policy violation, or similar event.
- The incident responder is not necessarily the forensic specialist who will conduct the analysis of the digital evidence.



- Pre-incident preparation
  - Take actions to prepare the organization and the CSIRT before an incident occurs.
- Detection of incidents
  - Identify a potential computer security incident.
- Initial response
  - Perform an initial investigation, recording the basic details surrounding the incident.
  - Assembling the incident response team, and notifying the individuals.
- Formulate response strategy
  - Based on the results of all the known facts, manage the best response and get management approval and deside strategy to overcome the situation.
- Investigate the incident
  - Perform a thorough collection of data
  - Review the data collected to determine
  - What happened,When it happened,Who did it, and How it can be prevented in the future.
- Reporting
  - Accurately report information about the investigation in a manner useful to decision makers.
- Resolution
  - Employ security measures and procedural changes, record lessons learned, and develop long term fixes for any problems identified.

## W22

**(a) Describe attack vector, cyberspace and IT act 2000. 03 RE**

- CyberSpace is a vertual spce where all data exist and works vertually such as files, games, emails, browsing webs etc. Where they are connected with network and interect with each other using intenet.

**(b) Explain hacking and its types. 04 RE**
**(c) Explain Incident response and digital forensics. 07 RE**
**OR(a) List three contemporary crimes? 03**

- **Cyberbullying**: The use of digital platforms to harass, intimidate, or threaten individuals.
- **Identity Thefting**: Stealing someone's personal information to commit fraud or theft.
- **Ransomware Attacks**: Cybercriminals encrypt data and demand payment to restore access to the victim's files or system.

**OR(b) Explain the types of cybercrimes. 04 RE**
**OR(c) Explain DVWA and Web goat 07**

- **DVWA (Damn Vulnerable Web Application):**DVWA is a deliberately insecure web application designed for security professionals, ethical hackers, and students to practice identifying and exploiting web vulnerabilities. It helps learners improve their skills and understand secure coding practices.
- **WebGoat:**WebGoat is another deliberately insecure web application created by OWASP (Open Web Application Security Project). It is designed to teach web application security through practical, interactive lessons.

**W23**

**(a) What is SQL injection? 03 RE**
**(b) List out different types of Traditional Problems Associated with Computer Crime. 04 RE**
**(c) Describe all HTTP utilities in details. 07 RE Curl OpenSSL Stunnel**
**OR(a) What is contemporary approach in criminology in the world of computer science? 03 RE**
**OR(b) Explain in details: Buffer Overflow. 04**

- Buffers are memory storage regions that temporarily hold data while it is being transferred from one location to another.
- A buffer overflow (or buffer overrun) occurs when the volume of data exceeds the storage capacity of the memory buffer.
- As a result, the program attempting to write the data to the buffer overwrites adjacent memory locations.
- Buffers are created to contain a limited amount of data.
- If data is more than the buffer limit, it can overflow into the nearby buffer and overwrite the valid data stored in it.
- Buffer overflow is an increasingly common type of security attack on data integrity/reliability.

**OR(c) Explain in details: Hacking, Attack vectors, Cyberspace and Criminal Behavior. 07 RE**

# Q5

## W21

**(a) Define the term: (i)Trojan Horse (ii)Spyware 03**

- A **Trojan Horse** is a type of malicious software that pretends to be a legitimate application or file to trick users into installing or running it. Once activated, it can perform harmful actions like stealing data, installing additional malware, or creating backdoors for hackers to access the system.
- **Spyware** is a type of software that secretly collects information from a user's computer or device without their consent. It monitors activities such as browsing history, keystrokes, or personal data and sends this information to a third party, often for malicious purposes like identity theft.

**(b) What is Destruction of Data. List out the different reason for it. 04 RE**
**OR(a) What is Keyloggers? Explain different types of Keyloggers. 03 RE**
**OR(b) Differentiate between Computer Viruses and Worms. 04 RE**
**OR(c) Define the Cyber Crime. Explain the different type of classification of Cyber Crime. 07 RE**

**W22**

**(a) Features of Trojan virus. 03 RE**
**(b) List four functions a backdoor can do to help the attacker. 04**

- A backdoor, is a secret entry point into a program or operating system that allows someone that is aware of the backdoor to gain access without going through the usual security access procedures.
- During the development of operating system or application, programmers add backdoors for maintenance hooks and troubleshooting. Backdoors allow them to examine operations inside the code while the code is running.
- One can reduse security of system.
- Individual may try to use prevelage for its own advantage.
- May steal sensitive information.
- One may use it to spoil the system with bugs and errors.

**(c) Explain how SQL Injection attacks can be prevented. 07**

- SQL injection is a code injection technique that exploits a security vulnerability occurring in the database layer of an application.
- Using escape character along with single quote (\') embedded in SQL statement .
- User input is not strongly typed and thereby unexpectedly executed.
- The main objective is to obtain information of the victims while accessing database.
- Malicious code is inserted into a web form field in the SQL injection
- **Ways to  prevente SQL Injection:**
- Web Application Firewall (WAF)
  - Deploy a WAF to monitor and block malicious SQL inputs. WAFs can detect and prevent SQL injection patterns.
- Regular Security Testing
  - Perform penetration testing and code audits to identify vulnerabilities. Use automated tools like OWASP ZAP or Burp Suite for testing.
- Error Message Suppression
  - Avoid exposing detailed error messages that can reveal database structure. Use generic error messages for failed queries.
- Use Proper Database Permission
  - Limit database user privileges to only what's necessary.
  - Avoid granting admin-level access to web applications.
- Use Parameterized Queries
  - Replace dynamic SQL queries with prepared statements.
  - Ensure that user input is treated as data, not executable code.
- Always have a backup
- Update and Patch Software
  - Regularly update the database management system (DBMS) and libraries to fix known vulnerabilities.
- Use Content Security Policies (CSP)
  - Implement CSPs to protect against other injection vectors that can lead to SQL injection indirectly.

**OR(a) What is Stegnography and list two examples. 03**

- Steganography is the art and science of writing hidden messages in such a way that no one can get knows the existence of the message except the intended user.
- Steganography is a method that attempts to hide the existence of message or communication.
- Eg. An image has been embeded with such a process that after decoding it a certain binary gets generated which tranlates to hiddel message
- Eg. Hidding secret message in pdf or document in the way that only person who know how to decode can identify.

**OR(b) Differentiate between 1. DOS and DDOS attack 2. Keyloggers and Spyware. 04 RE**

**OR(c) Explain the tools for attacking wireless Networks. 07 RE**

## W23

**(a) Explain Vulnerability Scanning. 03 RE**
**(b) What is OpenVas? Write advantage and disadvantage of OpenVas. 04  RE**
**(c) Describe credit card fraud that can be done through mobile or other wireless devices. 07 RE**
**OR(a) Explain passive attacks and active attacks with respect to cyber criminals? 03**

| Aspect | Passive Attacks | Active Attacks |
|---|---|---|
| **Definition** | Cyber criminals silently observe or intercept data without altering it. | Cyber criminals modify, disrupt, or manipulate data or systems actively. |
| **Objective** | To gather information (e.g., monitoring, eavesdropping). | To cause harm, steal data, disrupt operations, or gain unauthorized access. |
| **Detection** | Difficult to detect as there is no alteration of data. | Easier to detect due to noticeable changes or disruptions. |
| **Examples** | - Eavesdropping on network traffic<br>- Packet sniffing | - Denial of Service (DoS)<br>- SQL injection<br>- Malware attacks |
| **Impact** | Often preparatory for further attacks; minimal immediate damage. | Direct impact on systems, causing potential data loss, financial damage, or downtime. |

**OR(b) What is Packet Filter Vs Firewall? 04 RE**
**OR(c) What is Incident Response. Explain it process flow with appropriate diagram. 07 RE**