**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    - **Outdated Software:** Software that hasn’t been updated with the latest security patches remains vulnerable to known exploits.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:
    - **Find weaknesses:** Check if something is insecure.
    - **Test attacks:** Try hacking it (legally, of course!).
    - **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:
    - **Scans your system:** Finds problems, like old software or settings that can be abused.
    - **Gives reports:** Shows what’s wrong and how to fix it.
    - **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**

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

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

**W22**

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

**(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.

**(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**

**Q2**

**W21**

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

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

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

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

**W22**

**(a) Describe NAT with example 03**

**(b) Differentiate between Stateful and Stateless firewalls. 04**

**(c) Explain Injection tools like Tcpdump, Windump and Wireshark 07**

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

**W23**

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

**(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**

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

**Q3**

**W21**

**(a) Define Snort. 03 RE**

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

**(c) List out various Application Inspection tools. Explain any two. 07**

**OR(a) How do you protect Wireless Network? 03**

**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**

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

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

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

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

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

**W23**

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

**(b) Explain Wireshark and how do we use Wireshark to find a password in network? 04**

**(c) What is Hacking? Explain types of Hackers. 07**

**OR(a) Difference between Stateless Vs Stateful Firewalls. 03 RE**

**OR(b) Define Snort? What is the difference between IPS and IDS? 04**

**OR(c) Explain in details: Network Address Translation (NAT) with suitable diagram. 07**

**Q4**

**W21**

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

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

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

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

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

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

**W22**

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

**(b) Explain hacking and its types. 04 RE**

**(c) Explain Incident response and digital forensics. 07 RE**

**OR(a) List three contemporary crimes? 03**

**OR(b) Explain the types of cybercrimes. 04 RE**

**OR(c) Explain DVWA and Web goat 07**

**W23**

**(a) What is SQL injection? 03**

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

**(c) Describe all HTTP utilities in details. 07**

**OR(a) What is contemporary approach in criminology in the world of computer science? 03**

**OR(b) Explain in details: Buffer Overflow. 04**

**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**

**(b) What is Destruction of Data. List out the different reason for it. 04**

**(c) What are the Cyber-Crime Scenarios and explain its applicability for Legal Sections? 07**

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

**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**

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

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

**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**

**W23**

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

**(b) What is OpenVas? Write advantage and disadvantage of OpenVas. 04**

**(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**

**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**