USN									

Internal Assessment Test 3

Sub	Introduction to Cyber Security (Open Elective Course)			Sub code	**21CS653**	Branch	ECE, ME
Date	30.7.2024	Duration	**90 mins**	Max Marks	**50**	Sem /Sec	**VI SEM**

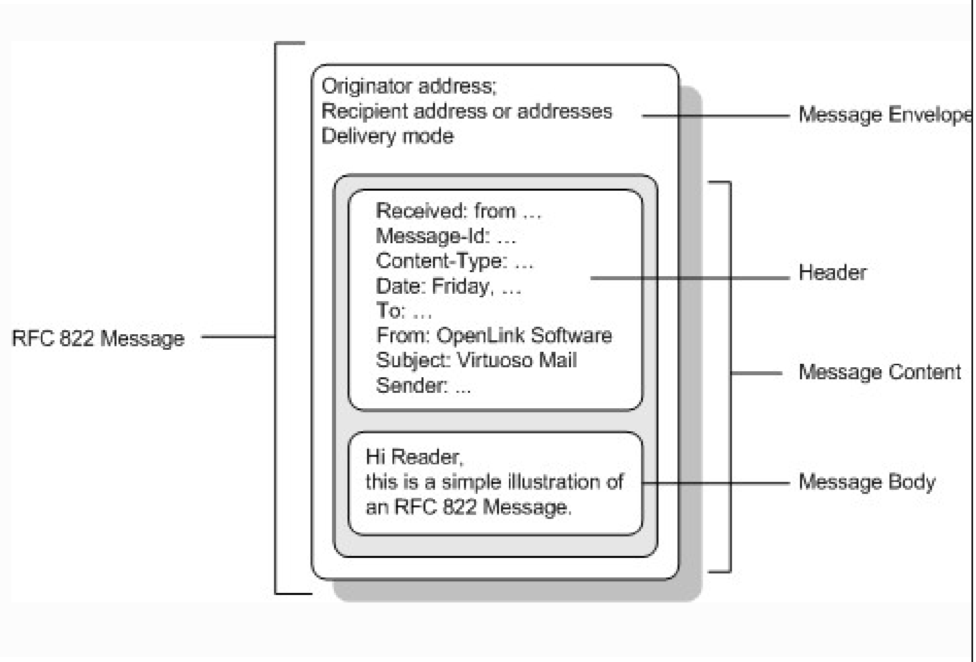
	Answer any FIVE FULL Questions	MARKS	CO	RBT
1.	a) What does RFC 822 cover? Explain various fields described in RFC 822 and explain which are the important fields in the context of Cybersecurity? What is the difference between RFC 822 and 2822? b) What is reverse DNS look up? Why is it required?	[9] [1]	CO1 CO2 CO3 CO4	L3

RFC is request for comments. (minimal answer expected). Additional info, RFC is "name of a series of working documents as the specifications for the Internet Protocols". RFC working groups were under Internet Engineering Task Force (IETF).

RFC 822 defines structure of emails that consists of various fields such as header (and various fields in header) and also body of the message.

Important fields are:

- ***Fields that identify the sender (From, Reply-to, Sender, Return-path etc)***
- ***Also various "received" fields that indicate the mail servers involved in routing the message(s) from the sender to your server. Email travels from one hop to other and that information can be obtained from these.***



- ***Originator address provides email address of sender. One should check if the email address matches with the supposed "sender name and domain". For example, "From" field might say that name of the sender is "CMRIT", but "from address" could be gmail.com instead of cmrit.ac.in. This indicates a spam email.***
- ***Return-path indicates path back to sender.***

- ***The only way to determine where a message "really" originated is to examine the message "headers."***
  - ***As E-mail goes through a number of different computers (hops) on the way from the sender to the intended recipient,***
  - ***Header information is added to the message at each machine along the way, until it reaches its destination.***

	• ***(The workstation on which the recipient reads the mail generally doesn’t add header info.)*** • ***It is important for investigators to know what information can—and can’t—be discerned from e-mail headers and to understand that headers can be spoofed (forged).*** • ***RFC 2822 is a newer/latest version of RFC 822 and this standard supersedes RFC 822*** • ***RFC 2822 updates RFC 822 to reflect current practice and incorporates incremental changes that were specified in other RFCs*** • **Reverse DNS lookup maps IP address → domain name. It is reverse process of Domain Name Service. This is useful in many cases to verify that IP address is genuine.** **E.g. While parsing email headers, one can get both name and IP address of the server (from where the email originated). Now one can do a “reverse lookup” of IP address and later check if domain name matches with what was perceived to be.**			
2.	• What is a firewall? (2 marks) • How is it different from a proxy? (1 mark) • What is “layered filtering” in a firewall? (1 marks) • List typical layered filtering options in a firewall with 2-3 key points about each of them. (3 x 2 = 6) ***Firewall stands between local computers and external/global network (e.g. Internet). Firewall products support the filtering of messages to either allow data to pass through or prevent it from doing so, according to specified criteria. A firewall acts as a barrier to prevent “bad data”— from unauthorized systems, coming to the internal network. It also prevents packets of a particular type or to or from a particular user or computer from spreading from the LAN to the outside network.*** ***Firewalls are specifically designed to control inbound and outbound access and cam prevent or allow packets to flow between local computers/network and external network. Proxy on the other hand just routes the data (only changing IP address). But proxy typically does not prevent or drop any packets (unless access to certain web sites is blocked by administrator).*** ***With layered filtering, firewalls analyze and filter/allow packets are different layers of protocol stack. E.g. packet (layer) filtering, circuit (layer) filtering and application (layer) filtering which maps to corresponding layers of OSI model.*** • ***Packet filtering does most of its work at the network layer. examining the information contained in the IP packet header of a message and then either permit the data to cross the firewall or reject the packet based on that information.*** • ***Circuit filters operate at a higher (transport) layer and restrict access on the basis of host machines (not users) by processing the information found in the TCP and UDP packet headers. For example, system admins can prohibit anyone using Computer A from using File Transfer Protocol (FTP) to access Computer B. Circuit filters don’t restrict access based on user information; they also cannot interpret the meanings of the packets.*** • ***The information that the packet filter uses to make its decision, includes the IP address of the source and/or destination computer(s) and the TCP or UDP port number*** • ***An application filter operates at the top layer, the application layer). Application filters can use the packet header information but are also able to allow or reject packets on the basis of the data contents and the user information. Administrators can use application filtering to control access based on a user’s identity and/or based on the particular task the user is attempting to perform. Application gateways are considered to be the most secure of the filtering technologies*** • ***Administrators can use application filtering to control access based on a user’s identity and/or based on the particular task the user is attempting to perform.*** •	[8] [2]	CO1 CO2 CO3 CO4	L3
3.	a) What is an IDS? What does it do and what action does it take? ***[3]*** What are the different types of IDS? Explain each with pros and cons. ***[1+6]*** ***IDS (Intrusion Detection System) can recognize that an attack of a specific type is being attempted and can perform a predefined action. E.g. It can send an e-mail message to the administrator, page the administrator (send text message), write an event entry to the event log, run a previously specified program or script, Stop the firewall service etc. IDS es can recognize many different common forms of network intrusion, such as port scans, LAND attacks, the Ping of Death, UDP bombs, out-of-band attacks, and others.*** ***is a specialized tool that knows how to read and interpret the contents of log files from routers, firewalls, servers, and other network devices. IDS can be software based or hardware based or both.***	[10]	CO1 CO2 CO3 CO4	L3

There are 3 main types of IDS.

- ***Network based IDS: Monitor network backbones and look for attack signatures***
- ***Host based IDS: Operate on hosts to defend and monitor the operating and file systems for signs of intrusion are called host-based IDSes***
- ***Application-based IDS: Monitor only specific, important applications***
    - ***E.g. DBMS, content management systems, accounting systems etc***

N/W based IDS pros: It can monitor an entire, large network with only a few well-situated nodes or devices and impose little overhead on a network. N/W based IDS does not add significant overhead or interfere with network operation. They are easy to secure against attack and may even be undetectable to attackers; they also require little effort to install and use on existing networks.

N/W based IDS cons: Network-based IDSes may not be able to monitor and analyze all traffic on large, busy networks. (So they may overlook attacks launched during peak traffic periods/miss them).
Network-based IDSes may not be able to monitor switch-based (high-speed) networks.
Network-based IDSes cannot analyze encrypted data, nor do they report whether attempted attacks succeed or fail.
Network-based IDSes require a certain amount of active, manual involvement from network administrators to gauge the effects of reported attacks.

Host based IDS:

- ***Pros (Host based):***
    - ***Can analyze activities on the host it monitors at a high level of detail***
        - ***It can often determine which processes and/or users are involved in malicious activities***
        - ***Host-based IDSes can use host-based encryption services to examine encrypted traffic, data, storage, and activity***
    - ***Many host-based IDSes use an agent-console model where agents run on (and monitor) individual hosts but report to a single centralized console***
- ***Cons:***
    - ***A host-based IDS does consume processing time, storage, memory, and other resources on the hosts where such systems operate.***
    - ***Expert attackers who compromise a host can also attack and disable host-based IDSes.***
    - ***Host-based IDSes can be foiled by DoS attacks (because they may prevent any traffic from reaching the host or prevent reporting on such attacks to a console elsewhere on a network)***
    - ***Data collection occurs on a per-host basis; writing to logs or reporting activity requires network traffic and can decrease network performance.***

Application based IDS (pros and cons)

- ***Pros:***
    - ***Concentrates on events occurring within some specific application, they often detect attacks through analysis of application log files and can usually identify many types of attacks or suspicious activity.***
    - ***Sometimes application-based IDSes can even track unauthorized activity from individual users***
    - ***They can also work with encrypted data, using application-based encryption/decryption services***
- ***Cons:***
    - ***Application-based IDSes are sometimes more vulnerable to attack than host-based IDSes.***
    - ***They can also consume significant application (and host) resources.***

4	a) What is Cryptography (and its purpose)? [2 marks] What is the difference between Cryptography and Encryption? [2] What are Ciphers and what are the different types of Ciphers? [3] What is penetration testing? [1] b) What are key loggers and different types of it? (In brief, 1-2 lines) • ***Purpose of Cryptography is to hide information or change it so that it is incomprehensible to people for whom it is not intended. It is about confidentiality and keeping the contents of the data secrete.***	[8] [2]	CO1, CO2 CO3, CO4	L3

	• ***Encryption involves applying an algorithm to plain text to turn it into something that will appear to be gibberish to anyone who doesn't have the key to decrypt it.*** • ***Cryptography is a much broader term than encryption; encryption is a form of cryptography. (all encryption is cryptography, but not the other way)*** • ***Cryptography provides an inner line of defense. It protects data from intruders who are able to penetrate the outer network defenses and also from those who are authorized to access the network but not this particular data.*** • ***Cipher: A method used to encrypt data while Cipher text is Data in encrypted form*** • ***Some common cipher/code types are:*** • ***Substitution*** • ***Transposition*** • ***Obscure languages*** • ***Penetration testing: Evaluating a system by attempting to circumvent the computer's or network's security measures. Idea behind pen testing is to find any security issues or vulnerabilities in house before product or solution is released or deployed.*** • ***Keystroke logging (keylogging), is the practice of capturing (or logging) the keys pressed on a keyboard, typically in a covert manner so that the user of keyboard is unaware of that*** • ***It is quicker and easier way of capturing the passwords and other information*** • ***Software keyloggers are software programs installed on computer systems and can record every keystroke*** • ***Usually located between the OS and the keyboard hardware (like a device driver)*** • ***Hardware Keyloggers: To install these keyloggers, physical access to the computer system is required*** • ***For example, keyloggers installed on ATM machines to capture ATM card PINs*** • ***These keyloggers look like an integrated part of such systems hence, bank customers are unaware of their presence***			
5	• What is "AAA" model in system and network security? Explain each of the "A"s in 3-4 lines. Explain how is AAA supported by an operating system (e.g. Windows) ***1 mark for naming each of the A, A, A and 2 X 3 = 6 marks for explanation*** ***3 marks for explaining how O.S supports AAA.*** • ***AAA - Authentication, Authorization and Accounting is an important concept in system and network security, Strong security rests on a 3 legged foundation*** • ***Authentication (provide identity), Authorization (to give permission) and Accounting (to log an audit trail)*** • ***Authentication ensures that users, processes, and services, that seek to consume system resources or access their contents provide sufficient proof of identity to enter systems and networks, before any such requests may be issued*** • ***E.g. A password, a USB key or user fingerprint or other biometrics*** • ***Authorization (or access control) ensures that requests for resources will not be granted unless requesters have the permissions necessary not only to read/inspect the contents of the resources. But also that they have explicit permissions to perform the kind of operation they seek to perform on the resource. A user can log in, but may or may not have privileges necessary to change VPN access passwords company-wide*** • ***Accounting relates to monitoring and tracking system activity. For example following information about users is tracked.*** • ***How long they were logged in, the data they sent or received, their IP address, Uniform Resource Identifier (URI) they used, and the different services they accessed. In some cases, users may also be charged (monetary value) for the services provided based on this tracking/data collected.*** • ***O.S (e.g. Windows) typically authenticates the using "login name" and "password" (or other***	[1+6+ 3= 10]	CO1, CO2, CO3 CO4	L3

	mechanism like biometrics). ***Once user logs in, what s/he can do, depends on authorization. For example, sysadmin can install new software on the system, but an ordinary user can't.*** ***For auditing, Windows typically maintains three audit logs to track user and system activity. Application log, System log and security log.*** ***Logs can be viewed using built-in Event Viewer utility*** • ***Application log: Messages, status information, and events reported from applications and nonessential services on the Windows computer.*** • ***System log Records errors, warnings, and information events generated by the Windows operating system itself and related core system services*** • ***Security log Displays success and failure records from audited activities.*** • ***When you enable auditing and set specific auditing policies or settings in Windows, this is the log in which such items appear.***			
6	a) What is a Trojan? [2] What is Backdoor? [2] Explain in 2-3 lines each. Compare Trojan with Backdoor. [4] ***Trojan Horse is apparently harmless program containing malicious or harmful code*** ***It can get control and cause harm (e.g. Ruining file allocation table of hard disk)*** ***Trojans can get into the system in a variety of ways*** ***Email, USB drive or other portable media, software downloaded from Internet etc*** ***Unlike virus, Trojans do not replicate themselves, but can be equally destructive.*** • ***A malware that allows unauthorized access to a system by bypassing normal authentication processes*** • ***It provides a way for attackers to remotely control the infected system (provided the system has some form of connectivity)*** • ***Can be installed by other malware such as Trojans or through exploiting system vulnerabilities*** • ***Difficult to detect and completely disable*** ***See comparison table below.*** b) What is an identity theft? Explain in brief with example [2] ***Identity theft, in which the Internet is used to obtain a victim's personal information,*** ***Such as Social Security and driver's license numbers, to assume that person's identity. Once that is done, criminal can commit acts on behalf of victim (using identity of victim) to obtain money or property or use credit cards or bank accounts belonging to the victim*** ***Many people shred their documents (papers), but they will simply throwaway other media (USB drives, CDs and DVDs containing their data). This gives opportunity to criminals to get some crucial information about victims by means of "dumpster diving".***	[8] [2]	CO1, CO3, CO4, CO2	L3

Feature	**Trojan**	**Backdoor**
Definition	Malware that disguises itself as legitimate software to deceive users into installing it.	Malware that allows unauthorized access to a system by bypassing normal authentication processes.
Primary Purpose	To deceive users into installing it and then perform various malicious actions.	To provide and maintain unauthorized remote access to the system.
Method of Infection	Typically requires user interaction, such as downloading and running an attachment or clicking a malicious link. User interaction required to get installed.	Can be installed by other malware (such as Trojans) or through exploiting system vulnerabilities. Often does not require user interaction for installation and is installed via another malware or exploit.
Functionality	Can steal data, install other malware, can deliver payloads, which can in turn create damage	Specialized in enabling and maintaining unauthorized remote access.

Visibility	Often presents as legitimate software to deceive users initially.	Operates stealthily in the background to avoid detection.
Examples	Fake antivirus software, game cracks, keygens.	Remote Access Trojans (RATs), hidden modifications in legitimate software.
Persistence Mechanisms	May or may not have persistence mechanisms; depends on the payload.	Typically includes mechanisms to remain active and accessible after reboots or removal attempts.