INSTITUTE OF AERONAUTICAL ENGINEERING

(Autonomous)

Dundigal - 500 043, Hyderabad, Telangana

Examinations Control Office

Examination	B TECH VI SEMESTER END EXAMINATIONS REGULAR JUNE 2025 REG UG20		
Month & Year	1-Jun	**Date**	25/06/2025
Course Name	NETWORK AND WEB SECURITY		
Course Code	ACIC03	**E-Code**	6085

Instructions to Evaluators

- Evaluators should spend at least 3-5 minutes on one answer booklet during the evaluation.
- Evaluators should cross check that marks are allotted for all the attempted questions.
- The marks should be assigned fairly according to the mark distribution specified in the scheme of evaluation.
- For questions that were attempted incorrectly, evaluators are required to award zero marks.
- The evaluator must give a proper justification in case of any mistakes identified in the marks provided.

START WRITING FROM HERE

Q.No.

1.a Simple Mail Transfer Protocol (SMTP):-

Simple mail transfer protocol is a Text based protocol which internally uses the TCP - connection to reliably send mails.

→ It is an Client-Server archichetucture base protocol which is used to send and recive emails.

Component of SMTP :-

(i) User Agent (UA) :- (Mail User Agent).

It is a software that is responsible for handing the creation of an e-mail and reading of an email.

→ There are various User agent avilable on Internet, like gmail, outlook, yahoo etc.

(ii) Mail Transfer Agent :- (MTA)

MTA is a mail server, that is responsible for reciving the mail from the User Agent and pass it to the Mail access Agent.

→ It is a main componet in the SMTP mail Transfer.

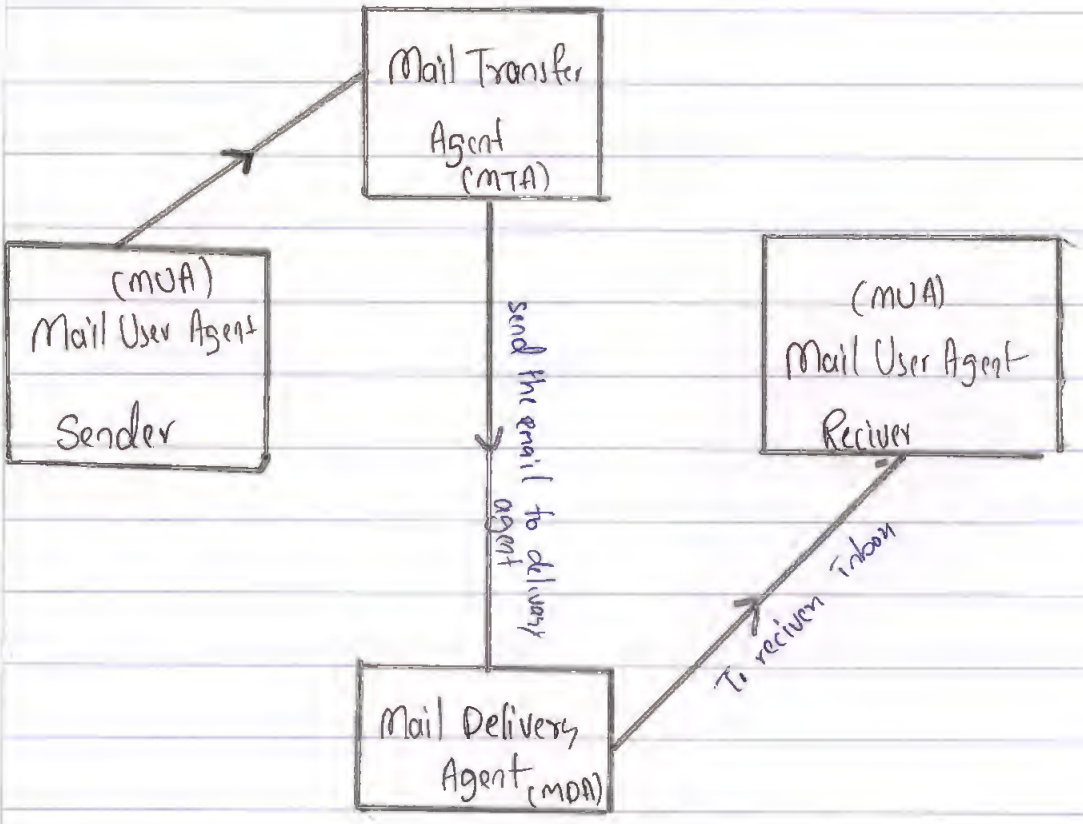
Q.No.

(iii) Mail Delivery Agent (MDA) :-

Mail Delivery Agent also known as Mail Access Agent (MAA), which is responsible for relaying the message / Mail to the destination.

→ Puts the email into the inbox of the Reciver.

Interaction between MUA, MTA and MDA :-



Q.No.

Step1 :- Sender creates and send the email using User agent like gmail, outlook etc

Step2 :- In the SMTP server, The Mail Transfer Agent (MTA), send the (Transfers) email to the of Mail Delivery Agent (MDA)

Step3 :- The Mail Delivery agent (MDA) will put the email in the reciver's inbox.

Security Issues in SMTP :-

Plain SMTP protocol have many security issues, so it is encrypted and authent-icated by UA to check its integrity

- Common Issues with SMTP :
  - → Pishing Attack
  - → Spam email
  - → Main in the Middle Attack
  - → Malware distribution
  - → Honey Trapping etc.,

Q.No.

1.b Domain Name System (DNS) :-

DNS is a distributed database system that converts the human readable domain names like (google.com) to it corresponding IP-Address like "195.168.51.91".

→ It act like a phone book of Internet.

DNS Components :-

- DNS Resolver,
- DNS Server,
- Root Server.

Security Issues :-

Unprotected DNS server have many security vulnerabilities like,

→ DNS cache hijacking / Poisoning
→ DNS Session hijacking.
→ DNS ID hijacking.
→ Tunneling.

To prevent these security issues DNS is enhanced with DNSSEC and NSEC3.

Q.No.

Mitigating Security Risks in DNS :-

The main and most common risk in DNS is cache poisoning, where attacker Modifies the cache in the DNS Resolver. The attacker send a Malinformadd DNS response to the Resolver, which is compromized by editing the IP - Address of the website. Resulting in security issues like opening Malicious websites, Installing Malware into computers.

→ Domain Name System Security Extention (DNSSEC) :-

DNSSEC is an security extention added to the DNS server. Which adds security keys to the Response. The DNS Resolver Validates the security keys to check the Integrity and authenticity of the DNS Response.

→ The data in the response is hashed and encrypted, using the public keys.

→ While The DNS - Resolver Trys to get an DNS responce from the server for a web domain, It will check the publicd security key of the responce

→

This proces strengthen the resolution proces.

Q.No.

by preventing the DNS - cache poisoning attacks, Addition the DNS is also wrapped with NSEC3 (Next Secure-3), which helps in preventing the Zone - enmuration Attacks

→ Zone Enumaration :- It is a process / technique of gathering information about domain and the sub-domains. In the context of DNS, it typically try to get the valid domine Address.

- The NSEC3 prevent this by implem-enting the authenticated ~~deny~~ denial-of-existance. As the NSEC3 is an extent-ion to the DNSSEC. It check the authenticity of the responce, If it is suspicious, then the NSEC3 will send the not-found response making it time taking and costly for attacker to get valied domine addresses

Q.No.	

2.a Network Intrusions :-

Network Intrusion is an illegal or a unauthorized activity or access gained by the attacker to exploit the network. The network intrusion may cause or lead to:

→ Data Theft
→ financial or Reputation loss
→ Stall of Network activity
→ Malware Installation
→ User and Owner privacy losses etc.

Detection of Intrusion in a Network :-

Intrusion detection is a method of finding the intrusion in the network to alert the admin and fix the issues. There are many Method that are used to Detect these Intrusions using the Intrusion Detection Systems.

→ Network Monitoring :-

Regularly or automate the monitoring the network to monitor the network activity, traffic using Monitoring Tools

Q.No.

→ Firewalls :-

Configure the firewalls to detect and filter the Network Traffic.

→ Logging and Reading :-

Check the logs of the networks to detect the unusual pattern in the traffic.

→ These are the few methods to detect the intrusions in a network, they usually monitor the network activities and find suspicious patterns in the activity to detect and alert the Admin.

Challenges in Intrusion Detection :-

→ Maintaining the secure Intrusion detection system is complex and expensive (IDS)

→ Hard to detect minor traffic changes due to model incapabilities, So use a capable model to detects an intrusion

→ False positives, Some time IDS detect normal traffic as an intrusion, resulting in call off the server, and resource wastage.

Q.No.

Key Components of a Real time Intrusion detection System (IDS):-

1. Monitoring System :- Checks the network traffic for unusual activities and usage.

2. Logging System - Records each and every activity in to the log files, to use it later for conforming the Intrusion.

3. Traffic Analyzer - Looks for suspicious activity or unusual traffic and find the pattern for intrusions.

4. Notifier - Sends Notification the admin, about the network Intrusion.

Q.No.

2.b **Port Scanning :-**

Port scanning is a type of security attack to find any open ports that are reciving data and sending data Attacker uses these ports to gain information or manupilate the data in the ports by running malicious scripts.

→ Types of Port scanning :-

- User Port Scanning
- Admin Port Scanning
- Application port Scanning
- Protocol port Scanning
- Application protocol port Scaning.

* Use Network segmentation and close unused ports to prevent attacked from the ~~prot~~ port scanning attack.

Performing a Detailed Port Scanning using NMap:-

NMap :- NMap is a software tool that is avilable for performing a Port Scanning attick on a machine.

Q.No.

Prerequisites :- ① Install and step setup NMap in your kali linux machine

② Aquire a vulnerable virtual machine and Run it on your local machine or use a cloud based virtual machine.

③ Provide the IP-address of this vulnerable machine to the NMap.

The Nmap will perform the port scanning attack on the provided IP address, and logs all the ports on the virtual Machine. And we need to detect the open ports that are either sending data, or recieving data to attack the port.

Potential Security Risks -

* Open ports
* Unsecure API end points
* Data theft
* Network & device Intrusion
* Malware Installation
* Network or activity Monitoring

Q.No.

4.a

Spyware :-

Spyware is a type of Malware (Malicio Software) that is used to monitor a computer Activity, like habits, preferences and activity with out the concern of the device / Computer Owner.

Key loggers :-

Keylogger is a type of spyware that is used to track the user activity with the computer. It will record keboard activity, Mouse/Track pad activity, and other input devices like scanners, ~~etc~~ etc., And the logs are sent to the attacker when the event triggers.

Privacy Concerns with Spyware and key loggers :-

Spyware and keylogger are security and privacy threats to the bothe individual user and the Organization. The spyware and the keylogger will steal the important data like passwords, bank information, important files, and personal information. They stalk up on the computer to gain important information about a person or an organization

Q.No.

Here are some important privacy threts due to the spyware and key loggers

→ UnAuthorized access of Camara and the microphone
→ Stealing data from Organization
→ Stealing important documents from a computer
→ Reading passwords of the User
→ financial losses due to the loss of the Bank credentials
→ loss of personal privacy
→ loss of personal information
→ Monitary and Confidentiality losses
→ loss of Trust etc

There are the few privacy concerns afflicted by the attack of the Spyware and Keyloggers.

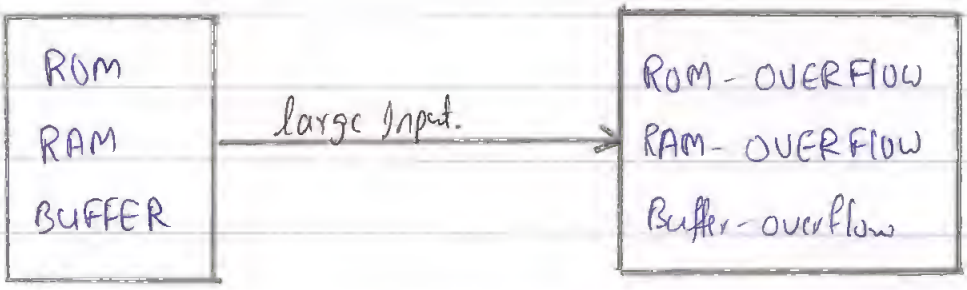
How to prevent an attack from spyware or keylogger:-

→ follow security patches and update regularly
→ Activate Antivirus software
→ Configure firewalls
→ Monitor System Traffic and Activity
→ Don't trust malicious Resources
→ Don't click on malicious or untrusted or illigimate links.

Q.No.

4b Buffer Overflow :-

Buffer overflow is a control hijacking method for gaining unauthorised accer to a system or a network. It usually work by filling upthe memory limit.



The attacker achive this by usually sending large payloads as input, causing the Buffer to overflowinto the RAM, and the attacker execute scripts to gain accer to the system. There are two types of Buffer overflow

(i) Stack Buffer Overflow
(ii) Heap Buffer Overflow

Considering a vulnerable 'C'-program, let us see how an attacker would gain an unauthorized shell accers.

In C- programming using of the builtin Methods like "gets" and concepts like

Q.No.

pointers are vulnerable to this Buffer overflow attack. The attacker inputs a large sized payload into the program. The input buffer which is reading the input will overflow due to the large size. And the data will be going into the Random Access Memory. Now the attacker has gained access to the system RAM. Now he ~~has~~ can store the shell command in the memory locations of the Random Access memory in the Basic Assembly language to run them. OR directly establish a connection with the targets CLI (Command Line Interface) of the shell. This way the attacker can read files, manuplate them and perform all possible activities ~~will be~~ illegally on the targets computer.

Defenses that can be applied:-

Now let us see some simple code-defences that can be applied to prevent this Buffer overflow attack

* Don't use "gets()" method, and use methods like scanf() etc to take inputs
* Provide input sanitization to avoid malicious inputs etc,

Q.No.

6.a Hyper Text Tranfer Protocol Secure (HTTPS) :-

Hyper text ~~tara~~ transfer protocol secure mode, is a secure version or extention of the HTTP protocol. Which is primarily used in web communicat-ion. Using HTTP the HTML, CSS, Javascript, text images and other files are transmitted between the client and the Server. But the HTTPS provide and excessive SSL / TLS (Secure Socket Layer) Certificate to the web application making it more secure compared to the plane HTTP.

And, No, The HTTPS alone doesn't protect the client server against the XSS (cross sitescripting) and CSRF (Cross site Request forgoing) attacks. The server and frontend need ~~b~~ to be secured in a way to with stand the XSS and CSRF attacks

Cross Site Scripting (XSS) :-

The Cross site Scripting is a security attack in web which allow the attacker to inject the Malicious code into

Q.No

the website, it could be temporary change, reflected changed or a stored change.

Example :-

→ HTML Injection : Attacker inject html code into the website using the dev-tools. low threat as the change is visible to attacker only

→ Javascript Injection : Attacker inject Javascript code into the script tag which can be triggered inside the Main website, Moderate threat as the data can be stolen.

→ SQL injection :- Attack put malicious values into the input fields gaining unauthorized access or unexpected behaviour in the application

Cross Site Request Forging :-

On a CSRF attack the attacker will forge the HTTP request of a server and malnupilate it by changing the parameters, headers, cookie, etc, finally gains data access or unauthorized activity to the

Q.No.

website.

Tools Used :-

- Postman, Javascript, dev-Tools etc

Here HTTPS will only encode the data packets which can be protected from attacks like Man-in-the middle. But here XSS and CSRF will not be detected and prevented by the HTTPS, as both will be sending the HTTPS forged Request to the Server or client.

Q.No.

6b Same - Site - Protocol - (SOP)

The Same site protocol (SOP) is the default browser requesting protocol used by the websites, unless they are modified for the Cross (x) site Communication using

- CORS (Cross origin Resource sharing)
- JSON with padding
- Using Server proxies etc,

Using this Cross - site - Communication could be helpful for API and resource sharing but also make it vulnerable to the Malicious attacks if not configured properly

Scenario where violating SOP, allowing malicious access :-

Now, let us simulate a scenario where violation of the Same - Origin ~~Polic~~ policy leading to unauthorized malicious access to user data

Consider a nodejs server running on the cloud platform like AWS or Vercel with CORS(Cross - origin - Resource - sharing) set to

Q.No.

all domains, Here instead of specifing a particular domain name in the CORS enabler, The developer has allowed any web address to make the http request.

Using this vulnerabilities the attacker will gain the unauthorized access to the sensitive user data. And at last the attacker could clone the whole we application using the http request and manage it with out the owners consent. This violation of SOP will effect the data loss, performance loss, as the attack will send more request to the api to gain information automatically slowing the server. Increases the ~~elevated~~ cloud charges due to increasing traffic.

Consequences:-

- → Data theft
- → Loss of User Trust
- → Increase in cloud charges
- → Financial loses etc

So, In conclusion it is safer to use the SOP or X-site-communication with proper configuration

Q.No.

7a Hyper Text Transfer Protocol Parameter Pollution (HPP) :-

. Http parameter pollution is a web based attack used by the third party actor to gain un-authorized access by sending Malinformed parameters to the server. This is done as with sending duplicate parameters, large payloads into the parameters. If not handled properly the server will exhibit abnormal activities resulting in the data breaches or unauthorized access.

In http parameter pollution (HPP) attack the attacker will send multiple parameters with the same name to the server. The server will confuse for the real parameter which could result in the crash or unexpected behaviour of the server.

Preventing HPP :-

* Disable Cross Site Scripting (XSS)
* Sanitize the parameter before processing.
* Write defencive code for Multiple parameter handling
* Protect from Cross Site Request forging (CSRF)

Q.No.

and defed CSRF, to dealdens the service

* Add rate limitten to limit the number of request
* Protect from DOS & DDOS attack, by blocting the IP-addresses
* Properly Authenticate the request before Serving it.
* Input validation and parameter validation,
* defect malicious or suspicious request
* Implement WAF (Web application firewalls) to filter dangerous/Malicious requests

Q.No.

7b. Context :- ed shopping cart application allows users to update item quantity.

Issue :- Odn attacker modifies a request to set a negative quantity for an item.

Task :- Discribe how could it be exploited and propose a solution to prevent it.

(i) Exploiting the issue :-

The attacker will send a payload which could look like this

```
body : {
    id : "51ab3azbcx1a3",
    itemid : "55675XXAB",
    quantity : -5
}.
```

This payload is asking the server to modify the cart item quantity of item "55675XX AB", to the value "-5", which is negative. Using this exploit, the attacker will be gain! Money or crash the server. how ?, let see,

Q.No.

the quantity is -5, and suppose the price of the item is 6700Rs, then,

1 item = 6700

2 item = 13400

and,

-5 items = -33,500 Rs

So the final cart value will be -33,500 Rs. When the attacker place the Order, then company will pay to the attacker resulting in monetary loss.

(ii) Solution:-

The simple solution is to validate the input to fix the logic flaw.

```
if (quantity == 0) {
        deleteItem();
}
else if (quantity < 0) {
        error();
}
else {
        update();
}
```

Q.No.	
	This simple condition will fix the logical flaw and prevent the above exploit.

Q.No.	

Q.No.	

Q.No.	

Q.No.	

Q.No.	

Q.No.	

Q.No.	

Q.No.	

ROUGH WORK

Content written here will not be considered for valuation

67
× 5

335