CBCS SCHEME

USN | | | | | | | | | | |

18EC821

Eighth Semester B.E. Degree Examination, June/July 2023
Network Security

Time: 3 hrs. Max. Marks: 100

Note: Answer any FIVE full questions, choosing ONE full question from each module.

Module-1

1 a. Illustrate the use of 4 chief principles necessary for providing security. **(10 Marks)**

b. The sole aim of the attacker is to maximize financial gain by attacking computer systems. Identify the attack and further elaborate the different varieties of same. **(10 Marks)**

OR

2 a. What is an active attack? Explain in detail how active attacks are classified. **(10 Marks)**

b. With real time examples, discuss phishing and pharming. **(10 Marks)**

Module-2

3 a. The web is faced with different types of security threats. Compare the threats on the web. **(10 Marks)**

b. Illustrate with diagram the step by step operation of SSL record protocol. Explain each step briefly. **(10 Marks)**

OR

4 a. Discuss the different alert codes supported by Transport Layer Security (TLS). **(10 Marks)**

b. With a neat diagram, explain Secure Shell (SSH) protocol stack. **(10 Marks)**

Module-3

5 a. Discuss applications of IP sec. **(05 Marks)**

b. List and explain IP sec documents. **(05 Marks)**

c. Explain Transport and Tunnel modes. **(10 Marks)**

OR

6 a. Discuss the purpose of padding and Anti-Replay service. **(10 Marks)**

b. Illustrate the working of basic combinations of security associations. **(10 Marks)**

Module-4

7 a. Explain 3 classes of intruders with examples, discuss intruder patterns of behavior. **(10 Marks)**

b. With a neat diagram, illustrate the profiles of intruder and authorized users. Also discuss approaches to intrusion detection. **(10 Marks)**

OR

8 a. Describe the overall taxonomy of software threats (Terminology of Malicious program). **(10 Marks)**

b. Explain the anti-virus approaches and also in detail discuss the generations of antivirus software. **(10 Marks)**

Module-5

9 a. Explain the four general techniques that the fire wall use to control access. **(05 Marks)**

b. Discuss the capabilities which one within the scope of a firewall. **(05 Marks)**

c. With a neat diagram, describe the working of packet filtering fire wall. **(10 Marks)**

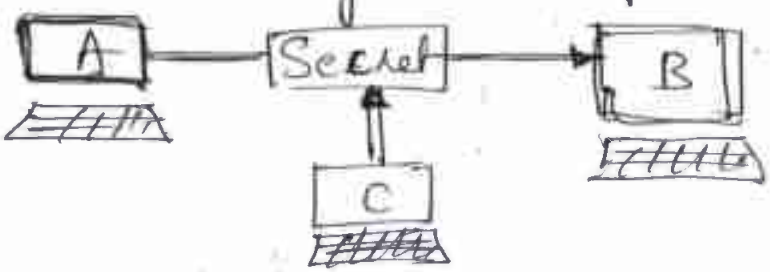
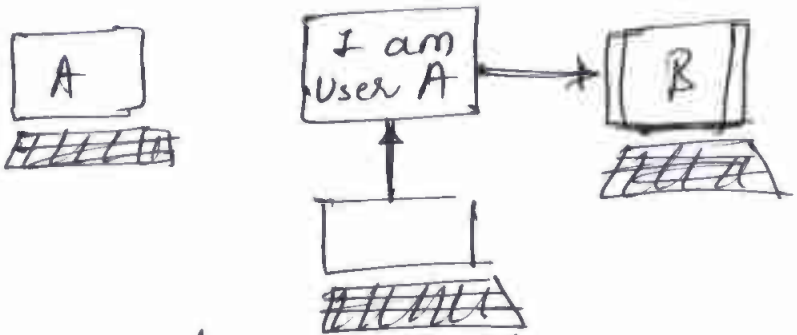
OR

10 a. Discuss the characteristics of Bastion Host. **(10 Marks)**

b. Explain Host based and personal firewalls. **(06 Marks)**

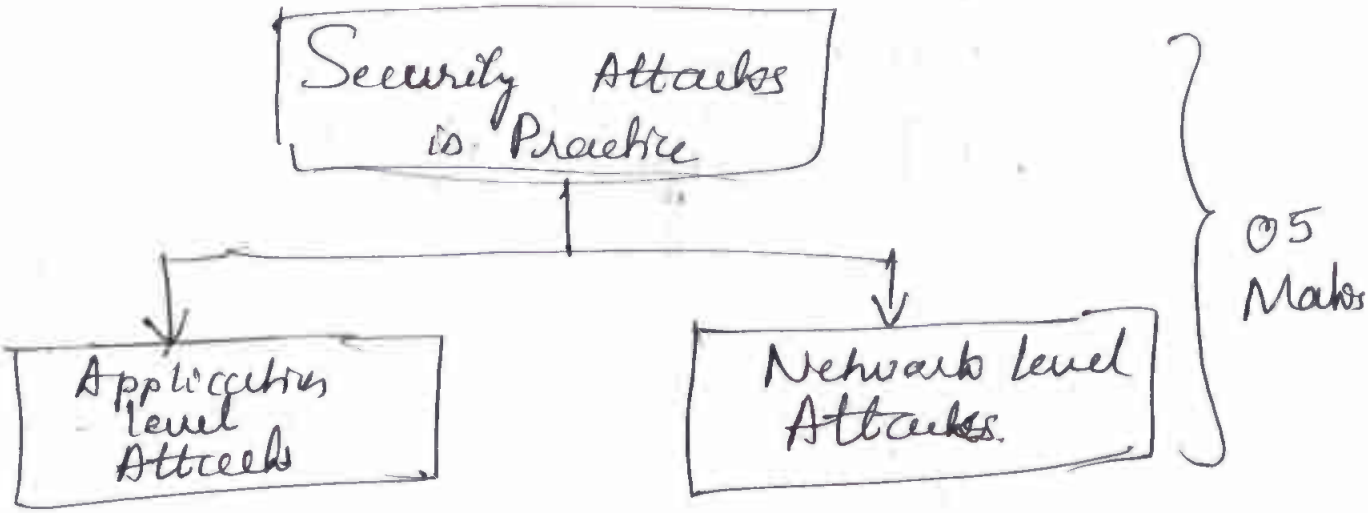
c. Explain the different purposes for which internal fire wall can be used. **(04 Marks)**

* * * * *

Question Number	Solution	Marks Allocated
Q 1 Ans.	Principles of Security (i) Confidentiality: Explanation  Interception causes loss of Message Confidentiality (ii) Authentication: Explaination  Absence of Authentication (iii) Integrity Explaination  (iv) Non-repudiation: Explaination Diagram → Establishing Non Repudiation	2.5 Mark 2.5 Mark 2.5 Mark 2.5 Mark

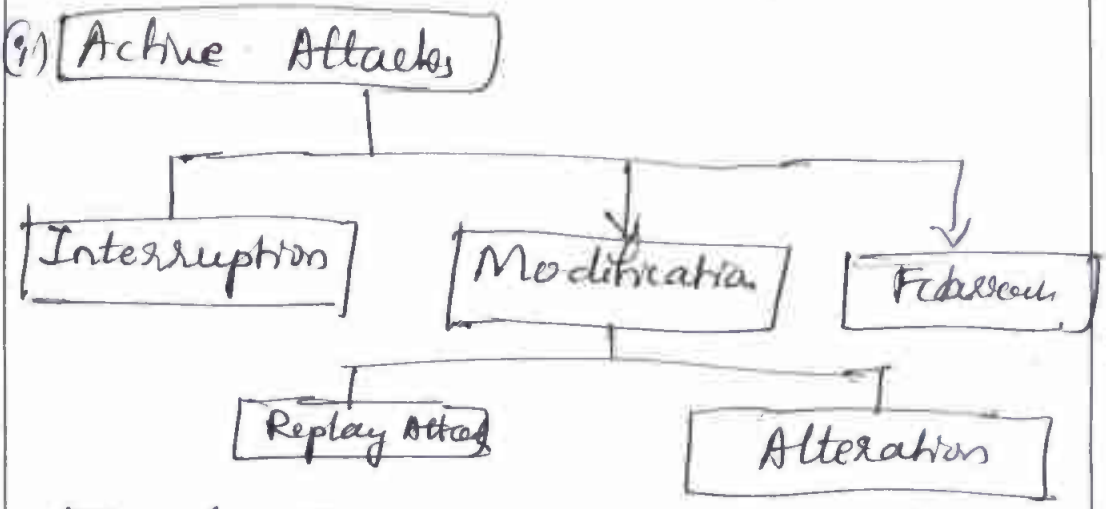
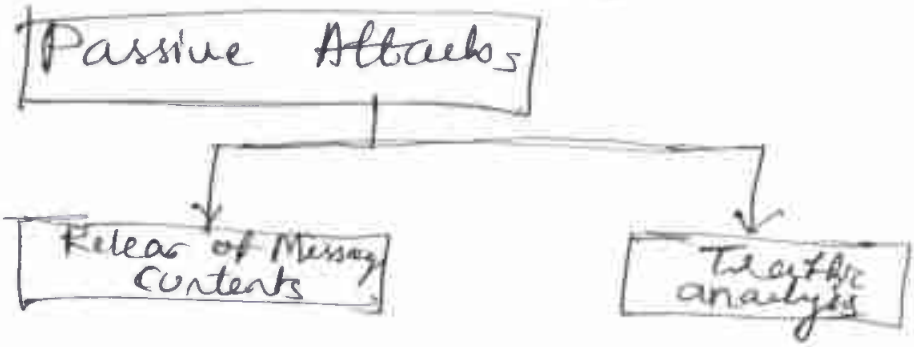
Q 1 (b)

Students can take real time examples of security attacks and can explain neatly with a relevent diagram. } 5 Marks



& Explaination

Subject Title : Network Security Subject Code : 18EC82

Question Number	Solution	Marks Allocated
Q 2 Ans (a)	(i) Active Attacks	
		2½ Marks
	Brief Explaination of each carries 2 Marks each	
	(ii) Passive Attacks	
		2.5 Marks
	Explaination	
	Examples with ———	5 Marks
Q 2 (b)	Definition	
	Virus:	02 Mark
	Worms:	02 Marks
	Cookies:	01 Mark

Q 2

(b) Packet Sniffing is passive attacks. attacker observe the conversation

Packet Spoofing: An attacker sends the packet with false source address. called spoofed address

Phishing:

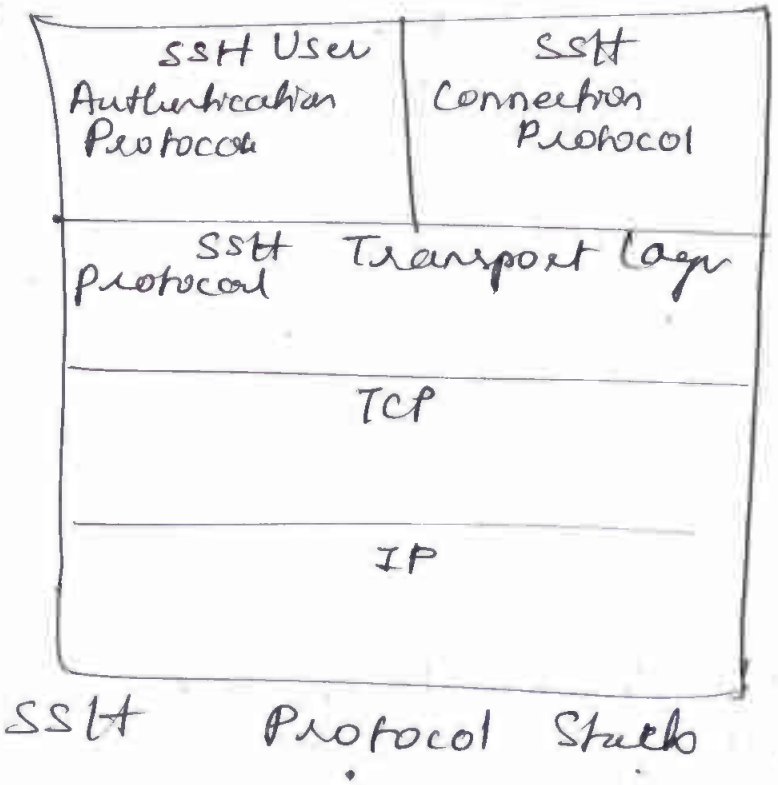
* Attacker creates identical fake web sites to a real websites
*

Subject Title : Network Security Subject Code : 18EC821

Question Number	Solution	Marks Allocated
Q 3 Ans (a)	SSL Protocol Stack SSL Handshake Protocol | SSL Change Cipher Spec Protocol | SSL Alert Protocol | HTTP SSL Record Protocol TCP IP Individual protocol working explaination	2 Marks 8 Marks
Q 3 (b)	Hand shake Protocol Explaination Client — Server client_hello server_hello certificate key exchg Certificate request server_hello_done Certificate Client key Exchg C_Verify Cipher_spec Finished change_cipher_spec Finished Phase 1: Establish security capabilities Phase 2: Server may send certificates Phase 3: Client sends the certificate if requested Phase 4: Change cipher Suite & finish handshake protocol	4 Marks

The working of handshake protocol carries — 6 Marks

Q 4
Ans (a)



4 Marks

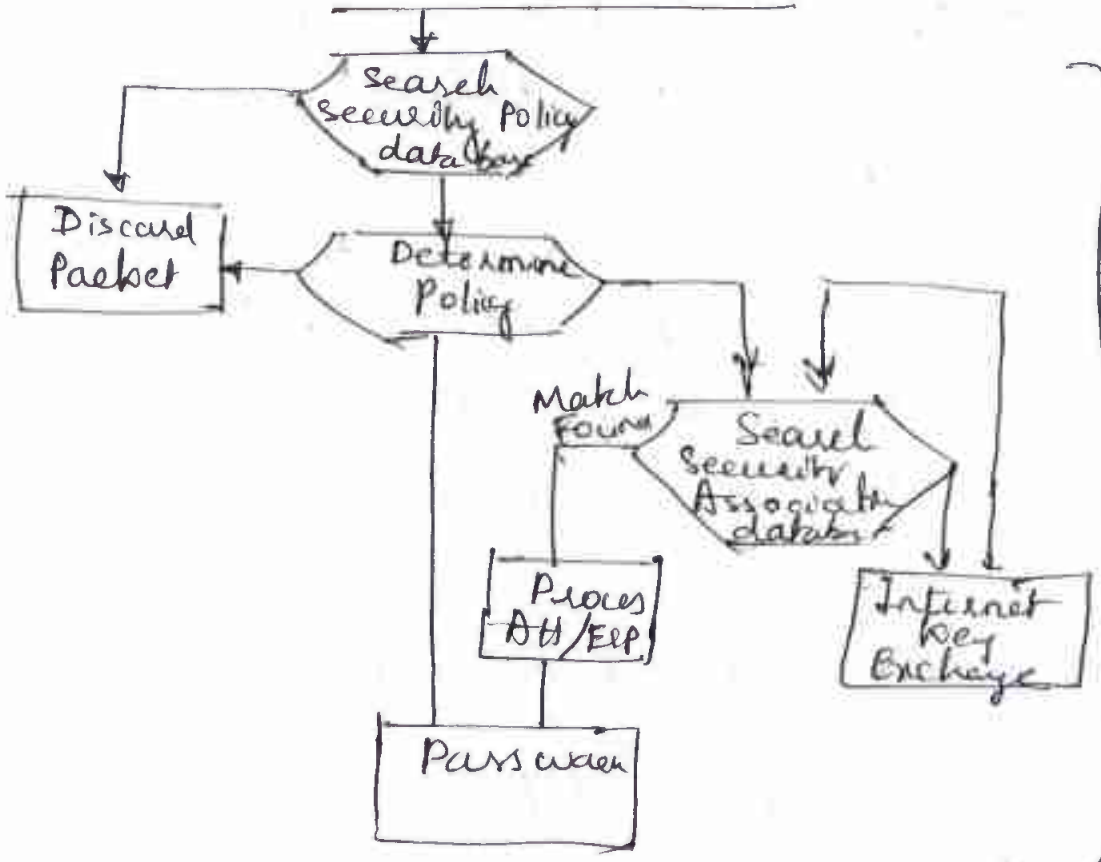
Explaination of the stacks of each protocols involved — 6 Marks

Subject Title : Network Security Subject Code : 18EC821

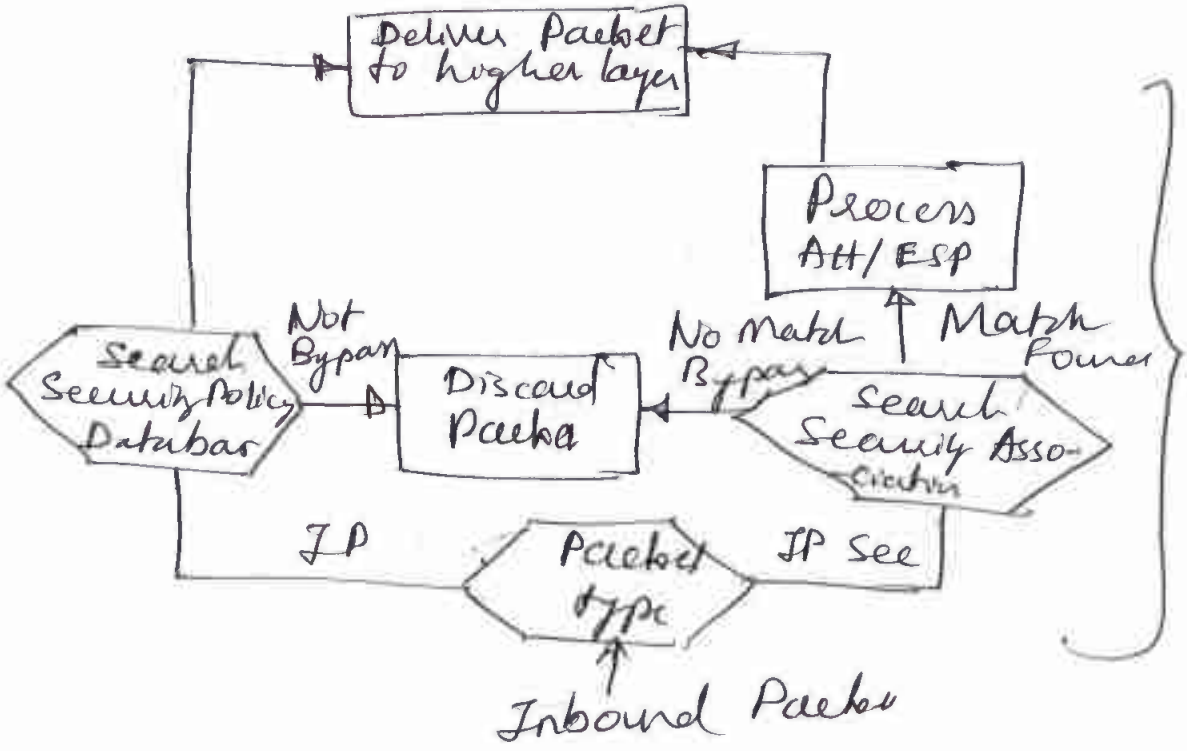
Question Number	Solution	Marks Allocated
Q 4 (b)	HTTPS = HTTP + SSL to implement secure connection between web server & client. address begins https:// rather than http:// when https is used the following elements are encrypted (i) URL of the requested document (ii) contents (iii) contents of browser form (iv) Cookies sent (v) Contents of HTTP Connection initiation: Connection Closure	5 Marks 2½ Marks 2½ Marks

Q 5

Ans : Processing model for outbound Packet



Explanation — 3 Marks



Explanation — 2 Marks

Subject Title : Network Security Subject Code : 18EC821

Question Number	Solution	Marks Allocated
Q 5 (b)	IP Sec Services (i) Access Control (ii) Connectionless integrity (iii) Data origin Authentication (iv) Rejection of replayed Packets (v) Confidentiality Explaination about the above	2 Mark 3 Mark
Q 5 (c)	IP Sec Documents can be categorised (i) Architecture (ii) Authentication Header (iii) Encapsulating Security payload (iv) Internet Key exchange (v) Cryptographic algorithm with Explaination	5 Mark

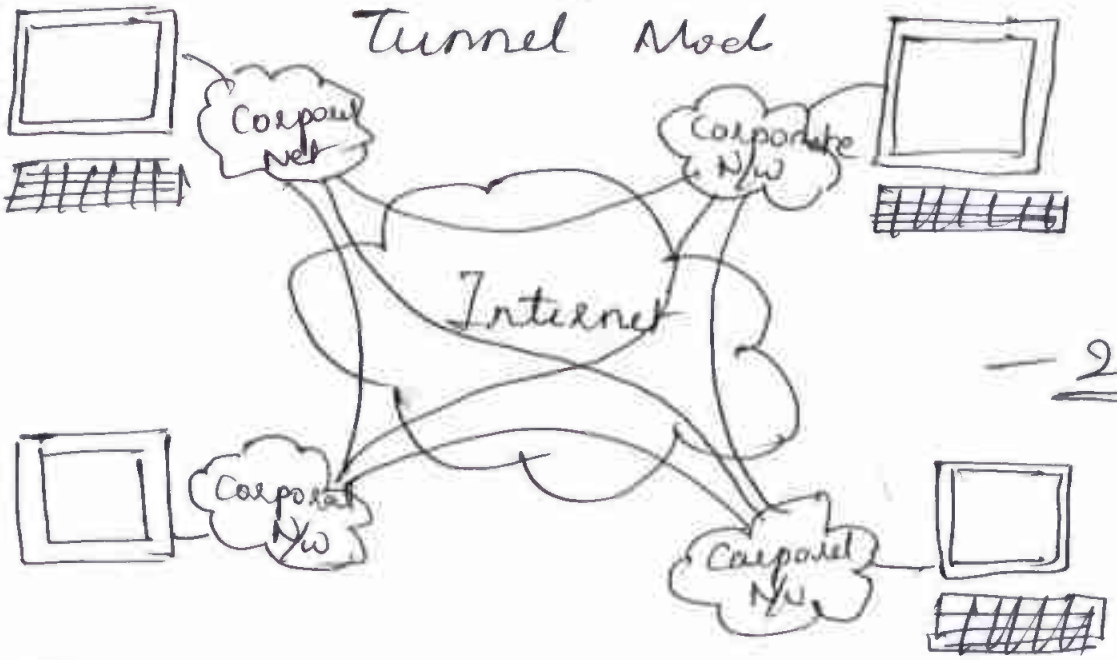
Q6
(a)

Transport level Security

— 2 Marks

Explanation Carrier — 3 Marks

Tunnel Mode

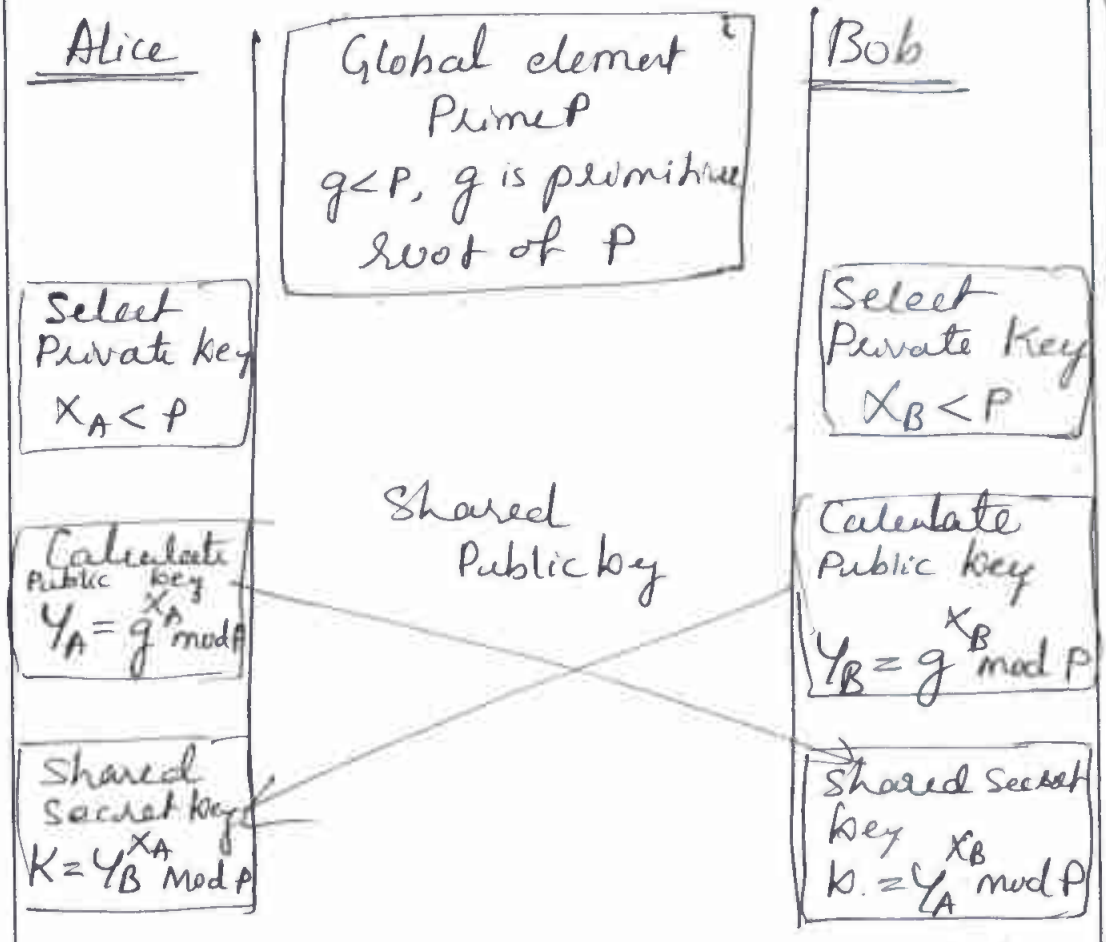


— 2 Marks

Explanation Carrier — 3 Marks

Subject Title : Network Security Subject Code : 18EC824

Question Number	Solution	Marks Allocated
Q 6 (b)	Diffie Hellman Key Exchange	



Both Parties Ended with K

* This can be explained with in terms of points also.

Example with values. carry — 3 Ma

Q 7 Three classes of Intruders

(a) (i) Masquerader;

(ii) Misfeasor;

(iii) Clandestine User;

} Brief Explanation — 5 Mark

Intruder Patterns of Behaviour -

(a) Hacker:

Examples

(b) Criminal Enterprise

Examples

(c) Internal Threat

Example

} 5 Marks

Q 7

(b) Intrusion Techniques

(i) One-way Functions

(ii) Access Control

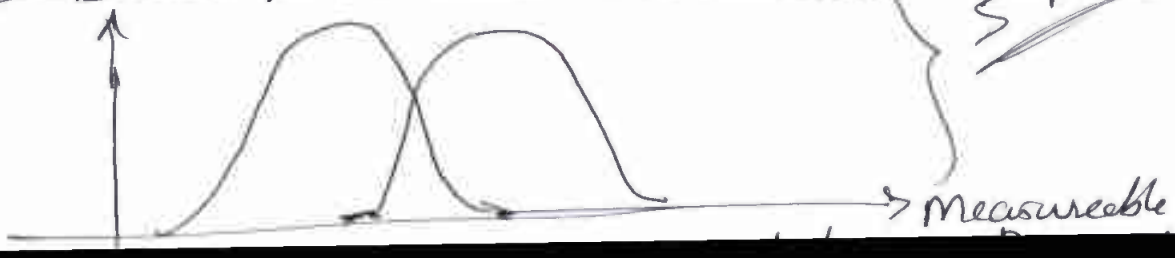
} Explanation — 5 Marks

Intrusion Detection

(i) Rule-based anomaly detection

(ii) Rule-Based penetration identification

} 5 Marks



Subject Title : Subject Code :

Question Number	Solution	Marks Allocated
Q 8 (a)	Types of Malicious Programs Virus Worms Logic bomb Trojan horse Backdoor Mobile code Exploits Downloader Auto-rooter Kit (Virus generator) Spammer programs Floodors	10 Mark
(b)	Multiple threat Malware (i) Multiparite (ii) Blended Attacks E-mail Windows shares Web services Web client	5 Mark

Page No.

8(C) Four Phases of Virus with Explanation

(i) Dormant Phase

(ii) Propagation Phase

(iii) Triggering Phase

(iv) Execution Phase

} 5 Mark

Subject Title : Subject Code :

Question Number	Solution	Marks Allocated
Q 9 (a)	Firewall Characteristics (i) Service Control (ii) Direction Control (iii) User Control (iv) Behavior Control Explaination of these	10 Marks
(b)	Limitations of Firewal (i) cannot protect ageinst the attack that bypasses the firewal (ii) Lap ors, PDA, or any storage device is used outside the corporate N/w then attached & used internally. (iii) It may not protected ageinst internal firewall	5 Marks
Q 9 (c)	Fire wall attacks (i) IP addres spoofing (ii) Source Routing attacks (iii) Tiny fragment attacks	5 Marks

10(a) Types of Firewalls

Diagram with detailed Explanation

(i) Packet Filtering Firewalls — 2.5 Mark

(ii) Stateful Inspection Firewalls — 2½ Mark

(iii) Application level Gateways — 2½ Mark

(iv) Circuit level Gateway — 2½ Mark

Total 10 Mark

Q 10

(a) DMZ Network

with Block diagram representation

(b) Virtual Private N/w

(c) Distributed Firewall

all the three Explanation with Need diagram — 10 Mark