CBCS SCHEME

USN | | | | | | | | | | 15EC835

Eighth Semester B.E. Degree Examination, Dec.2019/Jan.2020
Network and Cyber Security

Time: 3 hrs. Max. Marks: 80

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

Module-1

1 a. Define various parameters that are associated with session state and connection state of SSL protocol. (08 Marks)

b. Explain the additional alert codes in TLS over SSLVs. Describe SSL record protocol. (08 Marks)

OR

2 a. With relevant diagram explain the various phases of handshake protocol. (10 Marks)

b. Discuss sequence of steps involved during message exchange in user authentication protocols of SSH. (06 Marks)

Module-2

3 a. Describe with flow diagram transmission and reception of PGP messages. (06 Marks)

b. With relevant diagram explain the confidentiality and authentication services provided by PGP protocol. (10 Marks)

OR

4 a. Describe the various header fields defined in MIME. (04 Marks)

b. Describe the functions provided by SMIME. (04 Marks)

c. With relevant diagram, explain the IMIM functional flow. (08 Marks)

Module-3

5 a. Draw a diagram to illustrate IP security scenario and also explain benefits of IPSec. (08 Marks)

b. With relevant diagram, describe various fields in ESP packet format. (08 Marks)

OR

6 a. Draw and explain the IP traffic processing model for inbound and outbound packets. (10 Marks)

b. With relevant diagram, describe IKE header and payload format. (06 Marks)

Module-4

7 a. Mention the types of cyber anti-pattern templates. Explain the various components of these templates. (10 Marks)

b. Write a brief note on "No time for Security" anti-patterns. (06 Marks)

QP solutions prepared by Damodar S. H

20.07.2021
Head of the Department
Dept. of Electronic & Communication Engg.
KLS V.D.I.T., HALIYAL (U.K.)

OR

8 a. Explain the various specialized skills that should be available on-demand in IT security shops. (05 Marks)
b. What is the significance of signature based Malware detection and what are its limitations against polymorphic threats. (05 Marks)
c. Write a brief note on forces in cyber anti-pattern. (08 Marks)

Module-5

9 a. Describe the architectural problem solving patterns. (08 Marks)
b. Explain the role of Zachmann framework in cyber security. (08 Marks)

OR

10 a. Explain various technology included in HBS (Host Based Security). (10 Marks)
b. Why is network administration on essential skill for hands-on-cyber security professional? (06 Marks)

* * * * *

Eighth Semester B.E. Degree Examination: Dec 2019 / Jan 2020 MARKS

Network and Cyber Security: Question paper Solution

1.a) Define various parameters that are associated with Session state and connection state of SSL Protocol 08

> A connection state is defined by the following parameters.

* Server and client random: Byte sequences that are chosen by the server and client for each connection
* Server write MAC secret: Secrete key used in MAC operations on data sent by the server
* Client write MAC secret: The secret key used in MAC operations on data sent by the client.
* Server write key: The secret encryption key for data encrypted by the server and decrypted by the client 4
* Client write key: The symmetric encryption key for data encrypted by the client and decrypted by the server
* Initialization vectors (IV): Initialization vector is maintained for each key, when a block cipher is used in CBC Mode.
* Sequence Numbers: > Each party maintains separate sequence numbers for transmitted and received messages for each connection
  > Sequence numbers may not exceed $2^{64}-1$

> A session state is defined by the following parameters

* Session identifier: An arbitrary byte sequence chosen by the server to identify an active or resumable session state.
* Peer certificate: An X509.v3 certificate of the peer and may be null

(Damodar S.B)

* Compression Method: The algorithm used to compress data prior to encryption.
* Cipher Spec: Specifies the bulk data encryption algorithm such as null, AES, etc and a hash algorithm such as MD5, SHA-1 etc used for MAC calculation.
  * Also defines cryptographic attributes such as the hash size. 4
* Master secret: 48-byte secret shared between the client and the server
* Is resumable: It is a flag that indicates whether the session can be used to initiate new connections.

1.6) Explain the additional alert codes in TLS over SSL Vs. Describe SSL record protocol 08

> Additional Codes defined in TLS

Fatal:
i) Record_overflow ii) Unknown_ca iii) Access denied
iv) Decode_error v) Protocol_version vi) Insufficient_security
vii) Unsupported_extension viii) Internal_error
ix) Decrypt error x)

Remaining alerts
i) User Cancelled ii) No renegotiation

Listing — 1
Explanation of any 3 — 3

> SSL Record Protocol

The SSL Record Protocol provides two services for SSL connections:
* Confidentiality: The Handshake protocol defines a shared secret key that is used for conventional encryption of SSL payloads

(Damodar Sir)

MAR

2a) With relevant diagram explain the various phases of handshake protocol. — 10

- SSL Handshake protocol has four phases

* Phase 1: Establish Security Capabilities
  * The exchange is initiated by the client which sends the client hello message with the following parameters
    * Version: The highest SSL version understood by the client.
    * Random: A client generated random number which serves as nonce
    * SessionId: A variable length session identifier
      - A non zero value - client update
      - A zero value - client new connection
    * Cipher Suite: List of cryptographic algorithms supported by client in decreasing order of preference
    - Compression method: List of compression methods supported by client

* Phase 2: Server authentication and key exchange
  * The server sends a server-key-exchange message which contains list of secret keys to be used for subsequent data
  * The certificate-request message is sent next which includes two parameters certificate types and certificate-authorities
  * The final message in phase 2 is server-done message.

2 2

* Indicates the end of the server hello and associated messages.

* Phase 3: Client Authentication and key exchange
  * The client verifies the server certificates and checks whether the server_hello parameters are acceptable.
  * If all is satisfactory, the client sends a certificate message. If the server has requested a certificate If no suitable certificate is available, the client sends a no_certificate alert 2
  * Next is the client_key_exchange message which has the same parameters as the server key-exchange message.
  * Similarly the client may send a certificate verify message to provide explicit verification of a client certificate.
  * The client encrypts all the previous messages and master_secret with its private key.

* Phase 4: Finish
  * This phase completes the setting up a secure connection
  * The client sends a Change_Cipher_Spec message and copies the pending CipherSpec into the current CipherSpec 2
  * Moreover, the client then immediately sends the finished message under the new algorithms, key and secrets. Related Figure — 2M

(Damodar S H)

MAR

2.b) Discuss sequence of steps involved during message exchange in user authentication protocols of SSH 06

1) Sequence of steps involved during message exchange includes the following steps

1.) The Client sends a SSH_MSG_USERAUTH_REQUEST with a requested method name

2) The server checks to determine if the user name is valid. If not, the server returns SSH_MSG_USERAUTH_FAILURE. with the partial success value of false. If the user name is valid, the server proceeds to step 3

3) The server returns SSH_MSG_USERAUTH_FAILURE with a list of one or more authentication methods to be used

4) The client selects one of the acceptable authentication methods and sends a SSH_MSG_USERAUTH_REQUEST with that method name and the required method specific fields

5) If the authentication succeeds and more authentication methods are required, the server proceeds to step 3, using partial success value of true. If the authentication fails, the server proceeds to step 3, using partial success value of false.

6) When all required authentication methods succeed, the server sends a SSH_MSG_USERAUTH_SUCCESS message, and the authentication protocol is over.

1 X 6 = 06

(Damodar S.H)

MARKS

* The content of the finished message is the concatenation of two hash values.
* The server sends its own Change-Cipher-Spec message, transfer the pending state to the current cipher spec and sends finished.
* At this point the handshake is complete and the client and server may begin to exchange application layer data.

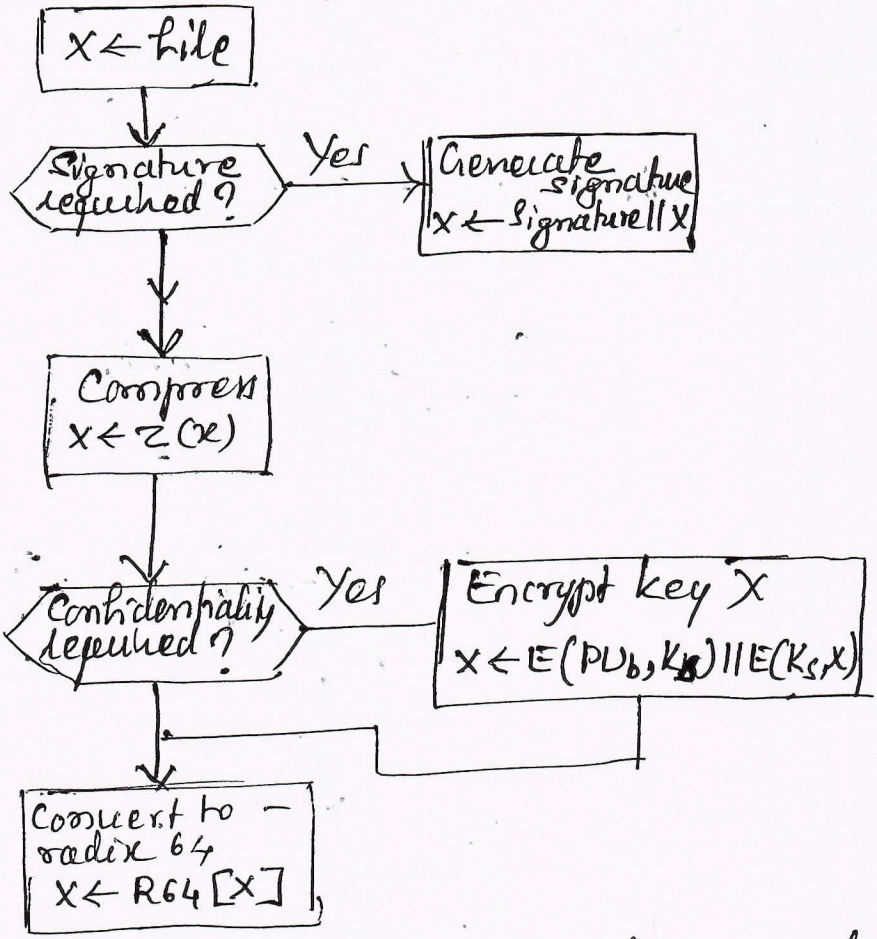
1X6=06

(Damodar S.H)

MARKS

3a) Describe with flow diagram transmission and reception of PGP messages 06

* Transmission of PGP message



3

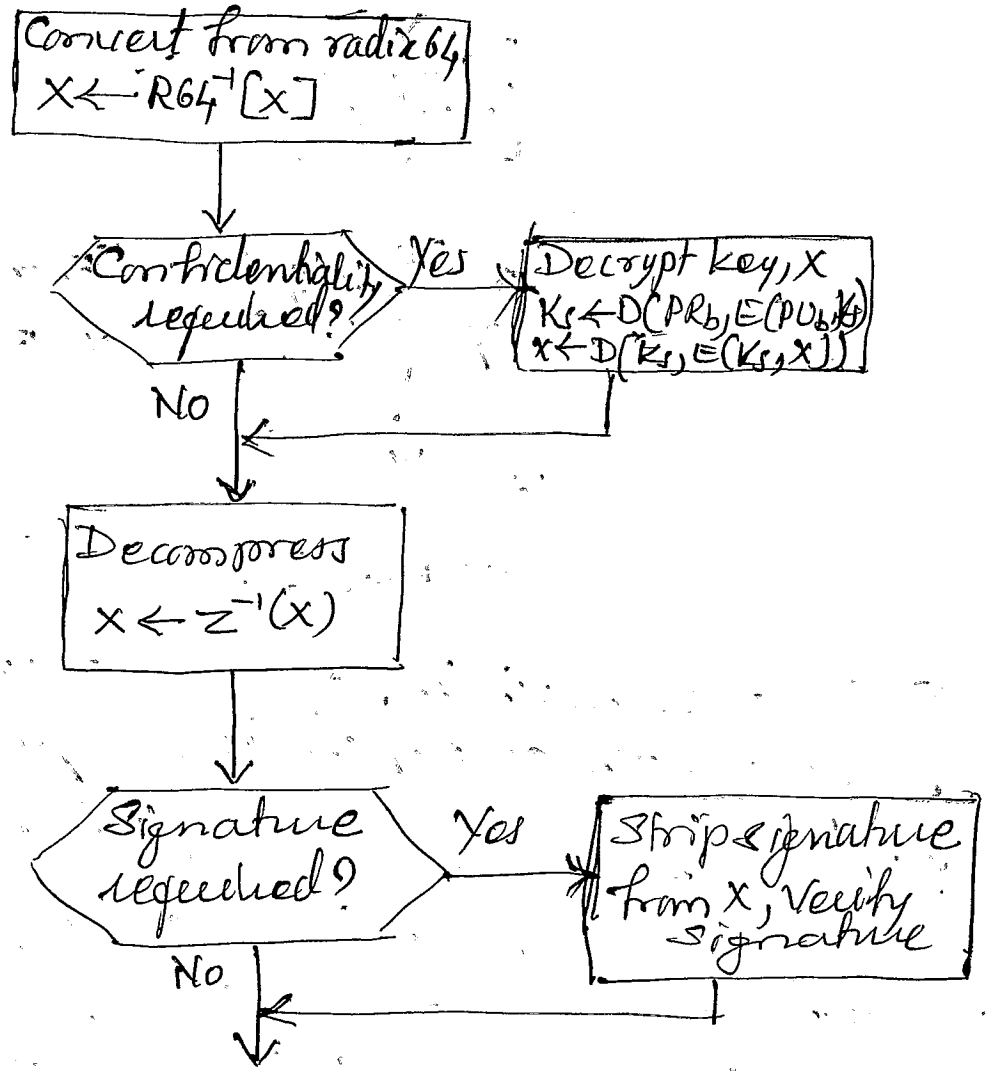
* On transmission, a signature is generated using a hash code of the uncompressed plaintext
* Then signature plus plaintext is compressed
* If confidentiality is required consisting of compressed plaintext or compressed signature plus plaintext is encrypted and prepended with the public key-encrypted symmetric encryption key.
* Finally, the entire block is converted to radix-64 format

* Reception of PGP messages
  * On reception, the incoming block is first converted

(Damodar S.H)

back from radix 64 format to binary.

* If the message is encrypted, the recipient recovers the session key and decrypts the message. The resulting block is then decompressed.
* If the message is signed, the recipient recovers the transmitted hash code and compares it to its own calculation of the hash code.

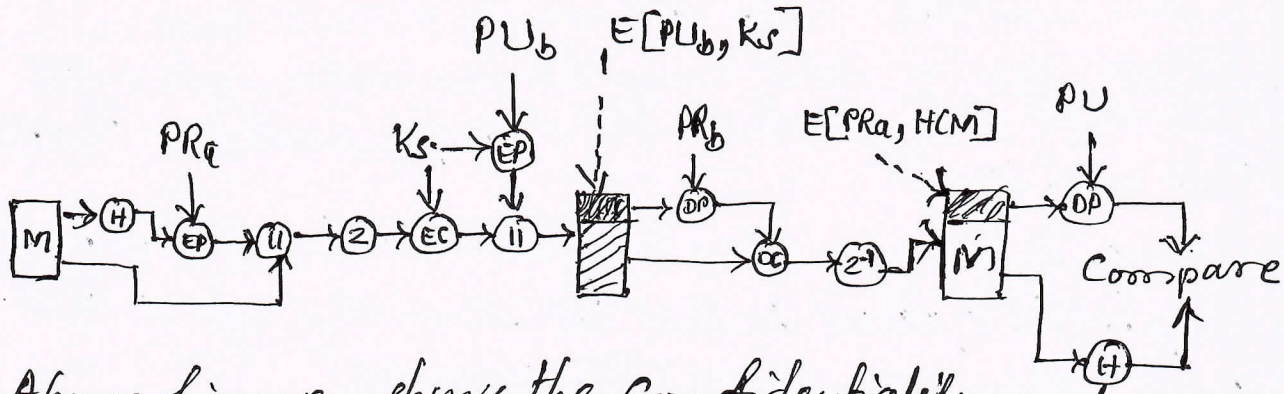


3

(Damodar S.H)

MARKS

3.b) With relevant diagram explain the confidentiality and authentication services provided by PGP Protocol. 10



5

Above figure shows the confidentiality and authentication services used provided by PGP protocol

* First signature is generated for plaintext message and prepended to the message.
* Plaintext message plus signature is encrypted using CAST-128 (or IDEA or 3DES), and the session key is encrypted using RSA (or ELGamal)
* It is generally convenient to store a signature with a plaintext version of a message

5

* For the purposes of third-party verification, if the signature is performed first, a third party need not be concerned with the symmetric key when verifying the signature
* In ~~summary~~ Summary, when both services are used, the sender first signs the message with its private key, then encrypts the message with a session key, and finally encrypts the session key with the recipient's public key.

(Damodar S.H)

4.a) Describe the various header fields defined in MIME — 04

> The five header fields defined in MIME are

* MIME-Version: Must have the parameter value 1.0 This field indicates that the message conforms to RFCs 2045 and 2046
* Content-Type: Describes the data contained in the body with sufficient detail so that the receiving agent can deal with the data in an appropriate manner.
* Content-Transfer-Encoding: Indicates the type of transformation that has been used to represent the body of the message in a way that is acceptable for mail transport — 4
* Content-ID: Used to identify MIME entities uniquely in multiple contexts.
* Content-Description: A text description of the object with the body: this is useful when the object is not readable

4.b) Describe the functions provided by S/MIME 04

> S/MIME provides the following functions

1) Enveloped data: Consists of encrypted content of any type and encrypted content and encryption keys for one or more recipients.
2) Signed data: A digital signature is formed by taking the message digest of the content to be signed and then encrypting that with the private key of the signer.
3) Clear signed data: A digital signature of the content is formed.

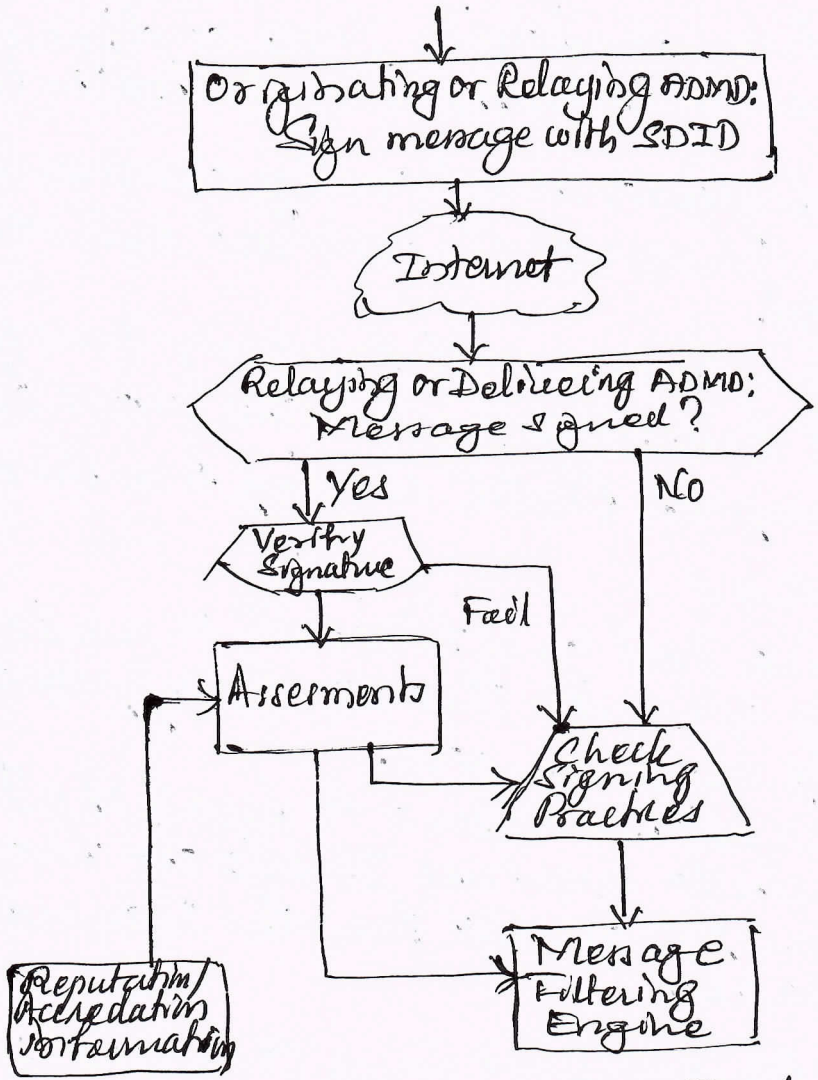
(Damodar S.H)

MARKS

4) Signed and enveloped data: Signed only and encrypted only entities may be nested, so that encrypted data may be signed and signed data or clear signed data may be encrypted.

4.c) With relevant diagram, explain the DKIM functional flow. 08

- Figure shows detailed look at the elements of DKIM Operation.
- Basic message processing is divided between a - signing Administrative Management Domain (ADMD) and verifying ADMD



4 M

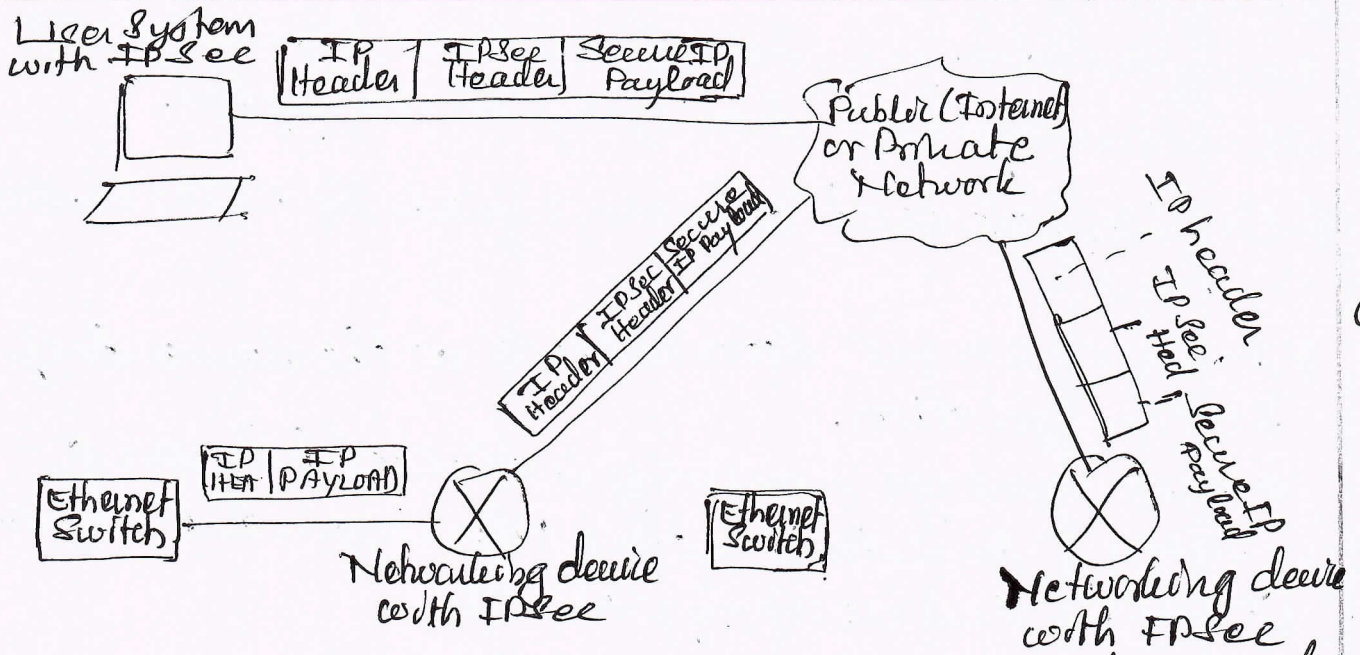
Explanation of above Figure 4

All

(Damodar S.H)

MARKS

5.a) Draw a diagram to illustrate IP Security scenario and also explain benefits of IPSec



04

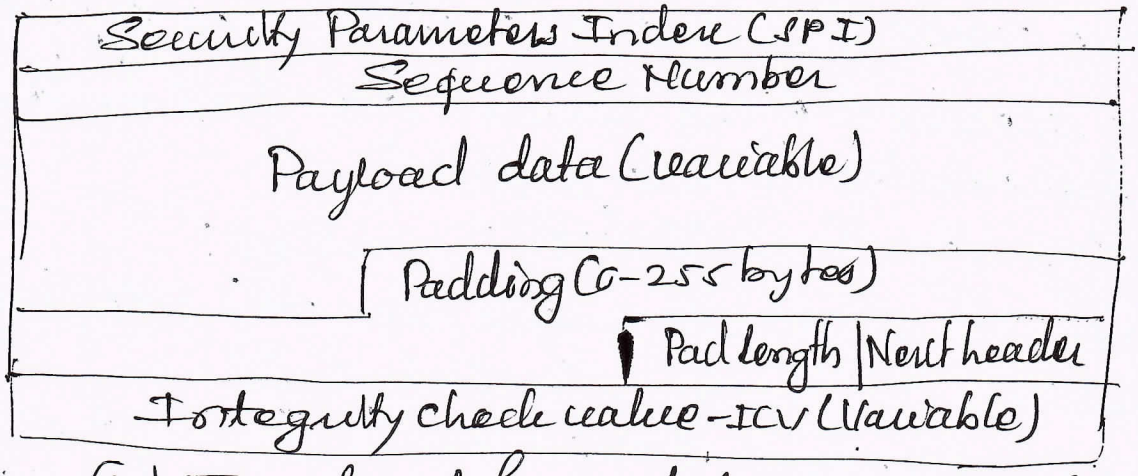
* An organization maintains LANs at dispersed locations. Non secure IP traffic is conducted on each LAN.
* IPSec Protocols operate in networking devices, such as a router or firewall, that connect each LAN to the outside world.
* The IPSec n/w device will typically encrypt and compress all traffic going into the WAN and decrypt and decompress traffic coming from the WAN

> Benefits of IPSec

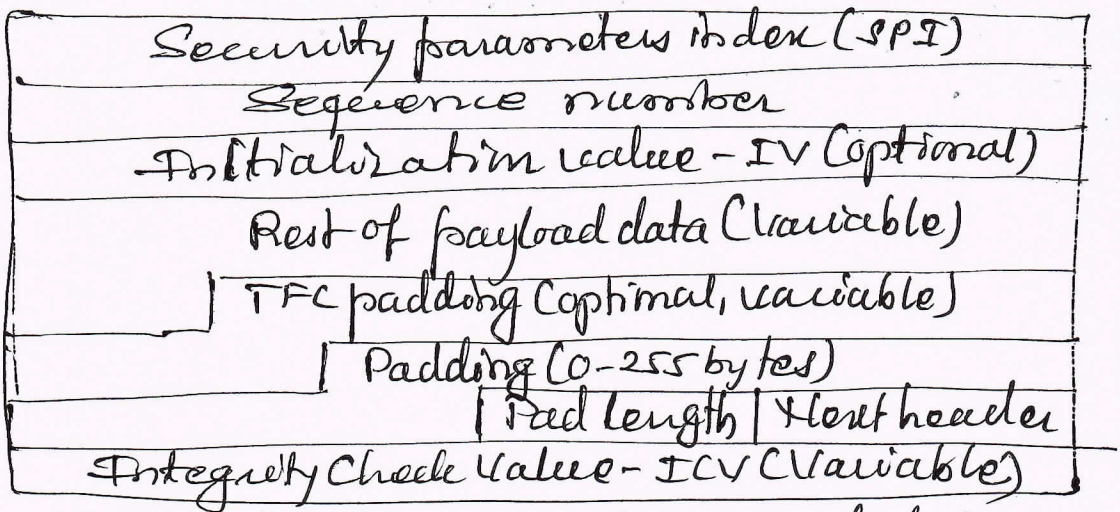
* When implemented in a firewall or router, it provides strong security that can be applied to all traffic crossing the perimeter.
* IPSec in a firewall is resistant to bypass if all traffic from the outside must use IP and the firewall is the only means of entrance from the Internet into the organization.
* IPSec is below the transport layer (TCP, UDP) and so is transparent to all applications

MARKS

5b) With relevant diagram describe various fields in ESP packet format 08



(a) Top-level format of an ESP Packet



(b) Substructure of payload data

ESP Packet Format

* Above figure shows the top-level format of an ESP packet. It contains the following Fields
* Security Parameters Index (32-bits): Identifies a security association
* Sequence Number (32 bits): Monotonically increasing counter value
* Payload data (Variable): This is a transport-level segment or IP packet that is protected by encryption
* Padding (0-255 bytes):

2

2

4

(Damodar S.H)

MARKS

* Pad Length (8-bits): Indicates the number of pad bytes immediately preceding this field.
* Next Header (8-bits): Identifies the type of data contained in the payload data field by identifying the first header in that payload.
* Integrity Check Value (Variable): Contains ICV computed over the ESP packet minus the Authentication Data field.
* Two additional fields may be present in the payload: Figure (6), an Initialization Vector (IV) if one is required by the encryption.

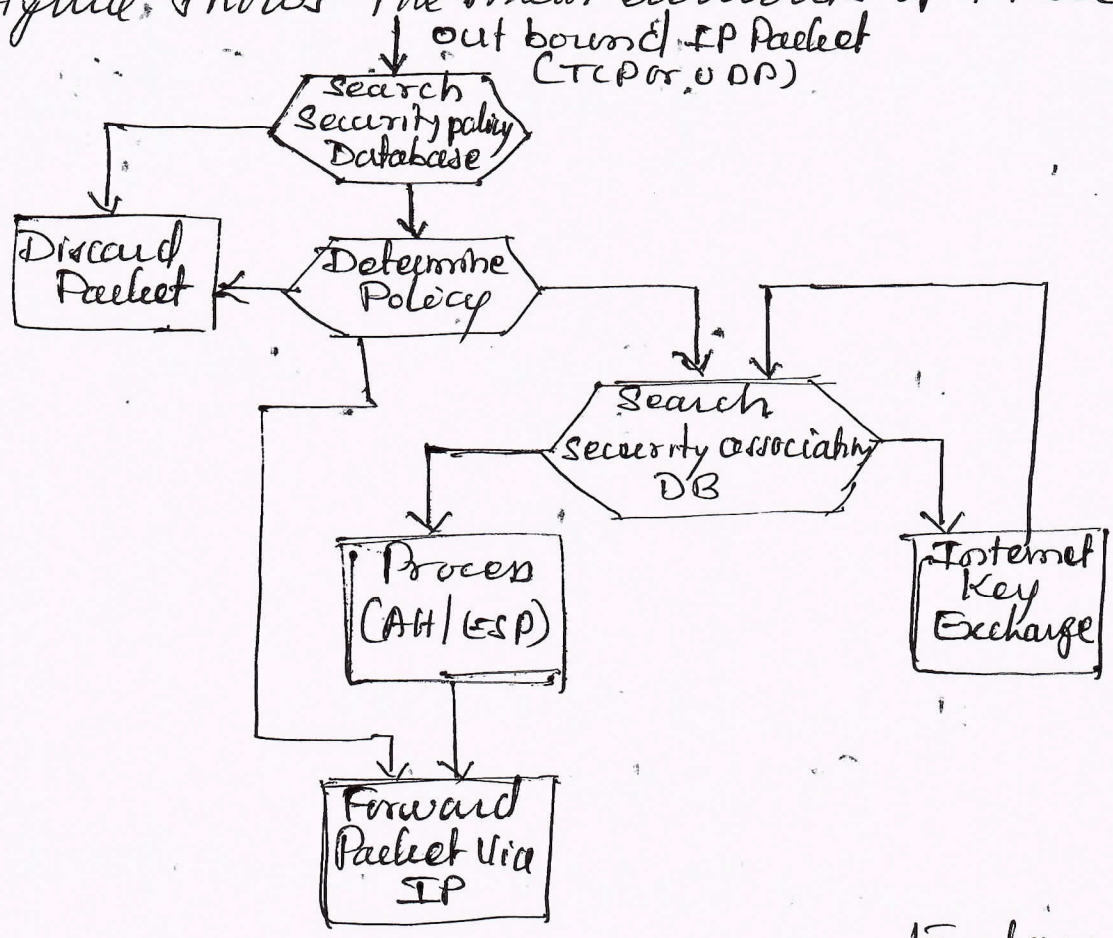
(Dasarodar S.H)

MARK

6a) Draw and explain the IP traffic processing model for inbound and outbound packets 10

⇒ IP sec is executed on a packet-by-packet basis
* Each outbound IP packet is processed by the IPSec layer before transmission and each inbound packet is processed by the IPSec layer after reception and before passing the packet contents on to the next higher layer.

Figure shows the main elements of IPSec.



3

Explanation 3

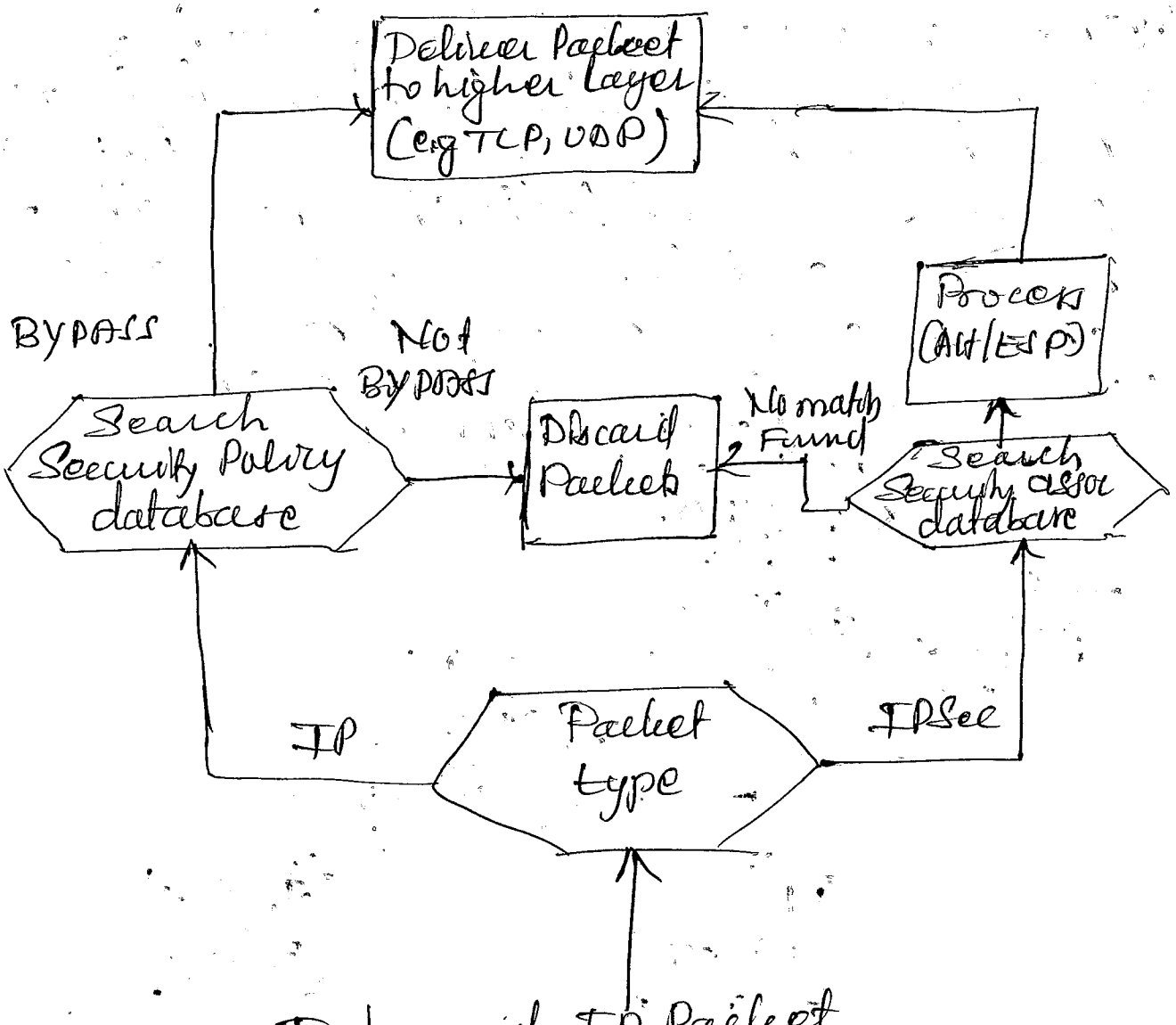
Processing Model for Outbound Packets

⇒ Inbound Packets

Following figure highlights the main elements of IPSec processing for inbound traffic.

(Dassodan S.H)

* An incoming IP Packet triggers the IPSec processing.



Inbound IP Packet (From Internet)

Processing Model for Inbound Packets

Explanation of steps — 3 Mks

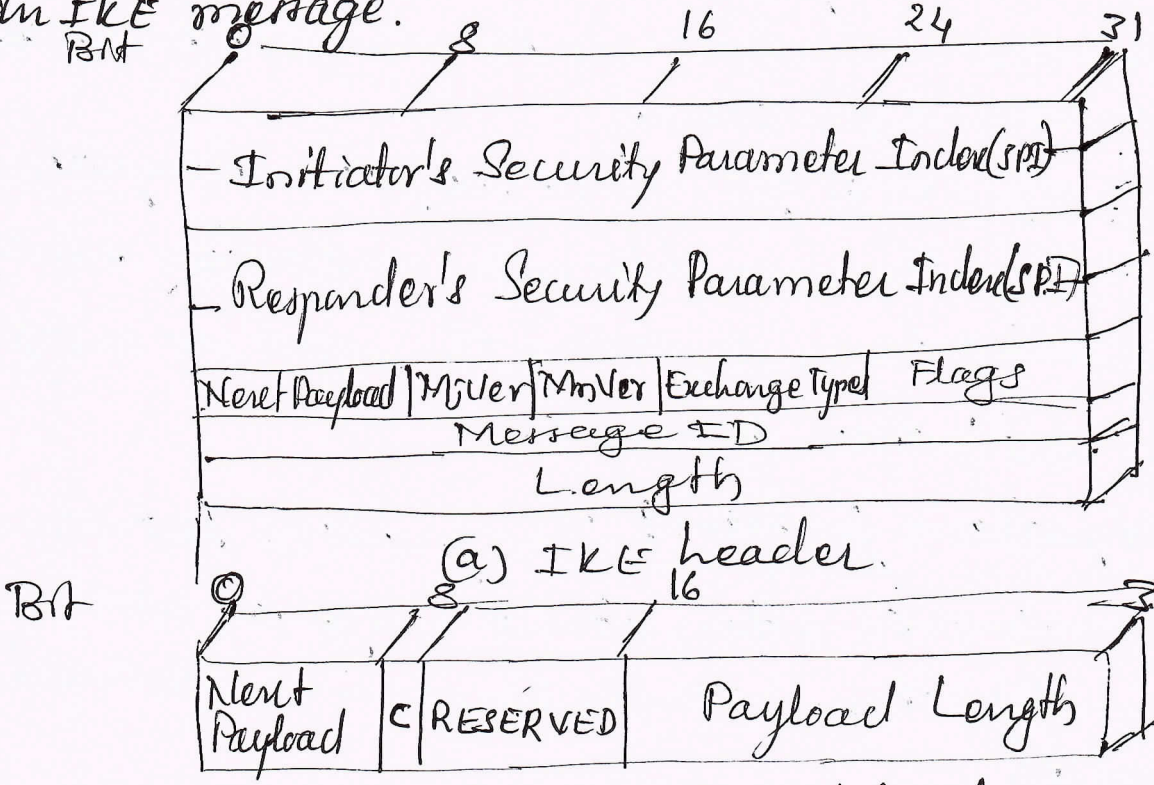
2

(Damodar S.H)

MARKS

6.b) With relevant diagram, describe IKE header and Payload format 06

An IKE message consists of an IKE header followed by one or more payloads
Below given figure shows the header format for an IKE message.



(a) IKE header

(b) Generic Payload header

Figure a consists of the following fields
1) Initiator SPI (64 bits) 2) Responder SPI (64 bits)
3) Next Payload (8-bits) 4) Major Version (4-bits)
5) Minor Version (4-bits) 6) Exchange Type (8-bits)
7) Flag (8-bits) 8) Message ID (32-bits)
9) Length (32-bits)

Explanation of IKE header 2
Explanation of Payload 2

(Damodar S.H)

7a) Mention types of cyber-anti-pattern templates. Explain, the various components of these templates. 10

) The two templates include the micro-Antipattern template and the full cyber Antipattern template

* Micro-Anti Templates

* The micro-Antipattern is a flexible and informal way to present antipatterns.

The components of a micro-Antipattern template are:

1.) Name: The name of the micro-antipattern is usually a pejorative term, suggesting the negative consequences of the antipattern presence. 2

2) Antipattern problem: The problem section summarizes alternative ways to resolve the antipattern design forces with improved benefits.

3) Refactored Solution: The solution section summa - rizes alternative ways to resolve the Antipattern design forces with improved benefits.

* Full cyber Antipattern Template

* The full cyber Antipattern template has two main parts: a header and a body

Header: Gives quick sense of the Antipattern and the solution

Body: This contains the pattern details

* The heading fields of the full cyber antipattern templates are:

(Damodar S.H)

MARKS

* Antipattern Name: A unique descriptive noun phrase
* Also known As: Some known names or analogies - names from different domains.
* Refactored Solution: Alternative solutions
* Unbalanced Primal Forces: Lists the primal design forces that are poorly resolved by this Antipattern
* Anecdotal Evidence: These are some quips that characterize this Antipattern.

4

* The body fields are
  * Background: Provides contextual explanations
  * Antipattern Solution: This field defines the Antipattern solution through diagrams, explanations, examples, and discussion of design forces
* Causes, Symptoms, and Consequences: This bulleted section lists the typical causes, common symptoms and resulting consequences of the Antipattern solution
* Known Exceptions: Identifies desirable antipattern solution
* Refactored Solution and Examples: Defines the Refactored solution. That is an alternative to the Antipattern solution.
* Related Solutions: If there are other potential - solutions to the antipattern, they are identified in this section

4

(Damodar S.D)

MAHE

7.b) Write a brief note on "No time for Security" — antipattern. 06

Antipattern Name: No Time for Security

Also known as: Add Security for Blame Security for Schedule slippage

Refactored Solution Names: Security requirement and real requirements, Cyber Risk Management 2

Unbalanced Primal forces: Management of — confidentiality, integrity and availability

Anecdotal Evidence: "Wait until its time to test the system and then worry about security

* Background: Security is usually the final — consideration in the development of a system. Sometimes security is left out altogether in the rush to get products out the door.

* Antipattern Solution: Developers of software projects and widget developers, often wait until the end of the development lifecycle to address security.

* Causes, Symptoms, and Consequences 2

- Security was never part of the requirements
- Saving on development costs and time - at the expense of security.
- Project is behind schedule
- Shared administrator accounts
- Not teaching the developers to be security aware.

* Known Exceptions & * Refactored Sol'n Examples — 2m
* Related solutions → Explanation of there

(Damodar S.H)

MARK

8 a) Explain the various specialized skills that should be available on-demand in IT security shops. 05

> List of specialized skills that should be available on-demand in IT security shops

* Network Device Specialist: Vendor-certified specialist specialist with deep knowledge for debugging and configuring the network devices
* Operating System Security Specialist: Specialist in configuring and hardning the security of each operating system. 1X5
* Database Security Specialist: Specialist in configuring the security of Specific database =5
* System Forensic Specialist: Specialist in in-depth analysis of systems, creating chains of evidence and other forensic investigation techniques.
* Reverse Engineering Malware Specialist: Security researches who captures malwares and analyses its characteristics.

8 b) What is the significance of signature based malware detection and what are limitations against Polymorphic threats 05

* Current signature-based antivirus engines miss 30 percent to 70 percent of malicious code, and nearly 100 percent of zero day infections, which by definition are unreported exploits
* Malicious signature growth exploding from 5 new ones per day
* The proliferation of malware signatures is exploding primarily due to polymorphic malware

malware techniques. For example, hash functions used by signature-based detectors yield very different values with only slight changes to a malicious file.

* Changing a string literal in the file is sufficient to trigger false negative.
* Other polymorphic techniques including varying character encodings, encryption, and random values in the files

8c) Write a brief note on forces in cyber anti-pattern 06

* The major types of forces in anti-pattern include primal, horizontal, and vertical forces.
* Primal forces are permanent design forces present in almost every design decision
* Horizontal forces are forces that can apply in all domains
* Vertical forces are domain or system specific design forces.
* The Primal design forces in cybersecurity domain include:
  * Management of functionality
  * Management of Confidentiality
  * Management of Integrity
  * Management of availability.

Confidentiality: is the protection of information

The system

Integrity: is protection of the coherence of data and system metadata

Availability: is the readiness of the system to execute its functionality in response to user requests.

9a) Describe the architectural problem solving patterns 08

Architectural Problem Solving Patterns
The key techniques are as follows

* Business Question Analysis:
  * Cater knowledge from enterprise subject matter experts to find out what questions the business management has
  * * Analyze each question to understand which columns are involved to answer the questions and which columns need to be mapped to which others. 1

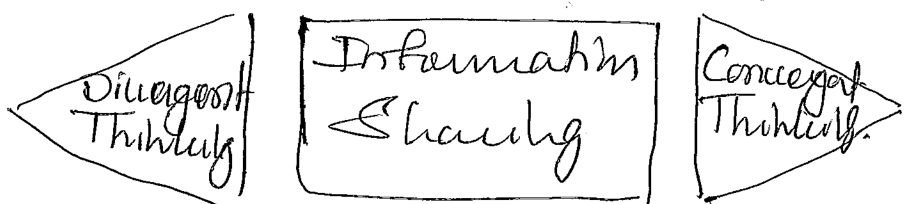
* Document Mining:
  * Obtain as much enterprise documentation as possible. Choose a column and go through each each document finding examples
  * Keep a list of what you found. 1

* Hierarchy Formation
  * Play a cards-on-the wall exercise with small groups and organize each list into a hierarchy possibly inventing some new categories in the middle of the tree 2
  * Redraw this electronically and print it as a readable poster

* Enterprise Workshop:
  * Bring the posters and some binders with the Raw 1 definitions to a workshop with enterprise stakeholders
  * Have the enterprise take ownership of the meeting and walk through each hierarchy to validate the models 2

Matrix Mining

* Carefully review the documents for cross-column relationships, that is, a sentence involving more than one column.
* Keep track of each relationship, including — document, quoted text, and page number
* Then conduct an enterprise workshop to validate the matrices.



Divergent Thinking	Information Sharing	Convergent Thinking
Brain storming	Presentation	Prioritizing
Brain Writing	Read / Write	Voting
Document Mining.	Making Definitions	Decision analysis
Mind Mapping		Hierarchy Formation

2

(Damodar S. H.)

9b) Explain the role of Zachman Framework in cyber-security

* The Zachman Framework, invented by Johan A Zachman is an intellectual tool for describing enterprises
* This framework slices and dices complexity into rows and columns.
* The columns are the six basic questions you could ask about any subject
  * Includes: What? How? where? who? when? why?
  * These are the same questions journalists ask to write newspaper stories — 5
  * When journalist has answered these six questions, he or she can claim to have complete story
* The Zachman Framework further slices and dices complexity into rows, the rows represent a general overview of the human roles
* The hierarchy of every complex enterprise has executives, business management, architects engineers, technicians and users
* Each of these roles can ask the same six basic questions, hence six cells per row
* Each row-column intersection is a cell — to be populated with models and specifications which are representation of the enterprise

Related figure — 3

(Dasudas.H)

10 a) Explain various technology involved included in HBS (Host Based Security)

* Host Based Security (HBS) can be implemented with a combination of location protections and services and enterprise services that manage local-configurations and services

* Antivirus protection: Scans for malicious files
  * Scan can be on demand, scheduled and continuous
  * Antivirus protection recognizes malware through signatures usually by matching the hash function with known malware database

* Anti-Spyware: Searches for suspicious applications that might be collecting data without the user knowledge
  * Spyware applications are often installed covertly
  * Both antivirus and anti-spyware programs either quarantine or remove the malicious file

* Host based Firewall: Determines which ports are open or closed, as well as which applications are allowed to communicate over the network.

* Root kit detection: is a scan that seeks serious malicious system infections, which might evade other defenses by cloaking their activities

for normal observations - for example directory listings.

* Patch management:

  * Ensures that the OS and applications have the latest developer-recommended updates
  * Application patching remedies a major — Vulnerability
  * Microsoft initiated a ritual monthly update — called Patch Tuesday
  * It is the second Tuesday of each month and coincides with patch updates from many — vendors

2

10 b) Why is network administration an essential skill for for hands-on - cyber security professional? 06

* Hands-on knowledge of network administration is an essential prerequisite to becoming an effective cybersecurity professional.
* Network administration includes the entire lifecycle of systems, from hardware installation to all system changes through to decommissioning.
* The first step in network administration are - setting up the hardware and cabling.
* Then second step is to install operating systems and configure system protections, such as - firewalls, antivirus utilities and antispyware tools.
* To complete the building or rebuilding of a new system offline, burn some data e.g. from another system with downloaded patches and applications.

2

2

* System management control enables you to manage users, services, and devices
* Remote administration is an essential capability for managing back-end servers
* Creating multiboot partioned disk enables you to consolidate security tools and applications

— x —