CS6004-CYBER FORENSICS

Question Bank

Unit-I

Network layer Security and Transport Layer security

Part A

1. Distinguish between HMAC and MAC.
2. List out the basic components of the IPSec architecture
3. Identify Security Associations with the help of three Parameters.
4. Give some basic differences between encryption and decryption.
5. What do you know about Key Management for IPSec?
6. Differentiate between SSL Protocol and TSL protocol.
7. Design ISKMP in terms of its header format.
8. Define a Pseudo-Random Function
9. Decide when and under which circumstances “FINISHED MESSAGE” used?
10. Develop the two ways for exchange of the premaster Secret.
11. Show in points the three services for SSL connections between Server and Client.
12. List the elements involved in the session states.
13. Classify using some specifications of SSL related Alerts which are always fatal to be used

Part B

1) i) Explain in detail about IPSec Protocol Documents. (6)
   ii) Explain in detail about HMAC with its Structure and suitable example . (10)

2) Give a brief account of IP ESP with some suitable diagrams. (16)

3) Illustrate briefly about the computation of HMAC using the following methods:-
   (i)HMAC-MD5 computation using the RFC method. (8)
   (ii)HMAC-SHA 1 computation using Alternative method. (8)

4) Analyze how is the Security Association used in the following parameters:-
   (i)Security Policy Database (4)
   (ii)Security Association Database (4)
   (iii)Transport Mode SA (4)
   (iv)Tunnel Mode SA (4)

5) Describe in detail about :-
   (i)Session and Connection State. (8)
   (ii)SSL Record Protocol. (8)

6) Explain in detail about SSL Handshaking Protocol between a Server and Client Connection with an appropriate diagram. (16)

7) Describe TLS Protocol with suitable example. (16)

8) Discuss about Key Management Protocol for IPSec. (16)

9) Describe TLS Protocol with suitable example. (16)

10) Examine a key Generation using Pseudo Random Function to expand secrets into blocks of data in TLS with a suitable example .(16)

Unit-II

E-MAIL SECURITY & FIREWALLS

Part A

1) Define PGP.
2) Define MIME.
3) What is meant by Huffman compression?
4) What is a Shannon–Fano coding?
5) List out the data fields contained in ASCII Armor Format
6) List out the strings contained in header line text.
7) Define an Armor head line.
8) Define Armor headers.
9) Define packet headers.
10) Define Cryptographic Message Syntax (CMS).
11) Define Digest Algorithm Identifier.
12) What is meant by Enveloped-data content type ?
13) Define firewall.
14) What are the three main categories of firewalls?
15) Define Key Encryption Algorithm Identifier.

Part B

1) Explain in detail the basic concepts of

   (i)Confidentiality via. Encryption (8)

   (ii)Authentication via. Digital Signature (8)

2) Formulate the idea behind using the following terms:

   (i)Compression (4)

   (ii)Radix-64 Conversion with an example (12)

3) Briefly explain the types of Firewalls with a neat diagram and examples. (16)

4) Explain in detail about :-

   (i)Role of Firewalls. (8)

   (ii)Firewall Related Terminology (8)

5) Describe the transaction protocols required for secure Payment Processing in SET (16)

6) Explain in detail about S/MIME and the general syntax it uses to support different content types. (16)

7) Explain briefly about the following security mechanisms:-

   (i)Logging and Alarms , VPN (4)

   (ii)DMZ and Choke Point (4)

   (iii) Key material Packets in PGP (8)

8) Demonstrate the SET system Participants with a diagram (16)

Unit-III

INTRODUCTION TO COMPUTER FORENSICS

Part A

1) Define the term "Computer Forensics".
2) What are the roles of a Computer in a Crime?
3) State the objectives of Computer Forensics.
4) Who Can Use Computer Forensic Evidence?
5) Mention some problems with Computer Forensic Evidence.
6) Define Computer Crime and digital crime.
7) What Is Phreaking?
8) State the motivations for computer intrusion or theft of information in contemporary society.
9) List some digital forensics tools.
10) What is CMOS?
11) Give the hierarchy of Contemporary Cybercriminals
12) What methods are available for recovering passwords?
13) What is FIOA?
14) List the tasks of a Computer Forensics Examination Protocol
15) State the types of computer records.

Part B

1) Examine the traditional Computer crimes associated with Cyber Forensics. (16)
2) Explain in detail about Identity Theft and Identity Fraud and mention the Points of differences between them. (16)
3) Explain in detail about Incident Response Methodology and the six steps associated with it (16)
4) Analyze briefly about the Forensic Duplication and Investigation (16)

5) Demonstrate how to use Remote Network Acquisition Tools in cyber Forensics. (16)

6) Discuss in detail about the following:-

   i) Systematic Approach in Computer Investigations. (10)

   ii) Conducting an Investigation in Computer Investigations. (6)

7) Examine the following terms in detail:-

   (i) Understanding Storage Formats for Digital Evidence (8)

   (ii) Using Acquisition Tools. (8)

8) Discuss in detail about the following:-

9) (i) Systematic Approach in Computer Investigations. (10)

   (ii) Conducting an Investigation in Computer Investigations. (6)

Unit-IV

EVIDENCE COLLECTION AND FORENSICS TOOLS

Part A

1. List out the disk drive components.
2. What is meant by ZBR?
3. Define track density.
4. List out the properties handled at the drive's hardware
5. Define Master boot record (MBT).
6. Define FAT.
7. List out the versions of FAT.
8. Define VFAT.
9. Define data runs.
10. What is meant by Encrypting File System (EFS)?
11. What is meant by trusted platform module?
12. List out some of the open-source encryption tools.
13. Define Registry.
14. Define Virtual machine.
15. What is National Software Reference Library (NSRL) project ?
16. What is meant by HAZMAT?
17. What are the functions of evidence custody form?

Part B

1) Illustrate how will the processing of an incident or a crime scene takes place in cyber forensics. (16)
2) Explain in detail about about how the understanding of File Systems plays a crucial role in cyber forensics. (16)

3) Explain in detail about the following :-

(i) Computer Forensics Software Tools (8)

(ii) Computer Forensics Hardware Tools (8)

4) Explain in detail about the following terms:-

(i) Disk Partitions (8)

(ii) Master Boot Record (2)

(iii) Examining FAT disks (6)

5) Describe the following terms in detail:-

(i) Examining NTFS Disks (6)

(ii) NTFS System Files (6)

(iii) NTFS Compressed Files (4)

6) Describe about how the whole disk encryption is performed in Cyber forensics (16)

7) Examine the MS-DOS Startup Tasks and about other Disk Operating Systems in Detail. (16)

8) Describe about the following mechanisms:

(i) Understanding File Systems (8)

(ii) Whole Disk Encryption (8)

Unit-V

ANALYSIS AND VALIDATION

Part A

1) List out the file systems in which FTK can perform forensic analysis.
2) Define scope creep.
3) What is meant by Known File Filters (KFF)?
4) What is meant by auto image checksum verification?
5) What is meant by data hiding?
6) List out some of the disk management tools.
7) What is meant by bit-shifting?
8) Define steganography.
9) List out the Steganalysis methods.
10) What is meant by key escrow?
11) List out some of the password cracking tools.
12) List out the three ways to recover passwords.
13) What is meant by remote acquisition?
14) Define layered network defense network strategy.
15) Define Defense in Depth (DiD) strategy.
16) List out the tools available to capture RAM

Part B

1) Discuss how will you validate the forensic data using:
   (i) Validating the hexadecimal Editors (8)
   (ii) Validating with Computer Forensics Programs (8)
2) Examine in detail the techniques used for Addressing Data Hiding. (16)

3) Describe Remote Acquisitions when used with

   (i) Runtime Software (8)

   (ii) Preparing Disk Explorer and HDHOST (4)

   (iii) Remote Connection with Disk Explorer (4)

4) Explain the following terms in detail:-

   (i) Securing a Network (8)

   (ii) Performing Live Acquisitions (8)

5) Briefly generalize the roles of the following term in investigations:-

   (i) E-mail in investigations (8)

   (ii) E-mail in Client and Server (8)

6) Describe in detail about using specialized E-mail Forensics Tools (16)

7) Describe in detail about Understanding E-mail Servers (16)

8) Assess how mobile devices play a crucial role in forensics by :

9) (i) Basics of mobile Forensics (8)

   (ii) Inside Mobile Devices (4)

   (iii) Inside PDAs (4)