www.firstranker.com

Code No: 07A81903 **R07** **Set No. 2**

IV B.Tech II Semester Examinations,APRIL 2011
INFORMATION SECURITY
Electronics And Computer Engineering

Time: 3 hours **Max Marks: 80**

Answer any FIVE Questions
All Questions carry equal marks

⋆ ⋆ ⋆ ⋆ ⋆

1. (a) What can be the two main attacks on corporate networks?
   (b) Give a detailed description of the two approaches to intrusion detection?[4+12]
2. (a) Define a Security attack. Explain in detail about the various types of attacks an Internetwork is vulnerable to.
   (b) Write about Man-in-the-middle attacks. [10+6]
3. Write about the following terms related to PGP and S/MIME:
   (a) Radix-64
   (b) Session key
   (c) Compression
   (d) Encryption
   (e) Decryption. [16]
4. (a) What action is taken by SSL when a fatal alert is received?
   (b) Discuss in detail the four phases of handshake protocol? [4+12]
5. (a) Explain the use of S-Boxes in AES algorithm.
   (b) Differentiate between DES and AES algorithms.
   (c) Enumerate the various cipher block modes of operation. [5+5+6]
6. (a) Explain in detail Anti-Replay mechanism in AH?
   (b) What is a cookie? How are they used in thwarting clogging attacks in Oakley algorithm? [8+8]
7. (a) What are the requirements for Public-key cryptography? Also enumerate some of the popular applications of Public-key cryptosystems.
   (b) Explain the motivation for Kerberos application, also listing the requirements for the same. [8+8]
8. It was stated that the inclusion of salt in the UNIX password scheme increases the difficulty of guessing by a factor of 4096. But the salt is stored in the plain text in the same entry as the corresponding cipher text password. Therefore, those two characters are known to the attacker and need not be guessed. Why is it asserted that the salt increases security? Wouldnt it by possible to thwart Completely all password crackers by dramatically increasing the salt size to Say, 24 or 48 bits?[16]

⋆ ⋆ ⋆ ⋆ ⋆

FIRSTRANKER

www.firstranker.com

www.firstranker.com

Code No: 07A81903 **R07** **Set No. 4**

IV B.Tech II Semester Examinations,APRIL 2011
INFORMATION SECURITY
Electronics And Computer Engineering

Time: 3 hours **Max Marks: 80**

Answer any FIVE Questions
All Questions carry equal marks

⋆ ⋆ ⋆ ⋆ ⋆

1. (a) With a suitable example show how the Digital Signature provides security. Also highlight the disadvantages of Digital signature.
   (b) Explain the terms used in relation with X.509 certificate:
      i. Version
      ii. Serial number
      iii. Signature algorithm identifier
      iv. Issuer unique identifier
      v. Subject unique identifier
      vi. Signature. [8+8]
2. (a) What is the data base that defines the parameter associated with each SA? What are the parameters defined in the database?
   (b) Explain how encapsulating security payload provides confidentiality services? [8+8]
3. (a) What is a cipher block mode of operation? Explain the use of these modes of operation for the block ciphers for encipherment,
   (b) Describe the different methods of Message authentication. [8+8]
4. (a) Show clearly how Confidentiality is ensured among users of PGP.
   (b) Give an overview of MIME and its functionality. [8+8]
5. (a) What is a Security attack? Give the classification of the Security attacks. Discuss the following terms in detail with relevant examples:
      i. Interruption
      ii. Interception
      iii. Modification
      iv. Fabrication
   (b) Explain UDP hijacking. [10+6]
6. (a) List the design goals for a firewall?
   (b) What are false Positives and false Negatives?
   (c) What are the Properties that a Multilevel Secure System must enforce? [6+4+6]
7. Explain how the following threats to web security can be defended by SSL.

FIRSTRANKER

www.firstranker.com

www.firstranker.com

(a) Known plaintext dictionary attack

(b) Replay attack

(c) Password sniffing

(d) SYN flooding. [16]

8. (a) Draw the figure showing VACM logic and explain?

(b) The encryption scheme used for UNIX passwords is one way; it is not possible to reverse it. Therefore, would it be accurate to say that this is, in fact, a hash code rather than an encryption of the password. [8+8]

⋆ ⋆ ⋆ ⋆ ⋆

FIRSTRANKER

www.firstranker.com

www.firstranker.com

Code No: 07A81903 **R07** **Set No. 1**

IV B.Tech II Semester Examinations,APRIL 2011
INFORMATION SECURITY
Electronics And Computer Engineering

Time: 3 hours **Max Marks: 80**

Answer any FIVE Questions
All Questions carry equal marks

⋆ ⋆ ⋆ ⋆ ⋆

1. (a) What are the business requirements for SET?
   (b) Mention the types of threats on the web? Discuss their consequences and mention the countermeasures? [8+8]
2. (a) What is Radix-64 format? Explain how both PGP and S/MIME perform the Radix-64 conversion is performed.
   (b) Describe the five principal services that Pretty Good Privacy (PGP) provides. [8+8]
3. (a) Make a comparison of transport and tunnel modes?
   (b) Mention the encryption and authentication algorithms used in ESP service? Discuss the purpose of padding in ESP protocol? [8+8]
4. (a) Explain the conventional encryption principles with a neat illustration.
   (b) Differentiate between Message authentication and User authentication. [8+8]
5. (a) Discuss in detail about network management architecture?
   (b) What are the deficiencies of SNMPV1?
   (c) Give a brief note of distributed network management. [8+4+4]
6. (a) Explain what each of the following means used in Kerberos:
      i. Authentication server
      ii. Ticket Granting server
      iii. Kerberos realm
      iv. Kerberos principal.
   (b) Explain the three alternative authentication procedures that X.509 uses across various applications. [8+8]
7. (a) What are two default policies that can be taken in a packet filter if there is no match to any rule? Which is more conservative? Explain with example rule sets both the policies?
   (b) What are the advantages of decomposing a user operation into elementary actions?
   (c) What are false negatives and false positives? [6+6+4]
8. (a) "Gaining control over the Routing tables at layer 3 is one of the attacks" - explain how Route tables modification is crucial.

FIRSTRANKER

www.firstranker.com

www.firstranker.com

(b) Explain how Buffer overflow is created for any known platforms (eg., WINDOWS NT / LINUX). [8+8]

⋆ ⋆ ⋆ ⋆ ⋆

FIRSTRANKER

www.firstranker.com

www.firstranker.com

Code No: 07A81903 **R07** **Set No. 3**

IV B.Tech II Semester Examinations,APRIL 2011
INFORMATION SECURITY
Electronics And Computer Engineering

Time: 3 hours **Max Marks: 80**

Answer any FIVE Questions
All Questions carry equal marks

⋆ ⋆ ⋆ ⋆ ⋆

1. (a) What are the advantages of screened-subnet firewall system?
   (b) Explain the concept of Trusted systems? [6+10]
2. (a) Describe the Internet standards and RFCs.
   (b) Explain how Address Resolution Protocol table becomes a victim for attacks. [8+8]
3. (a) Define Security Association? What parameters define SA?
   (b) Give the formats of IPSec AH and IPSec ESP? [8+8]
4. (a) What is an access policy? On what factors does access determination depends?
   (b) Discuss the two techniques for developing an effective an efficient proactive password checker? [8+8]
5. (a) Explain clearly the reasons why RSA algorithm is the most resorted algorithm for various security applications.
   (b) Explain Key distribution techniques. [8+8]
6. (a) Draw the diagrams showing the relative location of security facilities in TCP/IP protocol stack? Discuss the advantages of each?
   (b) What is SSL session? Can a session be shared among multiple connections? What are the parameters that define a session state? [8+8]
7. Discuss the following in relation with S/MIME:
   (a) RFC 822
   (b) MIME Header fields
   (c) MIME Content types. [5+5+6]
8. (a) Compare AES cipher versus RC4 encryption algorithm.
   (b) Compare and contrast SHA-1 and HMAC functions. [8+8]

⋆ ⋆ ⋆ ⋆ ⋆

FIRSTRANKER

www.firstranker.com