Module Name: PKI & Biometric

Q1. Find the pair of commands which will produce same message digest of a file in Linux machine. ?
a) md4sum , md5sum
b) sha1sum , sha160sum
c) shasum , sha1sum
d) sha160sum , shasum

Q2. Which of the following algorithm used in SSL /TLS Protocol. ?
a) AES &DES both
b) (b)RSA only
c) (c)DES & RSA both
d) (D) AES & RSA both

Q3. How many mixing and mashing rounds will be there in RC2 Algorithm?
a) 18, 2
b) 16, 2
c) 16, 4
d) 2, 15

Q4. How many servers are used in Kerberos for authentication purpose?
a) 4
b) 3
c) 1
d) 2

Q5. Diffie-Hellman algorithm's effectiveness depends on the difficulty of computing?

a) Discrete logarithms
b) Prime factors of composite number
c) Elliptic curve
d) Abelian group

Q6. The total Key Size used in RSA algorithm is.....?
a) 128 bits
b) 256 bits
c) 512 bits
d) 1024 bits

Q7. Which of the following statements are true about OCSP and CRL?
(I) The CRL is a list of subscribers paired with digital certificate status.
(II) The main limitation of CRL is the fact that updates must be frequently downloaded to keep the list current.
(III) The OCSP checks certificate status in real time.
(IV) The CRL allows the authenticity of a certificate to be immediately verified.

a) i only
b) both i and ii
c) i, ii, iv only
d) i, ii, iii only

Q8. To exchange e-mail messages, using PGP a user needs of .....?
a) secret key
b) Public key
c) both (a) & (b)
d) none

Q9. Which of the following protocol is used security and compression services to data generated from the application layer. ?

a) SSL/TLS
b) IPSec
c) PGP
d) none

Q10. What technology is being used to detect anomalies?
a) CVE
b) Sniffing
c) IDS
d) Capturing

Q11. Why would a digital certificate be added to a certificate revocation list (CRL)?
a) If the public key had become compromised
b) If the private key had become compromised
c) The certificate had become public
d) None of the above.
e)

Q12. What does OCSP stand for with respect to digital certificates?
a) Online Certificate Status Protocol
b) Online Certificate Service Provider
c) Open Certificate Systems Project
d) Open Certificates for Security and Privacy

Q13. Which of these is not an encryption algorithm?
a) Diffie hellman
b) AES
c) DES
d) RSA

Q14. In which mode of operation, IPSec protects information delivered from the transport layer to the network layer. ?
a) Transport
b) (b)tunnel
c) (c) both a &b
d) (d) none

Q15. Which of the following provides authentication at IP layer of OSI?
a) AH
b) ESP
c) AH and ESP both
d) SSL

Q16. Which of the following correct about SSL Protocol, it provides
a) message integrity
b) Compression
c) Confidentiality
d) All of the above

Q17. In e-mail system which of one security protocol is used for sending and receiving massage. ?
a) SSL
b) IPSec

c) PGP
d) SSL and PGP both

Q18. Which of the following protocol provides either authentication or encryption, or both, for packets at the IP level?

a) SSL
b) ESP
c) AH
d) PGP

Q19. The combination of key exchange, hash, and encryption algorithms defines a _____ for each SSL session. ?

a) A suite of protocol
b) List of protocol
c) Cipher suite
d) Combination of keys

Q20. Kerberos is an ---------- protocol?

a) Session initiation
b) Authentication
c) Key generation
d) None of the above

Q21. In which way does the Combined Encryption combine symmetric and asymmetric encryption?

a) First, the message is encrypted with symmetric encryption and afterwards it is encrypted asymmetrically together with the key.
b) The secret key is symmetrically transmitted, the message itself asymmetrically.
c) First, the message is encrypted with asymmetric encryption and afterwards it is encrypted symmetrically together with the key
d) The secret key is asymmetrically transmitted, the message itself symmetrically.

Q22. Which is the largest disadvantage of the symmetric Encryption?

a) More complex and therefore more time-consuming calculations
b) Problem of the secure transmission of the Secret Key.
c) Less secure encryption function.
d) Isn't used any more

Q23. Mishra is a certified ethical hacker working in CDAC, one day Mishra finds one employee that appears to be sending very large email to some other marketing company that recently underwent a string of thefts and corporate espionage incidents, even though they should have no reason to be communicating with them. Tracks down the actual emails sent and upon opening them, only finds picture files attached to them. These files seem perfectly harmless, usually containing some kind of joke. Mishra decides to use some special software to further examine the pictures and finds that each one had hidden text that was stored in each picture

What technique was used by the CDAC employee to send information to the rival marketing company?

a) The CDAC employee used cryptography to hide the information in the emails sent
b) The method used by the employee to hide the information was logical watermarking
c) The employee used steganography to hide information in the picture attachments
d) By using the pictures to hide information, the employee utilized picture fuzzing

Q24. Mayank work for CDAC as a Sales Manager. The company has tight network security restrictions. Mayank is trying to steal data from the company's Sales database (Sales.xls) and transfer them to his home computer. Mayank's company filters and monitors traffic that leaves from the internal network to the Internet.
How will Mayank achieve this without raising suspicion?

a) Encrypt the Sales.xls using PGP and e-mail it to your personal gmail account
b) You can conceal the Sales.xls database in another file like photo.jpg or other files and send it out in an innocent looking email or file transfer using Steganography techniques.
c) Package the Sales.xls using Trojan wrappers and telnet them back your home computer
d) Change the extension of Sales.xls to sales.txt and upload them as attachment to your hotmail account

Q25. SSL has been seen as the solution to a lot of common security problems. Administrator will often time make use of SSL to encrypt communications from points A to point B. Why do you think this could be a bad idea if there is an Intrusion Detection System deployed to monitor the traffic between point A and B?

a) SSL is redundant if you already have IDS's in place
b) SSL will trigger rules at regular interval and force the administrator to turn them off
c) SSL will slow down the IDS while it is breaking the encryption to see the packet content
d) SSL will blind the content of the packet and Intrusion Detection Systems will not be able to detect them

Q26. _____ is a type of symmetric-key encryption algorithm that transforms a fixed-length block of plaintext

(unencrypted text) data into a block of cipher text (encrypted text) data of the same length.

a) Stream Cipher
b) Hash Cipher
c) Block Cipher
d) Bit Cipher

Q27. One of the most common and the best way of cracking RSA encryption is to begin to derive the two prime numbers, which are used in the RSA PKI mathematical process. If the two numbers p and q are discovered through a _____ process, then the private key can be derived.

a) Factorization
b) Brute-forcing
c) Prime Detection
d) Hashing

Q28. In SSL, in which of the following choices does authentication happen through the Exchange of certificates?

a) Server
b) Client
c) Both A and B
d) Neither A nor B

Q29. Which component of a firewall provides filtering based on the IP addresses and types of connections (transport layer) information stored in the packet?
a) Packet filtering
b) Application proxies
c) Circuit level gateways
d) Virtual private networking

Q30. The _____ attack can endanger the security of the Diffie-Hellman method if two parties are not authenticated to each other.
a) man-in-the-middle
b) cipher text attack
c) plaintext attack
d) Ping flood

Q31. A digital signature implementation needs a_____ system.
a. symmetric-key
b. asymmetric-key
c. (a) or (b)
d. Both (a) and (b)

Q32. Using public-key cryptography, suppose Raghav wants to send a message to Neelima, and Neelima wants to be sure that the message was indeed sent by Raghav only. Then Raghav should (choose the appropriate scenario)
a) Encrypt the message with Neelima's private key and send the encrypted message to Neelima.
b) Encrypt the message with Neelima's public key and send Neelima the message.
c) Encrypt the message with his public key and send Neelima the message.
d) Encrypt the message with his private key and send the encrypted message to Neelima.

Q33. When you receive a public key that has been signed by a number of individuals, that key is part of ...?
a) The web of trust.
b) a certificate authority
c) a digital fingerprint.
d) an illegal scam

Q34. An organization known as _____ sends out information about known security holes in software
a) RSA
b) PKI
c) CERT
d) PGP

Q35. A firewall is .....?
a) An established network performance reference point.
b) Software or hardware used to isolate a private network from a public network.
c) A virus that infects macros.
d) A predefined encryption key used to encrypt and decrypt data transmissions

Q36. Firewalls operate by .....?
a) The pre-purchase phase.
b) Isolating Intranet from Extranet.
c) Screening packets to/from the Network and provide controllable filtering of network traffic.
d) None of the above.

Q37. Mechanism to protect private networks from outside attack is
a) Firewall
b) Antivirus
c) Digital signature
d) Formatting

Q38. A protocol developed by Netscape which handles data encryption in a transparent manner within the Web browser is called....
a) Netscape Navigator.
b) Secure socket layer.
c) IPSec.
d) VeriSign.

Q39. What is the port number of SSL Protocol?
a) 433
b) 469
c) 443
d) 25

Q40. PKCS stand for ...?
a) Private-Key Cryptography Standard
b) Public-Key Cryptography Standard
c) Public-Key Cryptography Scheme
d) Both (a) and (b)