Center for Development of Advanced Computing, *ACTechS*
(Dept. of IT, Ministry of Communications & Information Technology, Govt. of India)
B-30, Sector-62, NOIDA – 201301

Date : *29/01/08* *Maximum Marks : 50*
Maximum Time: 1 HR

1) A SYN flood is an example of what type of attack
   a) malicious code **b) denial of service**
   c) man in the middle d) spoofing

2) In what type of attack does an attacker resend the series of commands and codes used in a financial transaction in order to cause the transaction to be conducted multiple times
   a) spoofing **b) replay**
   c) man in the middle d) backdoor

3) The trick in both spoofing and TCP/IP hijacking is in trying to
   a) provide the correct authentication token
   b) finding two systems between which a trusted relationship exists
   c) guessing a password or brute forcing a password to gain initial access to the system or network
   d) maintaining the correct sequence numbers for the response packets

4) The trick in both spoofing and TCP/IP hijacking is in trying to the
   a) provide the correct authentication token
   b) finding two systems between which a trusted relationship exists
   c) guessing a password or brute forcing a password to gain initial access to the system or network
   d) maintaining the correct sequence numbers for the response packets

5) 128 bit encryption schemes are generally considered better than schemes that employ keys of 40 bits because
   a) The large number of possible keys in a 128 bit scheme makes it harder to attack
   b) 128 bit encryption encrypts more bits at one time and thus is faster
   c) keys should be a power of two to facilitate quicker encryption
   d) it would not be considered better. A 40 bit key would be better because it would have fewer possible weak keys.

6) The best way to minimize possible avenues of attack for your system is to
   a) Install a firewall an check the logs daily
   b) Monitor your intrusion detection system for possible attacks

c) **Limit the information that can be obtained on your organization and the services that are run by your internet visible systems**
d) Ensure that all patches have been applied for the services that are offered by your system.

7) A firewall can be classified as an example of
a) An ID based access control
b) A directory based access control
c) A rule based access control
d) A lattice based access control

8) IP sec provides which options as security services
a) ESP and AH
b) ESP and AP
c) EA and AP
d) EA and AH

9) What symmetric encryption protocols does S/MIME support
a) AES and RC4
b) IDEA and 3DES
c) 3DES AND RC2
d) RC4 and IDEA

10) Why do PGP and S/MIME need public key cryptography
a) Public keys are always necessary to determine if the e mail is encrypted
b) The public key is necessary to encrypt the symmetric key
c) The public key unlocks the password to the e mail
d) The public key is useless an just gives a false sense of privacy

11) SNMP is protocol used for which of the following functions
a) Secure e mail
b) Secure encryption of network packets
c) Remote access to user workstations
d) Remote access to network infrastructure

12) The purpose of a DMZ in a network is to
a) Provide easy connections to the internet without a interfering firewall
b) Allow server farms to be divided into similar functioning entities
c) Provide a place to lure and capture hackers
d) Act as a buffer between untrusted and trusted networks

13) SMTP is as protocol used for which of the following functions

a) E mail
b) Secure encryption of network places
c) Remote access to user work stations
d) None of the above

14) Which of the following is not a capability of the network based IDS

a) Can detect denial of service
b) Can decrypt and read encrypted traffic
c) Can decode UDP and TCP packets
d) Can be tuned to a particular network environment

15) An active IDS can

a) Respond to attacks with TCP resets
b) Monitor for malicious activity
c) A and B
d) None of the above

16) Honeypots are used to

a) Research behaviour of attackers
b) Collect evidence for prosecution
c) Process alarms from other IDSs
d) Attract customers to e commerce sites

17) Incident response

a) Usually involves a response plan
b) Is a reaction to a security incident
c) May involve law enforcement
d) All of the above

18) Buffer overflow attacks are best defeated by

a) Removing sample files
b) Selecting strong passwords
c) Setting appropriate permissions on files
d) Installing the latest patches

19) TCP wrappers

a) Verify checksums on every packet entering or leaving the system
b) Help prioritize netwok traffic for optimal throughput
c) Help restrict access to the local system
d) None of the above

20) Why is integrity important to cryptographic messages

a) To ensure that the message is properly formatted for decryption
b) To protect the keys from exposure
c) To show that the message has not been edited in transit
d) To show that no one has read the message

21) What is AES meant to replace

a) IDEA
b) DES
c) Diffie hellman
d) MD5

22) What does a hash function do

a) Creates a secure tunnel
b) Breaks encryption by trying every possible key
c) Multiplies two very large primes
d) Creates a unique digest of a message

23) How many bits are in a block of the SHA algorithm

a) 128
b) 64
c) 512
d) 1024

24) what kinds of encryption does a digital signature use

a) hashing and asymmetric
b) Asymmetric and symmetric
c) Hashing and symmetric
d) All the above

25) What is a brute force attack

a) Feeding certain plain text into the algorithm to deduce the key
b) Capturing cipher text with known plain text values to deduce the key
c) Sending every key value at the algorithm to find the key
d) Sending two large men to the key owners house to retrieve the key

26) What is the purpose of the digital certificate

a) It binds a CA to a users identity
b) It binds a CAs identity to the correct RA
c) It binds an individual to an RA
d) It binds an individual to a public key

27) Which of the following properly describes what a public key infrastructure(PKI) actually is

   a) A protocol written to work with a large subset of algorithms applications and protocols
   b) An algorithm that creates public private key pairs
   c) A framework that outlines specific technologies and algorithms that must be used
   d) A frame work that does not specify any technologies but provides a foundation for confidentiality integrity and availability services

28) Which of the following is a secure e mail standard

   a) POP3
   b) IMAP
   c) S/MIME
   d) SMTP

29) Policies are

   a) High level statements made by management
   b) Statements that lay out the organization position on some issue
   c) Mandatory but not specific in their details
   d) All of the above

30) What is the term for the principle employed by an organization to ensure that no single individual has the ability to conduct transaction alone

   a) Need to know
   b) Due care/ diligence
   c) Separation of duties
   d) No lone zone processing

31) Firewall should be situated

   a) Inside a corporate network
   b) Outside a corporate network
   c) Between corporate and outside network
   d) None of the above

32) Firewall is a specialized form of

   a) bridge
   b) disk
   c) printer
   d) router

33) application gateways are -----------packet filters

a) less secure than
b) more secure than
c) equal secure to
d) slower

34) SSL works between------------ and ----------------

a) Web browser , web server
b) Web browser, application server
c) Web server , application server
d) Application server, database server

35) Main purpose of SET is related to

a) Secure communication between browser and server
b) Digital signatures
c) Message digest
d) Secure credit card payments on the internet

Q) Explain the follwing:

1) Stegnography
2) Digital signature
3) Biometric authentication
4) TCP/IP
5) Sniffing and spoofing

Q) explain the diffie-hell man algorithm ?