BRAINWARE UNIVERSITY

Term End Examination 2021 - 22
Programme – Bachelor of Technology in Computer Science & Engineering
Course Name – Modelling Internet Attack
Course Code - PEC801B
(Semester VIII)

Time allotted : 1 Hrs.25 Min. **Full Marks : 70**

[The figure in the margin indicates full marks.]

Group-A

(Multiple Choice Type Question) 1 x 70=70

Choose the correct alternative from the following :

(1) The content of the message is modified
a) In active attack b) In passive attack
c) Both of them d) None of them

(2) What are the different method of attacking system
a) Social engineering b) Trojan horses
c) Viruses d) All of them

(3) DoS stands for
a) Denial of service b) Demand of service
c) Demand of server d) Damage of server

(4) How do we ensure data confidentiality
a) Message digest b) Hashing
c) Encryption and decryption d) None

(5) When one entity pretends to be a different entity, then it is called
a) Repudiation b) Replay
c) Masquerade d) None

(6) Which of the following is an example of passive online attack?
a) Phishing b) Social Engineering
c) Spamming d) Wire sniffing

(7) Which of the following is not an example of offline password attack?
a) Dictionary attack b) Rainbow attacks
c) Spamming attack d) Brute force attack

(8) Which of the following is not possible through hash value?
a) Digital Signatures b) Data retrieval in its original form
c) Password Check d) Data Integrity check

(9) "The Hash Function takes an input of arbitrary length and converts it into a fixed length output." the output of the hash function is known as

a) Hash value
b) Hash Code
c) Message Digest
d) All of the above

(10) Hashing is used in ___ and have variable levels of complexity and difficulty.

a) Cryptography
b) System approach
c) Cyber safe
d) None of the mentioned above

(11) What is the purpose of a Denial of Service attack?

a) Exploit a weakness in the TCP/IP stack
b) To execute a Trojan on a system
c) To shutdown services by turning them off
d) To overload a system so it is no longer operational

(12) Which is passive attack

a) Masquerade
b) Modification of messages
c) Repudiation
d) The release of message content

(13) In modification of message attack

a) Integrity is lost
b) Confidentiality is lost
c) Both of the above
d) None

(14) Types of attacks against systems

a) Reading data
b) Changing data
c) Denial of service
d) All of the above

(15) Any security service has following components

a) Message
b) Sender
c) Intended receiver
d) All of the above

(16) The codified language can be termed as

a) Clear text
b) Unclear text
c) Cipher text
d) Code text

(17) which of the following is message digest algorithm

a) AES
b) DES
c) MD5
d) None

(18) What is the sequence of a TCP connection?

a) SYN-ACK-FIN
b) SYN-SYN ACK-ACK
c) SYN-ACK
d) SYN-SYN-ACK

(19) A virus code consist of

a) Replicator
b) Concealer
c) Payload
d) All of the above

(20) SQL injection is an attack in which _____ code is inserted into strings that are later passed to an instance of SQL Server.

a) Malicious
b) Redundant
c) Clean
d) Non malicious

(21) _____ is time based SQL injection attack.

a) Quick detection
b) Initial Exploitation
c) Blind SQL Injection
d) Inline Comments

(22) At which of the following stage does SQL Injection occurs?

a) When the user is asked to logout
b) When the user is asked to input password
c) When the user is asked to input captcha
d) When the user is asked to input username

(23) XSS can be prevented by:

a) Input Validation
b) Input Sanitization
c) Escaping
d) All of the above

(24) What is the role of Key Distribution Center?

a) It is used to distribute keys to everyone in world
b) It intended to reduce the risks inherent in exchanging keys
c) All of the mentioned
d) None of the mentioned

(25) Which of the following is a type of independent malicious program that never required any host program?

a) Trojan Horse
b) Worm
c) Trap Door
d) Virus

(26) Which of the following attacks is/are likely to result in identity theft?

a) Phishing attack
b) Denial of service attack
c) Dictionary attack.
d) Virus infection

(27) Which header file contains the function rand() in C language

a) stdlib
b) iostream
c) stdio
d) time

(28) Kerberos is a

a) Network Setup protocol
b) Error detection protocol
c) Network authentication protocol
d) Error correction protocol

(29) What is the return type of the rand() function

a) float
b) int
c) double
d) char

(30) PRNG stands for

a) Personal Random Number Generator
b) Pseudo Random Number Generator
c) Primitive Random Number Generator
d) Private Random Number Generator

(31) MAC stants for

a) Message Addressing Code
b) Message Authentication Code
c) Method Authentication Code
d) None

(32) A virus that can cause multiple infections is know as what type of virus?

a) Multipartite
b) Stealth
c) Camouflage
d) Multi-infection

(33) MAC is

a) one to one mapping
b) many to one mapping
c) onto mapping
d) None

(34) PRNGs take in a input which is reffered to as

a) Bit stream
b) Entropy source
c) External varial
d) seed

(35) Full form of TCP

a) Transistor Control Protocal
b) Transmission Control Protocal
c) Technical Control Protocal
d) None

(36) For 150 bit message and 10 bit MAC,how many values are the MAC value dependent on

a) 2^140
b) 2^150
c) 2^10
d) 2^15

(37) What type of virus modifies itself to avoid detection?

a) Stealth virus
b) Polymorphic virus
c) Multipartite virus
d) Armored virus

(38) Which of the following will generate random numbers in the range 1-100 (both inclusive)

a) rand() % 100
b) rand() % 101
c) (rand() % (101)) + 1
d) (rand() % (100)) + 1

(39) A .....is an extension of an enterprise's private intranet across a public Network such as t he Internet across a public Network such as the Internet, creating a secure private connection.

a) VNP
b) VPN
c) VSN
d) VSPN

(40) In..... Mode, the authentication header is inserted immediately after the IP header.

a) Tunnel
b) Transport
c) Authentication
d) Both A and B

(41) Transport layer protocols deals with _____

a) application to application communication
b) process to process communication
c) node to node communication
d) man to man communication

(42) Which of the following protocols is the connection-less protocol?

a) UDP
b) TCP
c) IP
d) All of the these

(43) The value of acknowledgement field in a segment defines _____

a) sequence number of the byte received previously
b) total number of bytes to receive
c) sequence number of the next byte to be received
d) sequence of zeros and ones

(44) The connection establishment in TCP is called

a) 2 way handshaking
b) 2 way data transfer
c) 3 way data transfer
d) 3 way handshaking

(45) What is a wrapper?

a) A Trojaned system
b) A program used to combine a Trojan and legitima te software into a single executable
c) A program used to combine a Trojan and a backd oor into a single executable
d) A way of accessing a Trojaned system

(46) How do you distinguish between a virus and a worm?

a) A virus can infect the boot sector but a worm can not.
b) A worm spreads by itself but a virus must attach t o an e-mail.
c) A worm spreads by itself but a virus must attach t o another program.
d) A virus is written in C++ but a worm is written in shell code.

(47) The persist timer is used inTCP to

a) To detect crashes from the other end of the connec tion
b) to enable retransmission
c) To avoid deadlock condition
d) To time out FIN_WAIT1 condition

(48) What is the difference between a backdoor and a Trojan?

a) A Trojan usually provides a backdoor for a hacke r.
b) A backdoor must be installed first.
c) A Trojan is not a way to access a system.
d) A backdoor is provided only through a virus, not t hrough a Trojan.

(49) What is the purpose of using function srand()

a) to generate the rando m number
b) to enable rand()
c) to set the seed of the rand() funtion
d) to improve efficiency of rand() function

(50) Which of the following usually observe each activity on the internet of the victim, gather all info rmation in the background, and send it to someone else?

a) Malware
b) Spyware

c) Adware
d) All of the above

(51) Which one of the following refers to the technique used for verifying the integrity of the messag e?

a) Digital signature
b) Decryption algorithm
c) Protocol
d) Message Digest

(52) Which type of the following malware does not replicate or clone them self's through infection?

a) Rootkits
b) Trojans
c) Worms
d) Viruses

(53) DNS translates a Domain name into _____

a) Hex
b) Binary
c) IP
d) URL

(54) Which of the following known as the oldest phone hacking techniques used by hackers to make f ree calls?

a) Phreaking
b) Phishing
c) Cracking
d) Spraining

(55) A spoofing attack is

a) a prepared application that takes advantage of a k nown weakness.
b) a tool used to quickly check computers on a netw ork for known weaknesses.
c) an application that captures TCP/IP data packets, which can maliciously be used to capture passwor ds and other data while it is in transit either within the computer or over the network.
d) a situation in which one person or program succes sfully masquerades as another by falsifying data a nd thereby gaining illegitimate access.

(56) Which of the following is not a threat to web application

a) Session poisioning
b) Cookie snoofing
c) Cryptograpic interception
d) Phihing

(57) Which of the following protocol is not susceptible to sniffing

a) HTTP
b) TCP
c) SMTP
d) POP

(58) The handshake protocol and data exchange protocol are part of

a) CA
b) KDC
c) TLS
d) SSH

(59) When a DNS server accepts and uses incorrect information from a host that has no authority givi ng that information, then it is called _____

a) DNS lookup
b) DNS hijacking
c) DNS spoofing
d) DNS authorizing

(60) Which mode of IPsec should you use to assure the security and confidentiality of data within the same LAN?

a) AH transport mode
b) ESP transport mode
c) ESP tunnel mode
d) AH tunnel mode

(61) IPsec defines two protocols: and ?

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

(62) IPSec in the _____ mode does not protect the IP header.

a) transport
b) tunnel
c) either (a) or (b)
d) neither (a) nor (b)

(63) ESP provides

a) Source Authentication
b) Data Integrity

c) Privacy
d) All of the above

(64) Which two types of encryption protocols can be used to secure the authentication of computers u sing IPsec?

a) Kerberos V5
b) SHA
c) MD5
d) Both SHA and MD5

(65) _____ is a form of denial of service attack in which a hostile client repeatedly sends SYN p ackets to every port on the server using fake IP addresses

a) Cyber Crime
b) Memory Shaving
c) SYN flooding
d) Software Piracy

(66) Which 2 protocols are used in the Transport layer of the TCP/IP model?

a) UDP and HTTP
b) TCP and UDP
c) HTTP and TCP
d) ICMP and HTTP

(67) Define Non-Repudiation

a) It means that sender and receiver expect privacy
b) It means that the data received at the receiver is e xactly same as sent.
c) It means that a sender must not be able to deny se nding a message that he sent
d) It means that the receiver is ensured that the mess age is coming from the intended sender, not an im poster.

(68) Kerboros consists of__

a) Authorization Server
b) Client Server
c) Authentication server
d) Mail server

(69) Session hijacking can be thwarted with which of the following?

a) SSH
b) FTP
c) Authentication
d) Sniffing

(70) A man-in-the-middle attack is an attack where the attacking party does which of the following?

a) Infect the client system
b) Insert themselves into an active session
c) Insert themselves into a web application
d) Infect the server system