BRAINWARE UNIVERSITY

Term End Examination 2020 - 21

Programme – Master of Technology in Computer Science & Engineering

Course Name – Network Security

Course Code - PEC-MCS302C

Semester / Year - Semester III

Time allotted : 75 Minutes | Full Marks : 60

[The figure in the margin indicates full marks. Candidates are required to give their answers in their own words as far as practicable.]

Group-A

(Multiple Choice Type Question) 1 x 60=60

1. *(Answer any Sixty)*

(i) Which of the following is a form of DoS attack?

a) vulnerability attack
b) bandwidth flooding
c) connection flooding
d) all of these

(ii) Rail fence technique is an example of

a) substitution
b) transposition
c) product cipher
d) caesar cipher

(iii) 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 overload a system so it is no longer operational
d) to shut down services by turning them off

(iv) Which of them is not a wireless attack?

a) eavesdropping
b) MAC spoofing
c) wireless hijacking
d) phishing

(v) Confidentiality with asymmetric key cryptosystem has its own

a) entities
b) problems
c) data
d) translator

(vi) Encryption and decryption provide secrecy or confidentiality but not

a) authentication
b) integrity
c) privacy
d) all of these

(vii) When the data must arrive at the receiver exactly as they were sent, it's called

a) message confidentiality
b) message integrity
c) message splashing
d) message sending

(viii) The message must be encrypted at sender site and decrypted at

a) sender site
b) receiver site
c) both site
d) conference site

(ix) Input message in cryptography is called

a) plain text
b) cipher text
c) plain and cipher
d) none of these

(x) Which is not an objective of network security?

a) identification
b) authentication
c) access control
d) lock

(xi) Security features that control that can access resources in the OS.

a) identification
b) validation
c) authentication
d) access control

(xii) The protocol designed to make the security of wireless LAN as good as that of wired LAN.

a) WTLS
b) WEP
c) RSN
d) WP

(xiii) In cryptography, the order of the letters in a message is rearranged by

_____

a) transpositional ciphers

b) substitution ciphers

c) block cipher

d) quadratic ciphers

(xiv) SHA-1 has a message digest of

a) 160 bit

b) 620 bits

c) 512 bits

d) 860 bits

(xv) In message confidentiality the transmitted message must make sense to only intended

a) receiver

b) sender

c) translator

d) modulor

(xvi) A digital signature needs a

a) private key system

b) shared key system

c) private and public both key system

d) public key system

(xvii) RSA stands for:

a) Rivest Shamir and Adleman

b) Rock Shane and Amozen

c) Rivest Shane and Amozen

d) Rock Shamir and Adleman

(xviii) Which layer filter the proxy firewall:

a) application layer

b) transport layer

c) network layer

d) none of these

(xix) The protocol used to provide security to emails

a) POP

b) PGP

c) SNMP

d) HTTP

(xx) What is the number of operation required to come up with 2 messages having the same message digest in SHA-512?

a) 2^{256}

b) 2^{512}

c) 2^{1024}

d) 2^{128}

(xxi) Some characteristics of MD5 are

a) check summing a message

b) detecting if a file's contents have changed

c) splitting strings or files into dispersed sets

d) all of these

(xxii) Kerberos is an authentication scheme that can used to implement

a) public key cryptography

b) digital signature

c) hash function

d) none of these

(xxiii) PGP offers _____ block ciphers for message encryption

a) CAST

b) IDEA

c) Triple-DES

d) all of these

(xxiv) Which algorithm is used for public key encryption?

a) RSA

b) Diffie-Hellman

c) RSA and Diffie- Hellman

d) none of these

(xxv) For each _____ the kerberos key distribution center (KDC) maintains a database of the realm's principal and the principal's associated "secret keys".

a) key

b) realm

c) document

d) none of these

(xxvi) For a client-server authentication, the client requests from the KDC a _____ for access to a specific asset.

a) ticket
b) local
c) token
d) user

(xxvii) Which of the following is not a secure shell protocol?

a) transport layer protocol
b) secure layer protocol
c) connection protocol
d) user authentication protocol

(xxviii) Which one of the following does not undergo the encryption procedure?

a) pdl
b) pktl
c) seq#
d) padding

(xxix) Which port forwarding technique intercepts application-level traffic and redirects it from an insecure TCP connections to secure SSH tunnels?

a) local forwarding
b) remote forwarding
c) stable forwarding
d) none of the mentioned

(xxx) "When an attacker is able to eavesdrop on network traffic and identify the MAC address of a computer with network previleges." Which type of wireless network threat would you classify this under?

a) identity theft
b) man in the middle attack
c) network injection
d) accidental association

(xxxi) Pretty good privacy (PGP) uses which PRNG?

a) ANSI X9.82
b) RFC 4086
c) NIST SP 800-90
d) ANSI X9.17

(xxxii) Which of the following statements are true? i) Stream ciphers are fasters than block ciphers ii) Block ciphers can reuse keys iii) Block ciphers use lesser code than stream ciphers

a) i and ii
b) i only
c) ii and iii
d) all are true

(xxxiii) Consider knapsack that weighs 23 that has been made from the weights of the super increasing series {1, 2, 4, 9, 20, and 38}. Find the 'n'.

a) 011111
b) 010011
c) 010111
d) 010010

(xxxiv) In tunnel mode, IPSec protects the _____

a) entire IP packet
b) IP header
c) IP payload
d) IP trailer

(xxxv) The _____ mode of IPsec, take the whole IP packet to form secure communication between two gateways

a) transport
b) tunnel
c) either transport or tunnel
d) both transport and tunnel

(xxxvi) Which layer of the network does an IPsec VPN operate on?

a) layer 3
b) layer 4
c) layer 4 through 7
d) none of these

(xxxvii) Which of the following pieces of information can be found in the IP header?

a) source address of the IP packet
b) destination address for the IP packet
c) sequence number of the IP packet
d) both source address of the IP packet and destination address for the IP packet only

(xxxviii) We also don't want our undeliverable packets to hop around forever. What feature/flag limits the life of an IP packet on the network?

a) time to live counter
b) subnet mask
c) header checksum
d) wackamole field

(xxxix) WPA2 is used for security in _____

a) ethernet
b) bluetooth
c) wi-fi
d) email

(xl) What type of attack uses a fraudulent server with a relay address?

a) NTLM
b) MITM
c) NetBIOS
d) SMB

(xli) Which of the following is NOT an example of a smart card?

a) a credit card which can be used to operate a mobile phone
b) an electronic money card e.g mondex
c) a drivers licence containing current information about bookings etc
d) an access control card containing a digitized photo

(xlii) After the encryption stage in SSL, the maximum length of each fragment is

a) 214+1028
b) 214+2048
c) 216+1028
d) 216+2048

(xliii) Which protocol is used for the purpose of copying the pending state into the current state?

a) alert protocol
b) handshake protocol
c) upper-layer protocol
d) change cipher spec protocol

(xliv) Number of phases in the handshaking protocol?

a) 2
b) 3
c) 4
d) 5

(xlv) In the phase 2 of the handshake protocol action, the step server_key_exchange is not needed for which of the following cipher systems?

a) Fortezza
b) Anonymous Diffie- Hellman

c) Fixed Diffie-Hellman
d) RSA

(xlvi) Which among the following are uncontrolled and un-registered form of ephemeral ports in accordance to IANA?

a) well known ports
b) registered ports
c) dynamic ports
d) all of these

(xlvii) Which TCP timer signifies its contribution in measuring the time of connection maintenance in TIME_WAIT state?

a) keep alive timer
b) persist timer
c) retransmission timer
d) 2 maximum segment lifetime timer

(xlviii) Which one of the following is not a session state parameter?

a) master secret
b) cipher spec
c) peer certificate
d) server write key

(xlix) How can you help stop spam?

a) block certain email address known for sending spam
b) set up email filters based on keywords known to be in spam
c) unsubscribe from list serves
d) all of these

(l) Computer virus program is usually hidden in

a) operating system
b) application program
c) both operating system and application program
d) disk driver

(li) What are the examples of malware spreads?

a) social network
b) pirated software
c) removable media
d) all of these

(lii) Attack in which a user creates a packet that appears to be something else

a) smurfing
b) trojan
c) e-mail bombing
d) spoofing

(liii) A malicious code hidden inside a seemingly harmless piece of code.

a) worm
b) bomb
c) trojan horse
d) virus

(liv) The attack that focuses on capturing small packets from the network transmitted by other computers and reading the data content in search of any type of information is ____

a) phishing
b) eavesdropping
c) scams
d) exploits

(lv) Which of the following is not a software firewall?

a) windows firewall
b) outpost firewall pro
c) endian firewall
d) linksys firewall

(lvi) A firewall protects which of the following attacks?

a) phishing
b) dumpster diving
c) denial of service (DoS)
d) shoulder surfing

(lvii) Which among the following is correct characteristics about proxy server

a) a proxy server may act as a firewall by responding to input packets in the manner of an application while blocking other packets
b) a proxy server is a gateway from one network to another for a specific network application
c) it performs its tasks or functions as a proxy on behalf of the network user;
d) all of these

(lviii) Which of the following are the types of firewall?

a) packet filtering firewall
b) dual homed gateway firewall
c) screen host firewall
d) all of these

(lix) Can a proxy be used as a firewall? If so how?

a) no, proxies are data encryption stations whose sole purpose is to encrypt and re-rout data

b) no, proxies are firewalls that are maintained at locations other than that of the user

c) no, all a proxy does is re-rout internet traffic thus all the malicious signals that go with it

d) yes, a proxy acts as a network intermediary for the user that serves to control the flow of incoming and outgoing traffic

(lx) Which of the following layer is absent in the TCP/IP network model?

a) Application

b) Network

c) Transport

d) Presentation