BRAINWARE UNIVERSITY

Term End Examination 2021 - 22
Programme – Bachelor of Technology in Computer Science & Engineering
Course Name – Cryptography and Cyber Security
Course Code - BCSE604A
(Semester VI)

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) What is the kind of firewall is connected between the device and the network connecting to inter net.
  a) Hardware Firewall
  b) Software Firewall
  c) Stateful Inspection Firewall
  d) Microsoft Firewall

(2) Wireshark is a _____ tool
  a) network protocol analysis
  b) network connection security
  c) connection analysis
  d) defending malicious packet-filtering

(3) Aircrack-ng is used for _____
  a) Firewall bypassing
  b) Wi-Fi attacks
  c) Packet filtering
  d) System password cracking

(4) _____ scans TCP ports and resolves different hostnames.
  a) SuperScan
  b) Snort
  c) Ettercap
  d) QualysGuard

(5) _____ is a web application assessment security tool.
  a) LC4
  b) WebInspect
  c) Ettercap
  d) QualysGuard

(6) _____ is a code injecting method used for attacking the database of a system / website.
  a) HTML injection
  b) SQL Injection
  c) Malicious code injection
  d) XML Injection

(7) Stuxnet is a _____
  a) Worm
  b) Virus
  c) Trojan
  d) Antivirus

(8) _____ is the kind of firewall is connected between the device and the network con necting to internet.
  a) Hardware Firewall
  b) Software Firewall
  c) Stateful Inspection Firewall
  d) Microsoft Firewall

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

a) Phishing

b) Dumpster diving

c) Denial of Service (DoS)

d) Shoulder surfing

(10) Packet filtering firewalls are deployed on _____

a) routers

b) switches

c) hubs

d) repeaters

(11) ACL stands for _____

a) Access Condition List

b) Anti-Control List

c) Access Control Logs

d) Access Control List

(12) One advantage of Packet Filtering firewall is _____

a) more efficient

b) less complex

c) less costly

d) very fast

(13) Packet filtering firewalls are vulnerable to _____

a) hardware vulnerabilities

b) MiTM

c) phishing

d) spoofing

(14) Which of the following is a disadvantage of Circuit-level gateway firewalls?

a) They're expensive

b) They're complex in architecture

c) They do not filter individual packets

d) They're complex to setup

(15) _____ gateway firewalls are deployed in application-layer of OSI model.

a) Packet Filtering Firewalls

b) Circuit Level Gateway Firewalls

c) Application-level Gateway Firewalls

d) Stateful Multilayer Inspection Firewalls

(16) Application level gateway firewalls protect the network for specific _____

a) application layer protocol

b) session layer protocol

c) botnet attacks

d) network layer protocol

(17) _____ is an internet scam done by cyber-criminals where the user is convinced digitally to provide confidential information.

a) Phishing attack

b) DoS attack

c) Website attack

d) MiTM attack

(18) Email Phishing came into origin in the year _____

a) 1990

b) 2000

c) 2005

d) 2015

(19) _____ type of phishing became very popular as if it has been sent from a legitimate source with a legitimate link to its official website.

a) Algo-based phishing

b) Email-based phishing

c) Domain Phishing

d) Vishing

(20) _____ = voice + phishing.

a) Algo-based phishing

b) Vishing

c) Domain Phishing

d) Email-based phishing

(21) _____ or smishing is one of the simplest types of phishing where the target victims may get a fake order detail with a cancellation link.

a) Algo-based phishing

b) SMS phishing

c) Domain Phishing

d) Spear phishing

(22) _____ phishing is that type of phishing where the construction of a fake webpage is done for targeting definite keywords & waiting for the searcher to land on the fake webpage.

a) Voice

b) SMS

c) Search engine

d) Email

(23) Which of the following is not an example or type of phishing?

a) Tracking

b) Vishing

c) Smishing

d) Pharming

(24) Which of the following is not a vulnerability of the network layer?

a) Route spoofing

b) Identity & Resource ID Vulnerability

c) IP Address Spoofing

d) Weak or non-existent authentication

(25) Which of the following is an example of physical layer vulnerability?

a) MAC Address Spoofing

b) Physical Theft of Data

c) Route spoofing

d) Weak or non-existent authentication

(26) As a backup for securing your device, it is necessary to create a _____

a) backup point

b) copy of files in separate drives

c) copy of files in the same drives

d) restore point

(27) _____ is an application which now comes built-in Windows OS & it allows Windows users to encrypt all drive for security purpose.

a) MS Windows Defender

b) MSE

c) BitLocker

d) MS Office

(28) A _____ tries to formulate a web resource occupied or busy its users by flooding the URL of the victim with unlimited requests than the server can handle.

a) Phishing attack

b) DoS attack

c) Website attack

d) MiTM attack

(29) During a DoS attack, the regular traffic on the target _____ will be either dawdling down or entirely interrupted.

a) network

b) system

c) website

d) router

(30) DoS is abbreviated as _____

a) Denial of Service

b) Distribution of Server

c) Distribution of Service

d) Denial of Server

(31) _____ is a type of DoS threats to overload a server as it sends a large number of requests requiring resources for handling & processing.

a) Network Layer DoS

b) Physical Layer DoS

c) Transport Layer DoS

d) Application Layer DoS

(32) In _____ a sequence of actions is carried out on this block after a block of plain-text bits is chosen for generating a block of cipher-text bits.

a) Block Cipher

b) One-time pad

c) Hash functions

d) Vigenere Cipher

(33) The procedure to add bits to the last block is termed as _____

a) decryption

b) hashing

c) tuning

d) padding

(34) DES stands for _____

a) Data Encryption Security

b) Data Encrypted Standard

c) Device Encryption Standard

d) Data Encryption Standard

(35) _____ are the special type of programs used for recording and tracking user's keystroke.

a) Keylogger

b) Trojans

c) Virus

d) Worms

(36) These are a collective term for malicious spying programs used for secretly monitoring someone's activity and actions over a digital medium.

a) Malware

b) Remote Access Trojans

c) Keyloggers

d) Spyware

(37) XSS is abbreviated as _____

a) Extreme Secure Scripting

b) Cross Site Security

c) X Site Scripting

d) Cross Site Scripting

(38) Which Cryptographic system uses C1 = (e1r) mod p and C1 = (e2r x P) mod p at the encryption side?

a) Elgamal

b) RSA

c) Rabin

d) Whirlpool

(39) Compute private key (d, p, q) given public key (e=23, n=233 ´ 241=56,153).

a) 35212

b) 12543

c) 19367

d) 32432

(40) _____ framework made cracking of vulnerabilities easy like point and click.

a) .Net

b) Metasploit

c) Zeus

d) Ettercap

(41) _____ is a popular tool used for discovering networks as well as in security auditing.

a) Ettercap

b) Metasploit

c) Nmap

d) Burp Suit

(42) Which of this Nmap do not check?

a) services different hosts are offering

b) on what OS they are running

c) what kind of firewall is in use

d) what type of antivirus is in use

(43) Which of the following deals with network intrusion detection and real-time traffic analysis?

a) John the Ripper

b) L0phtCrack

c) Snort

d) Nessus

(44) Which of the below-mentioned tool is used for Wi-Fi hacking?

a) Wireshark

b) Nessus

c) Aircrack-ng

d) Snort

(45) Aircrack-ng is used for _____

a) Firewall bypassing

b) Wi-Fi attacks

c) Packet filtering

d) System password cracking

(46) _____ is a popular IP address and port scanner.

a) Cain and Abel

b) Snort

c) Angry IP Scanner

d) Ettercap

(47) _____ is a popular tool used for network analysis in multiprotocol diverse network.

a) Snort

b) SuperScan

c) Burp Suit

d) EtterPeak

(48) _____ scans TCP ports and resolves different hostnames.

a) SuperScan

b) Snort

c) Ettercap

d) QualysGuard

(49) In the _____ layer of OSI model, packet filtering firewalls are implemented.

a) Application layer

b) Session layer

c) Presentation layer

d) Network layer

(50) Packet filtering firewalls are deployed on _____

a) routers

b) switches

c) hubs

d) repeaters

(51) Firewall examines each _____ that are entering or leaving the internal network.

a) emails users

b) updates

c) connections

d) data packets

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

a) Windows Firewall

b) Outpost Firewall Pro

c) Endian Firewall | d) Linksys Firewall

(53) Which one of the following algorithm is not used in asymmetric-key cryptography?

a) rsa algorithm | b) diffie-hellman algorithm

c) electronic code book algorithm | d) dsa algorithm

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

a) transpositional ciphers | b) substitution ciphers

c) both transpositional ciphers and substitution ciphers | d) quadratic ciphers

(55) What is data encryption standard (DES)?

a) block cipher | b) stream cipher

c) bit cipher | d) byte cipher

(56) Which one of the following is a cryptographic protocol used to secure HTTP connection?

a) stream control transmission protocol (SCTP) | b) transport layer security (TLS)

c) explicit congestion notification (ECN) | d) resource reservation protocol

(57) ElGamal encryption system is _____

a) symmetric key encryption algorithm | b) asymmetric key encryption algorithm

c) not an encryption algorithm | d) block cipher method

(58) Cryptographic hash function takes an arbitrary block of data and returns _____

a) fixed size bit string | b) variable size bit string

c) both fixed size bit string and variable size bit string | d) variable sized byte string

(59) In tunnel mode, IPSec protects the _____

a) Entire IP packet | b) IP header

c) IP payload | d) IP trailer

(60) Which component is included in IP security?

a) Authentication Header (AH) | b) Encapsulating Security Payload (ESP)

c) Internet key Exchange (IKE) | d) All of the mentioned

(61) WPA2 is used for security in _____

a) Ethernet | b) Bluetooth

c) Wi-Fi | d) Email

(62) Extensible authentication protocol is authentication framework frequently used in _____

a) Wired personal area network | b) Wireless networks

c) Wired local area network | d) Wired metropolitan area network

(63) Pretty good privacy (PGP) is used in _____

a) Browser security | b) Email security

c) FTP security | d) WiFi security

(64) PGP encrypts data by using a block cipher called _____

a) International data encryption algorithm | b) Private data encryption algorithm

c) Internet data encryption algorithm | d) Local data encryption algorithm

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

a) DNS lookup | b) DNS hijacking

c) DNS spoofing | d) DNS authorizing

(66) What protocol is NOT used in the operation of a VPN?

a) PPTP | b) IPsec

c) YMUM | d) L2TP

(67) VPNs are financially speaking _____

a) Always more expensive than leased lines   b) Always cheaper than leased lines

c) Usually cheaper than leased lines   d) Usually more expensive than leased lines

(68) ESP (Encapsulating Security Protocol) is defined in which of the following standards?

a) IPsec   b) PPTP

c) PPP   d) L2TP

(69) A proxy firewall filters at _____

a) Physical layer   b) Data link layer

c) Network layer   d) Application layer

(70) Which of the following is / are the types of firewall?

a) Packet Filtering Firewall   b) Dual Homed Gateway Firewall

c) Screen Host Firewall   d) Dual Host Firewall