BRAINWARE UNIVERSITY

Term End Examination 2021 - 22
Programme – Bachelor of Science (Honours) in Advanced Networking & Cyber Security
Course Name – Digital Forensics
Course Code - BNCSC602
(Semester VI)

Time allotted : 1 Hrs.15 Min. **Full Marks : 60**

[The figure in the margin indicates full marks.]

Group-A

(Multiple Choice Type Question) 1 x 60=60

Choose the correct alternative from the following :

(1) In which year the term hacking was coined?

a) 1965-67 b) 1955-60
c) 1970-80 d) 1980-82

(2) From where the term 'hacker' first came to existence?

a) MIT b) California
c) Stanford University d) Bell's Lab

(3) Who deploy Malwares to a system or network?

a) Criminal organizations, Black hat hackers, malware developers, cyber-terrorists
b) Criminal organizations, White hat hackers malware developers, cyber-terrorists
c) Criminal organizations, Black hat hackers, software developers, cyber-terrorists
d) Criminal organizations, gray hat hackers, Malware developers, Penetration testers

(4) XSS is abbreviated as _____

a) Extreme Secure Scripting b) Cross Site Security
c) X Site Scripting d) Cross Site Scripting

(5) Hackers who help in finding bugs and vulnerabilities in a system & don't intend to crack a system are termed as _____

a) Black Hat hackers b) White Hat Hackers
c) Grey Hat Hackers d) Red Hat Hackers

(6) Which is the legal form of hacking based on which jobs are provided in IT industries and firms?

a) Cracking b) Non ethical Hacking
c) Ethical hacking d) Hactivism

(7) They are nefarious hackers, and their main motive is to gain financial profit by doing cyber crimes. Who are "they" referred to here?

a) Gray Hat Hackers
b) White Hat Hackers
c) Hactivists
d) Black Hat Hackers

(8) _____ are the combination of both white as well as black hat hackers.

a) Grey Hat hackers
b) Green Hat hackers
c) Blue Hat Hackers
d) Red Hat Hackers

(9) The amateur or newbie in the field of hacking who don't have many skills about coding an d in-depth working of security and hacking tools are called _____

a) Sponsored Hackers
b) Hactivists
c) Script Kiddies
d) Whistle Blowers

(10) Suicide Hackers are those _____

a) who break a system for some specific purpose with or without keeping in mind that they may suffer long term imprisonment due to their ma licious activity
b) individuals with no knowledge of codes but a n expert in using hacking tools
c) who know the consequences of their hacking a ctivities and hence try to prevent them by erasi ng their digital footprints
d) who are employed in an organization to do ma licious activities on other firms

(11) Criminal minded individuals who work for terrorist organizations and steal information of nations and other secret intelligence are _____

a) State sponsored hackers
b) Blue Hat Hackers
c) Cyber Terrorists
d) Red Hat Hackers

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

a) Eavesdropping
b) MAC Spoofing
c) Wireless Hijacking
d) Phishing

(13) Which method of hacking will record all your keystrokes?

a) Keyhijacking
b) Keyjacking
c) Keylogging
d) Keyboard monitoring

(14) _____ are the special type of programs used for recording and tracking user's keystro ke.

a) Keylogger
b) Trojans
c) Virus
d) Worms

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

a) Malware
b) Remote Access Trojans
c) Keyloggers
d) Spyware

(16) _____ is a violent act done using the Internet, which either threatens any technolog y user or leads to loss of life or otherwise harms anyone in order to accomplish political g ain.

a) Cyber-warfare
b) Cyber campaign
c) Cyber-terrorism
d) Cyber attack

(17) _____ is the practice and precautions taken to protect valuable information from unauth orized access, recording, disclosure or destruction

a) Network Security
b) Database Security
c) Information Security
d) Physical Security

(18) From the options below, which of them is not a threat to information security?

a) Disaster
b) Eavesdropping
c) Information leakage
d) Unchanged default password

(19) Which of the following information security technology is used for avoiding browser-base d hacking?

a) Anti-malware in browsers
b) Remote browser access
c) Adware remover in browsers
d) Incognito mode in a browser

(20) Compromising confidential information comes under _____

a) Bug
b) Threat
c) Vulnerability
d) Attack

(21) Lack of access control policy is a _____

a) Bug
b) Threat
c) Vulnerability
d) Attack

(22) How many basic processes or steps are there in ethical hacking?

a) 4
b) 5
c) 6
d) 7

(23) _____ is the information gathering phase in ethical hacking from the target user.

a) Reconnaissance
b) Scanning
c) Gaining access
d) Maintaining access

(24) Which of the following is not a reconnaissance tool or technique for information gathering

a) Hping
b) NMAP
c) Google Dorks
d) Nexpose

(25) _____ phase in ethical hacking is known as the pre-attack phase

a) Reconnaissance
b) Scanning
c) Gaining access
d) Maintaining access

(26) While looking for a single entry point where penetration testers can test the vulnerability, t hey use _____ phase of ethical hacking.

a) Reconnaissance
b) Scanning
c) Gaining access
d) Maintaining access

(27) Which of them does not comes under scanning methodologies?

a) Vulnerability scanning
b) Sweeping
c) Port Scanning
d) Google Dorks

(28) Which of them is not a scanning tool?

a) NMAP
b) Nexpose
c) Maltego
d) Nessus

(29) Which of the following comes after scanning phase in ethical hacking?

a) Scanning
b) Maintaining access
c) Reconnaissance
d) Gaining access

(30) _____ phase the hacker exploits the network or system vulnerabilities

a) Scanning
b) Reconnaissance
c) Maintaining access
d) Gaining access

(31) Which of the following is not done in gaining access phase?

a) Tunnelling
b) Buffer overflow
c) Session hijacking
d) Password cracking

(32) Which of the below-mentioned penetration testing tool is popularly used in gaining access phase

a) Maltego
b) NMAP

c) Metasploit
d) Nessus

(33) _____ ensures the integrity and security of data that are passing over a network.

a) Firewall
b) Antivirus
c) Pentesting Tools
d) Network-security protocols

(34) Which of the following is not a strong security protocol?

a) HTTPS
b) SSL
c) SMTP
d) SFTP

(35) Which of the following is not a secured mail transferring methodology?

a) POP3
b) SSMTP
c) Mail using PGP
d) S/MIME

(36) _____ is a set of conventions & rules set for communicating two or more devices re siding in the same network

a) Security policies
b) Protocols
c) Wireless network
d) Network algorithms

(37) HTTPS is abbreviated as _____

a) Hypertexts Transfer Protocol Secured
b) Secured Hyper Text Transfer Protocol
c) Hyperlinked Text Transfer Protocol Secured
d) Hyper Text Transfer Protocol Secure

(38) _____ is the entity for issuing digital certificates.

a) Certificate Authority (CA)
b) Cert Authority (CA)
c) Cert Authority (CA)
d) Certificate Authorization (CA)

(39) _____ is any action that might compromise cyber-security.

a) Threat
b) Vulnerability
c) Exploit
d) Attack

(40) Existence of weakness in a system or network is called _____

a) Threat
b) Vulnerability
c) Exploit
d) Attack

(41) When any IT product, system or network is in need for testing for security reasons, then th e term used is called _____

a) Threat
b) Vulnerability
c) Target of Evaluation
d) Attack

(42) _____ is an act of hacking by the means of which a political or social message is con veyed.

a) Hacktivism
b) Whistle-blowing
c) Surveillance
d) Pseudonymization

(43) _____ is the method of developing or creating a structurally similar yet unauthentic and illegitimate data of any firm or company.

a) Data copying
b) Data breaching
c) Data masking
d) Data duplicating

(44) Data masking is also known as _____

a) Data obfuscation
b) Data copying
c) Data breaching
d) Data duplicating

(45) Backdoors are also known as _____

a) Trap doors
b) Cover doors
c) Front doors
d) Back entry

(46) Adware are pre-chosen _____ developed to display ads.

a) banner
b) software
c) malware
d) shareware

(47) _____ is an attack technique occurs when excess data gets written to a memory block.
a) Over buffering
b) Buffering
c) Buffer overflow
d) Memory full

(48) Finding & publishing any user's identity with the help of different personal details is called _____
a) Doxing
b) Data breaching
c) Personal data copying
d) Secure File Transferring Protocol

(49) In IP address, IP is abbreviated as _____
a) Internet Program
b) Internet Protocol
c) Intuition Programs
d) Internet Pathway

(50) Whaling is the technique used to take deep and _____ information about any individual
a) sensitive
b) powerful
c) useless
d) casual

(51) _____ are a specific section of any virus or malware that performs illicit activities in a system
a) Malicious programs
b) Worms
c) Spyware
d) Payload

(52) _____ is a scenario when information is accessed without authorization.
a) Data infiltration
b) Data Hack
c) Information compromise
d) Data Breach

(53) _____ is an attempt to steal, spy, damage or destroy computer systems, networks or their associated information.
a) Cyber-security
b) Cyber attack
c) Digital hacking
d) Computer security

(54) _____ is a device which secretly collects data from credit / debit cards
a) Card Skimmer
b) Data Stealer
c) Card Copier
d) Card cloner

(55) _____ is a technique used when artificial clicks are made which increases revenue because of pay-per-click.
a) Clickjacking
b) Clickfraud
c) Keylogging
d) Click-hacking

(56) _____ is the practice implemented to spy someone using technology for gathering sensitive information
a) Cyber espionage
b) Cyber-spy
c) Digital Spying
d) Spyware

(57) _____ is the way or technique through which majority of the malware gets installed in our system.
a) Drive-by click
b) Drive-by download
c) Drive-by redirection
d) Drive-by injecting USB devices

(58) _____ is the term used for toolkits that are purchased and used for targeting different exploits.
a) Exploit bag
b) Exploit set
c) Exploit Toolkit
d) Exploit pack

(59) _____ is the hacking approach where cyber-criminals design fake websites or pages f or tricking or gaining additional traffic

a) Cyber-replication
b) Mimicking
c) Website-Duplication
d) Pharming

(60) When you book online tickets by swiping your card, the details of the card gets stored in _ _____

a) Database system
b) Point-of-sale system
c) Servers
d) Hard drives