



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)

Comes	Ci (1)
Γime: 1 Hr.15 Min.	Full Marks : 60
[The figure in the margin	
Alementa 12	51 m × 11
Grou	p-A
(Multiple Choice	Type Question) 1 x 60=60
Choose the correct alternative from the following	a po disservi
(1) From where the term 'hacker' first came to exist	stence?
a) MIT	b) California
c) Stanford University	d) Bell's Lab
(2) XSS is abbreviated as	
a) Extreme Secure Scripting	b) Cross Site Security
c) X Site Scripting	d) Cross Site Scripting
(3) Which is the legal form of hacking based on wh nd firms?	nich jobs are provided in IT industries a
a) Cracking	b) Non ethical Hacking
c) Ethical hacking	d) Hactivism
(4) 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
(5) Suicide Hackers are those	
 a) who break a system for some specific purpos e with or without keeping in mind that they may suffer long term imprisonment due to th eir malicious activity 	b) individuals with no knowledge of codes but an expert in using hacking tools
 c) who know the consequences of their hacking activities and hence try to prevent them by er asing their digital footprints 	d) who are employed in an organization to do malicious activities on other firms

b) MAC Spoofing

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

a) Eavesdropping

	d) Phishing
c) Wireless Hijacking	ed for recording and tracking user's keys
Dealawart University	b) Trojans
Barosat, Kolkata - 100 125	d) Worms
c) virus	ternet, which either threatens any techno
(8) is a violent act done using the model logy user or leads to loss of life or otherwise has	arms anyone in order to accomplish polit
ical gain.	
a) Cyber-warfare	b) Cyber campaign
c) Cyber-terrorism	d) Cyber attack
(9) 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
(10) Compromising confidential information comes	under
a) Bug	b) Threat
c) Vulnerability	d) Attack
(11) How many basic processes or steps are there in	ethical hacking?
a) 4	b) 5
c) 6	d) 7
(12) Which of the following is not a reconnaissance	
ing	
a) Hping	b) NMAP
c) Google Dorks	d) Nexpose
(13) While looking for a single entry point where per y, they use phase of ethical hacking.	enetration testers can test the vulnerabilit
a) Reconnaissance	b) Scanning
c) Gaining access	d) Maintaining access
(14) Which of them is not a scanning tool?	
a) NMAP	b) Nexpose
c) Maltego	d) Nessus
(15) phase the hacker exploits the netw	ork or system vulnerabilities
a) Scanning	b) Reconnaissance
c) Maintaining access	d) Gaining access
(16) Which of the below-mentioned penetration test ess phase	ing tool is popularly used in gaining acc
a) Maltego	b) NMAP
c) Metasploit	d) Nessus
(17) Which of the following is not a strong security	protocol?
a) HTTPS	b) SSL
c) SMTP	d) SFTP
	for communicating two or more devices
residing in the same network	
a) Security policies	b) Protocols
c) Wireless network	d) Network algorithms
(19) is the entity for issuing digital certification	cates.

a) Certificate Authority (CA)	b) Cert Authority (CA)
c) Cert Authority (CA)	d) Certificate Authorization (CA)
(20) Existence of weakness in a system or network is	called
a) Threat	b) Vulnerability
c) Exploit	d) Attack
(21) When any IT product, system or network is in n n the term used is called	eed for testing for security reasons, the
a) Threat	b) Vulnerability
c) Target of Evaluation	d) Attack
(22) is an act of hacking by the means of onveyed.	which a political or social message is c
a) Hacktivism	b) Whistle-blowing
c) Surveillance	d) Pseudonymization
(23) is the method of developing or creating and illegitimate data of any firm or company.	
a) Data copying	b) Data breaching
c) Data masking	d) Data duplicating 8 rateur
(24) Data masking is also known as	b) Data breaching d) Data duplicating Braining Barasal, K.
a) Data obfuscation	b) Data copying
c) Data breaching	d) Data duplicating
(25) Backdoors are also known as	* # **
a) Trap doors	b) Cover doors
The state of the s	d) Back entry
(26) Adware are pre-chosen developed to d	5
a) banner	b) software
c) malware	d) shareware
	ccess data gets written to a memory blo
a) Over buffering	b) Buffering
c) Buffer overflow	d) Memory full
(28) Finding & publishing any user's identity with the	ne help of different personal details is ca
a) Doxing	b) Data breaching
c) Personal data copying	d) Secure File Transferring Protocol
(29) In IP address, IP is abbreviated as	CONTRACTOR OF THE CONTRACTOR O
a) Internet Program	b) Internet Protocol
,	d) Internet Pathway
(30) Whaling is the technique used to take deep and idual	information about any indiv
a) sensitive	b) powerful
c) useless	d) casual
	malware that performs illicit activities
a) Malicious programs	b) Worms
c) Spyware	d) Payload

(32) is a scenario when infor	mation is accessed without authorization.
a) Data infiltration	b) Data Hack
c) Information compromise	d) Data Breach
(33) is an attempt to steal, sp	y, damage or destroy computer systems, networ
ks or their associated information.	Oratowers run.
a) Cyber-security	b) Cyber attack Barusat, nomato -700100
c) Digital hacking	d) Computer security
(34) is a device which secretly	collects data from credit / debit cards
a) Card Skimmer	b) Data Stealer
c) Card Copier	d) Card cloner
(35) is a technique used when the enue because of pay-per-click.	en artificial clicks are made which increases rev
a) Clickjacking	b) Clickfraud
c) Keylogging	d) Click-hacking
(36) is the practice implemente g sensitive information	d to spy someone using technology for gatherin
a) Cyber espionage	b) Cyber-spy
c) Digital Spying	d) Spyware
(37) is the way or technique alled in our system.	through which majority of the malware gets inst
a) Drive-by click	b) Drive-by download
c) Drive-by redirection	d) Drive-by injecting USB devices
(38) is the term used for toolkits that exploits.	t are purchased and used for targeting different
a) Exploit bag	b) Exploit set
c) Exploit Toolkit	d) Exploit pack
(39) is the hacking approach wh es for tricking or gaining additional traf	ere cyber-criminals design fake websites or pag
a) Cyber-replication	b) Mimicking
c) Website-Duplication	d) Pharming
(40) When you book online tickets by swipi	ng your card, the details of the card gets stored i
a) Database system	b) Point-of-sale system
c) Servers	d) Hard drives
(41) are deadly exploits where the inals but not known and fixed by the ov	vulnerability is known and found by cyber-crim wner of that application or company
a) Unknown attacks	b) Secret attacks
c) Elite exploits	d) Zero-day exploits
(42) Zero-day exploits are also called	the second of th
a) Zero-day attacks	b) Hidden attacks
c) Un-patched attacks	d) Un-fixed exploits
(43) Physical ports are usually referred to as	110
a) Jacks	b) Cables
c) Interfaces	d) Hardware plugs
	gned for logical connections

a) Logical ports	b) Physical ports
c) Networking cables	d) IP address
(45) Number of logical ports ranges from	
a) 0, 255	b) 1, 65535
c) 1, 65536	d) 0, 65536
(46) needs some control for data	
a) Antivirus	b) Network firewall
c) Intrusion Detection Systems (IDS)	
(47) Which of the following is the port nur	mber for FTP data
a) 20	b) 21
c) 22	d) 23
(48) Which of the following is the port nur	
a) 20	b) 21
c) 22	d) 23
(49) Which of the following is the port nur	
a) 20	b) 21
c) 22	
(50) Which of the following is the port nu	5
a) 20	b) 21
c) 22	d) 23
(51) Firewalls can be of kinds.	d) 23
a) 1	b) 2
c) 3	d) 4
	rewall is connected between the device and the ne
twork connecting to internet.	toward is connected between the device and the ne
a) Hardware Firewall	b) Software Firewall
c) Stateful Inspection Firewall	d) Microsoft Firewall
(53) is software that is installe fault with operating systems	ed using an internet connection or they come by-de
a) Hardware Firewall	b) Software Firewall
c) Stateful Inspection Firewall	d) Microsoft Firewall
(54) Which of the following is not a softw	/are firewall?
a) Windows Firewall	b) Outpost Firewall Pro
c) Endian Firewall	d) Linksys Firewall
	that are entering or leaving the internal networ
a) Emails users	b) Updates
c) Connections	d) Data packets
(56) A firewall protects which of the follow	owing attacks?
a) Phishing	b) Dumpster diving
c) Denial of Service (DoS)	d) Shoulder surfing
(57) There are types of firewall.	
a) 5	b) 4
c) 3	d) 2

(58) Packet filtering firewalls are depl	oyed on
a) Routers	b) Switches
c) Hubs	d) Repeaters
(59) In the layer of 6	OSI model, packet filtering firewalls are implemented.
a) Application layer	b) Session layer
c) Presentation layer	d) Network layer
(60) The defines the pack	tet filtering firewall rules
a) Access Control List	b) Protocols
c) Port	d) Policies

.