Program: BE Information Technology Engineering

Curriculum Scheme: Revised 2016

Examination: Third Year Semester VI

Course Code: ITDLO6023 and Course Name: Digital Forensics

Time: 1 hour Max. Marks: 50

==========

==========

Note to the students:- All the Questions are compulsory and carry equal marks .

Q1.	Which statements among the following is applicable to phishing
Option A:	inserted into software intentionally so as to execute a malicious program when triggered by a specific event
Option B:	flooding a resource with too many requests, thus consuming its available bandwidth resulting in server overload
Option C:	extracting confidential information such as password by posing as a legitimate program
Option D:	following the victims online to extract information and threaten verbally
Q2.	Which statement among the following is not applicable to cybercrime prevention
Option A:	making strong password
Option B:	Installing torrent
Option C:	Installing firewall
Option D:	Using antivirus software
Q3.	Which among the following is not applicable to hacking Methodology
Option A:	Reconnaissance
Option B:	Scanning
Option C:	Clearing tracks
Option D:	installing firewall
Q4.	Which statements among the following is applicable to data diddling
Option A:	unauthorized data alterations before or at the time of entering the data into a computer l and changing it back after processing is completed
Option B:	extracting confidential information such as password by posing as a legitimate program
Option C:	steal money very little at a time such that there's very little difference in final total
Option D:	Using torrents to download resources
Q5.	Which statements among the following is applicable to cyber stalking

Option A:	inserted into software intentionally so as to execute a malicious program when triggered by a specific event
Option B:	flooding a resource with too many requests, thus consuming its available bandwidth resulting in server overload
Option C:	extracting confidential information such as password by posing as a legitimate program
Option D:	following the victims online to extract information and threaten verbally
Q6.	Which of the following is the type of an attack that is conducted with the intention of accessing information illegally, without damaging the data integrity?
Option A:	Mobile Threats
Option B:	Advanced Persistent Threat
Option C:	Cloud Computing Threats
Option D:	Insider Attack
Q7.	File system traces include all of the following EXCEPT:
Option A:	Metadata
Option B:	CMOS settings
Option C:	Data object date-time stamps
Option D:	Swap file contents
Q8.	Forensically acceptable alternatives to using a Windows Evidence Acquisition Boot Disk include all but which of the following?
Option A:	Linux boot floppy
Option B:	Booting into safe mode
Option C:	FIRE bootable CD-ROM
Option D:	Hardware write blockers
Q9.	Definition of cybercrime is
Option A:	a criminal activity involving a computer, networked device or a network
Option B:	criminal activity involving a computer
Option C:	criminal activity involving a networked device
Option D:	any criminal activity that involves a network
Q10.	A copy which includes all necessary parts of evidence, which is closely related to the original evidence.
Option A:	Digital Evidence
Option B:	Best Evidence
Option C:	Original Evidence
Option D:	Complete Evidence
Q11.	CSIRT stands for _____
Option A:	Computer security incident response team
Option B:	Computer software incident resource team
Option C:	Common security incident resolution team

Option D:	Computer security incident resource team
Q12.	Forensic Duplication is necessary
Option A:	as it preserves original digital evidence & allows recreation of the duplicate image
Option B:	as it creates restored image
Option C:	as it creates and stores mirror image
Option D:	as it helps in live system duplication
Q13.	Analyzing data collected from different sites, Firewalls and IDS is called as..?
Option A:	Computer Forensics
Option B:	Network Forensics
Option C:	Mobile Devices Forensics
Option D:	Memory Forensics
Q14.	In central incident response team how many teams handle incidents occourring in whole organization?
Option A:	1
Option B:	2
Option C:	3
Option D:	4
Q15.	Restoration Process involves
Option A:	blind sector to sector copy of the duplicate file
Option B:	collection of Digital Evidence
Option C:	creation of response toolkit
Option D:	check the dependencies
Q16.	Securing and isolating the state of physical and logical evidences from being altered is referred as.....?
Option A:	Identification
Option B:	Preservation
Option C:	Collection
Option D:	Examination
Q17.	Which one among the following statements should be present in the layout of forensic report
Option A:	Findings
Option B:	Hacking tools
Option C:	Information related to importance of digital forensics
Option D:	Budget
Q18.	What type of attack accomplishes the confidential information by modes of human communication?
Option A:	Spoofing
Option B:	Cyber attack

Option C:	Social engineering
Option D:	Phishing
Q19.	What is not required for setting up Network Monitoring System?
Option A:	Printers and scanners
Option B:	Hardware- and software-based network diagnostic tools
Option C:	IDS sensors
Option D:	packet capture utilities
Q20.	Which of the following gives the user a quick way to access recently used items?
Option A:	Dynamic lock
Option B:	BitLocker
Option C:	Jump Lists
Option D:	Firewall
Q21.	Which one among the following statements is not applicable to a good forensic report writing
Option A:	Contain all the data required to support the conclusion
Option B:	Offer correct conclusions
Option C:	should be ready at the time of need
Option D:	open to different interpretations
Q22.	Which one among the following statements is not a task performed by computer forensic tools
Option A:	acquisition
Option B:	validation
Option C:	extraction
Option D:	compression
Q23.	Which one of the following is not the mail forensic tool
Option A:	Adcomplain
Option B:	AbusePipe
Option C:	EmailTracker
Option D:	Cryptcat
Q24.	Which one is not the mode of operation for SafeBack tool
Option A:	Back up Function
Option B:	Restore Function
Option C:	Verify Function
Option D:	Duplicate Function
Q25.	Which protocol is not the part of DDoS attack?
Option A:	FTP
Option B:	ICMP
Option C:	TCP

Option D:	UDP