University of Mumbai

Sample Question Bank

Program: **Electronics and Telecommunication Engineering**

Examination: TE Semester: VI

Course Code: **ECCDLO6013**

Course Name: **Digital Forensic**

==========

Q1.	Choose the correct option for the following questions. All the questions are compulsory and carry equal marks
1.	To list the processes that are currently in a running state, the following command can be used
Option A:	hosts
Option B:	ps
Option C:	netstat
Option D:	arp
2.	Which of the following is the disk-search utility which is used to perform a search from a physical level?
Option A:	PsLogList
Option B:	Dumpel.exe
Option C:	dtSearch
Option D:	hosts
3.	CSIRT stands for
Option A:	Computer Safety Incident Response Team
Option B:	Computer Security Incident Response Team
Option C:	Computer Security Incident Responsible Team
Option D:	Computer Security Information Response Team
4.	Which statute protect the privacy of individuals' healthcare data?
Option A:	Privacy Act
Option B:	HIPAA
Option C:	Computer Fraud and Abuse Act
Option D:	DMCA
5.	_____is a fraud type wherein the hacker tries to get personal information, including login credentials or any bank account information, by pretending to be a genuine entity in email, messages, or other communication channels.
Option A:	Spamming
Option B:	Phishing
Option C:	Password sniffing
Option D:	Denial-of-service
6.	This attack occurs when an unauthorized person uses the Internet hours paid for by another person.
Option A:	Password sniffing
Option B:	Denial-of-service
Option C:	Salami Attack

Option D:	Internet Time Theft
7.	A computer program that attaches itself to legitimate code and runs with the program.
Option A:	Virus
Option B:	Worm
Option C:	Trojan Horse
Option D:	Trapdoor
8.	In which phase of Incident Response Methodology, security measures and procedural changes are employed, lessons learned recorded, and long-term fixes for any problems are identified.
Option A:	Pre-incident preparation
Option B:	Formulate response strategy
Option C:	Investigate the incident
Option D:	Reporting
9.	What will be the first Response strategy for website defacement?
Option A:	Reconfigure Router
Option B:	Monitor, Repair, Investigate Website
Option C:	Performing Forensic duplication
Option D:	Law enforcement contacted
10.	Which statement is not true regarding Evidence Admissibility
Option A:	Evidence should not be competent.
Option B:	Evidence should be relevant.
Option C:	Evidence should be material.
Option D:	Evidence should be obtained legally.
11.	_____is a freely available tool that can be used to establish a communication channel between hosts.
Option A:	PsLoggedOn
Option B:	Netcat
Option C:	Netstat
Option D:	nbstat
12.	According to Rules of Forensic Duplication, how many copies of digital evidence is made
Option A:	One
Option B:	Two
Option C:	Three
	Four
13.	Which statement is true regarding Forensic Duplicate
Option A:	Stores every bit of information from source in a raw bitstream format.
Option B:	Stores every bit of information from the source in an altered form.
Option C:	Hardware does a bit-for-bit copy from one HDD to another
Option D:	Stores every bit of information from the source in binary form.
14.	In Passive attack,

Option A:	Modification in information take place
Option B:	A victim does not get informed about the attack
Option C:	System resources can be changed.
Option D:	Influence the services of the system.
15.	Which law carries the most weight among three types of law
Option A:	Statutory Law
Option B:	Case Law
Option C:	Common Law
Option D:	Local Law
16.	_____ is the deliberate desire of the person to obtain the outcome of the act
Option A:	Intent
Option B:	Knowledge
Option C:	Recklessness
Option D:	Negligence
17.	Which tool is used for sniffing the packet
Option A:	FTKImager
Option B:	Encase
Option C:	Wireshark
Option D:	Openstego
18.	In which Intrusion Detection System (IDS), detection of attacks is done by looking for specific patterns, such as byte sequences in network traffic, or known malicious instruction sequences used by malware.
Option A:	Anomaly based IDS
Option B:	Signature based IDS
Option C:	Host based IDS
Option D:	Network based IDS
19.	Which is not temporal/volatile data collection step
Option A:	List of users that are currently logged on.
Option B:	List of processes that are currently running.
Option C:	List of sockets that are open currently
Option D:	Reset Routing Table
20.	_____command that shows which users have remote-access privileges on the target system
Option A:	rasusers
Option B:	netstat
Option C:	Fport
Option D:	Arp
21.	NTFS stands for
Option A:	Next Technology File system
Option B:	New Technology File System
Option C:	New Transformed File System
Option D:	Null Type File System

22	FAT Stands for
Option A:	File Access Technology
Option B:	File Allocation Table
Option C:	Free Access Table
Option D:	File Allocation Technique
23.	Which of the following is not present in layers of file system
Option A:	Physical layer
Option B:	Data classification layer
Option C:	Application-level storage layer
Option D:	Network layer
24.	Evidence can be appropriately defined as
Option A:	Any information of probative value
Option B:	Any raw information
Option C:	Any digital information
Option D:	Any information stored in hard drive
25.	Valid definition of Digital Evidence is
Option A:	Digital data of probative value
Option B:	Any file stored in computer
Option C:	Data stored or transmitted using computer
Option D:	Data stored in removable disc
26.	Which of the following documentation specifies - who handled the evidence, where, when and for what purpose
Option A:	Chain of Custody
Option B:	Evidence inventory
Option C:	Preservation record
Option D:	Evidence intake
27.	Given the options as below, which is considered as best evidence
Option A:	First copy
Option B:	Forensic Duplicate
Option C:	Original Evidence
Option D:	Working Copy
28.	One of the advantage of digital evidence as compared to other type of physical evidence is --
Option A:	It never fails
Option B:	It can be forensically duplicated infinite number of times
Option C:	It need not be validated
Option D:	Maintaining chain of custody is not required
29.	Which of the following is an event generator tool for network traffic analysis?
Option A:	Snort
Option B:	tcptrace
Option C:	tcpflow
Option D:	Ethereal

30.	What is the use of port scanner?
Option A:	To determine the Router's Uptime
Option B:	To determine listening Sockets
Option C:	To Save the Router Configuration
Option D:	To see the Routing Table
31.	What happens when attacker attacks by using IP Spoofing?
Option A:	Sending computer impersonates another machine
Option B:	Messages being sent to the wrong computer
Option C:	Directing users to the wrong Web sites
Option D:	Incorrect entries in the ARP cache
32.	Which of the following is a method that can be used for Password cracking of a system?
Option A:	Trojan Horse
Option B:	Viruses
Option C:	Brute force
Option D:	Malware
33.	Identify the one that is not a security attack but a countermeasure
Option A:	Social Engineering
Option B:	Firewall
Option C:	Denial of Service
Option D:	Packet Sniffing
34.	In which of the following attack attacker can able to see and even make changes to Web pages that are transmitted to or from another computer?
Option A:	Web Spoofing
Option B:	Trojan Horse
Option C:	IP Spoofing
Option D:	Port Spoofing
35.	_____ is part of the standard Linux distribution used to make a bitstream copy of media.
Option A:	Safeback
Option B:	dd
Option C:	WinHex
Option D:	EnCase
36.	_____ is the technique used in organizations and firms to protect IT assets.
Option A:	Unethical hacking
Option B:	Ethical hacking
Option C:	Black hat hacking
Option D:	Gold hat hacking
37.	These junk emails may contain _____ that may harm the recipient.
Option A:	non-malicious computer programs
Option B:	malicious computer programs

Option C:	unsolicited messages
Option D:	hooking programs
38.	_____ regulates commercial e-mails.
Option A:	IPC
Option B:	CAN-SPAM
Option C:	DMCA
Option D:	CFAA
39.	CFAA stands for _____
Option A:	Cyber Fraud and Abuse Act
Option B:	Computer Fraud and Abuse Act
Option C:	Cyber Fraud Activity Analysis
Option D:	Cyber Fraud Activity Act
40.	_____ usually involve conflicts between persons or institutions.
Option A:	criminal cases
Option B:	Civil cases
Option C:	criminal and civil cases
Option D:	Family case

Subjective Questions

Q.1 Define Cybercrime. Discuss in detail various categories of Cybercrime
Q.2 Discuss violent and nonviolent cybercrimes in detail
Q.3 Define ethical hacking. Explain the life cycle of hacking
Q.4 Explain different types of hackers
Q. 5 Write a note on social engineering and prevention of cybercrime
Q. 6 Explain various hacking techniques
Q. 7 Write a note on computers' role in cybercrime
Q.8 Explain objectives, types, and process of digital forensic
Q. 9 Which are the challenges faced by digital forensic
Q. 10 Write a note on the Incident Response methodology
Q. 11 Explain in detail the phases after detection of incident
Q. 12 Define digital evidence. State and explain the rules of digital evidence
Q. 13 Explain the characteristics of digital evidence. Explain types of digital evidence
Q. 14 Explain the challenges in evidence handling
Q. 15 Explain the rules for people involved in data collection techniques
Q. 16 State the necessity and rules of forensic duplication
Q. 17 Explain the rules of forensic duplication to act as admissible evidence
Q. 18 Write a note on Forensic image formats
Q. 19 Write a note of Forensic duplication techniques
Q. 20 Explain live/volatile data collection from the windows system
Q. 21 Explain live/volatile data collection from Unix system
Q. 22 Explain the process of investigating windows and Unix systems
Q. 23 Write a note on investigating application and email tracking
Q. 24 Introduce Intrusion Detection Systems (IDS). Explain offerings of IDS
Q. 25 Explain types of IDS in detail
Q. 26 Compare and contrast intrusions and attacks
Q. 27 Explain the process for analyzing network traffic and collecting network-based evidence

Q. 28 Explain evidence handling
Q.29 Explain the process of investigating routers
Q. 30 Write a note on Constitutional law
Q. 31 Write a note on Criminal Law and Civil Law
Q. 32 Explain different levels of law
Q. 33 Write a note on CFAA, DMCA, CAN spam
Q. 34 Write a note on levels of Culpability

Note: This is the sample Question bank. The questions from the question bank may or may not be included in the university end sem examination.