Sample Questions

Information Technology

Subject Name: Ethical Hacking and Forensics Course Code: ITDO6014
Semester: VI

Multiple Choice Questions

	Choose the correct option for following questions. All the Questions carry equal marks
1.	Keyloggers are a form of_____
Option A:	Spyware
Option B:	Shoulder Surfing
Option C:	Social Engineering
Option D:	Trojan
2.	Hacking for a cause is called_____
Option A:	Activism
Option B:	Active hacking
Option C:	Hacktivism
Option D:	Black-hat hacking
3.	Scanning is performed in which phase of pen test
Option A:	Attack
Option B:	Pre Attack
Option C:	Post Attack
Option D:	Reconnaissance
4.	CSIRT stands for
Option A:	Computer security incident response team
Option B:	Computer software incident resource team
Option C:	Common security incident resolution
Option D:	Computer security incident resource
5.	Which of the following techniques is/are vulnerable to man-in-the-middle attack?
Option A:	AES
Option B:	RSA
Option C:	Diffie-Hellman key exchange
Option D:	DES
6.	Which of the following statement(s) is/are true about passive reconnaissance?
Option A:	Information about the target is collected indirectly.

Option B:	Information about the target is collected directly.
Option C:	There is no direct communication with the target system.
Option D:	There is direct communication with the target system.
7.	Assume that we want to connect to a target system (10.0.0.1) through ssh service, the username and password are “user” and “pwd” respectively. Which of the following commands can be used to create a ssh connection?
Option A:	ssh 10.0.0.1 -l user
Option B:	ssh 10.0.0.1 -l user -p pwd
Option C:	ssh 10.0.0.1 user pwd
Option D:	ssh user 10.0.0.1
8.	What are some of the features in Kali Linux?
Option A:	It is a secure operating system that has been designed as hack-proof.
Option B:	It is a Debian-based Linux distribution that have collection of tools that are useful for penetration testing.
Option C:	It is a software distribution created by the company Kali Inc.
Option D:	It is a software distribution created by the company RedHat Inc.
9.	Risks = Threats x Vulnerabilities is referred to as the:
Option A:	BIA equation
Option B:	Disaster recovery formula
Option C:	Threat assessment
Option D:	Risk equation
10.	Which statements among the following is applicable to salami slicing
Option A:	Unauthorized Data Alterations Before or At The Time Of Entering The Data Into A Computer L And Changing
Option B:	It Back After Processing Is Completed
Option C:	Extracting Confidential Information Such as Password by Posing as a legitimate program
Option D:	Legitimate Program
11.	A copy which includes all necessary parts of evidence, which is closely related to the original
Option A:	Evidence
Option B:	Digital Evidence
Option C:	Best Evidence
Option D:	Original Evidence
12.	Which one among the following is not a reconstruction tool computer forensics
Option A:	FTK imager
Option B:	SafeBack
Option C:	SnapBack
Option D:	Tableu

13.	Working from a duplicate image does NOT provide
Option A:	Preserves the original digital evidence.
Option B:	Prevents inadvertent alteration of original digital evidence during examination.
Option C:	Allows recreation of the duplicate image, if necessary.
Option D:	Maintains confidentiality of data
14.	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
15.	Verification of the duplicate is done using
Option A:	Hash Value
Option B:	Encrypted Text
Option C:	Overall Contents
Option D:	Plain String
16.	Which is not a step in the scientific method?
Option A:	Raise a question.
Option B:	Test the hypotheses.
Option C:	Wait to test.
Option D:	Draw a conclusion.
17.	How many c's in computer forensics?
Option A:	1
Option B:	2
Option C:	3
Option D:	4
18.	Recognizing and determining an incident based on network indicators is called
Option A:	Identification
Option B:	Preservation
Option C:	Collection
Option D:	Examination
19.	_____ occur when the number of bytes or characters input goes beyond the maximum number acceptable by the program
Option A:	Buffer overflows
Option B:	Unexpected input
Option C:	Configuration bugs
Option D:	Mail Bombs

20.	The system that is configured only to observe and analyze network traffic activity and alert an operator to potential vulnerabilities and attacks is called
Option A:	Active IDS
Option B:	Passive IDS
Option C:	Network-Based IDS
Option D:	Host-Based IDS
21.	Which of the following is the correct TCP three-way handshake process?
Option A:	SYN, SYN-ACK, ACK
Option B:	SYN, SYN-ACK, SYN
Option C:	SYN, ACK-SYN, ACK
Option D:	ACK, SYN-ACK, ACK
22.	What are the three types of scanning?
Option A:	Port, network, and services
Option B:	Port, network, and vulnerability
Option C:	Grey, black, and white hat
Option D:	Server, client, and network
23.	Which type of hacker represents the highest risk to your network?
Option A:	Script kiddies
Option B:	Grey-hat hackers
Option C:	Black-hat hackers
Option D:	Disgruntled employees
24.	Which is NOT a goal of forensic report
Option A:	Report should be ready in time.
Option B:	Contain all information required to explain your conclusions.
Option C:	Be able to withstand a barrage of legal scrutiny.
Option D:	Should not be understandable to decision makers
25.	Recognizing and determining an incident based on network indicators is called
Option A:	Identification
Option B:	Preservation
Option C:	Collection
Option D:	Examination
26.	The system that is configured only to observe and analyze network traffic activity and alert an operator to potential vulnerabilities and attacks is called
Option A:	Active IDS
Option B:	Passive IDS
Option C:	Network-Based IDS
Option D:	Host-Based IDS

27.	Working from a duplicate image does NOT provide
Option A:	Preserves the original digital evidence.
Option B:	Prevents inadvertent alteration of original digital evidence during examination.
Option C:	Allows recreation of the duplicate image, if necessary.
Option D:	Maintains confidentiality of data
28.	When an attacker gets the privilege access or interactive access to the router it is called as?
Option A:	Direct compromise
Option B:	Routing table manipulation
Option C:	Theft of information
Option D:	Denial of service
29.	A bit-by-bit copy of logical storage objects that reside on a logical storage device is refereed as _____
Option A:	Manual acquisition
Option B:	Logical acquisition
Option C:	File system acquisition
Option D:	Physical acquisition
30.	_____ is a scientific method of gathering evidences from digital devices, that can be presented in court of law
Option A:	Network Forensics
Option B:	Computer Forensics
Option C:	Mobile Forensics
Option D:	Digital Forensic
31.	_____ is a important aspect of computer security investigation because it allows investigators to spot unauthorized and unusual on a computer or server
Option A:	Network Forensics
Option B:	Computer Forensics
Option C:	Mobile Forensics
Option D:	Memory Forensics
32.	____ means monitoring the IP headers and TCP headers, without monitoring any contents within the packet themselves
Option A:	Trap And Trace
Option B:	Event Monitoring
Option C:	Full Content Monitoring
Option D:	Both A And B
33.	When an attacker gets the privilege access or interactive access to the router it is called as?
Option A:	Direct compromise

Option B:	Routing table manipulation
Option C:	Theft of information
Option D:	Denial of service
34.	Total steps of writing a report
Option A:	4
Option B:	7
Option C:	8
Option D:	9
35.	Recording the physical scene and duplicating digital evidence using standardized methods and procedures is called
Option A:	Identification
Option B:	Preservation
Option C:	Collection
Option D:	Examination
36.	In-depth systematic search of evidence relating to the network attack is called
Option A:	Identification
Option B:	Preservation
Option C:	Collection
Option D:	Examination
37.	_____ is also called Intrusion Detection and Prevention System (IDPS).
Option A:	Active IDS
Option B:	Passive IDS
Option C:	Network-Based IDS
Option D:	Host-Based IDS
38.	Which word best fits with this definition - officials set up a perimeter around a crime scene?
Option A:	Civilian
Option B:	Math
Option C:	Law Enforcement
Option D:	Police Officer
39.	The evidence and proof that can be obtained from the electronic source is called the…….
Option A:	Digital Evidence
Option B:	Explainable evidence
Option C:	Either A or B
Option D:	Both A and B
40.	If, while searching a computer for evidence of a specific crime, evidence of a

	new, Unrelated crime is discovered, the best course of action is:
Option A:	Abandon the original search, and pursue the new line of investigation
Option B:	Continue with the original search but also pursue the new inquiry
Option C:	Stop the search and obtain a warrant that addresses the new inquiry
Option D:	Continue with the original search, ignoring the new information

Descriptive Questions

10 marks each
1.Explain the phases of incident response Methodology with neat diagram.
2.Explain evidence handling procedure
3.Explain sample structure of incident reporting form.
4.Explain the steps for prevention of cyber crime
5.Explain the term Hacker, Cracker and Phreaker with example
6.Explain in brief various tools available for ethical hacking?
7.What all volatile information which you will be collecting before switching off computer system. Also explain its role in digital forensic investigation.
8.What is Digital Forensics? What are the phases of Digital Forensic process?
9.Define Forensic Duplicate? How you will create Forensic Duplicate of a hard drive
10.Workforce private Limited is a business process outsourcing (BPO) outfit handling business process outsourcing for various clients in North America and Europe. The employees of workforce become privy to confidential customer information during their work. The nature of this information ranges from medical records of individuals to financial data of companies. The unprocessed data is transmitted from client's location to workforce offices in Gurgaon, Pune, and Hyderabad through the internet using VPN (Virtual Private Network) connections on broadband. Workforce allows clients to transfer information via dedicated FTP server on internet, which can then be accessed and processed by its employee's workforce, through its website, workforce.com, allows its clients to log in and view billing and other information specific to them. Access to this information is restricted through the usual username – password combination found on most websites. Looking at the above scenario, discuss the threats workforce faces to its information and suggest controls which it may put in place to secure its information from such threats.
11.What are possible investigation phase carried out in Data Collection and Analysis.
12.Explain importance of forensic duplication and its methods.
13.List and explain in brief steps taken to collect live data from UNIX system
14.Write short notes on Intrusion detection and IPS
15.Explain guidelines for incident report writing. Give one report writing example
16.What are the steps involved in computer evidence handling? Explain in detail.
17.Explain with figure incident response methodology
18.Which types of forensic images created by incident response team for processing? Which one is most preferable

19.Explain the term network forensics, its major goal and function. What are the steps involved in a generic network forensic examination?

5 marks each
1.List and explain the different types of digital evidence
2.What are the challenges in handling evidence?
3.What is the relationship between incident response, incident handling, incident management?
4.Explain the steps in ethical hacking.
5.What is cybercrime? What are the different roles of computer with respects to cybercrime?
6.Discuss the techniques of tracing an email message.
7.Explain how law enforcement is done in computer forensic.
10.List down various Digital Forensic tools and explain one toll with case study example
11.Write short notes on Evidence validation
12.Explain the term; Forensic duplicate, Qualified Forensic Duplicate.
13.Explain technique used to recover the deleted files
14.Explain the phases after detection of an incident