Reg No:__________

A

COURSE CODE: INT250

COURSE TITLE: DIGITAL EVIDENCE ANALYSIS

Time Allowed: 3 hrs **Max. Marks: 70**

Read the following instructions carefully before attempting the question paper.

1. Match the Paper Code shaded on the OMR Sheet with the Paper code mentioned on the question paper and ensure that both are the same.
2. This question paper is divided into two parts A and B.
3. Part A contains 30 questions of 1 mark each. 0.25 marks will be deducted for each wrong answer.
4. Part B contains 5 questions of 10 marks each. Attempt any 4 questions out of these 5 questions. In case all the 5 questions are attempted then only the first four attempted question will be evaluated.
5. Attempt all the questions in serial order.
6. Do not write or mark anything on the question paper except your registration no. on the designated space.
7. After completion of first 90 minutes, the OMR sheet will be taken by the invigilator.
8. Submit the question paper and the rough sheet(s) along with the answer sheet to the invigilator before leaving the examination hall.

Part- A

Q1. 1. Infer the meaning of the statement 'documenting the crime scene'.
a)Cataloging the evidence b)Recording the evidence
c)Monitoring the evidence d)Preserving the evidence L2CO1

2. Show the option which is not included in the incident response process in an event of a cyber security incident.
a)Prepare b)Identify c)Restore d)Relive L2CO1

3. Which of the following relates to successful incident response
a) Isolate exceptions b)Assert, don't assume
c)Take post-incident measures d)All of the above L2CO1

4. Compare an incident response plan and a playbook
a) An incident response plan highlights overall roles and communication requirements; a playbook tells you what actions to take for threats.
b) An incident response plan tells you what actions to take for threats; a playbook highlights overall roles and communication requirements
c) An incident response plan bridges the gap between an organization's policies and procedures and security automation unlike a playbook.
d) An incident response plan defines a predefined set of actions to address a specific security incident unlike a playbook. L2CO1

5. Which of the following relates to Incident response tool?
a)Namios b)Squid Proxy c)USB d)ESF L2CO1

6. Which one of the following statements relates to dealing with Email security breach incident?
a) Deploying hardware, software, and security procedures to lock email.
b) Knowing normal behavior of a network so that one can spot any changes, breaches in the behavior of the network.
c)Phishing is one of the most commonly used methods that is used by hackers to gain access to the network
d)Sending couple of mails to same recipient. L2 CO1

7. Which of the following malware's risk type allows the attacker to access the administrative controls and enables to do almost anything he wants to do with the infected computers?
a)Remote access Trojan (RAT) b)Worms c)Rootkits d)Botnets L2CO1

8. Which of the following refers to a security incident that revolves around malware that locks a computer's files until a user pays a fee?
a)Ransomware b) Human negligence c) Data Breach d)None of these
L2CO2

9. Summarize three catastrophes, data is susceptible to.
a)Theft, becoming outdated, being lost b)Becoming corrupt, becoming outdated, being irrelevant
c)Corruption, sabotage, and loss d)Failure, loss of power, deletion L2CO2

10. Outline the policy that includes both the incident response policy and the disaster recovery plan.
a)Acceptable Use Policy b)Remote Access Policy
c)Change Management Policy d)Business Continuity Plan L2CO2

11. Choose the method that uses stochastic properties of the computer system to investigate activities lacking digital artifacts.
a) Steganography b) Stochastic forensics
c) Both A and B d) Steno forensics L3CO3

12. CCFP identifies with:
a) Cyber Certified Forensics Professional b) Certified Cyber Forensics Professional
c) Certified Cyber Forensics Program d) Certified Cyber Forensics Product L3CO3

13. Volatile data resides in?
a) Registries b) Cache c) RAM d) All of the above L3CO3

14. Identify the tools that create qualified forensic duplicate output files.
a)Safe Back b) EnCase c) FTK Imager d) All of the above
L3CO3

15. Choose the option that is a type of volatile information collected in digital forensics.
a)System time b)Logged-on user(s) c)Open files d)All of the above
L3CO3

16. Examine the role of eliminating the potential clues in network and select option from below:
a) To clear the configuration settings from networking equipment.
b) It can provide crucial clues to a security cracker to break into our network and the systems that reside on it.
c) Both A and B
d) None of the above L4CO4

17. Inspect and select the permission of system administrators on their network when it is necessary to protect the network and the data it contains.
a) Open unread e-mails. b) Monitor network traffic.
c) Modify system logs. d) Divulge user personal information.
L4CO4

18. Analyze the type of attack, when a hacker attempts to attack a host via the Internet.
a) Remote attack b) Physical access c) Local access d)Internal attack
L4CO4

19. Discover tcpdump tool and choose correct option
a) is a popular, lightweight command line tool b) captures packets
c) Analyzes network traffic d) All of the above L4CO4

20. You have successfully comprised a server having an IP address of 10.10.0.5. You would like to enumerate all machines in the same network quickly for network monitoring. What is the best Nmap command you will use?
a. nmap -T4 -q 10.10.0.0/24 b. nmap -T4 -F 10.10.0.0/24
c. nmap -T4 -r 10.10.1.0/24 d. nmap -T4 -O 10.10.0.0/24
L4CO4

21. Compare dcfldd and dd with correct option.
a)dcfldd supports the hashing of data when disk images are created contrary to dd
b)dd allows verification that the contents of the image have not been modified since the image was acquired contrary to dcfldd
c)dcfldd allows verification that the contents of the image have not been modified since the image was acquired contrary to dd.
d)Both a and c L4CO5

22. Omit the tool that cannot recover deleted files in computer forensics.
a)Autopsy b)Post mortem c) EaseUs d)Recuva L4CO5

23. A switch sending a copy of network packets to a monitoring network connection is called as
a) Port Mirroring b) Disk Mirroring c) Drive Mirroring d)RouterMirroring L4CO5

24. An attacker, using a rogue wireless AP, performed an MITM attack and injected an HTML code to embed a malicious applet in all HTTP connections. When users accessed any page, the applet ran and exploited many machines. What kind of tool is used by hacker in mentioned attack evidence?
a) Wireshark b) Ettercap c) Aircrack-ng d) Tcpdump L4CO5

25. The ELK stack is an acronym used to describe a collection of three open-source projects
a) Elasticsearch, Logstash, Kibana b)Evensearch, Logstash, Kibana
c) Elasticsearch, Logstack, Kibana d) Oddsearch, Logstack, Kibana L4CO5

26. Choose among the following principles states that sometimes it becomes more desirable to rescore the details of intrusion that to adopt more efficient measure to avoid it?
a)Least common mechanism b)Compromise recording
c)Psychological acceptability d)Work factor L5CO6

27. Decide the incorrect from the following statement in context to resource as in information availability.
a) By resource as in information availability, we can remove the single point of failure.
b) DoS attacks on the control system do not impact its availability.
c) Redundancy ensures that the system can operate in case of DoS attacks.
d) Ensuring backup systems is also part of resource availability L5CO6

28. Prioritize four major essential components of network security in light of investigation.
a) IPS, Firewall, NAC, SIEM b) IPS, Network Switch, SIEM, IDS
c) Router, IDS, NAC, HMI d) IDS, IPS, Server, Router L5CO6

29. Mark the one that is not an element in the computer forensic report template?
a) Executive summary b) Computer evidence analyzed
c) Attacker methodology d) Vision of the organization L5CO6

30. Conclude the role of router as response tool by the fact:
a) They can be targets of attack
b) They can be stepping-stones for attackers
c) They can provide valuable information and evidence that allow investigators to resolve complex network incidents.
d) They have limited storage capacity L5CO6

Part-B

Q.2 Illustrate the incident handling process highlighting the framework and components of incident response. L2CO1[10 Marks]

Q.3 Demonstrate the steps involved in incident response by formulating a response strategy in case of cyber attack of your own choice. L2 CO2[10 Marks]

× Q.4 Develop a response toolkit in context of live data collection. Justify that forensic duplicates are crucial and admissible evidence by quoting illustrative tools examples. L3CO3[10 Marks]

Q.5 Categorize local and remote acquisition in light of memory acquisition as host based evidence and compare features and merits of both. Give an illustrative example to perform a trap and trace for collecting network based evidence. L4 CO4 [10 Marks]

× Q.6 Classify and compare major data analysis techniques for digital forensic analysis highlighting tools, merits and limitations of each with suitable real life examples. L4CO5[10 Marks]

Q.7 Explain in detail the guidelines and template for computer forensic report taking suitable incidents and digital evidences of your own choice. L5 CO6 [10 Marks]

--- End of Question Paper ---