ion No.: [redacted]

Paper Code:A

Course Code:INT242

Course Title:CYBER SECURITY ESSENTIALS

Time Allowed: 01:30hrs.

Max Marks: 30

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 contains 30 questions of 1 mark each. 0.25 marks will be deducted for each wrong answer.

3. All questions are compulsory.

4. Do not write or mark anything on the question paper and/or on rough sheet(s) which could be helpful to any student in copying, except your registration number on the designated space.

5. Submit the question paper and the rough sheet(s) along with the OMR sheet to the invigilator before leaving the examination hall.

Q1) ______________ implies that specific information should only be known by specific individuals.

(a) Confidentiality (b) Integrity (c) Availability (d) None of the above

CO1, L2

Q2) ______________ signifies that the data is delivered and stored in the intended manner, and that any modifications are approved.

(a) Confidentiality (b) Integrity (c) Availability (d) None of the above

CO1, L2

Q3) ______________ means that those with permission to see or alter the information can access it.

(a) Confidentiality (b) Integrity (c) Availability (d) None of the above

CO1, L2

Q4) ______________ a site where security experts keep watch over and safeguard vital information assets across different business departments, including finance, operations, sales/marketing, and others.

(a) Security Operations Center (SOC) (b) Development and operations (DevOps)

(c) Cyber incident response team (CIRT) (d) Computer security incident response team (CSIRT)

CO1, L2

Q5) ______________ is a flaw that could be unintentionally or maliciously exploited to compromise security.

(a) Vulnerability (b) Threat (c) Risk (d) None of the above

CO1, L2

Q6) ______________ is the probability that something or someone will take advantage of a weakness and compromise security.

(a) Vulnerability (b) Threat (c) Risk (d) None of the above

CO1, L2

Q7) ______________ is the possibility and effect (or result) of a threat actor taking advantage of a weakness.

(a) Vulnerability (b) Threat (c) Risk (d) None of the above

CO1, L2

) Anyone without a valid account or authorization to access the target system is considered an ______________ threat actor or agent.

(a) External (b) Internal (c) Vulnerable (d) All of the above

CO1, L2

Q9) One who has been given access to the system is referred to as an ______________ threat actor.

(a) External (b) Internal (c) Vulnerable (d) All of the above

CO1, L2

Q10) The entire area where a threat actor could attempt to exploit a vulnerability is known as the ____________
[✓ (a) Attack surface] (b) Attack vector (c) Threat actor (d) All of the above

Q11) Which of the following define the grant sufficient rights (to users) to perform his or her job and no more? CO1, L2
(A) No Privilege (b) More Privilege (c) Least Privilege [✓ (d) Maximum Privilege]

Q12) Identify which of the following tasks and processes involved in onboarding include? CO2, L4
(a) Secure transmission of credentials (b) Asset allocation (c) Training/policies [✓ (d) All Above]

Q13) Statement: The Local Security Authority (LSA) compares the submitted credential to a hash stored in the Security Accounts Manager (SAM) database, which is part of the registry, refers to what? CO2, L4
(a) Windows local sign in (b) Windows network sign in (c) Remote sign in (d) Remote network sign in

Q14) Hybrid password attack uses a combination of: CO2, L4
(a) Dictionary Attack (b) Brute-force attacks [✓ (c) Dicitinary and brute-force attacks] (d) None of these

Q15) Creating an account or ID that uniquely represents the user, device, or process on the network is known as: CO2, L4
(a) Authentication [✓ (b) Identification] (c) Authorization (d) Accounting

Q16) Authentication design refers to selecting a technology that meets requirements for: CO2, L4
(a) Confidentiality (b) Integrity (c) Availability (d) All Above

Q17) Obfuscation is the art of making a message ____________ to understand. CO2, L4
(a) Easy (b) Difficult [✓ (c) as plain text that will be easy to] (d) None of these

Q18) A downgrade attack can be used to facilitate a man-in-the-middle attack by requesting that the server use a: CO2, L4
(a) Lower specification protocol (b) Weaker ciphers (c) Weaker key lengths. [✓ (d) All Above]

Q19) Which of the following refers to stream cipher? CO2, L4
(a) Ensures thekey produces a same ciphertext from the same plaintext.
[✓ (b) Each byte or bit of data in the plaintext is encrypted one at a time.]
(c) Plaintext is divided into equal-size blocks
(d) Uses Padding CO2, L4

Q20) Symmetric encryption is very _____ and it is used for _____ encryption of large amounts of data.
(a) fast,bulk (b) slow, small (c) slow,fast [✓ (d) slow,bulk]

Q21) Which is true of a signature-based IDS? CO2, L4
(a) It cannot work with an IPS (b) It only identifies known signatures
(c) It detects never-before-seen anomalies (d) It works best in large enterprises. CO3, L2

Q22) Which is true about a false positive?

(a) An alert that indicates nefarious activity

(b) An alert that indicates nefarious activity on a system that, upon further inspection, turns out to represent legitimate network traffic

(c) The lack of an alert for nefarious activity on a system that, upon further inspection, turns out to truly be nefarious activity

(d) All of these

CO3, L2

Q23) Statement I: Uses a definition of expected patterns to events.
Statement II: Identifies events that don't follow these patterns
The above two statements ary true for which type of Network Monitoring system?

(a) Signature-based [✓ (b) Anomaly-based] (c) Behavior-based (d) Heuristic

CO3, L2

Q24) Which among the following can mask your IP address?

(a) Firewall (b) Antivirus (c) Virtual Private Network (d) Incognito mode

CO3, L2

Q25) Which among the following are the Examples for Mailbox access protocols?

(a) Post Office Protocol (POP3), Internet Message Access Protocol (IMAP)

(b) Post Office Protocol (POP3), SSH FTP (SFTP)

(c) Internet Message Access Protocol (IMAP), Secure Real-time Transport Protocol (SRTP)

(d) All of these

CO3, L2

Q26) _______________ is an isolation practice of dividing a network into multiple subnets

(a) Network isolation (b) Network segregation [✓ (c) Subnetting] (d) Network Access Control

CO1, L1

Q27) _____________ is a more recent email protocol that improves upon Post Office Protocol's shortcomings

(a) Multipurpose Internet Mail Extensions (b) Real-Time Transport Protocol

(c) Internet Message Access Protocol (d) Dynamic Host Configuration Protocol

CO1, L2

Q28) Signs packet but does not encrypt payload Provides authentication/integrity only These two statements are true for?

(a) Authentication Header (AH) (b) Encapsulation Security Payload (ESP)

(c) Encapsulation Packet Payload (EPP) (d) Authentication Payload

CO1, L2

Q29) •Act to deny (block or drop), log, or accept a packet
•Inspect headers of individual packets
These two statements are true for which of the following?

(a) Enforcing a network across control list (ACL) (b) Enforcing a network access control list (ACL)

(c) Enforcing a network access configure list (ACL) (d) Enforcing a network access cost list (ACL)

CO1, L2

Q30) Which among the following is an Active response to threats?

(a) Reset session (b) Apply firewall filters on the fly to shun traffic (c) Bandwidth throttling (d) All of these

CO1, L2

--End of Question paper--