Total Pages-16

SECCS–03

1st Semester Examination Session December, 2024

Cyber Security Technique

Time : **2:00** Hrs. Max. Marks : **40**

समय : **2:00** घण्टा अधिकतम अंक : **40**

Roll No. (in Figures) :
अनुक्रमांक अंकों में : ....
Roll No. (in Words) : ....
अनुक्रमांक शब्दों में : ....
Examination Centre : ....
परीक्षा केन्द्र : ....

Invigilator's Signature / पर्यवेक्षक के हस्ताक्षर

Do not open the Booklet until you are asked to do so.
जब तक कहा न जाये, पुस्तिका न खोलें।
First Read all the instructions.
पहले सभी निर्देशों को पढ़ लें।

Important Instructions :

1. This paper consists of **40** Multiple Choice Questions (M.C.Q.). All questions are compulsory and carry **1** mark each. There is not negative marking.
2. Each question has four alternative responses marked (A), (B), (C) and (D). You have to choose an appropriate answer option and mark it on the OMR sheet.
3. For marking answers on OMR sheet, follow the detailed instructions given on the OMR Sheet.
4. Use only Blue or Black ball point pen for marking on OMR.

महत्वपूर्ण निर्देश :

1. इस प्रश्न–पत्र में **40** बहुविकल्पीय प्रश्न हैं। सभी प्रश्न अनिवार्य हैं व प्रत्येक प्रश्न **1** अंक का है। गलत उत्तर के लिए अंक नहीं काटे जायेंगे।
2. प्रत्येक प्रश्न के चार उत्तर विकल्प (A), (B), (C) एवं (D) दिए गए हैं। आपको उपयुक्त उत्तर विकल्प का चुनाव कर उत्तर ओ.एम.आर. प्रपत्र पर अंकित करना है।
3. ओ.एम.आर. प्रपत्र पर अपने सही उत्तर को चिह्नित करने के लिए प्रपत्र पर अंकित निर्देशों का पालन कीजिए।
4. ओ.एम.आर. पर चिह्न लगाने के लिए केवल नीली या काली बॉल प्वॉइन्ट पैन का ही इस्तेमाल कीजिए।

1. What is the primary purpose of an IT security policy ?

(A) To increase IT budget

(B) To define security protocols

(C) To make systems complex

(D) To enhance user experience

2. Which of the following is an example of physical security ?

(A) Antivirus software

(B) Firewall

(C) Security guards

(D) Encryption

3. What does “PGP” stand for in e-mail security ?

(A) Pretty Good Privacy

(B) Personal Group Policy

(C) Private Gateway Protocol

(D) Public Group Protection

4. Which of the following is a type of insider attack ?

(A) Phishing

(B) Malware injection

(C) Data theft by employees

(D) Ransomware

1. IT सुरक्षा नीति का प्राथमिक उद्देश्य क्या है ?

(A) IT बजट बढ़ाना

(B) सुरक्षा प्रोटोकॉल को परिभाषित करना

(C) सिस्टम को जटिल बनाना

(D) उपयोगकर्ता अनुभव को बढ़ाना

2. निम्नलिखित में से कौन भौतिक सुरक्षा का उदाहरण है ?

(A) एंटीवायरस सॉफ्टवेयर

(B) फायरवॉल

(C) सुरक्षा गार्ड

(D) एन्क्रिप्शन

3. ई–मेल सुरक्षा में “PGP” का पूर्ण रूप क्या है ?

(A) प्रिटी गुड प्राइवेसी

(B) पर्सनल ग्रुप पॉलिसी

(C) प्राइवेट गेटवे प्रोटोकॉल

(D) पब्लिक ग्रुप प्रोटेक्शन

4. निम्नलिखित में से कौन इनसाइडर अटैक का प्रकार है ?

(A) फिशिंग

(B) मैलवेयर इंजेक्शन

(C) कर्मचारियों द्वारा डेटा चोरी

(D) रैनसमवेयर

5. Which type of IDS focuses on analysing network traffic ?

(A) Host-based IDS

(B) Network-based IDS

(C) Signature-based IDS

(D) Behavior-based IDS

6. IDS is an abbreviation for :

(A) Intrusion detection system

(B) Internet detection system

(C) Intervention detection system

(D) Interface detection system

7. What does the McCumber Cube represent ?

(A) Security policies

(B) Dimensions of cybersecurity

(C) Types of malwares

(D) Risk assessment tools

8. Which wireless security protocol is considered outdated ?

(A) WPA2

(B) WPA

(C) WEP

(D) WPA3

5. कौन सा IDS नेटवर्क ट्रैफिक का विश्लेषण करने पर ध्यान केंद्रित करता है ?

(A) होस्ट–आधारित IDS

(B) नेटवर्क–आधारित IDS

(C) सिग्नेचर–आधारित IDS

(D) बिहेवियर–आधारित IDS

6. IDS किसका संक्षिप्त रूप है :

(A) इन्ट्रूजन डिटेक्शन सिस्टम

(B) इंटरनेट डिटेक्शन सिस्टम

(C) इंटरवेंशन डिटेक्शन सिस्टम

(D) इंटरफेस डिटेक्शन सिस्टम

7. McCumber Cube क्या दर्शाता है ?

(A) सुरक्षा नीतियाँ

(B) साइबर सुरक्षा के आयाम

(C) मैलवेयर के प्रकार

(D) जोखित आकलन उपकरण

8. कौन सा वायरलेस सुरक्षा प्रोटोकॉल पुराना (कालग्रस्त) माना जाता है ?

(A) WPA2

(B) WPA

(C) WEP

(D) WPA3

9. What is the primary function of ''spyware'' ?

(A) To collect user information without their knowledge.

(B) Provide free software tools

(C) Boost system performance

(D) Protect user passwords

10. Which type of malware disguises itself as legitimate software ?

(A) Worm

(B) Trojan horse

(C) Virus

(D) Spyware

11. Which is an example of mobile malware ?

(A) Email virus

(B) Android ransomware

(C) File virus

(D) Rootkit

9. ''स्पाइवेयर'' का प्राथमिक कार्य क्या है ?

(A) उपयोगकर्ता की जानकारी के बिना उनकी जानकारी एकत्र करना।

(B) मुफ्त सॉफ्टवेयर उपकरण प्रदान करें।

(C) सिस्टम प्रदर्शन को बढ़ावा देना।

(D) उपयोकर्ता पासवर्ड सुरक्षित रखें।

10. कौन सा मैलवेयर वैध सॉफ्टवेयर के रूप में प्रच्छन्न होता है ?

(A) वर्म

(B) ट्रोजन हॉर्स

(C) वायरस

(D) स्पायवेयर

11. मोबाइल मैलवेयर का एक उदाहरण क्या है ?

(A) ईमेल वायरस

(B) एंड्रॉइड रैनसमवेयर

(C) फाइल वायरस

(D) रूटकिट

12. What is the primary aim of a rootkit ?

(A) Steal passwords

(B) Gain unauthorized control

(C) Infect emails

(D) Encrypt files

13. What is XSS ?

(A) Cross-Site Scripting

(B) XML Security Standards

(C) External Site Security

(D) Cross-Site Software

14. Which protocol ensures secure communication on the web ?

(A) HTTP

(B) FTP

(C) HTTPS

(D) SMTP

15. What is "vishing" ?

(A) Phishing via SMS

(B) Phishing via phone calls

(C) Phishing via emails

(D) Phishing via web pop-ups

12. रूटकिट का मुख्य उद्देश्य क्या है ?

(A) पासवर्ड चुराना

(B) अनधिकृत नियंत्रण प्राप्त करना

(C) ईमेल संक्रमित करना

(D) फाइलों को एन्क्रिप्ट करना

13. XSS क्या है ?

(A) क्रॉस-साइट स्क्रिप्टिंग

(B) XML सुरक्षा मानक

(C) बाहरी साइट सुरक्षा

(D) क्रॉस-साइट सॉफ्टवेयर

14. कौन सा प्रोटोकॉल वेब पर सुरक्षित संचार सुनिश्चित करता है ?

(A) HTTP

(B) FTP

(C) HTTPS

(D) SMTP

15. ''विशिंग'' क्या है ?

(A) एसएमएस के माध्यम से फिशिंग

(B) फोन कॉल के माध्यम से फिशिंग

(C) ईमेल के माध्यम से फिशिंग

(D) वेब पॉप-अप के माध्यम से फिशिंग

16. Which tool is often used for social engineering attacks ?

(A) Firewalls

(B) Email spoofing tools

(C) Antivirus software

(D) Network routers

17. What does NCIIPC focus on ?

(A) Critical Infrastructure Protection

(B) Financial Transactions

(C) Wireless Communication

(D) Cloud Storage

18. Which county developed the "International Strategy for Cyberspace" ?

(A) United States

(B) Russia

(C) UAE

(D) Germany

16. सामाजिक इंजीनियरिंग हमलों के लिए अक्सर कौन सा उपकरण उपयोग किया जाता है ?

(A) फायरवॉल

(B) ईमेल स्पूफिंग टूल

(C) एंटीवायरस सॉफ्टवेयर

(D) नेटवर्क राउटर

17. NCIIPC का ध्यान किस पर है ?

(A) महत्वपूर्ण बुनियादी ढ़ांचा सुरक्षा

(B) वित्तीय लेन–देन

(C) वायरलेस संचार

(D) क्लाउड स्टोरेज

18. किस देश ने ''साइबरस्पेस के लिए अंतर्राष्ट्रीय रणनीति'' विकसित की ?

(A) संयुक्त राज्य अमेरिका

(B) रूस

(C) संयुक्त अरब अमीरात

(D) जर्मनी

19. Which cybersecurity principle ensures that data is not altered ?

(A) Confidentiality

(B) Integrity

(C) Availability

(D) Authentication

20. What does "pharming" attack involve ?

(A) Redirecting users to fraudulent websites

(B) Sending phishing emails

(C) Encrypting user files

(D) Exploiting wireless networks

21. What is the primary feature of a "zero-day attack" ?

(A) Attack occurs after system patches are applied

(B) Exploits vulnerabilities before they are patched

(C) Targets physical systems

(D) Relies on user error for execution.

19. कौन सा साइबर सुरक्षा सिद्धान्त डेटा को परिवर्तित न होने की गारंटी देता है ?

(A) गोपनीयता

(B) अखण्डता

(C) उपलब्धता

(D) प्रमाणीकरण

20. ''फार्मिंग'' हमला क्या करता है ?

(A) उपयोगकर्ताओं को धोखाधड़ी वाली वेबसाइटों पर पुनर्निर्देशित करना

(B) फिशिंग ईमेल भेजना

(C) उपयोगकर्ता फाइलों को एन्क्रिप्ट करना

(D) वायरलेस नेटवर्क का उपयोग करना

21. ''जीरो-डे हमला'' की मुख्य विशेषता क्या है ?

(A) हमला सिस्टम पैच लागू होने के बाद होता है

(B) कमजोरियों का पैच से पहले उपयोग करता है

(C) भौतिक सिस्टम को लक्षित करता है

(D) निष्पादन के लिए उपयोगकर्ता त्रुटि पर निर्भर करता है

22. What does a "DDoS" attack aim to do ?

(A) Encrypt sensitive data

(B) Overwhelm a network with traffic

(C) Steal user credentials

(D) Redirect email communications

23. Which protocol is often used for secure remote login ?

(A) FTP

(B) SSH

(C) HTTP

(D) POP3

24. What is the role of multi-factor o authentication (MFA) ?

(A) To bypass network firewalls

(B) To enhance user security

(C) To simplify login processes

(D) To encrypt files

22. "DDoS" हमला किस उद्देश्य से किया जाता है ?

(A) संवेदनशील डेटा एन्क्रिप्ट करना

(B) नेटवर्क को ट्रैफिक से भर देना

(C) उपयोगकर्ता क्रेडेंशियल चुराना

(D) ईमेल संचार को पुनर्निर्देशित करना

23. सुरक्षित रिमोट लॉगिन के लिए कौन सा प्रोटोकॉल सामान्यतः उपयोग किया जाता है ?

(A) FTP

(B) SSH

(C) HTTP

(D) POP3

24. मल्टी–फैक्टर ऑथेंटिकेशन (MFA) की भूमिका क्या है ?

(A) नेटवर्क फायरवॉल को बाईपास करना

(B) उपयोगकर्ता सुरक्षा को बढ़ाना

(C) लॉगिन प्रक्रिया को सरल बनाना

(D) फाइलों को एन्क्रिप्ट करना

25. Which component is crucial in a secure email communication system ?

(A) DNS server

(B) SMTP relay

(C) Encryption

(D) MAC address

26. What is "ransomware" primarily used for ?

(A) Gain unauthorized network access

(B) Encrypt data for ransom

(C) Deliver spam emails

(D) Exploit hardware vulnerabilities

27. What is "keylogging" ?

(A) A method to block access to websites

(B) Recording keystrokes to capture sensitive information

(C) Encrypting sensitive files

(D) Monitoring network traffic

25. सुरक्षित ईमेल संचार प्रणाली में कौन सा घटक महत्वपूर्ण है ?

(A) DNS सर्वर

(B) SMTP रिले

(C) एन्क्रिप्शन

(D) मैक एड्रेस

26. ''रैनसमवेयर'' का मुख्य उपयोग क्या है ?

(A) अनधिकृत नेटवर्क एक्सेस प्राप्त करना

(B) फिरौती के लिए डेटा एन्क्रिप्ट करना

(C) स्पैम ईमेल वितरित करना

(D) हार्डवेयर कमजोरियों का उपयोग करना

27. ''कीलॉगिंग'' क्या है ?

(A) वेबसाइटों तक पहुंच को ब्लॉक करने की विधि

(B) संवेदनशील जानकारी को कैप्चर करने के लिए की स्ट्रोक्स को रिकॉर्ड करना

(C) संवेदनशील फाइलों को एन्क्रिप्ट करना

(D) नेटवर्क ट्रैफिक की निगरानी करना

28. Which is a common risk assessment methodology ?

(A) NIST SP 800-30

(B) SQL Injection

(C) WPA Protocol

(D) DNS Spoofing

29. Which framework is commonly used in cybersecurity risk management ?

(A) NIST Cybersecurity Framework

(B) HTML Framework

(C) PHP Development Framework

(D) Blockchain Framework

30. What does the "C" in COBRA methodology stand for ?

(A) Cybersecurity

(B) Control

(C) Comprehensive

(D) Critical

28. जोखिम मूल्यांकन की एक सामान्य पद्धति कौन सी है ?

(A) NIST SP 800-30

(B) SQL इंजेक्शन

(C) WPA प्रोटोकॉल

(D) DNS स्पूफिंग

29. साइबर सुरक्षा जोखिम प्रबंधन में सामान्यतः कौन सा फ्रेमवर्क उपयोग किया जाता है ?

(A) NIST साइबर सुरक्षा फ्रेमवर्क

(B) HTML फ्रेमवर्क

(C) PHP विकास फ्रेमवर्क

(D) ब्लॉकचेन फ्रेमवर्क

30. COBRA पद्धति में "C" का क्या अर्थ है?

(A) साइबर सुरक्षा

(B) नियंत्रण

(C) व्यापक

(D) महत्वपूर्ण

31. Which tool is used for threat agent risk assessment ?

(A) TARA

(B) WPA2

(C) SQL Map

(D) OWASP ZAP

32. Which tool is commonly used to create a disk image ?

(A) FTK Imager

(B) Wireshark

(C) Kali Linux

(D) Burp Suite

33. Which organization oversees CERT-In ?

(A) Reserve Bank of India

(B) Ministry of Finance

(C) Ministry of Home Affairs

(D) Ministry of Electronics and IT

34. Which type of malware is designed to secretly monitor user activity ?

(A) Adware

(B) Spyware

(C) Worm

(D) Ransomware

31. खतरे वाले एजेंट जोखिम मूल्यांकन के लिए कौन सा उपकरण उपयोग किया जाता है ?

(A) TARA

(B) WPA2

(C) SQL मैप

(D) OWASP ZAP

32. डिस्क छवि बनाने के लिए सामान्यत: कौन सा उपकरण उपयोग किया जाता है ?

(A) FTK इमेजर

(B) वायर्शार्क

(C) काली लिनक्स

(D) बर्प सूट

33. कौन सा संगठन CERT-In की निगरानी करता है ?

(A) भारतीय रिजर्व बैंक

(B) वित्त मंत्रालय

(C) गृह मंत्रालय

(D) इलेक्ट्रॉनिक्स और आईटी मंत्रालय

34. कौन सा मैलवेयर उपयोगकर्ता गतिविधि को गुप्त रूप से मॉनिटर करने के लिए डिजाइन किया गया है ?

(A) एडवेयर

(B) स्पायवेयर

(C) वर्म

(D) रैनसमवेयर

35. What is "SQL injection" primarily used to exploit ?

(A) Web application vulnerabilities

(B) Network protocols

(C) Hardware configurations

(D) Antivirus software

36. Which cryptographic method ensures secure key exchange over public networks ?

(A) RSA

(B) AES

(C) DES

(D) MD5

37. CERT Stands for :

(A) Computer Emergency Response Team

(B) Central Emergency Response Team

(C) Collaborative Emergency Response Team.

(D) Call Emergency Response Team

35. SQL इंजेक्शन का मुख्य रूप से उपयोग किसे शोषित करने के लिए किया जाता है ?

(A) वेब एप्लिकेशन कमजोरियाँ

(B) नेटवर्क प्रोटोकॉल

(C) हार्डवेयर कॉन्फिगरेशन

(D) एंटीवायरस सॉफ्टवेयर

36. कौन सा क्रिप्टोग्राफिक विधि सार्वजनिक नेटवर्क पर सुरक्षित कुंजी विनिमय सुनिश्चित करता है ?

(A) RSA

(B) AES

(C) DES

(D) MD5

37. CERT का मतलब है :

(A) कम्प्यूटर आपातकालीन प्रतिक्रिया टीम

(B) केन्द्रीय आपातकालीन प्रतिक्रिया टीम

(C) सहयोगात्मक आपातकालीन प्रतिक्रिया टीम

(D) आपातकालीन प्रतिक्रिया टीम को बुलाओ

38. The critical sectors include Defense, Finance, Energy, Transportation and :

(A) Remediation

(B) Confidentiality

(C) Countering

(D) Telecommunications

38. महत्वपूर्ण क्षेत्रों में रक्षा, वित्त, ऊर्जा, परिवहन और शामिल हैं :

(A) निवारण

(B) गोपनीयता

(C) प्रतिकार करना

(D) दूरसंचार

39. WEP stands for :

(A) Wired Equivalent Privacy

(B) Wireless Equity Privacy

(C) Wired Equity Privacy

(D) Wireless Equivalent Privacy

39. WEP का मतलब है :

(A) वायर्ड इक्विवेलेंट प्राइवेसी

(B) वायरलेस इक्विटी प्राइवेसी

(C) वायर्ड इक्विटी प्राइवेसी

(D) वायरलेस इक्विवेलेंट प्राइवेसी

40. EXITO stands for :

(A) Exercise event Injection Toolkit

(B) Event Injection Toolkit

(C) Event Intrusion Toolkit

(D) Emergency event Injection Toolkit

40. EXITO का मतलब है :

(A) Exercise इवेंट इंजेक्शन टूलकिट

(B) इवेंट इंजेक्शन टूलकिट

(C) इवेंट इंट्रूज़न टूलकिट

(D) इमरजेंसी इवेंट इंजेक्शन टूलकिट

Rough Work/रफ कार्य

Rough Work/रफ कार्य