A-1152

No. of Pages: 16

SECCS-03

Cyber Security Technique

Examination, 2025 (June)

Time: 2 Hours

Max Mark: 40

Roll No. (In figures):--

अनुक्रमांक अंकों में

Roll No. (in words) :---

अनुक्रमांक शब्दों में

Examination Centre: --

परीक्षा केन्द्र

Invigilator's Signature

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 / महत्वपूर्ण निर्देश

1. This paper consists of 40 multiple choice questions (M.C.Q.). All questions are Compulsory and carry 01 mark each. There is no negative marking.
   इस प्रश्न पत्र में 40 बहुविकल्पीय प्रश्न हैं। सभी प्रश्न अनिवार्य हैं व प्रत्येक प्रश्न 01 अंक का है। गलत उत्तर के लिए अंक नहीं काटे जायेंगे।
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.
   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. For marking answers on OMR sheet, follow the detailed instructions given on the OMR Sheet.
   ओ0एम0आर0 प्रपत्र पर अपने सही उत्तर को चिन्हित करने के लिए प्रपत्र पर अंकित निर्देशों का पालन कीजिए।
4. Use only Blue or Black ball point pen for marking on OMR.
   ओ0एम0आर0 पर चिन्ह लगाने के लिए केवल नीली या काली बॉल प्वॉइन्ट पैन का ही इस्तेमाल कीजिए।

P.T.O.

1. MIME stands for

A. Main Internet Mail Extension.

B. Measure Internet Mail Extension

C. Maximum Internet Mail Extension.

D. Multipurpose Internet Mail extensions.

MIME का मतलब है

A. मेन इंटरनेट मेल एक्सटेंशन।

B. मेजर इंटरनेट मेल एक्सटेंशन।

C. मैक्सिमम इंटरनेट मेल एक्सटेंशन।

D. मल्टीपरपज इंटरनेट मेल एक्सटेंशन।

2. Hackers who help in finding bugs and vulnerabilities in a system & don't intend to crack a system are termed as

A. Black Hat hackers

B. White Hat Hackers

C. Grey Hat Hackers

D. Red Hat Hackers

हैकर्स जो सिस्टम में बग्स और कमजोरियों को ढूंढने में मदद करते हैं और सिस्टम को हैक करने का इरादा नहीं रखते हैं, उन्हें कहा जाता है:

A. ब्लैक हैट हैकर्स

B. व्हाइट हैट हैकर्स

C. ग्रे हैट हैकर्स

D. रेड हैट हैकर्स

3. Which is the legal form of hacking based on which jobs are provided in IT industries and firms?

A. Cracking

B. Non ethical Hacking

C. Ethical hacking

D. Hactivism

हैकिंग का कौन सा कानूनी रूप है जिसके आधार पर आईटी उद्योगों और फर्मों में नौकरियां प्रदान की जाती हैं?

A. क्रैकिंग

B. गैर नैतिक हैकिंग

C. एथिकल हैकिंग

D. सक्रियतावाद

4. Which one of the following can be considered as the class of computer threats?

A. Dos Attack

B. Phishing

C. Soliciting

D. Both A and C

निम्नलिखित में से किसे कंप्यूटर खतरों का वर्ग माना जा सकता है?

A. Dos अटैक

B. फ़िशिंग

C. सॉलिसिटिंग

D. A और C दोनों

5. A software that filters all data packets coming through the internet, a network, etc. is known as

A. Antivirus

B. Firewall

C. Cookies

D. Malware

P.T.O.

एक सॉफ्टवेयर प्रोग्राम जो इंटरनेट, नेटवर्क आदि के माध्यम से आने वाले सभी डेटा पैकेट को फ़िल्टर करता है, कहलाता है

A. एंटीवायरस

B. फ़ायरवॉल

C. कुकीज़

D. मैलवेयर

6. In which of these a person is continually chased/followed by another person or a group of various people?

A. Identity theft

B. Stalking

C. Bullying

D. Phishing

इनमें से किसमें एक व्यक्ति का दूसरे व्यक्ति या विभिन्न लोगों के समूह द्वारा लगातार पीछा किया जाता है?

A. आइडेंटिटी थेफ्ट

B. स्टॉकिंग

C. बुलिंग

D. फ़िशिंग

7. Which type of policy defines secure methods for remote connectivity?

A. Access Control Policy

B. Acceptable Use Policy

C. Remote Access Policy

D. Incident Response Policy

कौन सी नीति दूरस्थ कनेक्टिविटी के लिए सुरक्षित विधियों को परिभाषित करती है?

A. एक्सेस कंट्रोल पॉलिसी

B. स्वीकार्य उपयोग नीति

C. रिमोट एक्सेस नीति

D. घटना प्रतिक्रिया नीति

8. Which cryptographic technique ensures data integrity and authenticity?

A. PGP

B. MAC

C. MIME

D. Firewall

कौन सी क्रिप्टोग्राफिक तकनीक डेटा अखंडता और प्रामाणिकता सुनिश्चित करती है?

A. PGP

B. MAC

C. MIME

D. फायरवॉल

9. What is an example of malicious software?

A. Firewall

B. Virus

C. MAC

D. Security Token

P.T.O.

हानिकारक सॉफ़्टवेयर का एक उदाहरण क्या है?

A. फायरवॉल

B. वायरस

C. MAC

D. सुरक्षा टोकन

10. What is an example of physical security control?

A. Surveillance cameras

B. Data encryption

C. Firewall configuration

D. Remote access policies

भौतिक सुरक्षा नियंत्रण का एक उदाहरण क्या है?

A. निगरानी कैमरे

B. डेटा एन्क्रिप्शन

C. फायरवॉल कॉन्फ़िगरेशन

D. रिमोट एक्सेस नीतियां

11. What is the primary function of a security token?

A. Encrypting network traffic

B. Authenticating user identity

C. Detecting phishing attacks

D. Configuring firewalls

सुरक्षा टोकन का मुख्य कार्य क्या है?

A. नेटवर्क ट्रैफिक को एन्क्रिप्ट करना

B. उपयोगकर्ता पहचान का प्रमाणीकरण करना

C. फ़िशिंग हमलों का पता लगाना

D. फायरवॉल को कॉन्फ़िगर करना

12. What is the purpose of Multipurpose Internet Mail Extensions (MIME)?

A. To encrypt emails

B. To format multimedia content in emails

C. To authenticate message integrity

D. To block spam emails

मल्टीपर्पज इंटरनेट मेल एक्सटेंशन (MIME) का उद्देश्य क्या है?

A. ईमेल को एन्क्रिप्ट करना

B. ईमेल में मल्टीमीडिया सामग्री को प्रारूपित करना

C. संदेश की अखंडता को प्रमाणित करना

D. स्पैम ईमेल को ब्लॉक करना

13. What is the primary goal of a cybercrime?

A. To improve network performance

B. To cause financial, reputational, or data harm

C. To test security measures

D. To develop encryption protocols

साइबर अपराध का मुख्य उद्देश्य क्या है?

A. नेटवर्क प्रदर्शन में सुधार करना

B. वित्तीय, प्रतिष्ठा या डेटा को नुकसान पहुंचाना

C. सुरक्षा उपायों का परीक्षण करना

D. एन्क्रिप्शन प्रोटोकॉल विकसित करना

14. Which of the following is an example of an insider attack?

A. Phishing email sent by a hacker

B. A disgruntled employee leaking sensitive data

C. Distributed Denial of Service (DDoS)

D. Malware installed through fake websites

P.T.O.

निम्नलिखित में से कौन अंदरूनी हमले का उदाहरण है?

A. हैकर द्वारा भेजा गया फ़िशिंग ईमेल

B. नाराज़ कर्मचारी द्वारा संवेदनशील डेटा लीक करना

C. वितरीत सेवा बाधा (DDoS)

D. नकली वेबसाइटों के माध्यम से स्थापित मैलवेयर

15. What is one way to prevent insider attacks?

A. Conducting regular employee background checks

B. Installing firewalls

C. Using multi-factor authentication

D. Encrypting all outgoing emails

अंदरूनी हमलों को रोकने का एक तरीका क्या है?

A. नियमित रूप से कर्मचारी पृष्ठभूमि जांच करना

B. फायरवॉल स्थापित करना

C. मल्टी–फैक्टर प्रमाणीकरण का उपयोग करना

D. सभी प्रेषित ईमेल को एन्क्रिप्ट करना

16. Which of the following is an example of an outsider attack?

A. Employee sharing credentials

B. Manipulating internal policies

C. Ransomware spread by a hacker

D. System misconfiguration by an administrator

निम्नलिखित में से कौन बाहरी हमले का उदाहरण है?

A. कर्मचारी द्वारा क्रेडेंशियल साझा करना

B. आंतरिक नीतियों में हेरफेर

C. हैकर द्वारा फैलाया गया रैंसमवेयर

D. व्यवस्थापक द्वारा सिस्टम की गलत कॉन्फ़िगरेशन

17. What is one effective way to prevent outsider attacks?

A. Implementing physical security controls

B. Keeping software up-to-date with patches

C. Limiting employee internet access

D. Conducting regular HR audits

बाहरी हमलों को रोकने का एक प्रभावी तरीका क्या है?

A. भौतिक सुरक्षा नियंत्रण लागू करना

B. सॉफ़्टवेयर को पैच के साथ अद्यतन रखना

C. कर्मचारियों की इंटरनेट पहुंच सीमित करना

D. नियमित एचआर ऑडिट करना

18. What are the 3 P's of Cybercrime

A. patches, passwords, phishing

B. password, protection, phishing

C. protection, phishing, patches

D. prevention, protection, password

साइबर क्राइम के 3 P क्या हैं?

A. पैच, पासवर्ड, फ़िशिंग

B. पासवर्ड, सुरक्षा, फ़िशिंग

C. सुरक्षा, फ़िशिंग, पैच

D. रोकथाम, सुरक्षा, पासवर्ड

19. What is the significant challenge of cybercrime?

A. Lack of internet speed

B. Global jurisdiction issues

C. High software costs

D. Limited hardware capabilities

P.T.O.

साइबर अपराध की एक महत्वपूर्ण चुनौती क्या है?

A. इंटरनेट गति की कमी

B. वैश्विक अधिकार क्षेत्र के मुद्दे

C. उच्च सॉफ़्टवेयर लागत

D. सीमित हार्डवेयर क्षमताएँ

20. What is the effect of cybercrime on businesses?

A. Increased productivity

B. Financial losses and reputational damage

C. Improved data transparency

D. Enhanced customer trust

साइबर अपराध का व्यवसायों पर क्या प्रभाव पड़ता है?

A. उत्पादकता में वृद्धि

B. वित्तीय नुकसान और प्रतिष्ठा को नुकसान

C. डेटा पारदर्शिता में सुधार

D. ग्राहक विश्वास को बढ़ावा

21. What is the complexity of cybercrime investigations?

A. Lack of evidence

B. Multiple language and technologies involved

C. Easy identification of criminals

D. Simplified reporting mechanisms

साइबर अपराध की जांच की जटिलता क्या है?

A. सबूत की कमी

B. कई भाषाओं और प्रौद्योगिकियों का समावेश

C. अपराधियों की आसान पहचान

D. सरलीकृत रिपोर्टिंग तंत्र

22. What is the first step to reporting a cybercrime incident?
A. Update your antivirus software
B. Inform the local cybercrime authority
C. Change system passwords
D. Backup your data

साइबर अपराध घटना की रिपोर्ट करने का पहला कदम क्या है?
A. अपने एंटीवायरस सॉफ़्टवेयर को अपडेट करें
B. स्थानीय साइबर अपराध प्राधिकरण को सूचित करें
C. सिस्टम पासवर्ड बदलें
D. अपने डेटा का बैकअप लें

23. What is an example of a property-related cybercrime?
A. Data theft or ransomware attack
B. Online harassment
C. Hacking into government systems
D. Email spamming

संपत्ति से संबंधित साइबर अपराध का एक उदाहरण क्या है?
A. डेटा चोरी या रैंसमवेयर हमला
B. ऑनलाइन उत्पीड़न
C. सरकारी प्रणालियों में हैकिंग
D. ईमेल स्पैमिंग

24. Which type of attack involves using social engineering techniques?
A. Insider attack
B. DoS attack
C. Ransomware
D. Phishing

कौन सा हमला सोशल इंजीनियरिंग तकनीकों का उपयोग करता है?
A. अंदरूनी हमला
B. DoS हमला
C. रैंसमवेयर
D. फ़िशिंग

25. What is a botnet?
A. A network of infected devices controlled remotely by a hacker
B. A network of legitimate servers
C. A secure internet protocol for data transfer
D. A type of firewall configuration

P.T.O.

बोटनेट क्या है?

A. संक्रमित डिवाइसों का नेटवर्क जिसे दूरस्थ रूप से हैकर द्वारा नियंत्रित किया जाता है
B. वैध सर्वरों का नेटवर्क
C. डेटा ट्रांसफर के लिए एक सुरक्षित इंटरनेट प्रोटोकॉल
D. एक प्रकार का फायरवॉल कॉन्फ़िगरेशन

26. What is the primary purpose of a botnet?

A. To secure networks from attacks
B. To perform large-scale cyberattacks
C. To encrypt sensitive data
D. To monitor network performance

बोटनेट का मुख्य उद्देश्य क्या है?

A. हमलों से नेटवर्क को सुरक्षित करना
B. बड़े पैमाने पर साइबर हमले करना
C. संवेदनशील डेटा को एन्क्रिप्ट करना
D. नेटवर्क प्रदर्शन की निगरानी करना

27. What is one common use of botnets in cybercrime?

A. Distributed Denial of Service (DDoS) attacks
B. Employee performance monitoring
C. Securing organizational data
D. Improving server speeds

साइबर अपराध में बोटनेट का एक सामान्य उपयोग क्या है?

A. वितरित सेवा बाधा (DDoS) हमले
B. कर्मचारी प्रदर्शन की निगरानी
C. संगठनात्मक डेटा को सुरक्षित करना
D. सर्वर की गति में सुधार

28. A software program that masquerades as regular programs, such as games, disk utilities, and even antivirus programs

A. Trojan House
B. Worm
C. Virus
D. Rootkit

एक सॉफ़्टवेयर प्रोग्राम जो गेम, डिस्क यूटिलिटीज़ और यहां तक कि एंटीवायरस प्रोग्राम जैसे नियमित प्रोग्राम के रूप में सामने आता है

A. ट्रोजन हॉर्स
B. वर्म
C. वायरस
D. रूटकिट

29. A type of malware used as a digital mechanism for extortion.
- A. Rootkit
- B. Ransomware
- C. Trojan Horse
- D. Virus

एक प्रकार का मैलवेयर जिसका उपयोग जबरन वसूली के लिए डिजिटल तंत्र के रूप में किया जाता है।
- A. रूटकिट
- B. रैंसमवेयर
- C. ट्रोजन हॉर्स
- D. वायरस

30. A virus cannot perform its task of harming and replication unless it is allowed to
- A. Move
- B. Evolve
- C. Shift
- D. Execute

कोई वायरस नुकसान पहुंचाने और प्रतिकृति बनाने का अपना कार्य तब तक नहीं कर सकता जब तक उसे इसकी अनुमति न दी जाए।
- A. मूव
- B. इवाल्व
- C. शिफ्ट
- D. एक्सीक्यूट

31. HTML stands for
- A. Hypertext markup language
- B. Hypotext markup language
- C. Hypertext markdown language
- D. Hypotext markdown language

HTML का मतलब है
- A. हाइपरटेक्स्ट मार्कअप भाषा
- B. हाइपोटेक्स्ट मार्कअप भाषा
- C. हाइपरटेक्स्ट मार्कडाउन भाषा
- D. हाइपोटेक्स्ट मार्कडाउन भाषा

32. What is the primary purpose of an Intrusion Detection System (IDS)?
- A. To prevent all types of cyberattacks
- B. To detect and alert about potential security breaches
- C. To block malicious traffic automatically
- D. To encrypt sensitive data during transmission

P.T.O.

घुसपैठ पहचान प्रणाली (IDS) का मुख्य उद्देश्य क्या है?
A. सभी प्रकार के साइबर हमलों को रोकना
B. संभावित सुरक्षा उल्लंघनों का पता लगाना और अलर्ट करना
C. दुर्भावनापूर्ण ट्रैफिक को स्वचालित रूप से ब्लॉक करना
D. डेटा ट्रांसमिशन के दौरान संवेदनशील डेटा को एन्क्रिप्ट करना

33. Which type of IDS analyzes network traffic to detect suspicious activities?
A. Network-based IDS (NIDS)
B. Host-based IDS (HIDS)
C. Application-based IDS
D. Database-based IDS

कौन सा प्रकार का IDS नेटवर्क ट्रैफ़िक का विश्लेषण करके संदिग्ध गतिविधियों का पता लगाता है?
A. नेटवर्क आधारित IDS (NIDS)
B. होस्ट आधारित (HIDS)
C. अनुप्रयोग आधारित IDS
D. डेटाबेस आधारित IDS

34. How does a Signature-Based IDS identify threats?
A. By comparing network activity to predefined attack patterns
B. By using artificial intelligence to predict future attacks
C. By analyzing user behavior for anomalies
D. By blocking all unrecognized IP addresses

सिगनेचर आधारित IDS खतरों की पहचान कैसे करता है?
A. नेटवर्क गतिविधि की तुलना पूर्व–परिभाषित हमले के पैटर्न से करके
B. भविष्य के हमलों की भविष्यवाणी करने के लिए कृत्रिम बुद्धिमत्ता का उपयोग करके
C. उपयोगकर्ता के व्यवहार में असामान्यताओं का विश्लेषण करके
D. सभी अपरिचित IP पतों को ब्लॉक

35. HTTP stands for
A. Hypertext transfer protocol
B. Hypotext transfer protocol
C. Hypertext transmission protocol
D. Hypotext transmission protocol

HTTP का मतलब है
A. हाइपरटेक्स्ट ट्रांसफर प्रोटोकॉल
B. हाइपोटेक्स्ट ट्रांसफर प्रोटोकॉल
C. हाइपरटेक्स्ट ट्रांसमिशन प्रोटोकॉल
D. हाइपोटेक्स्ट ट्रांसमिशन प्रोटोकॉल

36. What is Cross-Site Scripting (XSS)?
  A. A type of attack that encrypts user data for ransom
  B. An injection attack where malicious scripts are executed in a user's browser
  C. A technique to secure websites using encryption protocols
  D. A method for optimizing website loading times

क्रॉस–साइट स्क्रिप्टिंग (XSS) क्या है?
  A. एक प्रकार का हमला जो उपयोगकर्ता डेटा को फिरौती के लिए एन्क्रिप्ट करता है
  B. एक इंजेक्शन हमला जिसमें उपयोगकर्ता के ब्राउज़र में दुर्भावनापूर्ण स्क्रिप्ट्स निष्पादित की जाती हैं
  C. वेबसाइटों को एन्क्रिप्शन प्रोटोकॉल का उपयोग करके सुरक्षित करने की तकनीक
  D. वेबसाइट लोडिंग समय को अनुकूलित करने की एक विधि

37. How can Cross-Site Scripting (XSS) attacks be prevented?
  A. By encrypting all user data before storing
  B. By validating and sanitizing user inputs on the server and client sides
  C. By disabling firewalls
  D. By blocking all cookies in the browser

क्रॉस–साइट स्क्रिप्टिंग (XSS) हमलों को कैसे रोका जा सकता है?
  A. उपयोगकर्ता डेटा को संग्रहित करने से पहले एन्क्रिप्ट करके
  B. उपयोगकर्ता इनपुट को सर्वर और क्लाइंट दोनों पक्षों पर मान्य और स्वच्छ करके
  C. फायरवॉल को अक्षम करके
  D. ब्राउज़र में सभी कुकीज़ को ब्लॉक करके

38. What is the primary function of the National Critical Information Infrastructure Protection Centre (NCIIPC)?
  A. To monitor social media platforms for threats
  B. To protect critical information infrastructure from cyber threats
  C. To provide training to cybersecurity professionals
  D. To regulate internet service providers

राष्ट्रीय महत्वपूर्ण सूचना बुनियादी ढांचा संरक्षण केंद्र (NCIIPC) का मुख्य कार्य क्या है?
  A. खतरों के लिए सोशल मीडिया प्लेटफॉर्म की निगरानी करना
  B. साइबर खतरों से महत्वपूर्ण सूचना बुनियादी ढांचे की सुरक्षा करना
  C. साइबर सुरक्षा पेशेवरों को प्रशिक्षण प्रदान करना
  D. इंटरनेट सेवा प्रदाताओं को नियंत्रित करना

39. What is a key objective of the National Cyber Security Policy of India?
  A. To restrict internet usage to government officials
  B. To strengthen the resilience of India' s cyberspace
  C. To develop commercial software for cyber protection
  D. To create awareness about social engineering attacks

P.T.O.

भारत की राष्ट्रीय साइबर सुरक्षा नीति का मुख्य उद्देश्य क्या है?

A. इंटरनेट उपयोग को सरकारी अधिकारियों तक सीमित करना

B. भारत के साइबरस्पेस की मजबूती बढ़ाना

C. साइबर सुरक्षा के लिए वाणिज्यिक सॉफ़्टवेयर विकसित करना

D. सामाजिक इंजीनियरिंग हमलों के बारे में जागरूकता बढ़ाना

40. Which organization is responsible for handling cybersecurity incidents in India?

A. Ministry of Home Affairs (MHA)

B. Data Security Council of India (DSCI)

C. Indian Computer Emergency Response Team (CERT-In)

D. National Intelligence Grid (NATGRID)

भारत में साइबर सुरक्षा घटनाओं को संभालने के लिए कौन सी संस्था जिम्मेदार है?

A. गृह मंत्रालय (MHA)

B. डेटा सुरक्षा परिषद भारत (DSCI)

C. भारतीय कंप्यूटर आपात प्रतिक्रिया टीम (CERT-In)

D. राष्ट्रीय खुफिया ग्रिड (NATGRID)

****