A-1157

No. of Pages: 16

SECCS-03

Cyber Security Technique

Examination, 2026 (Feb.)

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) एव (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।

1. Which policy defines secure behaviour rules inside any modern organization?

A) Hardware

B) Security Policy

C) Antivirus

D) Network Cable

कौन सी नीति आधुनिक संगठन में सुरक्षित व्यवहार के नियम बताती है?

A) हार्डवेयर

B) सुरक्षा नीति

C) एंटीवायरस

D) नेटवर्क केबल

2.Which control is commonly used for strong physical security protection today?

A) Firewall

B) CCTV Camera

C) Email Filter

D) Password

आज भौतिक सुरक्षा हेतु सबसे सामान्य उपयोग किया जाने वाला नियंत्रण कौन है?

A) फायरवॉल

B) सीसीटीवी कैमरा

C) ईमेल फ़िल्टर

D) पासवर्ड

3.Which device filters unwanted internet traffic using predefined network rules?

A) Switch

B) Network Firewall

C) Barcode scanner

D) Projector

कौन-सा उपकरण पहले से निर्धारित नेटवर्क नियमों का उपयोग करके अवांछित इंटरनेट ट्रैफ़िक को फ़िल्टर करता है?

A) स्विच

B) नेटवर्क फ़ायरवॉल

C) बारकोड स्कैनर

D) प्रोजेक्टर

4.Which technology is mainly used today for ensuring complete email security?

A) PGP

B) File compression

C) Audio software

D) USB cable

कौन सी तकनीक आज पूरी तरह ईमेल सुरक्षा सुनिश्चित करने हेतु उपयोग होती है?

A) PGP

B) फाइल कम्प्रेशन

C) ऑडियो सॉफ़्टवेयर

D) यूएसबी केबल

5.Which method ensures message integrity and authenticity during digital communication?

A) Deletion

B) Antivirus

C) Formatting

D) MAC

कौन सी विधि डिजिटल संचार में संदेश की अखंडता और प्रामाणिकता सुनिश्चित करती है?

A) डिलीशन

B) एंटीवायरस

C) फॉर्मेटिंग

D) MAC

6.Which term refers to any unwanted program that slows down a computer without user permission?

A) Malware

B) Folder

C) Bluetooth

D) Wallpaper

कौन-सा शब्द किसी भी अवांछित प्रोग्राम को दर्शाता है जो उपयोगकर्ता की अनुमति के बिना कंप्यूटर को धीमा कर देता है?

A) मैलवेयर

B) फ़ोल्डर

C) ब्लूटूथ

D) वॉलपेपर

7.Phishing attacks usually trick users using fraudulent emails to steal information?

A) Pen drive

B) Fake emails

C) Keyboard

D) Router

फ़िशिंग हमले सामान्यतः नकली ईमेल का उपयोग कर उपयोगकर्ता, की जानकारी चुराते हैं?

A) पेन ड्राइव

B) नकली ईमेल

C) कीबोर्ड

D) राउटर

8.How does a DoS attack try to overload targeted serves and stop important digital services?

A) Overloading servers

B) Boosting speed

C) Cleaning system

D) Encrypting files

DoS हमला लक्षित सर्वरों को कैसे ओवरलोड कर महत्वपूर्ण डिजिटल सेवाएँ बंद करने का प्रयास करता है?

A) सर्वर ओवरलोड

B) गति बढ़ाना

C) सिस्टम साफ करना

D) फाइलें एन्क्रिप्ट करना

9.Which document lists step-by-step instructions for completing organizational technical activities?

A) Security Policy

B) Procedure

C) Firewall

D) Regulation

कौन सा दस्तावेज़ संगठन में तकनीकी कार्य पूरा करने की क्रमबद्ध प्रक्रिया बताता है?

A) सुरक्षा नीति

B) प्रक्रिया

C) फायरवॉल

D) विनियमन

10.Which statement defines a software weakness that attackers can easily exploit?

A) Vulnerability

B) Strength

C) Certificate

D) Feature

कौन-सा कथन उस सॉफ़्टवेयर कमजोरी को दर्शाता है जिसका हमलावर द्वारा दुरुपयोग किया जा सकता है?

A) भेद्यता

B) मजबूती

C) प्रमाणपत्र

D) फीचर

11.Which individuals inside organizations intentionally misuse authorized access privileges?

A) Outsiders

B) Insiders

C) Vendors

D) Customers

कौन से व्यक्ति संगठन के भीतर अधिकृत एक्सेस का दुरुपयोग करते हैं?

A) बाहरी लोग

B) अंदरूनी लोग

C) विक्रेता

D) ग्राहक

12.Which of the following generally includes illegal activities performed using digital technologies?

A) Road accident

B) Electrical fault

C) Fire incident

D) Cyber-crime

निम्नलिखित में से कौन सा कार्य डिजिटल प्रौद्योगिकियों का उपयोग करके अवैध गतिविधियों को शामिल करता है?

A) सड़क दुर्घटना

B) विद्युत त्रुटि

C) आग घटना

D) साइबर अपराध

13.Which threat arises when unknown individuals attempt unauthorized access from the internet?

A) External threat

B) Backup process

C) File indexing

D) Power saving

इंटरनेट से अज्ञात व्यक्ति जब अनधिकृत एक्सेस करने का प्रयास करते हैं, तब कौन-सा खतरा उत्पन्न होता है?

A) बाहरी खतरा

B) बैकअप प्रक्रिया

C) फ़ाइल इंडेक्सिंग

D) पावर सेविंग

14.Which technique ensures that users can access only the data required for their role?

A) Open access

B) Least privilege

C) USB sharing

D) Public login

कौन-सी तकनीक सुनिश्चित करती है कि उपयोगकर्ता केवल वही डेटा एक्सेस कर सकें जो उनके कार्य के लिए आवश्यक है?

A) ओपन एक्सेस

B) न्यूनतम विशेषाधिकार

C) USB शेयरिंग

D) पब्लिक लॉगिन

15.Which Indian agency officially receives cyber-security incident related reports nationwide?

A) PWD

B) CERT-In

C) Health dept

D) Railways

भारत में साइबर सुरक्षा घटनाओं की रिपोर्ट आधिकारिक रूप से कौन-सी एजेंसी लेती है?

A) पीडब्ल्यूडी

B) CERT-In

C) स्वास्थ्य विभाग

D) रेलवे

16.Which IDS feature stores security events to support later incident analysis?

A) Logging

B) Cleaning

C) Formatting

D) Deleting

कौन सा IDS फीचर भविष्य की जांच हेतु सुरक्षा घटनाएँ संग्रहीत करता है?

A) लॉगिंग

B) क्लीनिंग

C) फॉर्मेटिंग

D) डिलिटिंग

17.Which security tool analyzes network packets to detect unusual connection patterns?

A) Text editor

B) Packet analyzer

C) Scanner

D) Router

कौन-सा सुरक्षा उपकरण नेटवर्क पैकेट का विश्लेषण करके असामान्य कनेक्शन पैटर्न का पता लगाता है?

A) टेक्स्ट एडिटर

B) पैकेट एनालाइज़र

C) स्कैनर

D) राउटर

18.Which intrusion detection system runs inside single host to detect threats?

A) NIDS

B) Router

C) ISP

D) HIDS

कौन सा घुसपैठ पहचान सिस्टम एकल होस्ट में चलकर खतरे पहचानता है?

A) NIDS

B) राउटर

C) ISP

D) HIDS

19.Which system identifies attacks using signature comparison with known patterns?

A) Misuse IDS

B) Anomaly

C) Scanner

D) Monitor

कौन सा सिस्टम ज्ञात पैटर्न के सिग्नेचर मिलान द्वारा हमले पहचानता है?

A) मिसयूज IDS

B) अनोमली

C) स्कैनर

D) मॉनिटर

20.Which policy guides organizations in responding to cybersecurity incidents effectively?

A) Incident Response Policy

B) Railway Policy

C) Traffic Rules

D) Postal Policy

साइबर सुरक्षा घटनाओं पर प्रभावी प्रतिक्रिया देने हेतु कौनसी नीति संगठन का मार्गदर्शन करती है?

A) इन्सिडेंट रिस्पॉन्स नीति

B) रेलवे नीति

C) ट्रैफिक नियम

D) पोस्टल नीति

21.Which step begins IT asset security by properly identifying valuable assets first?

A) Format

B) Identify asset

C) Delete files

D) Restart

कौन-सा चरण पहले मूल्यवान एसेट की पहचान कर सुरक्षा शुरू करता है?

A) फॉर्मेट

B) एसेट पहचान

C) फाइलें हटाना

D) रीस्टार्ट

22.Which hardware module provides secure protection for encryption keys and signatures?

A) HSM

B) HDD

C) RAM

D) Modem

कौनसा हार्डवेयर मॉड्यूल एन्क्रिप्शन कुंजियों हेतु सुरक्षित संरक्षण प्रदान करता है?

A) HSM

B) HDD

C) RAM

D) मॉडेम

23.Which protocol provides wireless network security for modern Wi-Fi connections?

A) FTP

B) WPA

C) HTTP

D) SSL

कौनसा प्रोटोकॉल आधुनिक वाई-फाई कनेक्शन के लिए वायरलेस सुरक्षा प्रदान करता है?

A) FTP

B) WPA

C) HTTP

D) SSL

24.Which firewall category includes both software-based and hardware-based defence systems?

A) Hardware

B) Software

C) Both

D) None

कौनसी फायरवॉल श्रेणी में सॉफ़्टवेयर व हार्डवेयर दोनों सुरक्षा शामिल हैं?

A) हार्डवेयर

B) सॉफ़्टवेयर

C) दोनों

D) कोई नहीं

25.Which communication technology uses radio waves for transmitting wireless internet signals?

A) Cable

B) Wi-Fi

C) Fiber

D) Light

कौनसी संचार तकनीक वायरलेस इंटरनेट संकेत भेजने हेतु रेडियो तरंगें उपयोग करती है?

A) केबल

B) वाई-फाई

C) फाइबर

D) प्रकाश

26.Which cyber security model uses three dimensions for assessing information protection?

A) 2D

B) Hexa model

C) 5D

D) McCumber Cube

कौनसा साइबर सुरक्षा मॉडल सूचना सुरक्षा मूल्यांकन हेतु तीन आयाम उपयोग करता है?

A) 2D

B) हेक्सा मॉडल

C) 5D

D) मैकम्बर क्यूब

27.Which cyber security maturity model helps organizations measure their cyber readiness?

A) ISP model

B) CMM model

C) CPU model

D) Audit tool

कौनसा साइबर मेच्योरिटी मॉडल संगठन की साइबर तैयारी मापने में मदद करता है?

A) ISP मॉडल

B) CMM मॉडल

C) CPU मॉडल

D) ऑडिट टूल

28.Which cyber exercises evaluate response effectiveness against simulated large cyber-attacks?

A) Gaming

B) Cyber exercises

C) Screen testing

D) Wifi testing

कौनसे साइबर अभ्यास बड़े नकली साइबर हमलों पर प्रतिक्रिया क्षमता मापते हैं?

A) गेमिंग

B) साइबर अभ्यास

C) स्क्रीन परीक्षण

D) वाईफाई परीक्षण

29.Which malware attaches itself to executable software files in computers?

A) OS

B) Screen

C) Virus

D) CPU

कौनसा मैलवेयर कंप्यूटर में निष्पादन योग्य फाइलों से जुड़ जाता है?

A) OS

B) स्क्रीन

C) वायरस

D) CPU

30.Which malicious program spreads automatically through networks without user action?

A) Worm

B) Mouse

C) RAM

D) Monitor

कौनसा हानिकारक प्रोग्राम बिना उपयोगकर्ता कार्रवाई के नेटवर्क में फैलता है?

A) वर्म

B) माउस

C) RAM

D) मॉनिटर

31.Which harmful program appears safe but secretly performs malicious activities?

A) Antivirus

B) Trojan

C) Cable

D) Folder

कौन सा हानिकारक प्रोग्राम सुरक्षित दिखता है लेकिन छुपकर नुकसान करता है?

A) एंटीवायरस

B) ट्रोजन

C) केबल

D) फोल्डर

32.Which dangerous malware encrypts user data and demands ransom for decryption?

A) Cleaner

B) Ransomware

C) Mouse

D) Scanner

कौनसा मैलवेयर उपयोगकर्ता डेटा एन्क्रिप्ट कर फिरौती मांगता है?

A) क्लीनर

B) रैनसमवेयर

C) माउस

D) स्कैनर

33.Which malware hides itself deeply inside systems to avoid detection completely?
A) Rootkit

B) Worm

C) Router

D) UPS

कौनसा मैलवेयर सिस्टम में गहराई से छिपकर पहचान से बचता है?

A) रूटकिट

B) वर्म

C) राउटर

D) यूपीएस

34.Which web attack injects malicious scripts into vulnerable websites to harm users?
A) XSS

B) Mouse error

C) USB fault

D) Wifi drop

कौनसा वेब हमला कमजोर वेबसाइट में हानिकारक स्क्रिप्ट डालकर उपयोगकर्ताओं को नुकसान पहुँचाता है?

A) XSS

B) माउस त्रुटि

C) यूएसबी त्रुटि

D) वाईफाई ड्रॉप

35.Which database attack manipulates SQL queries to gain unauthorized access?

A) Keyboard attack

B) SQL injection

C) Wifi issue

D) Audio bug

कौनसा डाटाबेस हमला SQL क्वेरी बदलकर अनधिकृत एक्सेस प्राप्त करता है?

A) कीबोर्ड हमला

B) SQL इंजेक्शन

C) वाईफाई समस्या

D) ऑडियो बग

36.Which method protects applications by sanitizing user-submitted data before processing?

A) Auto-save

B) Data sanitization

C) Screen rotation

D) Cache cleaning

कौन-सी विधि उपयोगकर्ता द्वारा भेजे गए डेटा को प्रोसेस करने से पहले साफ़ करके एप्लिकेशन की सुरक्षा करती है?

A) ऑटो-सेव

B) डेटा सैनिटाइजेशन

C) स्क्रीन रोटेशन

D) कैश क्लीनिंग

37.Which human-targeted cyber-attack manipulates trust to extract confidential information?

A) Server error

B) Cable cut

C) Antenna issue

D) Social engineering

कौनसा मानवलक्षित साइबर हमला भरोसा छलकर गोपनीय जानकारी चुराता है?

A) सर्वर त्रुटि

B) केबल कट

C) एंटीना समस्या

D) सोशल इंजीनियरिंग

38.Which voicebased attack tricks users using fraudulent phone calls and messages?

A) Sms

B) Vishing

C) Wifi

D) Printer

कौनसा आवाज आधारित हमला नकली फोन कॉलों द्वारा उपयोगकर्ता को धोखा देता है?

A) SMS

B) विशिंग

C) वाईफाई

D) प्रिंटर

39.Which social engineering technique uses free items to lure unsuspecting users?

A) Wifi

B) Keyboard

C) Baiting

D) Cable

कौनसी सोशल इंजीनियरिंग तकनीक मुफ्त वस्तुओं का लालच देकर उपयोगकर्ता, को फंसाती है?

A) वाईफाई

B) कीबोर्ड

C) बैटिंग

D) केबल

40.Which best defence prevents social engineering by continuous security awareness training?

A) Antivirus

B) Awareness training

C) Big walls

D) Extra cables

कौन सा सर्वोत्तम बचाव उपाय निरंतर सुरक्षा जागरुकता प्रशिक्षण के माध्यम से सोशल इंजीनियरिंग को रोकता है?

A) एंटीवायरस

B) जागरूकता प्रशिक्षण

C) बड़ी दीवारें

D) अतिरिक्त केबल

****