RAJASTHAN PUBLIC SERVICE COMMISSION, AJMER

SYLLABUS FOR SCREENING TEST FOR THE POST OF
SENIOR SCIENTIFIC OFFICER
CYBER FORENSIC DIVISION
STATE FORENSIC SCIENCE LABORATORY (HOME DEPARTMENT)

1. Computer Fundamental, Operating System and File System-

Computer System- History and development, Computer Organization and Architecture: Cache memory. Primary and Secondary Storage devices, Input- Output device.

Operating System and File System- Operating system, layered architecture/logical structure of operating system, types of OS, virtual machine, OS services, Process management, Memory management, Virtual Memory. Overview of operating system in Linux & windows.

File System concepts, naming, attributes, operations, types, structure, file organization & access (Sequential, Direct, Index Sequential) methods, memory mapped files, directory structures.

2. Computer Network and Internet concepts-

Introduction of computer networks, Network architecture, Introduction to TCP/IP Model, compare TCP/IP to (OSI) reference model, Network protocol: FTP, Telnet, DNS, DHCP, SNMP, SMTP, POP3 etc. Basic Mobile communication network Model, Wi-Fi network, Bluetooth, Broadband and optical fibre.

Concept of IP address and their version IPv4 and IPv6, Web Hosting Concepts and Domain name Registration Process.

3. Cyber Security-

Information security concepts, Overview: Background and current scenario, types of attacks, goals for security, E-commerce security, steganography.

Security threats and vulnerabilities, overview of security threats, weak/strong passwords, insecure network connections, malicious code, programming bugs, cybercrime and cyber terrorism, information warfare and surveillance, virus, Trojan, worms, botnet, ransomware, shells.

4. Analyst Application Security-

Basic Security concepts: hardware and software vulnerabilities.

Password Cracking and Prevention: Introduction, password cracking techniques, dictionary based attack, brute force attack, cracking common files password, cracking

web based password, password reset flaws, password change flaws, cracking Wi-Fi password, counter measures for users, counter measures for system administrators.
Authentication & Authorization vulnerabilities: Authentication concepts, scenarios, user enumeration, direct page requests, parameter modification, lack of SSL at login pages, bypassing weak CAPTCHA mechanisms, login without SSL, Authorization: RBAC, authorization bypassing, parameter tampering, forceful browsing, rendering based authorization, client side validation attacks, insecure direct object reference.
Input vulnerabilities: SQL injection, common implementation mistakes – authentication bypassing using SQL injection, cross site scripting.

5. Database Management System, Security and Vulnerabilities-

Contents of the Subject Introduction: Overview of DBMS, Advantages of DBMS, Basic DBMS terminology.
Data modeling using the Entity Relationship Model: mapping constraints, Generalization, Aggregation, Specialization, Extended ER model, relationships of higher degree.
Relational model: Storage Organizations for Relations, Relational Algebra, Set Operations, Relational Calculus, Concepts of Alternate key, candidate key, primary key, Foreign key, Integrity Rules, Data Dictionary.
Normalization: Functional dependencies, normal forms, first, second, third normal forms, BCNF, inclusion dependencies, loss less join decompositions.
Database Vulnerabilities, Threats & Physical Security: external and internal database threats; flaws in perimeter security.
Data security policy: database security risks; database security testing; database auditing models and tools; user management strategies; maintenance policy, assessment and (counter) measures.

6. Information System Security and Cryptography-

Cryptographic System, Classification of Cryptographic System, Substitution-Permutation Network, Feistel structure, Block Ciphers: DES, Double DES, AES, Stream Ciphers: LFSR, RC4.
Public Key Cryptography, RSA, Discrete Logarithm Problems, Diffie-Hellman, DSA, PKI.
Data Integrity, Hash Functions: MD5, SHA, Message Authentication Codes.
Emerging Application: Email Security, SSL/TLS, Web Security, Access Controls, Malwares, Firewalls, and Intruders. Digital Signature, User authentication - Token based, Biometric, Remote user authentication, Intrusion detection systems, honey pots, Denial of Service.

7. Malware Analysis-

Goals of Malware Analysis, AV Scanning, Hashing, Finding Strings, Packing and Obfuscation, PEfile format, Static, Linked Libraries and Functions, Static Analysis tools, Virtual Machines and their usage in malware analysis, Sandboxing, Basic dynamic analysis, Malware execution, Process Monitoring, Viewing processes, Registry snapshots, Creating fake networks.
Live malware analysis, dead malware analysis, analyzing traces of malware, system calls, api calls, registries, network activities. Anti-dynamic analysis techniques, VM detection techniques, Evasion techniques, Malware Sandbox, Monitoring with Process Monitor, Packet Sniffing with Wireshark, Kernel vs. User-Mode Debugging, OllyDbg, Breakpoints, Tracing, Exception Handling, Patching.
Android Malware Analysis: Android architecture, App development cycle, APKTool, APKInspector, Dex2Jar, JD-GUI, Static and Dynamic Analysis.

8. Machine Learning and Big Data Analysis-

Machine Learning Introduction: Well posed learning problems, Designing a Learning system, Perspective and Issues in Machine Learning. Concept Learning: Concept learning task, Concept learning as search, Find-S algorithm, Version space, Candidate Elimination algorithm, Inductive Bias. Decision Tree Learning: Decision tree representation, Appropriate problems for decision tree learning, Basic decision tree learning algorithm, hypothesis space search.
Big data storage and analysis, comparison with other systems, rational database management system, grid computing, volunteer computing, convergence of key trends, unstructured data, industry examples of big data, web analytics, big data and marketing, fraud and big data, risk and big data, credit risk management, big data and algorithmic trading, big data and healthcare, big data in medicine, advertising and big data, big data technologies.

9. Ethical Hacking and Wireless Hacking-

Securing permission: Securing file and folder permission, Using the encrypting file system, Securing registry permissions. Securing service: Managing service permission.
Wireless Hacking: Wireless Foot printing, Wireless Scanning and Enumeration, Gaining Access, Tools that exploiting WEP Weakness, Denial of Services Attacks, Firewalls: Firewalls landscape, Firewall Identification-Scanning Through firewalls, packet Filtering, Application Proxy Vulnerabilities, Denial of Service Attacks, Motivation of DoS Attackers, Types of DoS attacks, Generic DoS Attacks.
Remote Control Insecurities, Discovering Remote Control Software, Connection, Weakness.VNC, Microsoft Terminal Server and Citrix ICA, Advanced Techniques Session Hijacking, Web Hacking, Web server hacking, web application hacking, Hacking

the internet Use, Malicious Mobile code, SSL fraud, Email Hacking, IRC hacking, Global counter measures to Internet User Hacking.

10. Foundation of Multimedia Forensic and Image Processing-

Introduction of digital signals: audio, image and video; Digitization process: sampling and quantization; Image Enhancement Techniques: Spatial and frequency domain; Image Compression Techniques: Introduction, lossy and lossless compression, Run length coding, scalar and vector quantization, JPEG and JPEG 2000 compression techniques; Image description and representation techniques: Introduction, boundary descriptor: chain code and shape number, regional descriptor: color and texture descriptors; Introduction to pattern clustering and classification.

Basics of Multimedia; Devices for capturing image and video: digital camera and its components, acquisition process of digital image and video; Standards for video transmission; NTSC and PAL.

Image Enhancement in the Spatial Domain: Some Basic Gray Level Transformations, Histogram Processing, Enhancement Using Arithmetic/Logic Operations, Basics of Spatial Filtering, Smoothing.

Spatial Filters, Sharpening Spatial Filters, Combining Spatial Enhancement Methods. Image Restoration Filtering, Inverse Filtering .

Color Fundamentals: Color Models, Pseudo color Image Processing, Basics of Full-Color Image Processing, Color Transformations, Smoothing and Sharpening, Color Segmentation, Noise in Color Images, Color Image Compression.

11. Mobile Forensics and Mobile Technology-

Generation of mobile phones, types of mobile phones, basics of mobile phones and their components, identification of mobile phones, operating systems.

Mobile phone technology: e.g. Asynchronous Transfer Mode (ATM), Wireless Applications Protocols (WAP), Advanced Mobile Phone System (AMPS), Time Division Multiple Access (TDMA), Code Division Multiple Access (CDMA), Cellular Networks: GSM, GPRS, EDGE, UMTS, LTE, VoLTE.

Mobile phone data acquisition by manual, logical, file system extraction and physical, Advanced Acquisition techniques. Overview of mobile forensic software.

12. Computer Forensics and DVR Forensic-

Basics of computer forensics, acquisition methods, image format (Raw, DD, SMART, AFF, E01 etc.), disk and file encryption techniques, file signature analysis, windows registry analysis, artifacts recognition from slack space and unallocated space, metadata analysis.

Basics of DVR and NVR, Types of CCTV camera and their characteristics, Operating Systems, enhancement of video and Authentication of video.

Overview of Computer and DVR forensics software and tools: write blockers, imaging, and cloning devices.

13. Network Forensics and Cloud Forensics-

Introduction to cloud technology, secure cloud bases services, Cloud based Applications: Facebook, Instagram, Telegram, WhatsApp, Facebook Messenger.

Monitoring computer networks and activities, live packet capturing, network intrusion detection, Types of Network Attack. Searching and collection of digital evidence from the network.

Cell Site Analysis, CDR Analysis, Tower Dump, IP tracing, web domains analysis, IPDR Analysis, Mobile Phone tracing, Email Tracing.

14. Modern Digital devices and Digital Technologies-

Modern digital Devices: Computer, Laptop, tablet, Mobile Phones, PoS, ATM machine, Smart watch, Drone, IoT devices.

Crypto Currency, Blockchain Technologies, Cloud computing, Artificial Intelligence, Deep fake video technology, Dark Web, Anonymous browsing techniques.

15. Cyber Crimes & IT Act-

Cyber space, cyber-crimes and types of cyber-crimes, Social media-use and misuse, hacking, unauthorized access, spoofing, phishing, cyber terrorism, cyber stalking, social engineering, DOS and DDOS attack, skimming, financial crimes, identity theft, Trojans, viruses, logic bombs, malware attack.

The Information Technology Act, 2000 and its amendments. Related and relevant section of IPC, Indian Evidence Act, Indian Telegraph Act.

Search, seizure and Collection of digital evidence, Significance of hash value, chain of custody.

* * * * *

Pattern of Question Papers:
1. **Objective Type Paper.**
2. **Maximum Marks: 150**
3. **Number of Questions: 150**
4. **Duration of Paper : 2:30 Hours**
5. **All Questions carry equal marks.**
6. **Medium of Screening Test: Bilingual in Hindi & English.**
7. **There will be Negative Marking.**
   (For every wrong answer, one-third of marks prescribed for that particular question will be deducted).