Indian Statistical Institute, Kolkata

Computing Systems Security II

M.Tech CrS – 2024-2026

Mid Term Examination, 2025

Date: 13/09/2025

Full Marks: 30 Time: 2 hrs

1. In the context of Access Control in Operating Systems, give an example of each type of access control DAC, MAC and RBAC? 2
2. What is the difference between WinLogon and NetLogon? 2
3. Systems with many Setuid/Setgid binaries increase the attack surface. How can we scan a linux system to find them all out.? 2
4. What is the role of Network Segmentation in enhancing host security? Write only two points. 2
5. Why Security Audit is important and how does it differ from System hardening? 3
6. What is NAT and NAT Overload? 2
7. What is traffic data enrichment and how can it be used to enhance host security. 3
8. Answer any 14 questions. 14 x 1 = 14

   I. **What does the following iptables rule do?**
   iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

   II. **How to view the system logs of a specific service in most Linux distributions?**

   III. **Write an IPTABLES rule to keep track of all incoming HTTP requests on port 80.**

   IV. **Which tool can be used to capture and analyse packets at the interface level in real time? How can such a tool help in analysing network traffic (only one point).**

   V. **What do we get out of netstat command in Linux?**

   VI. **Which file controls password aging policy in Linux and how?**

   VII. **Which file defines the rotation policy for system logs?**

   VIII. **How many different tables Linux firewall IPTABLES have and what are they?**

   IX. **What is the utility of /etc/ca-certificates.conf file on a Linux host?**

   X. **How do you verify whether a TLS connection is using strong cryptographic primitives or not?**

XI. Suppose you have a directory called Project and you want to give read, write and execute permission to owner, read and execute permission to group members and only read permission to other users to all files in that directory. How do you achieve that?

XII. How can you use Linux firewall to drop all traffic from the IP address A.B.C.D?

XIII. You wanted to develop a small host based agent to keep track of all HTTPS outgoing connections (without decrypting traffic) from your network. Which HTTPS packet you will sniff to know all the domain, individual HTTPS connections have been made. Give details.

XIV. Write one or two functions of Windows Active Directory?

XV. How to check interface wise statistics like Tx/Rx packets, Tx/Rx bytes, dropped packets,?

XVI. When in a TLS connection, ECDH or DH based key agreement protocol is to be used, how both parties (client and server or both peers) agree on which DH group or EC curve is to be used? Explain in just one or two sentence.