



गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

RASHTRIYA RAKSHA UNIVERSITY

An Institution of National Importance



SCHOOL OF INFORMATION TECHNOLOGY, ARTIFICIAL INTELLIGENCE AND CYBER SECURITY (SITAICS)

Organizes

Training Program on Operating System Security

RISE RRU



Secure your dates: 6 Days

16th March 2026 to 21st March 2026 (14:00 to 16:30)

Connect Online

RRU RISE (<https://rise.rru.ac.in/Course/593/630>)

Open to All

Practitioners, Faculties & Students

Connection Time

Total Training Duration: 15 hours (2.5 hours per day)

FEE

Rs. 1000(inclusive of all taxes)

Completion Certificate

Convener: Dr. Chandresh Parekha

Coordinator: Mr. Vivek Joshi

Organizers: Ms. Khushali Patel & Mr. Dushyant Atram

Contact: +916357436707

About the Program

This program offers a structured deep dive into Operating System Security, focusing on how modern OS architectures enforce confidentiality, integrity, and availability at the system core. Participants will explore kernel design, secure boot chains, file system protection, OS hardening, logging, auditing, and sandboxing mechanisms across Windows and Linux environments.

Through real-world breach case studies and hands-on security scenarios, the program bridges theory with operational defense practices such as access control, encryption at rest, EDR, SELinux, and container isolation. Designed as an online offering, it is open to students, practitioners, and faculty seeking to strengthen foundational and applied OS security knowledge critical for enterprise, government, and defense-grade systems.

Key Features

Expert-Led Instruction by Experts of Cybersecurity from Rashtriya Raksha University (RRU), ensuring defense-grade and policy-aligned insights

Interactive Q&A Sessions enabling direct technical discussions on OS internals, threats, and mitigations

Real-World Case Study Analysis covering OS-level breaches, ransomware impact, and incident response workflows

Industry-Relevant Practices aligned with enterprise, government, and critical-infrastructure security standards

Certification from RRU (Under MHA) recognizing verified training in Operating System Security and system hardening

Expected Outcomes

Develop a strong foundational and practical understanding of OS security across Windows and Linux platforms

Gain the ability to analyze kernel-level threats, system calls abuse, and boot-chain vulnerabilities

Learn to secure file systems and storage using permissions, encryption, and secure deletion techniques

Acquire hands-on knowledge of OS hardening, logging, auditing, and monitoring for incident detection

Build competence in applying OS-level security controls such as SELinux, AppArmor, EDR, sandboxing, and containers for real-world environments

Program Schedule

Module	Syllabus	Time
Foundations of OS Security & Architecture	<ul style="list-style-type: none">• What is OS Security?• Role of OS in system security• OS security vs Network security• Security goals: CIA Triad in OS• Monolithic kernel vs Microkernel• Kernel security responsibilities• System calls & security implications• Boot process & Secure Boot	2.5 Hours
File System & Storage Security	<ul style="list-style-type: none">• File permissions and ownership• Encryption at rest• Secure deletion techniques• NTFS vs EXT4 security models• Journaling & integrity checks• Storage-level access control	2.5 Hours
OS Hardening Techniques	<ul style="list-style-type: none">• OS hardening checklist• Patch management strategies• Service minimization• Secure configuration benchmarks (CIS, DISA STIG)• User account policies & privilege management• Registry & configuration security	2.5 Hours
Logging, Monitoring & Auditing	<ul style="list-style-type: none">• Importance of logs in security• Windows Event Logs• Linux syslog• Auditd configuration & usage• OS-level incident response basics• Log correlation & SIEM integration	2.5 Hours
Security Tools & Enforcement Mechanisms	<ul style="list-style-type: none">• Antivirus & Endpoint Detection & Response (EDR)• SELinux & AppArmor policies• Host-based intrusion detection systems (HIDS)• Sandboxing concepts• Virtualization & container security• Policy enforcement & isolation	2.5 Hours
Case Studies, Threats & Best Practices	<ul style="list-style-type: none">• Real-world OS breaches (examples & lessons)• Ransomware impact on OS security• Incident response at OS level• OS security best practices summary• Future trends in OS security (Zero Trust, AI-driven defense)• Capstone discussion & practical scenarios	2.5 Hours

Convener

Dr. Chandresh Parekha
Director I/c (Academic and Research)
School of Information Technology,
Artificial Intelligence and Cyber Security
(SITAICS)

Coordinator

Mr. Vivek Joshi
Assistant Director Training &
Assistant Professor
School of Information Technology, Artificial
Intelligence and Cyber Security (SITAICS)

Organizers

Ms. Khushali Patel

Administrative Assistant Cum Coordinator
School of Information Technology,
Artificial Intelligence and Cyber Security
(SITAICS)

Mr. Dushyant Atram

Administrative Officer
School of Information Technology,
Artificial Intelligence and Cyber Security
(SITAICS)



गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

RASHTRIYA RAKSHA UNIVERSITY
An Institution of National Importance



SCHOOL OF INFORMATION TECHNOLOGY, ARTIFICIAL
INTELLIGENCE AND CYBER SECURITY
(SITAICS)

For any Queries Contact:
+916357436707 +916357244815