



RED HAT TRAINING

Redhat Security Linux Physical Virtual And Cloud Training Course

Master Red Hat Linux security across physical, virtual, and cloud environments. Gain critical skills to protect your systems effectively.

DURATION

2 hours

LEVEL

Intermediate

FORMAT

Instructor-Led

- Globally Recognized Certification

- Expert-Led Hands-On Training

- Flexible Scheduling

Computer Pride | 1st Floor, ICEA Building, Kenyatta Avenue, Nairobi | www.computer-pride.co.ke

COURSE OVERVIEW

This Red Hat Security Linux Physical, Virtual, and Cloud Training Course is an essential program for IT professionals aiming to master the robust security features of Red Hat Enterprise Linux across diverse deployment landscapes. Participants will gain in-depth knowledge and hands-on skills to fortify Linux systems, safeguarding them against an ever-evolving threat landscape. The course meticulously covers fundamental security principles, network security, access control, and system hardening techniques specifically tailored for Red Hat environments.

Beyond traditional physical server deployments, this course delves into the unique security challenges and solutions inherent in virtualized infrastructures and modern cloud platforms. You will learn to implement robust security policies, manage identities, configure firewall rules, and audit system integrity within virtual machines and cloud instances, ensuring compliance and data protection. By mastering these skills, you will be equipped to build and maintain secure Red Hat-based systems, enhancing organizational resilience and protecting critical data assets across any IT environment. This specialized training empowers you to become a key player in defending complex enterprise systems from sophisticated cyber threats.

Duration	2 hours
Level	Intermediate
Vendor	Red Hat

COURSE CURRICULUM

01 Module 1: Red Hat Security Fundamentals and System Hardening

- Introduction to Linux security principles and best practices
- User and group management for enhanced security
- Understanding and applying File Permissions and Access Control Lists (ACLs)
- SELinux policy enforcement, context management, and troubleshooting
- System hardening techniques: disabling unnecessary services, secure boot, and filesystem integrity

02 Module 2: Network Security and Firewall Management

- Network services and their associated security considerations
- Advanced FirewallD configuration and rule management
- Securing SSH and other remote access services
- Introduction to network packet filtering and intrusion detection concepts
- VPN basics and secure communication strategies

03 Module 3: Securing Virtualized Red Hat Environments

- Understanding virtualization security challenges (hypervisor, guest OS isolation)
- Securing KVM/libvirt environments and virtual machine hardening
- Managing security contexts and policies in virtualized setups
- Integration of guest OS security with host-level security features
- Best practices for virtual network security

04 Module 4: Red Hat Security in Cloud Deployments

- Cloud security models and the shared responsibility framework
- Securing RHEL instances in public cloud environments (e.g., AWS, Azure, GCP considerations)
- Container security principles with Podman and Docker (basic overview)
- Introduction to OpenShift security concepts: security context constraints, image security

- Identity and access management (IAM) integration in cloud-native Red Hat systems

05 Module 5: Auditing, Monitoring, and Compliance

- System logging with journalctl for security event analysis
- Auditd configuration, rule creation, and log analysis for compliance
- Overview of Intrusion Detection and Prevention Systems (IDS/IPS)
- Vulnerability scanning, patch management, and security updates strategy
- Compliance considerations for Red Hat systems (e.g., PCI DSS, HIPAA basics)

CAREER PATHWAYS

Graduates of this program are prepared for the following roles:

- > **Red Hat Linux Security Administrator**
- > **Cloud Linux Security Engineer**
- > **Virtualization Security Specialist**

FREQUENTLY ASKED QUESTIONS

Q: How does this Red Hat security course specifically address the unique security challenges of securing Linux workloads deployed across hybrid environments, including physical servers, virtual machines, and cloud instances?

This course is meticulously designed to provide a holistic view of Linux security across the modern IT landscape. It dedicates specific modules to the distinct considerations for physical server hardening, then transitions to securing virtualized environments by addressing hypervisor interactions and guest OS isolation. Finally, it covers cloud-native security principles, including container security and integrating RHEL instances into public cloud security frameworks, ensuring you can implement consistent security policies irrespective of deployment model.

Q: What prior Red Hat Enterprise Linux administration experience is recommended for participants to fully benefit from the advanced security topics covered in this training?

While there are no strict prerequisites, participants will gain the most value if they possess foundational Red Hat Enterprise Linux administration skills equivalent to Red Hat Certified System Administrator (RHCSA) level. This includes familiarity with command-line operations, basic system configuration, user and group management, and network configuration. A solid understanding of these fundamentals will allow you to quickly grasp and apply the advanced security concepts and hands-on exercises presented in the course.

Q: Beyond general system hardening, what specific Red Hat technologies or security tools will I gain proficiency in using to enhance system security?

This course goes beyond generic security concepts by focusing on Red Hat-specific tools and methodologies. You will gain hands-on experience with SELinux for mandatory access control, FirewallD for robust network filtering, and Auditd for comprehensive system auditing. Furthermore, the course will introduce security considerations related to Podman/Docker for containerized applications and touch upon security context constraints within OpenShift environments, equipping you with a practical toolkit for Red Hat security.

ABOUT COMPUTER PRIDE



East Africa's Premier IT Training Center

With over 15 years of excellence, Computer Pride delivers globally recognized certification programs from leading technology vendors. Located on Kenyatta Avenue in Nairobi's CBD, our state-of-the-art facilities and expert instructors have empowered thousands of professionals across East Africa.

15+

Years of Excellence

10,000+

Professionals Trained

50+

Vendor Certifications

READY TO ENROL?

Take the next step in your technology career.

Location

1st Flr, ICEA Building
Kenyatta Ave, Nairobi

Email

info@computer-pride.co.ke

Phone

+254 705 900 900

www.computer-pride.co.ke