

RHS342 Developing Red Hat Firewall Solutions

Introduction

The 2.4 version of the Linux kernel, with its extended network address translation and new stateful inspection capabilities have accelerated interest in, and adoption of, Red Hat Linux as an enterprise-ready firewall solution. Red Hat's RHCE curriculum provides an introduction to these capabilities.

Pre-Requisites

RH253, RH300, or RHCE certification or equivalent work experience is required for this course

Course participants should already know the essential elements of how to configure the services covered, as this course will be focusing on more advanced topics from the outset.

RHS333 or a strong background in cryptographic technologies is also required.

Goal

Assure a medium level of Security, Firewalling and Penetration Skills so that the participant is qualified for professional responsibilities in managing a Red Hat Linux Firewalling and Security Solution.

Audience

Network administrators, system administrators, consultants, and other IT professionals will benefit from the subjects covered in this course.

Course Details

Course code: RHS342

Duration: 4 days

Starting time: 9.00 am

Finishing time: 5.00 pm

Lunch and refreshments are provided.

Booking guidelines

Contact our Learning Consultants on 1300 86 87246 and we will assist you with your booking.



Learning Solutions

(1300 86 87246

1300 TO TRAIN

Course Outline

RHS342 builds on these skills and introduces new ones that will provide course participants with a more comprehensive understanding of firewalls, penetration, and intrusion detection using Red Hat Linux and other open source tools. The topics covered in this five-day class include the following:

Firewalling

- Firewalling Concepts
- Packetfilter (stateful)
- Application Level Gateways
- Firewall Architectures
- Screening Router
- Dual-homed Host
- DMZ
- VPN
- Implementing a Firewall using RHEL
- Stateful Firewalls using Red Hat Enterprise Linux and iptables
- Application-level Gateways using Squid and Postfix
- Firewall testing
- Testing the firewall using nmap
- Local Security
- Filesystem Security
- Auditing the system using Logwatch and Third Party tools

VPN

- VPN concepts and protocols
- CiPE
- IPSec

Implementing a VPN using CiPE

Implementing a VPN using IPSec

- Manual keyed connections using setkey
- Automatic keyed connections using racoon
- Using preshared keys for authentication
- Using X.509 certificates for authentication
- Administering connections using redhat-config-network

Implementing VPNs using RHEL in heterogenous networks

- Connecting to Windows 2000