

**Course Description:**

Red Hat Enterprise Linux has gained considerable momentum as the operating system of choice for deploying network services such as web, ftp, email, and file sharing. Red Hat's RHCE curriculum provides training in deploying these services and on the essential elements of securing them.

**Who Should Attend:**

The audience for this course includes system administrators, consultants, and other IT professionals responsible for the planning, implementation, and maintenance of network servers. While the emphasis is on running these services on Red Hat Enterprise Linux, and the content and labs will assume its use, system administrators and others using proprietary forms of Unix may also find many elements of this course relevant.

**Prerequisites:**

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.

**Benefits of Attendance:**

Upon completion of this course, students will be able to:

- Master basic service security.
- Understand cryptography.
- Log system activity.
- Secure BIND and DNS.
- Improve NFS security.
- Manage FTP access.

**Course Outline:****The Threat Model and Protection Methods**

Internet threat model and the attacker's plan  
System security and service availability  
An overview of protection mechanisms

**Basic Service Security**

SELinux  
Host-based access control  
Firewalls using Netfilter and iptables  
TCP wrappers  
xinetd and service limits

**Cryptography**

Overview of cryptographic techniques  
Management of SSL certificates  
Using GnuPG

**Logging and NTP**

Time synchronization with NTP  
Logging: syslog and its weaknesses  
Protecting log servers

**BIND and DNS Security**

BIND vulnerabilities  
DNS Security: attacks on DNS  
Access control lists  
Transaction signatures  
Restricting zone transfers and recursive queries  
DNS Topologies  
Bogus servers and blackholes  
Views  
Monitoring and logging  
Dynamic DNS security

**Network Authentication: RPC, NIS, and Kerberos**

Vulnerabilities  
Network-managed users and account management  
RPC and NIS security issues  
Improving NIS security  
Using Kerberos authentication  
Debugging Kerberized Services  
Kerberos Cross-Realm Trust  
Kerberos Encryption

**Network File System**

Overview of NFS versions 2, 3, and 4  
Security in NFS versions 2 and 3  
Improvements in security in NFS4  
Troubleshooting NFS4  
Client-side mount options

**OpenSSH**

Vulnerabilities  
Server configuration and the SSH protocols  
Authentication and access control

Client-side security  
Protecting private keys  
Port-forwarding and X11-forwarding issues

**Electronic Mail with Sendmail**

Vulnerabilities  
Server topologies  
Email encryption  
Access control and STARTTLS  
Anti-spam mechanisms

**Postfix**

Vulnerabilities  
Security and Postfix design  
Configuring SASL/TLS

**FTP**

Vulnerabilities  
The FTP protocol and FTP servers  
Logging  
Anonymous FTP  
Access control

**Apache security**

Vulnerabilities  
Access control  
Authentication: files, passwords, Kerberos  
Security implications of common configuration options  
CGI security  
Server side includes  
suEXEC

**Intrusion Detection and Recovery**

Intrusion risks  
Security policy  
Detecting possible intrusions  
Monitoring network traffic and open ports  
Detecting modified files  
Investigating and verifying detected intrusions  
Recovering from, reporting, and documenting intrusions