

RHS333 Training Class Content

RHS333 goes beyond the essential security coverage offered in the RHCE curriculum and delves deeper into the security features, capabilities, and risks associated with the most commonly deployed services. Among the topics covered in this four-day, hands-on course are the following:

- Mastering basic service security
 - · Review of host security
 - · Advanced TCP wrappers configuration
 - · Advanced xinetd configuration
- Understanding cryptography
 - · Overview of cryptographic techniques
 - · Management of SSL certificates
- Logging system activity
 - · Clock synchronization with NTP
 - · Configuring centralized syslog management
- Securing BIND and DNS
 - · Name server topology and "views"
 - · Configuration of appropriate recursion and response policies
 - · Using TSIG authentication keys
 - · Running BIND in a chroot environment
- Network user authentication security
 - · Managing portmap and NIS risks
 - · Using Kerberos authentication
- Improving NFS security
 - · NFS security limitations
 - · Configurations to avoid
- The secure shell: OpenSSH
 - · Protocol and service security
 - · Protecting public-key authentication
 - · Port-forwarding and X11-forwarding issues
- Securing E-mail with Sendmail and Postfix
 - · User mail spool access issues
 - · Overview of Postfix configuration
 - · Access control and STARTTLS
 - · Anti-spam features
 - · Introduction to Procmail
- Managing FTP access
 - · Controlling local and anonymous users
- Apache security
 - · User authentication and access control
 - · Common misconfigurations
 - · Containing CGI risks
- Basics of intrusion response
 - · Monitoring for suspicious activity
 - · Verifying suspected intrusions
 - · Recovering from an intrusion