RHS333 Red Hat Enterprise Security: Network Services Description

Goals:

RHS333 trains people with RHCE-level competency to understand, prevent, detect, and properly respond to sophisticated security threats aimed at enterprise systems. The course equips system administrators and security professionals with the skills and knowledge to harden computers against both internal and external attacks, providing in-depth analysis of the ever-changing threat models as they pertain to Red Hat Enterprise Linux. RH333 builds on the security skills developed in other Red Hat training courses so that administrators can design and implement an adequate security profile for critical enterprise systems.

Audience:

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.

Course Contents

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:

1. The Threat Model and Protection Methods
    - Internet threat model and the attacker's plan
    - System security and service availability
    - An overview of protection mechanisms
2. Basic Service Security
    - SELinux
    - Host-based access control
    - Firewalls using Netfilter and iptables
    - TCP wrappers

    - xinetd and service limits
3. Cryptography
    - Overview of cryptographic techniques
    - Management of SSL certificates
    - Using GnuPG
4. Logging and NTP
    - Time synchronization with NTP
    - Logging: syslog and its weaknesses
    - Protecting log servers
5. 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
6. 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
7. 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
8. OpenSSH
    - Vulnerabilities
    - Server configuration and the SSH protocols
    - Authentication and access control
    - Client-side security
    - Protecting private keys
    - Port-forwarding and X11-forwarding issues
9. Electronic Mail with Sendmail
    - Vulnerabilities
    - Server topologies
    - Email encryption

    - Access control and STARTTLS
    - Anti-spam mechanisms
10. Postfix
    - Vulnerabilities
    - Security and Postfix design
    - Configuring SASL/TLS
11. FTP
    - Vulnerabilities
    - The FTP protocol and FTP servers
    - Logging
    - Anonymous FTP
    - Access control
12. Apache security
    - Vulnerabilities
    - Access control
    - Authentication: files, passwords, Kerberos
    - Security implications of common configuration options
    - CGI security
    - Server side includes
    - suEXEC
13. 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