RHS333-Bundle: Red Hat Enterprise Security: Network Services + EX333

Duration: 5 Days **Course Code: RHS334**

Overview:

Red Hat® Enterprise Security: Network Services with Exam is an intensive course that provides 4 days of instruction and labs that show students how to use the latest technologies to secure services. This class advances beyond the essential security coverage offered in the Red Hat Certified Engineer (RHCE®) curriculum and delves more deeply into the security features, capabilities, and risks associated with the most commonly deployed services.

Target Audience:

Experienced Linux® system administrators responsible for the overall security of their systems and networked services and RHCEs interested in earning Red Hat Certificates of Expertise or Red Hat Certified Security Specialist (RHCSS) or Red Hat Certified Architect (RHCA) certifications

Prerequisites:

- Knowledge of the essential elements of how to configure the services covered, as this course focuses on more advanced topics
- RHCE certification or equivalent experience

Testing and Certification

- Red Hat Enterprise Security Network Services Expertise Exam (EX333)
- This course prepares you for these credentials
- Red Hat Certified Architect — RHCA
- Red Hat Certified Security Specialist — RHCSS
- Certificates of Expertise

Follow-on-Courses:

- RH423, Red Hat Enterprise Directory Services and Authentication
- RHS429, Red Hat Enterprise SELinux Policy Administration

Content:

- Understanding cryptography
- Securing BIND and DNS
- Hardening RPC services
- Using Kerberos for centrally managed user authentication
- Improving NFS security with Kerberos and NFSv4
- Advanced uses of Secure Shell
- Building a secure email infrastructure
- Securing FTP and Apache HTTPD services
- Basics of intrusion detection and response

- Understanding cryptography
- Securing BIND and DNS
- Hardening RPC services
- Using Kerberos for centrally managed user authentication
- Improving NFS security with Kerberos and NFSv4
- Advanced uses of Secure Shell
- Building a secure email infrastructure
- Securing FTP and Apache HTTPD services
- Basics of intrusion detection and response

- Understanding cryptography
- Securing BIND and DNS
- Hardening RPC services
- Using Kerberos for centrally managed user authentication
- Improving NFS security with Kerberos and NFSv4
- Advanced uses of Secure Shell
- Building a secure email infrastructure
- Securing FTP and Apache HTTPD services
- Basics of intrusion detection and response

- Understanding cryptography
- Securing BIND and DNS
- Hardening RPC services
- Using Kerberos for centrally managed user authentication
- Improving NFS security with Kerberos and NFSv4
- Advanced uses of Secure Shell
- Building a secure email infrastructure
- Securing FTP and Apache HTTPD services
- Basics of intrusion detection and response

- Understanding cryptography
- Securing BIND and DNS
- Hardening RPC services
- Using Kerberos for centrally managed user authentication
- Improving NFS security with Kerberos and NFSv4
- Advanced uses of Secure Shell
- Building a secure email infrastructure
- Securing FTP and Apache HTTPD services
- Basics of intrusion detection and response

- Understanding cryptography
- Securing BIND and DNS
- Hardening RPC services
- Using Kerberos for centrally managed user authentication
- Improving NFS security with Kerberos and NFSv4
- Advanced uses of Secure Shell
- Building a secure email infrastructure
- Securing FTP and Apache HTTPD services
- Basics of intrusion detection and response

- Understanding cryptography
- Securing BIND and DNS
- Hardening RPC services
- Using Kerberos for centrally managed user authentication
- Improving NFS security with Kerberos and NFSv4
- Advanced uses of Secure Shell
- Building a secure email infrastructure
- Securing FTP and Apache HTTPD services
- Basics of intrusion detection and response

- Understanding cryptography
- Securing BIND and DNS
- Hardening RPC services
- Using Kerberos for centrally managed user authentication
- Improving NFS security with Kerberos and NFSv4
- Advanced uses of Secure Shell
- Building a secure email infrastructure
- Securing FTP and Apache HTTPD services
- Basics of intrusion detection and response

- Understanding cryptography
- Securing BIND and DNS
- Hardening RPC services
- Using Kerberos for centrally managed user authentication
- Improving NFS security with Kerberos and NFSv4
- Advanced uses of Secure Shell
- Building a secure email infrastructure
- Securing FTP and Apache HTTPD services
- Basics of intrusion detection and response

Further Information:

For More information, or to book your course, please call us on Head Office Tel.: +974 40316639

training@globalknowledge.qa

www.globalknowledge.qa

Global Knowledge, Qatar Financial Center, Burj Doha,Level 21, P.O.Box 27110, West Bay, Doha, Qatar