Course data sheet

Hewlett Packard
Enterprise

Enterprise Linux Server Hardening (GL413) HJ7F5S

HPE course number	HJ7F5S
Course length	4 days
Delivery mode	ILT
View schedule, local pricing, and register	**View now**
View related courses	**View now**

This course explains the hardening of a RHEL Linux System.

Why HPE Education Services?

- IDC MarketScape leader 5 years running for IT education and training*
- Recognized by IDC for leading with global coverage, unmatched technical expertise, and targeted education consulting services*
- Key partnerships with industry leaders OpenStack®, VMware®, Linux®, Microsoft®, ITIL, PMI, CSA, and SUSE
- Complete continuum of training delivery options—self-paced eLearning, custom education consulting, traditional classroom, video on-demand instruction, live virtual instructor-led with hands-on lab, dedicated onsite training
- Simplified purchase option with HPE Training Credits

Prerequisites

- Knowledge equivalent to U8583S: Linux Fundamentals (GL120) and H7091S: Enterprise Linux Systems Administration (GL250)

*Realize Technology Value with Training, IDC Infographic 2037, Sponsored by HPE, October 2017

Detailed course outline

Security Concepts

- Basic security principles
- RHEL7 default install
- Minimization – discovery
- Service discovery
- Hardening
- Security concepts

Scanning, Probing, and Mapping Vulnerabilities

- The security environment
- Stealth reconnaissance
- The WHOIS database
- Interrogating DNS
- Discovering hosts
- Discovering reachable services
- Reconnaissance with SNMP
- Discovery of RPC services
- Enumerating NFS shares
- Nessus/OpenVAS insecurity scanner
- Configuring OpenVAS
- Intrusion detection systems
- Snort rules
- Writing snort rules

Tracking Security Updates and Software Maintenance

- Security advisories
- Managing software
- RPM features
- RPM architecture
- RPM package files
- Working with RPMs
- Querying and verifying with RPM
- Updating the kernel RPM
- Dealing with RPM and YUM digest changes
- Using the YUM command
- Using YUM history
- YUM plugins and RHN Subscription Manager
- YUM repositories

Manage the Filesystem

- Partitioning disks with fdisk and gdisk
- Resizing a GPT partition with gdisk
- Partitioning disks with parted
- Filesystem creation
- Persistent block devices
- Mounting filesystems
- Filesystem maintenance
- Swap

Securing the Filesystem

- Configuring disk quotas
- Setting quotas
- Viewing and monitoring quotas
- Filesystem attributes
- Filesystem mount optionqs
- GPG – GNU Privacy Guard
- File encryption with OpenSSL
- File encryption with encfs
- Linux Unified Key Setup (LUKS)

Manage Special Permissions

- File and directory permissions
- File creation permissions with umask
- SUID and SGID on files
- SGID and sticky bit on directories
- Changing file permissions
- User private group scheme

Manage File Access Controls

- File Access Control Lists
- Manipulating FACLs
- Viewing FACLs
- Backing up FACLs

Monitor for Filesystem Changes

- Host Intrusion Detection Systems (HIDS)
- Using RPM as a HIDS
- Introduction to AIDE
- AIDE installation
- AIDE policies
- AIDE usage

Manage User Accounts

- Approaches to storing user accounts
- User and group concepts
- User administration
- Modifying accounts
- Group administration
- RHEL DS client configuration
- System Security Services Daemon (SSSD)

Password Security and PAM

- Unix passwords
- Password aging
- Auditing passwords
- PAM overview
- PAM module types
- PAM order of processing
- PAM control statements
- PAM modules

Using FreeIPA for Centralized Authentication	• What is FreeIPA? • FreeIPA features • FreeIPA installation	• FreeIPA client installation • User, group, and host management • FreeIPA Active Directory integration
Log File Administration	• System logging • systemd journal • systemd journal's journalctl • Secure logging with journal's log sealing • gnome-system-log	• Rsyslog • /etc/rsyslog.conf • Log management • Log anomaly detector • Sending logs from the shell
Accountability with Kernel auditd	• Accountability and auditing • Simple session auditing • Simple process accounting and command history • Kernel-level auditing • Configuring the audit daemon	• Controlling kernel audit system • Creating audit rules • Searching audit logs • Generating audit log reports • Audit log analysis
Securing Services	• Xinetd • Xinetd connection limiting and access control • Xinetd: resource limits, redirection, logging • TCP wrappers • The /etc/hosts.allow and /etc/hosts.deny files • /etc/hosts.{allow,deny} shortcuts • Advanced TCP wrappers • FirewallD	• Netfilter: stateful packet filter firewall • Netfilter concepts • Using the iptables command • Netfilter rule syntax • Targets • Common match_specs • Connection tracking
SELinux	• DAC vs. MAC • Shortcomings of traditional Unix security • SELinux goals • SELinux evolution • SELinux modes • Gathering SELinux information • SELinux virtual filesystem • SELinux contexts • Managing contexts • The SELinux policy • Choosing an SELinux policy	• Policy layout • Tuning and adapting policy • Booleans • Permissive domains • Managing file context database • Managing port contexts • SELinux policy tools • Examining policy • SELinux troubleshooting • SELinux troubleshooting continued

Learn more at
hpe.com/ww/learnlinux

Follow us:

Hewlett Packard
Enterprise

HJ7F5S A.00, September 2019