Hewlett Packard Enterprise

Enterprise Linux Security Administration (GL550) U8630S

HPE course number	U8630S
Course length	5 Days
Delivery mode	ILT, VILT
View schedule, local pricing, and register	**View now**
View related courses	**View now**

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

This highly technical course focuses on properly securing machines running the Linux operating systems. A broad range of general security techniques, such as packet filtering, password policies, and file integrity checking are covered. Advanced security technologies, such as Kerberos and SELinux are taught. Special attention is given to securing commonly deployed network services. At the end of the course, students have an excellent understanding of the potential security vulnerabilities -- know how to audit existing machines, and how to securely deploy new network services.

Prerequisites

This class covers advanced security topics and is intended for experienced systems administrators. Candidates should have current Linux or UNIX systems administration experience equivalent to the U8583S “Linux Fundamentals”, H7091S “Enterprise Linux Systems Administration”, and H7092S “Enterprise Linux Networking Services”.

Supported distributions

- Red Hat Enterprise Linux 7
- SUSE Linux Enterprise 12

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

Detailed course outline

Module 1: Security Concepts	• Basic Security Principles • RHEL7 Default Install • RHEL7 Firewall • SLES12 Default Install • SUSE Basic Firewall Configuration	• SLES12: File Security • Minimization – Discovery • Service Discovery • Hardening • Security Concepts
Lab Tasks	• Removing Packages Using RPM • Firewall Configuration • Process Discovery	• Operation of the setuid() and capset() System Calls • Operation of the chroot() System Call
Module 2: 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
Lab Tasks	• NMAP • OpenVAS	• Advanced nmap Options
Module 3: Password Security and PAM	• Unix Passwords • Password Aging • Auditing Passwords • PAM Overview • PAM Module Types • PAM Order of Processing • PAM Control Statements • PAM Modules • pam_unix • pam_cracklib.so • pam_pwcheck.so • pam_env.so • pam_xauth.so	• pam_tally2.so • pam_wheel.so • pam_limits.so • pam_nologin.so • pam_deny.so • pam_warn.so • pam_securetty.so • pam_time.so • pam_access.so • pam_listfile.so • pam_lastlog.so • pam_console.so
Lab Tasks	• John the Ripper • Cracklib • Using pam_listfile to Implement Arbitrary ACLs • Using pam_limits to Restrict Simultaneous Logins	• Using pam_nologin to Restrict Logins • Using pam_access to Restrict Logins • su & pam
Module 4: Secure Network Time Protocol (NTP)	• The Importance of Time • Hardware and System Clock • Time Measurements • NTP Terms and Definitions • Synchronization Methods • NTP Evolution • Time Server Hierarchy	• Operational Modes • NTP Clients • Configuring NTP Clients • Configuring NTP Servers • Securing NTP • NTP Packet Integrity • Useful NTP Commands

Lab Tasks	• Configuring and Securing NTP	• Peering NTP with Multiple Systems
Module 5: Kerberos Concepts and Components	• Common Security Problems • Account Proliferation • The Kerberos Solution • Kerberos History • Kerberos Implementations • Kerberos Concepts • Kerberos Principals • Kerberos Safeguards • Kerberos Components • Authentication Process	• Identification Types • Logging In • Gaining Privileges • Using Privileges • Kerberos Components and the KDC • Kerberized Services Review • KDC Server Daemons • Configuration Files • Utilities Overview
Module 6: Implementing Kerberos	• Plan Topology and Implementation • Kerberos 5 Client Software • Kerberos 5 Server Software • Synchronize Clocks • Create Master KDC • Configuring the Master KDC • KDC Logging • Kerberos Realm Defaults • Specifying [realms] • Specifying [domain_realm] • Allow Administrative Access • Create KDC Databases • Create Administrators • Install Keys for Services • Start Services • Add Host Principals	• Add Common Service Principals • Configure Slave KDCs • Create Principals for Slaves • Define Slaves as KDCs • Copy Configuration to Slaves • Install Principals on Slaves • Synchronization of Database • Propagate Data to Slaves • Create Stash on Slaves • Start Slave Daemons • Client Configuration • Install krb5.conf on Clients • Client PAM Configuration • Install Client Host Keys
Lab Tasks	• Implementing Kerberos	
Module 7: Administering and Using Kerberos	• Administrative Tasks • Key Tables • Managing Keytabs • Managing Principals • Viewing Principals • Adding, Deleting, and Modifying Principals • Principal Policy • Overall Goals for Users • Signing In to Kerberos • Ticket types	• Viewing Tickets • Removing Tickets • Passwords • Changing Passwords • Giving Others Access • Using Kerberized Services • Kerberized FTP • Enabling Kerberized Services • OpenSSH and Kerberos
Lab Tasks	• Using Kerberized Clients • Forwarding Kerberos Tickets	• OpenSSH with Kerberos • Wireshark and Kerberos

Module 8: Securing the Filesystem	• Filesystem Mount Options • NFS Properties • NFS Export Option • NFSv4 and GSSAPI Auth • Implementing NFSv4	• Implementing Kerberos with NFS • GPG – GNU Privacy Guard • File Encryption with OpenSSL • File Encryption with encfs • Linux Unified Key Setup (LUKS)
Lab Tasks	• Securing Filesystems • Securing NFS • Implementing NFSv4	• File Encryption with GPG • File Encryption with OpenSSL • LUKS-on-disk format Encrypted Filesystem
Module 9: AIDE	• Host Intrusion Detection Systems • Using RPM as a HIDS • Introduction to AIDE	• AIDE Installation • AIDE Policies • AIDE Usage
Lab Tasks	• File Integrity Checking with RPM	• File Integrity Checking with AIDE
Module 10: Accountability with Kernel Auditd	• Accountability and Auditing • Simple Session Auditing • Simple Process Accounting & 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
Lab Tasks	• Auditing Login/Logout • Auditing File Access	• Auditing Command Execution
Module 11: SELinux	• DAC vs. MAC • Shortcomings of Traditional Unix Security • AppArmor • 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
Lab Tasks	• Exploring SELinux Modes • Exploring AppArmor Modes • SELinux Contexts in Action • Exploring AppArmor	• Managing SELinux Booleans • Creating Policy with Audit2allow • Creating & Compiling Policy from Source
Module 12: Securing Apache	• Apache Overview • httpd.conf – Server Settings • Configuring CGI • Turning Off Unneeded Modules • Delegating Administration • Apache Access Controls (mod_access) • HTTP User Authentication • Standard Auth Modules	• HTTP Digest Authentication • TLS Using mod_ssl.so • Authentication via SQL • Authentication via LDAP • Authentication via Kerberos • Scrubbing HTTP Headers • Metering HTTP Bandwidth

Lab Tasks	• Hardening Apache by Minimizing Loaded Modules • Scrubbing Apache & PHP Version Headers • Protecting Web Content • Protecting Web Content • Using the suexec Mechanism	• Create a TLS CA key pair • Using SSL CA Certificates with Apache • Enable Apache SSL Client Certificate Authentication • Enabling SSO in Apache with mod_auth_kerb
Module 13: Securing PostgreSQL	• PostgreSQL Overview • PostgreSQL Default Config • Configuring TLS	• Client Authentication Basics • Advanced Authentication • Ident-based Authentication
Lab Tasks	• Configure PostgreSQL • PostgreSQL with TLS	• PostgreSQL with Kerberos Authentication • Securing PostgreSQL with Web Based Applications
Appendix A: Securing Email Systems	• SMTP Implementations • Security Considerations	• chrooting Postfix • Email with GSSAPI/Kerberos Auth
Lab Tasks	• Postfix in a Change Root Environment	

Learn more at
hpe.com/ww/learnlinux

Follow us:

c04586449, December 2017, U8630S G.01

Hewlett Packard
Enterprise