HP Education Services course data sheet

HP-UX Security H3541S

Course Overview

This course examines the most common HP-UX system security vulnerabilities, and introduces a variety of tools and techniques that can be used to prevent hackers from exploiting these vulnerabilities.

Price	USD $4,000
Links to local schedules, pricing and registration	**US/Canada** **Mexico/Latin America** **Brazil**
Course title	HP-UX Security
HP course #	H3541S
Category	HP-UX / HP Integrity
Duration	5 days

Special note

This fast-paced hands-on course examines a variety of popular tools and techniques for hardening and securing HP-UX systems. The course is 50% lecture / 50% lab.

Audience

- Experienced system and network administrators responsible for securing and monitoring HP-UX systems

Prerequisites

- HP-UX System and Network Administration I (H3064S) and HP-UX System and Network Administration II (H3065S) or
- HP-UX for experienced UNIX system administrators (H5875S) or equivalent experience
- Equivalent experience

Benefits to you

- Learn how to use Role Based Access Control (RBAC), Secure Shell (SSH), Host Intrusion Detection System (HIDS), Software Assistant (SWA), IPFilter, Bastille, and other HP supported tools to harden and secure HP-UX systems

- Create secure, isolated execution environments for applications with HP-UX security compartments and Secure Resource Partitions
- Learn how to use Tripwire, John the Ripper, nmap, lsof, and other open source tools to further improve HP-UX system security

Course outline

Introduction

- Why security?
- HP-UX security tools
- HP-UX security certifications
- Course agenda

Securing user accounts: user passwords

- Understanding the /etc/passwd file
- Understanding the /etc/shadow file
- DES-based password encryption
- SHA512 password encryption
- Enabling shadow passwords
- Enabling SHA512 passwords
- Enabling long passwords
- Managing passwords
- Configuring password aging
- Cracking passwords with John the Ripper
- Authenticating users via PAM
- Configuring /etc/pam.conf

Securing user accounts: special cases

- Protecting user accounts: guidelines
- Protecting the root account: guidelines
- Limiting root and operator access via /etc/security
- Limiting root and operator access via sudo
- Limiting root and operator access via the restricted SAM builder
- Limiting root and operator access via the SMH
- Configuring accounts for guest users
- Configuring accounts for single application users
- Configuring accounts for teams and groups
- Preventing dormant accounts

Securing user accounts: Standard Mode Security Extensions (SMSE)

- Configuring SMSE user security
- Understanding Standard Mode Security Enhancements Benefits
- Understanding SMSE attributes and repositories
- Configuring /etc/security.dsc
- Configuring /etc/default/security
- Configuring /etc/passwd and /etc/shadow
- Configuring /var/adm/userdb/ via userdbset, userdbget, and userdbck
- Enforcing SMSE security policies

Securing user accounts: Role Based Access Control (RBAC)

- RBAC features and benefits
- Installing RBAC
- Configuring & assigning RBAC roles
- Configuring & assigning RBAC authorizations
- Configuring RBAC commands & privileges
- Verifying the RBAC database
- Configuring RBAC logging & auditing
- Running commands with privrun
- Editing files with privedit
- Enabling RBAC keystroke logging

Protecting data via file permissions and JFS Access Control Lists (ACLs)

- Understanding how hackers exploit improper file and directory permissions
- Viewing and changing file permissions
- Searching for files with improper permissions
- Configuring and using the SUID bit
- Configuring and using the SGID bit
- Configuring and using the sticky bit
- Configuring and using JFS ACLs

Protecting data via swverify, md5sum, and Tripwire

- File integrity checking overview
- Verifying executable integrity with swverify
- Verifying file integrity with md5sum
- Verifying file integrity with Tripwire
- Installing Tripwire
- Creating Tripwire keys
- Creating the Tripwire configuration file
- Creating the Tripwire policy file
- Creating the Tripwire database
- Performing a Tripwire integrity check
- Updating the Tripwire database
- Updating the Tripwire policy file

Protecting data via Encrypted Volumes and File Systems (EVFS)

- EVFS, EVS, and EFS features and benefits
- EVFS architecture
- EVFS volumes
- EVFS volume encryption keys, user keys, and recovery keys
  - Step 1: Installing and configuring EVS software
  - Step 2: Creating user keys
  - Step 3: Creating recovery keys
  - Step 4: Creating an LVM or VxVM volume
  - Step 5: Creating EVS device files
  - Step 6: Creating and populating the volume's EMD
  - Step 7: Enabling the EVS volume
  - Step 8: Creating and mounting a file system
  - Step 9: Enabling autostart

  - Step 10: Migrating data to the EVS volume
  - Step 11: Backing up the EVS configuration
- Managing EVS volume users
- Managing the EVS key database
- Extending an EVS volume
- Reducing an EVS volume
- Removing EVS volumes
- Backing up EVS volumes
- EVS limitations
- EVS and TPM/TCS integration overview

Securing network services: inetd & tcpwrapper

- inetd service overview
- inetd configuration file overview
- Securing inetd
- Securing the inetd internal services
- Securing the RPC services
- Securing the Berkeley services
- Securing FTP
- Securing FTP service classes
- Securing anonymous FTP
- Securing guest FTP
- Securing other ftpaccess security features
- Securing other inetd services
- Securing other non-inetd services
- Securing inetd via TCPwrapper

Securing network services: SSH

- Legacy Network Service Vulnerabilities: DNS
- Legacy Network Service Vulnerabilities: Sniffers
- Legacy Network Service Vulnerabilities: IP spoofing
- Solution: Securing the Network Infrastructure
- Solution: Using Symmetric Key Encryption
- Solution: Using Public Key Encryption
- Solution: Using Public Key Authentication
- HP-UX Encryption & Authentication Product overview
- Configuring SSH encryption & server authentication
- Configuring SSH client/user authentication
- Configuring SSH single sign-on
- Managing SSH keys
- Using the UNIX SSH Clients
- Using PuTTY SSH Clients

Securing network services: IPFilter & nmap

- Firewall overview
- Packet filtering firewalls
- Network Address Translation firewalls
- Host versus perimeter firewalls
- Installing IPFilter

- Managing IPFilter rulesets
- Configuring a default deny policy
- Preventing IP and loopback spoofing
- Controlling ICMP service access
- Controlling access to UDP services
- Controlling access to TCP services
- Controlling access via active and passive FTP
- Testing IPFilter rulesets with ipftest
- Testing IPFilter rulesets with nmap
- Monitoring IPFilter & Nessus

Hardening HP-UX with Bastille

- Bastille overview
- Installing Bastille
- Generating a Bastille assessment
- Creating a Bastille configuration file
- Applying a Bastille configuration file
- Applying a pre-configured Bastille configuration file
- Applying a pre-configured Bastille configuration via Ignite-UX
- Reviewing the Bastille logs
- Monitoring changes with bastille_drift
- Reverting to the pre-Bastille configuration
- Integrating Bastille and HP SIM

Monitoring activity via system log files

- Monitoring log files
- Monitoring logins via last, lastb, and who
- Monitoring processes via ps, top, and whodo
- Monitoring file access via ll, fuser, and lsof
- Monitoring network connections via netstat, idlookup, and lsof
- Monitoring inetd connections
- Monitoring system activity via syslogd
- Configuring /etc/syslog.conf
- Hiding connections, processes, and arguments
- Doctoring log files and time stamps

Monitoring activity via SMSE auditing

- Auditing overview
- Trusted system versus SMSE auditing
- Enabling and disabling auditing
- Verifying auditing
- & system calls to audit
- Selecting users to audit
- Selecting system calls, aliases, and events to audit
- Creating and applying an audit profile
- Viewing and filtering audit trails via auditdp
- Switching audit trails
- Understanding audomon AFS & FSS switches
- Understanding audomon audit trail names

- Configuring audomon parameters
- Configuring audomon custom scripts

Monitoring suspicious activity via HP's Host Intrusion Detection System (HIDS)

- HIDS overview
- HIDS architecture
- Installing HP's HIDS product
- Configuring HIDS detection templates and properties
- Configuring HIDS surveillance groups
- Configuring HIDS surveillance schedules
- Configuring HIDS response scripts
- Assigning surveillance schedules to clients
- Monitoring HIDS alerts and errors

Managing security patches with Software Assistant (SWA)

- Security patch overview
- SWA overview
- Reading US-CERT advisory bulletins
- Reading HP-UX security bulletins
- Installing swa
- Generating swa reports
- Viewing swa reports
- Retrieving swa recommended patches
- Installing swa patches
- Installing other products recommended by swa
- Applying other manual changes
- Regenerating swa reports
- Purging swa caches
- Viewing swa logs
- Customizing swa defaults
- Integrating SWA and HP SIM
- Preventing unauthorized swa and swlist access
- Preventing buffer overflow attacks
- Setting the executable_stack kernel parameter
- Setting the chatr +es executable stack option

Hardening HP-UX with Bastille

- Bastille overview
- Installing Bastille
- Generating a Bastille assessment
- Creating a Bastille configuration file
- Applying a Bastille configuration file
- Applying a pre-configured Bastille configuration file
- Applying a pre-configured Bastille configuration via Ignite-UX
- Reviewing the Bastille logs
- Monitoring changes with bastille_drift
- Reverting to the pre-Bastille configuration

Isolating applications via security compartments

- Security compartment concepts
- & Using FGP TRIALMODE
- Compartment rule concepts
- INIT compartment concepts
- Installing compartment software
- Enabling compartment functionality
- Creating and modifying compartments
- Viewing compartments
- Adding network interface rules
- Adding file permission rules
- Adding a compartment-specific directory
- Viewing compartments
- Configuring compartment administrators
- Configuring compartment users
- Executing commands in compartments
- Removing compartments
- Disabling compartment functionality

Isolating Applications via Secure Resource Partitions

- SRP concepts
- SRP example
- SRP subsystems
- SRP templates
- SRP services
- Installing SRP
- Enabling and configuring SRP
- Verifying the SRP configuration
- Creating an SRP interactively
- Creating an SRP non-interactively
- Adding the init, prm, network, ipfilter, login, and ipsec services to an SRP
- Adding the ssh, apache, tomcat, and oracle templates to an SRP
- Adding the custom template to an SRP
- Deploying an application in an SRP
- Updating an SRP
- Viewing the SRP configuration & status
- Starting & stopping an SRP
- Accessing an SRP
- Removing an SRP

Appendix: Improving user and password security with trusted systems

- Trusted system overview
- Configuring password format policies
- Configuring password aging policies
- Configuring user account policies
- Configuring terminal security policies

- Configuring access control policies
- Configuring password aging policies
- Understanding the /tcb directory structure

Appendix: Implementing chroot()

- Limiting file access via chroot()
- Configuring chroot()ed applications

Appendix: Implementing Fine Grained Privileges (FGP)

- Limiting privileges via FGP
- Installing FGP Software
- Installing FGP Software
- Recognized Privileges
- Permitted, Effective, and Retained Privilege Sets
- Configuring FGP Privileges via setfilexsec
- Configuring FGP Privileges via RBAC
- Configuring & Using FGP TRIALMODE

Appendix: Configuring Process Resource Manager (PRM)

- Allocating resources without PRM
- Allocating resources with PRM
- PRM advantages
- PRM managers
- PRM groups
- PRM Fair Share Scheduler concepts & configuration
- PRM PSET concepts & configuration
- PRM memory manager concepts & configuration
- Reviewing available resources
- Analyzing application requirements
- Enabling PRM
- Creating and updating the PRM configuration file
- Monitoring resource usage

Learn more at
hp.com/us/training/americas

H3541S Ver H.00

c04725202 July 2015