



hp services

education

course description

internet security

h7076s

course overview

This three-day course presents specific Internet security tools and products used on UNIX systems that are needed to ensure secure communications across the public Internet. Lectures, demonstrations, and exercises feature specific commercial security products offered by HP, and standards-based network security tools from industry vendors, including HP IPSec/9000, Virtual Private Networks (VPN), Public Key Infrastructure (PKI), Lightweight Directory Access Protocol (LDAP), Kerberos and Kerberized Internet Services, and Intrusion Detection Software (IDS/9000).

audience

HP-UX system administrators who are responsible for the security of their systems on the Internet

benefits to you

- Receive practical skills to use on your job and increase your productivity: Quickly gain the knowledge and expertise needed to protect Internet communications between two UNIX systems. Be able to detect intrusions and security violations on multiple systems from a single point.
- Realize maximum benefits through familiarity with a range of technologies and validate your training investment: Learn to install and configure Internet security tools and products to protect systems on the Internet.

pre-requisites

Practical UNIX System and Internet Security (H3541S) or equivalent experience.

course objectives

- On completion of this course, you will be able to do the following:
- Identify and use security tools within various network environments.
 - Describe types of virtual private networks (VPNs) and vendors supporting these VPNs.
 - Be familiar with the features of IPFilter/9000, a system firewall packet-filtering product, and be able to install it on the HP-UX operating system.
 - Install and configure a VPN using the SocksV5 software.
 - Demonstrate a thorough understanding of IPSec features, including confidentiality, authentication, integrity, packet filtering, non-repudiation, and management.
 - Demonstrate an understanding of IPSec configuration elements.
 - Understand and use of the Lightweight Directory Access Protocol (LDAP).
 - Use intrusion detection software to monitor and detect changes to critical system files.

next steps

Check out our advanced HP-UX courses on other topic areas, including the following: high availability, networking, performance, and operations.

to order

You can order this course online at <http://education.hp.com>. At the site, select a country, then choose "registration" or "Book a course" and fill out the online registration form.

why hp education services?

- Experienced and best-in-field HP instructors
- Comprehensive student materials
- State-of-the-art classroom facilities
- Hands-on practice
- Focus on job-specific skills
- More than 260 locations worldwide
- Customized on-site delivery
- Online instructor-led and self-paced training at <http://itresourcecenter.hp.com>

detailed course outline: internet security (h7076s)

module

Introduction to Internet Security

key topics

- Welcome to Internet security
- Network model for this course
- Topics and goals of the Practical UNIX System Security course
- Topics and goals of the Internet Security course
- Elements of Internet security

Virtual Private Networks (VPNs)

- The security problem with IP today
- Types of Virtual Private Networks
- HP solutions for VPNs
- Network-to-Network VPNs
- Remote access VPNs
- Host-to-Host VPNs
- VPN software products
- HP IPFilter/9000 system firewall product
- Installing HP IPFilter/9000
- Lab: Implementing a simple IPFilter system firewall

IPSec Overview

- IPSec functionality
- Autonomy of a network packet
- Network tracing and logging
- Capturing packets off the Internet
- Symmetric cryptography: encryption and decryption
- How Encapsulating Security Payload (ESP) protocol provides data integrity and privacy
- Authentication symmetric-key hash functions
- How authentication headers work
- Symmetric key bootstrap problem
- Internet Key Exchange (IKE) overview
- Protecting against an IKE daemon bluff
- Application data flow with and without IPSec
- Overcoming security obstacles
- Review: IPSec concepts

IPSec Configuration

- IPSec product requirements
- IPSec topologies
- IPSec filtering and actions on an IP packet
- Cookbook for configuring IPSec
- IPSec GUI manager
- IPSec manager: creating a policy
- IPSec policy: filtering parameters
- IPSec: creating an internet key exchange policy
- IPSec: defining pre-shared keys
- Start IPSec functionality and monitor IPSec status
- Lab: IPSec configuration and connection testing

Lightweight Directory Access Protocol (LDAP) Overview and Configuration

- The LDAP directory service
- LDAP directory tree
- LDAP object class and attributes
- LDAP installation and configuration procedure
- Configuring the first LDAP client and installing additional LDAP clients
- Netscape Directory Server installation and configuration
- Installing LDAP client services installation and defining POSIX object classes
- Testing the LDAP configuration
- Lab: LDAP-UX client services integration

Public Key Infrastructure (PKI) Overview and Configuration

- PKI architecture
- Symmetric key cryptography
- Public key cryptography
- Message digest and message authentication codes
- Digital signatures
- PKI key distribution
- Private key distribution
- Application data flow without security
- Lab: PKI integration

Intrusion Detection Software

- Intrusion Detection Software (IDS) basics
- IDS client/server architecture
- IDS pre-configured detection templates for identifying unauthorized system activity
- Surveillance groups
- Surveillance schedules
- Surveillance schedules for each host
- IDS system management window (HP IDS/9000)
- Alert browser screen for displaying potential security breaches
- Error browser for viewing errors on systems running IDS/9000 agents
- Lab: IDS/9000 installation and configuration

Kerberos Overview

- What is Kerberos?
- How Kerberos encrypts data
- Kerberos user and application authentication
- Application verification
- Kerberos ticket granting service
- User authentication with ticket
- Kerberos realms
- Kerberos KDC server configuration
- Lab: Kerberos KDC configuration

Kerberos Client Services

- Kerberos client services
- Installing Kerberos client systems
- Kerberos user programs
- Installing Kerberos application servers
- The pam.conf file
- Using Kerberos in Authentication Mode
- Lab: Configuring Kerberos client services

Miscellaneous Network Security Features

- Other network security features
- DNSSEC security features
- Secure Internet routing
- New e-mail security features
- Anti-spamming e-mail security features

for more information

To locate country contact information and to learn more about HP Education Services, please visit our worldwide web site on the internet at <http://education.hp.com>.

Technical information in this document is subject to change without notice.

©Copyright Hewlett-Packard Company 2001. All Rights Reserved. Reproduction, adaptation, or translation without prior written permission is prohibited except as allowed under the copyright laws.

05/01 rev. b
H7076s

