HP-UX Security

H3541S

Delivery Type: Classroom

Duration: 5 days

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. The 5-day course is 50% lecture and 50% hands-on labs using HP servers.

Pre-Requisites

- ✓ HP-UX System and Network Administration I (H3064S)
- ✓ HP-UX System and Network Administration II (H3065S) H3064S
- ✓ HP-UX System and Network Administration for Experienced UNIX® System Administrators. H5875S

or equivalent experience

Objectives

- ✓ Download and install security patches.
- ✓ Manage your passwords, enable password ageing, and verify user password security.
- ✓ Install, configure and manage RBAC.
- ✓ Configure HIDS to monitor security incidents on client systems.
- ✓ Identify, configure and disable network services to imporve security.
- ✓ Enable and configure Bastille for standardized security policies.
- ✓ Understand the information hackers attempt to gather about a target system and how they monitor and hide their activities.
- ✓ Identify software vulnerabilities and prevent buffer overflow attacks.
- ✓ Manage user security attributes and user accounts.
- ✓ Configure and user JFS ACLs to secure files and directories.
- ✓ Identify files and directories at risk for backdoor access.
- ✓ Install and configure an IPFilter system firewall to block and allow service access.

Target Audience

This course is suitable for experienced UNIX system and network administrators who need to better secure their HP-UX systems.

Follow on Courses

HP-UX Security II: Security Containment HC721S