# HP-UX Security

## Duration: 5 Days  Course Code: H3541S

### 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.

### Target Audience:

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

### 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.

### Prerequisites:

- 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

### Follow-on-Courses:

- HP-UX Security II: Security Containment HC721S

### Further Information:

For More information, or to book your course, please call us on Head Office + 254 713 027 191

training@clclearningafrica.com

www.clclearningafrica.com

Computer Learning Centre 2nd Floor Museum Hill Centre, Muthithi Road, Westlands, Nairobi, Kenya