

# Course Outline



Tel: +44 (0) 118 979 4000 Fax: +44 (0) 118 979 4000

Email: [training@ptr.co.uk](mailto:training@ptr.co.uk) Web: [www.ptr.co.uk](http://www.ptr.co.uk)

## Unix Audit & Security

### Course Description:

The course is intended for those who need to find out what UNIX is and where the different components are located, with a specific security objective in mind. In conjunction with an explanation of the technology, the prime risks and defences will be pointed out. Delegates who will benefit most from this course are typically computer auditors, security specialists and security conscious managers. The course also serves as a useful general introduction to UNIX.

Having acquired a high level understanding of UNIX, you will learn how to assess security hands on. All aspects are covered, both business and technical. You will hear commentary on certain real disasters that have happened to high profile companies in the past.

Planning for audits and discussion of suitable tests forms a substantial part of the course. Delegates will get a chance to run audit and security related commands. See what the administrators do. Find out how you could script your own TRIPWIRE.

Though the course is designed specifically for a SUN Solaris installation, it will serve as a good general overview for any flavour of UNIX.

### Pre-requisites:

Delegates should have had some experience of using UNIX beforehand and be able to enter simple shell commands, like 'ls' and 'more', in a terminal environment. Shell programming and C programming experience would be an advantage.

### Course Content:

# Course Outline



Tel: +44 (0) 118 979 4000

Fax: +44 (0) 118 979 4000

Email: [training@ptr.co.uk](mailto:training@ptr.co.uk)

Web: [www.ptr.co.uk](http://www.ptr.co.uk)

- **Introduction To Audit & Security**
  - Audit & Security
  - Security
  - Audit
  - Checklist-Based Auditing
  - Risk-Based Auditing
  - Audit Plan
  - Check Lists
  - DISA Database STIG
  - NIST
  - The Big Picture
  
- **Access Control**
  - Intrusion Prevention
  - Intrusion Detection
  - Secure Data Storage
  - Secure Data Access
  - UNIX Deployment Model
  - Managing Logins
  - Login Processes
  - Local Login
    - ('Old'; System V &ndash; up to Sys V Rel 3)
    - ('New'; System V &ndash; from Sys V Rel 4)
  - (BSD Unix)
  - Network Login
  - Accepting a login name
  - Logon Banners
  
- **Introduction To UNIX**
  - History Of Unix
  - Unix Features
  - Unix System V
  - Standards
  - UNIX Architecture

21a Peach Street Wokingham Berkshire RG40 1XJ

**Tel** 0118 979 4000 **Fax** 0118 979 4035 **Email** [training@ptr.co.uk](mailto:training@ptr.co.uk) **www.ptr.co.uk**

Registered Office: Grenville Court Britwell Road Burnham Bucks SL1 8DF Company Registered No: 2442290 – VAT registration No:532 1929 56

# Course Outline



Tel: +44 (0) 118 979 4000

Fax: +44 (0) 118 979 4000

Email: [training@ptr.co.uk](mailto:training@ptr.co.uk)

Web: [www.ptr.co.uk](http://www.ptr.co.uk)

- **Introduction To UNIX**
  - UNIX Standards
  - Product Standards
  - Application Programming Interface
  - Commands & Utilities
  - Operating System Versions
  - Solaris
  - HP-UX
  - AIX
  - IRIX
  - Linux
  - Patch Levels
  
- **UNIX Startup & Shutdown**
  - Power On
  - Kernel Processes
  - init
  - System V
  - BSD
  - Changing Run Levels
  - Changing run levels with init
  - Graceful Run Level Changes
  - Quick Shutdown
  - Firmware
  - boot to Single User Mode
  - Start Solaris Installation
  - boot From alternative boot disk
  - Emergency boot From CDROM
  
- **Creating & Maintaining User Accounts**
  - /etc/passwd
  - /etc/shadow
  - useradd
  - The group file
  - The Shells

21a Peach Street Wokingham Berkshire RG40 1XJ

**Tel** 0118 979 4000 **Fax** 0118 979 4035 **Email** [training@ptr.co.uk](mailto:training@ptr.co.uk) **www.ptr.co.uk**

Registered Office: Grenville Court Britwell Road Burnham Bucks SL1 8DF Company Registered No: 2442290 – VAT registration No:532 1929 56

# Course Outline



Tel: +44 (0) 118 979 4000

Fax: +44 (0) 118 979 4000

Email: [training@ptr.co.uk](mailto:training@ptr.co.uk)

Web: [www.ptr.co.uk](http://www.ptr.co.uk)

- **Creating & Maintaining User Accounts**
  - Customising User Environments - Initialisation Scripts
  - Password Management
  - Lock A User Account
  - The root Account
  - Restricting Root Access
  - Encrypting Root Network Access
  - Reserved User Accounts
  - Single-User Mode
  - Multi-User Mode
  - Shared User Accounts
  - Duplicate User ID Accounts
  
- **System Security**
  - Usernames & Passwords
  - /etc/passwd and /etc/shadow
  - Password Ageing
  - Login Control with /etc/default/login
  - Switching User with su
  - su Control with /etc/default/su
  - Limiting The Number Of Failed Login Attempts
  - Setting Minimum Password Length
  - Password Character Mix
  - Password Repeating Characters
  - Standard File & Directory Permissions
  - File & Directory Permissions
  - Special Permissions SUID & GUID
  - Access Control Lists
  
- **Process Management**
  - Processes Overview
  - Parent & Child
  - Killing Application Processes
  - Changing Process Priorities

21a Peach Street Wokingham Berkshire RG40 1XJ

**Tel** 0118 979 4000 **Fax** 0118 979 4035 **Email** [training@ptr.co.uk](mailto:training@ptr.co.uk) **www.ptr.co.uk**

Registered Office: Grenville Court Britwell Road Burnham Bucks SL1 8DF Company Registered No: 2442290 – VAT registration No:532 1929 56

# Course Outline



Tel: +44 (0) 118 979 4000

Fax: +44 (0) 118 979 4000

Email: [training@ptr.co.uk](mailto:training@ptr.co.uk)

Web: [www.ptr.co.uk](http://www.ptr.co.uk)

- **Process Management**
  - Changing Priority of Running Processes With renice
- **Scheduling & Job Control**
  - Delayed Execution with the at Command
  - Restricting Access To at
  - Cron
  - Restricting Access To cron
  - Logging
- **Disk Management**
  - Partition and Volume Group Layout
  - Disk Layout
  - Solaris Partitions & Slices
  - Device Files
  - Logical Device Names
  - RAID
  - Physical Device Names
  - UNIX File Systems
    - Traditional UNIX Filesystem
    - Journaled File Systems
    - Mounting a Filesystem
    - Unmounting a File System
    - Mounting At Boot Time
    - Traditional File System Corruption
    - File System Checking With fsck
  - NFS File Systems
  - RAM Based File Systems
  - Swap Management
- **Backing Up**
  - Backup Media
  - Why Backup?
  - Backup Types
  - Full Backup

21a Peach Street Wokingham Berkshire RG40 1XJ

**Tel** 0118 979 4000 **Fax** 0118 979 4035 **Email** [training@ptr.co.uk](mailto:training@ptr.co.uk) **www.ptr.co.uk**

Registered Office: Grenville Court Britwell Road Burnham Bucks SL1 8DF Company Registered No: 2442290 – VAT registration No:532 1929 56

# Course Outline



Tel: +44 (0) 118 979 4000

Fax: +44 (0) 118 979 4000

Email: [training@ptr.co.uk](mailto:training@ptr.co.uk)

Web: [www.ptr.co.uk](http://www.ptr.co.uk)

- **Backing Up**
  - Incremental Backup
  - Partial Backup
  - Backing Up With tar
  - Absolute and Relative Paths
  - Image Copying With dd
  - Backing Up With cpio
  - Backing Up With dump
  - Dump Levels
  
- **Network Services**
  - TELNET
  - Secure Shell
  - FTP
  - Restricting FTP access
  - Anonymous FTP
  - Secure FTP
  - The R Commands
  - Host-Level Security with /etc/hosts.equiv
  - User-Level Security with .rhosts
  - The rlogin Command
  - The rcp Command
  - The rsh & rcmd Commands
  
- **UNIX Vulnerabilites**
  - Intrusion Detection
  - Network Services
  - /etc/inetd.conf
  - /etc/hosts.allow
  - Denial Of Service Attacks
  - Trojan Horses, Viruses & Worms
  - Vi Editor
  - .exerc
  - Shell Escapes
  - Set user ID programs

21a Peach Street Wokingham Berkshire RG40 1XJ

**Tel** 0118 979 4000 **Fax** 0118 979 4035 **Email** [training@ptr.co.uk](mailto:training@ptr.co.uk) **www.ptr.co.uk**

Registered Office: Grenville Court Britwell Road Burnham Bucks SL1 8DF Company Registered No: 2442290 – VAT registration No:532 1929 56

# Course Outline



Tel: +44 (0) 118 979 4000

Fax: +44 (0) 118 979 4000

Email: [training@ptr.co.uk](mailto:training@ptr.co.uk)

Web: [www.ptr.co.uk](http://www.ptr.co.uk)

- **UNIX Vulnerabilites**
  - Booting from CD
  - File System Ownership & Permissions
  - File system Corruption
  - Startup and Shutdown Scripts
  - UNIX services
  - Network Service User Equivalence
  - Backup storage
  - System Clock
  
- **UNIX Auditing**
  - The find command
  - The grep command
  - The who command
  - The last command
  - The ps command
  - System Accounting

**Course Duration:**

**2 Days**