

## Securing the Solaris 10 Operating Environment

### Course Summary

**Length:** 5 Days

**Prerequisite:** Solaris 10 System Administration Part 1 and Part 2

#### **Recommendation Statement:**

To succeed fully in this course, students should already know how to:

Manage files and directories · Control the user work environment · Archive files · Use remote commands · Manage file systems · Install software · Perform system boot procedures · Perform user and security administration · Manage network printers and system processes · Perform system backups and restores · Understand system startup procedures and the SMF.

#### **Description:**

This course teaches the student how to harden and secure the Solaris 10 operating environment. The operating system will be Solaris 10 (SunOS 5.10 release 10/09)- Sun's implementation of SystemV release4. The course is taught on both Sun SPARC and x-86-based servers

#### **Objectives**

Upon completion of this course, you should be able to:

- Understand the Solaris 10 OS Security Features
- Understand the Solaris 10 Network Security Features

#### **Topics**

- Describe Solaris 10 Security
- Understand Minimization
- Using the Solaris Basic Security Module (BSM)
- Patching the OS
- Detect and Prevent Trojan and Backdoor attacks
- Administering User Accounts and User Rights
- Administering Password Security
- Securing Root Access
- Secure File Systems
- Basic Audit Reporting Tool (BART)
- Securing Network Services
- Secure Remote Access
- Automate Server Hardening
- Securing the Solaris OE using Zones

#### **Audience**

This course is designed for System Administrators that must harden and secure the Solaris 10 operating Environment.

## **Securing the Solaris 10 Operating Environment**

Detailed Course Outline – 5 Days

### **Describe Solaris 10 Security**

- Understand security principles
- Understand how auditing and patching impacts security

### **Understand Minimization**

- Understand a minimal installation
- Software installation clusters
- Creating a consistent configuration

### **Using the Solaris Basic Security Module (BSM)**

- Configure Auditing
- Create an Audit trail
- Interpret audit data
- BSM Device management

### **Patching the OS**

- Describe methods of analyzing and patching the OS
- Signed vs. unsigned patches
- Specifying a WEB Proxy

### **Detect and Prevent Trojan and Backdoor attacks**

- Using Rootkit utilities
- Detect and Prevent DoS attacks

### **Administering User Accounts and User Rights**

- Configure special user security
- Limit users with restricted shells
- Configure RBAC
- Control Access
- Implementing Password Strength, Syntax Checking, History and Aging Improvements

### **Administering Password Security**

- Examine and set password policies
- Using the crack utility

### **Securing Root Access**

- Control root access using Role Based Access Accounts
- Installing and configuring sudo

## **Secure File Systems**

- File system audit tools
- Secure /tmp
- Examine file system permissions
- Understanding setuid and setgid permissions
- Using Access Control Lists (ACLs)
- Understand crypt

## **Basic Audit Reporting Tool (BART)**

- Implement the Basic Audit and Report Tool (BART) for File Integrity

## **Securing Network Services**

- Understand SMF
- Understand least privilege
- Securing Berkeley "r" commands
- Disabling unnecessary network services
- Reconfigure and limit network services
- Explore TCP wrappers
- Configure TCP wrappers
- Limiting service privileges

## **Secure Remote Access**

- Describe the secure shell (SSH)
- Configure (SSH)
- Using SSH and SFTP

## **Automate Server Hardening**

- Describe the system hardening process
- Harden a system using SST
- Installing and configuring SST

## **Securing the Solaris OE using Zones**

- Describe security concerns in Solaris zones
- Global zone vs. non-global zone
- Resource management
- Implement security in Solaris zones
- Patching zones