

Course Description

This course provides students with the knowledge and skills to customize security on Solaris 10 operating systems.

Who Can Benefit

Students who can benefit from this course are security, system, and network administrators who are responsible for customizing security on Solaris 10 systems.

Prerequisites

To succeed fully in this course, students should be able to:

- Administer users, packages, and applications on Solaris 10 systems
- Administer networking and routing on Solaris 10 systems
- Describe basic system and network security concepts
- Administer services and zones on Solaris 10 systems

Skills Gained

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

Install, configure, and administer systems installed with the Solaris 10 Operating System (OS) and understand the following Solaris 10 OS security concepts:

- Principles and features
- Installing systems securely
- Principle of Least Privilege
- File integrity and privacy
- Application and network security
- Auditing and zone security

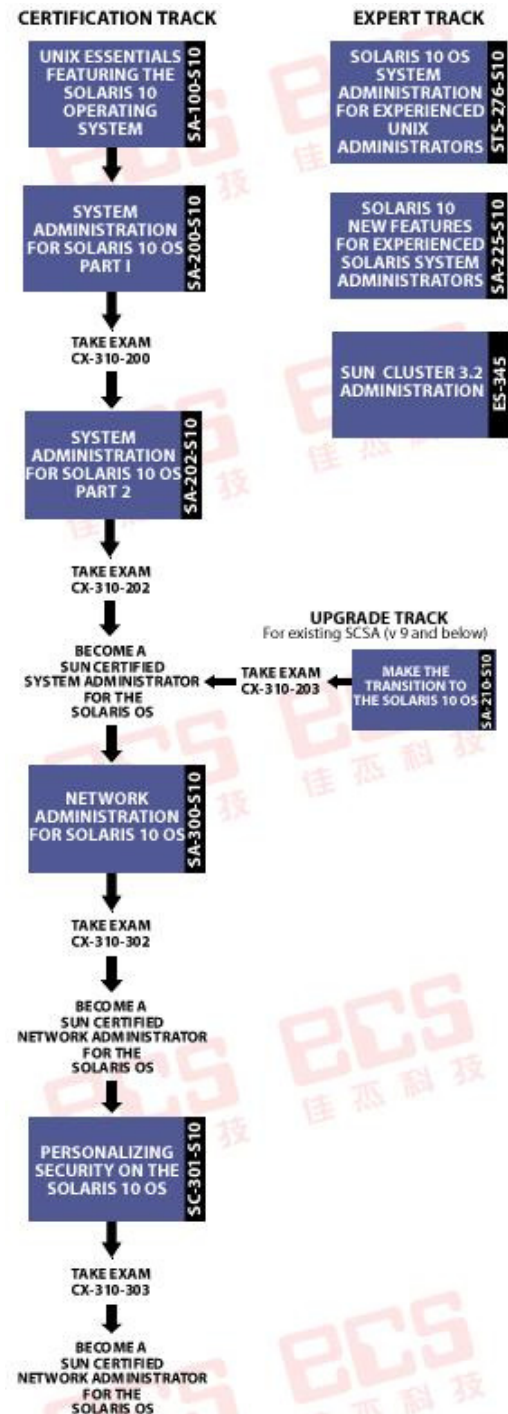
Related Courses

Before:

- Completed Solaris 10 System Administration Courses
- Network Administration for the Solaris 10 Operating System (SA-300-S10)

After:

- Solaris Operating System Network Intrusion Detection (SC-345)
- Solaris 10 New Features for Experienced Solaris System Administrators (SA-225-S10)
- Enterprise Security Using Kerberos (SC-360)
- Computer Security Forensics and System Recovery (SC-410)



REGISTRATION AND INFORMATION

education@ecs.com.sg
www.ecs.com.sg/training

Outline

Module 1 - Describing Basic Security Principles

- Describe the need for a security policy
- Describe the need to securely configure systems
- Describe hardening systems
- Describe minimized systems
- Describe appropriate system configuration
- Describe the need for auditing
- Describe logging to meet legislative compliance

Module 2 - Listing Applicable Solaris 10 Security Features

- Describe these new features included in the Solaris 10 Operating System (OS):
- The device policy
- Kerberos-enabled applications, Lightweight Directory Access Protocol (LDAP), and interoperability enhancements
- Process rights management
- Solaris Containers
- User rights management (Role Based Access Control)
- Password strength, syntax checking, history, and aging improvements
- Basic Audit and Report Tool (BART) for file integrity
- IPfilter stateful packet filtering firewall
- Solaris Secure Shell
- IPsec/Internet Key Exchange (IKE) performance enhancements
- Solaris auditing
- Trusted Extensions
- SSL encryption with PKCS#11 interface and OpenSSL
- PAM improvements
- MD5 hash functions built into the Solaris OS

Module 3 - Describing Minimization

- Describe a minimal installation
- Describe software installation clusters (metaclusters)
- Examine loose compared to strict minimization
- Provide consistent, known configuration for installations

Module 4 - Managing Patches

- Describe the Solaris 10 Update Manager
- Describe signed patches
- Understand how to verify signatures for a signed patches
- Specify a web proxy when installing a signed patch

Module 5 - Performing Hardening

- Understand what is involved when performing system hardening
- Use the Solaris Security Toolkit (SST)
- Understand the software component of SST
- Use SST for system hardening
- Use SST for system security audits

Module 6 - Implementing Process Rights Management

- Describe process rights management
- Describe process privileges
- Understand how to determine rights required by processes
- Understand how to debug privileges
- Assign minimum rights to a process

Module 7 - Implementing User Rights Management

- Describe access controls
- Understand and use Role Based Access Control
- Explain what is meant by a rights profile
- Understand and use a role
- Explain authorizations and privileges in RBAC
- Configure and use password history
- Configure password selection constraints
- Understand how to use strong cryptographic algorithms for passwords

Module 8 - Utilizing the Solaris Cryptographic Framework

- Describe the role of the Solaris Cryptographic Framework
- Administer and maintain the Solaris Cryptographic Framework
- Explain and use the digest(1), mac(1), encrypt(1), and decrypt(1) commands
- Manage the Solaris Cryptographic Framework environment
- Describe how the Solaris Cryptographic Framework can be used with Java applications, web servers, and the Sun Crypt accelerator cards

Module 9 - Managing File system Security

- Use the elfsign(1) command to verify Solaris 10 OS Executable and Linkable Format (ELF) objects
- Describe and use the Basic Audit and Report Tool
- Describe secure execution

Module 10 - Using the Service Management Facility

- Describe the Service Management Facility
- Describe the concept of least privilege
- Describe authorization
- Limit a service's privileges
- Examine a service's current privileges

Continue next page ...

REGISTRATION AND INFORMATION

education@ecs.com.sg
www.ecs.com.sg/training

Module 11 - Securing Networks

- Describe network access controls
- Describe TCP Wrappers in the Solaris 10 OS
- Implement the Solaris IP Filter Stateful Packet Filtering Firewall
- Describe Kerberos security
- Understand and use Solaris Secure Shell
- Describe the security features of NFSv4

Module 12 - Implementing IPsec

- Describe IP Security (IPsec) and the Internet Key Exchange (IKE) protocols
- Describe the various ways IPsec can be configured
- Describe two ways to configure IKE
- Describe methods used for troubleshooting IPsec and IKE configurations

Module 13 - Performing Auditing and Logging

- Describe Solaris auditing
- Configure an audit policy
- Implement Solaris auditing
- Configure auditing on a system implementing Solaris zones
- Access the audit data from the audit trail
- Describe how the audit records can be used
- Protect audit information on a system or in the enterprise

Module 14 - Implementing Security in Solaris Zones

- Describe security characteristics of a Solaris system with zones installed
- Understand the differences between the subjects already covered and how they apply to the Solaris operating system with zones installed
- Describe the global zone
- Explain when and how to use zones
- Describe resource management in a zone
- Address zones and network security
- Understand patching zones

Module 15 - How Security Components Work Together

- Describe how security components work together
- Describe how technologies interact
- Describe infrastructure requirements