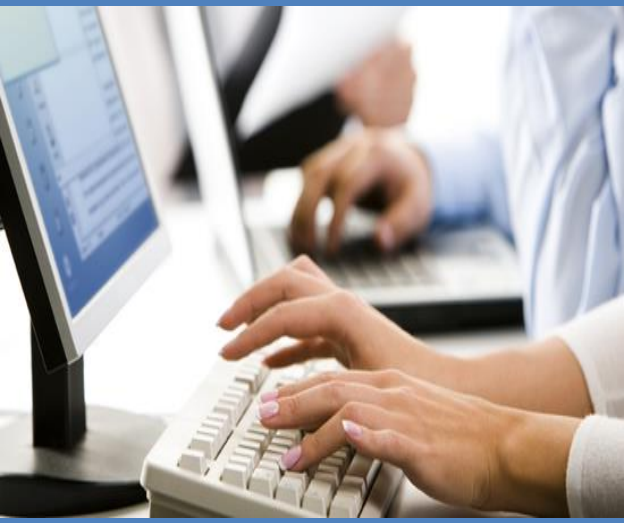
AIX Security for Power Systems – Customer Onsite

Education & Training Services

Skills and expertise to help you increase the business value from your Power Systems investment.



Purpose:
Today's leaders face multiple challenges, including the need to secure the enterprise against a barrage of new and evolving sophisticated threats. The IBM business-driven approach to enterprise security helps to identify gaps in your existing capabilities across the people, processes, applications, data, technology and physical facilities across your organization.

The goal of this workshop is to provide participants a detailed knowledge and hands-on experience in implementing AIX security mechanisms under AIX 6.1, AIX 7.1 and AIX 7.2.

For additional details on other workshops, please visit: https://www.tlcpak.com/educ.html

Audience:
This course is intended for persons who:

- Want to learn what the security mechanisms are built-in AIX Version 7.2 and 7.1
- Will plan, implement, or distribute a security policy in AIX

The audience for this training includes:

- AIX technical support individuals
- System administrators
- System architects

Prerequisites:
Students should have basic AIX administration experience. The AIX prerequisite may be met by attending the following curse or having equivalent AIX skills:

- Power Systems for AIX II - AIX Implementation and Administration (AN120)

Information is not just an important element of your organization's success; it's an essential business asset that must be kept secure.

* This course is also available for customers using AIX 6.1

High-level Objectives:

On completion of this workshop participants should be able to:

- Security in an IT Environment
- Describe security threats to a computer system
- Understand AIX Base Security in detail
- List the AIX commands and components that can meet both the base system and network security threats.
- Configure, distribute, and monitor a security policy using AIX Security Expert.
- Configure the Role Based Access Control (RBAC) feature
- Implement the encrypted file systems feature

Course Contents

Security in an IT Environment

- Define the importance of IT Security
- Describe common threats to IT security
- Define a basic model of security architecture
- Understanding Logical and physical security
- List common AIX security services and threats
- List AIX mechanisms for host security
- List general guidelines for security policies
- Firewall Technologies
- Enterprise Security in a view
- Integrating the physical, logical security layer
- IBM Security Framework.

AIX Security for Power Systems – Customer Onsite

Education & Training Services

AIX Base System Security
- Understand the concepts of users and groups.
- Controlling root access on the system.
- Define the uses of SUID, SGID and SVTX bits.
- Understanding system wide security critical logs.
- Users initialization process in AIX.
- Assigning security privileges to a normal user.
- Add/Change/Delete user and group accounts.
- Setting up a long character user login ID.
- Locking and unlocking a user account.
- Assigning users with ADMIN rights.
- AIX security files associated with Users & Groups.
- AIX security checkpoint for security administrator.
- Documenting Security Policy and Setup.

AIX Network Security
- Potential security breaches in TCP/IP
- Check common security requirements: Availability, Integrity, Confidentiality and Monitoring
- Understanding TCP/IP start-up flow
- TCP/IP network services – Ports and Sockets
- Use AIX Network Monitoring tools – iptrace, ipreport, netpmon and securetcpip
- Understanding network configuration files
- Why ssh is secure as compare to telnet
- Hardening host security.

Implementing Role Based Accessed Control
- Introduction to AIX Role Back Access Control
- Traditional approach to AIX system administration
- Understanding available roles and authorizations
- Describe the role of Kernel Security Table
- The RBAC Framework. Understand AIX RBAC commands
- Configuring Role Based Access Control
- Understanding Domain RBAC.

Implementing Encrypted Filesystems
- Introduction to Encrypted File System
- AIX Encrypted File System usability
- Understanding CryptoLite cryptographic library
- Create and test EFS and related commands.

Implementing & Distrubuting a Security Policy with AIXpert
- Holistic view of AIX security framework
- Learn about AIX security and regulatory and compliance
- Understand AIXpert and different levels of securities levels
- Illustrates how to configure security levels
- Understand AIXpert file repositories
- Distributing a security policy
- Undo a security policy
- Check the consistency of the security policy
- AIX security policy hardening groups
- Disabling the remote logins
- Actions against server tampering

.

* This course is also available for customers using AIX 6.1

Maintaining Systems Availability
- System continuous availability
- Understand Denial of Service (DoS) attack
- DoS Vs. DDoS – A Basic AIX Example
- Basic tools for detecting DoS attacks
- AIX host security checklist
- List common warning signs of a security breach
- AIX commands used to detect intrusion
- Real Time countermeasures
- Cleaning up the system after intrusion

Course Code
SC181

Course Duration
2 Day

Course Location
Customer onsite (Karachi, Lahore and Islamabad)

Terms & Conditions
100% payment in advance

This course shall be conducted by certified experienced facilitators imparting IBM AIX courses and workshops both locally and internationally for over 20 years.

For additional information please write to us at: info@tlcpak.com
or send us your nominations at www.tlcpak.com/nomination.html