Aruba Network Security Fundamentals

The Aruba Network Security Fundamentals course covers foundational security concepts and prepares candidates to take the exam to achieve Aruba Certified Networking Security Associate (ACNSA) certification. The course describes common security threats and vulnerabilities and provides an overview of important security technologies. It teaches how to create a trusted network infrastructure with Aruba mobility solutions and switches. In addition to discussing device hardening, the course discusses implementing security at the edge with AAA, basic roles and firewall policies, dynamic segmentation, and endpoint classification. The course will further explain basic threat detection technologies and how to collect logs and alarms and use them to initiate an investigation.

Duration: 32 HOURS

Course Content

- **Security Threats and Aruba Security Strategy**
  - Threats Overview
  - Attack Stages
  - Aruba Security Strategy
- **Security Technologies**
  - Regulatory Compliance
  - Secure Communications: Symmetric Encryption and Hash-Based Authentication
  - Secure Communications: Asymmetric Encryption and Digital Certificates
  - Secure Communications: TLS
  - Authentication, Authorization, Accounting (AAA)
- **Harden Aruba Switches**
  - Hardening Overview

    - Set Up Out-of-Band Management
    - Authenticate Managers Securely
    - Ensure Physical Security and Other Hardening Actions
- **Harden ArubaOS Wireless Devices**
    - Lock Down Administrative Access
    - Lock Down Services
    - Use CPSec
- **Enhance LAN Security**
    - Spanning Tree Protections
    - DHCP Snooping and ARP Protection
    - Secure Routing Technologies
- **Network Authentication Technologies**
    - Network Authentication
    - WLAN Security—Encryption + Authentication
- **Enforce Edge Security with an Aruba Infrastructure**
    - Enforce WPA3-Enterprise
    - Enforce 802.1X on the Wired Network
- **Enforce Role-Based Authentication and Access Control**
    - Aruba Role-Based Firewall Policies
    - Dynamic Segmentation
- **Identify and Classify Endpoints**
    - Endpoint Classification Introduction
    - DHCP Fingerprinting with ArubaOS Mobility Devices
    - Aruba ClearPass Policy Manager Device Profiler
    - ClearPass Device Insight
- **Branch Security**
    - Introduction to Aruba SD-Branch Solutions
- **Implement Threat Detection and Forensics**
    - Understand Forensics
    - Analyze ArubaOS WIP Events
- **Troubleshoot and Monitor**
    - Introduction to Troubleshooting Authentication Issues
    - Using ClearPass Tools to Troubleshoot Some Common Issues
    - Packet Captures
    - Monitoring