KOENIG
step forward

Aruba Network Security Fundamentals, Rev. 20.41

Module 1: **Security Threats and Aruba Security Strategy**

- Threats Overview
- Attack Stages
- Aruba Security Strategy

Module 2: 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

Module 3: Harden Aruba Switches

- Hardening Overview
- Set Up Out-of-Band Management
- Authenticate Managers Securely
- Ensure Physical Security and Other Hardening Actions

Module 4: Harden ArubaOS Wireless Devices

- Lock Down Administrative Access
- Lock Down Services
- Use CPSec

Module 5: Enhance LAN Security

- Spanning Tree Protections
- DHCP Snooping and ARP Protection
- Secure Routing Technologies

Module 6: Network Authentication Technologies

- Network Authentication
- WLAN Security—Encryption + Authentication

Module 7: Enforce Edge Security with an Aruba Infrastructure

- Enforce WPA3-Enterprise
- Enforce 802.1X on the Wired Network

Module 8: Enforce Role-Based Authentication and Access Control

- Aruba Role-Based Firewall Policies
- Dynamic Segmentation

Module 9: Identify and Classify Endpoints

- Endpoint Classification Introduction

- DHCP Fingerprinting with ArubaOS Mobility Devices
- Aruba Clear Pass Policy Manager Device Profiler
- Clear Pass Device Insight

Module 10: Branch Security

- Introduction to Aruba SD-Branch Solutions

Module 11: Implement Threat Detection and Forensics

- Understand Forensics
- Analyze ArubaOS WIP Events

Module 12: Troubleshoot and Monitor

- Introduction to Troubleshooting Authentication Issues
- Using Clear Pass Tools to Troubleshoot Some Common Issues
- Packet Captures
- Monitoring