

Course Training

HPE Aruba Networking Certified Associate – Network Security (ACA-NS) Exam HPE6 – A78

รายละเอียดหลักสูตร

หลักสูตร HPE Aruba Networking Security Fundamentals มุ่งเน้นการสอนแนวคิดพื้นฐานด้านความปลอดภัยทางไซเบอร์ และเตรียมความพร้อมให้แก่ผู้เรียนสำหรับการทดสอบเพื่อรับใบรับรองวิชาชีพ ACA - Network Security (ACA-NS) ทั้งนี้ หลักสูตรจะอธิบายถึงภัยคุกคามและช่องโหว่ด้านความปลอดภัยที่พบได้บ่อย พร้อมทั้งให้ภาพรวมของเทคโนโลยีความปลอดภัยที่สำคัญ ผู้เรียนจะได้ศึกษาวิธีการสร้างโครงสร้างพื้นฐานเครือข่ายที่น่าเชื่อถือด้วยโซลูชันโมบิลิตี (Mobility Solutions) และสวิตช์ของ HPE Aruba Networking

วัตถุประสงค์ของหลักสูตร

หลังจากผ่านหลักสูตรนี้ ผู้เรียนจะมีความเข้าใจเกี่ยวกับแนวทางการเพิ่มความปลอดภัยให้แก่อุปกรณ์ (Device Hardening) และหลักสูตรนี้ยังครอบคลุมถึงการดำเนินงานด้านความปลอดภัยที่ปลายสายเครือข่าย (Edge Security) ด้วยระบบ AAA, บทบาทหน้าที่ขั้นพื้นฐานและนโยบายไฟร์วอลล์, การแบ่งส่วนเครือข่ายแบบไดนามิก (Dynamic Segmentation) ตลอดจนการจัดประเภทอุปกรณ์ปลายทาง (Endpoint Classification) ยิ่งไปกว่านั้น หลักสูตรจะอธิบายเพิ่มเติมเกี่ยวกับเทคโนโลยีการตรวจจับภัยคุกคามเบื้องต้น รวมถึงวิธีการรวบรวมบันทึกเหตุการณ์ (Logs) และการแจ้งเตือน (Alarms) เพื่อนำไปใช้เป็นข้อมูลเริ่มต้นในการตรวจสอบและสืบสวนต่อไปโดยเมื่อผ่านการรับรองแล้ว

ผู้เรียนจะสามารถเข้าใจและอธิบายหัวข้อดังต่อไปนี้ :

- Security Threats and Security Strategy
- Security Technologies
- Hardening AOS-CX Switches
- Hardening AOS Devices
- Secure LAN Protocols
- Network Authentication and Encryption Technologies
- Edge Security with HPE Aruba Networking

คุณสมบัติก่อนเข้าอบรม

ขอแนะนำอย่างยิ่งให้ผู้สมัครเข้าอบรมมีความรู้ความเข้าใจพื้นฐานเกี่ยวกับแนวคิดด้านระบบเครือข่ายและความปลอดภัยทางไซเบอร์ ก่อนที่จะเข้ารับการศึกษในหลักสูตรนี้

ผู้ที่เหมาะสมกับหลักสูตร

หลักสูตรนี้เหมาะสำหรับผู้ที่มีประสบการณ์ทำงานด้านเครือข่ายในระดับเริ่มต้นประมาณ 6 เดือน โดยอาจเป็นผู้ที่ทำหน้าที่ดูแลสนับสนุน หรือบำรุงรักษาระบบเครือข่ายแบบมีสาย ไม่ว่าจะทำงานเป็นส่วนหนึ่งของทีม หรือรับผิดชอบงานขนาดเล็กด้วยตนเอง ซึ่งรวมถึงบทบาทงานอย่างผู้ดูแลเครือข่ายเบื้องต้น เจ้าหน้าที่ซัพพอร์ตระดับ Tier 1 หรือ Tier 2 ช่างเทคนิคภาคสนาม รวมถึงผู้ดูแลระบบเครือข่ายโดยทั่วไป

Lab Task and Details

Day 1

Item	Subject	Details	Personal Lab & Devices	Remark
1	Hardening AOS-CX Switches	- Out-of-Band management overview - Out-of-Band management configuration and verifying - Out-of-Band management monitoring and troubleshooting - RBAC (Role Base Access Control) overview - RBAC configuration and verifying - RBAC monitoring and management - Control Plane Policing (CoPP) overview - CoPP configuration and verifying - CoPP monitoring and troubleshooting	Aruba-6300F Aruba-6000	
2	Hardening AOS Devices (Mobility Controllers & APs)	- Administrative Lockdown overview - Administrative Lockdown configuration and verifying - Administrative Lockdown monitoring and troubleshooting - Control Plane Security (CPSec) overview - CPSec configuration and verifying - CPSec monitoring management	Aruba-6300F Aruba-6000 vWLC AP615	

Day 2

Item	Subject	Details	Personal Lab & Devices	Remark
3	Secure LAN Protocols	- DHCP snooping overview - DHCP snooping configuration and verifying - DHCP snooping monitoring and troubleshooting - Dynamic ARP Inspection (DAI) overview - DAI configuration and verifying - DAI monitoring and troubleshooting - Spanning Tree Protections function overview - Root Guard overview and configuration - Root Guard monitoring and troubleshooting - BPDU Guard overview and configuration - BPDU Guard monitoring and troubleshooting	Aruba-6300F Aruba-6000 vWLC AP615	

Day 3

Item	Subject	Details	Personal Lab & Devices	Remark
4	Network Authentication & Edge Security (AAA & 802.1X)	- 802.1X & MAB overview - MAC Authentication Bypass (MAB) overview - MAB configuration and verifying - MAB monitoring and troubleshooting - 802.1X overview - 802.1X configuration and verifying - 802.1X monitoring and troubleshooting - Certificate-Based Authentication overview - Certificate-Based Authentication configuration and verifying - Certificate-Based Authentication monitoring and troubleshooting - ClearPass policies overview	Aruba-6300F Aruba-6000 vWLC AP615 ClearPass	
5	Role-Based Firewall Policies	- User Role overview - User Role configuration and verifying - User Role usage and monitoring - Firewall Rules Application overview - Firewall Rules Application configuration and verifying - Firewall Rules Application usage and monitoring	Aruba-6300F Aruba-6000 vWLC AP615 ClearPass	

Day 4

Item	Subject	Details	Personal Lab & Devices	Remark
6	User-Based Tunneling (UBT)	- User-Based Tunneling (UBT) overview - User-Based Tunneling (UBT) usage case - UBT configuration and verifying - UBT monitoring and troubleshooting	Aruba-6300F Aruba-6000 vWLC AP615	
7	Endpoint Classification & Profiling	- DHCP Fingerprinting overview - DHCP Fingerprinting usage case - DHCP Fingerprinting configuration and verifying - DHCP Fingerprinting result	Aruba-6300F Aruba-6000 vWLC AP615 ClearPass	

Day 5

Item	Subject	Details	Personal Lab & Devices	Remark
8	Threat Detection, Logs & Forensics	- SIEM/Syslog Integration overview - Syslog integration configuration and verifying - Syslog integration monitoring and troubleshooting - ArubaOS WIDS/WIPS Analysis overview - ArubaOS WIDS/WIPS Analysis usage case - ArubaOS WIDS/WIPS Analysis monitoring	Aruba-6300F Aruba-6000 vWLC AP615 ClearPass	