JODOI IT&SERVICE CO., LTD.

CompTIA Security + by Jodoi (WorkShop)

INTRODUCTION

CompTIA Security+ คือใบรับรองทางมาตรฐานวิชาชีพที่เป็นกลางไม่อิงผู้ขายและผู้ผลิตอุปกรณ์รายใด ข้อสอบ CompTIA Security+ เป็นที่ยอมรับในระดับสากลด้านความรู้และทักษะการรักษาความปลอดภัยในระดับซึ่งเป็นรากฐาน และถูกนำไปประยุกต์ใช้อย่างแพร่หลายโดยองค์กรและผู้เชี่ยวชาญด้านการรักษาความปลอดภัยทั่วโลก

ผู้ที่สอบผ่านมาตรฐาน CompTIA Security+ จะมีความรู้และทักษะที่จำเป็นในการระบุความเสี่ยง (Risk Identification) การนำความรู้ไปใช้ในกิจกรรมการลดความเสี่ยง (Risk Mitigation) และสามารถดำเนินการด้านโครงสร้างพื้นฐาน การประยุกต์ใช้ข้อมูล และการรักษาความปลอดภัยในการปฏิบัติงานได้อย่างปลอดภัย นอกจากนี้ ผู้สมัครจะสามารถนำ Security Control มาใช้ในการรักษาความปลอดภัยในสามมุมมองด้าน Information Security ได้แก่ ความลับ (Confidentiality) ความถูกต้อง (Integrity) และความพร้อมใช้ (Availability) การเลือกเทคโนโลยีและผลิตภัณฑ์ที่เหมาะสม การแก้ไขสถานการณ์ฉุกเฉินซึ่งเกี่ยวข้องกับความปลอดภัย และการใช้งานด้วยความตระหนักถึงนโยบาย กฎหมาย และระเบียบข้อบังคับต่างๆ ที่เกี่ยวข้อง

CompTIA Security+ เหมาะสำหรับผู้ที่ต้องการเป็นมืออาชีพทางด้าน IT Security ซึ่งควรมีคุณสมบัติดังนี้

- มีประสบการณ์เป็นผู้ดูแลระบบไอที ซึ่งมุ่งเน้นด้านการรักษาความปลอดภัยของระบบ อย่างน้อย 2 ปี
- มีประสบการณ์ในงานประจำทางด้านเทคนิคที่เกี่ยวข้องกับการรักษาความปลอดภัยของข้อมูล (Information Security)
- มีความรู้ที่กว้างและหลากหลาย เกี่ยวกับการดำเนินงานและข้อควรคำนึงในด้านความปลอดภัย

CompTIA Security+ เหมาะสำหรับผู้ที่ปฏิบัติงานในตำแหน่งทางด้านไอที ซึ่งต้องเกี่ยวข้องกับงานเทคนิคทั้งในระดับปฏิบัติการและระดับนโยบาย เช่น IT Support, System Engineer, Network Engineer, IT Auditor, IT Manager, System Manager, Network Manager, IT Project Manager ตลอดจนผู้ที่ทำงานทางด้านพัฒนาโปรแกรม เช่น Programmer, System Analyst เป็นต้น

CompTIA Security+ ได้รับการรับรองโดย ANSI และสอดคล้องกับมาตรฐาน ISO 17024 ซึ่งจะต้องมีการปรับปรุงวัตถุประสงค์ให้ทันสมัยอยู่เสมอ หัวข้อต่างๆ ในวัตถุประสงค์ของ CompTIA Security+ เป็นผลลัพธ์จากการประชุมเชิงปฏิบัติการของผู้เชี่ยวชาญเฉพาะเรื่อง (Subject Matter Expert) รวมทั้งผลการสำรวจเกี่ยวกับทักษะและความรู้ของ Information Security Professional ที่มีประสบการณ์ไม่ต่ำกว่าสองปี

กำหนดเวลาอบรม

อบรมจำนวน 3 วัน ตั้งแต่ เวลา 9.00 น. – 16.00 น.

เน้นการปฏิบัติ จาก Software Windows , Linux และอุปกรณ์ Cisco

รายละเอียดการสอน

Day 1

Lab 1 - Lab System Monitor

Lab 2 - Lab Logging

Lab 3 - Lab Radius Server

Lab 4 - Lab Port Security

Lab 5 - Lab ACL

Day 2

Lab 6 - Lab SSH Server

Lab 7 - Lab WLAN

Lab 8 - Lab VLAN

Lab 9 - Lab NAT

Lab10 - Lab DHCP Server & DNS Server

Day 3

Lab 11 - Lab VPN

Lab 12 - Lab SNMP

Lab 13 - Lab DDoS

Lab 14 - Lab Backup & Restore

Lab 15 - Lab SLA

LAB 16 - Lab - NMAP

- Exam Tutor

คำอธิบาย Lab – Comtia Security+

1) **Lab System Monitor**

เป็นการตรวจสอบการทำงานของระบบ และการตั้งค่าที่เหมาะสม โดยจะมีการ Setup Lab ด้วย GNS3 (Graphic Network Simulator 3) และ VMWare เพื่อเชื่อมต่อ Network รวมถึงการตรวจสอบการทำงานของ Router, Linux Server และ Windows

Learning Outcome (LO) - ผู้เรียนมีความเข้าใจการทำงาน และการตั้งค่าที่เหมาะสมของระบบ
- ผู้เรียนสามารถตรวจสอบการทำงานของ Router, Linux Server และ Windows

2) **Lab Logging**

เป็นการศึกษาเกี่ยวกับการจัดเก็บ System Log และการกำหนด Logging severity level รวมถึงการ Config และการใช้งาน Kiwi Syslog

Learning Outcome (LO) - ผู้เรียนมีความเข้าใจการทำงาน และสามารถกำหนด Logging severity level
- ผู้เรียนสามารถ Config และใช้งาน Kiwi Syslog ได้

3) **Lab Radius Server**

เป็นการได้ศึกษาเกี่ยวกับหลักการ AAA (Accounting, Authentication, Authorization) และการปรับแต่ง Radius Server (Free Radius) บน Linux Server

Learning Outcome (LO) - ผู้เรียนมีความเข้าใจหลักการ AAA (Accounting, Authentication, Authorization)
- ผู้เรียนสามารถปรับแต่ง Radius Server (Free Radius) บน Linux Server ได้

4) **Lab Port Security**

เป็นการศึกษาเกี่ยวกับหลักการ และการใช้งาน Port Security และ MAC Address Filtering

Learning Outcome (LO) – ผู้เรียนมีความเข้าใจหลักการ และการใช้งาน Port Security และ MAC Address Filtering

5) **Lab ACL**

เป็นการศึกษาเกี่ยวกับหลักการและการตั้งค่า Firewall และ ACL (Access Control List)

Learning Outcome (LO) – ผู้เรียนมีความเข้าใจหลักการ และการตั้งค่า Firewall และ ACL (Access Control List)

6) **Lab SSH Server**

เป็นศึกษาหลักการ Cryptography และการปรับแต่ง SSH Server บน Linux Server เพื่อสร้างความปลอดภัย รวมถึงการใช้งาน Wireshark (network protocol analyzer) และการโจมตีแบบ Man-in-the-Middle Attack

Learning Outcome (LO) - ผู้เรียนมีความเข้าใจหลักการ Cryptography และการปรับแต่ง SSH Server บน Linux Server
- ผู้เรียนสามารถใช้งาน Wireshark (Network Protocol Analyzer)
- ผู้เรียนมีความเข้าใจการโจมตีแบบ Man-in-the-Middle Attack

7) Lab WLAN

เป็นการศึกษาเกี่ยวกับระบบ Wireless LAN (Wi-Fi) และ Wireless Security และการโจมตีแบบ Password Attack (Brute force Attack)

Learning Outcome (LO) – ผู้เรียนมีความเข้าใจหลักการของระบบ Wireless LAN (Wi-Fi) และ Wireless Security
- ผู้เรียนมีความเข้าใจการโจมตีแบบ Password Attack (Brute force Attack)

8) Lab VLAN & Inter-VLAN

เป็นการศึกษาเกี่ยวกับระบบ VLAN และการสร้าง Inter-VLAN รวมถึงการตั้งค่า Firewall หรือ ACLเพื่อเพิ่มระดับความปลอดภัย

Learning Outcome (LO) – ผู้เรียนมีความเข้าใจหลักการของ VLAN และการสร้าง Inter-VLAN
- ผู้เรียนสามารถตั้งค่า Firewall หรือ ACLเพื่อเพิ่มระดับความปลอดภัย

9) Lab NAT

เป็นการศึกษาเกี่ยวกับระบบ NAT (Network Address Translation), PAT (Network Address Translation) และPrivate IP และการจัดทำ NAT บน Windows และเชื่อมต่อไปยัง GNS3

Learning Outcome (LO) – ผู้เรียนมีความเข้าใจหลักการของระบบ NAT (Network Address Translation), PAT (Network Address Translation) และPrivate IP
- ผู้เรียนสามารถทำ NAT บน Windows และเชื่อมต่อไปยัง GNS3 ได้

10) Lab DHCP Server & DNS Server

เป็นการศึกษาเกี่ยวกับระบบ DNS Server และการใช้ command nslookup รวมถึงการปรับแต่ง DHCP Server

Learning Outcome (LO) – ผู้เรียนมีความเข้าใจหลักการของระบบ DNS Server และ command nslookup
- ผู้เรียนสามารถปรับแต่ง DHCP Server ได้

11) Lab VPN

เป็นการเกี่ยวกับระบบ VPN (Virtual Private Network) และ IPSec (Internet Protocol security) รวมถึงการ Config VPN Server และ VPN Client

Learning Outcome (LO) – ผู้เรียนมีความเข้าใจหลักการของระบบ VPN (Virtual Private Network) และ IPSec (Internet Protocol security)
- ผู้เรียนสามารถ Config VPN Server และ VPN Client ได้

12) Lab SNMP

เป็นการศึกษาเกี่ยวกับระบบ SNMP (Simple Network Management Protocol) version 2C และ SNMP version 3 และการใช้งานโปรแกรม SNMP Manager (PRTG : Paessler Router Traffic Grapher) รวมถึงการโจมตีแบบ Man-in-the-Middle Attack

Learning Outcome (LO) – ผู้เรียนมีความเข้าใจหลักการของระบบ SNMP (Simple Network Management Protocol) version 2C และ SNMP version 3
- ผู้เรียนสามารถใช้งานโปรแกรม SNMP Manager (PRTG : Paessler Router Traffic Grapher) ได้

- ผู้เรียนสามารถตรวจสอบการโจมตีแบบ Man-in-the-Middle Attack โดยใช้โปรแกรม PRTG

13) Lab DDoS

เป็นการศึกษาเกี่ยวกับการโจมตีแบบ Distributed Denial-of-Service (DDoS) Attack และตัวอย่างแนวทางการป้องกันการโจมตี

Learning Outcome (LO) – ผู้เรียนมีความเข้าใจหลักการของการโจมตีแบบ Distributed Denial-of-Service (DDoS) Attack และแนวทางการป้องกันการโจมตี

14) Lab Backup & Restore

เป็นการศึกษาเกี่ยวกับการ Backup Config, การ Restore Config และ DR Site

Learning Outcome (LO) – ผู้เรียนมีความเข้าใจหลักการของการ Backup Config, การ Restore Config และ DR Site

15) Lab SLA

เป็นการศึกษาเกี่ยวกับ SLA (Service Level Agreements) และตัวอย่างการกำหนดค่า SLA

Learning Outcome (LO) – ผู้เรียนมีความเข้าใจหลักการของ SLA (Service Level Agreements) และสามารถกำหนดค่า SLA ได้

16) Lab NMAP

เป็นการศึกษาเกี่ยวกับการใช้ NMAP (Network Mapper) ในการสแกน และตรวจสอบ ความปลอดภัยของเครือข่าย และตัวอย่างการเจาะระบบ เพื่อหาช่องโหว่ของเครือข่าย

Learning Outcome (LO) - ผู้เรียนมีความเข้าใจหลักการของ NMAP (Network Mapper)
- ผู้เรียนสามารถสแกน และตรวจสอบความปลอดภัยของเครือข่าย และสามารถเจาะระบบ เพื่อหาช่องโหว่ของเครือข่ายได้

สนใจติดต่อสอบถามได้ที่

บริษัท โจดอย ไอทีแอนด์เซอร์วิส จำกัด

300/98 ซอยลาดพร้าว 20 ถนนลาดพร้าว แขวงจอมพล เขตจตุจักร กทม. 10900

โทร. 02-053-2717

Mobile: 085-221-2007 Website : http://www.jodoi.com