ศูนย์อบรม EZ-ADMIN Training Center
โดยบริษัท จีเนียสย์ ดีเวลลอป จำกัด
98/29 ถนนโพธิ์แก้ว แขวงนวมินทร์ เขตบึงกุ่ม กรุงเทพฯ 10240 | Mail : contact@ez-admin.com, ezgenius54@gmail.com
Tel : 02-5096715 Mobile : 082-5674413, 086-4133928 Fax : 02-5096716

หลักสูตรตรวจสอบช่องโหว่ วิเคราะห์แพ็กเก็ต และแก้ปัญหาของระบบเครือข่ายคอมพิวเตอร์ทั้งแบบมีสายและไร้สายด้วย Wireshark

"หลักสูตรที่จะทำให้ผู้ดูแลระบบเสมือนมีดวงตาพิเศษที่มองเห็นการทำงานของระบบเครือข่ายได้อย่างทั่วถึง เพื่อใช้ในการวิเคราะห์สาเหตุ ตรวจสอบช่องโหว่ แก้ปัญหา และคาดการณ์สิ่งที่จะเกิดขึ้นล่วงหน้าได้อย่างแม่นยำ"

มี 2 Level

- Analyzing and Troubleshooting with Wireshark – Wireshark Level1 (ตรวจสอบระบบ วิเคราะห์แพ็กเก็ต และแก้ปัญหาของระบบเครือข่ายให้ตรงจุดด้วย Wireshark)
- Advanced Protocol Analyzing and Network Security Analysis Using Wireshark – Wireshark Level 2 (เจาะลึกการวิเคราะห์โปรโตคอลสำคัญและตรวจสอบช่องโหว่และการโจมตีต่างๆ จากไวรัสและ Hacker ด้วย Wireshark)

ปัญหาระบบเครือข่ายคอมพิวเตอร์ในปัจจุบันไม่ว่าจะมีขนาดเล็กหรือใหญ่ ก็เริ่มมีความซับซ้อนและแก้ไขได้ยาก จนบางครั้งผู้ดูแลระบบก็ไม่รู้จะแก้ไขได้อย่างไร เพราะนอกจากจะมีอุปกรณ์หลายประเภทที่เชื่อมต่อเข้ามามากขึ้นแล้ว ที่สำคัญก็คือ ข้อมูลที่วิ่งอยู่บนเครือข่าย ไม่สามารถมองเห็นด้วยตาเปล่าได้ ทำให้การแก้ปัญหาส่วนใหญ่เกิดจาก การคาดเดา เราจึงต้องอาศัยโปรแกรมประเภท Sniffer ที่เข้ามาช่วยในการวิเคราะห์และแก้ปัญหาที่เกิดขึ้นได้อย่างตรงจุด ไม่ต้องเดาสุ่มหรือลองผิดลองถูก ซึ่งโปรแกรมที่นิยมใช้งานด้านนี้ ก็คือ Wireshark

Wireshark เป็นโปรแกรม Sniffer ทำหน้าที่ดักจับแพ็กเก็ตที่วิ่งในระบบเครือข่าย เพื่อนำมาตรวจสอบและวิเคราะห์รายละเอียด ในส่วนต่างๆ ของแพ็กเก็ตได้อย่างลึกซึ้ง ทำให้ผู้ดูแลระบบสามารถทราบถึงช่องโหว่ของระบบ การโจมตีจาก Hacker หรือความผิดพลาดและข้อบกพร่องของเครือข่ายที่เกิดขึ้นได้อย่างแม่นยำส่งผลให้การแก้ไขปัญหาทำได้อย่างถูกต้องและรวดเร็ว

นอกจากการแก้ปัญหาแล้ว Wireshark ยังช่วยในเรื่องของการออกแบบและปรับปรุงค่าการทำงานในระบบเครือข่าย ทั้งแบบมีสายและไร้สายได้อย่างมีประสิทธิภาพและมีความปลอดภัยมากขึ้นอีกด้วย

*** ผู้เรียนควรผ่านหลักสูตร Network Basic (NS-01) หรือมีพื้นฐานระบบเครือข่ายคอมพิวเตอร์มาบ้างแล้ว เช่น มีความรู้ความเข้าใจเกี่ยวกับการทำงานของ TCP, กำหนดค่า IP Address ให้กับเครื่องต่างๆ ในเน็ตเวิร์กได้อย่างถูกต้อง หรือสามารถเชื่อมต่อคอมพิวเตอร์เข้ากับระบบเน็ตเวิร์กเบื้องต้นได้

ศูนย์อบรม EZ-ADMIN Training Center
โดยบริษัท จีเนียสย์ ดีเวลลอป จำกัด
98/29 ถนนโพธิ์แก้ว แขวงนวมินทร์ เขตบึงกุ่ม กรุงเทพฯ 10240 | Mail : contact@ez-admin.com, ezgenius54@gmail.com
Tel : 02-5096715 Mobile : 082-5674413, 086-4133928 Fax : 02-5096716

หลักสูตร WSH-L1 (Wireshark Level 1) เรียน 2 วัน

Analyzing and Troubleshooting with Wireshark

(ตรวจสอบระบบ วิเคราะห์แพ็กเก็ต และแก้ปัญหาของระบบเครือข่ายให้ตรงจุดด้วย Wireshark)

หลักสูตรเริ่มต้นสำหรับผู้ดูแลระบบที่ต้องการใช้งาน Wireshark เพื่อตรวจสอบ วิเคราะห์ และแก้ปัญหาต่างๆ ที่เกิดขึ้นในระบบเครือข่ายได้อย่างถูกต้องและมีประสิทธิภาพ เช่น หาสาเหตุความล่าช้าของระบบ การเชื่อมต่อเครือข่าย หรือเซิร์ฟเวอร์ไม่ได้ ระบบเครือข่ายถูกโจมตี หรือต้องการตรวจสอบช่องโหว่ในระบบ เป็นต้น

- โดยหลักสูตรนี้จะเริ่มตั้งแต่พื้นฐานการทำงานของ OSI Model ที่จำเป็นต่อการใช้งานร่วมกับ Wireshark ซึ่งเป็นเรื่องสำคัญที่จะช่วยให้ผู้เรียนเข้าใจข้อความที่ Wireshark รายงานออกมา เช่น ทำความเข้าใจ Protocols และ Addressing ในแต่ละ Layer, TCP 3 Way Handshake หรือ TCP 4 Way Disconnect เป็นต้น
- การติดตั้ง การปรับแต่ง และการกำหนดค่าการทำงานพื้นฐานของ Wireshark ที่จะช่วยให้การทำงานของโปรแกรมมีประสิทธิภาพมากยิ่งขึ้น เช่น กำหนดค่าเริ่มต้นของการ Capture Filter, การกำหนดค่า Interface ที่ใช้งาน, การปรับแต่งการแสดงผล, การ Save, การ Export การดักจับแพ็กเก็ต, การสร้าง Profiles, การปรับแต่งรายงาน และการสั่งพิมพ์
- การดักจับแพ็กเก็ตในระบบเครือข่าย เพื่อนำมาวิเคราะห์และแก้ปัญหาของระบบที่เกิดขึ้น ผู้เรียนจะได้ทำ LAB จากหลายๆ สถานะการณ์ที่แตกต่างกันออกไป เพื่อให้ทราบว่าแต่ละแพ็กเก็ตที่จับมาได้ หมายความว่าอย่างไร และจะแก้ปัญหายังไง ทั้งปัญหาที่เกิดขึ้นจากระบบเครือข่าย แอปพลิเคชั่นที่ใช้ อุปกรณ์ที่ทำงานผิดพลาด ช่องโหว่ของระบบ รวมถึงผู้เรียนสามารถนำไปประยุกต์ใช้กับการทำงานจริงได้อย่างถูกต้อง เช่น การทำ ARP Analysis, ICMP Analysis, DNS Analysis, HTTP Analysis, TCP and UDP Analysis เป็นต้น

จบหลักสูตรแล้วได้อะไร?

- สามารถวิเคราะห์ ตรวจสอบ และแก้ปัญหาของระบบเครือข่ายขนาดเล็กและกลาง ในระดับพื้นฐาน ได้อย่างมีประสิทธภาพ
- สามารถนำไปประกอบอาชีพด้าน ผู้ดูแลระบบเครือข่ายในระดับ Engineer หรือผู้วิเคราะห์และตรวจสอบการทำงานของระบบเครือข่าย เป็นต้น

ศูนย์อบรม EZ-ADMIN Training Center
โดยบริษัท จีเนียสย์ ดีเวลลอป จำกัด
98/29 ถนนโพธิ์แก้ว แขวงนวมินทร์ เขตบึงกุ่ม กรุงเทพฯ 10240 | Mail : contact@ez-admin.com, ezgenius54@gmail.com
Tel : 02-5096715 Mobile : 082-5674413, 086-4133928 Fax : 02-5096716

หลักสูตร WSH-L2 (Wireshark Level 2) เรียน 2 วัน

Advanced Protocol Analyzing and Network Security Analysis Using Wireshark

(เจาะลึกการวิเคราะห์โปรโตคอลสำคัญและตรวจสอบช่องโหว่และการโจมตีต่างๆ จากไวรัสและ Hacker ด้วย Wireshark)

หลักสูตรสำหรับผู้ที่มีพื้นฐานการใช้งาน Wireshark มาบ้างแล้ว โดยหลักสูตรนี้จะเน้นไปที่การวิเคราะห์แพ็กเก็ตและโปรโตคอลสำคัญในระดับที่ลึกมากขึ้น เพื่อนำไปตรวจสอบช่องโหว่ ข้อบกพร่อง หรือแก้ปัญหาระบบเครือข่ายในสถานการณ์จริงที่มีความซับซ้อนได้เป็นอย่างดี

- การตรวจสอบและวิเคราะห์การทำงานของโปรโตคอลสำคัญที่ส่งผลกระทบต่อระบบเครือข่ายในปัจจุบัน เพื่อนำไปปรับปรุงหรือวางแผนแก้ปัญญาได้อย่างเหมาะสม เช่น การตรวจสอบและวิเคราะห์การทำงานของ Ethernet, VLAN, ARP, ICMP, DNS, DHCP, TCP Connection หรือ IP Packet เป็นต้น
- การดักจับและวิเคราะห์แพ็กเก็ตที่ใช้โปรโตคอลที่มีการเข้ารหัส เช่น SSH, HTTPS หรือ TLS Traffic
- การใช้ Wireshark ตรวจสอบและแก้ปัญหาการทำงานของ ACLs (Access Control List) ของแอปพลิเคชั่นต่างๆ ที่เกี่ยวข้อง เช่น DNS, TFTP หรือ TCP เป็นต้น
- ตรวจสอบและวิเคราะห์การโจมตีแบบ Denial of Service, การปลอมแปลงหรือหลอกล่อในระบบ LAN ด้วย ARP Poisoning, การติดเชื้อ Malware, การถูก Brute Force Attacks หรือการบุกรุกเข้ามาในระบบของ Hacker เป็นต้น โดยจะมีการใช้งาน Wireshark ร่วมกับ Tools อื่นๆ เพื่อใช้ในการวิเคราะห์ระบบและทำ LAB จำลองการโจมตีต่างๆ เช่น Kali Linux, Metasploit, Burp Suite, Snort หรือ Security Onion เป็นต้น

จบหลักสูตรแล้วได้อะไร?

- สามารถวิเคราะห์ ตรวจสอบ และแก้ปัญหาของระบบเครือข่ายขนาดกลางและใหญ่ในขั้นสูง หรือที่มีความซับซ้อนมากๆ ได้อย่างถูกต้องและมีประสิทธภาพ
- สามารถนำไปประกอบอาชีพด้าน ผู้ดูแลระบบเครือข่ายในระดับ Engineer, Manager นักออกแบบ ระบบเครือข่าย หรือผู้วิเคราะห์และตรวจสอบการทำงานของระบบเครือข่าย เป็นต้น
- สามารถวิเคราะห์ ตรวจสอบ ช่องโหว่และการโจมตีต่างๆ จากไฟล์ Malware หรือ Hacker ได้อย่างรวดเร็วและแม่นยำ
- สามารถพยากรณ์เหตุการณ์หรือผลลัพธ์ที่จะเกิดขึ้นจากการถูกโจมตีจากไวรัส ประเภทต่างๆ หรือ Hacker ได้อย่างถูกต้อง เพื่อเตรียมนำไปหาทางแก้ปัญหาหรือป้องกันได้อย่างมีประสิทธิภาพ
- สามารถนำไปประกอบอาชีพด้าน ผู้ดูแลระบบด้านความปลอดภัยของระบบเครือข่าย, นักทดสอบการป้องกันการโจมตีจาก Hacker (Penetration Testing), ผู้ประเมินความเสี่ยงจากช่องโหว่ของระบบ (Vulnerability Assessment), หรือผู้วิเคราะห์และตรวจสอบการทำงานของระบบเครือข่าย เป็นต้น