บริษัท จีเนียสย์ ดีเวลลอป จำกัด
เลขที่ 47/401 ห้อง N007031 อาคารนาริตะ ชั้น 7 ถ.ป๊อปปูล่า ต.บ้านใหม่ อ.ปากเกร็ด จ.นนทบุรี 11120
โทร. 082-5674413, 086-4133928 อีเมล contact@ez-admin.com, ezgenius54@gmail.com

หลักสูตร Wireshark - Level 1 : Analyzing and Troubleshooting with wireshark

(ตรวจสอบระบบ วิเคราะห์แพ็กเก็ต และแก้ปัญหาของระบบเครือข่ายให้ตรงจุดด้วย Wireshark)

หลักสูตรเริ่มต้นสำหรับผู้ดูแลระบบที่ต้องการใช้งาน Wireshark เพื่อตรวจสอบ วิเคราะห์ และแก้ปัญหาต่างๆ ที่เกิดขึ้นในระบบเครือข่ายได้อย่างถูกต้องและมีประสิทธิภาพ เช่น หาสาเหตุความล่าช้าของระบบ การเชื่อมต่อเครือข่ายหรือเซิร์ฟเวอร์ไม่ได้ 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

หัวข้ออบรม

1. รู้จัก Wireshark และรูปแบบการเชื่อมต่อเพื่อดักจับข้อมูลในระบบเครือข่าย
    - รู้จัก Wireshark
    - Wireshark ช่วยตรวจสอบอะไรได้บ้าง
    - รูปแบบการเชื่อมต่อ Wireshark ในระบบเครือข่าย
2. กำหนดค่าการทำงานของ Port Mirroring ใน Switch ยี่ห้อต่างๆ
    - การเปิดโหมด Span ใน Switch ของ Cisco
    - การกำหนด Port Mirroring ใน Unifi Switch
    - การกำหนด Port Mirroring ใน Ubiquiti EdgeRouter
    - การกำหนด Port Mirroring ใน MikroTik
    - ข้อควรระวังในการกำหนด Port Mirroring
3. การติดตั้งและใช้งานโปรแกรม Wireshark เบื้องต้น
    - การติดตั้งโปรแกรม Wireshark
    - เริ่มต้นใช้งานและรู้จักส่วนประกอบสำคัญของ Wireshark

บริษัท จีเนียสย์ ดีเวลลอป จำกัด
เลขที่ 47/401 ห้อง N007031 อาคารนาริตะ ชั้น 7 ถ.ป๊อปปูล่า ต.บ้านใหม่ อ.ปากเกร็ด จ.นนทบุรี 11120
โทร. 082-5674413, 086-4133928 อีเมล contact@ez-admin.com, ezgenius54@gmail.com

- หัวข้อต่างๆ ใน Packet List Pane
- รู้จักกับสัญลักษณ์ต่างๆ ของ Related Packets Indicator
- การกำหนดค่า Capture Options
- การ Export File สำหรับตรวจสอบข้อมูลภายหลัง
- การสร้าง Profile เพื่อกำหนดสภาพแวดล้อมการทำงานของโปรแกรมตามที่กำหนด

4. ทบทวนเรื่องของ TCP/IP Model 5 Layer และพื้นฐานการทำงานของ TCP
    - TCP/IP Model 5 Layer
    - การทำงานของ TCP
    - 3-Way Handshake
    - สถานะของ TCP Flags
    - Window Size และการ Sliding Window
    - การทำงานของ UDP
5. พื้นฐานการวิเคราะห์แพ็กเก็ตของ Wireshark
    - การสร้างภาพระบบเครือข่ายจากการวิเคราะห์แพ็กเก็ต
    - การใช้ Wireshark ดักจับรหัสพาสเวิร์ดและตรวจสอบข้อมูลต่างๆ ในแพ็กเก็ต
6. ตรวจสอบความผิดปกติของการติดต่อสื่อสารกันในระบบเครือข่าย
    - ตรวจสอบคุณสมบัติและรายละเอียดของ Trace File
    - ตรวจสอบสถิติของการติดต่อสื่อสารกันระหว่างเครื่องต้นทางและเครื่องปลายทาง
    - แท็บ Ethernet
    - แท็บ IPv4
    - แท็บ IPv6
    - แท็บ TCP
    - แท็บ UDP
7. การคัดกรองข้อมูลที่ต้องการดักจับ หรือให้แสดงผลด้วย Capture Filter และ Display Filter
    - การคัดกรองข้อมูลที่ต้องการดักจับด้วย Capture Filter
    - Capture Filter ที่ใช้งานบ่อย
    - การคัดกรองข้อมูลที่ต้องการดักจับด้วย Display Filter
    - Display Filter ที่ใช้งานบ่อย
8. วิเคราะห์และตรวจสอบปัญหาการทำงานของระบบเครือข่าย
    - วิเคราะห์การทำงานของ TCP และโปรโตคอลสำคัญที่เกี่ยวข้องในการติดต่อกับเครื่อง Server
    - วิเคราะห์ปัญหา Server และโปรโตคอล HTTP ตอบกลับล่าช้า
    - วิเคราะห์ปัญหาการเกิด TCP Transmission จำนวนมาก
    - วิเคราะห์ปัญหา DNS Server ตอบสนองต่อการร้องขอข้อมูลล่าช้า
    - วิเคราะห์ปัญหาการเกิด Broadcast Storm หรือ ARP Storm