บริษัท จีเนียสย์ ดีเวลลอป จำกัด (สำนักงานใหญ่)
เลขที่ 20/65 หมู่ 10 ต.ระแหง อ.ลาดหลุมแก้ว จ.ปทุมธานี 12140 โทร.02-0777514, 095-8635165
อีเมล contact@ez-admin.com Line: @ezgenius www.ez-admin.com www.ez-genius.com

หลักสูตรอบรม Analyzing and Troubleshooting with Wireshark (Wireshark Level1)

1. รู้จัก Wireshark และรูปแบบการเชื่อมต่อเพื่อดักจับข้อมูลในระบบเครือข่าย
    - รู้จัก Wireshark
    - Wireshark ช่วยตรวจสอบอะไรได้บ้าง
    - รูปแบบการเชื่อมต่อ Wireshark ในระบบเครือข่าย
    - ประโยชน์ของการทำ Network Visibility
    - ประเภทของโปรแกรม Network Monitor
    - ความสามารถของ Wireshark
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
    - การกำหนด Port Mirroring ใน HP
    - ข้อควรระวังในการทำงานของ Port Mirroring
3. การติดตั้งและใช้งานโปรแกรม Wireshark เบื้องต้น
    - การติดตั้งโปรแกรม Wireshark
    - เริ่มต้นใช้งานและรู้จักส่วนประกอบสำคัญของ Wireshark
    - หัวข้อต่างๆ ใน Packet List Pane
    - รู้จักกับสัญลักษณ์ต่างๆ ของ Related Packets Indicator
    - การกำหนดค่า Capture Options
    - การ Export File สำหรับตรวจสอบข้อมูลภายหลัง
    - การสร้าง Profile เพื่อกำหนดสภาพแวดล้อมการทำงานของโปรแกรมตามที่ต้องการ
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
    - การวิเคราะห์แพ็กเก็ตแบบแยกส่วนต่างๆ (Dissect a Packet)
    - การวิเคราะห์แพ็กเก็ตการทำงานเบื้องต้นของ TCP
    - การวิเคราะห์แพ็กเก็ตของ Services ต่างๆ ที่สำคัญของระบบเครือข่าย เช่น ARP, DNS, HTTP, FTP, DHCP และ RDP
6. ตรวจสอบความผิดปกติของการติดต่อสื่อสารกันในระบบเครือข่าย
    - ตรวจสอบคุณสมบัติและรายละเอียดของ Trace File
    - การใช้ Converstation ตรวจสอบสถิติของการติดต่อสื่อสารกันระหว่างเครื่องต้นทางและเครื่องปลายทาง
    - แท็บ Ethernet
    - แท็บ IPv4
    - แท็บ IPv6
    - แท็บ TCP
    - แท็บ UDP
    - การอ่านค่า Relative Start และ Duration เพื่อหาความผิดปกติ
    - การใช้ Expert Info ตรวจสอบความผิดปกติของระบบเครือข่าย
    - สัญญาณเตือนถึงความผิดปกติที่ควรตรวจสอบ
7. การคัดกรองข้อมูลที่ต้องการดักจับหรือให้แสดงผลด้วย Capture Filter และ Display Filter
    - การคัดกรองข้อมูลที่ต้องการดักจับด้วย Capture Filter
    - Capture Filter ที่ใช้งานบ่อย
    - การคัดกรองข้อมูลที่ต้องการแสดงผลด้วย Display Filter
    - Display Filter ที่ใช้งานบ่อย

- การทำ Display Filter ในส่วนต่างๆ ของ Wireshark
- การสร้างปุ่ม Display Filter ที่ใช้งานบ่อยเพื่อสะดวกในการใช้งาน
- การประกอบแพ็กเก็ตที่แยกส่วนจากแอปพลิเคชั่นต่างๆ กลับมาเป็นแพ็กเก็ตที่สมบูรณ์อีกครั้ง

8. วิเคราะห์และตรวจสอบปัญหาการทำงานของระบบเครือข่าย
    - วิเคราะห์ปัญหา Server และโปรโตคอล HTTP ตอบกลับล่าช้า
    - วิเคราะห์ปัญหาการเกิด TCP Retransmission และกฎของการจัดลำดับสี (Coloring Rules)
    - วิเคราะห์ปัญหา DNS Server ตอบสนองต่อการร้องขอข้อมูลล่าช้า (DNS Response Time)
    - วิเคราะห์ปัญหาการเกิด Broadcast Storm หรือ ARP Storm
    - วิเคราะห์ปัญหาจากการสูญเสียแพ็กเก็ต (Packet Loss)
    - วิเคราะห์ปัญหาที่เกิดจากความแออัดของระบบเครือข่าย (Network Congestion)
    - วิเคราะห์ปัญหาที่เกิดจากความล่าช้าของแอปพลิเคชั่นที่ใช้งาน (Application Response Time)
    - วิเคราะห์ปัญหาที่เกิดจากเครื่อง Server ไม่พร้อมให้บริการ (Busy Servers)
    - วิเคราะห์การทำงานของ TCP และโปรโตคอลสำคัญที่เกี่ยวข้องในการติดต่อกับเครื่อง Server (TCP Protocol Issues)
9. การสร้างกราฟจากแพ็กเก็ตทั้งหมดเพื่อให้ง่ายต่อการตรวจสอบข้อมูลและวิเคราะห์ปัญหาต่างๆ
    - การสร้าง I/O Graph เพื่อเปรียบเทียบความเร็วในการตอบสนองข้อมูลของแอปพลิเคชั่นต่างๆ
    - การสร้าง TCP Stream Graphs แสดงภาพการเคลื่อนที่ของแพ็กเก็ตเพื่อความผิดปกติที่เกิดขึ้นของระบบเครือข่าย
    - การสร้าง Throughput Graphs แสดงภาพความเร็วการโอนถ่ายข้อมูลเพื่อตรวจสอบปัญหาความล่าช้าในระบบเครือข่าย