Group IT04 USB Scan & Extractor

SC362006 Information and Communication Technology Security

อาจารย์ประจำวิชา: ศ.ดร.จักรชัย โสอินทร์, อ.ชาติชาย ปุณริบูรณ์

หลักการและเหตุผล

ในปัจจุบัน ระบบความปลอดภัยส่วนใหญ่เน้นการป้องกันที่ซอฟต์แวร์ แต่จุดอ่อนที่ใหญ่ที่สุดยังคงเป็น "มนุษย์" การโจมตีผ่านพอร์ต USB ยังคงเป็นวิธีที่ได้ผลสูงเนื่องจากความไว้วางใจของผู้ใช้โดยทั่วไปผู้ใช้จะระมัดระวังเมื่อพบไฟล์แปลกปลอม แต่จะให้ความไว้วางใจสูงต่อโปรแกรมจำพวก"SecurityScanner"โปรเจกต์นี้จึงเลือกใช้หน้ากากของโปรแกรมตรวจเช็คไวรัส USB Checkerเป็นเหยื่อล่อ เพื่อเข้าถึงสิทธิ์ระดับสูงในระบบ และทำการสืบหาข้อมูล รวมถึงดึงข้อมูลเครือข่ายเชิงลึกออกมาโดยที่ผู้ใช้ไม่ทันสังเกต

งานของเรา (Scope)

Hardware: ใช้ Raspberry Pi เป็นศูนย์ควบคุมและรับข้อมูล
OS: Raspberry Pi OS Lite (Linux 64-bit)
Detection: สามารถดักจับอุปกรณ์ประเภท HID (BadUSB) และแจ้งเตือนได้
Scanning: สแกนไวรัสด้วยฐานข้อมูล ClamAV (Open Source)
Data Extraction: ดึงข้อมูลชื่อผู้ใช้ ชื่อเครื่อง MAC Address และสถานะการเชื่อมต่อเครือข่ายทั้ง IPv4 และ IPv6

วัตถุประสงค์

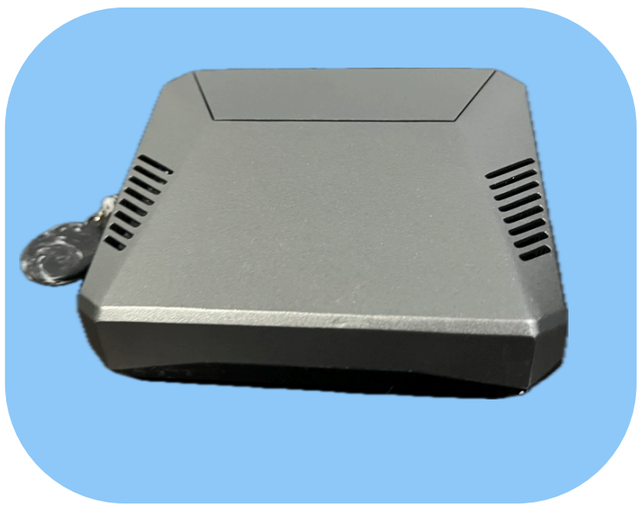
1.เพื่อพัฒนาชุดคำสั่งที่สามารถหลบเลี่ยงการตรวจจับของ Antivirus มาตรฐาน
2.เพื่อศึกษาและจำลองเทคนิคการดึงข้อมูลเครือข่าย ออกไปยังเครื่องควบคุมภายนอก
3.เพื่อสร้างระบบระบุตัวตนเป้าหมายผ่านลายนิ้วมือดิจิทัล และพฤติกรรมการเชื่อมต่อ

ทำงานอย่างไร

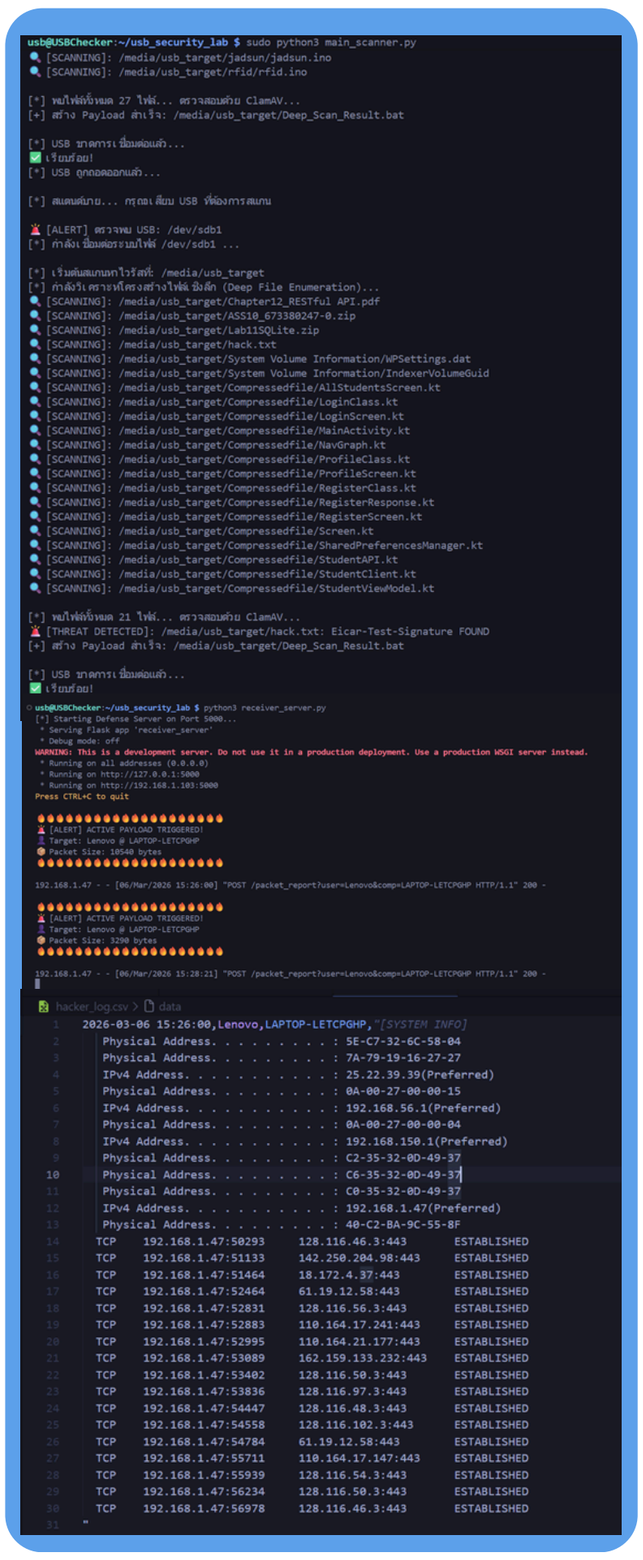
1. รอเชื่อมต่อ USB ผ่าน Linux Kernel
2. ทำการเชื่อมต่ออุปกรณ์เข้ากับระบบ
3. Engine ตรวจสอบไฟล์ทั้งหมด เช็คว่ามีไฟล์อันตรายไหม
4. เมื่อสแกนเสร็จสิ้น ทำการสร้างไฟล์อาบยาพิษลง USB
5. Payload ทำการสิทธิ์ Admin และแอบสร้าง Snapshot ข้อมูลเครือข่ายในโฟลเดอร์ลับ (Temp)
6. PowerShell ส่งข้อมูลทั้งหมดกลับไปยัง Raspberry Pi ผ่าน HTTP POST

แตกต่างจากคนอื่นอย่างไร

มีการเพิ่มไฟล์ USB_Security_Report.pdf.bat ที่เป็น Vulnerability Assessment เพื่อดูว่าเครื่องเป้าหมายมีช่องโหว่ในการดักจับข้อมูล หรือไม่



ตัวอย่างการทำงาน



สมาชิกในกลุ่ม

นายศาศวัต เข็มพิลา 673380244-6
นายภูมิรพี สุธีดวงสมร 673380235-7
นายสินชัย สินธุ์มาลัย 673380247-0
นายธีร์ธวัช สมัครสมาน 673380222-6
นายนนรวี ทองภู 673380223-4
นายยงศิลป์ ทาระบุตร 673380237-3

อ้างอิง

https://www.linkedin.com/posts/vanr_usbsecurity-malwareprevention-raspberrypi-activity-7370160065485426688-do4i
https://youtu.be/x1xvLkYC_fo?si=5tPmhbz9p0k-C6v4