ระบบ phishing ผ่านหน้าเว็บปลอม สำหรับการเก็บข้อมูลผู้ใช้งาน

Group7 Sec.1

อุปกรณ์ที่พัฒนา

ESP32

หลักการและเหตุผล

ในยุคปัจจุบัน การหลอกลวงทางไซเบอร์ที่ผู้โจมตีปลอมตัวเป็นองค์กรหรือบุคคลที่น่าเชื่อถือ เพื่อหลอกให้ผู้ใช้เปิดเผยข้อมูลส่วนตัว โดยเฉพาะในมหาวิทยาลัยหรือองค์กรขนาดเล็ก การใช้ ESP32 ร่วมกับ XAMPP เป็นทางเลือกที่สะดวกและประหยัดในการสร้างระบบ Captive Portal เพื่อควบคุมการเข้าใช้งานและเก็บข้อมูลผู้ใช้งาน

วัตถุประสงค์

- เพื่อดักจับและโจรกรรมข้อมูลผ่านเว็บไซต์ปลอม
- สร้าง wifi ปลอมขึ้นมาเพื่อทำให้ผู้ใช้สับสนเพื่อดักจับข้อมูล
- เพื่อบันทึกข้อมูลผู้ใช้งาน (Username, Password, เวลา login) ลงใน XAMPP Web Server

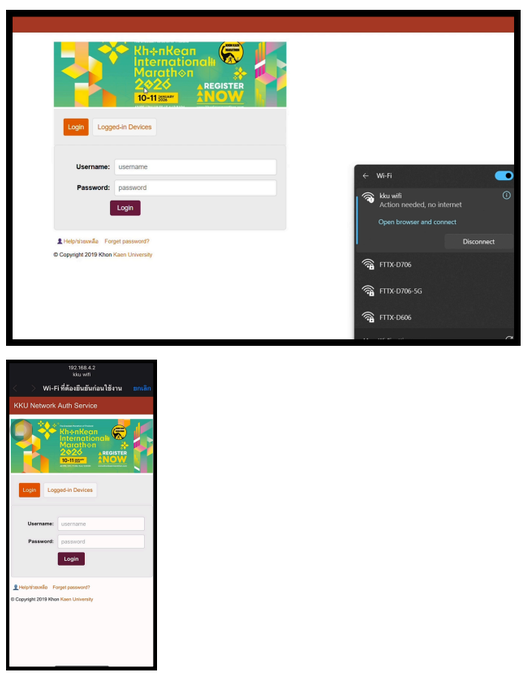
ขอบเขตการศึกษา

- รองรับการเชื่อมต่อ WiFi ภายในวง LAN เล็กหรือสภาพแวดล้อมทดลอง
- การบันทึกข้อมูลจำกัดอยู่ที่ ไฟล์ JSON (log.json) บน PC
- ไม่ได้มีระบบยืนยันตัวตนจริง หรือเข้ารหัสข้อมูลผู้ใช้งานขั้นสูง

วิธีการดำเนินงาน

ให้ESP32 ใช้ฟังก์ชัน WiFi.softAP เพื่อสร้าง Access Point และตั้งค่า IP แบบ Static (192.168.4.1) ด้วย WiFi.softAPConfig() ESP32 ทำงานเป็น ตัวกลาง ระหว่าง Client และ PC และทำการ Captive Portal โดยให้ DNS Server บน ESP32 ดักทุก URL และชี้ไปที่ IP ของ ESP32 ใช้ Web Server ตรวจสอบ request ที่ไม่พบและ redirect ไปยัง IP ของXAMPP ที่รันบน PC ทำให้ผู้ใช้งานเข้าสู่หน้า login โดยอัตโนมัติ การจัดการข้อมูล PHP Script จะรับค่า POST จากฟอร์ม login ตรวจสอบ และบันทึกข้อมูลพร้อมเวลา login ลงในไฟล์ log.json

ตัวอย่างการดำเนินงาน



อ้างอิง

https://mnot.github.io/I-D/capport-problem/

สรุปผล

ระบบจะสร้างระบบ Captive Portal ด้วย ESP32 โดยใช้หลักการของ Access Point, DNS Redirect และ HTTP 302 เพื่อบังคับให้ผู้ใช้ที่เชื่อมต่อ Wi-Fi ถูกนำไปยังหน้าเว็บเฉพาะที่กำหนดไว้เพื่อหลอกลวงข้อมูล

ผู้จัดทำ

นาย ภูมิภัทร รีพิมพ์	673380019-3
นาย กันตพัฒน์ จินาพร	673380203-0
นาย นเรนทร์ฤทธิ์ โทสาล	673380225-0
นายจิรภัทร พบวงษา	673380208-0