Wi-Fi Phishing using ESP32

Borcelle

หลักการและเหตุผล

ปัจจุบันเครือข่ายWi-Fiสาธารณะถูกใช้งานอย่างแพร่หลาย เช่น ใน มหาวิทยาลัย ร้านกาแฟ และสนามบิน ทำให้ผู้ใช้จำนวนมากเชื่อมต่อเครือข่าย โดยไม่ได้ตรวจสอบความปลอดภัย

หนึ่งในเทคนิคการโจมตีที่พบได้คือ Wi-Fi Phishing หรือ Evil Twin Attack ซึ่งเป็นการสร้าง Access Point ปลอม ที่มีชื่อเหมือนเครือข่ายจริง เพื่อหลอกให้ผู้ใช้เชื่อมต่อและกรอกข้อมูลผ่านหน้า Login ปลอม

วัตถุประสงค์เพื่อ

ศึกษาการโจมตีแบบ Wi-Fi Phishing

ศึกษาการทำงานของ Access Point

สร้างระบบจำลองเพื่อใช้ในการเรียนรู้ด้าน Cybersecurity

งานที่เกี่ยวข้อง

ESP32 Evil Twin Attack Project

งานนี้เป็นการพัฒนาเครื่องมือทดสอบความปลอดภัยเครือข่ายโดยใช้ ESP32 เพื่อสร้าง Fake AccessPoint ที่มีชื่อเหมือนกับเครือข่ายจริง เมื่อผู้ใช้เชื่อมต่อ ระบบจะเปลี่ยนเส้นทางไปยัง Captive Portal ปลอม เพื่อศึกษาพฤติกรรมของผู้ใช้ในการกรอกข้อมูล

แนวคิดของงาน

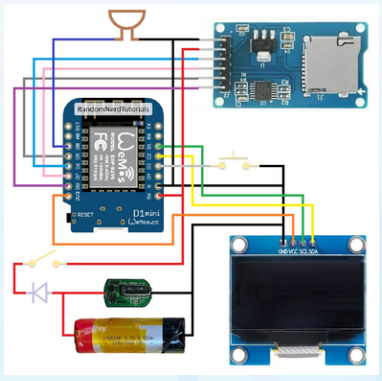
- ใช้ ESP32 สร้าง Access Point ปลอม
- ใช้ Web Server บน ESP32 ทำหน้า Login
- เก็บข้อมูลที่ผู้ใช้กรอกเพื่อวิเคราะห์ความเสี่ยง

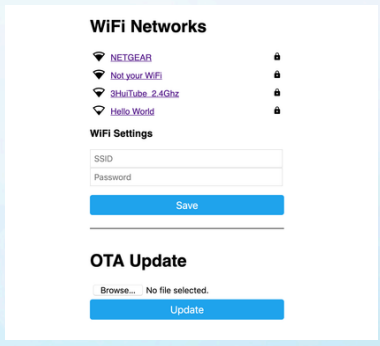
งานที่เกี่ยวข้อง

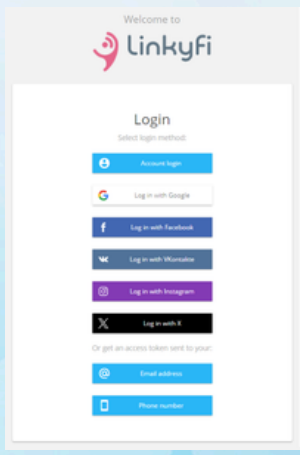
Wi-FiCaptivePortal Phishing for Security Awareness งานวิจัยหลายงานด้าน Cybersecurity Education ใช้เทคนิค Captive Portal Phishing เพื่อจำลองสถานการณ์การโจมตีในเครือข่าย Wi-Fi สาธารณะ

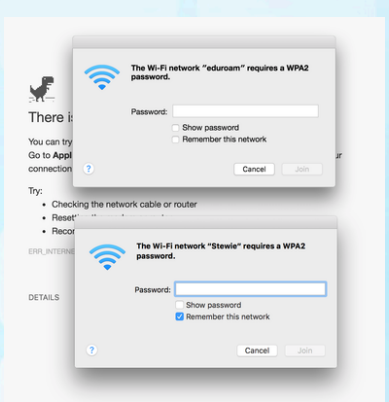
แนวคิดของงาน

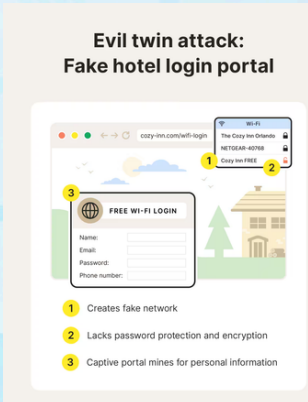
- สร้างหน้า Login ปลอมเหมือน Wi-Fi ของมหาวิทยาลัยหรือร้านกาแฟ
- เมื่อผู้ใช้เชื่อมต่อจะถูก redirect ไปยังหน้า login
- ศึกษาพฤติกรรมการกรอกข้อมูลของผู้ใช้

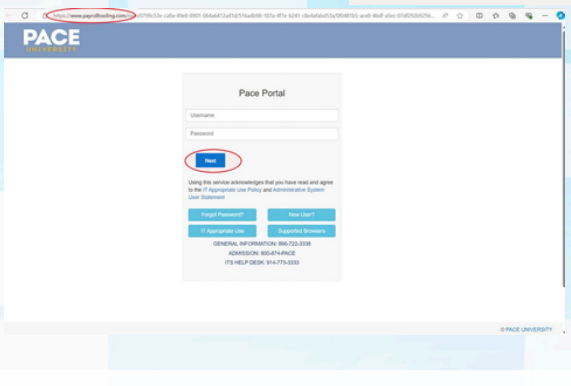












ตัวอย่างโค้ด

```
/*
  Deva DIY
  www.devadiy.com
  ตัวอย่างการสร้างเว็บ WiFi Manager
*/

#include <WiFi.h>
#include <AsyncTCP.h>
#include <ESPAsyncWebServer.h>
#include <EEPROM.h>
#include "wifimanager.h"
#include "style_wifimanager.h"

// สร้าง AsyncWebServer object พอร์ต 80
AsyncWebServer server(80);

//ตัวแปรบันทึกค่า ssid รหัสผ่านจากแบบฟอร์ม WiFi manager
const char* ssid = "";
const char* password = "";

// ตัวแปรบันทึกค่า ssid รหัสผ่าน ลงใน เมมโมรี่
struct EepromObj_wifimanager {
  char parm_ssid[64] = "";
  char parm_pass[24] = "";
};
EepromObj_wifimanager saveparm;

// ตั้งค่าพิน GPIO led onboard
const int led = 2;

// ตรวจสอบแต่ละตัวอักษร
bool isAlphaNumericString(const String &str) {
  for (size_t i = 0; i < str.length(); i++) {
    if (!isAlphaNumeric(str.charAt(i))) {
      return false;
    }
  }
  return true;
}

// อ่านข้อมูลจากเมมโมรี
void readParm() {
  EEPROM.get(2, saveparm);
  ssid = saveparm.parm_ssid;
  password = saveparm.parm_pass;
  delay(500);

  Serial.print("SSID : ");
  Serial.println(ssid);
  Serial.print("PASSWORD : ");
  Serial.println(password);
}

// เขียนข้อมูลลงในเมมโมรี
void writeParm() {
  EEPROM.put(2, saveparm);
  EEPROM.commit();
  delay(500);
  Serial.println("Saved Parm to Memory");
}

// เริ่มต้นใช้งานการเชื่อมต่อ WiFi
bool WiFi_init() {
  unsigned long pastTime = 0;
  unsigned long nowTime = 0;
  unsigned long timeOut = 10000;

  // ตรวจสอบ ssid มีข้อมูลบันทึกอยู่หรือไม่
  if (String(ssid) == "") {
    Serial.println("Unable connect to Wi-Fi");
    return false;
  }

  // ตั้งค่า esp32 WiFi Mode : Station
  WiFi.mode(WIFI_STA);
  // เชื่อมต่อเครือข่าย WiFi ด้วย ssid, password
  WiFi.begin(ssid, password);

  // ตรวจสอบการเชื่อมต่อ WiFi ถ้าใช้เวลาเชื่อมต่อเกิน timeOut ให้หยุดการเชื่อมต่อ
  pastTime = millis();
```

งานของเราทำอะไร

การทำงาน

อุปกรณ์ที่ใช้ในโครงงาน

- บอร์ด ESP32
- สาย USB สำหรับเชื่อมต่อคอมพิวเตอร์
- คอมพิวเตอร์ที่ติดตั้ง Arduino IDE

ESP32 จะทำหน้าที่เป็นทั้ง Access Point (AP) ตั้งค่า ESP32 ให้เป็น Access Point และให้ESP32 เป็น web server ขั้นตอนแรกคือให้ ESP32 ปล่อยสัญญาณ Wi-Fi เอง หลังจากสร้างWiFiแล้วESP32จะเปิดWeb Server Web Server นี้มีหน้าที่

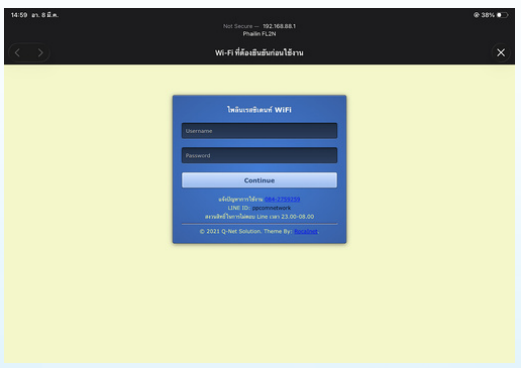
- แสดงหน้าเว็บ
- รับข้อมูลจากผู้ใช้
- เมื่อผู้ใช้กรอกข้อมูล เช่น
- Password

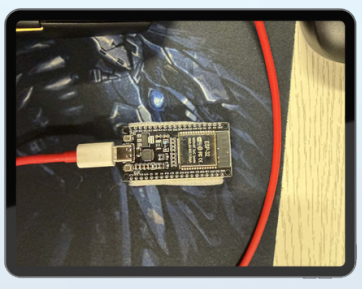
แล้วกด Submit ข้อมูลจะถูกส่งไปยังESP32 Web Server จากนั้น ESP32 จะสามารถ

- แสดงข้อมูลใน Serial Monitor หรือบันทึกข้อมูลไว้

ความแตกต่างจากงานอื่น

ใช้ ESP32 เป็นอุปกรณ์หลักเป็นระบบ ต้นทุนต่ำ (Low-Cost Device) เน้นการศึกษา การทำงานของ Access Point และ Captive Portal ใช้เป็น เครื่องมือทดลองในวิชา Wireless





แหล่งอ้างอิง:

ใช้ ESP32 เป็นอุปกรณ์หลักเป็นระบบ ต้นทุนต่ำ (Low-Cost Device)เน้นการศึกษา การทำงานของ Access Point และ Captive Portalใช้เป็น เครื่องมือทดลองในวิชา Wireless