



Fake Captive Portal

SC362006 : INFORMATION AND COMMUNICATION TECHNOLOGY SECURITY

หลักการและเหตุผล

เนื่องในปัจจุบันการ Fake Captive Portal เป็นเรื่องที่พบเห็นได้บ่อย ในหลากหลายรูปแบบ คณะผู้จัดทำจึงต้องการศึกษาและหาความรู้เกี่ยวกับการ Fake Captive Portal เพื่อรู้แนวทางป้องกันการ Fake Captive Portal และนำไปต่อยอดในอนาคต

วัตถุประสงค์

- เพื่อศึกษาวิธีการและหลักการทำงานของ Clone Phishing
- เพื่อนำความรู้และหลักการที่ได้เรียนรู้มาต่อยอดและประยุกต์ใช้กับการทำงานต่อไป
- เพื่อที่จะสามารถตรวจสอบข้อมูลของผู้ที่ login ได้ เช่น Username Password ของผู้ใช้เพื่อการศึกษา

คณะผู้จัดทำ กลุ่มที่ 11

- | | |
|----------------------|-------------|
| 1.เจษฎาภรณ์ ศิริเกตุ | 643020359-3 |
| 2.เพชร ศรีสุพัฒน์ | 643020394-1 |
| 3.พีรสา ลุนหงส์ | 643020400-2 |
| 4.ปิยะรัตน์ อุดชิวะ | 643021111-4 |
| 5.ภัทรศยา ศรีสง่า | 643021115-6 |
| 6. มณิกา เตโซ | 643021117-2 |

อาจารย์ที่ปรึกษา

รศ.ดร. จักรชัย ไสอินทร์

วิธีการใช้งาน

1. อัพโหลดโค้ดขึ้นบอร์ด ESP8266
2. ใช้ Labtop เพื่อเชื่อมต่อ WIFI ของ ESP8266
3. เปิดโปรแกรม Xampp เพื่อเปิด WebServer
4. ใช้อุปกรณ์ที่เชื่อมต่อ WIFI ได้ มาเชื่อมต่อกับ WIFI ของ ESP 8266
5. เมื่อเชื่อมต่อเสร็จ หน้าเว็บจะเด็งมาให้ login แล้วเราก็กรอก username และ password
6. เมื่อกรอกแล้ว username และ password ก็จะเก็บไว้ที่ไฟล์ database.txt ที่โฟลเดอร์htdocs

สรุปผล

สร้างระบบเครือข่าย Wi-Fi ปลอมที่ดูเหมือนเครือข่าย Wi-Fi ของ KRU ของจริงขึ้นมา โดยจะใช้ ESP8266 เพื่อเปลี่ยนเส้นทางไปยังเว็บไซต์ปลอม เพื่อดักจับข้อมูลไว้แต่ไม่สามารถใช้อินเทอร์เน็ตได้

อ้างอิง

[HTTPS://LOGIN.KKU.AC.TH/](https://login.kku.ac.th/)

[HTTPS://GITHUB.COM/ADAMFF1/ESP8266-CAPTIVE-PORTAL.GIT](https://github.com/adamff1/esp8266-captive-portal.git)

โปรแกรมที่ใช้



Visual Studio Code