WEB PHISHING

กลุ่ม: 21

วิชา ความมั่นคงเทคโนโลยีสารสนเทศและการสื่อสาร

ปีการศึกษา: 2/2568

อาจารย์ที่ปรึกษา: ศ.ดร.จักรชัย โสอินทร์ และ ผศ.ดร.สาธิต กระเวนกิจ

01 หลักการและเหตุผล

Web Phishing คือการหลอกลวงทางออนไลน์เพื่อขโมยข้อมูลสำคัญ เช่น รหัสผ่าน หมายเลขบัตรเครดิต หรือข้อมูลยืนยันตัวตน โดยผู้โจมตีสร้างเว็บไซต์ปลอมที่เลียนแบบแพลตฟอร์มจริงเพื่อหลอกให้เป้าหมายป้อนข้อมูล
หลักการของ Web Phishing

- สร้างเว็บไซต์ปลอม
- การล่อลวงเป้าหมาย
- การเก็บข้อมูล
- ผลประโยชน์ทางการเงิน
- การโจรกรรมข้อมูล
- การสร้างความเสียหาย

02 วัตถุประสงค์

ด้านการศึกษา

- เพื่อการศึกษาเทคนิคการโจมตี

ด้านการพัฒนา

- เพื่อการพัฒนาแนวทางการโจมตีที่หลากหลาย

ติดตั้งและปรับแต่ง

- เพื่อจำลองการโจมตีด้วยวิธีการPhishing

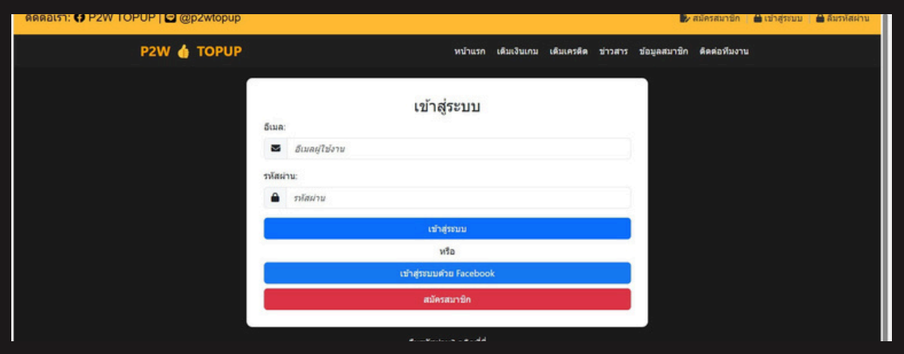
03 ทฤษฎีที่เกี่ยวข้อง

- Phishing: การใช้เว็บไซต์หรืออีเมลปลอมเพื่อหลอกลวงเหยื่อให้เปิดเผยข้อมูลส่วนตัว
- Risk Management: การประเมินและหาวิธีเพิ่มโอกาสในการโจมตีไซเบอร์ให้สำเร็จ โดยลดข้อผิดพลาดที่อาจเกิดขึ้น
- Authentication & Authorization (AAA): การหลอกลวงระบบยืนยันตัวตนและสิทธิ์การเข้าถึง เพื่อให้สามารถเข้าถึงข้อมูลหรือทรัพยากรที่จำกัด

04 การดำเนินงาน

1.การเลือกเป้าหมายเว็บไซต์
2.การสร้างหน้าเว็บไซต์ปลอม
3.การตั้งค่าเซิร์ฟเวอร์
4.การตั้งค่าเพื่อรับข้อมูลเหยื่อ
5.การหลอกล่อเหยื่อ

05 การแสดงผล



06 โปรแกรมที่ใช้ VS CODE

07 อ้างอิง

TOO GOOD TO BE TRUE HTTPS://YOUTU.BE/WSXMICWMLQI?SI=J11TSIVXHQVUQBLD

08 สรุป

นำเสนอแนวทางการทำงานของ Web Phishing ตั้งแต่หลักการหลอกลวงจนถึงการขโมยข้อมูล รวมถึงแนวทางศึกษาป้องกันและพัฒนาระบบรักษาความปลอดภัยทางไซเบอร์

09 สมาชิกกลุ่ม

1. 663380583-3 นางสาวแพรไหม หงษ์สำเริง
2. 663380364-5 นางสาวศราพร เบ้าหินลาด
3. 663380565-5 นางสาวบัญจรัตน์ โยธีเสวต
4. 663380575-2 นางสาวศรัณญา ชัยปลื้ม
5. 663380579-4 นางสาวอริศรา สีพาเสน
6. 663380365-3 นายสาริษฐ์ บุตรช่วง