Group 10 Sec. 2

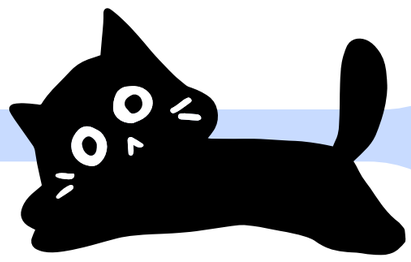
Wi-Fi Disconnect & ARP Poisoning

อาจารย์ประจำวิชา: ศ.ดร.จักรชัย โสอินทร์

SC362006 INFORMATION AND COMMUNICATION TECHNOLOGY SECURITY

หลักการและเหตุผล

Wi-Fi Disconnection Simulator:
ARP Poisoning ปัจจุบัน การโจมตีทางไซเบอร์ผ่านเครือข่ายไร้สาย **(Wi-Fi)** เป็นภัยคุกคามสำคัญ หนึ่งในเทคนิคที่ใช้คือ **ARP Poisoning** ซึ่งนำไปสู่การโจมตีแบบ **Man-in-the-Middle (MitM)** ทำให้แฮ็กเกอร์สามารถดักฟัง แก้ไข หรือขโมยข้อมูลได้ โปรแกรมนี้ถูกพัฒนาขึ้นเพื่อจำลองการปลดการเชื่อมต่อ **Wi-Fi** ของเป้าหมาย และสาธิตผลกระทบของช่องโหว่ดังกล่าวในเครือข่าย



วัตถุประสงค์

1. ศึกษาหลักการทำงานของ **Wi-Fi Deauthentication Attack** และ **ARP Poisoning**
2. จำลองการปลดการเชื่อมต่อ **Wi-Fi** และดักฟังข้อมูลผ่าน **ARP Poisoning**
3. ศึกษาความเสี่ยงใน **Wi-Fi** เข้าใจช่องโหว่ในเครือข่าย **Wi-Fi** ที่อาจถูกโจมตี และวิธีที่ผู้โจมตีดักจับข้อมูลจากเครือข่ายที่ไม่มีการเข้ารหัส

วิธีการใช้งาน

1. สแกนหา **Wi-Fi** และตัดการเชื่อมต่อ **Wi-Fi** ของเหยื่อ
2. เลือก **Wi-Fi** ที่ต้องการ
3. ตัดการเชื่อมต่อ **Wi-Fi** ของเหยื่อเพื่อให้เหยื่อเชื่อมต่อกับ **Wi-Fi** ใหม่
4. ดักจับรหัส **Wi-Fi** ที่เข้ารหัสได้
5. ถอดรหัสรหัส **Wi-Fi** ที่จับได้
6. เข้าร่วม **Wi-Fi** ของเหยื่อเมื่อได้รหัส
7. ทำ **ARP Poisoning** กับ **Wi-Fi** ของเหยื่อ
8. ใช้ **Wireshark** ในการดักจับข้อมูลจากเหยื่อ

ขอบเขต

1. ศึกษาการทำงานของ Wi-Fi Deauthentication Attack และ ARP Poisoning
2. ทดลองปลดการเชื่อมต่อ Wi-Fi และทำ ARP Poisoning ในเครือข่ายที่ควบคุมได้
3. ใช้อุปกรณ์และซอฟต์แวร์เฉพาะที่ได้รับอนุญาต เช่น Kali Linux และ Wireshark
4. วิเคราะห์ผลกระทบของการโจมตีต่อการเชื่อมต่อ Wi-Fi ของอุปกรณ์เป้าหมาย

ความสามารถ

ตัดการเชื่อมต่อ WI-FI ของเหยื่อและ ทำ ความสามารถในการตัดการเชื่อมต่อ WI-FI ของเหยื่อและทำการโจมตี ARP (ARP Poisoning) เพื่อแทรกแซงการส่งข้อมูลในเครือข่าย

ข้อสรุป

การจำลองตัดการเชื่อมต่อ **Wi-Fi** และดักจับข้อมูลเกี่ยวข้องกับการตัดการเชื่อมต่อ **Wi-Fi** ของเหยื่อให้หลุดจากเครือข่าย และเชื่อมต่อกับเครือข่ายที่เราเตรียมไว้ จากนั้นดักจับรหัส **Wi-Fi** ที่เข้ารหัสและถอดรหัสออกมา เพื่อเข้าสู่เครือข่ายของเหยื่อ หลังจากนั้นทำการโจมตี **ARP Poisoning** และใช้ **Wireshark** ในการดักจับข้อมูลที่ส่งผ่านเครือข่ายเพื่อสอดแนมและวิเคราะห์ข้อมูลที่รั่วไหล

เครื่องมือ

4 มีนาคม **2568**

อ้างอิง:
https://youtu.be/X49lIPHcurE?feature=shared

สมาชิก **Group 10 Sec. 2**

1. นางสาวณัฐณิชา รัตน์เพ็ชร 663380001-1
2. นายวัฒนวิทย์ สะมะโน 663380005-3
3. นายปภพ แสงสมนึก 663380490-0
4. นางสาวไพรินทร์ พรมสะอาด 663380196-0