



IP CAMERA PENTESTING

CP422031 Introduction to Cybersecurity

Group13 sec2

อาจารย์ที่ปรึกษา:

ศ.ดร.จักรชัย โสอินทร์

ผศ. ดร.สาริต กระเวนกิจ

หลักการและเหตุผล

เนื่องจาก IP Camera เป็นอุปกรณ์ที่เชื่อมต่อกับอินเทอร์เน็ต และอาจถูกโจมตีโดยผู้ไม่ประสงค์ดี กล้อง IP Camera แม้จะเป็นอุปกรณ์ที่มีประโยชน์ในการเฝ้าระวังความปลอดภัย แต่ก็มีความเสี่ยงที่ผู้ใช้งานต้องตระหนักถึง หากไม่ต้องการให้ข้อมูลส่วนตัว รั่วไหล จึงทำการจำลองการแฮกcctv camera ไว้ศึกษาช่องโหว่ที่อาจเกิดขึ้นในกล้อง

วัตถุประสงค์

- 1.เพื่อศึกษาการจำลองการโจมตีและการป้องกันภาพและวิดีโอจากกล้อง
- 2.เพื่อพัฒนาความรู้เกี่ยวกับการโจมตีแบบ Brute force Attack

ขอบเขตการศึกษา

1. Brute force Attack

Brute Force Attack ใช้การเดาUSERNAME PASSWORD PATHผ่านทุกความเป็นไปได้ของตัวอักษรในแต่ละหลัก

2.RTSP Protocol

ใช้ในการควบคุมการสตรีมวิดีโอแบบเรียลไทม์ โดยกล้องวงจรปิด (IP Camera) หลายรุ่นรองรับ RTSP เพื่อให้ผู้ใช้สามารถดูวิดีโอผ่านเครือข่าย

3. Network Scanning

สแกนเครือข่ายเพื่อค้นหาอุปกรณ์ที่กำลังเปิดให้บริการ RTSP เช่น การใช้เครื่องมืออย่าง nmap เพื่อค้นหาอุปกรณ์เป้าหมาย

เครื่องมือที่ใช้

SOFTWARE



CHAT GPT



LINUX



NMAP

HARDWARE



CAMERA SECURITY

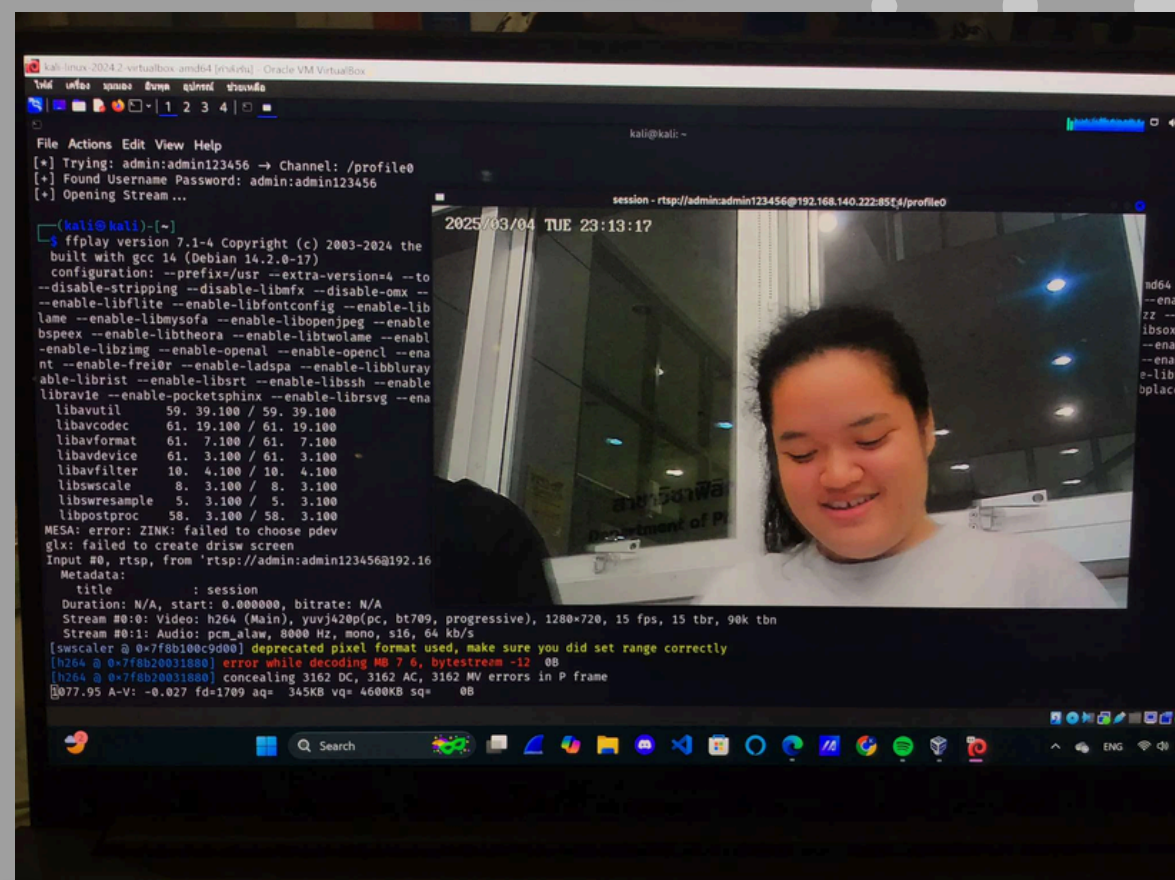
สมาชิก

- 663380092-2 นางสาวกนกนิภา ปัญเศษ
- 663380108-3 นางสาวณัฐชนก นาคจันทร์
- 663380111-4 นางสาวนภัสวรรณ ชัยบาล
- 663380122-9 นายภูริพัฒน์ เกิดกลาง
- 663380135-0 นายสุรสิทธิ์ สวัสดิผล
- 663380471-4 นายพุทธิชา รัตนา

หลักการทำงาน

เริ่มจากการหา IP address wifi ,IP address camera และพอร์ต RTSP โดยการ nmap เมื่อได้ข้อมูลเหล่านี้ รวมถึงพอร์ตที่ RTSP เปิดใช้งาน จะนำข้อมูลเหล่านั้นมาทำการbruteforce เพื่อหา username password และchannel ของ IP camera (v360pro)โดยการเขียนscript และสร้างไฟล์เก็บข้อมูลusername password และchannel เมื่อสามารถเข้าถึง IP camera จะสามารถดู Streaming ของกล้องนั้นๆ ได้

ผลลัพธ์



สรุปผล

จากการศึกษาและทดสอบการโจมตีแบบ Brute Force ผ่าน RTSP Protocol โดยเริ่มจากการใช้ Nmap เพื่อสแกนพอร์ตที่เปิดใช้งานบนกล้อง IP ซึ่งส่วนใหญ่จะใช้พอร์ต 554 หรือ 8554 สำหรับ RTSP จากนั้นใช้เครื่องมือ Hydra เพื่อทำการโจมตีรหัสผ่านด้วยไฟล์ password.txt เพื่อลองเข้าถึงผ่าน RTSP URL หากสำเร็จจะสามารถดูสตรีมของกล้องได้ การทดสอบนี้สามารถสรุปได้ว่า การโจมตีผ่าน RTSP สามารถทำได้สำเร็จเมื่อมีการตั้งค่านิรหัสผ่านที่อ่อนแอและไม่ได้ป้องกันอย่างเพียงพอ

อ้างอิง

- 1.https://csperson.kku.ac.th/chakchai/images/362006_2023/1.png
- 2.https://ipcamtalk.com/threads/how-to-enable-onvif-rtsp-etc-on-alliexpress-v360-pro-camera.75308/?utm_source=chatgpt.com&fbclid=IwY2xjawlXl9LeHRuA2FlbQlxMAABHZGR16G40IwjXi9KdwnRzCIGtx-CJSl8tkYyqN4x_hbq3Fd8rrP7Prig_aem_H_KSnJKRxnMDeAQoqF30rg