หัวข้อนำเสนอเรื่อง

Traffic Protection

หลักการ

ดักจับ packet ที่วิ่งเข้ามา ผ่าน TUN Interface / VPN เพื่ออ่าน Payload ที่ไม่ได้เข้ารหัสภายใน packet บนมือถือ

วัตถุประสงค์

เพื่อศึกษาการทำงานการดักจับ packet บนมือถือ และทดสอบการทำงานของการส่ง payload เพิ่มเติมไปยังแอปพลิเคชั่น

ขอบเขต/ฟังก์ชันการทำงาน

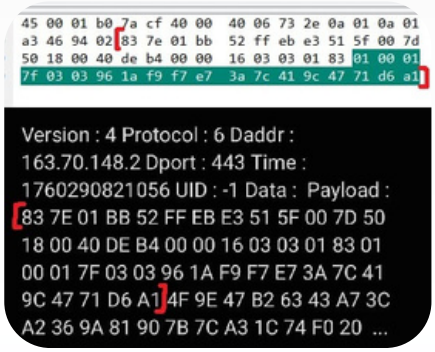
ส่ง payload จากการดักจับ packet เข้าไปเก็บใน SQL Lite Database และเรียกการใช้งานเพื่อดึง payload ในฐานข้อมูลไปแสดงผลบนแอปพลิเคชัน

ผลลัพธ์การทำงาน

Payload TCP และ UDP ที่วิ่งเข้าและออกผ่าน TUN Interface และนำมาแสดงผลบน Application NetGuard สามารถอ่านได้ใกล้เคียงกับ Wireshark ลักษณะของ Packet ที่ดักจับได้และนำมาลงบนไฟล์ PCAP มีลักษณะเล็ก และอ่านได้บ้างเป็นบางคำ

วิธีการทำงาน

ส่ง payload ไปแสดงผลบน application ได้โดย packet ที่ดักจับได้ในการทดสอบ เข้ามาจากภาษาซีเป็น TLS Record Header ของ HTTPS เข้าไปเก็บใน SQL Lite Database และส่งไปถอดรหัสที่ Java บน ActivityTraf.java ผลการทดสอบเปรียบเทียบกับการถอดรหัสด้วย Wireshark พบว่าผลลัพธ์ตรงกัน และ payload ที่ส่งเข้ามามีเนื้อหาที่แตกต่างกันเล็กน้อย



เครื่องมือที่ใช้

รายละเอียดวิชา 422011 Introduction to Computer Networking
Group 9 Sec. 2

เสนออาจารย์

ศาสตราจารย์ดอกเตอร์ จักรชัย โสอินทร์

ผู้จัดทำ

1. นางสาวมนัสนันท์ เสนารถ รหัสนักศึกษา 673380183-0
2. นายสิทธิพล มีสอาด รหัสนักศึกษา 673380492-7
3. นาย จักรี สิทธิพันธ์ รหัสนักศึกษา 673380478-1
4. นายเพชรไพฑูรย์ วงษ์พิมล รหัสนักศึกษา 673380495-1
5. นางสาวภัทราพร โกศล รหัสนักศึกษา 673380485-4
6. นางสาว ญาณิน วชิรโกวิทย์ รหัสนักศึกษา 673380156-3

เอกสารอ้างอิง

[1] กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี
https://www.thaipoliceonline.go.th

[2] Bangkok Post
https://www.bangkokpost.com

[3] Proteus-Cyber
https://proteuscyber.com

[4] GitHub
https://github.com

[5] App DNS666
https://dns66.th.uptodown.com

[6] F-Droid
https://f-droid.org/packages/com.celzero.bravedns

[7] AstrurGeek
https://asturgeek.es/2023/02/trackercontrol-una-app-para-controlar-el-tracking-android