

Traffic Protection



วัตถุประสงค์

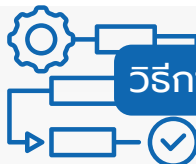
**ขอบเขต/ฟังก์ชันการทำงาน**

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 ที่จับได้ในการทดสอบ เข้ามาจากภาษาซีเป็น TLS Record Header ของ HTTPS เข้าไปเก็บใน SQL Lite Database และส่งไปถอดรหัสที่ Java บน ActivityTraf.java

ผลการทดสอบเปรียบเทียบกับ การถอดรหัสด้วย Wireshark พบว่าผลลัพธ์ตรงกัน และ payload ที่ส่งเข้ามามีเนื้อหาที่แตกต่างกันเล็กน้อย

```
Version : 4 Protocol : 6 Daddr :  
163.70.148.2 Dport : 443 Time :  
1760292289685 UID : -1 Data : Payload :  
AE 14 01 BB F7 9F 27 EA 5B D0 62 C3 50  
18 00 40 9E 6A 00 00 16 03 03 01 83 01  
00 01 F7 03 03 7D B6 5B 0F 09 45 FO FE  
B5 D5 18 30 1A E0 1D 18 56 76 C9 15  
C5 45 8B CF E6 CB B3 75 B1 7B B6 20 ...  
Payload UTF-8 :  
*****@bP@()*[]*  
E*****[!v**E****,u{*(  
.y*****i*****q/a/  
#@xX*o2gateway.instagram.comh  
2+3&$%D*%fu*|  
*****B*****(-e*e*N*)-  
  
)*****S/  
*****Ey*F*4*****Q*1*****  
*@G*E*f*****\^*o*z]a*****  
*****S*o*p*****U*****  
*Sk*ga*Ka*****F3E*66t*q*R)w-z*
```

```
45 00 01 b0 7a cf 40 00 40 06 73 2e 0a 01 0a 01
a3 46 94 02 83 7e 01 bb 52 ff eb e3 51 5f 00 7d
50 18 00 40 de b4 00 00 16 03 03 01 83 01 00 01
7f 03 03 96 1a f9 f7 e7 3a 7c 41 9c 47 71 d6 a1
```

```
Version : 4 Protocol : 6 Daddr :  
163.70.148.2 Dport : 443 Time :  
1760290821056 UID : -1 Data : Payload :  
83 7E 01 BB 52 FF EB E3 51 5F 00 7D 50  
18 00 04 DE B4 00 00 16 03 03 01 83 01  
00 01 7F 03 96 1A F9 F7 E7 3A 7C 41  
9C 47 71 D6 A1 4F 9E 47 B2 63 43 A7 3C  
A2 36 9A 81 90 7B 7C A3 1C 74 F0 20 ...
```

```
Version : 4 Protocol : 17 Daddr :  
115.178.58.10 Dport : 53 Time :  
1760429277923 UID : -1 Data : Payload :  
7A 7D 01 00 00 01 00 00 00 00 00 00 07  
67 61 74 65 77 61 79 09 69 6E 73 74 61 67  
72 61 6D 03 03 6F 6D 00 00 1C 00 01  
Payload UTF-8: z}gateway instagramcom
```



เครื่องมือที่ใช้



รายละเอียดวิชา 422011 Introduction to Computer Networking
Group 9 Sec. 2



เสนออาจารย์

ศาสตราจารย์ดอกเตอร์ จักรชัย โสอินทร์

ผู้จัดทำ

- | | |
|----------------------------|--------------------------|
| 1.นางสาวมนัสนันท์ เสนารต | รหัสนักศึกษา 673380183-0 |
| 2.นายสิทธิพล มีสอาด | รหัสนักศึกษา 673380492-7 |
| 3.นาย จักร์ สิริพันธ์ | รหัสนักศึกษา 673380478-1 |
| 4.นายเพชรไพฑูรย์ วงษ์พิมล | รหัสนักศึกษา 673380495-1 |
| 5.นางสาวภัทรพร โทศล | รหัสนักศึกษา 673380485-4 |
| 6.นางสาว ญานัน 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>