HACK ANDROID

ที่มาและความสำคัญ

การโจรกรรมทางข้อมูลนั้นมีหลายรูปแบบ ที่เข้ามาบุกรุก ลวงข้อมูลโดยการแฝงตัวมาในรูปแบบของโปรแกรมที่กดติดตั้งดังนั้นจึงเลือกศึกษาการโจมตีแบบ BACKDOOR (แบคดอร์) เมื่อเราโดนแบค ดอร์ ติดเข้าในเครื่องแล้ว แฮกเกอร์ (HACKER) จะสามารถเข้ามาขโมยข้อมูลต่างๆของเครื่องเหยื่อได้ โดยที่เหยื่อยังไม่ทันรู้ตัวด้วยซ้ำ การทำงานของแบคดอร์ จะทำงานทุกครั้งโดยเริ่มตั้งแต่เหยื่อเปิดอุปกรณ์ขึ้นมาและทางคณะผู้จัดทำได้เลือกแฮกโทรศัพท์ในระบบANDROID

วัตถุประสงค์

1. เพื่อศึกษาการโจมตีแบบแบคดอร์
2. เพื่อศึกษาการแฮกข้อมูลจากโทรศัพท์ในระบบANDROID

เครื่องมือที่ใช้

THE FAT RAT

หลักการทำงาน

ติดตั้งไฟล์ APK โปรแกรม ที่เครื่องเป้าหมายสั่งการทำงานโดยเครื่องของผู้โจมตี

ผลลัพธ์ที่ได้

calllog_dump_20180301133555.txt

```
1
2  ================
3  [+] Call log dump
4  ================
5
6  Date: 2018-03-01 13:35:56 -0500
7  OS: Android 5.0 - Linux 3.4.39-5764310 (armv71)
8  Remote IP: 192.168.137.222
9  Remote Port: 45003
10
11 #1
12 Number  : 0874355833
13 Name    :ฟ้าพม
14 Date    : Thu Mar 01 13:11:47 GMT+07:00 2018
15 Type    : INCOMING
16 Duration: 20
17
18 #2
19 Number  : 0874355833
20 Name    :ฟ้าพม
21 Date    : Thu Mar 01 13:09:12 GMT+07:00 2018
22 Type    : MISSED
23 Duration: 0
24
25 #3
26 Number  : 0874355833
27 Name    :ฟ้าพม
28 Date    : Thu Mar 01 13:08:19 GMT+07:00 2018
29 Type    : MISSED
30 Duration: 0
31
32 #4
33 Number  : 0874355833
34 Name    :ฟ้าพม
35 Date    : Thu Mar 01 13:07:09 GMT+07:00 2018
36 Type    : MISSED
37 Duration: 0
```

GROUP20 SEC.2 รายวิชา วิชา 322376 ความมั่นคงเทคโนโลยีสารสนเทศและการสื่อสาร