

DRONE



PENETRATION TESTING 101

hero.debian [at] gmail [dot] com

About Me ;)



Hero Suhartono, lahir di Jakarta, 1 Desember 19xx, ayah dari 3 (tiga) putri **Faiza Debian,** **Fivana Gutsy dan Feisty Risqia.**

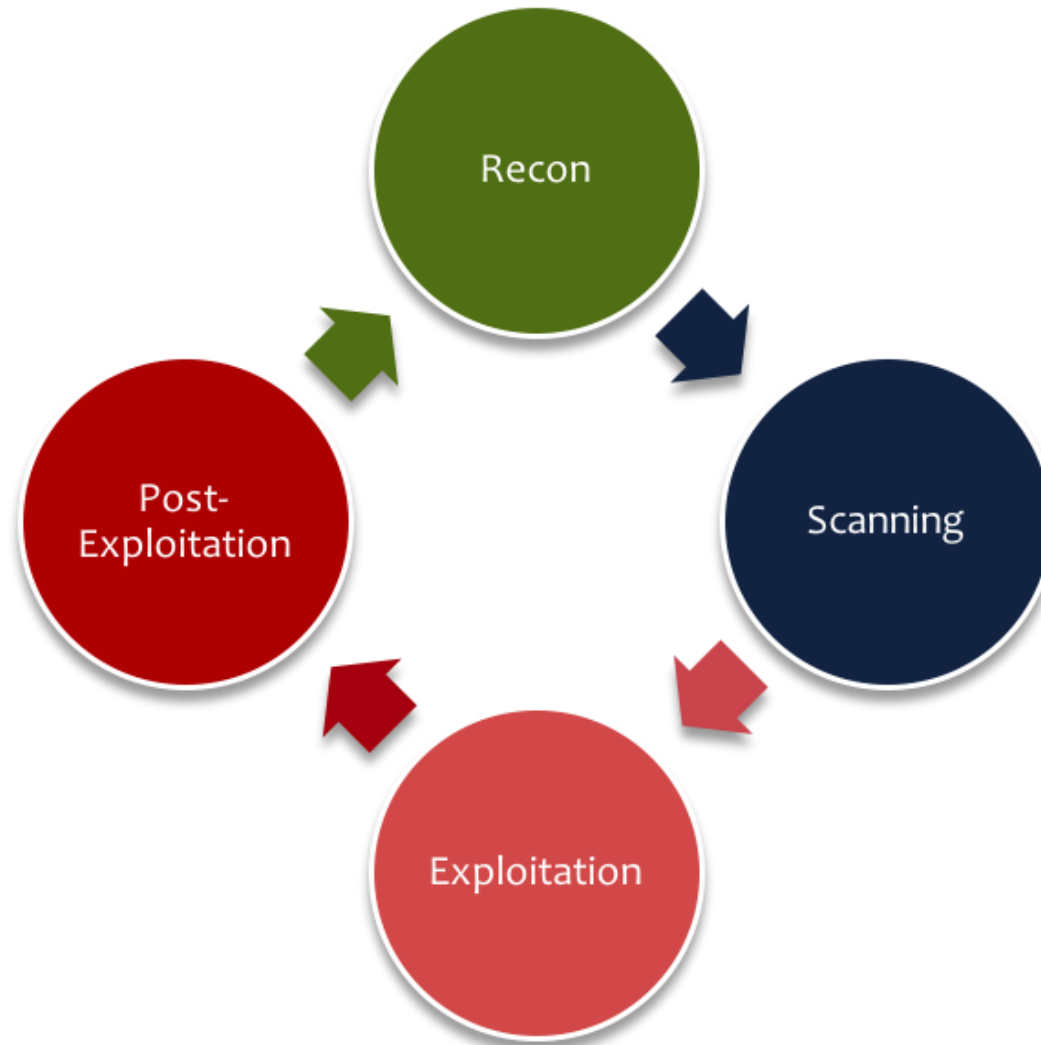
Email : hero.debian@gmail.com

Penetration Testing



Penetration Testing merupakan rangkaian kegiatan dimana seseorang mencoba mensimulasikan serangan yang bisa dilakukan terhadap suatu sistem & jaringan milik organisasi/perusahaan tertentu untuk menemukan kelemahan yang ada pada sistem jaringan tersebut.

Penetration Testing



Drone



Drone adalah pesawat tanpa awak (unmanned aerial vehicle) yang mampu mengendalikan dirinya sendiri atau dikendalikan oleh pilot dari jarak jauh/secara remote.



Drone Attacking



Drone Defenses - Categories

BY PRODUCT TYPE - EMERGING LEADERS IN 'ROGUE DRONE' DEFENSE



PREDATOR BIRD



DRONE NETTING



DRONE SHOOTING



DRONE SHOOTING



JAMMING



EMP



CYBER



GEOFENCING



NO-FLY ZONES



SHUTTERS



CONFETTI GUN



MISSILE



LASER



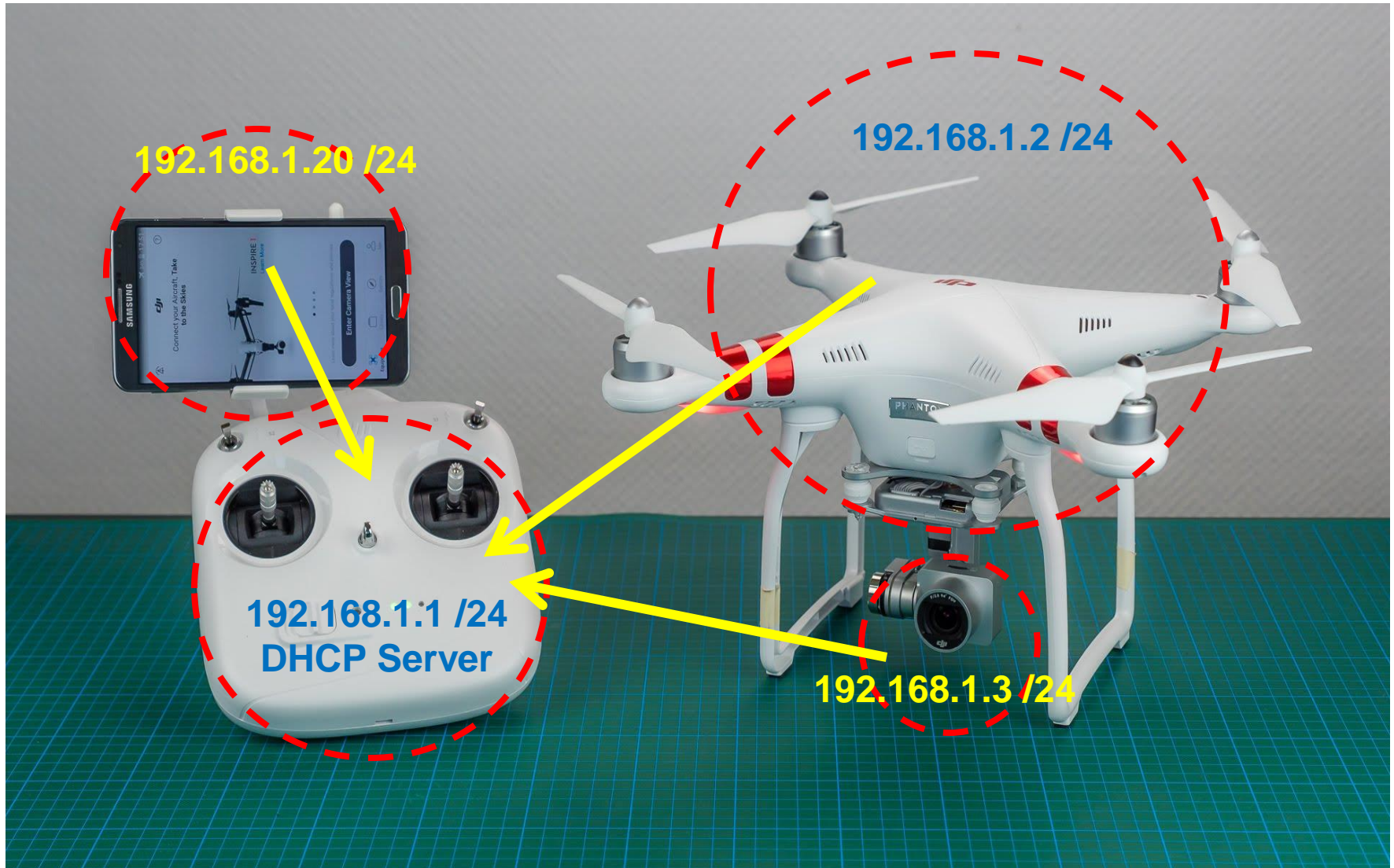
Drone Radio Jamming

Parrot 2.0 Hacking

My Target : Dji Phantom 3 std



My Target : Dji Phantom 3 std





Wireless Wardriving







```
root@DebianGutsy: ~  
File Edit View Search Terminal Help  
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
```

WPA Key : 12341234

Scanning



OS	Host	
	192.168.1.1	<pre>nmap -T4 -A -v 192.168.1.0/24 Nmap scan report for 192.168.1.1 Host is up (0.0026s latency). Not shown: 999 closed ports PORT STATE SERVICE VERSION 21/tcp open ftp vsftpd 3.0.2 MAC Address: 60:60:1F:2F:86:15 (SZ DJI Technology Co.) Device type: general purpose Running: Linux 3.X OS CPE: cpe:/o:linux:linux_kernel:3 OS details: Linux 3.2 - 3.10 Uptime guess: 497.100 days (since Wed Jun 1 13:34:44 2016) Network Distance: 1 hop TCP Sequence Prediction: Difficulty=257 (Good luck!) IP ID Sequence Generation: All zeros Service Info: OS: Unix TRACEROUTE HOP RTT ADDRESS 1 2.61 ms 192.168.1.1</pre>
	192.168.1.2	
	192.168.1.3	
	192.168.1.22	

Scanning



OS	Host
	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 **192.168.1.2**
Host is up (0.0061s latency).
Not shown: 998 closed ports

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	vsftpd 3.0.2
5678/tcp	open	tcpwrapped	

MAC Address: 60:60:1F:12:D3:A6 (SZ DJI Technology Co.)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 3.10
Uptime guess: 497.100 days (since Wed Jun 1 13:34:27 2016)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=256 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Unix

TRACEROUTE
HOP RTT ADDRESS
1 6.12 ms **192.168.1.2**

Scanning



Hosts

Services

OS	Host
	192.168.1.1
	192.168.1.2
	192.168.1.3
	192.168.1.22

Filter Hosts

Nmap Output

Ports / Hosts

Topology

Host Details

Scans

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 22:39:37 2017)

Network Distance: 1 hop

TCP Sequence Prediction: Difficulty=261 (Good Luck!)

Explotasi : FTP @Gimbal



Index of ftp://192.168.1.3/ - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Index of ftp://192.168.1.3/

ftp://192.168.1.3

Most Visited Offensive Security Kali Linux Kali Docs Exploit-DB Aircrack-ng

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

Full Control

Exploitasi : FTP @Controller & @aircraft
















1. Download djigo.apk
2. Reversing djigo.apk
 - dDex2jar
 - jd-gui
3. Script contents
4. Class contents



Exploitasi : FTP @Controller & @aircraft



	assets	10/23/2017 10:50 ...	File folder	
	com	10/23/2017 10:50 ...	File folder	
	it	10/23/2017 10:50 ...	File folder	
	lib	10/23/2017 10:50 ...	File folder	
	META-INF	10/23/2017 10:50 ...	File folder	
	res	10/23/2017 10:51 ...	File folder	
	tae_sdk_plugins	10/23/2017 10:51 ...	File folder	
	AndroidManifest.xml	8/25/2017 3:47 PM	XML Document	63 KB
	classes.dex	8/25/2017 3:47 PM	DEX File	7,116 KB
	classes2.dex	8/25/2017 3:47 PM	DEX File	8,255 KB
	classes3.dex	8/25/2017 3:47 PM	DEX File	6,081 KB
	classes4.dex	8/25/2017 3:47 PM	DEX File	5,966 KB
	resources.arsc	8/25/2017 3:47 PM	ARSC File	6,141 KB

Exploitasi : FTP @Controller & @aircraft



DJIStartupReceiver.class - Java Decompiler

File Edit Navigation Search Help

classes-dex2jar.jar

a.a
android
antistatic.spinnerwheel
b
bitter.jnibridge
bolts
c
cn.sharesdk
com
dji
b
common.ui.dialog
dbox.upgrade.p4
device
e
gs
internal.version
log
logic
middleware
nfz
phone
pilot
active
b
battery.a
college.model
countrycode

DJIJoyStickView.class DJIStartupReceiver.class

```
package dji.pilot.main;

import android.content.BroadcastReceiver;
import android.content.Context;
import android.content.Intent;
import dji.log.DJILogHelper;
import dji.pilot2.main.model.a;
import org.greenrobot.eventbus.EventBus;

public class DJIStartupReceiver
    extends BroadcastReceiver
{
    public static final String a = "dji.go4.STARTUP";

    public void onReceive(Context paramContext, Intent paramIntent)
    {
        DJILogHelper.getInstance().LOGD(DJIStartupReceiver.class.getName(), "onReceive");
        String str = paramIntent.getAction();
        boolean bool1 = paramIntent.getPackage().equals(paramContext.getPackageName());
        boolean bool2 = str.equals("dji.go4.STARTUP");
        if ((bool1) && (bool2)) {
            EventBus.getDefault().post(a);
        }
    }
}
```

apk → res → raw → upgrade_config.json

```

"version": 1,
"products": [
  {
    "productId": 2,
    "groups": [
      {
        "groupName": "SkyWifi",
        "weight": 20,
        "isCameraGroup": false,
        "isSingleFile": true,
        "upgradeMode": 0,
        "devices": ["0700"],
        "ftpDstFileName": "HG310.bin",
        "ftpPwd": "Big~9China",
        "ftpUrl": "192.168.1.2",
        "ftpUsername": "root",
        "pushDevice": 1
      },
      {
        "groupName": "GroundWifi",
        "weight": 20,
        "isCameraGroup": false,
        "isSingleFile": true,
        "upgradeMode": 0,
        "devices": ["2700"],
        "ftpDstFileName": "HG310.bin",
        "ftpPwd": "Big~9China",
        "ftpUrl": "192.168.1.1",
        "ftpUsername": "root",
        "pushDevice": 1
      }
    ]
  },
  {
    "productId": 12,
    "groups": [
      {
        "groupName": "Camera",
        "weight": 40,
        "isCameraGroup": true,
        "isSingleFile": false,
        "upgradeMode": 0,
        "devices": [
          "0100", "0101", "0305", "0306", "0400", "0900", "1100", "1101", "1200", "1201",
          "extraStartFile": "P3C_APP_START",
          "ftpDstFileName": "P3C_FW_V99.99.9999.bin",
          "ftpPwd": "",
          "ftpUrl": "192.168.1.3",
          "ftpUsername": "",
          "pushDevice": 1
        }
      },
      {
        "groupName": "RC",
        "weight": 20,
        "isCameraGroup": false,
        "isSingleFile": true,
        "upgradeMode": 1,
        "devices": ["1400"]
      }
    ]
  }
]

```

Exploitasi : FTP @Controller & @aircraft



apk → res → raw → [upgrade config.json](#)

```
EVTi1JSAkhJ10QYHAFp4rCCrKqr7uX4nwIjbimxeUXX4n0SXmwpRtUvTmHNKiR6dwv/S1Isiwyq  
fppJnQIjMWimvMwOX5utKuKApH5ZUoc7a2DpD  
+LMrUx8NqHFSPJD86jZBQaaqNptU0iJeNG5OUEm9zinwiWdotcYqUQHXY7tr5uu1d1uQp92esxg  
i1s97w2EUA  
+Her165I4zyJP80FyR8N8Cxb6QCRAg0VmSzmhN71q4v1CyVuxiwACP6V/7z0rk/M7RLD6u01Iof  
Zwep/sw7YgdrpVMndUnVGqWvbyJSRwbRn+ObKJ3GT0qOW7AU3Fz1ek/oNG/1NQ/  
+FYpeNMwT6V1cfffKa+z4g6uMIfHqtPCt  
+USoxaQDHCXXqndgDtEuL5nj45cqL5tUtgKo0YIdn51DAjq3DJVY40RmqY1E4U2xzfcE1Vsaw9z  
0JzVWyBjB/Ee13Je1CsJc2FS26JLJfD1JwijB8mHoWuzMBVTr971HeZcd751SgR6VeeEg5qXVk1  
/1voiOVgeAwo0ke1hSGi1KMHbgY/QdnwYC7GEUEEP1FC4hyn61PG7xK7eYxgBIMksMnBeKNyiC  
R8nYa4VOuqyDQCVeBGbvpvywNBC0j251/PmR15L6u7yAa89LqouwEwu0tAD1DavWyI21akfKVIy  
Pwkr3BnhQyeLNftkT6WK+1E1/WMja7s84d4Q1wRbg4GvQ46XRp4Jr/o2otFqHUD3oPQmDgnRQ  
+Tqo2zSyXQ  
+RSRX1IQ3gNprr83vwGHZ8P5DV/YUILSKUEx1CXokdo5tvc2YHTM9MtKP/csyMaXuTRTpNXyL5b  
q1pHqF2j1yt67LL6hxf8dXPpXTtEapjb1k50pZPDPJcR838sTF07XS  
+SyjaSIKVIKY6Qz4ed11OHcZz061R97RPVPYTVQC+w2rhjzMyJ9p4Qq6DS2ZnS  
+6XvCftcsgzqkcER9RVoRqCFfMS1M6BM9N18t1XYJqLDwc3qy90h  
+e6sdpsTokhZo5IOP162GWuZPj5EysDLHwkUuJvrtcDZ3icc6xT20y/CvfsbMPmVSxRc5roYp5J  
XmgjAzJgCTCZErEdFUudtSHEZHstmoFQ3IMue66868+rXVxfZ6nph0B32Yng04bcBLS23xPaAsn  
gufKzASm+Gy/opAOaQUPD8ggLtLxU8+1SbQwvoq0c6RNvk0pISaIEfnt3w2bdNDVqhrJn2nB  
+p3f24StAnYz51quF90cTZ1otBu0MdUhwTAFUhypDNs71xo8Z6P8XFuc3hbomWHBA  
+146Sb0xuh90son9epKDPw44j1EWuGMEMdtVSFjCLHucqfLwhSrJuz
```

DoS & Fake AP





















Red Indicator

Exploitasi : Firmware reversing



<https://github.com/mefistotelis/phantom-firmware-tools>

 mefistotelis	comm_dissector: Use existing dissector for more text types. ...	Latest commit 94d15a1 16 hours ago
 comm_dissector	comm_dissector: Use existing dissector for more text types.	16 hours ago
 symbols	Symbols: Updated all symbol files to the current progress.	3 months ago
 tests	tests: Improved logs to include file names in "###" strings.	3 months ago
 README.md	docs: Added comm_dat2pcap description and example use.	5 days ago
 amba_fwpack.py	amba_fwpack: Prepared the tool for future support of multiple format	6 months ago
 amba_romfs.py	all: Modified script headers to use Python 3 by default.	10 months ago
 amba_sys2elf.py	amba_sys2elf: Completely remade the tool to be just a wrapper.	10 months ago
 amba_sys2elf_template.elf	amba_sys2elf: Completely remade the tool to be just a wrapper.	10 months ago
 amba_ubifs.sh	all: Added executable attribute to scripts.	10 months ago
 arm_bin2elf.py	Added executable attrib to some Python scripts.	3 months ago
 arm_bin2elf_template.elf	arm_bin2elf: Made the tool useable.	10 months ago
 comm_dat2pcap.py	comm_dissector: Updated docs to mention two protocols.	3 days ago
 comm_serial2pcap.py	comm_dissector: Updated docs to mention two protocols.	3 days ago
 dji_flyc_nofly_ed.py	Added executable attrib to some Python scripts.	3 months ago
 dji_flyc_param_ed.py	dji_flyc_param_ed: Fix min/max values order in new fmt.	2 months ago
 dji_fwcon.py	Fix #51	a month ago
 supported_firmwares.csv	doc: Added new entries to supported fw list.	4 months ago

Exploitasi : Firmware reversing



root@DebianGutsy: /home/DroneFirmwareTools/phantom-firmware-tools-master

File Edit View Search Terminal Help

```
root@DebianGutsy:/home/DroneFirmwareTools/phantom-firmware-tools-master# python dji_fwcon.py -vv -x -p P3C_FW_V01.09.0200.
bin
P3C_FW_V01.09.0200.bin: Opening for extraction
P3C_FW_V01.09.0200.bin: Package format version 2016 detected
P3C_FW_V01.09.0200.bin: Header:
[
  'entry_count': 17,
  'hdrend_offs': 950,
  'magic': 305419896L,
  'magic_ver': 1,
  'manufacturer': 'DJI',
  'model': 'P3C',
  'padding': '000000000000000000000000',
  'timestamp': 1497882136L,
  'ver_latest': 17367240L,
  'ver_latest_enc': 157907892,
  'ver_rollback': 0L,
  'ver_rollback_enc': 140540796}
P3C_FW_V01.09.0200.bin: Module index 0
[
  'decrypted_len': 97368L,
  'decrypted_md5': 'ca67ff4709f6c33868e7743c90dcb538',
  'dt_offs': 950L,
  'encrypt_type': 0,
  'reserved2': 1,
  'spcoding': 0,
  'splvalue': 0,
  'stored_len': 97368L,
  'stored_md5': 'ca67ff4709f6c33868e7743c90dcb538',
  'target': 'm0400',
  'target_name': 'gimbal mdl 0',
```

Exploitasi : Firmware reversing



hasil

File Edit View Go Bookmarks Help

home DroneFirmwareTools phantom-firmware-tools-master hasil hasil_ubifs

Search

Name	Size	Type	Date Modified
hasil_ubifs	2 items	folder	Sat 21 Oct 2017 11:34:29 AM WIB
hasil_romfs	3 items	folder	Sat 21 Oct 2017 11:30:14 AM WIB
hasil_amba	13 items	folder	Sat 21 Oct 2017 11:24:29 AM WIB
P3C_FW_V01.09.0200_m2901.ini	201 bytes	plain text document	Sat 21 Oct 2017 11:11:03 AM WIB
P3C_FW_V01.09.0200_m2901.bin	59.6 kB	unknown	Sat 21 Oct 2017 11:11:03 AM WIB
P3C_FW_V01.09.0200_m2900.ini	201 bytes	plain text document	Sat 21 Oct 2017 11:11:03 AM WIB
P3C_FW_V01.09.0200_m2900.bin	42.1 MB	unknown	Sat 21 Oct 2017 11:11:03 AM WIB
P3C_FW_V01.09.0200_m2700.ini	197 bytes	plain text document	Sat 21 Oct 2017 11:11:03 AM WIB
P3C_FW_V01.09.0200_m2700.bin	4.0 MB	unknown	Sat 21 Oct 2017 11:11:03 AM WIB
P3C_FW_V01.09.0200_m1400.ini	212 bytes	plain text document	Sat 21 Oct 2017 11:11:03 AM WIB
P3C_FW_V01.09.0200_m1400.bin	62.1 kB	unknown	Sat 21 Oct 2017 11:11:03 AM WIB
P3C_FW_V01.09.0200_m1203.ini	202 bytes	plain text document	Sat 21 Oct 2017 11:11:03 AM WIB
P3C_FW_V01.09.0200_m1203.bin	3.6 kB	unknown	Sat 21 Oct 2017 11:11:03 AM WIB
P3C_FW_V01.09.0200_m1202.ini	202 bytes	plain text document	Sat 21 Oct 2017 11:11:03 AM WIB
P3C_FW_V01.09.0200_m1202.bin	3.6 kB	unknown	Sat 21 Oct 2017 11:11:03 AM WIB
P3C_FW_V01.09.0200_m1201.ini	202 bytes	plain text document	Sat 21 Oct 2017 11:11:03 AM WIB
P3C_FW_V01.09.0200_m1201.bin	3.6 kB	unknown	Sat 21 Oct 2017 11:11:03 AM WIB
P3C_FW_V01.09.0200_m1200.ini	202 bytes	plain text document	Sat 21 Oct 2017 11:11:03 AM WIB
P3C_FW_V01.09.0200_m1200.bin	3.6 kB	unknown	Sat 21 Oct 2017 11:11:03 AM WIB
P3C_FW_V01.09.0200_m1101.ini	200 bytes	plain text document	Sat 21 Oct 2017 11:11:02 AM WIB

"P3C_FW_V01.09.0200_m0700.bin" selected (4.0 MB), Free space: 75.3 GB

Devices

- 4.1 GB F...
- SYSTEM_DRV
- 270 GB Files...
- Data
- Lenovo_Reco...

Computer

- Home
- Desktop
- File System
- Trash

Network

- Browse Net...

Exploitasi : Drone Jammer



Drones Jammer



A simple drone Jammer designed to hack unwelcomed civilian drones within your backyard range.

Designed by:
Ahmad Jisrawi
jisrawi@gmail.com
<https://twitter.com/ajisrawi>



live
DEMO



Kesimpulan



1. Tidak ada sistem yang 100% aman
2. Apapun Drone-nya : lakukan perubahan wireless key
3. Lakukan upgrade firmware secara berkala
4. Jika memungkinkan lakukan firmware custom untuk meningkatkan keamanan
5. Apapun Drone-nya : bisa dilakukan Penetration Testing

thank you!