

Thiết bị không
dây: không chỉ là
thiết bị phát sóng

Người trình bày: Vi Minh Toại

SECURITY BOOTCAMP 2013



Đơn vị tổ chức:



Đơn vị tài trợ:



Safety from thinking

Sơ lược về diễn giả

- Họ và Tên: Vi Minh Toại
- Đơn vị công tác: Ngân hàng Á Châu – Khối CNTT
- Vị trí công tác: Chuyên viên an ninh mạng
- Công ty hợp tác: công ty cổ phần tin học IT247
(www.it247.vn)
- Địa chỉ email: toaivm@acb.com.vn,
toaivm@it247.vn, minhtoai@yahoo.com
- ĐT: 090 688 5538



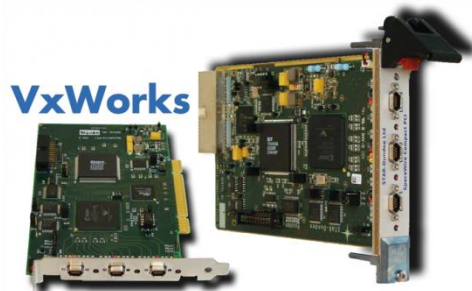
Sơ lược về thiết bị không dây

- TB không dây là thiết bị hoạt động như router và có thêm chức năng phát sóng không dây
- Hầu hết các TB không dây bao gồm: 1 WAN, 1 - 4 LAN, USB (tùy chọn), phát sóng chuẩn A/B/G/N/AC.
- Có loại cho phép sử dụng USB 3G, làm print server,...



OS trên TB không dây

- Hầu hết đều sử dụng Linux, một số ít sử dụng VxWorks, được cấu hình chủ yếu sử dụng giao diện web.
- Bên cạnh các OS của hãng, một số thiết bị được hỗ trợ bởi OS mã nguồn mở là Openwrt, có tính tùy biến cao.



OpenWrt
Wireless Freedom

Giới thiệu về OS Openwrt

- Openwrt là HĐH mã nguồn mở, dựa trên nhân Linux, có tính tùy biến cao.
- Dự án Openwrt khởi động từ năm 2004. Phiên bản Openwrt đầu tiên dựa trên mã nguồn Linksys GPL của thiết bị WRT54G và buildroot của dự án uclibc
- Ưu điểm:
 - ✓ Miễn phí và “mở”
 - ✓ Dễ truy xuất
 - ✓ Hướng về cộng đồng
 - ✓ Có nhiều “packages” cài đặt thêm
 - ✓ Tinh chỉnh cấu hình theo ý muốn



Phiên bản của Openwrt

- Dòng đời các phiên bản:

1. White Russian
2. Kamikaze
3. Backfire (version 10 up)
4. Attitude Adjustment 12.09 (hiện tại)
5. Barrier Breaker (đang phát triển)

Một số thiết bị hỗ trợ Openwrt

- TPLink MR3020/MR3040
- TPLink MR3220/MR3240
- Linksys WRT54G
- Linksys WRT150N
- Dlink DIR300/DIR600
- Thêm nhiều thiết bị trong link sau
<http://wiki.openwrt.org/toh/start>



Hỗ trợ các phụ kiện

- USB to Sound
- Webcam
- USB Bluetooth
- USB Drive
- USB Hub
- USB 3G Modem
- ...



Các tính năng mở rộng của Openwrt

- Phát nhạc không dây qua thiết bị, điều khiển bởi máy tính PC/ĐTĐĐ
- Làm camera theo dõi không dây
- Print server
- Xác thực enterprise qua RADIUS
- Tổng đài điện thoại
- SSH tunnel, sử dụng các công cụ bảo mật trên chính thiết bị không dây
- ...

Cách cấu hình

- Sử dụng giao diện web LuCI
- Sử dụng command

Pineapple | Attitude Adjustment (r36088) | Load: 0.07 0.15 0.07 | Auto Refresh: on

Status System Network Logout

Overview Firewall Routes System Log Kernel Log Processes Realtime Graphs

Status

System

Router Name	Pineapple
Router Model	TP-Link TL-MR3020 v1
Firmware Version	OpenWrt Firmware Attitude Adjustment (r36088) / LuCI 0.11.1 Release (0.11.1)
Kernel Version	3.3.8
Local Time	Mon Jul 15 05:48:51 2013
Uptime	0h 4m 22s
Load Average	0.06, 0.14, 0.07

Memory

Total Available	17056 kB / 29212 kB (58%)
Free	1240 kB / 29212 kB (4%)
Cached	7636 kB / 29212 kB (26%)
Buffered	8180 kB / 29212 kB (28%)

Network

IPv4 WAN Status

Type: static	
Address: 172.16.42.1	
Netmask: 255.255.255.0	
Gateway: 172.16.42.42	
DNS 1: 8.8.8.8	
Connected: 0h 2m 46s	

Active Connections

31 / 16384 (0%)

```
login as: root
root@172.16.42.1's password:

BusyBox v1.19.4 (2013-05-05 14:06:49 BST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

_ _ _ _ _
| _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ |
| | W I R E L E S S F R E E D O M | <, . v, // ) ) ) ) )
_ _ _ _ _

ATTITUDE ADJUSTMENT (MK4 Ver. 3.0) ----- ;\|\|\|/;/
* 1/4 oz Vodka Pour all ingredients into mixing ,'\</>\</>'
* 1/4 oz Gin tin with ice, strain into glass., 'X/\></>'
* 1/4 oz Amaretto ;>||></>
* 1/4 oz Triple sec |<|>>X/</>|\
* 1/4 oz Peach schnapps `</></></>||
* 1/4 oz Sour mix '\</></>/'
* 1 splash Cranberry juice `</></>'
-----WiFi_Pineapple MKIV

root@Pineapple:~# █
```

Công cụ bảo mật trên thiết bị không dây







- Cài đặt Openwrt
- Cài đặt các extension khác như:
 - Nmap
 - Nbtscan
 - Dsniff/arpspoof
 - Kismet
 - Tcpdump
 - Aircrack
 - ...

Công cụ bảo mật Pineapple

- Công cụ dùng cho Pentesting trên wifi
- Công cụ có khả năng thực hiện các cuộc xâm nhập bằng wifi, tấn công man in the middle, “yes man”,...
- Giá: 99 USD
- Link web:
hakshop.myshopify.com/collections/wifi-pineapple



Giao diện quản trị Pineapple

→  172.16.42.1:1471/#     

06:02:07 up 17 min, load average: 0.35, 0.21, 0.11

Info	Karma	Resources	Configuration
Firmware Version: 3.0.0 Pine Number:	MK4 Karma Disabled. Start Autostart Enabled. Disable	Refresh Mem: total used 29212 28340 -/+ buffers: 19616 Swap: 524284 4	DNSSpoof Disabled. Start Cron Enabled. Disable
AutoSSH	Network	Logs	Pineapple Bar
AutoSSH: Disconnected. Connect	Refresh Wifi Enabled. Disable Internet IP: Show POE / LAN: 172.16.42.1 WAN / LAN: N/A WAN / Mobile: N/A	To follow a custom log, open the large tile.	This will show infusions waiting to be updated.

Thực hiện demo

- Tùy chọn phát nhạc không dây trên thiết bị wifi từ điện thoại di động
- Sử dụng thiết bị wifi để thực hiện xâm nhập

Một số trang web tham khảo

- openwrt.org
- www.minipwner.com/index.php/minipwner-build
- samiux.blogspot.com/2013/05/howto-tp-link-tl-mr3020-as-wifi.html

Câu hỏi và Trả lời

- Mọi thắc mắc xin vui lòng liên hệ:
- toaivm@acb.com.vn, toaivm@it247.vn,
minhtoai@yahoo.com
- ĐT: 090 688 5538

TRÂN TRỌNG CẢM ƠN