Karmetasploit Configuration a11y.text Karmetasploit Configuration There is a bit of setup required to get Karmetasploit up and going on Kali Linux Rolling. The first step is to obtain the run control file for Karmetasploit: root@kali : ~ # wget

```
https://www.offsec.com/wp-content/uploads/2015/04/karma.rc_.txt --2015-04-03 16:17:27--
https://www.offsec.com/downloads/karma.rc
Resolving www.offensive-security.com (www.offensive-security.com)... 198.50.176.211
Connecting to www.offensive-security.com (www.offensive-security.com)|198.50.176.211|:443...
connected.
HTTP request sent, awaiting response... 200 OK
Length: 1089 (1.1K) [text/plain]

Saving to: `karma.rc' 100%[======================================>] 1,089 --.-K/s in 0s

2015-04-03 16:17:28 (35.9 MB/s) - `karma.rc' saved [1089/1089]
```

root@kali:~# Having obtained that requirement, we need to set up a bit of the infrastructure that will be required. When clients attach to the fake AP we run, they will be expecting to be assigned an IP address. As such, we need to put a DHCP server in place. Letâ€™s install a DHCP server onto Kali. root@kali : ~ # apt update ...snip... root@kali : ~ # apt -y install isc-dhcp-server Reading package lists... Done

```
Building dependency tree
Reading state information... Done
...snip...
```

root@kali:~# Next, letâ€™s configure our dhcpd.conf file. We will replace the configuration file with the following output: root@kali : ~ # cat /etc/dhcp/dhcpd.conf option domain-name-servers 10.0.0.1;

```
default-lease-time 60;
```

```
max-lease-time 72;

ddns-update-style none;

authoritative;

log-facility local7;

subnet 10.0.0.0 netmask 255.255.255.0 {
  range 10.0.0.100 10.0.0.254;
  option routers 10.0.0.1;
  option domain-name-servers 10.0.0.1;
}
root@kali:~# Then we need to install a couple of requirements. root@kali : ~ # apt -y install
libsqlite3-dev Reading package lists... Done
Building dependency tree
Reading state information... Done
...snip... root@kali : ~ # gem install activerecord sqlite3 Fetching: activerecord-5.0.0.1.gem (100%)
Successfully installed activerecord-5.0.0.1
Parsing documentation for activerecord-5.0.0.1
Installing ri documentation for activerecord-5.0.0.1
Done installing documentation for activerecord after 7 seconds
Fetching: sqlite3-1.3.12.gem (100%)
Building native extensions.  This could take a while...
Successfully installed sqlite3-1.3.12
Parsing documentation for sqlite3-1.3.12
```

```
Installing ri documentation for sqlite3-1.3.12
Done installing documentation for sqlite3 after 0 seconds
2 gems installed
root@kali:~# Now we are ready to go. First off, we need to locate our wireless card, then start our
wireless adapter in monitor mode with airmon-ng . Afterwards we use airbase-ng to start a new
wireless network. root@kali : ~ # airmon-ng PHY     Interface       Driver          Chipset

phy0 wlan0          ath9k_htc Atheros Communications, Inc. AR9271 802.11n root@kali : ~ #
airmon-ng start wlan0 PHY Interface Driver  Chipset

phy0 wlan0  ath9k_htc Atheros Communications, Inc. AR9271 802.11n

  (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
  (mac80211 station mode vif disabled for [phy0]wlan0)

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

PID     Name
693     dhclient
934     wpa_supplicant root@kali : ~ # airbase-ng -P -C 30 -e "U R PWND" -v wlan0mon For
information, no action required: Using gettimeofday() instead of /dev/rtc
22:52:25  Created tap interface at0
22:52:25  Trying to set MTU on at0 to 1500
22:52:25  Trying to set MTU on wlan0mon to 1800
```

22:52:25 Access Point with BSSID 00:C0:CA:82:D9:63 started. Airbase-ng has created a new interface for us, â€˜at0â€™. This is the interface we will now use. We will now assign ourselves an IP address. root@kali : ~ # ifconfig at0 up 10.0 .0.1 netmask 255.255 .255.0 root@kali:~# Before we run our DHCP server, we need to create a lease database, then we can get it to listening on our new interface. root@kali : ~ # touch /var/lib/dhcp/dhcpd.leases root@kali : ~ # dhcpd -cf /etc/dhcp/dhcpd.conf at0 Internet Systems Consortium DHCP Server 4.3.3

```
Copyright 2004-2015 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/
Config file: /etc/dhcp/dhcpd.conf
Database file: /var/lib/dhcp/dhcpd.leases
PID file: /var/run/dhcpd.pid
Wrote 0 leases to leases file.
Listening on LPF/at0/00:c0:ca:82:d9:63/10.0.0.0/24
Sending on   LPF/at0/00:c0:ca:82:d9:63/10.0.0.0/24
Sending on   Socket/fallback/fallback-net root@kali : ~ # ps aux | grep [ d ] hcpd root      2373  0.0 0.4  28448  9532 ?        Ss   13:45   0:00 dhcpd -cf /etc/dhcp/dhcpd.conf at0
```

root@kali:~# Next Karmetasploit in Action Prev Karmetasploit