Rawal Shripal
(Offensive Security Society – OSS)

SETTING UP A RASPBERRY PI AS AN ACCESS POINT FOR MITM

REQUIREMENTS:

1. Raspberry Pi (with built-in WLAN).
2. WiFi adapter (with master mode).
3. SD Card (4GB or greater) with Raspbian on it.
4. Power supply for your Pi.
5. An SD or MicroSD card reader.
6. Mouse, keyboard, and a monitor.

PREPARATION:

1. Install the OS onto your SD card.
2. Boot the Pi and configure.

CREATING AN ACCESS POINT:

- Plug in the WiFi module when the Pi is off, so you don't cause a power surge.
- Check your wifi adapter using **ifconfig -a**
- Use the following command to update your Raspbian
    1. **Sudo apt-get update**
    2. **Sudo apt-get dist-upgrade**
- Install all the required software
    1. **Sudo apt-get install dnsmasq hostapd**
    2. **Sudo apt-get install bridge-utils**
    3. **Sudo apt-get install isc-dhcp-server**
    4. **Sudo apt-get install iptables-persistent** (Say yes for all 'config' screen)
- Follow the below steps to turn off the new software
    1. **Sudo systemctl stop dnsmasq**
    2. **Sudo systemctl stop hostapd**

- Configuring a static IP
  1. **Sudo nano /etc/dhcpcd.conf**

     Add **denyinterfaces wlan0** and **denyinterfaces wlan1**to the end of the file (but above any other)
  2. **Sudo nano /etc/dhcp/dhcpd.conf**

     Find the lines that say

     Option domain-name "example.org";

     Option domain-name-servers ns1.example.org, ns2.example.org;

     And change them to add a **#** at the beginning of both lines.

     # Option domain-name "example.org";

     # Option domain-name-servers ns1.example.org, ns2.example.org;

     Find the lines that say

     # If this DHCP server is the official DHCP server for the local

     # network, the authoritative directive should be uncommented.

     # authoritative;

     And remove the #, so it says

     # If this DHCP server is the official DHCP server for the local

     # network, the authoritative directive should be uncommented.

     authoritative;
  3. Run **sudo nano /etc/default/isc-dhcp-server** and scroll down to **INTERFACES=""** and update it to say **INTERFACES="wlan0"** (If you have **INTERFACESv4** and **v6** add **wlan0** to both)
  4. **Sudo nano /etc/network/interfaces**

     Find the ***wlan0*** section and edit it so that it looks like following:

     allow-hotplug wlan0

     iface wlan0 inet static

     address 192.168.0.1

     netmask 255.255.255.0

     network 192.168.0.0

if your interface file is empty or doesn't contain a wlan0 entry, search on google for default interfaces file and paste all the default file content to your system file and then proceed.

5. Now restart the dhcpcd daemon

   Sudo service dhcpcd restart

   Sudo ifdown wlan0

   Sudo ifup wlan0

6. Configuring the DHCP server

   Sudo mv /etc/dnsmasq.conf /etc/dnsmasq.conf.orig

   Sudo nano /etc/dnsmasq.conf

7. Add the following lines to your newly created file.

   Interface=wlan0

   dhcp-range=192.168.0.2,192.168.0.20,255.255.255.0,24h

8. Configuring your access point host software.

   Sudo nano /etc/hostapd/hostapd.conf

   This file is currently empty, add the below lines to the file and save.

   interface=wlan0

   driver=nl80211

   ssid=" NetworkName"

   hw_mode=g

   channel=7

   wmm_enabled=0

   macaddr_acl=0

   auth_algs=1

   ignore_broadcast_ssid=0

   wpa=2

   wpa_passphrase=" Password"

   wpa_key_mgmt=WPA-PSK

   wpa_pairwise=TKIP

   rsn_pairwise=CCMP

9. Now we need to tell the system where to find this file.

   Sudo nano /etc/default/hostapd

   Find the line with **#DAEMON_CONF,** and replace it with:

   DAEMON_CONF="/etc/hostapd/hostapd.conf" (don't forget to remove the **#** at the start of the line)

   Likewise, run sudo nano /etc/init.d/hostapd and find the line

   DAEMON_CONF=, and replace it with:

   DAEMON_CONF="/etc/hostapd/hostapd.conf"

10. Now start up the services

    Sudo service hostapd start

    Sudo service dnsmasq start

- You have successfully created an access point, now using a wireless device search for network. The SSID you specified in the hostapd configuration should now be accessible with a password.

SHARING THE INTERNET CONNECTION:

- Configure network address translation
  1. Run **sudo nano /etc/sysctl.conf** scroll to the bottom and add **net.ipv4.ip_forward=1** on a new line and save.
  2. Also run **sudo sh -c "echo 1 > /proc/sys/net/ipv4/ip_forward"** to acticate it immedidately.
  3. Run the following commands to create the network translation between the wifi port **wlan0** and **wlan1**

     Sudo iptables -t nat -A POSTROUTING -o wlan1 -j MASQUERADE

     Sudo iptables -A FORWARD -i wlan1 -o wlan -m state --state RELATED,ESTABLISHED -j ACCEPT

     Sudo iptables -A FORWARD -i wlan0 -o wlan1 -j ACCEPT

4. You can check to see whats in the tables with

   Sudo iptables -t nat -S

   Sudo iptables -S

5. To make this happen on every reboot run

   Sudo sh -c "iptables-save > /etc/iptables/rules.v4"

LET'S TEST THE INTERNET CONNECTION:

1. Finally, we can test the access point host, run

   Sudo /usr/sbin/hostapd /etc/hostapd/hostapd.conf

Now you can see the SSID that you've created. You can try connecting and disconnecting from the SSID with the password you've set before. Connect And check for the internet connection.

(Note:- This tutorial is only for educational purposes. Please do not try this on any individual without his/her consent. If caught doing unethical activities this is a punishable offense. I'm not responsible if any damage is done.)

!!!!!!!CONGRATULATIONS!!!!!!!

YOU'VE SUCCESSFULLY CREATED AN ACCESS POINT FOR MITM WITH A RASPBERRY PI