

Section 9

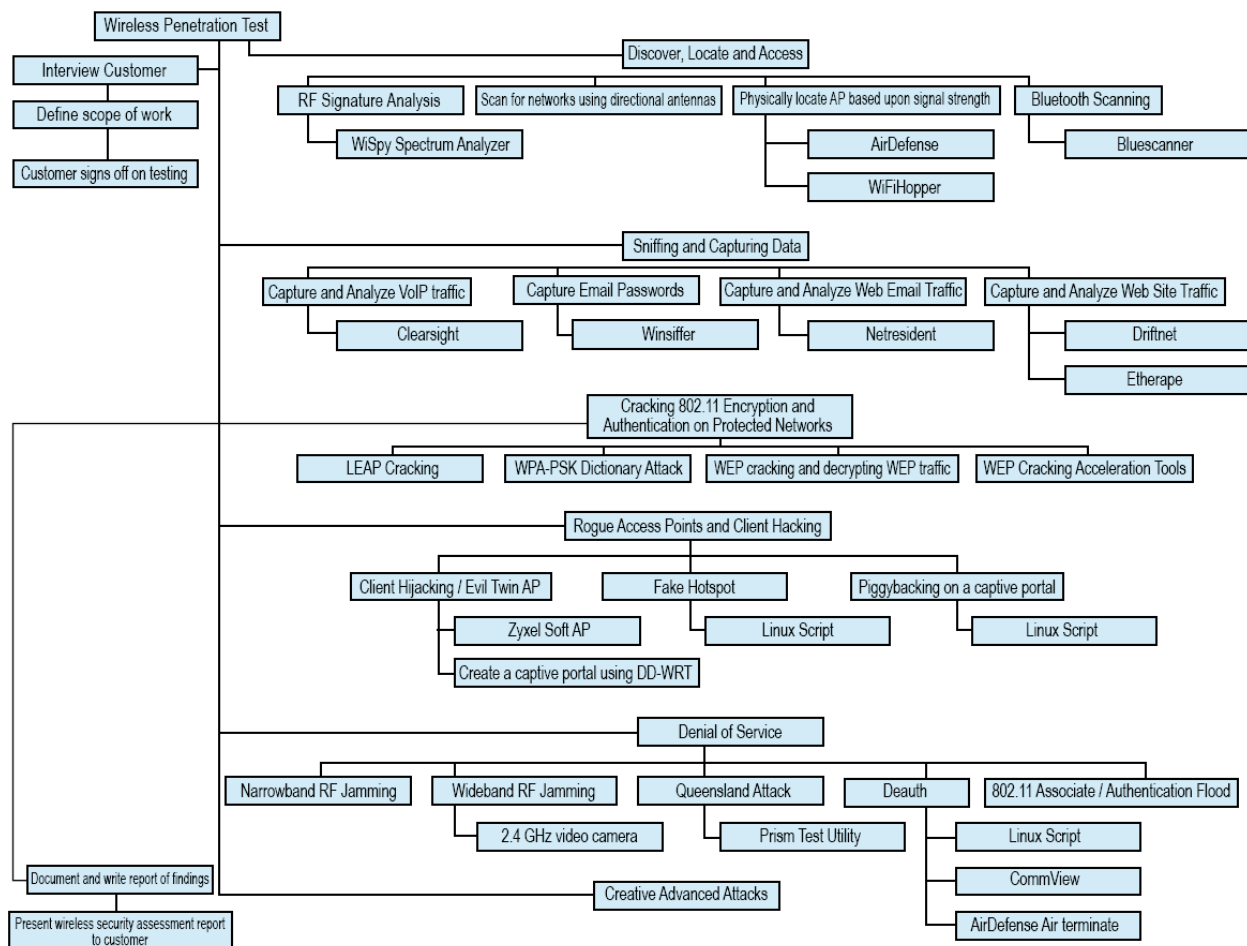
Assessment Flow & Using Linux Custom Script

We've covered many tools and software over the last couple of days. We've included even more in your student kit. One of the best additional items is a fully-functional script to help you use some of the more esoteric Linux Wireless Attack tools.

In previous labs we've included a couple of pieces - in this section we've included a full long lab exercise to walk you through the entire script and what it can do.

But first we'll cover a process flow you can use to perform a Wireless LAN Security Assessment with your kit.

If you want a full Penetration Test - there are some resources and other training you can attend. We've designed this course to help with the Wireless LAN component alone.



Lab 9.1: 80h2 Custom Wireless Tools Script

This custom script wraps popular wireless security tools into an easier-to-use script that takes a lot of work out of the hands of the security auditor.

Product Information

Source

Hotlabs.org

Where, When, Why

This script is designed to give you more time to focus on the task at hand - not all the syntax and details that goes into parameters needed by popular wireless tools. It is designed to go along with the outline of this course and is, of course, optional. Most of the tools that are in use can also be freely used from the command line.

Usage and Features

- Use Linux based wireless security auditing tools without having the need to fully understand the Linux environment

Requirements / Dependencies

- Wireless LAN Security Assessment Toolkit Laptop
- Linux operating system
- Wireless networking card that supports monitor and injection modes
- Included Ubiquiti Wireless NIC

Note: This script was designed specifically for the WLSAT equipment and is not intended to be run on any other platform!

What you will do in this lab:

- Walk through the different features of the 8oh2 script

Lab Part 1



- Step 1. **Double-click the 8oh2 eleven icon** on the desktop.
- Step 2. The discovery part of the script is located at the top giving you 2 choices: Kismet, or Airodump-ng.

```

::::: DISCOVERY OF ACCESS POINTS AND CLIENTS:::::
K - View clients and access points with Kismet
A - View clients and Access points with Airodump
  
```

- Step 3. Type **'K'** and hit **enter** for Kismet.

```

Network List (Autofit)
Name           T U Ch  Packts  Flags  IP Range      Size
! default      A N 006    18  A4  192.168.2.102 214B
! linksys      A N 006    36  T3  192.168.2.0   3k
! yourap       A Y 006    43           0.0.0.0       0B
digis-000      A N 011     1           0.0.0.0       0B
  
```

Kismet will then start to discover access points and clients in the area.

- Step 4. Press **'Q'** to stop and return to the menu.
- Step 5. Back at the menu you also have a choice to discover with Airodump-ng. Press **'A'** and hit **enter**.

```

CH 1 ][ Elapsed: 36 s ][ 2007-05-08 13:04

BSSID          PWR  Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
00:0F:66:85:F5:32  48    110      4   0   6   54  WEP  WEP    yourap
00:18:39:47:AE:AB  29     43     59   0   6   48  OPN             linksys
00:11:95:77:9C:8E  26     38      1   0   6   54  OPN             default
00:02:B3:CF:27:60  17      4      3   0  11  11  OPN             digis-000

BSSID          STATION          PWR  Lost  Packets  Probes
00:18:39:47:AE:AB  00:18:DE:AB:D6:FB  52  128    47
00:18:39:47:AE:AB  00:19:4F:D5:03:20  42   0     2
  
```

Airodump-ng will then hop on all channels to show you the access points and clients in the area.

Press **CTRL + C** or close the window to stop discovering.

Lab Part 2 - Using the custom 8oh2 script to sniff and capture data

- Step 1. To view traffic of an open wireless network type **'3'** and hit **enter**.

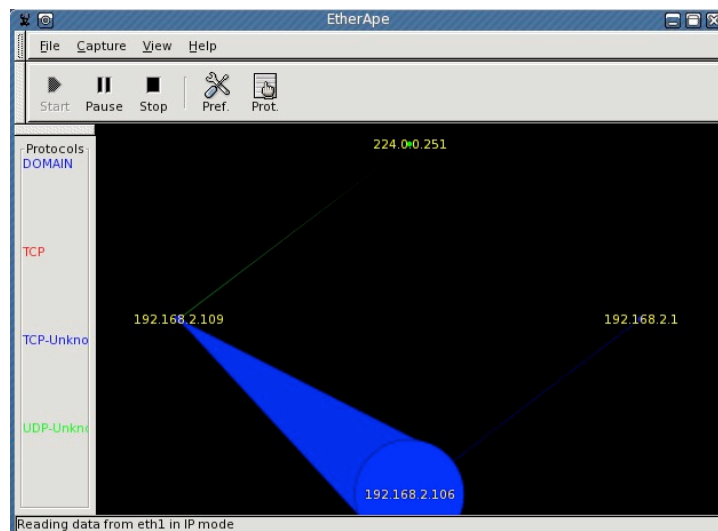
```

:::: SNIFFING AND CAPTURING DATA ON OPEN WIRELESS NETWORKS ::::
3 - View traffic of open wireless networks
U - View live network/bandwidth utilization
  
```

- Step 2. An airodump-ng window will appear, showing you all the networks in the area including their channel. The script then asks you for input: First hit **enter** if you see the Airodump window. **If not type 'R'** to reload airodump.
- Step 3. Enter the **channel of the target wireless network** and hit **enter**.
- Step 4. Wireshark will then appear listening to traffic on that network.

No. .	Time	Source	Destination	Protocol	Info
8	0.196600	192.168.2.106	192.168.2.109	TCP	5902 > 2878 [ACK] Seq=0 Ack=0 Win=582
10	0.198552	192.168.2.106	192.168.2.109	TCP	[TCP Previous segment lost] 5902 > 28
17	0.205109	192.168.2.106	192.168.2.109	TCP	[TCP Previous segment lost] 5902 > 28
18	0.207208	192.168.2.106	192.168.2.109	TCP	[TCP Previous segment lost] 5902 > 28
20	0.208502	192.168.2.106	192.168.2.109	TCP	[TCP Previous segment lost] 5902 > 28
26	0.212084	192.168.2.106	192.168.2.109	TCP	[TCP Previous segment lost] 5902 > 28
33	0.372324	192.168.2.106	192.168.2.109	TCP	[TCP Previous segment lost] 5902 > 28
34	0.373722	192.168.2.106	192.168.2.109	TCP	[TCP Previous segment lost] 5902 > 28
37	0.375562	192.168.2.106	192.168.2.109	TCP	[TCP Previous segment lost] 5902 > 28
42	0.378937	192.168.2.106	192.168.2.109	TCP	[TCP Previous segment lost] 5902 > 28
48	0.384422	192.168.2.106	192.168.2.109	TCP	[TCP Previous segment lost] 5902 > 28
50	0.384958	192.168.2.106	192.168.2.109	TCP	5902 > 2878 [ACK] Seq=62199 Ack=10 Wi

- Step 5. The script lets you know that it is capturing all data to a file in the /tmp directory and to **hit any key** to return to the menu.
- Step 6. Back at the main menu you may type 'U' to view live communications on the network using Etherape.



Close Etherape to return to the menu.

Lab Part 3 - Using the custom 80h2 script to crack WEP key encryption

Step 1. To crack WEP key encryption type **'1'**.

```

          ::::: CRACKING 802.11 ENCRYPTION :::::

1 - Collect IV's of WEP enabled access point
   E - Crack WEP KEY from collected IV's
2 - Collect EAPOL 4-Way handshake of a WPA enabled access point
   W - Crack WPA key from collected handshake
L - Crack LEAP protocol
  
```

Step 2. Airodump will appear giving you a list of possible targets.

Step 3. Press **enter** unless you need to reload airodump.

Step 4. You will then be asked a series of questions.

```

Press "R" to reload the window otherwise press "Enter" to continue;

Enter the channel of your target access point: 6
Would you like to switch to monitor only that channel? y/ny
Would you like to launch a replay attack to collect IV's much faster? y/n y
Enter the BSSID of your target access point: 00:0F:66:85:F5:32
Enter the ESSID (SSID) of the target access point: yourap
Enter the STATION MAC that is associated to your target access point. Enter
'None' to attempt to fake an association. 00:19:4F:d5:03:20█
  
```

Enter the **channel of your target access point** (my target "yourap" is on channel 6) and hit **enter**.

Type **'y'** to monitor only that channel.

Type **'y'** to launch a replay attack against the target network.

Enter the **BBID of your target access point** (found in the airodump window).

Enter the **SSID of your target access point** (found in the airodump window).

Enter the **station MAC of a client who is connected to the network**. Type **'None'** to attempt a fake an association.

Step 5. Once you hit **enter**, a replay attack will be launched against the target. This will dramatically decrease the time it takes to collect enough IV's to crack the WEP key.

```

CH 6 ][ Elapsed: 10 mins ][ 2007-05-08 13:40
BSSID          PWR RXQ Beacons   #Data, #/s CH MB ENC CIPHER AUTH ESSID
00:0F:66:85:F5:32 60 100   6085    8050 215 6 54 WEP WEP   OPN  yourap
00:11:95:77:9C:8E 29 55    5801    5945 166 6 54 OPN      default
00:18:39:47:AE:AB 26 86    5327   15599 191 6 48 OPN      linksys

BSSID          STATION          PWR  Lost  Packets  Probes
00:0F:66:85:F5:32 00:19:4F:D5:03:20 65    0   14551  tXw,Parsons,inp_bg,Free_WiFi
00:18:39:47:AE:AB 00:18:DE:AB:D6:FB 82    2    8304
00:18:39:47:AE:AB 00:0C:F1:15:52:B3 20   117   4252

```

Once an ARP packet is collected, you will notice how fast you collect #Data packets.

- Step 6. To crack the WEP key, return to the main menu of the script and choose **'E'** that is right below our current selection.
- Step 7. Select **option '2'** to pick from a list of target MAC addresses.
- Step 8. Then you will need to give your guess as to what bit encryption is in use (there is no way to know so we should probably start with the weakest and move up). Type **'64'** and hit **enter**.

```

1 - Enter a single MAC address
2 - Pick from a list

Do you have a target MAC address or would you like to pick from a list? 2
You have no way of determining the key length. Please provide the assumed key length: 64/128/256/512 64
Opening /tmp/all_channels-01.cap
Opening /tmp/all_channels-02.cap
Opening /tmp/all_channels-03.cap
Opening /tmp/ivs_for_channel_6-01.cap
Read 701147 packets.

# BSSID          ESSID          Encryption
1 00:40:96:29:96:8D onbravo8       WPA (0 handshake)
2 00:11:21:19:FD:07 WPA (0 handshake)
3 00:11:95:77:9C:8E default        None (192,168,2,104)
4 00:0F:66:85:F5:32 yourap         WEP (118637 IVs)
5 00:18:39:47:AE:AB linksys        None (192,168,2,1)
6 00:02:B3:CF:27:60 digis-000     None (10,11,19,1)
7 00:40:96:36:BE:FD onbravo8       None (0,0,0,0)
8 00:02:B3:BA:84:67 digis-000     None (0,0,0,0)
9 00:02:B3:C3:B7:E8 None (0,0,0,0)
10 DF:AD:9B:74:F1:D0 WEP (1 IVs)
11 00:18:39:DA:66:CA fritz         No data - WEP or WPA
12 00:16:B6:B3:23:6C linksys        None (0,0,0,0)

Index number of target network ? █

```

- Step 9. Find your target access point and type the **corresponding number**. In my case 'yourap' is number 4. You should see a very large number of IV's that are collected.

- Step 10. Aircrack will work with the supplied IV's until it has either cracked the WEP key or failed. As we can see 154,825 IV's was more than enough to crack this 64-bit key in 0 seconds!

```

Aircrack-ng 0.7 r214

[00:00:00] Tested 166 keys (got 154825 IVs)

KB  depth  byte(vote)
0   0/ 4   A1( 28) F6( 22) 3F( 15) 6E( 13) 07( 5) 25( 5)
1   0/ 10  A2( 66) 51( 28) B8( 26) 56( 20) 96( 19) 8A( 16)
2   0/ 2   A3(105) AF( 23) 59( 13) AA( 13) D3( 13) 41( 12)
3   0/ 1   A4(194) A6( 29) 1E( 28) BB( 23) 46( 22) A5( 22)

                                KEY FOUND! [ A1:A2:A3:A4:A5 ]
                                Probability: 100%

Press any key to return to the menu: █

```

- Step 11. Press **any key** to return to the menu.

Lab Part 4 - Using the custom 8oh2 script to crack WPA encryption

- Step 1. Select **'2'** at the main menu.

```

2 - Collect EAPOL 4-Way handshake of a WPA enabled access point
W - Crack WPA key from collected handshake

```

- Step 2. Airodump will appear giving you a list of possible targets. Press **enter** unless you need to reload airodump.

- Step 3. You will then be asked a series of questions.

```

Press "R" to reload the window otherwise press "Enter" to continue:

```

```

Enter the channel of your target access point: 6
Would you like to switch to monitor only that channel? y/ny█

```

Enter the **channel of your target access point**.

Answer **'y'** to monitor only that channel.

- Step 4. Then you will be asked information regarding the access points and clients:

Enter the **BSSID of the target access point** and hit **enter**.

Enter a **station MAC of a connected client** and hit **enter**.

```

Enter the BSSID of your WPA enabled target access point:
00:0F:66:85:F5:32
Enter the STATION MAC that is associated to your target access point. Enter
'None' to attempt to deauth all stations: 00:0f:66:85:f5:32█

```

- Step 5. The script will then attempt to deauth the connected client in order to listen for the 4-Way handshake needed for brute-forcing. In the newer versions of airodump-ng it should show you when you have collected a handshake by the indication in the top right-hand corner:

```
CH 6 ][ BAT: 52 mins ][ Elapsed: 1 min ][ 2007-05-08 20:41 ][ WPA handshake: 00:0F:66:85:F5:32
```

- Step 6. Now that we have collected the handshake we can submit it to our script for bruteforcing by selecting **'W'** at the main menu.

```
default wordlist is /pentest/password/dictionaries/master.txt :::

1 - Enter a single MAC address
2 - Pick from a list

you have a target MAC address or would you like to pick from a list?
```

- Step 7. Choose **'2'** to pick from a list.
- Step 8. Find your target access point and type the corresponding number. In my case 'yourap' is number 1. You should at least 1 handshake. Depending on the strength of the key used, the dictionary file being used, and the speed of your processor this attack will vary in time.

```
Aircrack-ng 0.7 r214

[00:28:34] 219858 keys tested (127,66 k/s)

KEY FOUND! [ very secure! ]

Master Key      : BC 12 75 08 4A E5 C3 53 B5 50 BA DF 03 7E AD 0A
                  73 EA 28 FC 51 43 AD 49 89 69 39 1F 5B DD F9 32

Transcient Key  : 9E B1 88 F8 10 63 89 59 33 3F E3 76 64 63 2F 2E
                  8D A5 55 6C F2 EB 6B D8 E5 13 21 6B 4C CB 95 BA
                  62 52 0F 3C 89 BC 00 39 B9 37 1D DA F9 B3 1D 4E
                  F5 1C AA 68 2E 62 81 C5 ED 8D C0 D5 6C 40 57 35

EAPOL HMAC     : 6E 57 9E CA 05 8B 7E 3E 90 F4 E8 2B 5F 06 A9 0E
```

As you can see the key has been recovered but it took 28 minutes for it to get to the bottom of the supplied wordlist.

Lab Part 5 - Using the custom script to create a fake hotspot

- Step 1. At the main menu type **'H'** to setup a fake hotspot.

```
::::: ROUGE ACCESS POINTS AND CLIENT HIJACKING ::::::

H - Setup a rouge hotspot
I - Piggyback a paying customer at a paid hotspot
```

- Step 2. Then select **1 – Turn laptop into a captive portal** and follow the instructions.

The first variable we declare is what you would like to call your access point. Since our page emulates a real T-Mobile Hotspot login page we can call our access point **'T-Mobile'** and hit **enter**.

Next we need to enter in our DHCP scope for our DHCP to properly assign addresses. **Make sure you separate the starting and ending addresses with a comma!** For example if I wanted to start with address 172.16.1.100 and end with 172.16.1.200 I would type the following:

DHCP Range: **172.16.1.100,172.16.1.200**

Next we will assign the address of the machine/access point so that the clients can appropriately view what is on our webserver by answering the next question What will the access point IP be?

172.16.1.9

Then finally we end the configuration with the desired channel of our access point.

6

NOTE: if you plan on conducting a denial of service attack to get users to switch to your network you might want to choose a different channel than your victim's current channel.

- Step 3. Wait for the configurations to take place. Now every person that chooses to connect to your access point will get assigned an IP address within the scope that you defined. This script is designed to act similar to a captive portal meaning the clients can't go to any website until they supply a username and a password. If you **connect with a different client** you will see any attempt to go to any website will result in a 'redirect' to the fake T-Mobile login page. Since this is just a demonstration the attack does not go any further than the collection of usernames and passwords.

The screenshot shows the T-Mobile HotSpot Customer Connection Center. The header includes the T-Mobile logo and the slogan "Get more from life". Below the header is a navigation menu with items like "About the Service", "Service Plans", "Locations", "What You Need", "Sign Up", "Account Management", "Support", and "Contact Us". The main content area features a promotional message: "Your fast connection to your fast-paced life." followed by a description of the service and a "See Details" link. To the right is a "Connect to the Internet" section with input fields for "User Name:" and "Password:", a "Log in" button, and links for "Roaming on T-Mobile HotSpot?", "Forgot your password?", and "New User?".

Once a victim browses to your site and attempts to login the information presented to the User Name and Password fields will be echoed on the next screen:



A simple addition of a database could be setup to easily document each attempt but we feel that a php script is sufficient for a demonstration.

NOTE: This web server is designed to issue the fake T-Mobile login page but you can add any page you want to do the document directory of `/usr/local/apache/htdocs/T-Mobile/T-mobile_safe` or change the directory in the `/usr/local/apache/conf/httpd.conf` file to point to a different default page.

- Step 4. By hitting **enter** and the prompt of the custom script you can go back to the hotspot menu you can choose '**L**' to view any clients that have connected to your access point if you wish to perform any further attacks against the connected hosts.
- Step 5. Once you are done conducting your attack make sure you choose option '**D**' to destroy and take down the access point. Failure to do so will result in your card staying in access point mode and the DHCP leases will remain recorded the next time you use this script.

Lab Part 6 - Piggybacking a paying customer at a paid hotspot

- Step 1. All that is required to use this part of the script is a MAC address of a user who has already paid. Lab 5.5 concentrated on ways to discover these addresses. Once you have that information use the script to enter that MAC address and assume the IP address of the paid customer.

```
This assumes that you are already connected to the target hotspot
What is the mac address of your target? [ ]
```

Once you enter the MAC address of the paid customer then you should be able to use their services. This script can also be used to quickly change your IP address but keep in mind this script is designed for use with the eth1 interface.

Lab Part 7 - Deauthing a wireless client

- Step 1. Select option '**D**' to deauth one station. Airodump-ng will appear so that you can select your target.

```
***** DENIAL OF SERVICE (DoS) *****
D - Deauthenticate a station
```

BSSID	STATION	PWR	Lost	Packets	Probes
00:18:39:47:AE:AB	00:19:C1:B3:DD:55	51	290	711	linksys
00:18:39:DA:66:CA	00:12:17:6D:FF:B0	10	0	78	fritz
00:02:B3:CF:27:60	00:02:6F:3E:95:BA	-1	0	32	

- Step 2. **Pick a target** from the STATION list.
- Step 3. The custom script is waiting for you to input your targets BSSID (the access points MAC), and the victim station MAC. **Enter them in** and press **enter** to see the attack take place.

Lab Part 8 - Disrupt service to everyone on a network

- Step 1. Select option **'Dx'**.
- Step 2. Airodump-ng will appear giving you a list of possible targets.
- Step 3. All you have to do is pick one STATION on a network by supplying the script with the MAC address of that station and the channel they are on.

```
What is the MAC address of -any- station on that network? 00:02:b3:cf:27:65
What channel is the victim network on? 6

Press Ctrl + C when you want to stop the attack.
Press any key to continue█
```

- Step 4. Once you supply that information, every client that is on that network will stop transmitting packets.
- Step 5. Press **Ctrl + C** to stop the attack as it is a persistent attack
-