

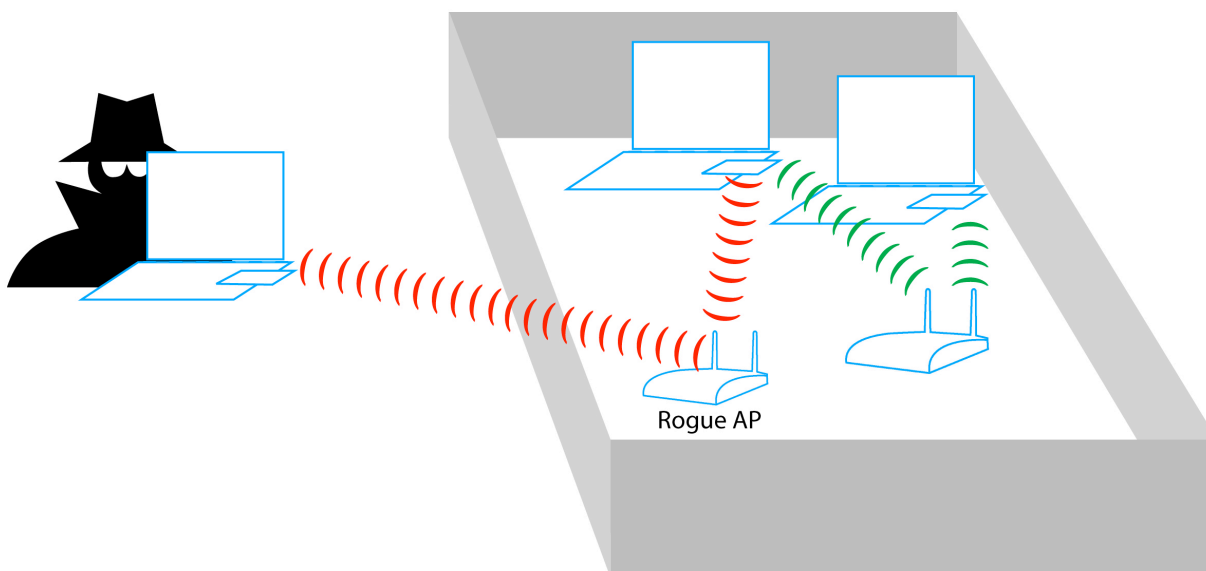
Section 5

Access Points & Client Hijacking

We've all heard about how 'evil' Rogue Access Points can be. Well, to really understand them, we're going to help you make some!

We'll use the various devices in your kit to setup Soft AP Rogues, Captive Portals, Client Hijackings, make a fake Hotspot and other 'cool' techniques hackers use to gain access to personal information.

Have fun - but remember... *"With great power comes great responsibility."*



LAB 5.1: Using ZyXEL Soft AP

The purpose of this lab is to learn how to create a soft AP and how to hijack client stations thus creating a DoS and enabling a peer attack or a Man in the middle attack.

What you will do in this lab:

- Configure the ZyXEL client as a soft AP
- Set the SSID of the ZyXEL Soft AP
- Give users internet access via a soft AP using internet Connection Sharing

Lab Part 1 - Configure the ZyXEL Soft AP to attract users to a fake internet connection

Step 1. Plug in the Zyxel AG-225H USB adapter.



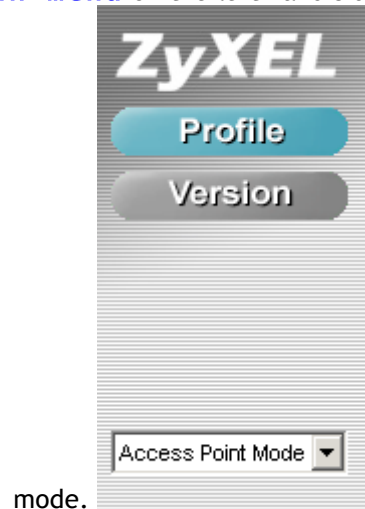
Step 2. Launch the **zyxel** utility. **Start → wireless Tools → zyxel AG-225H(v2) utility**

Note: You'll need to choose the version of the Zyxel utility that matches the revision of your AG-225H USB Adapter -

It may appear in the system tray in the lower right corner of the task bar as a icon with the letter Z.



- Step 3. Click the **drop down menu** on the left hand side to choose Access Point

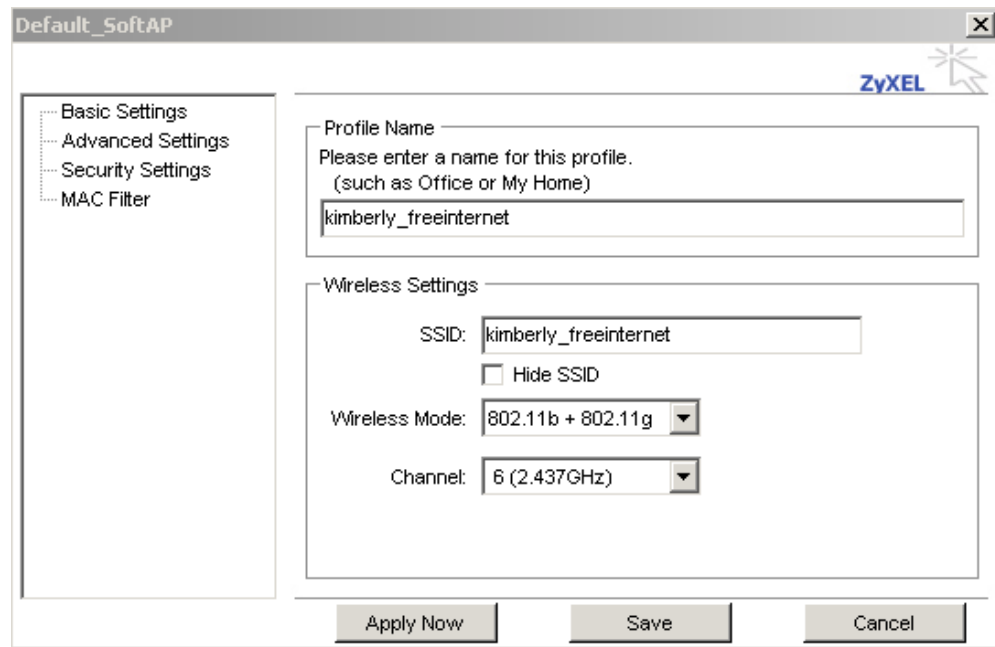


- Step 4. Click the **Name Default_SoftAP** and **click the properties button**.

Profile List (current profile tagged #)

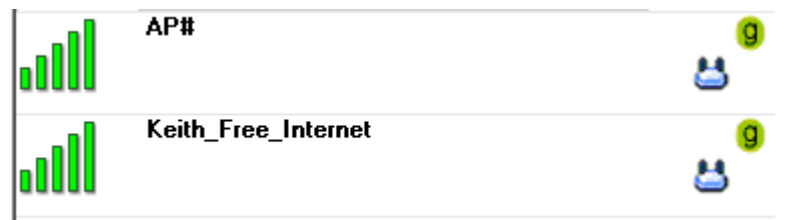
Name	SSID	Wireless Mode	Security	
(#)Default_S...	WLAN_AP	802.11b + 802.11g	Disabled	

- Step 5. Type your *yourname_freeinternet* in the profile name field and the SSID field.



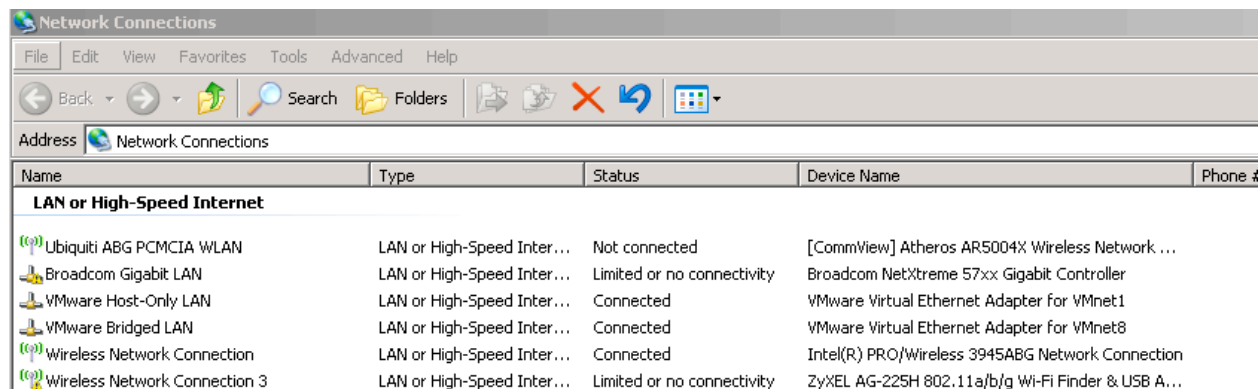
Step 6. Click the **apply now** button. Wait for the Status to show the updated information.

1



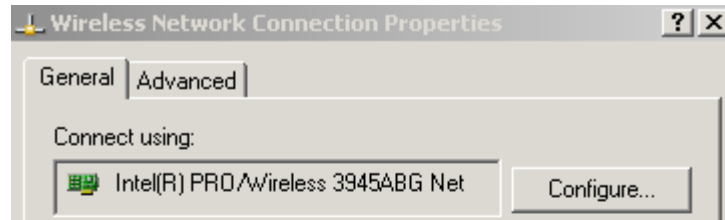
Lab Part 2 - Share your internet connection on your WLSAT laptop

Step 1. Open **your network connections** on the WLSAT laptop.

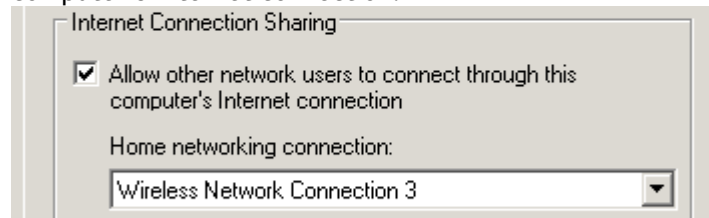


Step 2. Connect the Intel internal ABG NIC to the classroom AP.

- Step 3. Right click the **Intel Internal ABG NIC** and choose **properties**.



- Step 4. Click the **advanced tab**.
- Step 5. Check the box **allow other network users** to connect through this computer's internet connection.



- Step 6. Choose the **wireless network connection 3** (this is the name for the internal adapter) from the dropdown box for Home Networking Connection.

LAN or High-Speed Internet

Ubiquiti ABG PCMCIA WLAN	LAN or High-Speed Internet	[CommView] Atheros AR5004X Wireless Network ...
Broadcom Gigabit LAN	LAN or High-Speed Internet	Broadcom NetXtreme 57xx Gigabit Controller
VMware Host-Only LAN	LAN or High-Speed Internet	VMware Virtual Ethernet Adapter for VMnet1
VMware Bridged LAN	LAN or High-Speed Internet	VMware Virtual Ethernet Adapter for VMnet8
Wireless Network Connection	LAN or High-Speed Internet	Intel(R) PRO/Wireless 3945ABG Network Connection
Wireless Network Connection 3	LAN or High-Speed Internet	ZyXEL AG-225H 802.11a/b/g Wi-Fi Finder & USB A...

NOTE: The Intel Internal wireless adapter is connected to the internet and it is being shared with users of the ZyXel wireless adapter which is configured as an access point. If you have a wired network connection to the internet then you would configure Internet Connection Sharing in the properties of that adapter.

- Step 7. Click **OK**.
- Step 8. Verify you have internet connectivity from your **WLSAT laptop**.

Lab Part 3 - Test the connection from your wireless client

- Step 1. Connect your Nokia N800 to **the yourname_freeinternet** SSID.
- Step 2. Verify your Nokia is connected to the ZyXEL Soft AP by viewing the station MAC address in the **ZyXEL** program.
- Step 3. Open a **web browser** and verify you have internet access. - **Hitcast** on the Nokia N800 and click the play button.

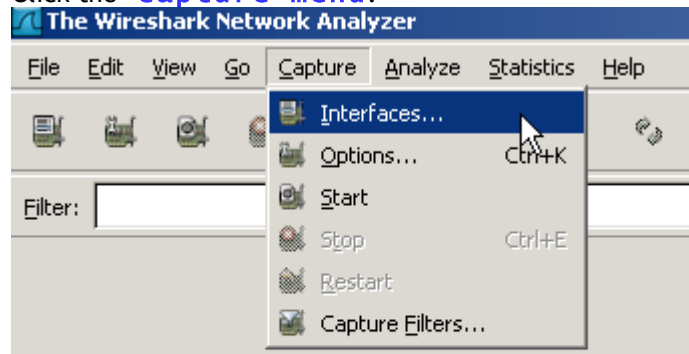
Lab Part 4 - Perform a man in the middle attack by monitor the client's traffic on the WLSAT laptop - Using Wireshark

Step 4. Plug in the *Airpcap* USB device.

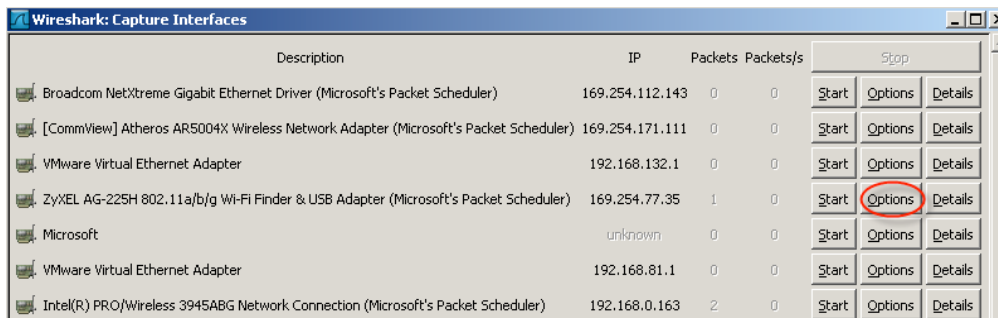


Step 1. Open Wireshark - **start** → **wireless tools** → **wireshark**

Step 2. Click the **capture menu**.



Step 3. Click **interfaces**.



Step 4. Click the **options button** next to the ZyXEL adapter.

Step 5. Click the **check box update list of packets** in real time.

Step 6. Click the **start button**.

Step 7. Review the packets being sent by the Nokia N800 to the internet via the WLSAT laptop.

NOTE: This same lab could be performed using a Wireless Broadband Air card for Internet connectivity.

What you learned in this Lab:

In this Lab you learned to:

- a. Setup up a soft AP
 - b. Route hijacked users through your WLSAT laptop to the internet
 - c. Create an evil twin attack
-

Variables

SSID name of the Soft AP - yourname_freeinternet

Linksys DD-WRT AP IP address - 192.168.1.1

Lab 5.3: Client Hijacking / Evil Twin AP

In this attack you can trick wireless clients to connect to your access point instead of the actual access point; therefore, having more control over the victim clients who connect.

Product Information

Where, When, Why

In a penetration test, you will benefit from clients coming over to your the network you control. Once a client is connected you can continue to attack their machine by direct means (exploit vulnerable services), indirect means, (DNS cache poisoning), or by tricking them into giving you their sensitive information (spoofed authentication on a page they are expecting to log into).

Usage and Features

- Allows more control over a connected wireless client


Requirements / Dependencies

- SSID of target
- Software or Hardware access point (we will be using a software ap)

What you will do in this lab:

- Find a victim access point
- Spoof that access point
- Have clients connect to our access point

Lab Part 1 - Setting up an evil twin access point using the madwifi drivers and utilities

- Step 1. To open a command prompt click on the **terminal icon** in the lower left-hand corner. 
- Step 2. We want to get a quick idea of what is happening 'in the air' so that we can properly get people to migrate to our access point. We will set our ath0 interface into monitor mode and then use **airodump-ng** to view who is within range:
ath_mon -script to put our ath0 interface into monitor mode.
airodump-ng ath0 - to view what is happening within range of our interface.

```

ESSID

yourap
Bob's wireless
Cinnamon Altoid
<length: 8>
livingroom1
Apt 305 Secure
Timp207
JC
<length: 8>
jasonj_dsl
jasonj_main
west
Booyaw208
mine
MMM
linksys
MTCLESAP
thrasymachus
Killer Bunny
digis-000
Kfir
<length: 0>
Husky AE
<length: 0>

```

We can easily see any access point within range. We are going to target the SSID *'yourap'*.

- Step 3. Armed with the name of our access point, we want to setup an evil twin ap of the same ssid using the utilities that come standard with the Linux atheros madwifi drivers:

wlanconfig ath0 destroy - this will take the interface down completely.

wlanconfig ath0 create wlandev wifi0 wlanmode ap - this will put our interface into ap mode.

iwconfig ath0 essid 'yourap' - this will assign an ssid to your access point.

iwconfig ath0 channel 6 - set interface to channel 6.

ifconfig ath0 192.168.10.250 netmask 255.255.255.0 -set the ip address and subnet mask of the access point.

ifconfig ath0 up -bring the interface up and start sending beacons.

- Step 4. Using another client and discovery utility (kismet, network stumbler) we should see both SSID's of *'yourap'* on different channels and with different MAC addresses.

- Step 5. Now that your evil twin access point is transmitting its beacons, anybody can see it but there is nothing providing them with DHCP addresses... so let's give them an address we specify using *dnsmasq*.

You will need to edit the `/etc/dnsmasq.conf` file in order to declare the range that you want to assign addresses (this way you can supply addresses in the scope of the legitimate network that they usually

connect to). If you are not worried about giving the victim clients a different address then you can leave the already-added address range of 192.168.10.50-150. Otherwise you will need to edit the following line(s):

At the command prompt type *kate /etc/dnsmasq.conf* and **scroll down** to line number **129** to find the entry `dhcp-range=192.168.10.50,192.168.10.150,12h`. This is where you would **enter a different ip address range**.

For example, if you target network uses the 172.16.x.x network and wanted to give out 50 addresses you could simply change that line to read `dhcp-range=172.16.1.50,172.16.1.100,12h`. **Save the file** and **exit**.

- Step 6. Now you will need to change your ip address to that of the network you changed in the dnsmasq.conf file. **If you didn't change anything you need not do this!**

```
ifconfig ath0 172.16.1.x netmask xxx.xxx.xxx.xxx
```

Type **dnsmasq** at a command prompt to start the server. Now when clients find your ssid they will connect to it and get an ip address. From here you can conduct your LAN attacks against the victim clients that connect.

NOTE: *dnsmasq* allows you to become dns server as well as a dhcp server which means that you control dns requests made by hosts on your network. If you edited the `/etc/dnsmasq.conf` file to reflect any desired changes you could conduct phishing type attacks.

Lab 5.4: Using Linux script to create a fake hotspot

In our previous module we learned how to manually setup an evil twin AP. Now we will use a custom script to do the same thing but throw a fake ‘phishing’ style login page at our victim.

Product Information

Source

HotLabs.org

Custom script created for this class. Feel free to make any changes you wish.

www.hotlabs.org

Where, When, Why

These types of attacks happen every day and most victims have no idea that it has happened. An attacker may take advantage of user’s gullible or naive nature in order to collect passwords and other sensitive information. We will demonstrate, to a point, the effectiveness of this attack but the rest will be up to your own creativity.


Requirements / Dependencies

- Madwifi drivers
- Dnsmasq
- Creativity

What you will do in this lab:

- Setup a fake hotspot
- Have a victim connect
- Obtain their username and password

Lab Part 1 - Using the custom script to create a fake hotspot

- Step 1. To open a command prompt **click** on the **terminal icon** in the lower left-hand corner. 
- Step 2. Type **./8oh2** in order to launch the custom script.

```

80h2eleven Attack
ath0 Mode: Managed          eth1 IP: 192.168.1.100

::::: DISCOVERY OF ACCESS POINTS AND CLIENTS:::::

K - View clients and access points with Kismet
A - View clients and Access points with Airodump

::::: SNIFFING AND CAPTURING DATA ON OPEN WIRELESS NETWORKS ::::::

3 - View traffic of open wireless networks
L - View live network/bandwidth utilization

::::: 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
? - Crack LEAP protocol

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

H - Setup a rouge hotspot
M - Man-in-the-middle attack menu
I - Piggyback a paying customer at a paid hotspot
? - Send beacons for fake hotspots

::::: DENIAL OF SERVICE (DoS) ::::::

D - Deauthenticate a station
? - Deauthenticate all stations on a specific channel (PoC)

Q - Quit

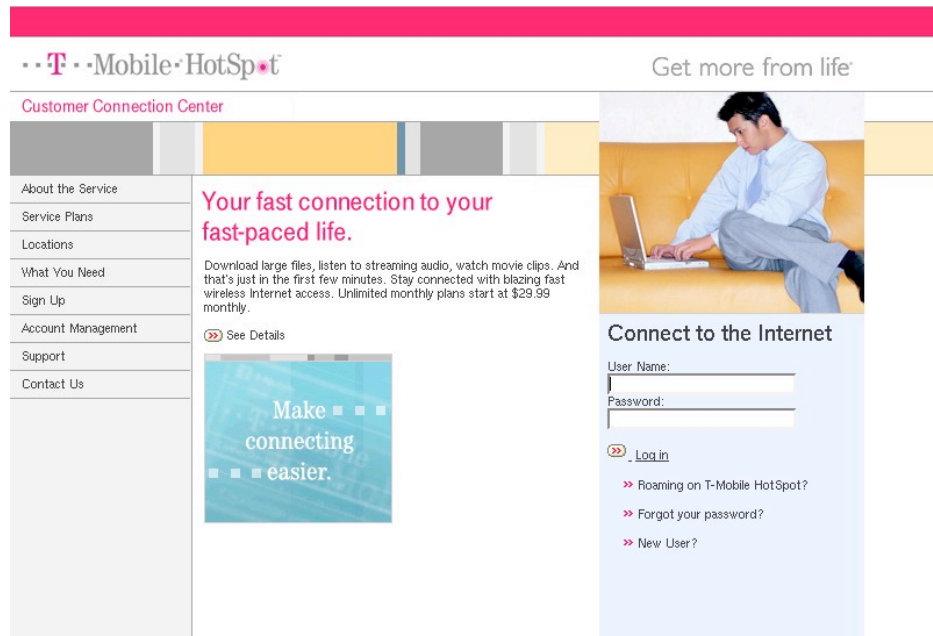
Enter Selection: █

```

- Step 3. From here you simply type **'H'** to select the Hotspot Menu.
- Step 4. Then select **'1 - Turn laptop into a captive portal'** and follow the instructions.
- Step 5. 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 click **enter**.
- Step 6. 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**
- Step 7. Now we will assign the address of the machine/access point so that the clients can appropriately view what is on our web server by answering the next question- What will the access point IP be?
- 172.16.1.9**
- Step 8. 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 9. 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.



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 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 10. By clicking **enter** and the **prompt of the custom script**, you can go back to the hotspot menu and 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 11. 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 5.5: Piggybacking on a captive portal

This is a very common method used to bypass authentication at hotspots that deploy captive portals to control their traffic. Captive portals will let you freely connect to the access point but you are limited to the pages you can view until you supply a username and password and/or pay. These techniques will allow you to quickly bypass such restrictions.

Product Information

Where, When, Why

Sitting in the airport waiting for your flight; all you want to do is check your email and don't want to pay \$19.95 for 5 minutes of internet access. In comes the piggybacking technique...

Usage and Features

- Use otherwise restricted networks for free network access
- Provide a somewhat anonymous method of surfing the net or attack a client

Requirements / Dependencies

- Network card that supports MAC address changing

What you will do in this lab:

- Gather enough information to conduct our piggyback
- Change our network card settings to emulate that of a paid/authenticated user

Lab Part 1 - Setting up for a piggyback

- Step 1. In order for a piggyback to be successful we need some information: *Our IP address, The IP of the access point, the MAC/IP of a privileged user, and it would help to also have the IP of the captive portal default page.*

We can obtain these by the following steps:

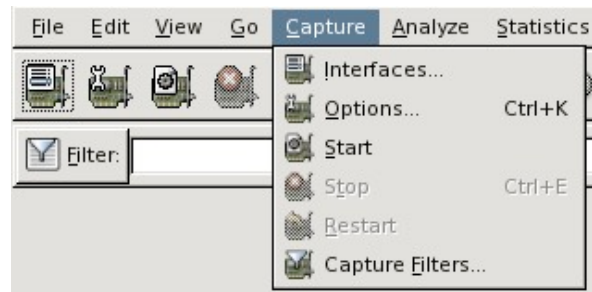
Our IP address: opening up a command prompt and typing ifconfig or ipconfig (depending on your operating system)

IP of access point: when we typed ifconfig/ipconfig we were also given a default gateway; most likely that is your access point IP address.

- Step 2. Now that we have that information we can find hosts that are already connected and passing information to another website other than that of the default captive portal page.

From the command prompt type **wireshark** and **hit enter**.

Once **wireshark** is opened you will need to configure it before you use it. **Select Capture > Interfaces**.

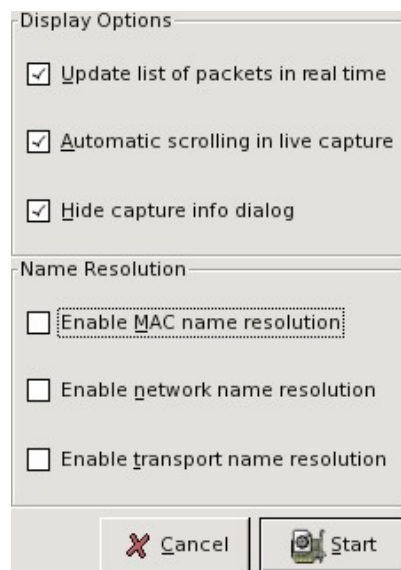


- Step 3. Then you will want to **select the interface** that we will use to view traffic of our target network. In our case it's the **ath0** interface.



- Step 4. It is evident that we have traffic on this network as our packets are increasing. **Select Options** to configure the interface.

The changes we will make will allow us to see the traffic in real-time so that we can view who is privileged and who is stuck at the captive-portal page. **Simply put the check mark in all the boxes under display options and remove all the checks from the Name Resolution section and hit Start.**



- Step 5. The next step is to analyze traffic to the captive-portal page and take note of its IP address (which you could do by simply watching yourself browse the captive portal page). Now *any* traffic is *not* destined to that address is a possible user worth piggybacking so search for that type of traffic.

NOTE: As soon as I hit start I saw this traffic in wireshark which means I already know that a user is freely roaming the internet and using services that would otherwise be restricted unless a correct username and password were supplied at the captive portal page. A user is using AOL instant messenger and this is a notification that a buddy has logged onto AOL ready to chat. This could be a potential user to piggyback in order to get free internet.

Source	Destination	Protocol	Info
Cisco-Li_25:15:5c	Ubiquiti_53:c5:56	MDS Header	[Malformed Packet]
Cisco-Li_25:15:5c	IntelCor_13:f1:ed	MDS Header	[Malformed Packet]
64.12.165.97	192.168.73.107	TCP	aol > 2620 [ACK] Seq
205.188.7.217	192.168.73.107	AIM Buddylist	Oncoming Buddy: Grk
205.188.7.217	192.168.73.107	AIM Buddylist	Oncoming Buddy: Grk

- Step 6. You want the source to be part of your local network and the destination will be anything except the captive-portal page. For example if a user wants to browse to google and has not logged into the portal then they will be stuck at the same page you browsed. However, if they browse to google and they are logged in then they will be brought to the actual google page which will show up destined to an address such as 64.233.187.99.

Once you have found a client that is freely browsing then all that is left to do it to assume their identity. We need their MAC address as most captive portals base their filtering on MAC addresses we just need to take on a MAC that the captive portals access control list already has already granted rights to browse past the captive portal. We can obtain the MAC by 1 of 2 methods.

1. Look inside wireshark to find the layer 2 (Link layer) information. Select the packet of the privileged user and collapse the Ethernet II field and look for the Source. Take note of the MAC

165	450.620947	192.168.73.1	192.168.73.107	TCP	2869 > 1027 [A
166	450.622528	192.168.73.1	192.168.73.107	TCP	2869 > 1027 [P
167	450.622703	192.168.73.1	192.168.73.107	TCP	2869 > 1027 [F

▶	Frame 165 (54 bytes on wire, 54 bytes captured)
▼	Ethernet II, Src: Cisco-Li_25:15:5a (00:16:b6:25:15:5a), Dst: IntelCor_13:f1:ed (00:13:ce:13:f1:ed)
▶	Destination: IntelCor_13:f1:ed (00:13:ce:13:f1:ed)
▶	Source: Cisco-Li_25:15:5a (00:16:b6:25:15:5a)

2. Ping the IP address and look in our arp table to find the layer 2 information. From a command prompt type **ping <ip.address>** and then type **arp -a** and take note of the MAC that is associated with the IP of the privileged user.

- Step 7. Once the MAC address is obtained we can change our interface to reflect that of the privileged user.

From a command prompt type the following commands:

ifconfig eth1 down - to take our interface down for configuration

ifconfig eth1 hw ether mac:goes:here up - to assign our interface the obtained MAC and then bring it back up for use

dhcpcd eth1 - to get the same IP of the privileged user

NOTE: you can save yourself the trouble of getting a DHCP assigned address by statically configuring your card to take on the IP of the privileged user with the following commands:

ifconfig eth1 down

ifconfig eth1 ip.goes.here netmask net.mask.goes.here hw ether mac:goes:here up

Now you are free to use the internet!

What you learned in this Lab:

In this Lab you learned:

- How to piggyback a privileged user on a captive portal

Lab Part 2 - Using alternative methods to bypass authentication on a captive portal

What you will do in this lab:

- Get familiar with other tools to help aid in bypassing authentication on a captive portal
-

Due to the nature of captive portals, and the way they handle filtering, it is possible to bypass authentication even if there is nobody to piggyback. You may have noticed that even though all your attempts to browse to a website result in the display of the default captive portal page, you are still able to ping outside to the internet which means ICMP traffic freely leaves the network. With a little forethought and preparation you can easily use any captive portal to browse the internet for free.

ICMPTX found at <http://thomer.com/icmptx/> can setup an ICMP tunnel between your computer on the captive portal network and a computer sitting somewhere accessible on the internet listening for your ICMP packets that contain your desired webpage. The proxy is obviously setup before hand and always listening 'just in case'. Tunneling methods obviously do not require any interaction with any other user on the network and/or piggybacking a privileged user.

NOTE: Author Siim Pader describes his adventures with tunneling on a captive portal at this website:
http://www.linuxexposed.com/index.php?option=com_content&task=view&id=153&Itemid=1

Another alternative is to just use *wireshark* to sniff someone logging into a captive portal and use their credentials.

Lab 5.6: Ethernet Over Power - Demo



Your instructor will be doing this Demonstration using Netgear equipment, but there are other brands of like equipment you could use in a Penetration Test.

The WGXB102 54 Mbps Wall-Plugged Wireless Range Extender Kit has two pieces of equipment, the XE102 Wall-Plugged Ethernet Bridge and WGX102 Wall-Plugged Wireless Access Point, allowing your wireless network to originate from any point in your home.

With the WGX102, the wireless network can originate at any point of your choosing, with no visible wires and no desk or floor space consumed, allowing it to blend into your target's environment.

Product Information

Where, When, Why

This technique is used to show the vulnerability of a client's network to a new form of Rogue Access Point.

The first half of the Wireless Range Extender is an Ethernet Over Power Bridge. This connects from an RJ45 Ethernet jack, and plugs into the building's 110v power system.

The second end of this matched pair is an Access Point (the other end of the Ethernet Bridge) that also plugs into the building's 110v power system.

The Ethernet signal leaves the jack, is converted to run over 110v, and then at the AP is returned to Ethernet and 'shared' over RF as 802.11 packets. Easily transmitted unsuspected to a 'Rogue' outside your building. Thus giving the hacker access directly onto your inside wired network.

Usage and Features

- Bridges an inside Ethernet connection - inside your corporate firewall - out via 802.11 wireless packets.
- Runs over simple building 110v wiring.
- Inexpensive enough to 'leave behind' after an attack.

Requirements / Dependencies

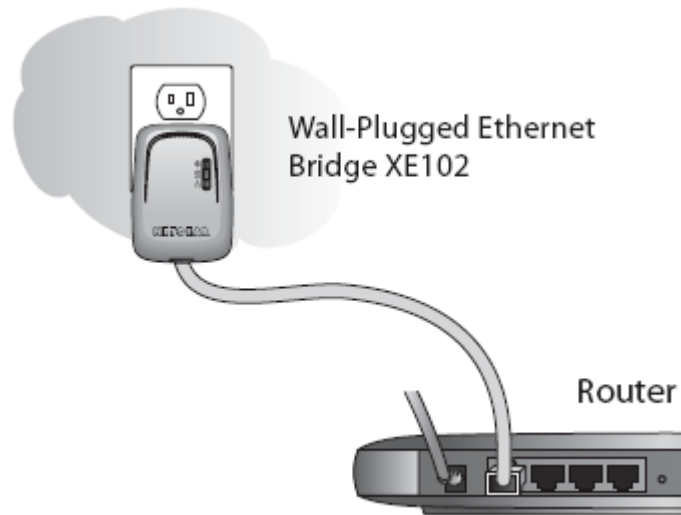
- Physical Access to the inside corporate network jack. Perhaps only 5 seconds needed to jack into an RJ-45 and then plug into the buildings wiring.

What you will do in this Demonstration:

- See how easy it is to setup and use a Ethernet Over Power Rogue Access Point.

You'll need to have the two parts of the Ethernet Over Power devices as well as a short Cat-5 cable.

- Step 8. Plug the Ethernet Bridge side into the wall, and connect the Cat-5 cable to a LAN port.



- Step 9. Somewhere else in your building, plug the Access Point device into the wall. Preferably close to an outside wall, so the 'Hacker' can easily see the Access Point's RF signal.
- Step 10. Hacker connects to the AP, the AP converts the 802.11 to Ethernet Over Power, transfers the packets via the 110v power lines to the Ethernet Bridge. The Ethernet Bridge converts the Ethernet Over Power signals into standard Ethernet and places the packets over the Cat-5 cable to the Ethernet port.
- Step 11.

NOTE: To be really devious, you would pre-set the Access Point to the SSID of the target client.

NOTE: You might also want to add pre-printed labels on the front of the devices with something like, "Facilities - DO NOT REMOVE" to increase the chances that your equipment stays online as long as possible.

- Step 12. With Netgear devices you cannot change the MAC address of the AP, but with other types of Ethernet Over Power have that ability to Hide the MAC address as one of the existing 'real' corporate Access Points.