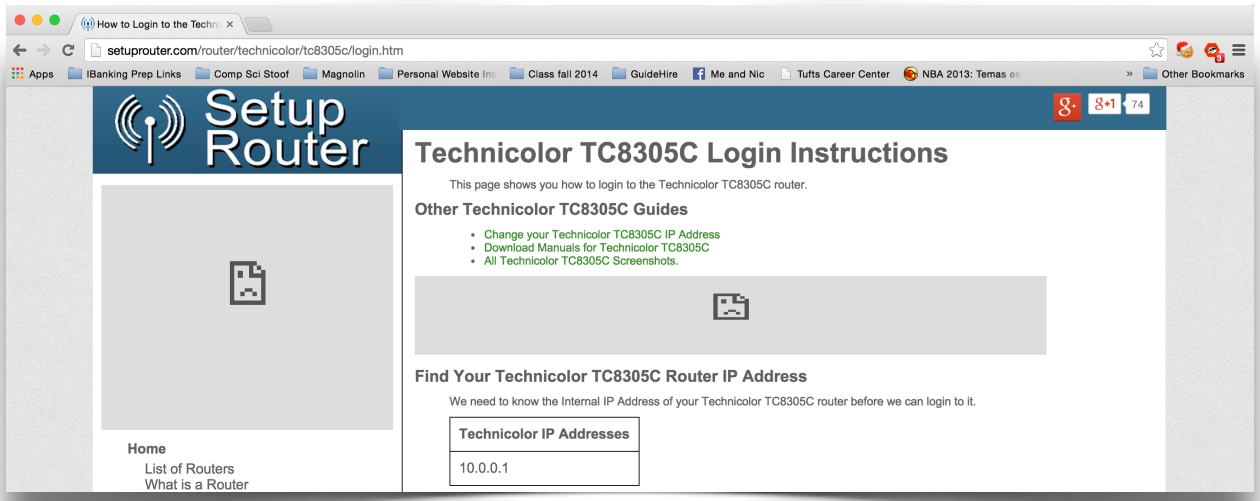
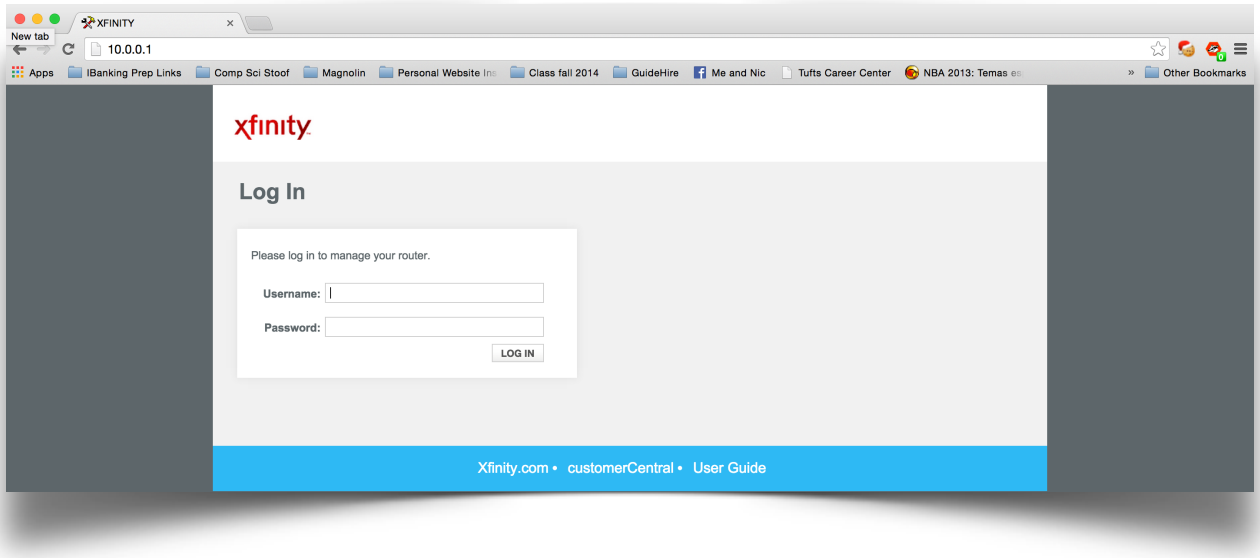
For my supporting material I decided to try to hack into my home router. My home router was brought by my roommate who set everything up and I had little knowledge about it's set up aside from the WiFi password, the network name and the internet provider, XFinity.

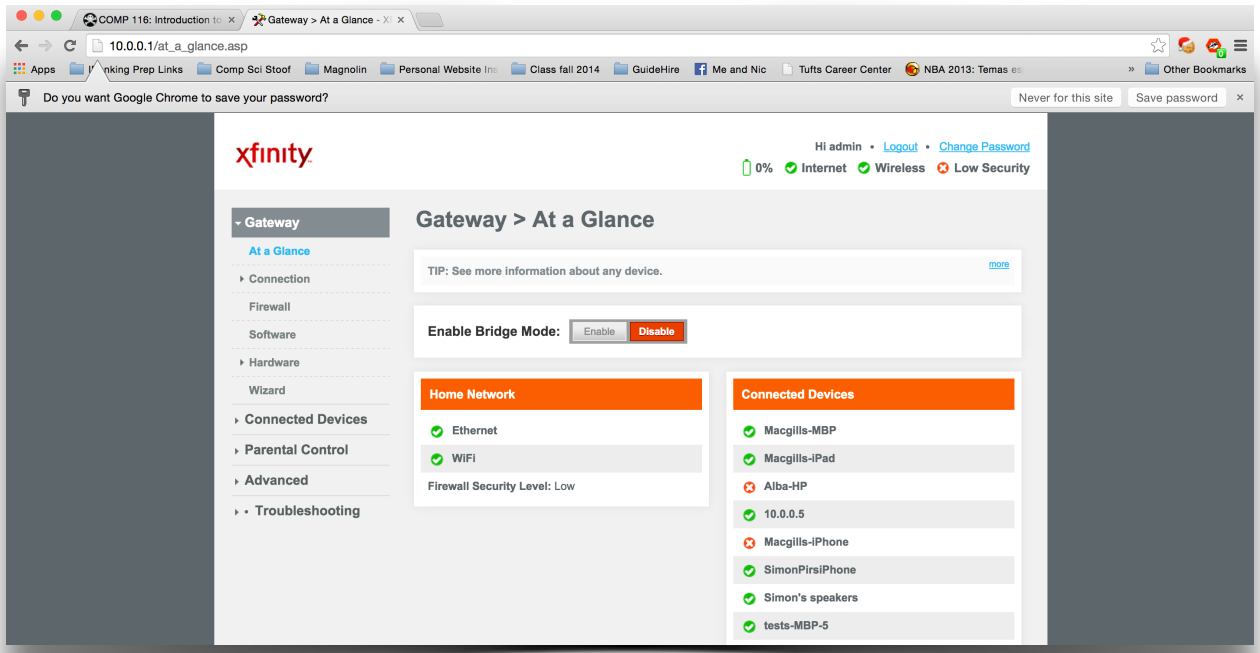
1. The first thing I did was check the model of the router. It was a **Technicolor TC8395C**.
2. I then googled the make to see what came up. The first link showed me the IP Address of the server.



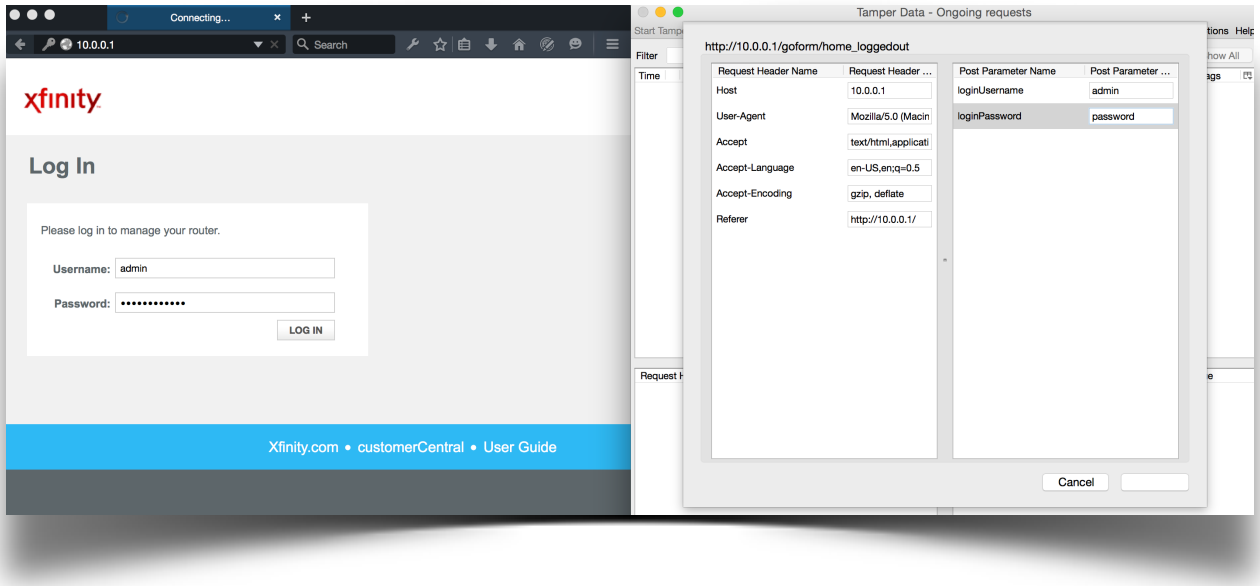
3. I then navigated to that ip address and a login screen appeared.

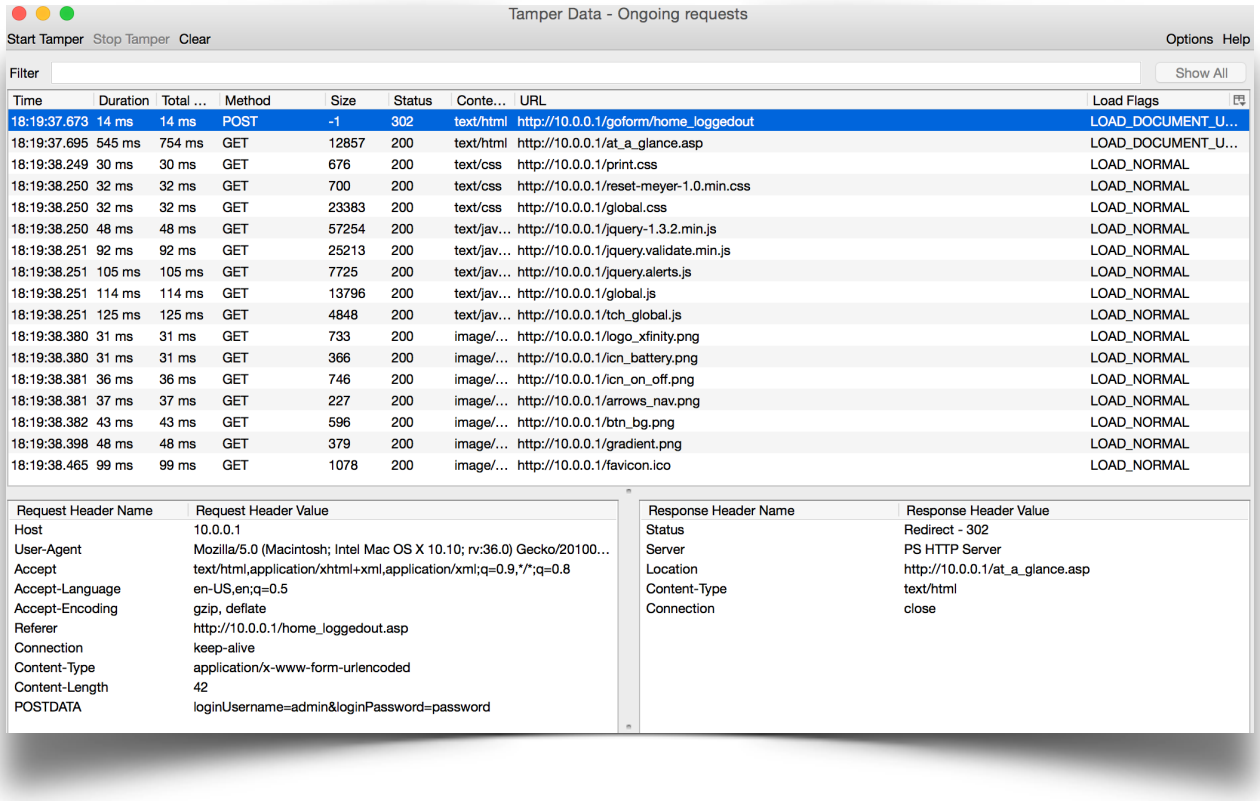


4. Before I even googled what the default password and username were for **Technicolor TC8395C** routers I just guessed ‘admin’ and ‘password’ and I gained access.



5. I also noticed that the username and password were not encrypted. You can see that they are “loginUsername” and “loginPassword” in the POST data.

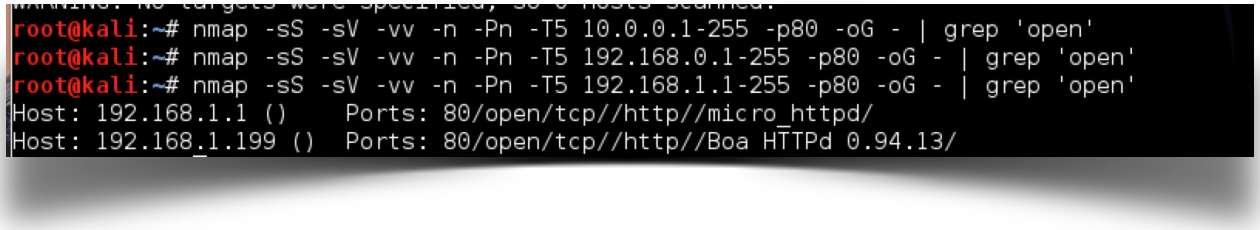



Tamper Data - Ongoing requests
Start Tamper
Stop Tamper
Clear
Options
Help
Filter
Show All
Time Duration Total … Method Size Status Conte… URL Load Flags
18:19:37.673 14 ms 14 ms POST -1 302 text/html http://10.0.0.1/goform/home_loggedout LOAD_DOCUMENT_U…
18:19:37.695 545 ms 754 ms GET 12857 200 text/html http://10.0.0.1/at_a_glance.asp LOAD_DOCUMENT_U…
18:19:38.249 30 ms 30 ms GET 676 200 text/css http://10.0.0.1/print.css LOAD_NORMAL
18:19:38.250 32 ms 32 ms GET 700 200 text/css http://10.0.0.1/reset-meyer-1.0.min.css LOAD_NORMAL
18:19:38.250 32 ms 32 ms GET 23383 200 text/css http://10.0.0.1/global.css LOAD_NORMAL
18:19:38.250 48 ms 48 ms GET 57254 200 text/jav… http://10.0.0.1/jquery-1.3.2.min.js LOAD_NORMAL
18:19:38.251 92 ms 92 ms GET 25213 200 text/jav… http://10.0.0.1/jquery.validate.min.js LOAD_NORMAL
18:19:38.251 105 ms 105 ms GET 7725 200 text/jav… http://10.0.0.1/jquery.alerts.js LOAD_NORMAL
18:19:38.251 114 ms 114 ms GET 13796 200 text/jav… http://10.0.0.1/global.js LOAD_NORMAL
18:19:38.251 125 ms 125 ms GET 4848 200 text/jav… http://10.0.0.1/tch_global.js LOAD_NORMAL
18:19:38.380 31 ms 31 ms GET 733 200 image/… http://10.0.0.1/logo_xfinity.png LOAD_NORMAL
18:19:38.380 31 ms 31 ms GET 366 200 image/… http://10.0.0.1/icn_battery.png LOAD_NORMAL
18:19:38.381 36 ms 36 ms GET 746 200 image/… http://10.0.0.1/icn_on_off.png LOAD_NORMAL
18:19:38.381 37 ms 37 ms GET 227 200 image/… http://10.0.0.1/arrows_nav.png LOAD_NORMAL
18:19:38.382 43 ms 43 ms GET 596 200 image/… http://10.0.0.1/btn_bg.png LOAD_NORMAL
18:19:38.398 48 ms 48 ms GET 379 200 image/… http://10.0.0.1/gradient.png LOAD_NORMAL
18:19:38.465 99 ms 99 ms GET 1078 200 image/… http://10.0.0.1/favicon.ico LOAD_NORMAL
Request Header Name
Request Header Value
Host 10.0.0.1
User-Agent Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:36.0) Gecko/20100…
Accept text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language en-US,en;q=0.5
Accept-Encoding gzip, deflate
Referer http://10.0.0.1/home_loggedout.asp
Connection keep-alive
Content-Type application/x-www-form-urlencoded
Content-Length 42
POSTDATA loginUsername=admin&loginPassword=password
Response Header Name
Response Header Value
Status Redirect - 302
Server PS HTTP Server
Location http://10.0.0.1/at_a_glance.asp
Content-Type text/html
Connection close

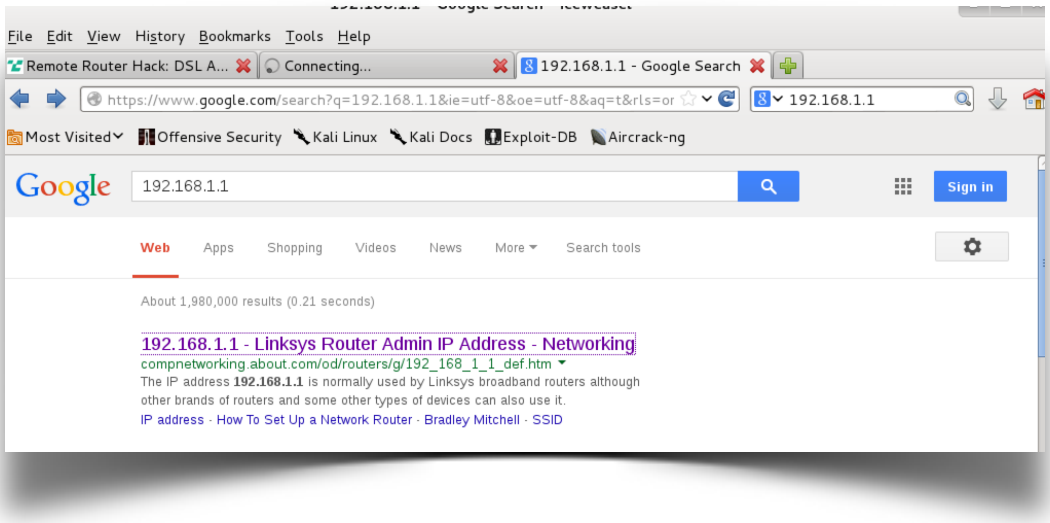
Because hacking my own router was too easy, I decided to try to hack into the router of my favorite coffee shop, Darwin's, on Mass. Avenue in Central Square.

1. I went to the local coffee shop, *Darwin's* on Massachusetts Avenue with my computer and I connected to their WiFi network "D3" with the password they gave me at the register.

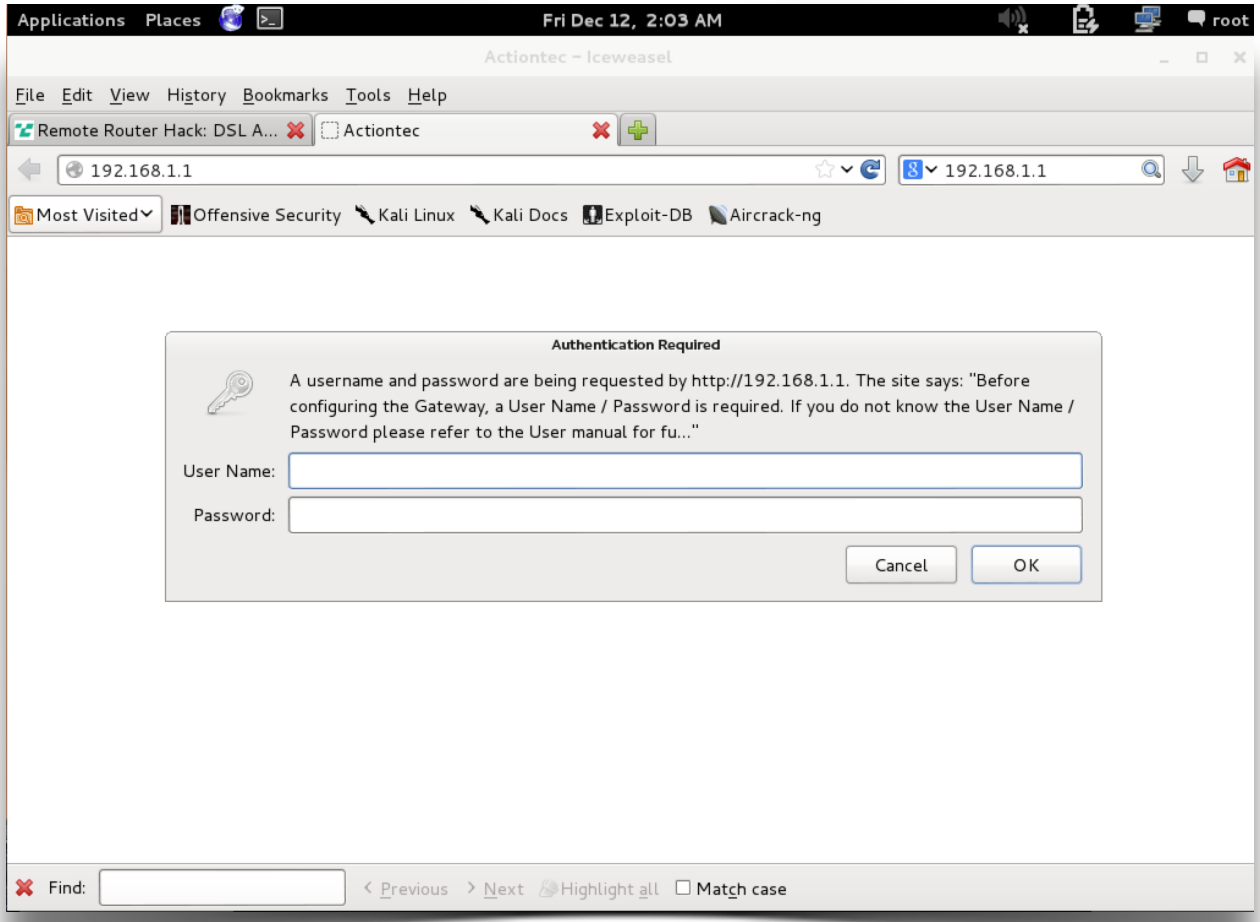
2. After connecting I google common default server ip addresses and I ran an nmap scan to see if I could find any on the network. I only looked for port 80 because if the web interface for routers is almost always on port 80, the HTTP port.



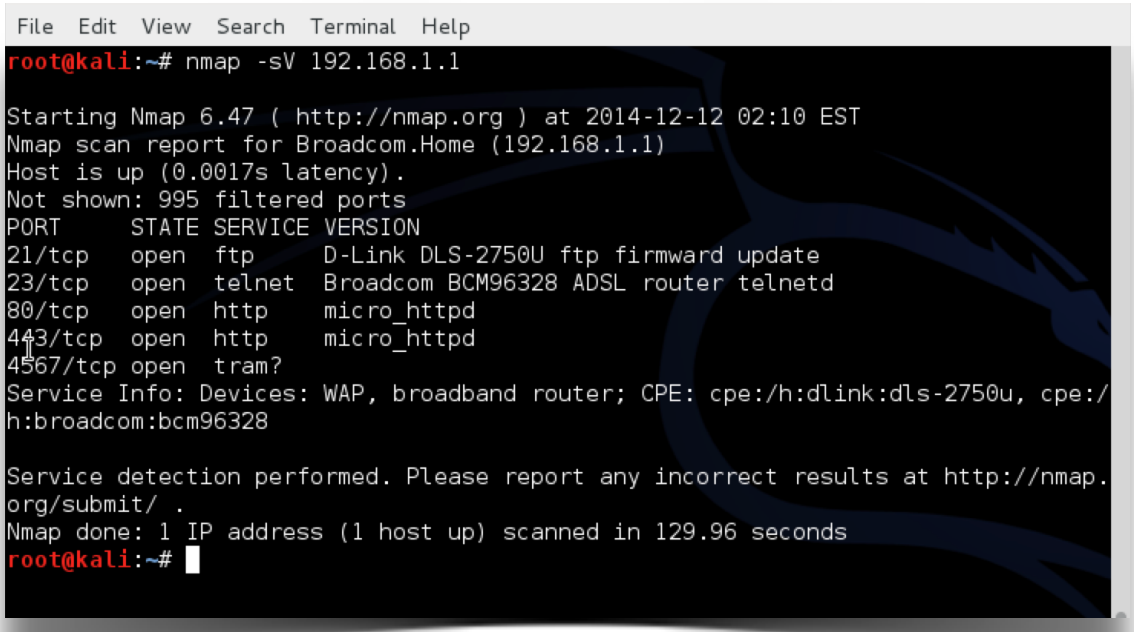
3. As you can see on my last nmap on ip addresses 192.168.1.1 to 192.168.1.255 I found that at the ip addresses 192.168.1.1 and 192.168.1.199 had open port 80s. After a quick google search I found out that port 192.168.1.1 is associated with linksys routers.



4. I navigated to ip address 192.168.1.1 and immediately came upon a login page. As you can see below this is clearly a router because it says “Before configuring the Gateway…”



5. I did another quick nmap scan on the ip address to see what other ports were open and to see if I could gather any other information on the router. Immediately I figured out it was the D-Link DLS-2750U router running Broadcom ADSL software. You can see below under version. I also saw that 5 ports were open.



6. I google for the default passwords for the D-Link DLS-2750U and found them to be ‘admin’ and ‘admin.’

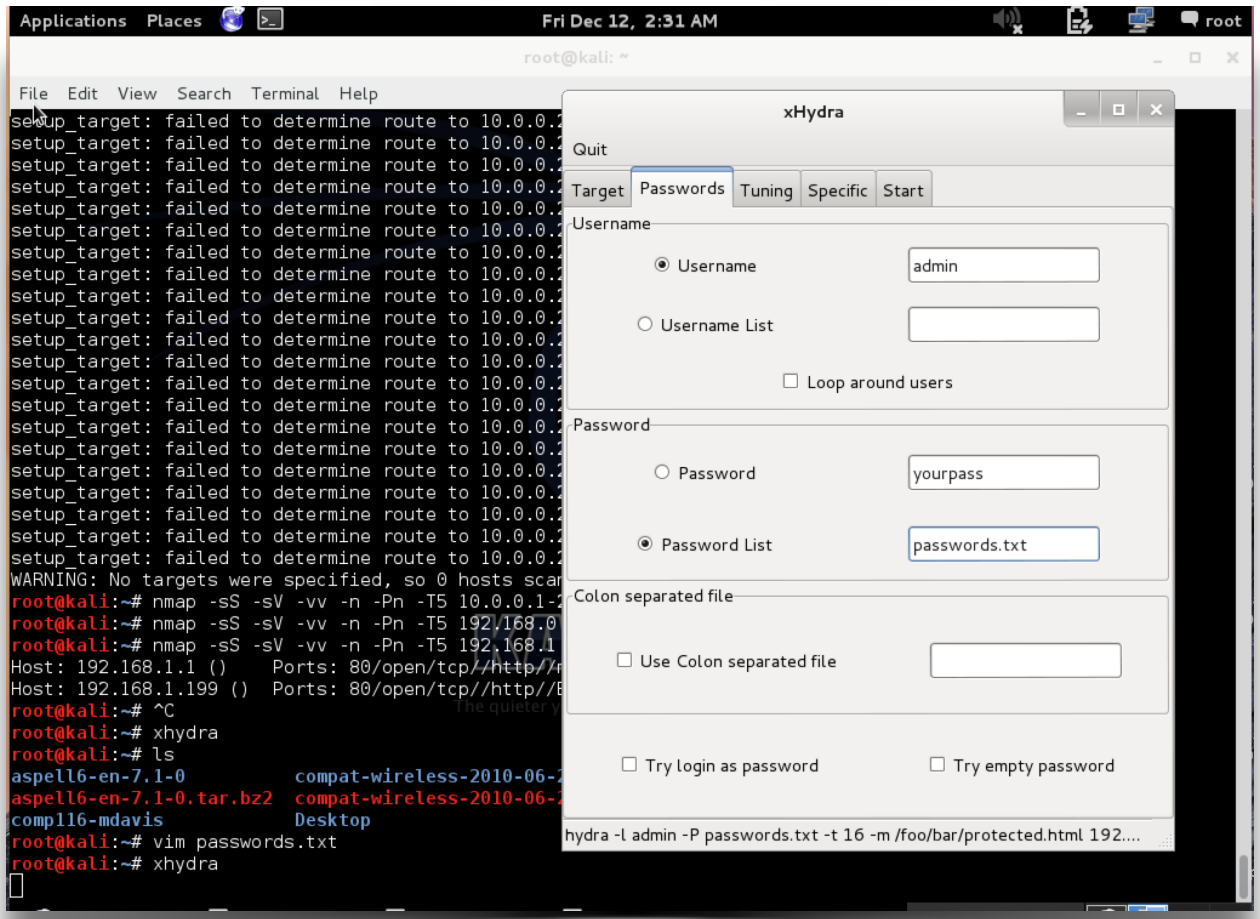
Dlink DSL-2750U-Etisalat Default Username and Password

You need to know the username and password to login to your Dlink DSL-2750U-Etisalat. All of the default usernames and passwords for the Dlink DSL-2750U-Etisalat are listed below.

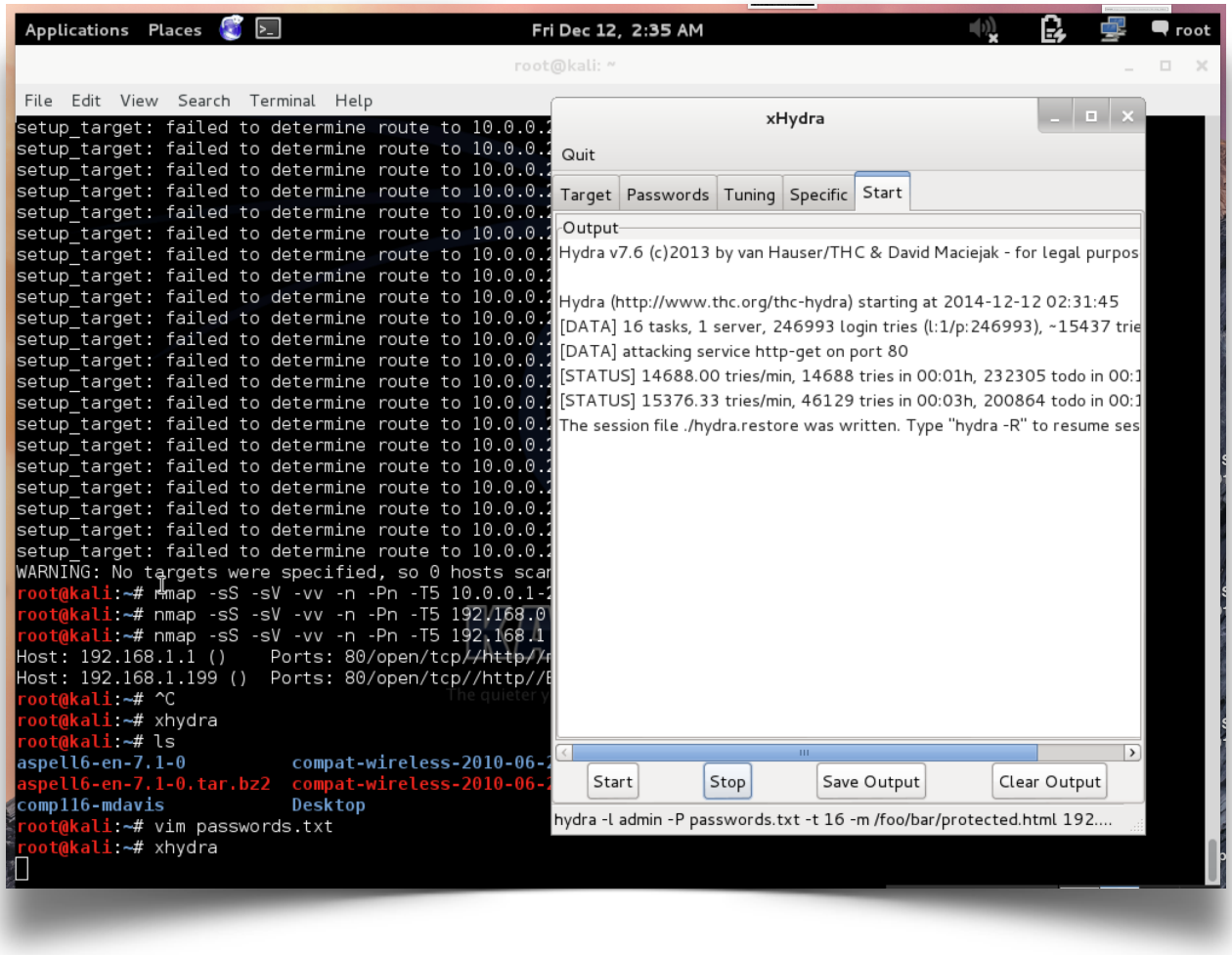
Dlink Usernames	Dlink Passwords
admin	admin

Enter your username and password in the dialog box that pops up. It looks like this:

7. Unfortunately ‘admin’ and ‘admin’ did not work meaning that someone had changed the password and potentially the username as well. I decided to try running a program on Kali Linux called XHydra. I passed it a standard wordlist for passwords and with the username ‘admin.’ I targeted 192.68.1.1 at port 80.



8. I let XHydra run for about 3 minutes before quitting. I did want to completely hack the router but I wanted to show that anyone could easily brute-force the password and username as there was not limit to login attempts. In fact, in about 3 minutes, XHydra attempted 46,129 password combinations with the username ‘admin.’



Conclusion: Had I truly been determined I could have let XHyrda run for a few hours while I had coffee and most likely brute-forced my way into the Darwin’s router. Hundreds of people connect to Darwin’s WiFi every week and I would have gained access to all of their web data. Additionally, I most likely would have gained access to the internal workings of Darwin’s coffee shop with a little maneuvering. I hope this shows the importance of router security and the potential risks associated with bad router defense.