**Assignment #3: Using ARP Poisoning to sniff out Usernames and Passwords form HTTP Sites DUE: February 25, 2020**

**IMPORTANT NOTE:**

**\*\* DO NOT perform this experiment on the GSU network. You can either do it on your own Network at home or go to Langdale room 876 during TA’s Office Hours to do it there. \*\***

ASSIGNMENT DELIVERABLES:

* Screenshot of the Virtual Machine running
* Screenshot of Ettercap running
* Screenshot of Ettercap capturing login credentials
* In one paragraph (200 -300 words) describe what ARP Poisoning is and how it works.
* Submit a single file with all the screen shots labeled and the paragraph summary.
* Submit file as “FirstName\_LastName.docx”

**Instructions:**

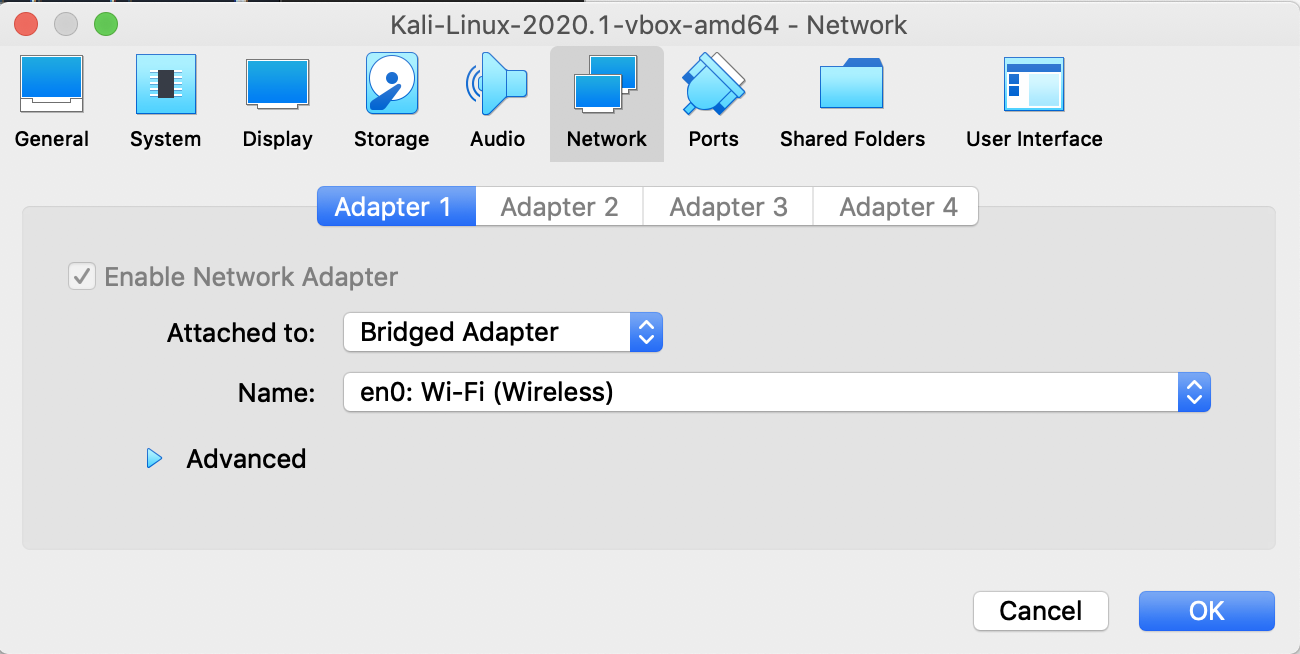
1. Download and Install Oracle VirtualBox for your specific OS from the following website:

<https://www.virtualbox.org/wiki/Downloads>

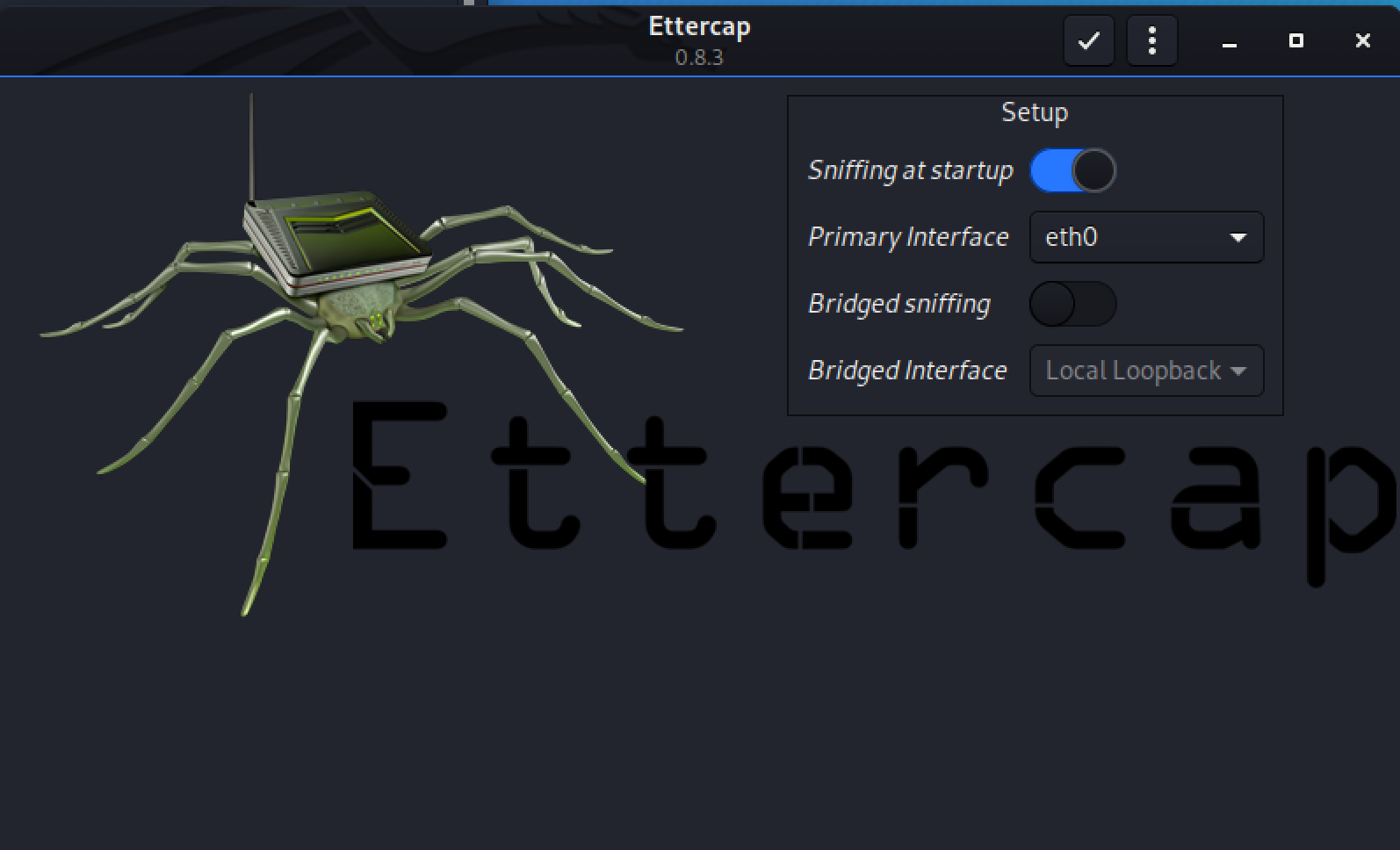
1. Download and the Kali Linux image for VirtualBox from the following website:

<https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/#1572305786515-43ed3ee1-b9c8>

1. Startup VirtualBox and click file from the menu bar and hit “Import Appliance”
2. Load the Kali Linux image
3. Go to Settings in VirtualBox and under Network Settings, select Bridged Adapter like so:



1. Then press the start icon on the VirtualBox page.
2. The default username and password are “kali” and “kali”
3. In order to get the latest packages do the following in the terminal of the Kali Linux OS in the following order:
   1. sudo apt-get update
   2. sudo apt-get upgrade -y
   3. sudo apt-get dist-upgrade -y
   4. sudo apt-get install ettercap-graphical
4. Next open type in the command “ip a” and under the section “eth0” look for the IP address following the word inet. This IP address is your Virtual Machine’s IP address on your LAN connection.
5. Next, switch over to your physical computer and open your terminal and find its IP address on your LAN. Take note of this IP address.
6. Next, while still on your physical computer’s terminal, type in the command “netstat -rn” and under the section heading of “Internet:” look for destination of default. The gateway associated with that contains the IP address of your router. Take note of this IP address.
7. Once the above commands are done, enter the following command in the Kali Linux OS terminal:
   1. sudo “ettercap -G”
8. You should see this screen now with the selected options for Setup:



1. At this point, click the check mark button on the menu bar of Ettercap. You should see the following screen:



1. Now hit the green circled icon first and then the red circled icon. This will show you a list of connected hosts on your LAN.



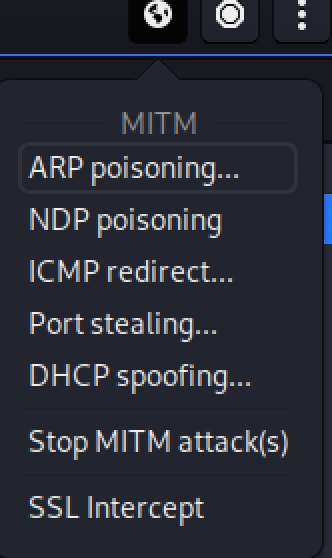


1. Click the IP address corresponding to your physical computer and hit the “Add to Target 1” button.
2. Click the IP address corresponding to your router address and hit the “Add to Target 2” button.
3. Next hit the following button:

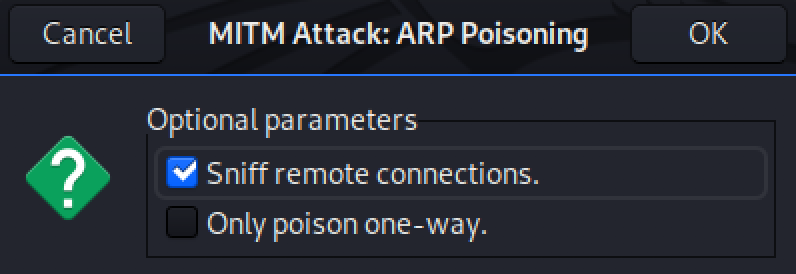




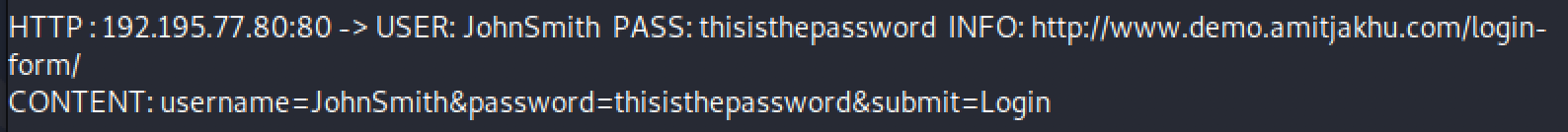
1. Next go to the heading called ARP poisoning as shown below:



1. Make sure your settings are the same as below and then press “OK”:



1. Since Ettercap is not able to sniff out HTTPS messages, we will use an HTTP site.
2. Go to the following site on your physical machine and type in a random username and password of your choosing and hit submit
   1. <http://www.demo.amitjakhu.com/login-form/>
   2. NOTE: You must do step 20 before doing step 22
3. Once you have submitted the login credentials go to Ettercap on your virtual machine and notice in the Ettercap window that it caught both your username and password.



1. That’s it. Go ahead and close the Ettercap window and then shutdown your Virtual Machine.