Lab 7

Password Cracking and Network Poisoning

Shrutika Joshi

University of Maryland Baltimore County

Presented To – Ian Coston

Date – 19th OCT 2023

Introduction

In this lab, you are going to crack Windows passwords using weak NTLM hashing, crack website passwords that use basic authentication, and poison a network via ARP poisoning.

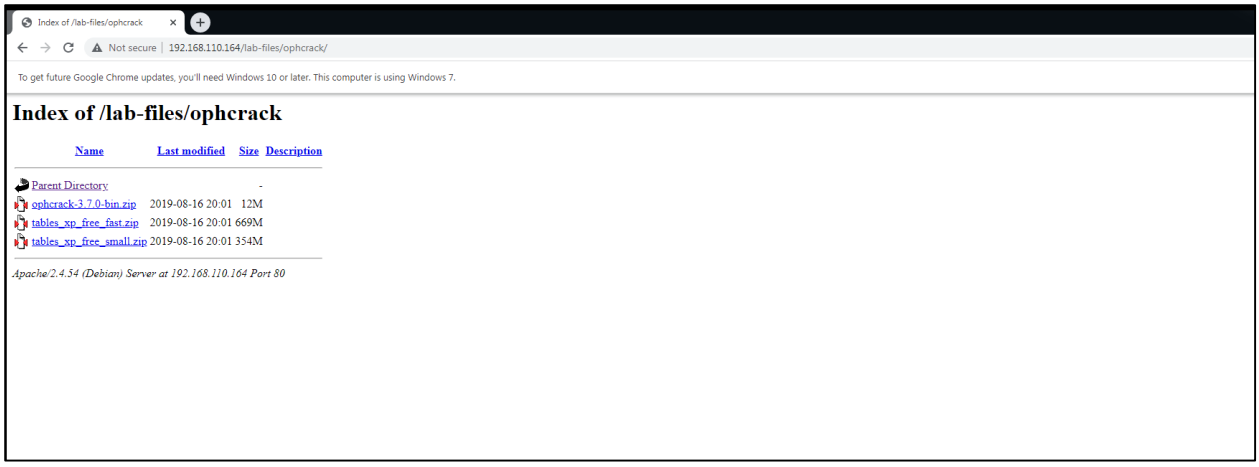
Pre-Lab

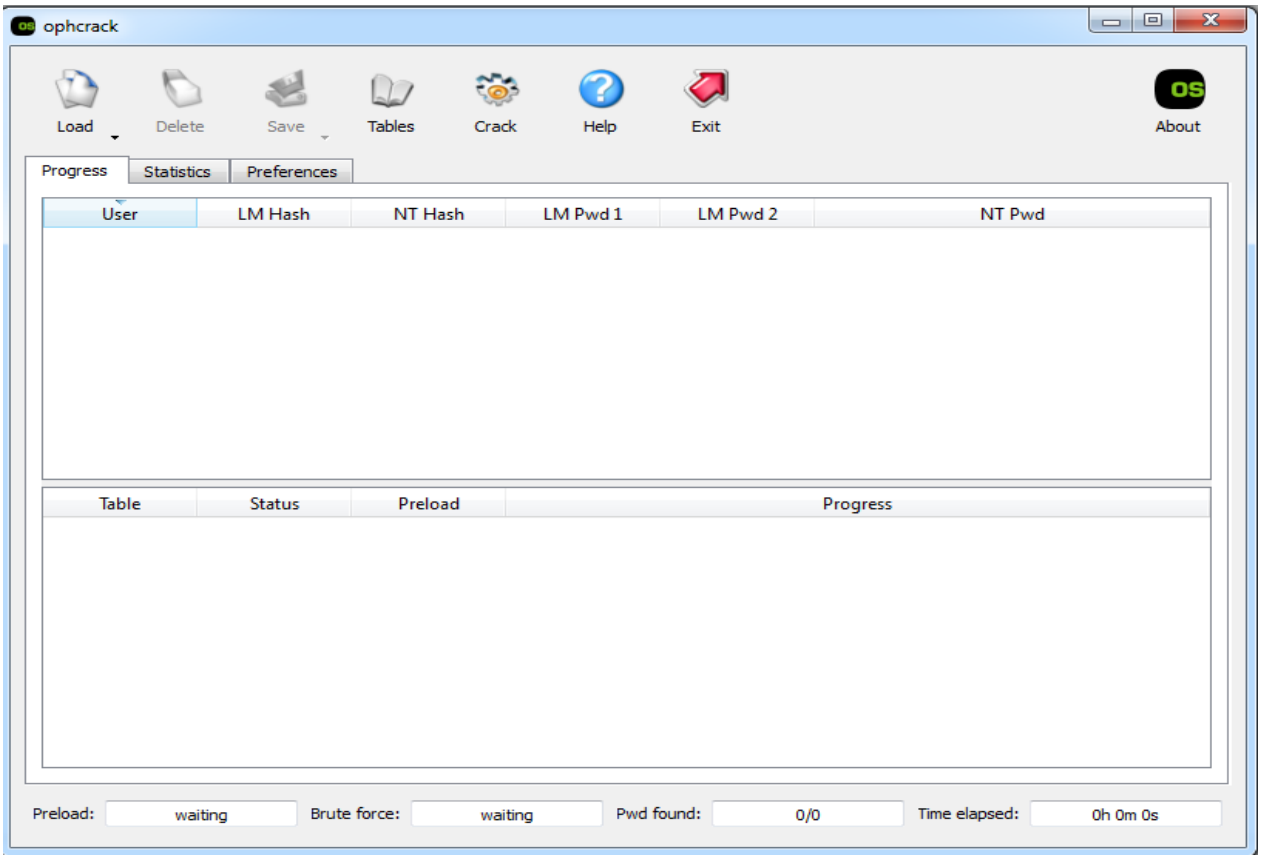
For this lab, you will require Kali Linux and Windows XP and Windows 7 machines,

Practical

1. Password Cracking on a Windows XP system

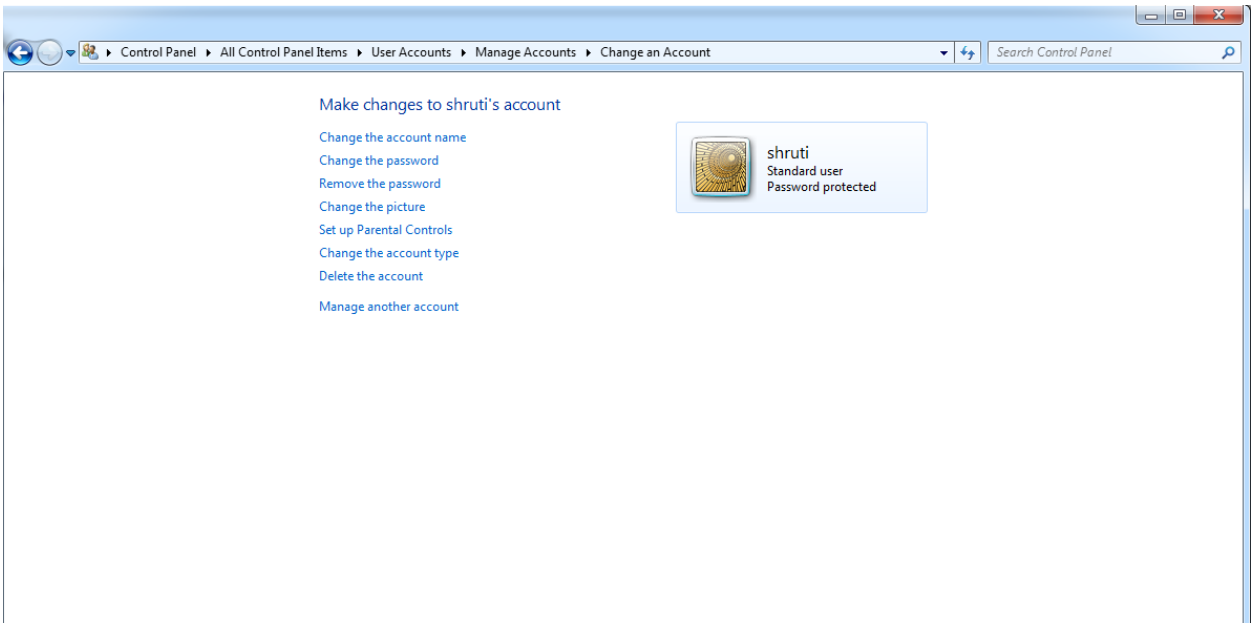
Inside of your Windows XP VM, download the 0phcrack utility and the tables from your Kali VM's website by browsing to http://[Kali IP address] (ophcrack directory). Once downloaded, unzip all files including the table zips. To run Ophcrack, browse into the ophcrack directory/x86/ and doubleclick the ophcrack.exe file.



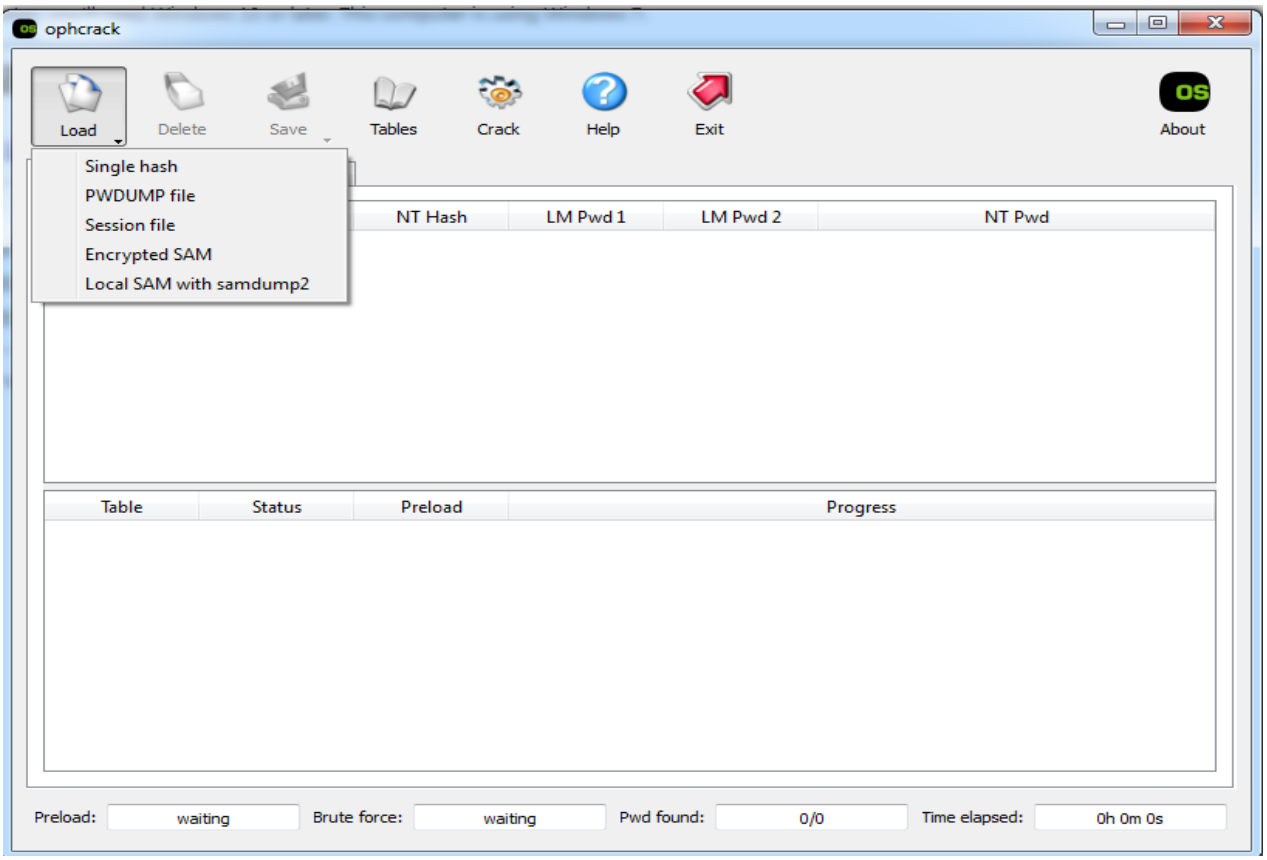


After ensuring Ophcrack loads, create a local Windows user with the password of

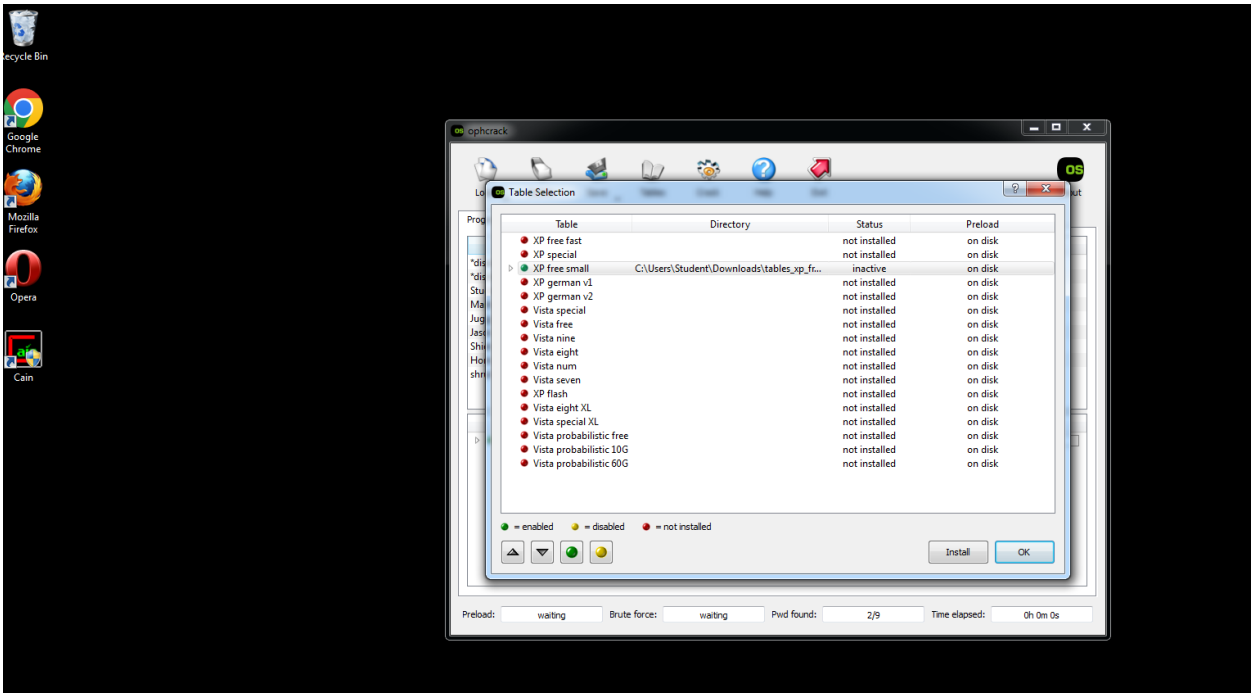
“Password1234” (Go to Start-> Control Panel -> user accounts)



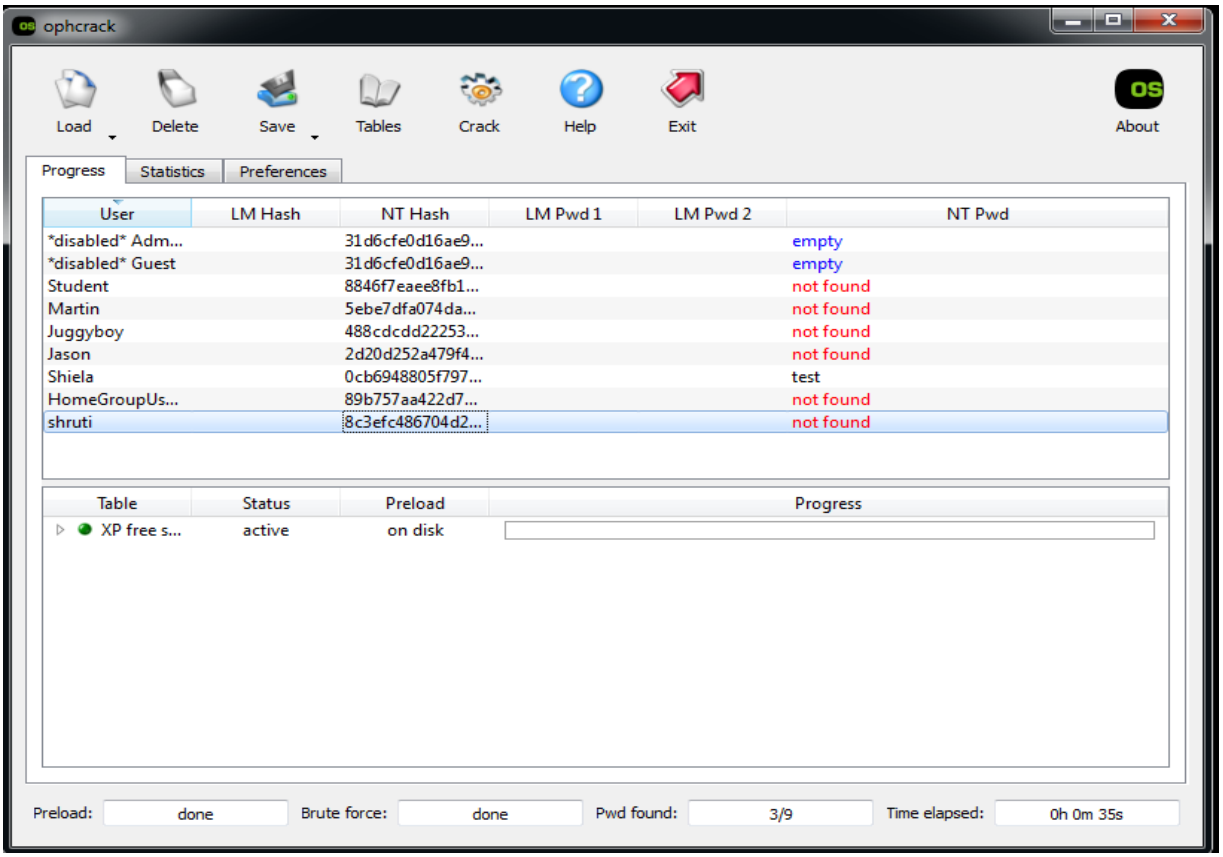
Inside of Ophcrack, select "Load" then "Local SAM with samdump2". This will load in the local SAM file of the workstation you are currently on.



Next Go to the "Tables" icon and ensure that XP free small is enabled (there is a green dot by it). If it is not then hit the Install icon and browse to the location of the unzipped tables file you downloaded.



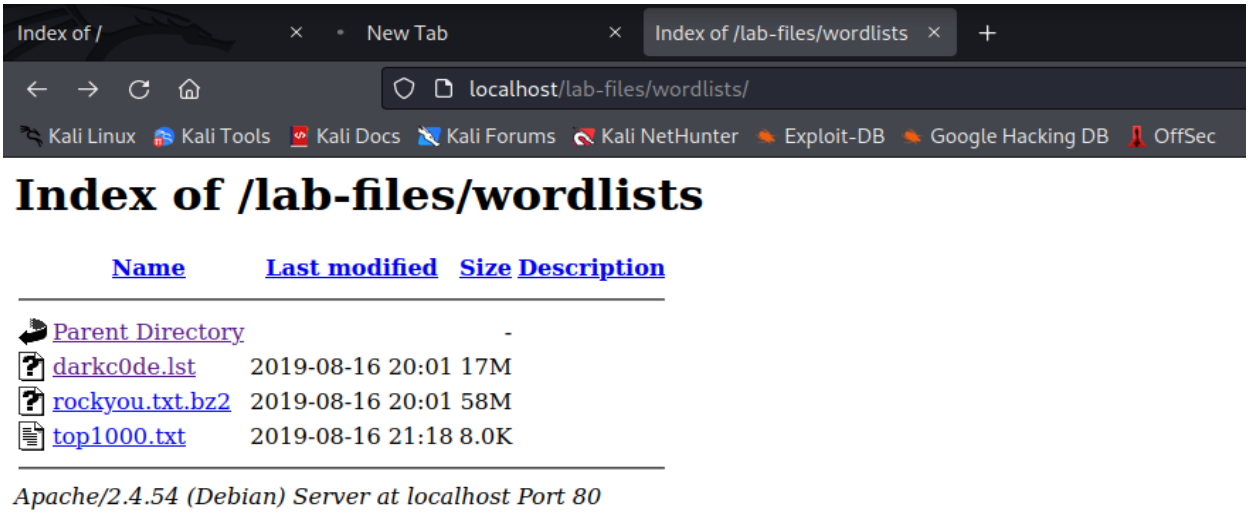
Go back to the Main screen and look at the users passwords that you are trying to crack. Ophcrack will attempt to crack all of the passwords on this list. Press the crack button.



2. Password Cracking a website

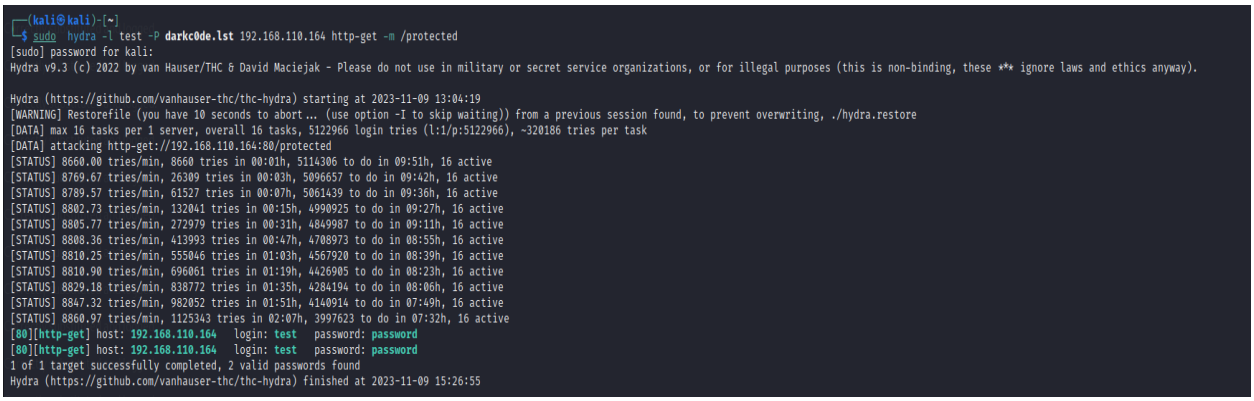
In Kali open up firefox and go to the site http://localhost/protected/. If the web browser prompts about a problem with the certificate click “Continue”.

Download the darkc0de.lst wordlist from your Kali Webserver by navigating to http://localhost/lab-files/wordlists. Save the file in a directory of your choosing, such as Desktop or Downloads.



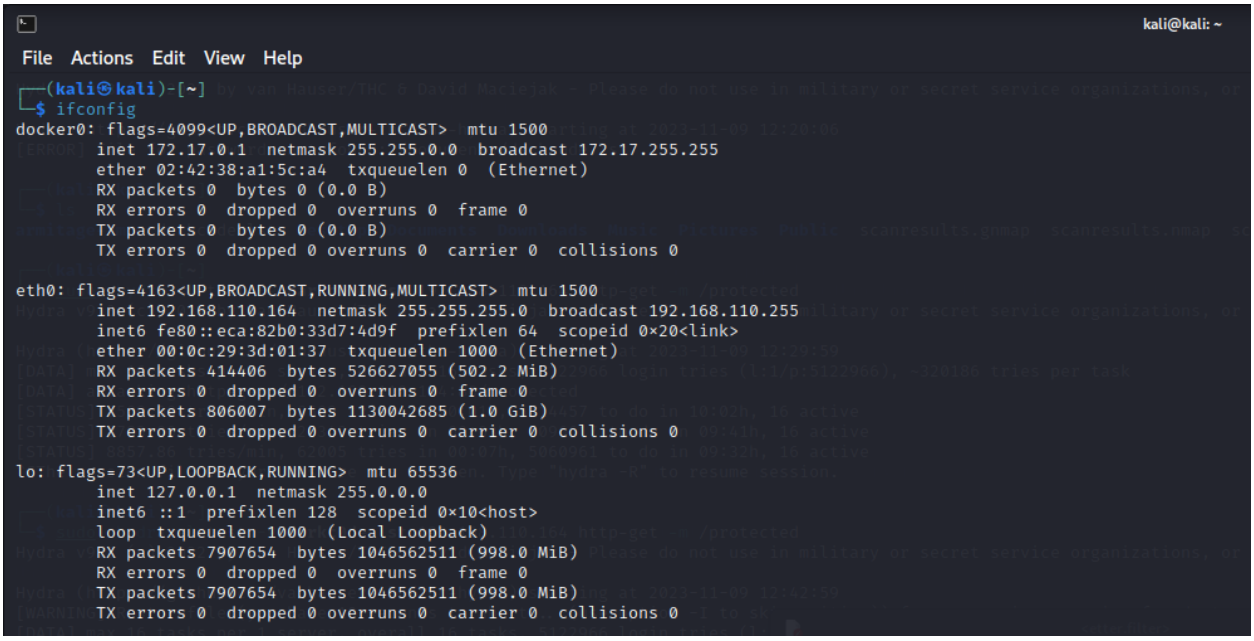
From the terminal, run the following command which will launch an attack against the web server to brute force the password:

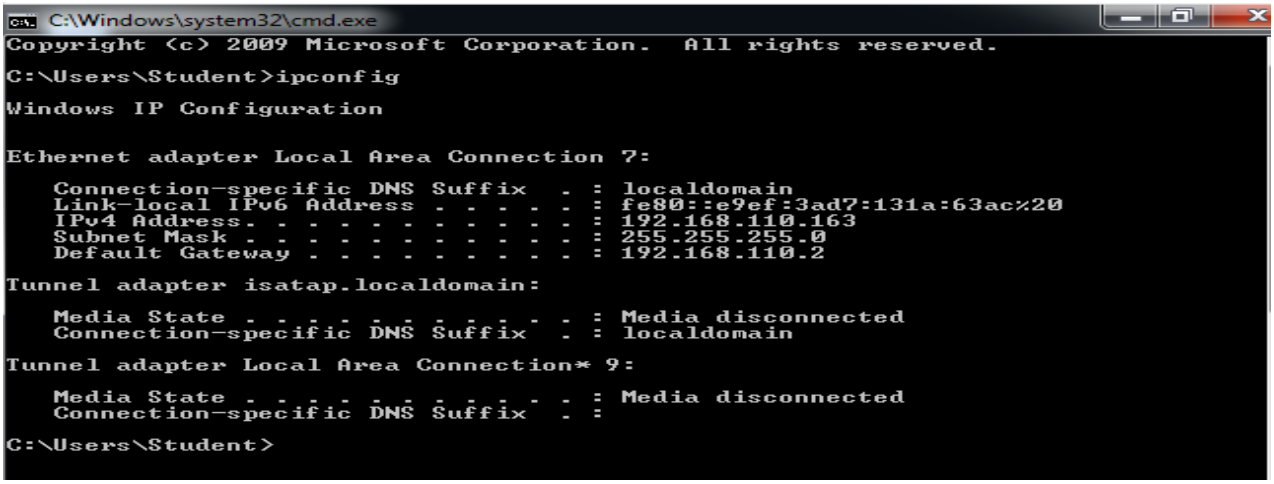
Command - `hydra -l test -P /[directory path]/darkc0de.lst [Kali IP address] http-get -m /protected`



1. Sniffing/Poisoning the Network

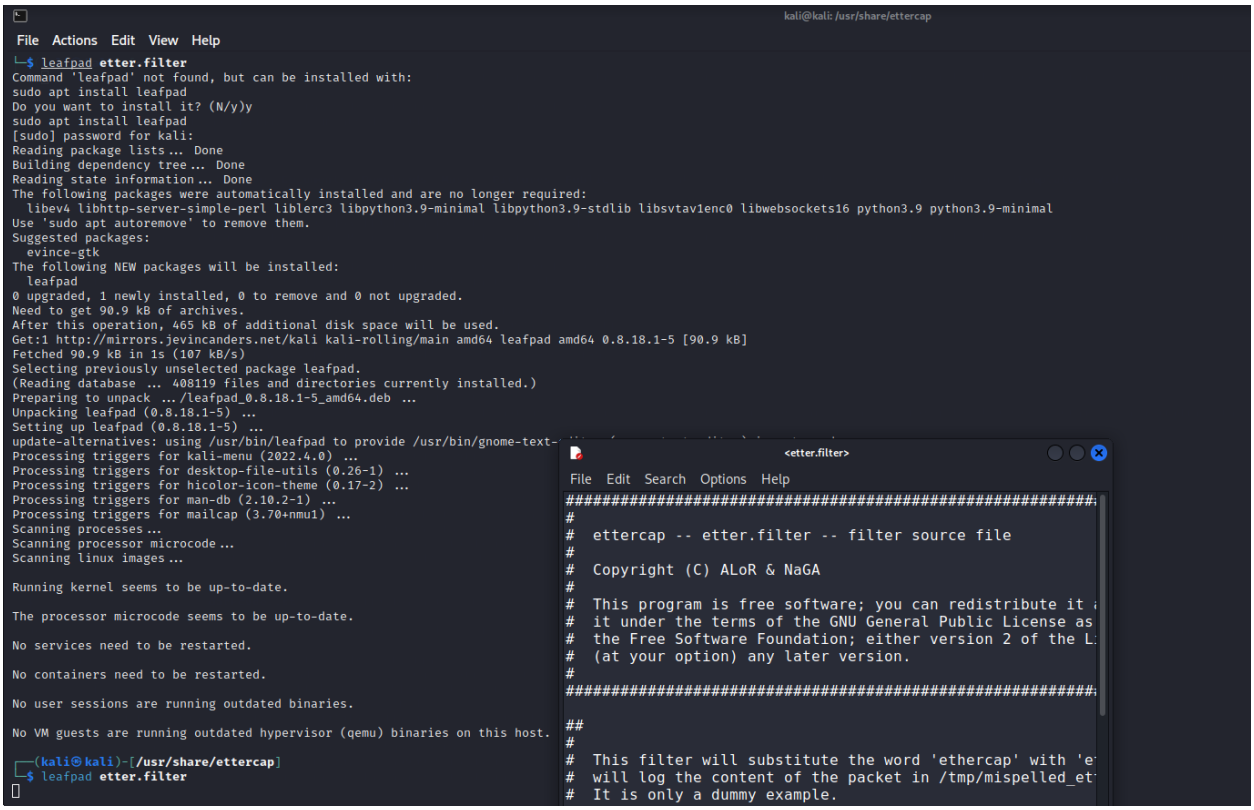
Power on your Windows 7, webserver, and Kali VMs, and take note of your IP addresses and your router IP.

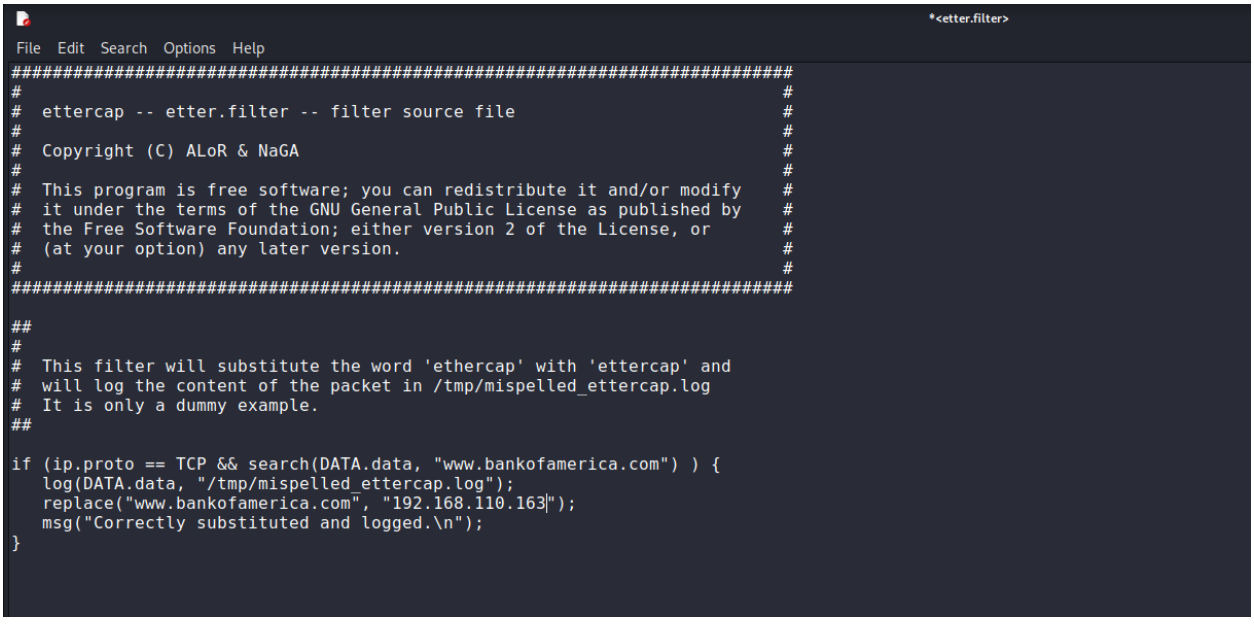




Within Kali, Open a terminal and change directory to /usr/share/ettercap

Open the file etter.filter in an editor of your choice. Using command - `leafpad etter.filter`





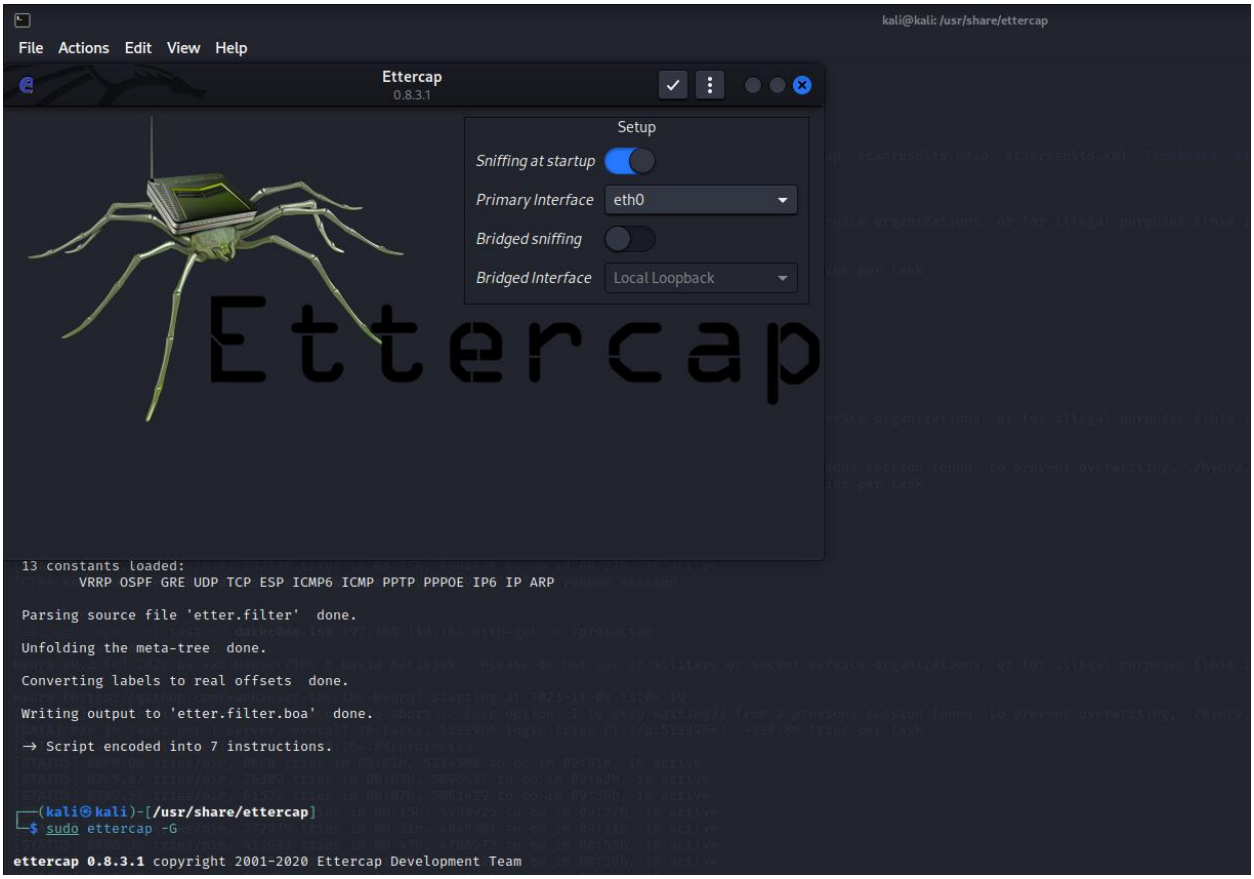
Save your new file. At the command prompt, run the following to "compile" the new rule.

Command - `etterfilter etter.filter -o etter.filter.boa`

```
┌──(kali㉿kali)-[/usr/share/ettercap]
└─$ sudo etterfilter etter.filter -o etter.filter.boa

etterfilter 0.8.3.1 copyright 2001-2020 Ettercap Development Team


 14 protocol tables loaded:
       DECODED DATA udp tcp esp gre icmp ipv6 ip arp wifi fddi tr eth

 13 constants loaded:
       VRRP OSPF GRE UDP TCP ESP ICMP6 ICMP PPTP PPPOE IP6 IP ARP

 Parsing source file 'etter.filter'  done.

 Unfolding the meta-tree  done.

 Converting labels to real offsets  done.

 Writing output to 'etter.filter.boa'  done.

 → Script encoded into 7 instructions.
```

Open Ettercap in GUI mode using the following command:

Command - `ettercap -G`



From the menu, select Sniff, and Unified Sniffing. Select your interface (should be eth0)

From the Hosts menu, select Hosts List, and then select Scan for hosts. This should return your Windows 7 VM's IP, and the router for your subnet.

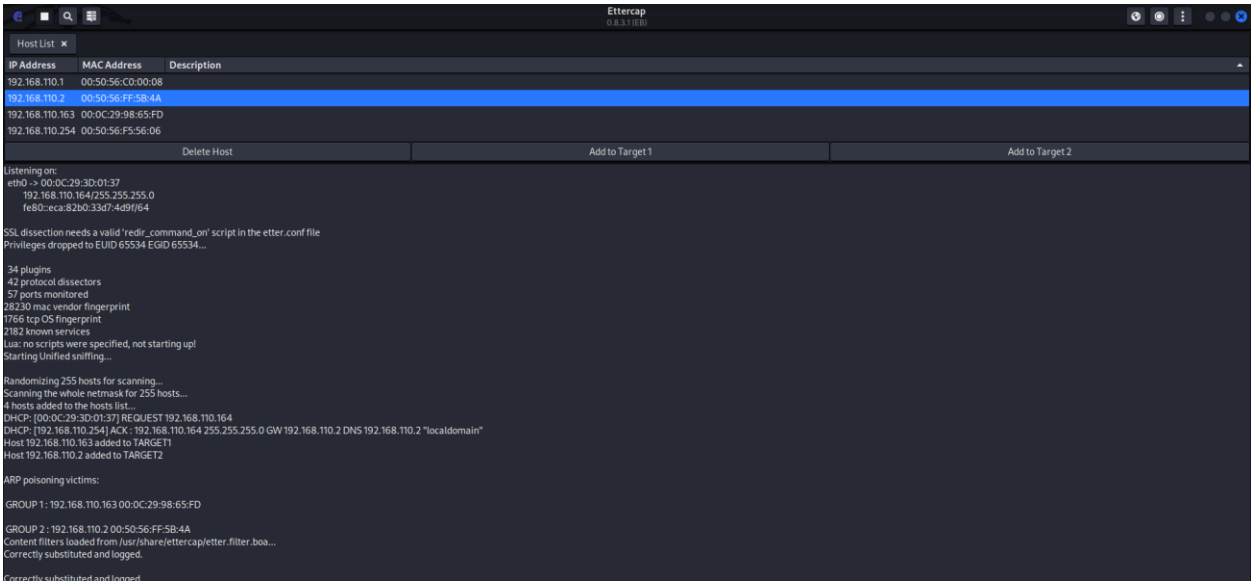
Highlight your Windows 7 VM and select "Add to Target 1". Highlight your Router and select "Add to Target 2"

From the Mitm menu, select "ARP Poisoning" and check the "Sniff remote connections" option.

From the Filers menu, select "Load a Filter" and then select the etter.filter.boa file we created earlier.

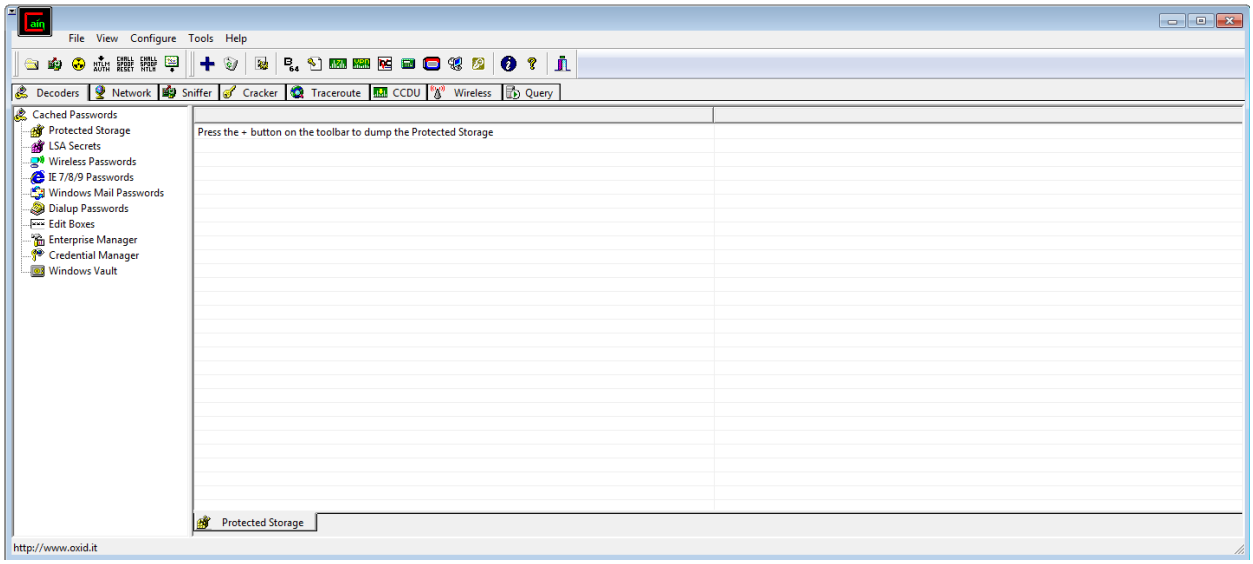
On your Windows 7 VM, browse to www.bankofamerica.com You may receive a Certificate Warning message, if so, select proceed anyway.

The result should be that the browser was redirected to a pretty basic login page that is hosted off of the webserver VM.

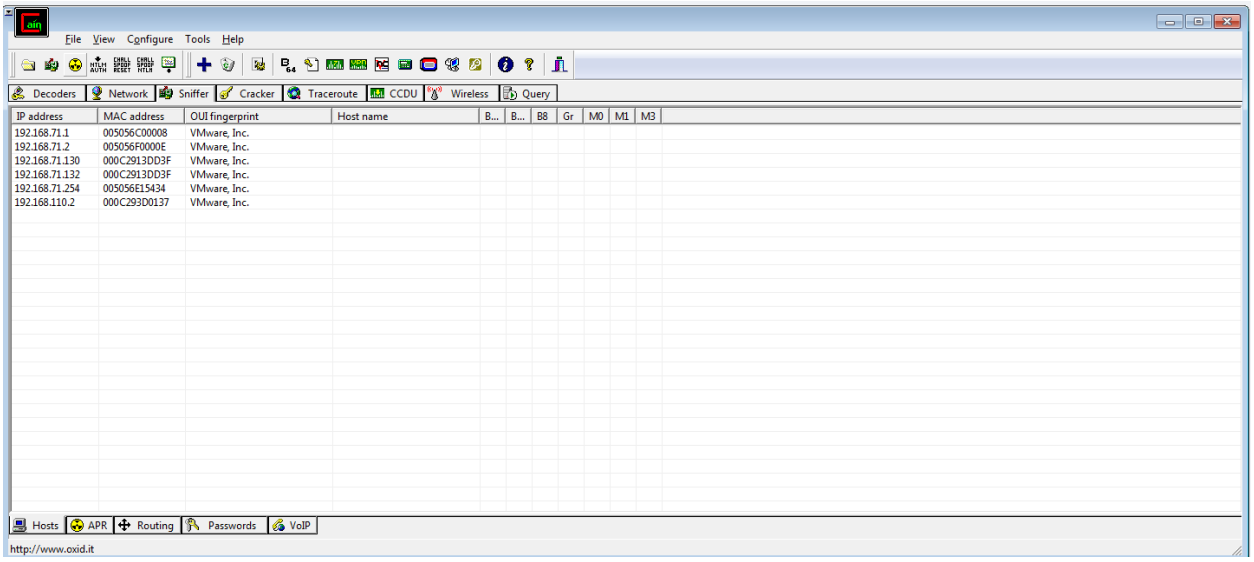


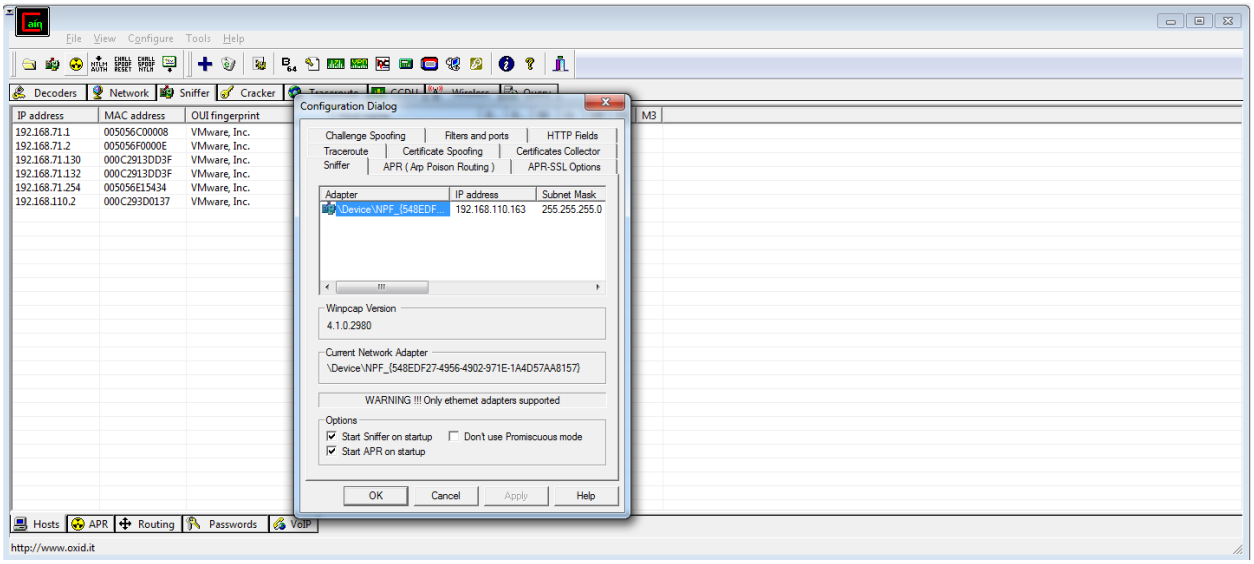
2. Using Cain/Abel to perform network poisoning

Loan Cain on the VM. Click on the Sniffer Tab, and then click on Configure to select your network adapter. Enable Sniffing by clicking the second icon from the left (looks like a network card).



Right Click in the empty table space and choose “Scan MAC addresses” in order to populate “victims” on the network

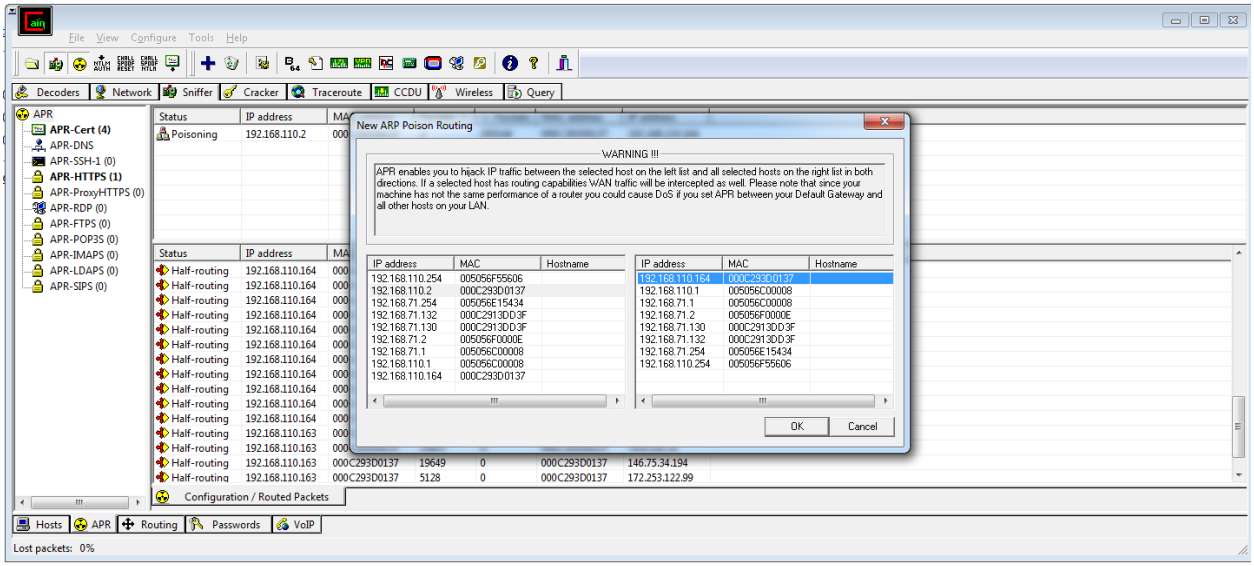




Click the APR tab. Click on the + sign in the toolbar to add a new ARP poison routing entry.

Choose the gateway for the network on the left side, on the right side select which victims you want to poison.

Once selected, click on the 3rd icon from the left (looks like a biohazard symbol) to begin poisoning. If any of the “Victim” systems you selected above are performing any tasks on the network, Cain will show them in the appropriate categories under the “Passwords” tab.



Now click on the APR-DNS heading in the left side listings under APR, and click on the + sign

Enter the address you want to spoof, such as facebook.com and the corresponding spoofed information. Click on resolve to bring up the dialog box to enter the named URL to resolve to IP, such as myspace.com