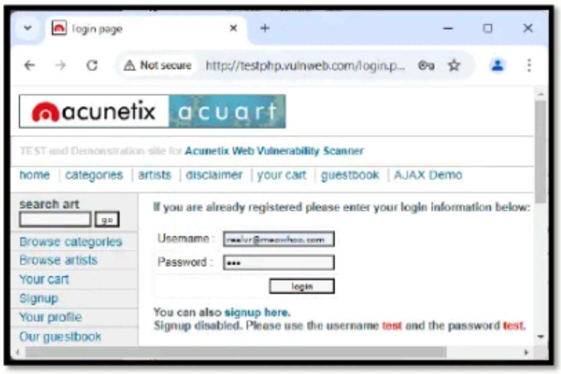
Step 9: Go to http://testphp.vulnweb.com/login.php and enter any username and password. Click on Login. Finally, from Passwords tab below, go to the HTTP tab, you can view the username and password entered here.


login page
Not secure http://testphp.vulnweb.com/login.p...
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
login

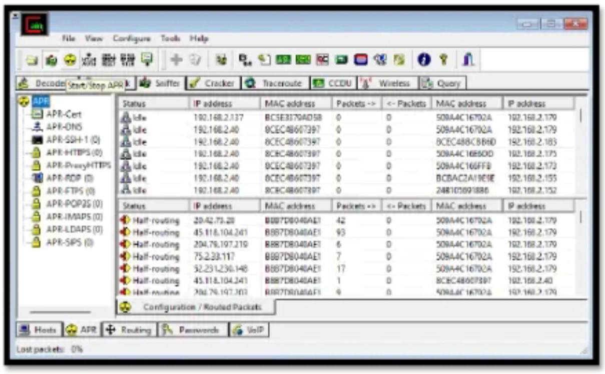
If you are already registered please enter your login information below:

Username : [illegible]

Password : •••

You can also signup here.
Signup disabled. Please use the username test and the password test.

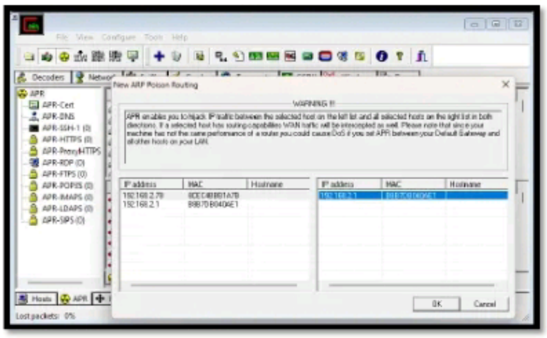
Step 6: Click on the "+" icon at the top. Select Start/Stop ARP.


File View Configure Tools Help
Decoders Start/Stop APR Sniffer Cracker Traceroute CCDU Wireless Query
APR
APR-Cert
APR-DNS
APR-SSH-1 (0)
APR-HTTPS (0)
APR-ProxyHTTPS
APR-RDP (0)
APR-FTPS (0)
APR-POP3S (0)
APR-IMAPS (0)
APR-LDAPS (0)
APR-SIPS (0)
Configuration / Routed Packets
Hosts APR Routing Passwords VoIP
Lost packets: 0%

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Idle	192.168.2.137	BC5E3379AD58	0	0	509A4C16702A	192.168.2.179
Idle	192.168.2.40	8CEC4B607397	0	0	509A4C16702A	192.168.2.179
Idle	192.168.2.40	8CEC4B607397	0	0	8CEC4B8CB86D	192.168.2.183
Idle	192.168.2.40	8CEC4B607397	0	0	509A4C16B6DD	192.168.2.175
Idle	192.168.2.40	8CEC4B607397	0	0	509A4C166FFB	192.168.2.173
Idle	192.168.2.40	8CEC4B607397	0	0	BCBAC2A19E9E	192.168.2.155
Idle	192.168.2.40	8CEC4B607397	0	0	248105891886	192.168.2.152

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Half-routing	20.42.73.28	BBB7DB040AE1	42	0	509A4C16702A	192.168.2.179
Half-routing	45.118.104.241	BBB7DB040AE1	93	0	509A4C16702A	192.168.2.179
Half-routing	204.79.197.219	BBB7DB040AE1	6	0	509A4C16702A	192.168.2.179
Half-routing	75.2.33.117	BBB7DB040AE1	7	0	509A4C16702A	192.168.2.179
Half-routing	52.231.230.148	BBB7DB040AE1	17	0	509A4C16702A	192.168.2.179
Half-routing	45.118.104.241	BBB7DB040AE1	1	0	8CEC4B607397	192.168.2.40
Half-routing	204.79.197.203	BBB7DB040AE1	9	0	509A4C16702A	192.168.2.179

Step 7: Select any ipv4 address from the left and select all the ip addresses and click on ok.



New ARP Poison Routing

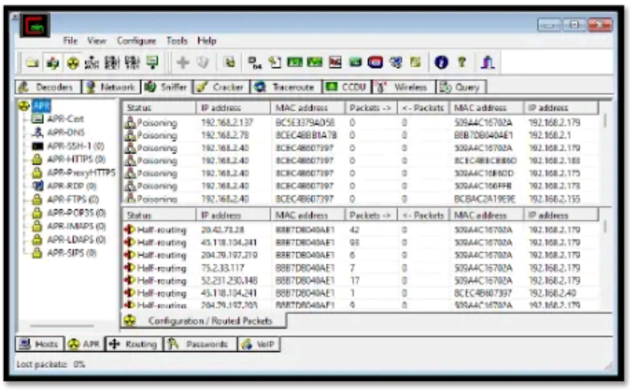
WARNING !!!

APR enables you to hijack IP traffic between the selected host on the left list and all selected hosts on the right list in both directions. If a selected host has routing capabilities WAN traffic will be intercepted as well. Please note that since your machine has not the same performance of a router you could cause DoS if you set APR between your Default Gateway and all other hosts on your LAN.

IP address	MAC	Hostname
192.168.2.78	8CEC4B8B1A78	
192.168.2.1	BBB7DB040AE1	

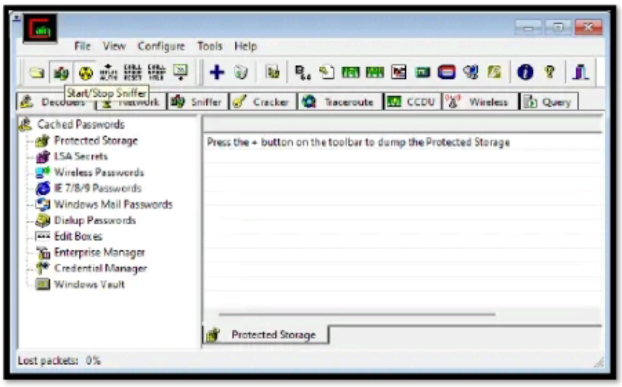
IP address	MAC	Hostname
192.168.2.1	BBB7DB040AE1	

Step 8: It gives status of all devices connected to the WiFi.


File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
APR
APR-Cert
APR-DNS
APR-SSH-1 (0)
APR-HTTPS (0)
APR-ProxyHTTPS
APR-RDP (0)
APR-FTPS (0)
APR-POP3S (0)
APR-IMAPS (0)
APR-LDAPS (0)
APR-SIPS (0)
Configuration / Routed Packets
Hosts APR Routing Passwords VoIP
Lost packets: 0%

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Poisoning	192.168.2.137	BC5E3379AD58	0	0	509A4C16702A	192.168.2.179
Poisoning	192.168.2.78	8CEC4B8B1A78	0	0	BBB7DB040AE1	192.168.2.1
Poisoning	192.168.2.40	8CEC4B607397	0	0	509A4C16702A	192.168.2.179
Poisoning	192.168.2.40	8CEC4B607397	0	0	8CEC4B8CB86D	192.168.2.183
Poisoning	192.168.2.40	8CEC4B607397	0	0	509A4C16B6DD	192.168.2.175
Poisoning	192.168.2.40	8CEC4B607397	0	0	509A4C166FFB	192.168.2.173
Poisoning	192.168.2.40	8CEC4B607397	0	0	BCBAC2A19E9E	192.168.2.155

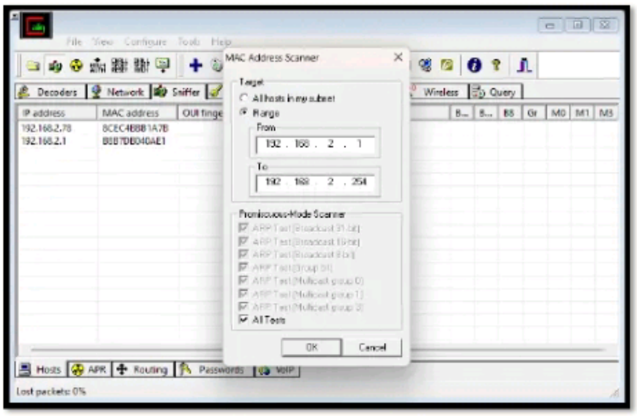
Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Half-routing	20.42.73.28	BBB7DB040AE1	42	0	509A4C16702A	192.168.2.179
Half-routing	45.118.104.241	BBB7DB040AE1	93	0	509A4C16702A	192.168.2.179
Half-routing	204.79.197.219	BBB7DB040AE1	6	0	509A4C16702A	192.168.2.179
Half-routing	75.2.33.117	BBB7DB040AE1	7	0	509A4C16702A	192.168.2.179
Half-routing	52.231.230.148	BBB7DB040AE1	17	0	509A4C16702A	192.168.2.179
Half-routing	45.118.104.241	BBB7DB040AE1	1	0	8CEC4B607397	192.168.2.40
Half-routing	204.79.197.203	BBB7DB040AE1	9	0	509A4C16702A	192.168.2.179



Press the + button on the toolbar to dump the Protected Storage

Lost packets: 0%

Step 4: Click on the "+" icon on the top. Select all tests and click on ok.


File View Configure Tools Help
Decoders Network Sniffer Wireless Query
Hosts APR Routing Passwords VoIP

IP address	MAC address	OUI finge
192.168.2.78	8CEC4BBB1A7B	
192.168.2.1	B8B7DB040AE1	

MAC Address Scanner

Target

○ All hosts in my subnet

● Range

From 192 . 168 . 2 . 1

To 192 . 168 . 2 . 254

Promiscuous-Mode Scanner

☑ ARP Test (Broadcast 31-bit)

☑ ARP Test (Broadcast 16-bit)

☑ ARP Test (Broadcast 8-bit)

☑ ARP Test (Group bit)

☑ ARP Test (Multicast group 0)

☑ ARP Test (Multicast group 1)

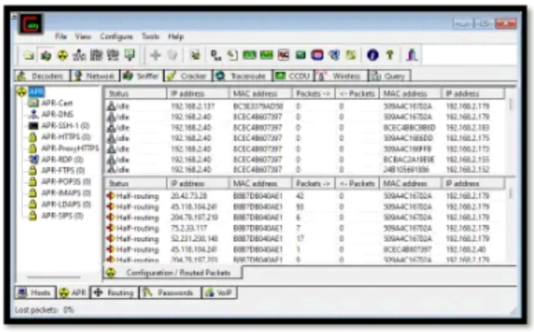
☑ ARP Test (Multicast group 3)

☑ All Tests

OK Cancel

Lost packets: 0%

Step 5: It will show all the connected hosts. Now select the ARP button from the bottom.

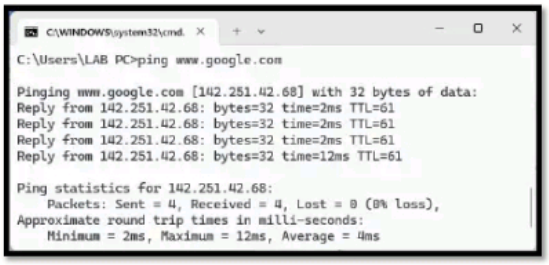

File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
APR
APR-Cert
APR-DNS
APR-SSH-1 (0)
APR-HTTPS (0)
APR-ProxyHTTPS
APR-RDP (0)
APR-FTPS (0)
APR-POP3S (0)
APR-IMAPS (0)
APR-LDAPS (0)
APR-SIPS (0)
Configuration / Routed Packets
Hosts APR Routing Passwords VoIP

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Idle	192.168.2.137	BC5E33794D58	0	0	509A4C16702A	192.168.2.179
Idle	192.168.2.40	8CEC4B607397	0	0	509A4C16702A	192.168.2.179
Idle	192.168.2.40	8CEC4B607397	0	0	8CEC4BBCBB0D	192.168.2.183
Idle	192.168.2.40	8CEC4B607397	0	0	509A4C16E6DD	192.168.2.175
Idle	192.168.2.40	8CEC4B607397	0	0	509A4C160FFB	192.168.2.173
Idle	192.168.2.40	8CEC4B607397	0	0	BCBAC2A19E8E	192.168.2.155
Idle	192.168.2.40	8CEC4B607397	0	0	24B105691886	192.168.2.152

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Half-routing	20.42.73.28	B8B7DB040AE1	42	0	509A4C16702A	192.168.2.179
Half-routing	45.118.104.241	B8B7DB040AE1	93	0	509A4C16702A	192.168.2.179
Half-routing	204.79.197.219	B8B7DB040AE1	6	0	509A4C16702A	192.168.2.179
Half-routing	75.2.33.117	B8B7DB040AE1	7	0	509A4C16702A	192.168.2.179
Half-routing	52.231.230.148	B8B7DB040AE1	17	0	509A4C16702A	192.168.2.179
Half-routing	45.118.104.241	B8B7DB040AE1	1	0	8CEC4B607397	192.168.2.40
Half-routing	204.79.197.203	B8B7DB040AE1	6	0	509A4C16702A	192.168.2.179

Lost packets: 0%

2. ping www.google.com

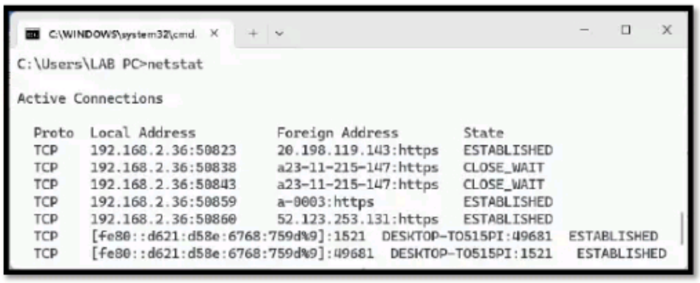


```
C:\Users\LAB PC>ping www.google.com

Pinging www.google.com [142.251.42.68] with 32 bytes of data:
Reply from 142.251.42.68: bytes=32 time=2ms TTL=61
Reply from 142.251.42.68: bytes=32 time=2ms TTL=61
Reply from 142.251.42.68: bytes=32 time=2ms TTL=61
Reply from 142.251.42.68: bytes=32 time=12ms TTL=61

Ping statistics for 142.251.42.68:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 12ms, Average = 4ms
```

3. netstat

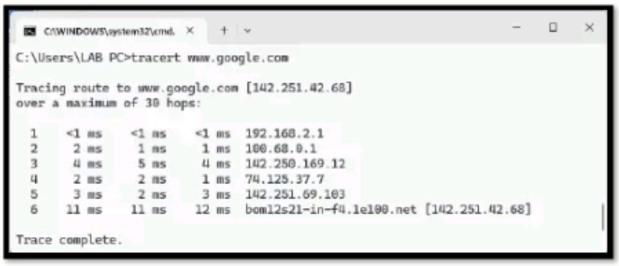


```
C:\Users\LAB PC>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.2.36:50823     20.198.119.143:https   ESTABLISHED
  TCP    192.168.2.36:50838     a23-11-215-147:https   CLOSE_WAIT
  TCP    192.168.2.36:50843     a23-11-215-147:https   CLOSE_WAIT
  TCP    192.168.2.36:50859     a-0003:https           ESTABLISHED
  TCP    192.168.2.36:50860     52.123.253.131:https   ESTABLISHED
  TCP    [fe80::d621:d58e:6768:759d%9]:1521  DESKTOP-TO515PI:49681  ESTABLISHED
  TCP    [fe80::d621:d58e:6768:759d%9]:49681  DESKTOP-TO515PI:1521   ESTABLISHED
```

4. tracert www.google.com



```
C:\Users\LAB PC>tracert www.google.com

Tracing route to www.google.com [142.251.42.68]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.2.1
  2     2 ms     1 ms     1 ms  100.68.0.1
  3     4 ms     5 ms     4 ms  142.250.169.12
  4     2 ms     2 ms     1 ms  74.125.37.7
  5     3 ms     2 ms     3 ms  142.251.69.103
  6    11 ms    11 ms    12 ms  bom12s21-in-f4.1e100.net [142.251.42.68]

Trace complete.
```

Step 2: For ARP Poisoning, disable all the security features from your computer and open Cain and Abel tool.

Step 3: Select icon named Start/Stop Sniffer. Select the desired adapter and click on ok.

Practical – 3

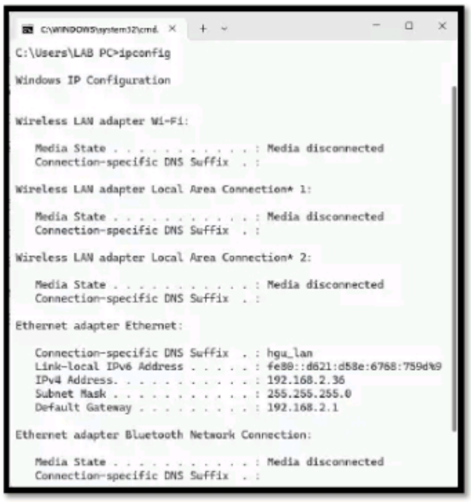
Aim: Linux Network Analysis and ARP Poisoning

- Linux Network Analysis:
  - Execute the ipconfig command to retrieve network interface information.
  - Use the ping command to test network connectivity and analyze the output.
  - Analyze the netstat command output to view active network connections.
  - Perform a traceroute to trace the route packets take to reach a target host.
- ARP Poisoning:
  - Use ARP poisoning techniques to redirect network traffic on a Windows system.
  - Analyze the effects of ARP poisoning on network communication and security.

Solution:

Step 1: Type the following commands in command prompt and analyze the information.

1. ipconfig



```
C:\Users\LAB PC>ipconfig

Windows IP Configuration


Wireless LAN adapter Wi-Fi:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : hgu_lan
   Link-local IPv6 Address . . . . . : fe80::d621:d58e:6768:759d%9
   IPv4 Address. . . . . . . . . . . : 192.168.2.36
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.2.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```