ASSIGNMENT REPORT: ARP SPOOFING BY- SRIDHAR S

Setup

Attack Machine: Kali Linux

Target Machine: Windows

Kali Linux IPaddress	192.168.37.130
Windows IPaddress	192.168.37.129
Default Gateway	192.168.37.2

Both machines are virtualized and connected within the same network.

Steps Executed

1. Network Configuration Verification

On Kali Linux: Terminal

ifconfig

Output displayed the IP address and network configuration of the attacking machine.

On Windows: CMD

ipconfig

Output displayed the IP address and network configuration of the target machine.

2. ARP Table Check (Windows)

Command executed:

arp -a

Verified the initial ARP table entries, ensuring normal gateway configurations.

3. Enable IP Forwarding (Kali Linux)

Verified IP forwarding status:

cat /proc/sys/net/ipv4/ip_forward

If the result was not "1", enabled IP forwarding:

echo 1 > /proc/sys/net/ipv4/ip_forward

4. Launching Ettercap

Opened Ettercap on Kali Linux.

Clicked the Search button to list available hosts in the network.

5. Target Selection in Ettercap

Selected the gateway address from the host list and set it as Target 1.

Selected the Windows machine IP address and set it as Target 2.

6. ARP Poisoning Attack

Enabled ARP Poisoning in Ettercap.

Started the attack.

Observed that the victims were successfully added to groups (Group 1 and Group 2).

7. ARP Table Check (Windows)

Rechecked the ARP table on the Windows machine:

arp -a

Verified that the physical address of the gateway had changed to match the physical address of the Kali Linux machine.

8. Packet Capture using Wireshark

Started Wireshark on Kali Linux, listening on the "eth0" interface.

9. HTTP Traffic Monitoring

Opened a browser on the Windows machine and accessed an HTTP website.

Observed HTTP data captured on Wireshark in real-time.

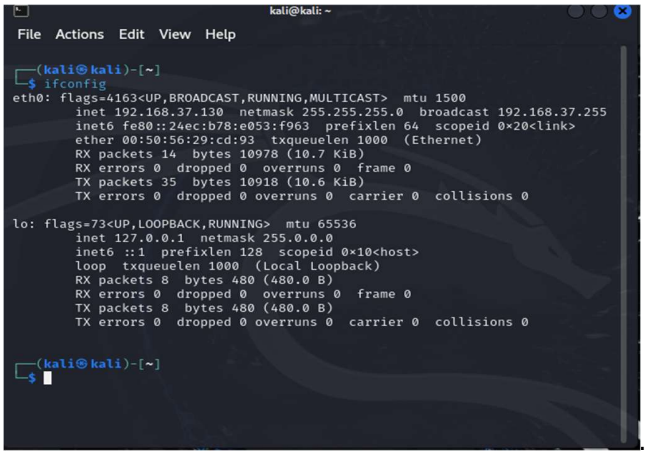
Result

The ARP Spoofing attack was successful. The target machine's ARP table was manipulated to redirect traffic through the attack machine. HTTP data from the target machine was intercepted and analyzed using Wireshark.

Screenshots

(Included the following screenshots for reference):

Ifconfig & Ipconfig

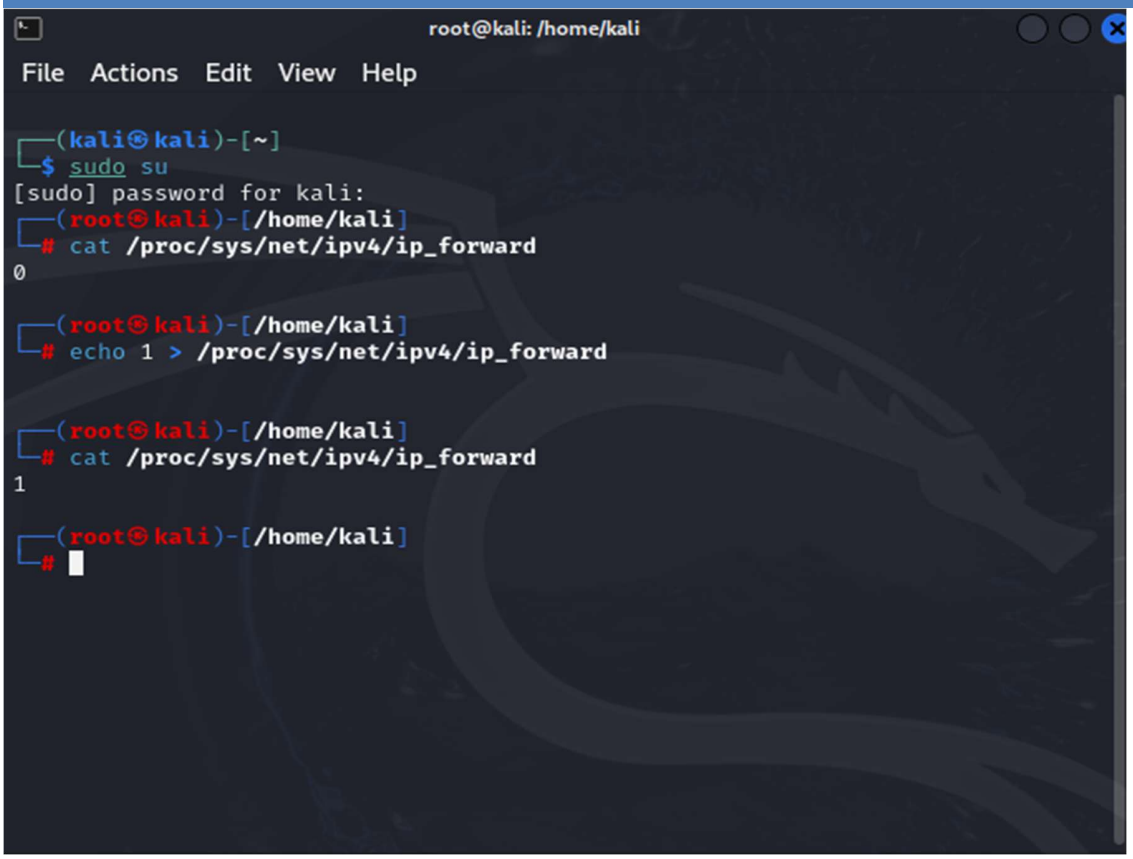


```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\admin>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::2921:c230:3005:703a%3
   IPv4 Address. . . . . . . . . . . : 192.168.37.129
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.37.2

Tunnel adapter isatap.localdomain:

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

C:\Users\admin>_
```

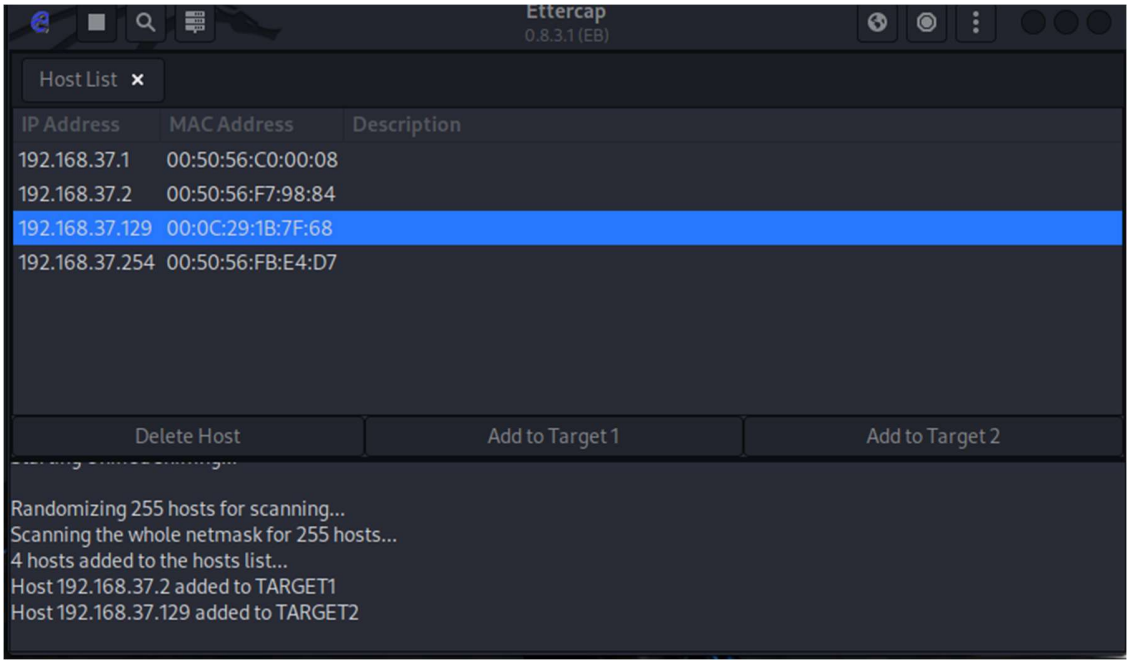
- Initial ARP table (`arp -a`) from Windows.

```
Select Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\admin>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::2921:c230:3005:703a%3
   IPv4 Address. . . . . . . . . . . : 192.168.37.129
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.37.2

Tunnel adapter isatap.localdomain:

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

C:\Users\admin>arp -a

Interface: 192.168.37.129 --- 0x3
  Internet Address      Physical Address      Type
  192.168.37.1          00-50-56-c0-00-08     dynamic
  192.168.37.2          00-50-56-f7-98-84     dynamic
  192.168.37.130        00-50-56-29-cd-93     dynamic
  192.168.37.254        00-50-56-fb-e4-d7     dynamic
  192.168.37.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.9             01-00-5e-00-00-09     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\admin>
```

- IP forwarding command and its result in Kali Linux.

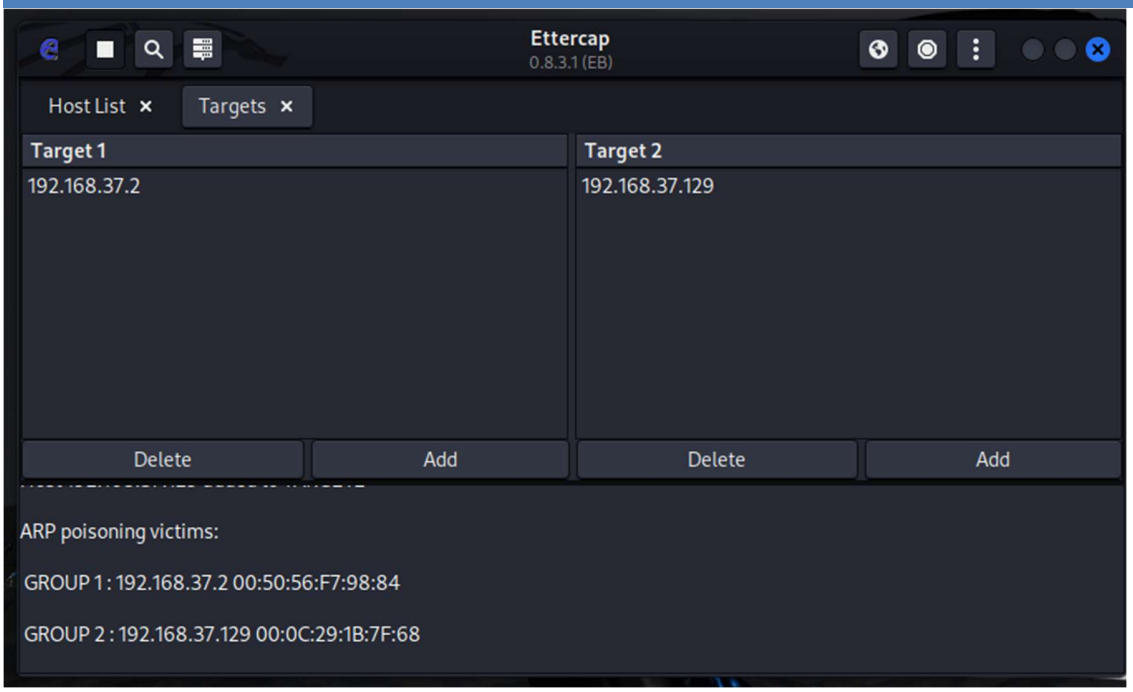


- Ettercap host list and target selection.

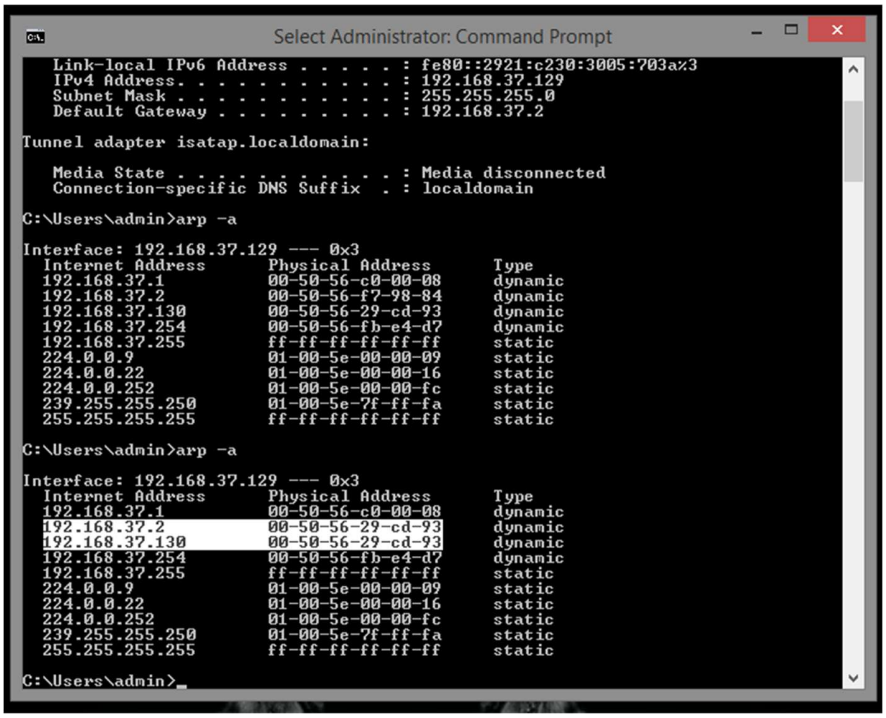


- Ettercap showing ARP Poisoning groups.

ASSIGNMENT REPORT: ARP SPOOFING BY- SRIDHAR S

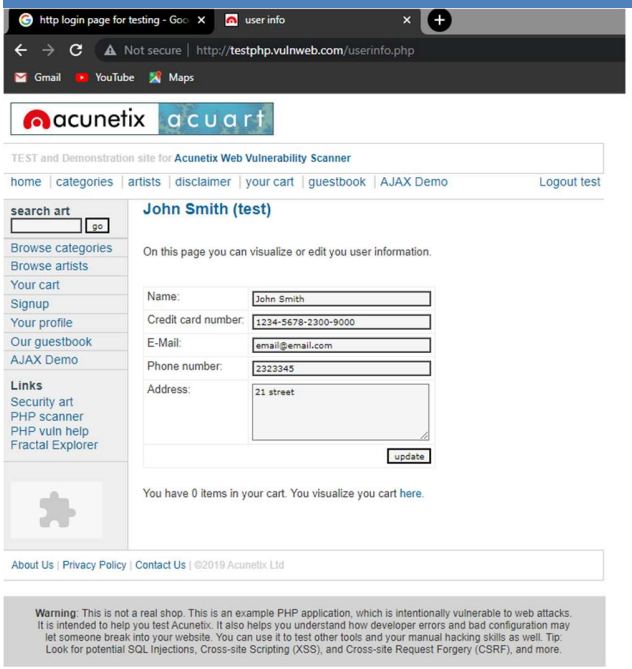


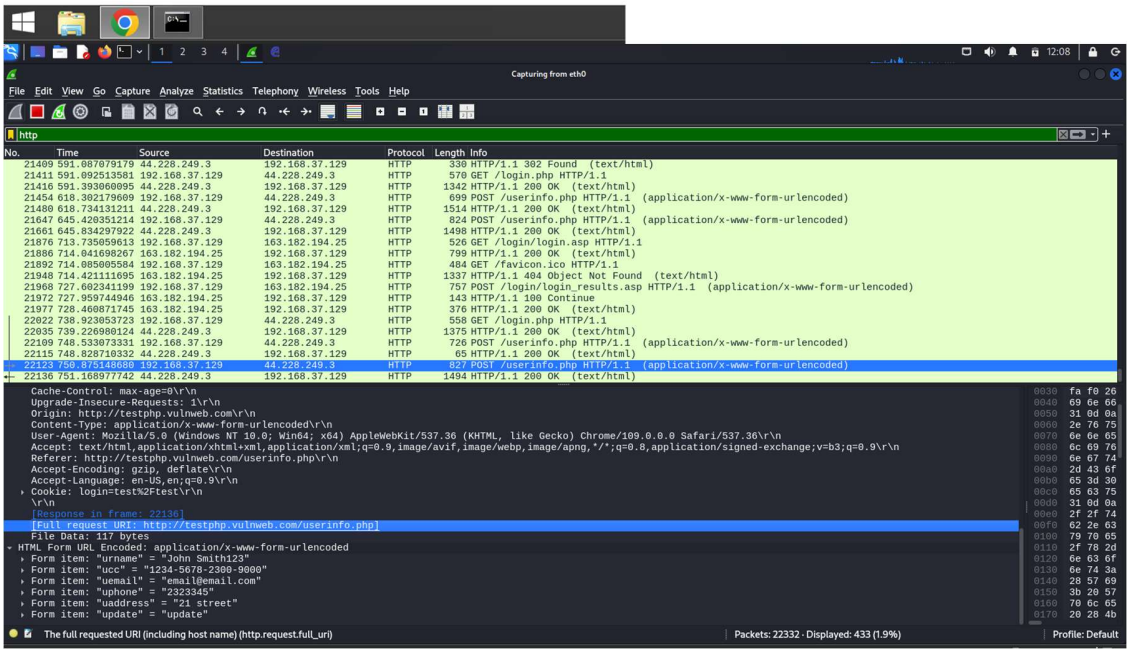
- Modified ARP table from Windows.



- Captured HTTP traffic in Wireshark.

ASSIGNMENT REPORT: ARP SPOOFING BY- SRIDHAR S





ASSIGNMENT REPORT: ARP SPOOFING BY- SRIDHAR S