

1-MAC-Spoofing

Name	Email
Omar Ashraf ElSayed Younes Abulila	omarabolilaofficial@gmail.com

Task Solution Source Code
https://github.com/omarafal/we-innovate-tasks/tree/main/1-MAC-Spoofing

Task

Create a script that changes the MAC address every three minutes and then resets it upon exit.

Task Solution Overview

NOTE: The script is assumed to run inside a Linux machine. If run on any other machine, it will always fail.

A typical MAC address consists of 6 bytes and (on Linux) is stored at `/sys/class/net/[INTERFACE]/address`.

The script takes in one argument; the targeted interface.

Setting the first byte to `0x02` indicates that this MAC address is **locally administered** and we can use it to spoof. The remaining 5 bytes are randomly chosen numbers between `0x00` and `0xFF`.

Before setting the new random address, we have to first safely store away our original MAC address so as not to lose it and then restore it once the user is done using the script.

Task Solution Explanation

```
1 from random import randint
2 import time
3 import sys
4 import os
5
6 def rand_mac():
7     final_addr = "02"
8
9     for _ in range(0, 5):
10         final_addr += f":{randint(0, 255):02X}"
11
12     return final_addr
```

The first four lines import the necessary libraries to generate random numbers, sleep for a specified time, grab command line arguments and to finally execute commands.

The function `rand_mac` generates the 5 random bytes and appends them to the fixated `0x02` byte and then returns the new address.

Now the `main` function:

```
1 def main(intf):
2     try:
3         with open(f"/sys/class/net/{intf}/address") as file:
4             org = file.read().strip()
5
6             # store in temp file just in case
7             with open("./spoof.tmp", "w") as file:
8                 file.write(org)
9     except:
10         print("This is not a valid interface.\n")
11         sys.exit(1)
```

This first part opens the file where the MAC address is stored and grabs the original one. It then stores it in a temporary file just in case something went wrong like the terminal suddenly closing. That way if anything happens, the user still has a copy of the original MAC address.

This temporary file gets deleted after the script is done executing successfully.

```

1  try:
2      while True:
3          new_add = rand_mac()
4
5          os.system(f"sudo ip link set dev {intf} down")
6          os.system(f"sudo ip link set dev {intf} address {new_add}")
7          os.system(f"sudo ip link set dev {intf} up")
8
9          print("\nMAC address changed.\n")
10         print(f"Running: ip link show {intf}")
11         os.system(f"ip link show {intf}")
12         time.sleep(60*3)

```

This code inside the `main` function is responsible for setting the new MAC address that is returned from the `rand_mac` function then printing out the information regarding the provided interface to prove that it changed.

Finally, it sleeps for 3 minutes before re-doing all of this again; setting a new random MAC address.

```

1  except KeyboardInterrupt:
2      print("\nCleaning up before exiting.\nResetting MAC address.")
3
4      try:
5          os.system(f"sudo ip link set dev {intf} down")
6          os.system(f"sudo ip link set dev {intf} address {org}")
7          os.system(f"sudo ip link set dev {intf} up")
8      except:
9          print("Something went wrong.\n")
10         sys.exit(1)
11     # to protect the temp file just in case
12     if os.path.exists("./spoof.tmp"):
13         os.remove("./spoof.tmp")

```

This final major piece of code is responsible for cleaning up when the user hits `Ctrl+C` to stop the script.

The "cleanup" consists of resetting the MAC address to its original one as well as deleting the temporary file that contained it since it won't be necessary to keep if the original address was set successfully.

```

1  if __name__ == "__main__":
2      try:
3          intf = sys.argv[1] # grab interface
4      except IndexError:
5          print("Usage: python macspoofer.py [INTERFACE]\n")
6          sys.exit(1)
7
8      main(intf)

```

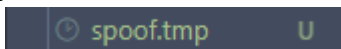
At last, the user receives a message if no arguments were passed to the script at all to show the user how to correctly use the script.

Task Output Showcase

The output of the initial run:

```
omarafal@OMAR-DES: /mnt/d/WE-INNOVATE/we-innovate-tasks/1-MAC-Spoofers$ python3 macspoof.py eth0
MAC address changed.
Running: ip link show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP mode DEFAULT group default qlen 1000
    link/ether 02:d2:32:3f:e4:db brd ff:ff:ff:ff:ff:ff permaddr 00:15:5d:5d:6f:6a
```

We can then notice that a temporary file has been created:



If we leave it for three minutes we would see how the address has changed once more:

```
omarafal@OMAR-DES: /mnt/d/WE-INNOVATE/we-innovate-tasks/1-MAC-Spoofers$ python3 macspoof.py eth0
MAC address changed.
Running: ip link show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP mode DEFAULT group default qlen 1000
    link/ether 02:d2:32:3f:e4:db brd ff:ff:ff:ff:ff:ff permaddr 00:15:5d:5d:6f:6a

MAC address changed.
Running: ip link show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP mode DEFAULT group default qlen 1000
    link/ether 02:5c:df:2c:64:fc brd ff:ff:ff:ff:ff:ff permaddr 00:15:5d:5d:6f:6a
```

Now, if we interrupt and close the script:

```
omarafal@OMAR-DES: /mnt/d/WE-INNOVATE/we-innovate-tasks/1-MAC-Spoofers$ python3 macspoof.py eth0
MAC address changed.
Running: ip link show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP mode DEFAULT group default qlen 1000
    link/ether 02:d2:32:3f:e4:db brd ff:ff:ff:ff:ff:ff permaddr 00:15:5d:5d:6f:6a

MAC address changed.
Running: ip link show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP mode DEFAULT group default qlen 1000
    link/ether 02:5c:df:2c:64:fc brd ff:ff:ff:ff:ff:ff permaddr 00:15:5d:5d:6f:6a
^C
Cleaning up before exiting.
Resetting MAC address.
omarafal@OMAR-DES: /mnt/d/WE-INNOVATE/we-innovate-tasks/1-MAC-Spoofers$
```

And we would notice that the temporary file is gone and the MAC has been reset:

```
omarafal@OMAR-DES: /mnt/d/WE-INNOVATE/we-innovate-tasks/1-MAC-Spoofers$ ip link show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP mode DEFAULT group default qlen 1000
    link/ether 00:15:5d:5d:6f:6a brd ff:ff:ff:ff:ff:ff
omarafal@OMAR-DES: /mnt/d/WE-INNOVATE/we-innovate-tasks/1-MAC-Spoofers$
```