سپهر مقیسه

مبانی امنیت اطلاعات

تکلیف عملی سوم

پاییز ۱۴۰۱

بخش اول

در این بخش، در کد سرور یک سوکت روی آدرس ۰.۰.۰.۰ و پورت ۵۰۰۰ اصطلاحا bind میکنیم و منتظر برقراری اتصال میشویم. درکلاینت نیز تنها به آدرس سرور وصل شده و سپس سوکت را میبندیم. در شکلهای زیر، خروجی کد سرور و کلاینت را در این مرحله میبینیم.

```
SUS@ASUS MINGW64 /d/security system/src/pythonProject7
 python malware.py
onnected to localhost on port 5000
```

```
ASUS@ASUS MINGW64 /d/security system/src/pythonProject7
$ python server.py
Listening on 0.0.0.0:5000
==> 127.0.0.1 connected on port 34438
```

بخش دوم

برای ارسال پیام بین دو سوکت، پروتکل سادهای را استفاده میکنیم .در این پروتکل، در ابتدای ارسال هر پیام، اندازه پیام در ۴ بایت ارسال میشود و سپس پیام مربوطه ارسال میشود .توابع ارسال و دریافت پیامها در فایل sock_helper.py آمده است.

در این بخش، پس از اجرای کلاینت و اتصال آن به سرور، در تابع get_host_data() ، اطلاعاتی برای نمونه از سیستم قربانی جمع آوری شده و در قالب یک دیکشنری برگردانده میشود .سپس این دیکشنری به jsonتبدیل شده و به کمک پروتکل ساده مان، به سرور ارسال میشود .نتیجه اجرای کلاینت و نمایش اطلاعات قربانی روی سرور را در شکل زیر میبینیم.

```
{'CPU': {'Physical cores': 4, 'Total cores': 8},
 'Memory': {'Available': '2.82GB',
            'Percentage': '76.3%',
                                          'Netmask': '255.255.255.0'},
            'Wi-Fi': {'Broadcast IP': None,
                      'IP': '192.168.1.178',
                      'Netmask': '255.255.255.0'},
            'vEthernet (WSL)': {'Broadcast IP': None,
                                'IP': '172.17.176.1',
                                'Netmask': '255.255.240.0'}},
 'Swap': {'Free': '1.11GB',
          'Percentage': '88.1%',
          'Total': '9.34GB',
          'Used': '8.23GB'},
 'System': {'Boot Time': '2022/12/19 21:29:15',
            'Host Name': 'ASUS',
            'Machine': 'AMD64',
            'Processor': 'Intel64 Family 6 Model 142 Stepping 10, GenuineIntel',
            'Release': '10',
            'System': 'Windows',
            'Version': '10.0.19041'}}
--------------------
```

بخش سوم

برای این بخش، پس ا ز اینکه کلاینت به سرور متصل شد، منتظر دریافت پیام sysinfo از سرور میماند و پس از آن اطلاعات را ارسال میکند.

در بخش سرور نیز، علاوه بر امکان اتصال همزمان چندین کلاینت(با قرار دادن سوکت های آنها در یک لیست)، دو دستور sysinfo وclose اضافه شده است .هر دوی این دستورها به عنوان پارامتر، شماره قربانی را دریافت میکنند و دستور اول در پاسخ، اطلاعات سیستم قربانی را ارسال میکند .دستور دوم نیز اتصال را پایان میدهد .در شکل زیر، یک سناریو از اتصال کلاینت ها، دریافت اطلاعات آنها و بستن اتصال را مشاهده میکنیم .

```
ASUS@ASUS MINGW64 /d/security system/src/pythonProject7
 'Memory': {'Available': '2.78GB',
            'Percentage': '76.6%',
            'Total': '11.88GB',
            'Used': '9.10GB'},
 'Network': {'Bluetooth Network Connection': {'Broadcast IP': None,
                                              'IP': '169.254.42.173',
                                              'Netmask': '255.255.0.0'},
             'Ethernet': {'Broadcast IP': None,
                          'IP': '169.254.248.100',
                          'Netmask': '255.255.0.0'},
             'HotspotShield Network Adapter': {'Broadcast IP': None,
                                               'IP': '100.127.255.249',
                                               'Netmask': '255.255.255.248'},
             'Local Area Connection': {'Broadcast IP': None,
                                       'IP': '169.254.254.42',
                                       'Netmask': '255.255.0.0'},
             'Local Area Connection 2': {'Broadcast IP': None,
                                         'IP': '169.254.33.150',
                                         'Netmask': '255.255.0.0'},
             'Local Area Connection* 1': {'Broadcast IP': None,
                                          'IP': '169.254.3.12',
                                          'Netmask': '255.255.0.0'},
             'Local Area Connection* 10': {'Broadcast IP': None,
                                           'IP': '169.254.226.204',
                                           'Netmask': '255.255.0.0'},
             'Loopback Pseudo-Interface 1': {'Broadcast IP': None,
                                             'IP': '127.0.0.1',
                                             'Netmask': '255.0.0.0'},
             'ProtonVPN TUN': {'Broadcast IP': None,
                               'IP': '169.254.160.23',
                               'Netmask': '255.255.0.0'},
             'VMware Network Adapter VMnet1': {'Broadcast IP': None,
                                               'IP': '192.168.68.1',
                                               'Netmask': '255.255.255.0'},
             'VMware Network Adapter VMnet8': {'Broadcast IP': None,
                                               'IP': '192.168.198.1',
                                               'Netmask': '255.255.255.0'},
             'Wi-Fi': {'Broadcast IP': None,
                       'IP': '192.168.1.178',
                       'Netmask': '255.255.255.0'},
             'vEthernet (WSL)': {'Broadcast IP': None,
                                 'IP': '172.17.176.1',
                                 'Netmask': '255.255.240.0'}},
 'Swap': {'Free': '1.12GB',
          'Percentage': '88.1%',
          'Total': '9.34GB',
          'Used': '8.23GB'},
 'System': {'Boot Time': '2022/12/19 21:29:15',
            'Host Name': 'ASUS',
            'Machine': 'AMD64',
            'Processor': 'Intel64 Family 6 Model 142 Stepping 10, GenuineIntel',
            'Release': '10',
            'System': 'Windows',
            'Version': '10.0.19041'}}
====================
Type sysinfo/close and number to get the info or close the session
        [1] 127.0.0.1:34501
close 1
====================
```