

سیستم هکینگ

فهرست مطالب

بخش اول	۲
بخش دوم	۳
بخش سوم	۳
سایر بخش ها	۴
طراحی واسط کاربری ابتدایی	۴
تفاوت سیستم عامل ها	۶

بخش اول

برای پیاده سازی سرور از لینک زیر استفاده می کنیم.

<https://github.com/amir78729/python-TCP-client-server-template/blob/main/Server.py>

با اجرای سرور، منتظر کلاینت ها می مانیم:

```

Run: server
/Users/tapsi/PycharmProjects/internet-security-prj-1/venv/bin/python /Users/tapsi/PycharmProjects/HackingSystem/server.py
[SERVER STARTS] Server is starting...
  
```

برای پیاده سازی بدافزار نیز از لینک زیر استفاده می کنیم.

<https://github.com/amir78729/python-TCP-client-server-template/blob/main/Client.py>

به محض اجرای بدافزار، سرور متوجه حضور او خواهد شد و کلاینت میتواند برای آن پیام ارسال نماید.

```

Run: malware
/Users/tapsi/PycharmProjects/internet-security-prj-1/venv/bin/python /Users/tapsi/PycharmProjects/HackingSystem/Client.py
ENTER YOUR MESSAGE (TYPE "/" TO EXIT)

Run: server
/Users/tapsi/PycharmProjects/internet-security-prj-1/venv/bin/python /Users/tapsi/PycharmProjects/HackingSystem/server.py
[SERVER STARTS] Server is starting...
[NEW CONNECTION] connected from ('127.0.0.1', 60090).
  
```

```

Run: malware
/Users/tapsi/PycharmProjects/internet-security-prj-1/venv/bin/python /Users/tapsi/PycharmProjects/HackingSystem/Client.py
ENTER YOUR MESSAGE (TYPE "/" TO EXIT) message

Run: server
/Users/tapsi/PycharmProjects/internet-security-prj-1/venv/bin/python /Users/tapsi/PycharmProjects/HackingSystem/server.py
[SERVER STARTS] Server is starting...
[NEW CONNECTION] connected from ('127.0.0.1', 60090).
[MESSAGE RECIEVED] message
  
```

بخش دوم

به کمک کتابخانه‌هایی مانند os, psutil, locale, re و platform می‌توانیم اطلاعات را از سیستم بدست آوریم. با اجرای کد بدافزار، این اطلاعات به صورت خودکار برای سرور فرستاده می‌شود. در این مرحله تمام اطلاعات بدست نمی‌آیند و در ادامه سعی خواهیم کرد که این اطلاعات را تکمیل کنیم.

```

HackingSystem server.py
Project Run: malware
/Users/tapsi/PycharmProjects/internet-security-prj-1/venv/bin/python /Users/tapsi/...
Process finished with exit code 0

server
[MESSAGE RECIEVED]
-----
Host Name: Amirhossein-Macbook-Pro.Local
OS Name: Darwin
OS Version: 20.6.0
OS Manufacturer: ?
OS Configuration: x86_64
Registered Owner: ?
Registered Organization: ?
Product ID: ?
Original Install Date: ?
System Boot Time: 1641121920.0s
System Manufacturer: ?
System Model: ?
System Type: ?
Processor(s): i386
BIOS Version: ?
Windows Directory: ?
System Directory: ?
Boot Device: ?
System Locale: en_US.UTF-8
Input Locale: ?
Time Zone: +0330
Total Physical Memory: ?
Available Physical Memory: ?
Virtual Memory: Max Size: 8.0 GB
Virtual Memory: Available: 2.1483 GB
Virtual Memory: In Use: 5.8517 GB
Page File Location(s): ?
Domain: ?
Logon Server: ?
Hotfix(s): ?
OS Architecture: x86_64
Mac Address: a6:83:e7:64:3c:d9
RAM: 8 GB
  
```

بخش سوم

در این بخش باید وقتی بدافزار فعال شد پیامی در سرور نمایش داده شود.

```

Run: malware
/Users/tapsi/PycharmProjects/internet-security-prj-1/venv/bin/python /Users/tapsi/...
Tue Jan 4 03:44:44 2022 [RUNNING MALWARE]

server
/Users/tapsi/PycharmProjects/internet-security-prj-1/venv/bin/python /Users/tapsi/P...
Tue Jan 4 03:44:42 2022 [WAITING] waiting for a malware...
Tue Jan 4 03:44:44 2022 [VICTIM DETECTED] new connection from 127.0.0.1:58941
  
```

هنگامی که سرور ورودی sysinfo را وارد می‌کند، اطلاعات از سوی بدافزار برای سرور ارسال شود.

```

Run: malware x
/Users/tapsi/PycharmProjects/internet-security-prj-1/venv/bin/python /Users/tapsi/PycharmProjects/internet-security-prj-1/venv/bin/python /Users/tapsi/PycharmProjects/internet-security-prj-1/venv/bin/python
Tue Jan 4 03:44:44 2022 [RUNNING MALWARE]
Tue Jan 4 03:45:22 2022 [SENDING DATA TO SERVER]

server x
/Users/tapsi/PycharmProjects/internet-security-prj-1/venv/bin/python /Users/tapsi/PycharmProjects/internet-security-prj-1/venv/bin/python /Users/tapsi/PycharmProjects/internet-security-prj-1/venv/bin/python
Tue Jan 4 03:44:42 2022 [WAITING] waiting for a malware...
Tue Jan 4 03:44:44 2022 [VICTIM DETECTED] new connection from 127.0.0.1:58941
Tue Jan 4 03:45:22 2022 [MESSAGE RECEIVED] malware:
-----
Host Name: Amirhossein-Macbook-Pro.local
OS Name: Darwin
OS Version: 20.6.0
OS Manufacturer: ?
OS Configuration: x86_64
Registered Owner: ?
Registered Organization: ?
Product ID: ?
Original Install Date: ?
System Boot Time: 1641121920.0s
System Manufacturer: ?
System Model: ?
System Type: ?
Processor(s): i386
BIOS Version: ?

```

در این فرآیند تنها یک کانکشن ساخته می‌شود. همچنین بد افزار نیز میتواند برای سرور پیام ارسال نماید.

```

Run: malware x
/Users/tapsi/PycharmProjects/internet-security-prj-1/venv/bin/python /Users/tapsi/PycharmProjects/internet-security-prj-1/venv/bin/python /Users/tapsi/PycharmProjects/internet-security-prj-1/venv/bin/python
Tue Jan 4 03:44:44 2022 [RUNNING MALWARE]
Tue Jan 4 03:45:22 2022 [SENDING DATA TO SERVER]
a message from malware to server

server x
/Users/tapsi/PycharmProjects/internet-security-prj-1/venv/bin/python /Users/tapsi/PycharmProjects/internet-security-prj-1/venv/bin/python /Users/tapsi/PycharmProjects/internet-security-prj-1/venv/bin/python
Tue Jan 4 03:46:28 2022 [MESSAGE RECEIVED] malware: a message from malware to server
-----
BIOS Version: ?
Windows Directory: ?
System Directory: ?
Boot Device: ?
System Locale: en_US(UTF-8)
Input Locale: ?
Time Zone: +0330
Total Physical Memory: ?
Available Physical Memory: ?
Virtual Memory: Max Size: 8.0 GB
Virtual Memory: Available: 2.0201 GB
Virtual Memory: In Use: 5.979900000000001 GB
Page File Location(s): ?
Domain: ?
Logon Server: ?
Hotfix(s): ?
OS Architecture: x86_64
Mac Address: a6:83:e7:64:3c:d9
RAM: 8 GB

```

همچنین سرور می‌تواند با ارسال q-ارتباط با بدافزار فعلی را خاتمه دهد و منتظر بدافزارهای دیگر باشد.

```

Run: malware x
/Users/tapsi/PycharmProjects/internet-security-prj-1/venv/bin/python /Users/tapsi/PycharmProjects/internet-security-prj-1/venv/bin/python /Users/tapsi/PycharmProjects/internet-security-prj-1/venv/bin/python
Tue Jan 4 03:44:44 2022 [RUNNING MALWARE]
Tue Jan 4 03:45:22 2022 [SENDING DATA TO SERVER]
a message from malware to server
Tue Jan 4 03:47:38 2022 [TERMINATING MALWARE]
Process finished with exit code 0

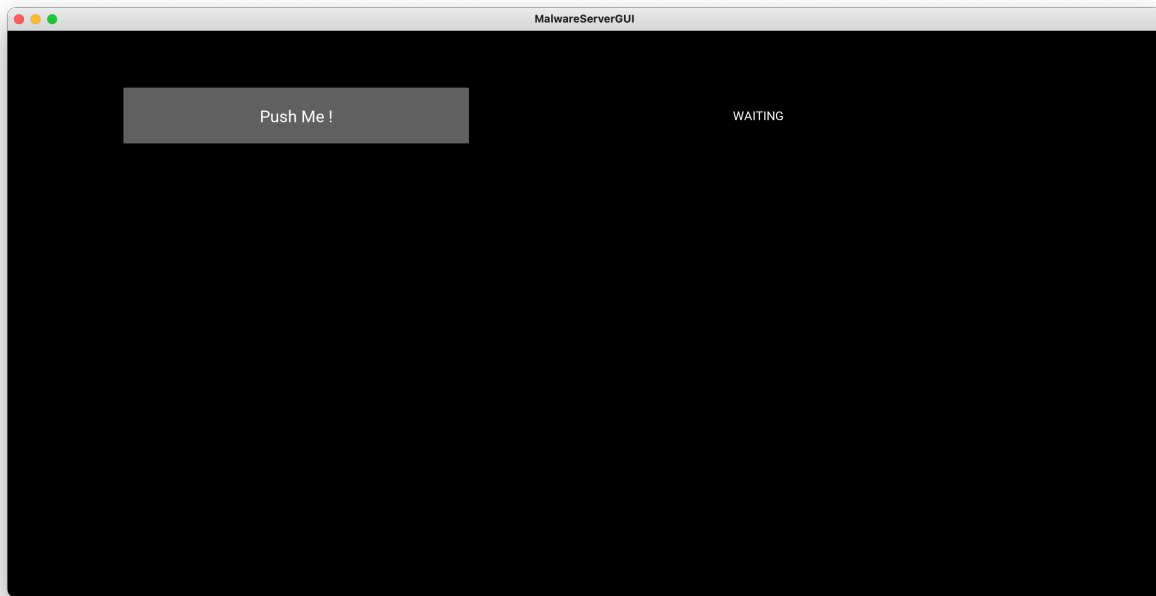
server x
/Users/tapsi/PycharmProjects/internet-security-prj-1/venv/bin/python /Users/tapsi/PycharmProjects/internet-security-prj-1/venv/bin/python /Users/tapsi/PycharmProjects/internet-security-prj-1/venv/bin/python
Tue Jan 4 03:46:28 2022 [MESSAGE RECEIVED] malware: a message from malware to server
Tue Jan 4 03:47:38 2022 [CONNECTION LOST]
Tue Jan 4 03:47:38 2022 [WAITING] waiting for a malware...

```

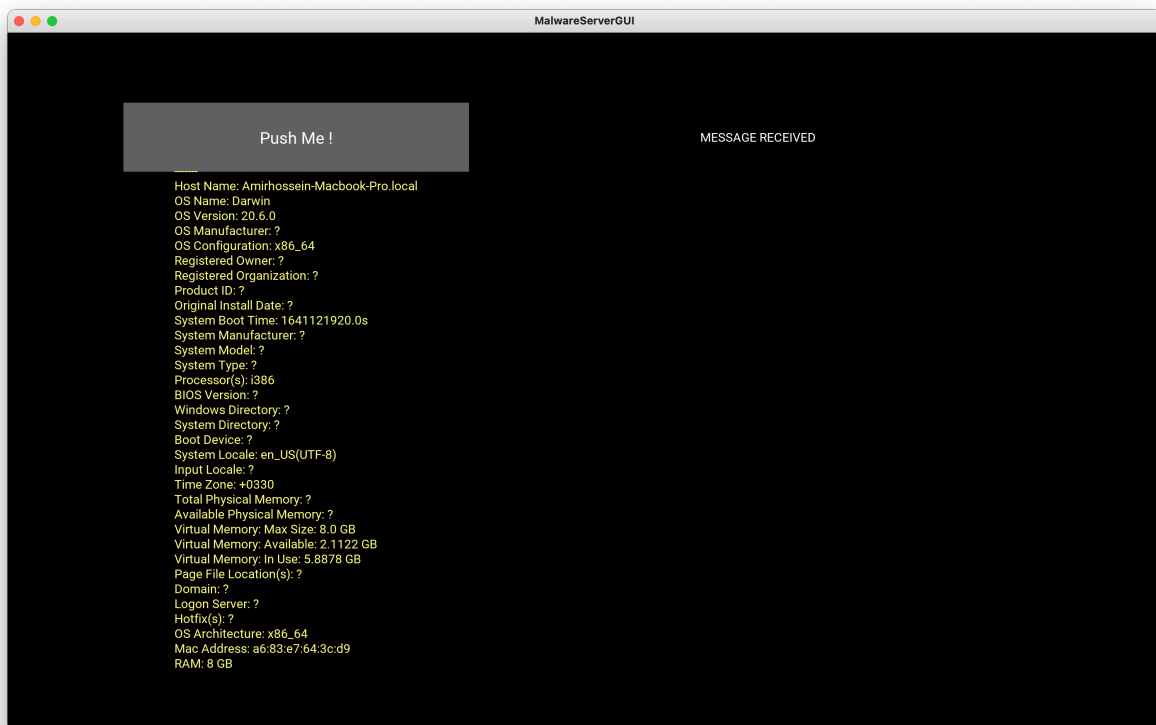
سایر بخش‌ها

طراحی واسط کاربری ابتدایی

برای سرور می‌توان به کمک کتابخانه‌ی kivy یک واسط کاربری ساده طراحی کرد. در ابتدا



با اجرا شدن بدافزار روی سیستم قربانی و فشردن دکمه اطلاعات خواسته شده نمایش داده می شود



تفاوت سیستم عامل‌ها

در ویندوز میتونم به کمک systeminfo تمام اطلاعات خواسته شده را دریافت کرد اما چنین دستوری در محیط یونیکس وجود ندارد و باید به کمک کتابخانه‌های مختلف اطلاعات را به دست آورد. در نتیجه می‌خواهیم در سیستم‌های ویندوزی از systeminfo و در سایر سیستم‌های عامل مانند گذشته عمل کنیم.

به کمک platform.system() میتوانیم سیستم عامل را تشخیص دهیم. خروجی برای ویندوز به صورت زیر می‌باشد:

```
Host Name:                Desktop-Guest10
OS Name:                  Microsoft Windows 10 Home Single Language
OS Version:               10.0.19042 N/A Build 19042
OS Manufacturer:         Microsoft Corporation
OS Configuration:        Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:         Asus
Registered Organization:   N/A
Product ID:                00342-41391-34007-AAOEM
Original Install Date:     2021-03-17, 10:45:43
System Boot Time:          2021-12-17, 02:33:36
System Manufacturer:       ASUS
System Model:              VivoBook Flip 14 TP410UF
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 142 Stepping 10 GenuineIntel ~1792 Mhz
BIOS Version:              American Megatrends Inc. TP410UF.305, 2019-06-05
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:                \Device\HarddiskVolume2
System Locale:              en-us;English (United States)
Input Locale:               en-us;English (United States)
Time Zone:                  (UTC+03:30) Tehran
Total Physical Memory:      16,267 MB
Available Physical Memory:  6,026 MB
Virtual Memory: Max Size:   21,387 MB
Virtual Memory: Available:  7,092 MB
Virtual Memory: In Use:     14,295 MB
Page File Location(s):      C:\pagefile.sys
```

برای سیستم‌عامل‌های دیگر نیز به صورت گذشته عمل می‌کنیم:

```
Host Name: Amirhossein-Macbook-Pro-Local
OS Name: Darwin
OS Version: 20.6.0
OS Manufacturer: ?
OS Configuration: x86_64
Registered Owner: ?
Registered Organization: ?
Product ID: ?
Original Install Date: ?
System Boot Time: 1641121920.0s
System Manufacturer: ?
System Model: ?
System Type: ?
Processor(s): 1386
BIOS Version: ?
Windows Directory: ?
System Directory: ?
Boot Device: ?
System Locale: en_US.UTF-8
Input Locale: ?
Time Zone: +0330
Total Physical Memory: ?
Available Physical Memory: ?
Virtual Memory: Max Size: 8.0 GB
Virtual Memory: Available: 2.2628 GB
Virtual Memory: In Use: 5.7972 GB
Page File Location(s): ?
Domain: ?
Logon Server: ?
Hotfix(s): ?
OS Architecture: x86_64
Mac Address: a6:83:e7:64:3c:d9
RAM: 8 GB
```