نام و نام خانوادگی: **امیرحسین علی‌بخشی**
شماره‌ی دانشجویی: **۹۷۳۱۰۹۶**

سیستم هکینگ

استاد: **دکتر شهریاری**
درس: **مبانی امنیت اطلاعات**

فهرست مطالب

بخش اول

برای پیاده‌سازی سرور از لینک زیر استفاده می‌کنیم.

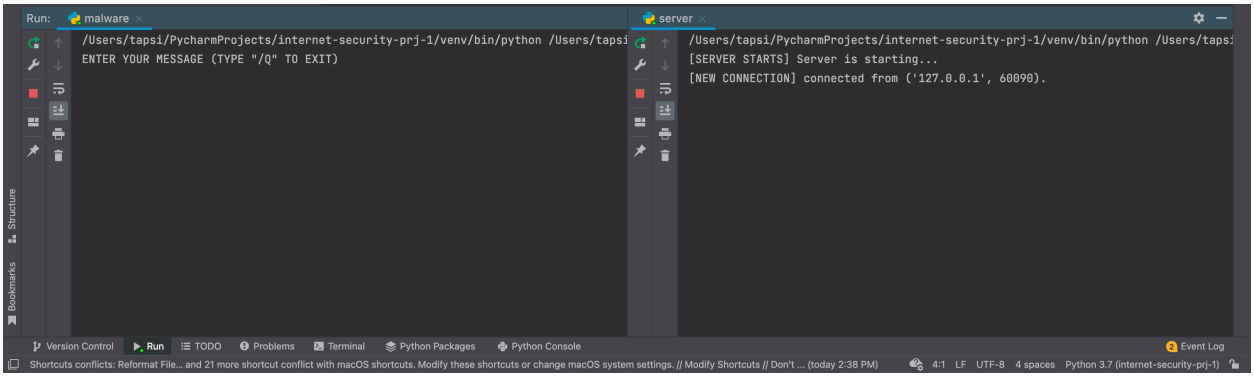
https://github.com/amir78729/python-TCP-client-server-template/blob/main/Server.py

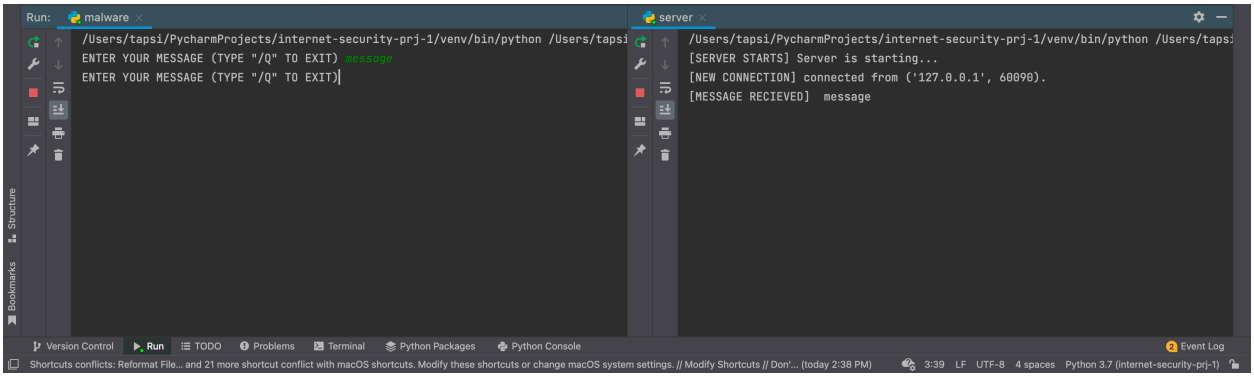
با اجرای سرور، منتظر کلاینت‌ها می‌مانیم:

برای پیاده‌سازی بدافزار نیز از لینک زیر استفاده می‌کنیم.

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

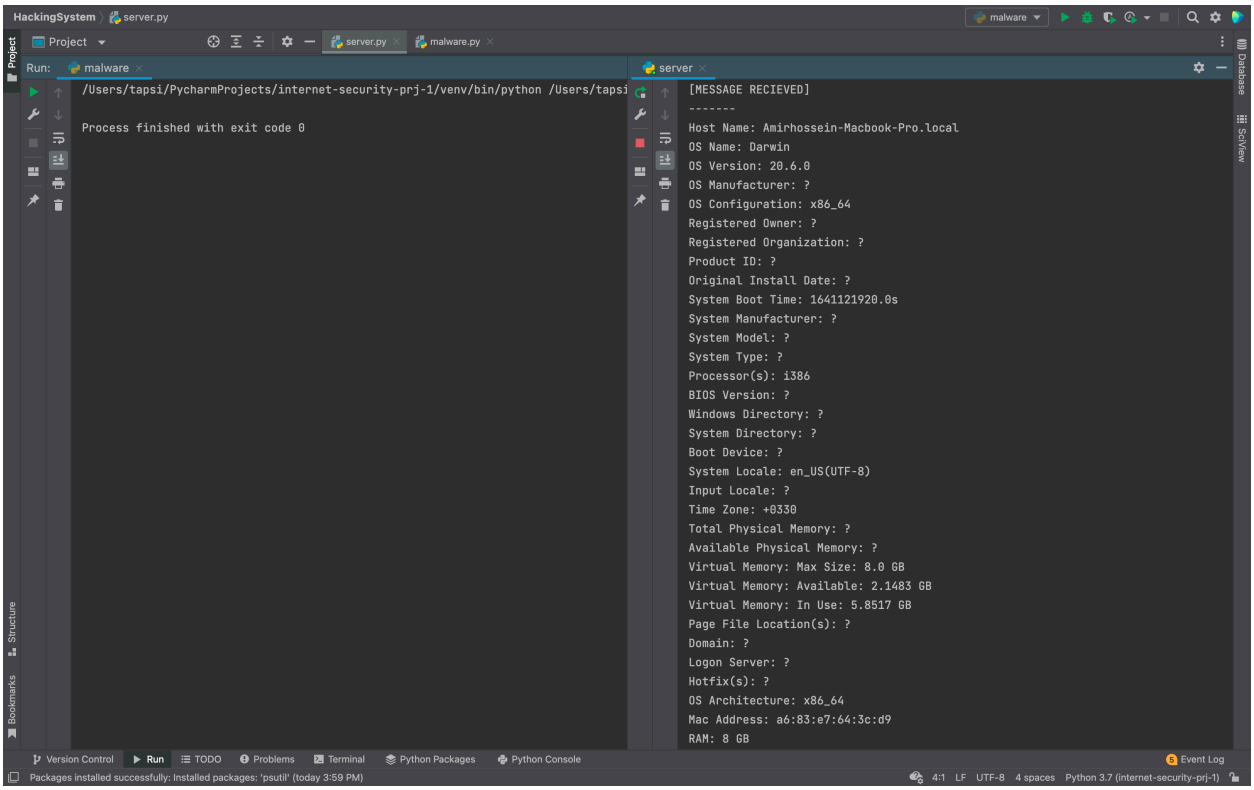
به محض اجرای بدافزار، سرور متوجه حضور او خواهد شد و کلاینت میتواند برای آن پیام ارسال نماید.





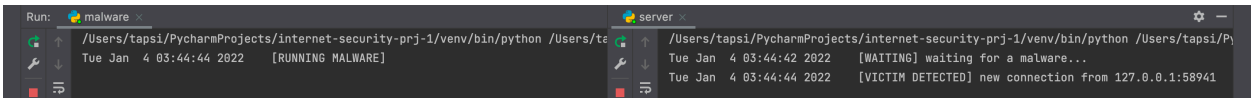
بخش دوم

به کمک کتاب‌خانه‌هایی مانند os، psutil، re،locale 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 نمی‌ایند و در ادامه سعی خواهیم کرد که این اطلاعات را تکمیل کنیم.

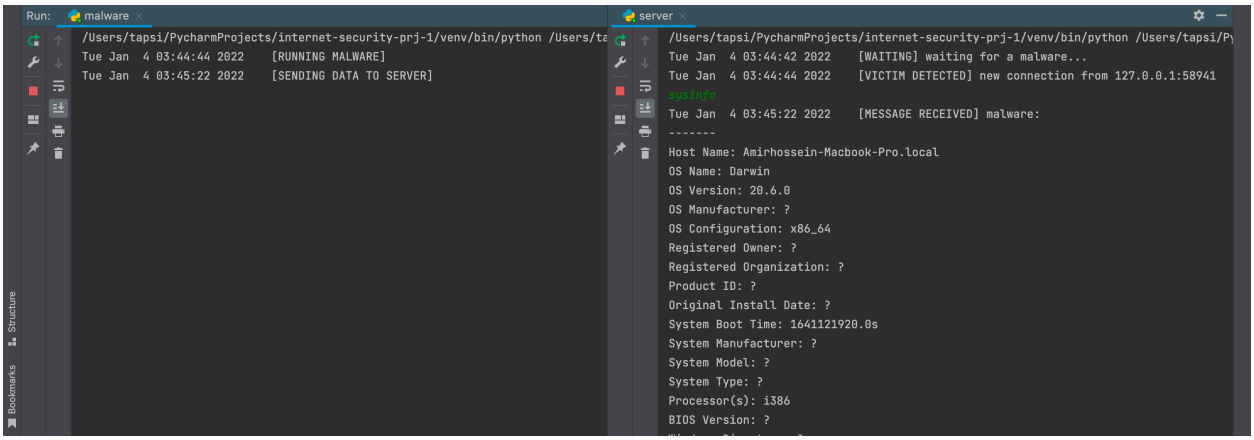


بخش سوم

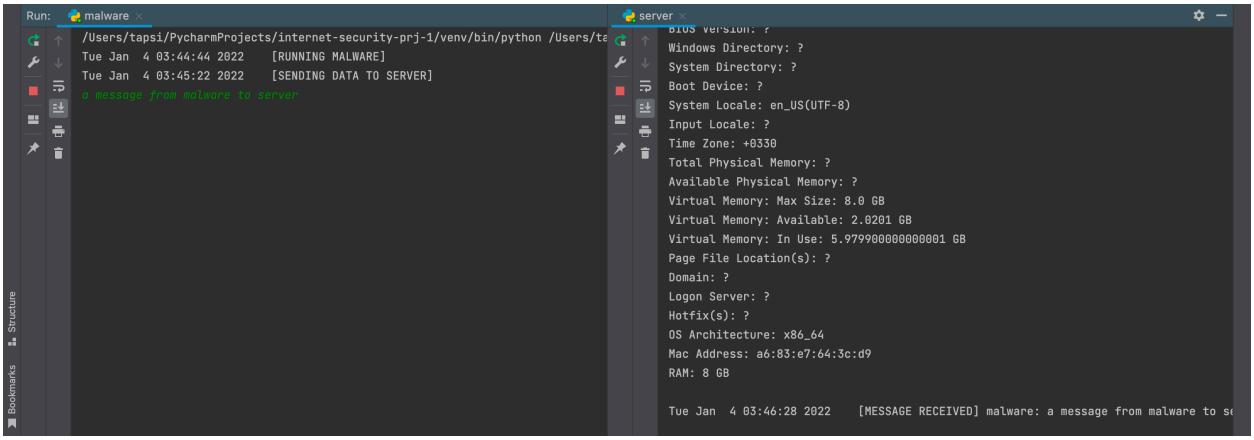
در این بخش باید وقتی بدافزار فعال شد پیامی در سرور نمایش داده شود.



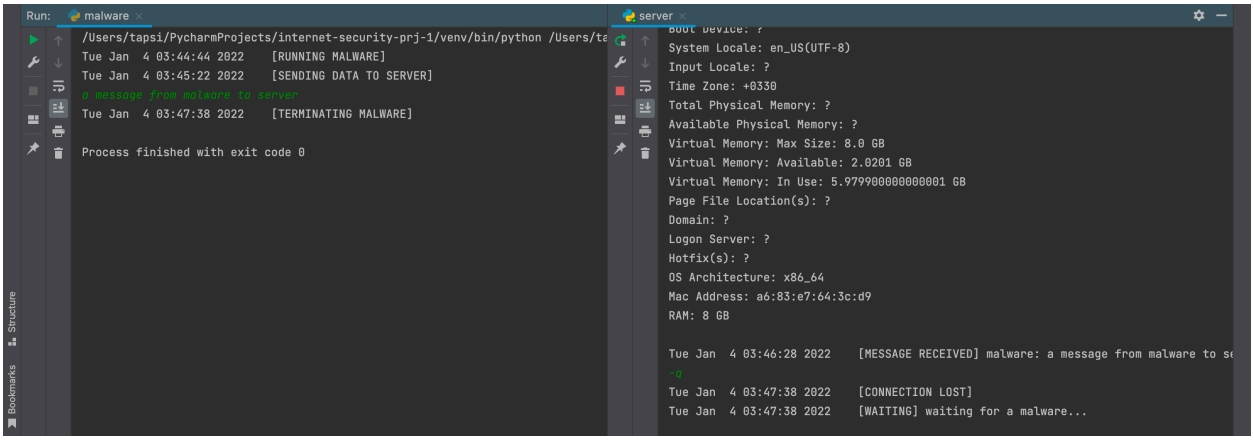
هنگامی که سرور ورودی sysinfo را وارد می‌کند، اطلاعات از سوی بدافزار برای سرور ارسال شود.



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



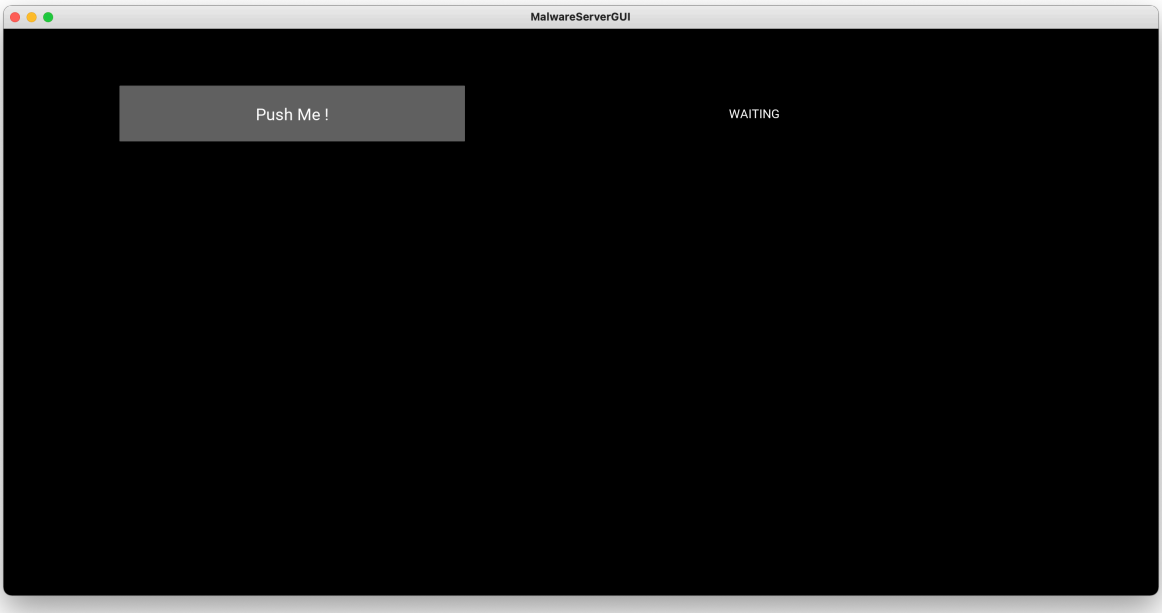
همچنین سرور می‌تواند با ارسال q- ارتباط با بدافزار فعلی را خاتمه دهد و منتظر بدافزارهای دیگر باشد.



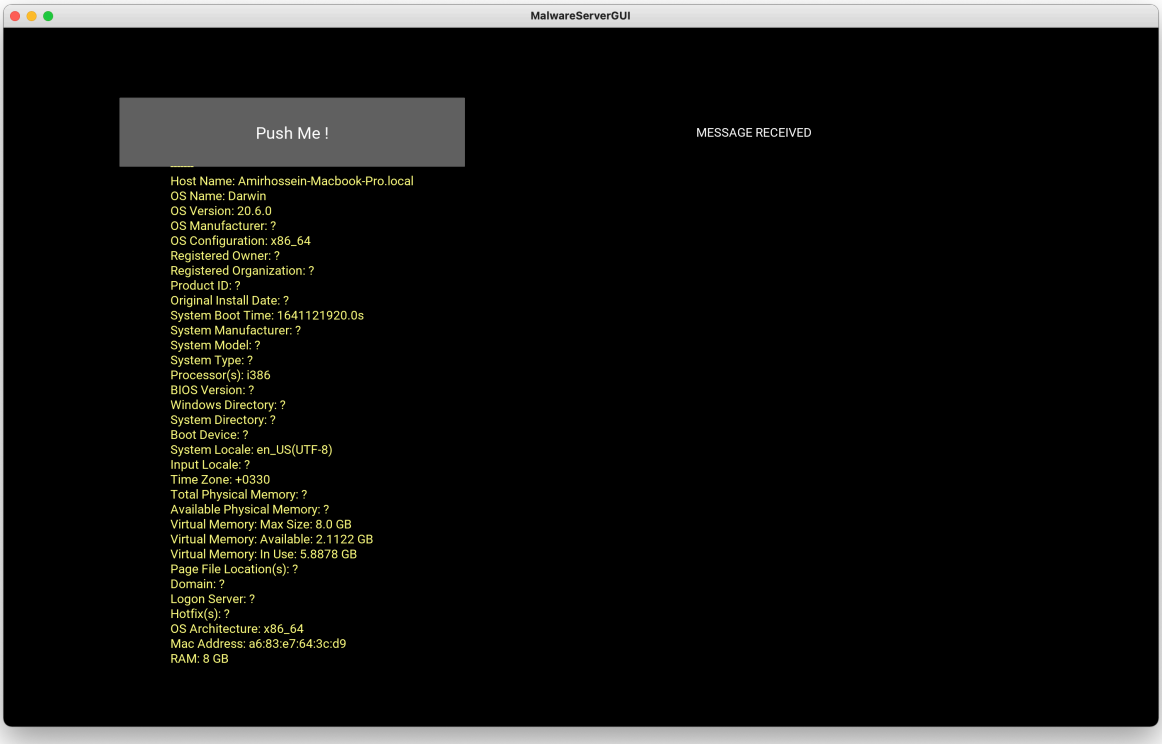
سایر بخش‌ها

طراحی واسط کاربری ابتدایی

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



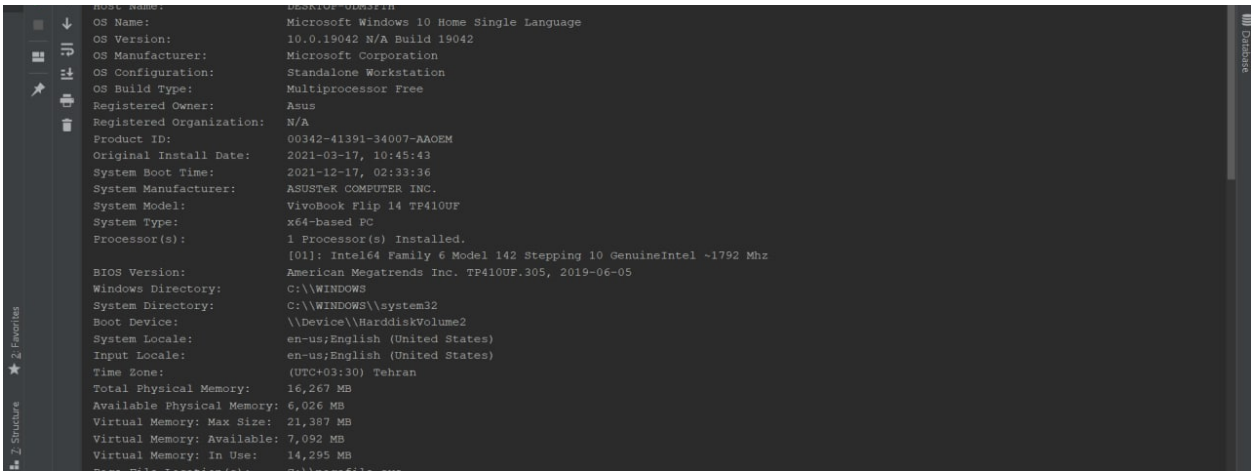
با اجرا شدن بدافزار روی سیستم قربانی و فشردن دکمه اطلاعات خواسته شده نمایش داده می‌شود



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:



برای سیستم‌عامل های دیگر نیز به صورت گذشته عمل می‌کنیم: