تمرین پنجم آزمایشگاه شبکه

سرویس های مخفی در تور

ارش محرابی

کد در گیت هاب:

https://github.com/arash-mehrabi-z/computer-networks-lab/tree/main/tor_hidden_service

سرور:

من برای یکی از تمرینات درس مهندسی اینترنت یک سرور HTTP با قابلیت امکان اتصال چند client به آن دولوپ کردم که از ریکوئست های GET و HEAD پشتیبانی می‌کند و برای این تمرین هم از آن استفاده می کنم. کدی که برای آن زده‌ام در دایرکتوری web_server موجود است.

اجرا کردن سرور به عنوان سرویس مخفی TOR:

برای این کار به دایرکتوری زیر رفته:

```
arash@arash-X450CC:/etc/tor$ whereis tor
tor: /usr/bin/tor /usr/sbin/tor /etc/tor /usr/share/tor /usr/share/man/man1/tor.1.gz
arash@arash-X450CC:/etc/tor$ cd /etc/tor/
arash@arash-X450CC:/etc/tor$ ls
torrc  torsocks.conf
arash@arash-X450CC:/etc/tor$
```

و فایل torrc را ویرایش می کنیم:

```
################ This section is just for location-hidden services ###

## Once you have configured a hidden service, you can look at the
## contents of the file ".../hidden_service/hostname" for the address
## to tell people.
##
## HiddenServicePort x y:z says to redirect requests on port x to the
## address y:z.

HiddenServiceDir /var/lib/tor/hidden_service/
HiddenServicePort 80 127.0.0.1:8080

#HiddenServiceDir /var/lib/tor/other_hidden_service/
#HiddenServicePort 80 127.0.0.1:80
#HiddenServicePort 22 127.0.0.1:22
```

و دو خط HiddenServiceDir و HiddenServicePort را uncomment می کنیم. همچنین پورت خروجی را از ۸۰ به یک مقدار دلخواه (در این مثال ۸۰۸۰) تغییر می دهیم.

بعد سرویس تور را آغاز می‌کنیم تا به همه درخواست های ورودی از پورت ۸۰ گوش کند و آن‌ها را به پورت ۸۰۸۰ localhost بفرستد.

حالا باید به دنبال یافتن آدرس ONION خود باشیم. برای این کار، کار های زیر را انجام می دهیم:

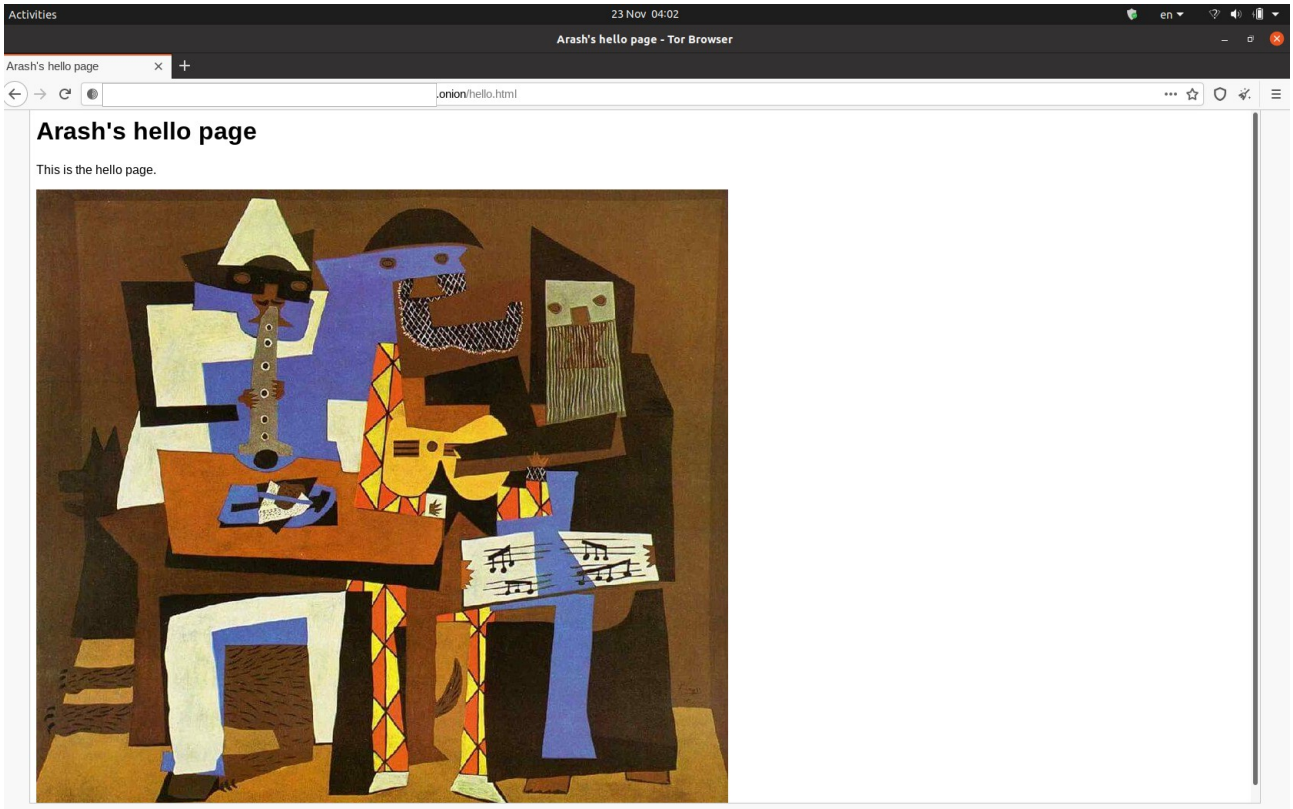
```
arash@arash-X450CC:/etc/tor$ sudo su
[sudo] password for arash:
root@arash-X450CC:/etc/tor# cd /var/lib/tor/hidden_service/
root@arash-X450CC:/var/lib/tor/hidden_service# ls
authorized_clients  hostname  hs_ed25519_public_key  hs_ed25519_secret_key
root@arash-X450CC:/var/lib/tor/hidden_service# cat hostname
```

و آدرسی که اکو می‌شود را یادداشت می کنیم.

حالا با run کردن سرورHTTP :

```
arash@arash-X450CC:~/learning/computer_networks_lab/assignment/cnl/tor_hidden_service/web_server$ python3 src/main.py
Listening at ('127.0.0.1', 8080)
```

و با وارد کردن آدرس ONION می‌بینیم که تور موفق شد به سرور ریکوئست HTTP بزند و جوابش را بگیرد.



اتفاقی که افتاده در حقیقت این است که به وسیله ۶ واسط، برازر تور به وب سروری که در ماشین من اجرا می‌شود یک ریکوئست GET زده (حتی با اینکه من آدرس IP Valid ندارم) و توانسته جوابش را بگیرد.

ریکوئست با script به وسیله SOCKS5 :

برای اینکه به وسیله کد و با SOCKS5 در پایتون بتوانیم ریکوئست بزنیم کافی است از کتابخانه requests استفاده کنیم. یک session درست می‌کنیم و دو تا پراکسی socks5 را به این صورت روی پورت های TOR تنظیم می کنیم:

```
session = requests.session()
session.proxies = {}
session.proxies['http'] = 'socks5h://localhost:9050'
session.proxies['https'] = 'socks5h://localhost:9050'

r = session.get('PUT_YOUR_ONION_ADDRESS_HERE')
print(r.content)
```

سپس به آدرس ONION مورد نظر request می‌زنیم. در این مثال نتیجه چنین است:

```
arash@arash-X450CC:~/learning/computer_networks_lab/assignment/cnl/tor_hidden_service$ python3 connect_to_hidden_service.py
b'<html>\n    <head>\n        <title>Arash\'s hello page</title>\n    </head>\n    <body>\n        <h1>Arash\'s hello page</h1>\n        <p>This is the hello page.</p>\n
    <img src="three-musicians.jpg">\n    </body>\n</html>'
arash@arash-X450CC:~/learning/computer_networks_lab/assignment/cnl/tor_hidden_service$
```

که می‌بینیم که با موفقیت جواب HTML لازم را دریافت کرده است.