

به نام خالق سبز بهاران



پروژه اول

شبکه‌های کامپیوتری

نیم‌سال دوم ۱۴۰۰ - ۱۴۰۱

دانشکده‌ی برق و کامپیوتر

دانشگاه صنعتی اصفهان

اسفند ماه ۱۴۰۰

استاد درس:

جناب آقای دکتر حیدرپور

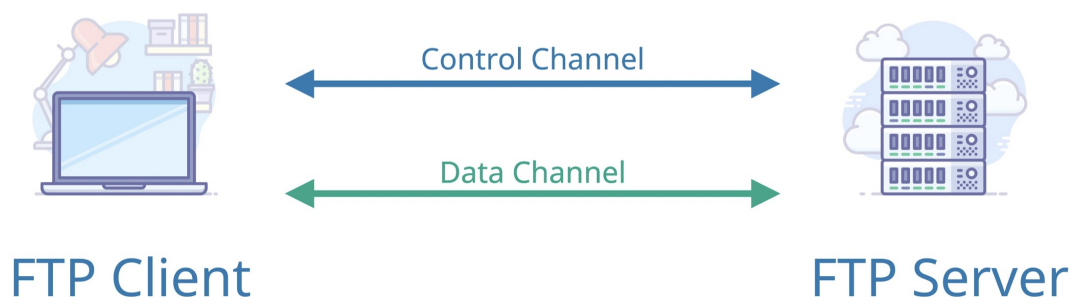
طراحان پروژه:

علی علایی - ساجده نیک نداف - محمدمهدی برقی - محمد جلالی

در این تکلیف قرار است با استفاده از برنامه نویسی سوکت با پایتون که در کلاس آموزش دیده اید یک کلاینت و سرور برای نسخه ای ساده شده از FTP پیاده سازی کنید.

۱ مقدمه ای بر پروتکل FTP

FTP مخفف File Transfer Protocol یک پروتکل در لایه ی کاربرد برای انتقال فایل است. این پروتکل شباهت های زیادی با HTTP دارد مثلاً هر دو از TCP به عنوان پروتکل لایه انتقال استفاده می کنند. اما مهم ترین اختلاف آن ها در این است که FTP از دو ارتباط موازی برای عملکرد خود استفاده می کند (به شکل ۱ توجه کنید):



شکل ۱: نحوه عملکرد پروتکل FTP

۱. کانال کنترلی (Control Channel): این ارتباط یک ارتباط کنترلی است که در ابتدا ایجاد می شود و وظیفه ی آن احراز هویت، ارسال لیست محتوای موجود در directory و سایر دستورات کنترلی است.

۲. کانال داده (Data Channel): این ارتباط برای دریافت و ارسال فایل ها بین سرور و کلاینت ایجاد می شود.

به همین دلیل که FTP دستورات کنترلی خود را روی یک ارتباط جداگانه می فرستد، گفته می شود که اطلاعات کنترلی را خارج از باند (out-of-bound) می فرستد. در صورتی که همان طور که می دانید، دستورات request و response در پروتکل HTTP روی همان ارتباطی منتقل می شود که انتقال فایل با آن انجام می شود. به همین دلیل گفته می شود که HTTP اطلاعات کنترلی خود را در داخل باند (in-bound) ارسال می کند.

۲ کلاینت

برنامه ی کلاینت پس از اجرا باید به سرور متصل شود. سپس شروع به دریافت دستورات کاربر و ارسال آن ها به سرور کند. در زیر لیست دستوراتی که باید پیاده سازی شوند نمایش داده شده است :

۱. HELP : نمایش لیست دستورات (۵ نمره)

۲. LIST : برای دریافت لیست فایل ها و سایز هر فایل (۲۰)

در پایان مجموع سایز کل فایل های موجود در فولدر فعلی نمایش داده می شود.
فولدر ها با علامت > در ابتدای نامشان مشخص می شوند .

۳. DWLD fileName : برای دانلود فایل "filePath" از روی سرور (۲۵ نمره)

۴. PWD : نمایش مکان فعلی ما در سرور (۱۰ نمره)

۵. CD dirName : برای باز کردن فولدر "dirName" (۱۰ نمره)

۳ سرور

ابتدا یک پوشه برای سرور ایجاد کنید و داخل آن موارد زیر را قرار دهید:

۱. یک فایل با نام server.py که در آن برنامه ی سرور را می نویسید.

۲. یک فایل با نام hi.txt که متن دلخواهی داخل آن نوشته اید.

۳. یک فولدر با نام dir1 که داخل آن موارد زیر قرار دارد :

(آ) به انتخاب خودتان، یک تصویر به اسم img.png با حجم حدود یک مگابایت یا یک فایل یک مگابیتی به اسم bigFile.bin که به روش زیر می توانید تولید کنید :
windows : عبارت زیر را داخل cmd اجرا کنید

```
> fsutil file createnew bigFile.bin 1048576
```

mac و linux : عبارت زیر را داخل shell اجرا کنید

```
> dd if=/dev/zero of=bigFile.bin bs=1048576 count=1
```

(ب) یک فولدر با نام inner که داخل آن یک فایل دیگر با نام test وجود دارد و محتوای آن به دلخواه خودتان است.

برنامه سرور شما باید پس از اجرا، یک سوکت روی آدرس 127.0.0.1 و پورت 2121 ایجاد کرده و روی این پورت شنود کند تا کلاینت به آن متصل شود.

پس از اتصال کلاینت ، باید منتظر ارسال دستور از طرف کلاینت بماند و به آن پاسخ مناسب دهد. چنانچه درخواست برای دانلود یک فایل بود، سرور ابتدا یک عدد تصادفی بین 3000 تا 50000 به عنوان شماره پورت برای کانال داده ایجاد می کند و یک سوکت TCP روی آن ایجاد کرده و همین عدد را برای کلاینت هم می فرستد و منتظر می شود تا کلاینت به آن متصل شود. پس از اتصال

کلاینت، کل فایل درخواستی را به صورت یک جا (و نه قطعه قطعه) برای کلاینت ارسال می کند. توجه شود که این ارتباط باید به صورت ناپایدار (nonpersistent) باشد و پس از ارسال فایل بسته شود.

سوال : چرا این روند برعکس نیست یعنی کلاینت یک پورت را باز نمی کند و آن را به سرور اطلاع دهد و سرور فایل را روی آن

پورت برای کلاینت ارسال کند؟ (۵ نمره) **chon client Firewall darad vali server nadarad**

پس از نوشتن کد های سرور و کلاینت هر دو را اجرا کنید و برای هر دستور از خروجی ها اسکرین شات تهیه کنید و در فایل پاسخ نامه به همراه جواب سوال ها قرار دهید.

توجه : در راستای درک بهتر عملکرد مورد انتظار، نمونه ای از اجرای این سیستم و خروجی های مناسب در فیلم اجرای پروژه نشان داده شده است.

نمره اضافه : تمام request bad های زیر را سمت سرور مدیریت کنید و پیغام خروجی مناسب سمت کلاینت نمایش دهید. (۱۰ نمره)

۱. تمام ورودی هایی با فرمت و شکل نامناسب که به هر شکلی میتوانند باعث عدم اجرای صحیح برنامه و قطع اجرای آن شوند.

۲. ورودی هایی برای دستورات CD و DWLD که باعث شود فایلی دانلود شود یا فولدري باز شود که در زیرشاخه های فولدر

اصلی سرور قرار ندارد. (مثل فایل های سیستم عامل)

این حمله چه نام دارد؟ **Path Traversal Attack**

۴ آشنایی و کار با Wireshark

ابتدا با استفاده از این لینک ، وایرشارک را نصب کنید و با کارایی آن آشنا شوید و سپس به سوالات زیر پاسخ دهید :

۱. وایرشارک را باز کرده و capture کردن بسته های loopback را آغاز کنید. سپس ابتدا سرور و سپس کلاینت را اجرا کنید. به وایرشارک برگردید و از سه بسته ای که برای handshaking پروتکل TCP ارسال شده اسکرین شات بگیرید (برای این که فقط بسته های TCP را ببینید میتوانید کلمه ی tcp را در نوار فیلتر وارد کنید). (۱۰ نمره)

توجه : اگر از سیستم عامل windows استفاده میکنید، ممکن است نتوانید بسته های loopback را capture و مشاهده کنید. برای حل این مشکل پس از نصب وایرشارک باید فایل RawCap.exe که برای شما قرار داده شده را روی سیستم خود کپی کنید سپس یکی از روش های زیر را استفاده کنید:

(آ) در محل فایل RawCap.exe دستور زیر را در cmd وارد کنید:

```
> RawCap.exe -q 127.0.0.1 - | "C:\Program Files\Wireshark\Wireshark.exe" -i - -k
```

اگر وایرشارک را در محل دیگری نصب کرده اید آدرس فایل اجرایی آن را به جای "C:\..." قرار دهید.

(ب) در محل فایل RawCap.exe دستور زیر را در cmd وارد کنید:

```
> RawCap.exe 127.0.0.1 \\.\pipe\RawCap
```

بعد از آن وایرشارک را اجرا کنید و در قسمت capture ، قسمت options روی گزینه ی Manage Interfaces کلیک کرده و در بخش Pipes گزینه ی افزودن را انتخاب کنید و یک named pipe به اسم \\.\pipe\RawCap ایجاد کرده و تغییرات را ذخیره کنید.

۲. (آ) آیا TCP محدودیتی برای اندازه بسته‌ها دارد؟ فایل‌های بزرگ چگونه توسط سوکت TCP ارسال میشوند؟ (۵ نمره)

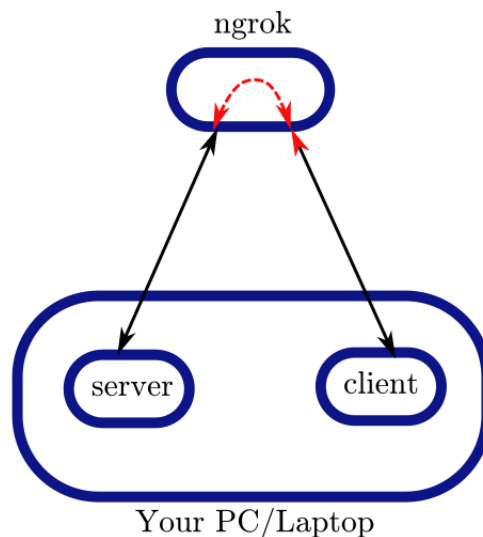
(ب) برای مشاهده‌ی عملی جواب قسمت قبل، ابتدا وایرشارک را روشن کنید و سپس در کلاینت درخواست دانلود فایل

bigFile.txt را بدهید. از نتایج وایرشارک اسکرین‌شات بگیرید. TCP برای دانلود این فایل چند بسته فرستاده است؟ (۱۰ نمره)

(نمره)

۵ استفاده از ابزار ngrok

در این بخش با استفاده از سامانه ngrok می‌خواهیم به جای اتصال کلاینت به سرور به صورت محلی (استفاده از loopback) از یک آدرس IP عمومی استفاده کنیم که توسط سامانه ngrok در اختیار سرور قرار می‌گیرد تا کلاینت‌ها بتوانند از هر جایی به سرور متصل شوند. در این حالت ساختار اتصال بین کلاینت و سرور به صورت زیر است: (شکل ۲)



شکل ۲: ساختار اتصالات ngrok

برای آشنایی و نحوه کار با ngrok به فایل مربوطه که در مجموعه فایل‌های این پروژه موجود است مراجعه فرمایید. از آنجایی که شما در طی پروژه دو کانال ارتباطی دارید طبق مراحل که در ادامه ذکر می‌شود پیش بروید:

۱. ابتدا کانال کنترلی را از طریق ngrok ایجاد نمایید. و دستورات HELP, LIST, PWD و CD را از طریق کلاینت و سرور متصل شده به ngrok اجرا کنید. (۱۵ نمره)

۲. مجدداً مراحل مربوط به قسمت ۱.۴ را تکرار کنید (به جای آدرس loopback باید از آدرس IP ای که سرور به آن متصل است و ارسال و دریافت پکت‌ها از طریق آن انجام می‌شود، استفاده کنید) و در نهایت به همراه تصاویر و توضیحات تفاوت با حالتی که از ngrok استفاده نشده بود را توضیح دهید. (۱۰ نمره)

۳. در مرحله بعد شرایط دانلود فایل‌ها از طریق ایجاد کانال داده با ngrok را ایجاد کنید. آیا این کار ممکن است؟ اگر بله چگونه

و اگر خیر چه مشکلی وجود دارد؟
 kheyr , chon dar tabe'e DWLD darim yek port jadid misazim va bayad be ngrok fahmund ke port jadid (random port az 3000 ta 50000) ro baraye client befreste.

راهکار خود را برای حل این مشکل توضیح دهید (نیازی به پیاده سازی عملی راه حل نیست و نمره امتیازی دارد) (۱۰ + ۱۰)

نمره امتیازی)
 dar tabe'e DWLD yetori ngrok ro run konim va az ghesmate "wab interface" arguman haye host va port ro baraye client befrestim ta client betune host va port khodesh ro barabar ba in 2 meghdar gharar bede va download shekl begire.

۶ شیوه تحویل

برای این تمرین می بایست یک پوشه به نام studentid_prog1 بسازید (به جای studentid باید شماره دانشجویی خود را قرار دهید) که شامل دو فایل زیر باشد:

۱. یک فایل pdf: شامل پاسخ به تمام سوالات (ترجیحا به زبان فارسی) و اسکرین شات های خواسته شده

۲. یک پوشه با نام Source که در آن یک پوشه برای کلاینت و یک پوشه برای سرور قرار دارد و کد های پایتون سرور و کلاینت داخل فولدر های مربوطه هستند.

در نهایت این فایل ها را فشرده کنید و یک فایل با نام studentid_prog1 و فرمت zip یا rar در سامانه یکتا ارسال کنید.

موفق باشید.