**آشنائی با پروتکل FTP ( بخش اول )**

امروزه از پروتکل های متعددی در شبکه های کامپیوتری استفاده می گردد که صرفا" تعداد اندکی از آنان به منظور انتقال داده طراحی و پیاده سازی شده اند . اینترنت نیز به عنوان يك شبکه گسترده از این قاعده مستثنی نبوده و در این رابطه از پروتکل های متعددی استفاده می شود.

برای بسیاری از کاربران اینترنت همه چیز محدود به وب و پروتکل مرتبط با آن یعنی HTTP است ، در صورتی که در این عرصه از پروتکل های متعدد دیگری نیز استفاده می گردد. FTP نمونه ای در این زمینه است .

## پروتکل FTP چیست ؟

تصویر اولیه اینترنت در ذهن بسیاری از کاربران، استفاده از منابع اطلاعاتی و حرکت از سایتی به سایت دیگر است و شاید به همین دلیل باشد که اینترنت در طی سالیان اخیر به سرعت رشد و متداول شده است . بسیاری از کارشناسان این عرصه اعتقاد دارند که اینترنت گسترش و عمومیت خود را مدیون سرویس وب می باشد .

فرض کنید که سرویس وب را از اینترنت حذف نمائیم . برای بسیاری از ما این سوال مطرح خواهد شد که چه نوع استفاده ای را می توانیم از اینترنت داشته باشیم ؟ در صورت تحقق چنین شرایطی ، یکی از عملیاتی که کاربران قادر به انجام آن خواهند بود ، دریافت داده ، فایل های صوتی ، تصویری و سایر نمونه فایل های دیگر با استفاده از پروتکل FTP (برگرفته از Transfer File Protocol ) است.

## ویژگی های پروتکل FTP

- پروتکل FTP ، اولین تلاش انجام شده برای ایجاد يك استاندارد به منظور مبادله فایل بر روی شبکه های مبتنی بر پروتکل TCP/IP است که از اوایل سال ۱۹۷۰ مطرح و مشخصات استاندارد آن طی RFC 959 در اکتبر سال ۱۹۸۵ ارائه گردید .
- پروتکل FTP دارای حداکثر انعطاف لازم و در عین حال امکان پذیر به منظور استفاده در شبکه های مختلف با توجه به نوع پروتکل شبکه است .
- پروتکل FTP از مدل سرویس گیرنده - سرویس دهنده تبعیت می نماید . برخلاف HTTP که يك حاکم مطلق در عرصه مرورگرهای وب و سرویس دهندگان وب است ، نمی توان ادعای مشابهی را در رابطه با پروتکل FTP داشت و هم اینك مجموعه ای گسترده از سرویس گیرندگان و سرویس دهندگان FTP وجود دارد .
- برای ارسال فایل با استفاده از پروتکل FTP به يك سرویس گیرنده FTP نیاز می باشد . ویندوز دارای يك برنامه سرویس گیرنده FTP از قبل تعبیه شده می باشد ولی دارای محدودیت های مختص به خود می باشد . در این رابطه نرم افزارهای متعددی تاکنون طراحی و پیاده سازی شده است:

ulletProof FTP ، WS FTP Professional، FTP Explorer و Smart FTP نمونه هائی در این زمینه می باشند .

- پروتکل FTP را می توان به عنوان یك سیستم پرس وجو نیز تلقی نمود چراکه سرویس گیرندگان و سرویس دهندگان گفتگوی لازم به منظور تائید یکدیگر و ارسال فایل را انجام می دهند. علاوه بر این، پروتکل فوق مشخص می نماید که سرویس گیرنده و سرویس دهنده، داده را بر روی کانال گفتگو ارسال نمی نمایند . در مقابل ، سرویس گیرنده و سرویس دهنده در خصوص نحوه ارسال فایل ها بر روی اتصالات مجزا و جداگانه ( یك اتصال برای هر ارسال داده ) با یکدیگر گفتگو خواهند کرد ( نمایش لیست فایل های موجود در یك دایرکتوری نیز به عنوان یك ارسال فایل تلقی می گردد ) .
- پروتکل FTP امکان استفاده از سیستم فایل را مشابه پوسته یونیکس و یا خط دستور ویندوز در اختیار کاربران قرار می دهد .
- سرویس گیرنده در ابتدا یك پیام را برای سرویس دهنده ارسال و سرویس دهنده نیز به آن پاسخ خواهد داد و در ادامه ارتباط غیرفعال می گردد . وضعیت فوق با سایر پروتکل هائی که به صورت تراکنشی کار می کنند ، متفاوت می باشد ( نظیر پروتکل HTTP ) . برنامه های سرویس گیرنده زمانی قادر به شبیه سازی یك محیط تراکنشی می باشند که از مسائلی که قرار است در آینده محقق شوند ، آگاهی داشته باشند . در واقع ، پروتکل FTP یك دنباله stateful از یك و یا چندین تراکنش است.
- سرویس گیرندگان ، مسئولیت ایجاد و مقداردهی اولیه درخواست ها را برعهده دارند که با استفاده از دستورات اولیه FTP انجام می گردد. دستورات فوق ، عموما" سه و یا چهار حرفی می باشند (مثلا" برای تغییر دایرکتوری از دستور CWD استفاده می شود ). سرویس دهنده نیز بر اساس یك فرمت استاندارد به سرویس گیرندگان پاسخ خواهد داد ( سه رقم که به دنبال آن از space استفاده شده است به همراه یك متن تشریحی ) . سرویس گیرندگان می بایست صرفا" به کد عددی نتیجه استناد نمایند چراکه متن تشریحی تغییر پذیر بوده و در عمل برای اشکال زدائی مفید است ( برای کاربران حرفه ای ) .
- پروتکل FTP دارای امکانات حمایتی لازم برای ارسال داده با نوع های مختلف می باشد . دو فرمت متداول، اسکی برای متن ( سرویس گیرنده با ارسال دستور TYPE A ،موضوع را به اطلاع سرویس دهنده می رساند ) و image برای داده های باینری است ( توسط TYPE I مشخص می گردد) . ارسال داده با فرمت اسکی در مواردی که ماشین سرویس دهنده و ماشین سرویس گیرنده از استانداردهای متفاوتی برای متن استفاده می نمایند ، مفید بوده و یك سرویس گیرنده می تواند پس از دریافت داده آن را به فرمت مورد نظر خود ترجمه و استفاده نماید . مثلا" در نسخه های ویندوز از یك دنباله carriage return و linefeed برای نشان دادن انتهای خط استفاده می گردد در صورتی که در سیستم های مبتنی بر یونیکس صرفا" از یك linefeed استفاده می شود . برای ارسال هرنوع داده که به ترجمه نیاز نداشته باشد،می توان از ارسال باینری استفاده نمود.
- اتخاذ تصمیم در رابطه با نوع ارسال فایل ها در اختیار سرویس گیرنده است ( برخلاف HTTP که می تواند به سرویس گیرنده نوع داده ارسالی را اطلاع دهد ) . معمولا" سرویس گیرندگان ارسال باینری را انتخاب می نمایند و پس از دریافت فایل ، ترجمه لازم را انجام خواهند داد . ارسال باینری ذاتا" دارای کارآئی بیشتری است چراکه سرویس دهنده و

سرویس گیرنده نیازی به انجام تراکنش های on the fly نخواهند داشت . ارسال اسکی گزینه پیش فرض انتخابی توسط پروتکل FTP است و در صورت نیاز به ارسال باینری ، سرویس گیرنده می بایست این موضوع را از سرویس دهنده درخواست نماید .

- یك اتصال پروتکل TCP/IP ( نسخه شماره چهار) شامل دو نقطه مجزا می باشد که هر نقطه از یك آدرس IP و یك شماره پورت استفاده می نماید . برقراری ارتباط بین یك سرویس گیرنده و یك سرویس دهنده منوط به وجود چهار عنصر اطلاعاتی است : آدرس سرویس دهنده ،پورت سرویس دهنده ، آدرس سرویس گیرنده و پورت سرویس گیرنده . در زمان برقراری یك ارتباط ، سرویس گیرنده از یك شماره پورت استفاده می نماید . این شماره پورت می تواند متناسب با نوع عملکرد برنامه سرویس گیرنده به صورت اختیاری و یا اجباری باشد . مثلا" برخی برنامه های سرویس گیرنده به منظور ارتباط با سرویس دهنده ، نیازمند استفاده از یك شماره پورت خاص می باشند ( نظیر برنامه های سرویس گیرنده وب و یا مرورگرهای وب که از پورت شماره ۸۰ به منظور ارتباط با سرویس دهنده وب استفاده می نماید) . در مواردی که الزامی در خصوص شماره پورت وجود ندارد از یك شماره پورت موقتی و یا ephemeral استفاده می گردد . این نوع پورت ها موقتی بوده و توسط IP stack ماشین مربوطه به متقاضیان نسبت داده شده و پس از خاتمه ارتباط ، پورت آزاد می گردد . با توجه به این که اکثر IP Stacks بلافاصله از پورت موقت آزاد شده استفاده نخواهند کرد ( تا زمانی که تمام pool تکمیل نشده باشد ) ،در صورتی که سرویس گیرنده مجددا" درخواست برقراری یك ارتباط را نماید ، یك شماره پورت موقتی دیگر به وی تخصیص داده می شود .
- پروتکل FTP منحصرا" از پروتکل TCP استفاده می نماید( هرگز از پروتکل UDP استفاده نمی شود) . معمولا" پروتکل های لایه Application ( با توجه به مدل مرجع OSI ) از یکی از پروتکل های TCP و یا UDP استفاده می نمایند ( به جزء پروتکل DNS ) . پروتکل FTP نیز از برخی جهات شرایط خاص خود را دارد و برای انجام وظایف محوله از دو پورت استفاده می نماید . این پروتکل معمولا" از پورت شماره ۲۰ برای ارسال داده و از پورت ۲۱ برای گوش دادن به فرامین استفاده می نماید . توجه داشته باشید که برای ارسال داده همواره از پورت ۲۰ استفاده نمی گردد و ممکن است در برخی موارد از پورت های دیگر استفاده شود .
- اکثر سرویس دهندگان FTP از روش خاصی برای رمزنگاری اطلاعات استفاده نمی نمایند و در زمان login سرویس گیرنده به سرویس دهنده ، اطلاعات مربوط به نام و رمز عبور کاربر به صورت متن معمولی در شبکه ارسال می گردد . افرادی که دارای یك Packet sniffer بین سرویس گیرنده و سرویس دهنده می باشند ، می توانند به سادگی اقدام به سرقت نام و رمز عبور نمایند . علاوه بر سرقت رمزهای عبور ، مهاجمان می توانند تمامی مکالمات بر روی اتصالات FTP را شنود و محتویات داده های ارسالی را مشاهده نمایند . پیشنهادات متعددی به منظور ایمن سازی سرویس دهنده FTP مطرح می گردد ولی تا زمانی که رمزنگاری و امکانات حفاظتی در سطح لایه پروتکل IP اعمال نگردد ( مثلا" رمزنگاری توسط IPsecs ) ، نمی بایست از FTP استفاده گردد خصوصا" اگر بر روی شبکه اطلاعات مهم و حیاتی ارسال و یا دریافت می گردد .

- همانند بسیاری از پروتکل های لایه Application ، پروتکل FTP دارای کدهای وضعیت خطاء مختص به خود می باشد ( همانند HTTP ) که اطلاعات لازم در خصوص وضعیت ارتباط ایجاد شده و یا درخواستی را ارائه می نماید . زمانی که یك درخواست ( PUT , GET ) برای یك سرویس دهنده FTP ارسال می گردد ، سرویس دهنده پاسخ خود را به صورت یك رشته اعلام می نماید . اولین خط این رشته معمولا" شامل نام سرویس دهنده و نسخه نرم افزار FTP است .در ادامه می توان دستورات GET و یا PUT را برای سرویس دهنده ارسال نمود . سرویس دهنده با ارائه یك پیام وضعیت به درخواست سرویس گیرندگان پاسخ می دهد . کدهای وضعیت برگردانده شده را می توان در پنج گروه متفاوت تقسیم نمود :

کدهای xx۱ : پاسخ اولیه

کدهای xx۲ : درخواست بدون خطاء اجراء گردید .

کدهای xx۳ : به اطلاعات بشتری نیاز است .

کدهای xx٤ : یك خطاء موقت ایجاد شده است .

کدهای xx٥ : یك خطاء دائمی ایجاد شده است .

متداولترین کدهای وضعیت FTP به همراه مفهوم هریك در جدول زیر نشان داده شده است :

| سری ۱۰۰ کدهای وضعیت | |
|---|---|
| 110 | Restart reply |
| 120 | Service ready in x minutes |
| 125 | Connection currently open, transfer starting |
| 150 | File status okay, about to open data |
| 200 سری کدهای وضعیت | |
| 200 | Command okay |
| 202 | Command not implemented, superfluous at this site |
| 211 | System status/help reply |
| 212 | Directory status |

| | |
|---|---|
| 213 | File status |
| 214 | System Help message |
| 215 | NAME system type |
| 220 | Service ready for next user. |
| 221 | Service closing control connection. Logged off where appropriate |
| 225 | Data connection open; no transfer in progress. |
| 226 | Closing data connection. Requested action successful |
| 227 | Entering Passive Mode |
| 230 | User logged in, continue |
| 250 | Requested file action okay, completed |
| 257 | "PATHNAME" created. |
| سری کدهای وضعیت 300 | |
| 331 | User name okay, need password. |
| 332 | Need account for login |
| 350 | Requested file action pending further information. |
| سری کدهای وضعیت 400 | |
| 421 | Service not available, closing control connection. |
| 425 | Can't open data connection |
| 426 | Connection closed; transfer aborted. |

| | |
|---|---|
| 450 | Requested file action not taken. File not available - busy etc.. |
| 451 | Request aborted: error on server in processing. |
| 452 | Requested action not taken. Insufficient resources on system |
| 500 سری کدهای وضعیت | |
| 500 | Syntax error, command unrecognized |
| 501 | Syntax error in parameters or arguments. |
| 502 | Command not implemented. |
| 503 | Bad sequence of commands |
| 504 | Command not implemented for that parameter. |
| 530 | Not logged in. |
| 532 | Need account for storing files |
| 550 | Requested action not taken. File unavailable |
| 552 | Requested file action aborted. Exceeded storage allocation |
| 553 | Requested action not taken. File name not allowed |
| مفهوم برخی از کدهای متداول | |
| 226 | دستور بدون هیچگونه خطائی اجراء گردید . |
| 230 | زمانی این کد نمایش داده می شود که یك سرویس گیرنده رمز عبور خود را به درستی درج و عملیات login با موفقیت انجام شده باشد . |
| 231 | کد فوق نشاندهنده دریافت username ارسالی سرویس گیرنده توسط سرویس دهنده می باشد و تائیدی است بر اعلام وصول Username ( نه |

| | |
|---|---|
| صحت آن ) . | |
| دستور تایپ شده دارای خطاء گرامری است و می بایست مجددا" دستور تایپ گردد . | 501 |
| عملیات login با موفقیت انجام نشده است . ممکن است Username و یا رمز عبور اشتباه باشد . | 530 |
| فایل مشخص شده در دستور تایپ شده نامعتبر است . | 550 |

در بخش دوم به بررسی نحوه عملکرد پروتکل FTP خواهیم پرداخت .

---

### آشنائی با پروتکل FTP ( بخش دوم )

FTP ، یك پروتکل ارسال فایل است که با استفاده از آن سرویس گیرندگان می توانند به سرویس دهندگان متصل و صرفنظر از نوع سرویس دهنده اقدام به دریافت و یا ارسال فایل نمایند . پروتکل FTP به منظور ارائه خدمات خود از دو حالت متفاوت استفاده می نماید : Active Mode و Passive Mode . مهمترین تفاوت بین روش های فوق جایگاه سرویس دهنده و یا سرویس گیرنده در ایجاد و خاتمه یك ارتباط است .

همانگونه که در بخش اول اشاره گردید ، یك اتصال پروتکل TCP/IP ( نسخه شماره چهار) شامل دو نقطه مجزا می باشد که هر نقطه از یك آدرس IP و یك شماره پورت استفاده می نماید . برقراری ارتباط بین یك سرویس گیرنده و یك سرویس دهنده منوط به وجود چهار عنصر اطلاعاتی است : آدرس سرویس دهنده ،پورت سرویس دهنده ، آدرس سرویس گیرنده و پورت سرویس گیرنده . در زمان برقراری یك ارتباط ، سرویس گیرنده از یك شماره پورت استفاده می نماید . این شماره پورت می تواند متناسب با نوع عملکرد برنامه سرویس گیرنده به صورت اختیاری و یا اجباری باشد . مثلا" برخی برنامه های سرویس گیرنده به منظور ارتباط با سرویس دهنده ، نیازمند استفاده از یك شماره پورت خاص می باشند ( نظیر برنامه های سرویس گیرنده وب و یا مرورگرهای وب که از پورت شماره ۸۰ به منظور ارتباط با سرویس دهنده وب استفاده می نماید) . در مواردی که الزامی در خصوص شماره پورت وجود ندارد از یك شماره پورت موقتی و یا ephemeral استفاده می گردد . این نوع پورت ها موقتی بوده و توسط IP stack ماشین مربوطه به متقاضیان نسبت داده شده و پس از خاتمه ارتباط ، پورت آزاد می گردد . با توجه به این که اکثر IP Stacks بلافاصله از پورت موقت آزاد شده استفاده نخواهند کرد ( تا زمانی که تمام pool تکمیل نشده باشد ) ،در صورتی که سرویس گیرنده مجددا" درخواست برقراری یك ارتباط را نماید ، یك شماره پورت موقتی دیگر به وی تخصیص داده می شود .

پس از این مقدمه ، در ادامه به بررسی هر یك از روش های Active و Passive در پروتکل FTP خواهیم پرداخت .

### Active Mode

Active Mode ، روش سنتی ارتباط بین یك سرویس گیرنده FTP و یك سرویس دهنده می باشد که عملکرد آن بر اساس فرآیند زیر است :

- سرویس گیرنده یك ارتباط با پورت ۲۱ سرویس دهنده FTP برقرار می نماید . پورت ۲۱ ، پورتی است که سرویس دهنده به آن گوش فرا می دهد تا از صدور فرامین آگاه و آنان را به ترتیب پاسخ دهد . سرویس گیرنده برای برقراری ارتباط با سرویس دهنده از یك پورت تصادفی و موقتی ( بزرگتر از ۱۰۲٤ ) استفاده می نماید( پورت x ).
- سرویس گیرنده شماره پورت لازم برای ارتباط سرویس دهنده با خود را از طریق صدور دستور PORT N+1 به وی اطلاع می دهد ( پورت x+1 )
- سرویس دهنده یك ارتباط را از طریق پورت ۲۰ خود با پورت مشخص شده سرویس گیرنده ( پورت x+1 ) برقرار می نماید .

| | |
|---|---|
| سرویس گیرنده | لطفا" به من از طریق پورت ۱۹۳۱ بر روی آدرس IP: ۱۹۲.۱٦۸.۱.۲ متصل و سپس داده را ارسال نمائید . |
| سرویس دهنده | تائید دستور |

در فرآیند فوق ، ارتباط توسط سرویس گیرنده آغاز و پاسخ به آن توسط سرویس دهنده و از طریق پورت x+1 که توسط سرویس گیرنده مشخص شده است ، انجام می شود . در صورتی که سرویس گیرنده از سیستم ها و دستگاه های امنیتی خاصی نظیر فایروال استفاده کرده باشد ، می بایست تمهیدات لازم به منظور ارتباط کامپیوترهای میزبان راه دور به سرویس گیرنده پیش بینی تا آنان بتوانند به هر پورت بالاتر از ۱۰۲٤ سرویس گیرنده دستیابی داشته باشند . بدین منظور لازم است که پورت های اشاره شده بر روی ماشین سرویس گیرنده open باشند . این موضوع می تواند تهدیدات و چالش های امنیتی متعددی را برای سرویس گیرندگان به دنبال داشته باشد .

### Passive Mode

در Passive Mode ، که به آن " مدیریت و یا اداره سرویس گیرندگان FTP" نیز گفته می شود از فرآیند زیر استفاده می گردد :

- سرویس گیرنده دو پورت را فعال می نماید ( پورت x و x+1 )
- ارتباط اولیه از طریق پورت x سرویس گیرنده با پورت ۲۱ سرویس دهنده آغاز می گردد .
- سرویس دهنده یك پورت را فعال ( Y ) و به سرویس گیرنده شماره پورت را اعلام می نماید .
- در ادامه سرویس گیرنده یك اتصال از طریق پورت x+1 با پورت y سرویس دهنده برقرار می نماید .

| | |
|---|---|
| سرویس گیرنده | لطفا" به من بگوئید  که از کجا می توانم داده را دریافت نمایم |
| سرویس دهنده | با من از طریق پورت ٤٠٢٣  بر روی آدرس IP: ١٩٢.١٦٨.١.٢٥ ارتباط برقرار نمائید . |

در فرآیند فوق ، سرویس گیرنده دارای نقش محوری است و فایروال موجود بر روی سرویس گیرنده می تواند درخواست های دریافتی غیرمجاز به پورت های بالاتر از ١٠٢٤ را به منظور افزایش امنیت بلاك نمایند .  در صورتی که بر روی کامپیوترهای سرویس دهنده نیز فایروال نصب شده باشد ، می بایست پیکربندی لازم به منظور استفاده از پورت های بالاتر از ١٠٢٤ بر روی آن انجام و آنان open گردند . باز نمودن پورت های فوق بر روی سرویس دهنده می تواند چالش های امنیتی خاصی را برای سرویس دهنده به دنبال داشته باشد .

متاسفانه تمامی سرویس گیرندگان FTP از Passive Mode حمایت نمی نمایند . اگر یك سرویس گیرنده بتواند به یك سرویس دهنده  login نماید ولی قادر به ارسال داده بر روی آن نباشد ، نشاندهنده این موضوع است که فایروال و یا Gateway برای استفاده از Mode Passive  به درستی پیکربندی نشده است .

### ملاحضات امنیتی

در صورتی که فایروال های موجود بر روی کامپیوترهای سرویس گیرنده به درستی پیکربندی نگردند ، آنان نمی توانند از  Active Mode استفاده نمایند .  در Passive Mode استحکام سیستم امنیتی در سمت سرویس دهنده و توسط فایروال مربوطه انجام خواهد شد . بنابراین لازم است به سرویس دهنده اجازه داده شود که به اتصالات هر پورت بالاتر از ١٠٢٤ پاسخ دهد . ترافیك فوق ، معمولا" توسط فایروال سرویس دهنده بلاك می گردد . در چنین شرایطی امکان استفاده از Passive Mode وجود نخواهد داشت .

### Passive Mode  و یا Mode Active ؟

با توجه به مستندات درج شده در RFC 1579 ، استفاده از Passive Mode به دلایل متعددی به Active Mode ترجیح داده می شود :

- تعداد سرویس دهندگان موجود بر روی اینترنت به مراتب کمتر از سرویس گیرندگان می باشد .
- با استفاده از امکانات موجود می توان سرویس دهندگان را پیکربندی تا بتوانند از مجموعه پورت های محدود و تعریف شده ای با در نظر گرفتن مسائل امنیتی ، استفاده نمایند.

### پیکربندی فایروال

جدول زیر پیکربندی فایروال در Active Mode و Passive Mode را نشان می دهد .

| Active Mode | |
|---|---|
| Server Inbound | from any client port >1024 to port 21 on the server |
| Server Outbound | from port 20 on the client on any port > 1024 |
| Client Inbound | ports 20 from the server to any port >1024 on client |
| Client Outbound | from any port >1024 to port 21 on the server |
| **Passive Mode** | |
| Server Inbound | port 21 and any port >1024 from client/anywhere, from any port >1024 |
| Server Outbound | port 21 and any port >1024 to client/anywhere, to any port >1024 |
| Client Inbound | Return traffic, any port > 1024 from server using any port >1024 |

### و اما يك نكته ديگر در رابطه با پروتكل FTP !

در صورتی که در زمان دریافت يك فايل با استفاده از پروتكل FTP مشكلات خاصی ايجاد که منجر به قطع ارتباط با سرويس دهنده FTP گردد ، سرويس گيرنده می تواند با مشخص كردن يك offset از فايل دريافتی به سرويس دهنده اعلام نمايد كه عمليات ارسال را از جائی كه ارتباط قطع شده است ، ادامه دهد ( سرويس گيرنده از محلی شروع به دريافت فايل می نمايد كه ارتباط غيرفعال شده بود ) . استفاده از ويژگی فوق به امكانات سرويس دهنده FTP بستگی دارد .