Subject: آشنایی با سرویس دهنده اینترنتی

Year. Month. Date. ( )

فصل اول : پروتکل HTTP

HTTP پروتکلی با قابلیت های فراوان است که علی رغم برخی محدودیت ها دارای سابقه درخشانی در شبکه های کامپیوتری (اینترانت و اینترنت) است .

HTTP = Hyper Text Transfer Protocol

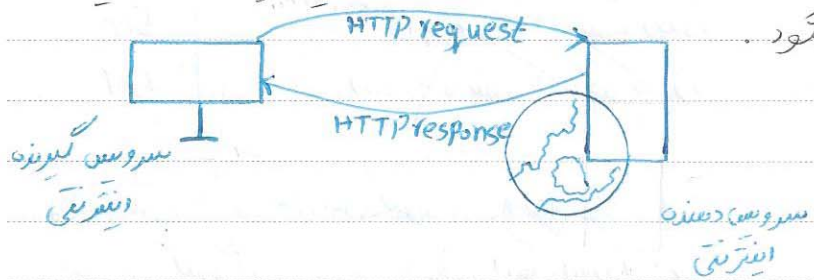
زمانی که مرورگر وب درخواست یک صفحه را از سرویس دهنده وب می نماید در واقع یک HTTP request را ارسال و سرویس دهنده وب نیز پاسخ آن را با یک HTTP response خواهد داد

یک پیام HTTP یک درخواست (request) یا یک پاسخ (response) است که از یک ساختار خاص تبعیت می نماید.

HTTP به یک پروتکل خاص لایه حمل وابستگی نداشته و عموماً از پروتکل TCP استفاده می نماید. (از پورت شناخته شده ۸۰)

کدهای وضعیت :

مانند بسیاری از پروتکل ها ، پروتکل HTTP بر اساس یک مدل سرویس گیرنده - سرویس دهنده کار می کند . به شکل زیر دقت شود .



کدهای وضعیت توسط تعداد زیادی از پروتکل های لایه application استفاده می گردد و می توان آنها را به ۵ گروه عمده تقسیم نمود . جدول زیر گروه های پنج گانه کدهای وضعیت را در ارتباط با پروتکل HTTP نشان می دهد .

کد	عملکرد
1xx	برای استفاده در آینده
2xx	انجام موفقیت آمیز تراکنش
3xx	راهنمایی مجدد
4xx	بروز خطا سمت سرویس گیرنده
5xx	" " " دهنده

Subject:
Year. Month. Date. ( )

هر یک از کدهای فوق دارای کدهای وضعیت زیر مجموعه‌ای می‌باشند که بیانگر جزئیات عملیات است. جدول زیر برخی از کدهای وضعیت هر یک از گروه های کدهای فوق را در ارتباط با پروتکل HTTP نشان می دهد.

کد وضعیت	عملکرد
200	تراکنش با موفقیت انجام شده است
201	دستور POST با موفقیت انجام شده است
202	درخواست ارسالی دریافت گردید
300	منبع درخواستی در مکان های مختلفی پیدا شده
301	منبع درخواستی به صورت دائم منتقل شده
302	منبع درخواستی به صورت موقت منتقل شده
400	درخواست نامناسب از جانب سرویس گیرنده
401	درخواست غیر مجاز
404	منبع درخواستی پیدا نگردید
500	بروز خطا بروی سرویس دهنده
501	متد استفاده شده پیاده سازی نشده است

درخواست های سرویس گیرندگان و دستورات :

سرویس گیرندگان وب به منظور استفاده از خدمات سرویس دهندگان وب از مجموعه پیام هایی که از مجموعه دستورات توسط پروتکل HTTP استفاده می نماید که مهمترین این دستورات عبارتند از :

GET = سرویس گیرنده وب درخواست یک منبع موجود بروی سرویس دهندهٔ وب را می نماید.

POST = سرویس گیرنده وب اطلاعاتی را برای سرویس دهندهٔ وب ارسال می نماید.

PUT = سرویس گیرندهٔ وب یک سند جایگزین را برای سرویس دهندهٔ وب ارسال می نماید.

Subject:
Year. Month. Date. ( )

HEAD = سرویس گیرنده وب اطلاعات خاصی را در ارتباط با یک منبع موجود برروی سرویس دهنده وب درخواست می نماید (عدم نیاز به خود منبع)

DELETE = سرویس گیرنده وب درخواست حذف یک سند موجود برروی سرویس دهنده را می نماید

TRACE = سرویس گیرندگان وب Proxy معروف به خود را تعریف می نمایند . از متد فوق اغلب برای اشکال زدایی استفاده می گردد .

OPTIONS = سایر پتانسیل های موجود به منظور کار برروی یک سند توسط یک سرویس گیرنده وب درخواست می گردد .

CONNECT = سرویس گیرنده وب به عنوان یک Proxy به یک سرویس دهنده HTTPS متصل می گردد .

در اغلب موارد صرفاً از متد GET و در برخی موارد از HEAD استفاده می گردد . درصورت اشکال زدایی یک برنامه وب از تمامی امکانات فوق استفاده می شود .

مراحل ایجاد یک تراکنش :

یک سرویس گیرنده وب قبل از اینکه بتواند با یک سرویس دهنده وب داده ای را مبادله نماید می بایست با آن ارتباط برقرار کند . بدین منظور از پروتکل TCP/IP استفاده می گردد . همانگونه که اشاره شد سرویس گیرنده و سرویس دهنده وب برای ارسال یک درخواست و پاسخ به آن از پروتکل HTTP استفاده نموده و ارتباط ایجاد شده بین خود را صرفا برای یک تراکنش نگه داری می نمایند (HTTP یک پروتکل stateless است)

فرآیند ایجاد یک تراکنش بین سرویس گیرنده و سرویس دهنده وب را می توان در ۴ مرحله زیر خلاصه نمود :

۱- در ابتدای بایست یک ارتباط و یا اتصال مبتنی بر پروتکل TCP/IP بین یک سرویس دهنده و یک سرویس گیرنده وب ایجاد گردد : برقراری ارتباط) به منظور تشخیص نوع پروتکل استفاده شده برنامه ها از یک عدد منحصر به فرد با نام شماره پورت استفاده می نمایند (پروتکل FTP از پورت ۲۱ ،

Subject:
Year. Month. Date. ( )

پروتکل Telnet از پورت ۲۳ ، پروتکل SMTP از پورت ۲۵ و پروتکل HTTP از پورت ۸۰ استفاده می‌نماید.

۲- ایجاد و یا مدور یک درخواست توسط سرویس گیرنده

۳- پاسخ سرویس دهنده به درخواست سرویس گیرنده

۴- سرویس دهنده مسئولیت خاتمه ارتباط TCP با سرویس گیرندهٔ Web دارد پس از پاسخ به درخواست سرویس گیرنده بر تکیده دارد (خاتمه و یا توقف ارتباط) به منظور برخورد با مسائل غیر قابل پیش بینی هم سرویس گیرنده و هم سرویس دهنده می‌بایست قادر به مدیریت یک ارتباط باشند مثلاً پس از فعال نمودن دکمه stop در مرورگر می‌بایست به ارتباط ایجاد شده توسط سرویس گیرنده خاتمه داده شود.

فصل دوم: پروتکل امنیتی SSL

SSL یا Secure Socket Layer راه حلی جهت برقراری ارتباطات ایمن میان یک سرویس دهنده و یک سرویس گیرنده است که توسط شرکت Netscape ارائه شده است. در واقع SSL پروتکلی است که پایین تر از لایه کاربرد (لایه ۴ از مدل TCP/IP) و بالاتر از لایه انتقال (لایه ۳ از مدل TCP/IP) قرار می‌گیرد.

لایه‌های مدل TCP/IP

Application Layer ⟹ محل قرارگیری پروتکل امنیتی SSL

Transport Layer

Internet Layer

Network Interface Layer

مزیت استفاده از این پروتکل بهره گیری از موارد امنیتی تعبیه شدهٔ آن برای حمل کردن پروتکل های غیر امن لایه کاربردی نظیر HTTP ، LDAP ، IMAP و ... می‌باشد که براساس آن الگوریتم های رمزنگاری برروی داده های ساده (plain text) که قرار است از یک کانال ارتباطی غیر امن مثل اینترنت عبور کند اعمال می‌شود و محرمانه ماندن داده ها در طول کانال انتقال تضمین می‌گردد. به بیانی دیگر شرکتی که صلاحیت صدور و اعطای گواهی های دیجیتال SSL را دارد برای هر کدام از دو طرفی که

Subject:
Year. Month. Date. ( )

قرار است ارتباطات میان شبکه‌ای امن داشته باشند، گواهی‌های مخصوص سرویس دهنده و سرویس گیرنده را صادر کرده و با مکانیزم‌های احراز هویت خاص خود، هویت هرکدام از طرفین را برای طرف مقابل تایید می‌کند. الته غیر از این کار می‌بایست تضمین کند که اگر اطلاعات حین انتقال مورد سرقت قرار گیرند برای رباینده قابل درک و استفاده نباشد که این کار با کمک الگوریتم‌های رمزنگاری و کلیدهای رمزنگاری متقارن و نامتقارن انجام می‌دهد.

ملزومات یک ارتباط مبتنی بر پروتکل امنیتی SSL:

برای داشتن ارتباطات امن مبتنی بر SSL عموماً به دو نوع گواهی دیجیتال SSL یکی برای سرویس دهنده و دیگری برای سرویس گیرنده و یک مرکز صدور و اعطای گواهینامه دیجیتال (CA) نیاز می‌باشد. وظیفه CA این است که هویت طرفین ارتباط، نشانی‌ها، حساب‌های بانکی و تاریخ انقضای گواهینامه را بداند و بر اساس آنها هویت‌ها را تعیین نماید.

مکانیزم‌های تشکیل دهندهٔ SSL:

۱- تایید هویت سرویس دهنده: با استفاده از این ویژگی در SSL کاربر از صحت هویت یک سرویس دهنده مطمئن می‌شود. تمام قرارهای مبتنی بر SSL سمت سرویس گیرنده مثلاً یک مرورگر وب مانند Internet Explorer از تکنیک‌های استاندارد رمزنگاری مبتنی بر کلید عمومی و مقایسه با کلیدهای عمومی یک سرویس دهنده (مثلاً یک برنامه سرویس دهنده وب مثل IIS) می‌توانند از هویت او مطلع شود و پس از اطمینان کامل، کاربر می‌تواند نسبت به وارد نمودن اطلاعات خود مانند شماره کارت‌های اعتباری و یا گذرواژه‌ها اقدام نماید.

۲- تایید هویت سرویس گیرنده: برعکس حالت قبل در اینجا سرویس دهنده است که می‌بایست از صحت هویت سرویس گیرنده اطمینان یابد. طی این مکانیزم تمام قرارهای مبتنی بر SSL سمت سرویس دهنده پس از مقایسه نام سرویس گیرنده با نام‌های مجاز موجود در لیست سرویس گیرنده‌های مجاز که در داخل سرویس دهنده تعریف می‌شود و در صورت وجود، اجازه استفاده از سرویس‌های مجاز را به او می‌دهد.

Subject:
Year. Month. Date. ( )

۳- ارتباطات رمز شده : کلیه اطلاعات مبادله شده میان سرویس دهنده و سرویس گیرنده می بایست توسط نرم افزارهای موجود در سمت سرویس دهنده و سرویس گیرنده رمزنگاری یا Encrypt شده و در طرف مقابل رمزگشایی یا Decrypt شوند تا حداکثر محرمانه بودن یا Confidentiality در این گروه سیستم ها لحاظ شود.

اجزاء پروتکل SSL :

پروتکل SSL دو زیر پروتکل تحت عناوین زیر دارد :

۱- SSL Record protocol :

نوع قالب بندی داده های ارسالی را تعیین می کند.

۲- SSL Handshake protocol :

براساس قالب تعیین شده در پروتکل قبلی مقدمات ارسال داده ها میان سرویس دهنده ها و سرویس گیرنده های مبتنی بر SSL را تحمیل می کند.

بخش بندی پروتکل SSL به دو زیر پروتکل دارای مزایایی است از جمله :

۱- در ابتدا و در مراحل اولیه ارتباط (Handshake) ، هویت سرویس دهنده برای سرویس گیرنده مشخص می گردد.

۲- در همان ابتدای شروع مبادلات ، سرویس دهنده و سرویس گیرنده نوع الگوریتم رمزنگاری مبادلی را تعیین می کنند.

۳- در صورت لزوم هویت سرویس گیرنده نیز برای سرویس دهنده احراز می گردد.

۴- در صورت استفاده از تکنیک های رمزنگاری مبتنی بر کلید عمومی ، می توانند کلیدهای اشتراکی مخفی را ایجاد نمایند.

۵- ارتباطات بر مبنای SSL رمزنگاری می شود.

الگوریتم های رمزنگاری پشتیبانی شده در SSL :

در استاندارد SSL از اغلب الگوریتم های عمومی رمزنگاری و مبادلات کلید یا Key Exchange Algorithm مانند RSA ، RC4 ، RC2 ، MD5 ، KEA ، DSA ، DES ، RSA key Exchange

Subject:
Year. Month. Date. ( )

SHA.1 , skipjack, DES3 پشتیبانی می‌شود.

بسته به اینکه نرم افزارهای سمت سرویس دهنده و خود سرویس دهنده نیز از موارد مذکور پشتیبانی نمایند ارتباطات SSL می‌تواند براساس هرکدام از این الگوریتم‌ها صورت پذیرد.

البته بسته به طول کلید مورد استفاده در الگوریتم و قدرت ذاتی الگوریتم می‌توان آنها را در رده‌های مختلفی قرار داد که توصیه می‌شود با توجه به سناریوهای مورد نظر از الگوریتم‌های قوی‌تر مانند DES3 با طول کلید 168bit برای رمزنگاری داده‌ها و نیز الگوریتم SHA1 برای مکانیزم‌های تایید پیغام MD5 استفاده شود و یا اینکه اگر امنیت در این خصوص نیاز نبود می‌توان در مواردی خاص از الگوریتم رمزنگاری RC4 با طول کلید 40bit و الگوریتم تایید پیغام MD5 استفاده نمود.

الگوریتم‌های رمزنگاری: ۱- بازگشت پذیر
۲- بازگشت ناپذیر

نحوه عملکرد داخلی پروتکل SSL:

همانطور که می‌دانید SSL می‌تواند از ترکیب رمزنگاری متقارن و نامتقارن استفاده کند.
رمزنگاری کلید متقارن سریع‌تر از رمزنگاری کلید عمومی است و از طرف دیگر رمزنگاری کلید نامتقارن پروتکل SSL به دو نیز پروتکل دارای مزایایی است از جمله رمزنگاری کلید عمومی تکنیک‌های احراز هویت قوی‌تری را ارائه می‌کند.

یک جلسهٔ SSL یا SSL session با یک تبادل پیغام ساده تحت عنوان SSL Handshake شروع می‌شود. این پیغام اولیه به سرویس دهنده این امکان را می‌دهد که یک کلید متقارن را ایجاد نمایند تا برای رمزنگاری‌ها و رمزگشایی سریع‌تر در جریان ادامهٔ مبادلات مورد استفاده قرار می‌گیرد. گام‌هایی که قبل از برگزاری این جلسه انجام می‌شود براساس الگوریتم RSA RSA key Exchange عبارتند از:

1- سرویس گیرنده نسخهٔ SSL مورد استفادهٔ خود، تنظیمات اولیه درباره نحوهٔ رمزنگاری و یک دادهٔ تصادفی را برای شروع درخواست یک ارتباط امن مبتنی بر SSL به سمت سرویس دهنده ارسال می‌کند.

2. سرویس دهنده نیز در پاسخ نسخهٔ SSL مورد استفادهٔ خود، تنظیمات رمزنگاری و

Subject:
Year. Month. Date. ( )

داده تصادفی تولید شده توسط خودش به سرویس گیرنده می فرستد و نیز سرویس دهنده گواهینامه خودش نیز برای سرویس گیرنده ارسال می کند و اگر سرویس گیرنده از سرویس دهنده درخواستی داشت که نیاز مند احراز هویت سرویس گیرنده بود آنرا نیز از سرویس گیرنده درخواست می کند.

3- سپس سرویس گیرنده با استفاده از اطلاعاتی که از سرویس دهنده مجاز درخود دارد، داده ها را بررسی می کند و اگر سرویس دهنده مذکور تایید هویت شد وارد مرحله بعدی می شود و در غیراینصورت با پیغام هشداری به کاربر ادامه عملیات قطع می گردد.

4- سرویس گیرنده یک مقدار به نام Secret Premaster را برای شروع جلسه ایجاد می کند و آن را با استفاده از کلید عمومی که اطلاعات آن محموله در سرویس دهنده موجود است) رمزنگاری می کند و این مقدار رمز شده را به سرویس دهنده ارسال می کند.

5- اگر سرویس دهنده به گواهینامه سرویس گیرنده نیاز داشت می بایست در این گام برای سرویس دهنده ارسال شود و اگر سرویس گیرنده نتواند هویت خودش به سرویس دهنده اثبات کند ارتباط از همینجا قطع می شود.

6- به محض اینکه هویت سرویس گیرنده برای سرویس دهنده احراز شد، سرویس دهنده با استفاده از کلید اختصاصی خودش مقدار Se Premaster را رمزگشایی می کند و سپس اقدام به تحمید مقداری به نام Master secret می نماید.
Secret

7- هم سرویس دهنده و هم سرویس گیرنده با استفاده از مقدار Master secret کلید جلسه (session key) را تولید می کنند که در واقع کلید متقارن مورد استفاده در عمل رمزنگاری و رمزگشایی داده ها همین انتقال اطلاعات است که در این مرحله به نوعی جامعیت داده ها بررسی می شود.

8- سرویس گیرنده پیغامی را به سرویس دهنده می فرستد تا به او اطلاع دهد داده ای که توسط سرویس گیرنده ارسال می شود به وسیله کلید جلسه رمزنگاری خواهد شد و در ادامه پیغام رمز شده نیز ارسال می شود تا سرویس دهنده از پایان یافتن Hanelshacke سمت سرویس گیرنده مطلع شود.

9- سرویس دهنده پیغامی را به سرویس گیرنده ارسال می کند تا او نیز از پایان Handshacke

Subject:
Year. Month. Date. ( )

سمت سرویس گیرنده آگاه نماید و نیز اینکه داده‌ی بعدی که ارسال خواهد شد توسط کلید جلسه رمز می‌شود.

10 - در این مرحله SSL Handshake تمام می‌شود و از این به بعد جلسه‌ی SSL شروع می‌شود و هر دو عضو سرویس دهنده و سرویس گیرنده شروع به رمزنگاری، رمزگشایی و ارسال داده‌ها می‌کنند.

توضیح قفل امنیت SSL:

پیچیدگی‌های SSL برای کاربران شما پوشیده است ولی مرورگر اینترنت آنها در صورت برقراری ارتباط امن وجود این ارتباط را توسط نمایش یک قفل کوچک در پایین صفحه متذکر می‌شود.
کلیک بر روی قفل کوچک باعث نمایش گواهینامه شما به همراه سایر جزئیات می‌شود.
گواهینامه‌های SSL تضمینی برای شرکت‌ها و اشخاص حقیقی معتبر ساخته می‌شوند. زمانی که یک مرورگر اینترنت به یک سایت از طریق ارتباط امن متصل می‌شود، علاوه بر دریافت گواهینامه SSL، پارامترهای رمزنگاری تاریخ انقضای گواهی‌نامه، معتبر بودن صادر کننده گواهینامه و مجاز بودن سایت به استفاده از این نوع گواهی‌نامه را نیز بررسی می‌کند و هر کدام از این موارد که تایید نشود یک پیغام اخطار به کاربر اعلام می‌دهد.

۳ - پروتکل FTP (File Transfer protocol):

a. پروتکل FTP چیست؟ } در جزوه PDF
b. ویژگی‌های پروتکل FTP:

نرم افزارهای مورد استفاده برای کار با FTP: File Zilla - Smart FTP - Cute FTP - FTP Browser ...

ویژگی دیگر این است که همانند بسیاری از پروتکل‌های لایه application لایه کاربرد پروتکل FTP نیز دارای کدهای وضعیت خطا مختص به خود می‌باشد که اطلاعات لازم در خصوص وضعیت ارتباط ایجاد شده و یا درخواستی را ارائه می‌نمایند.
زمانی که یک درخواست (GET یا PUT) برای سرویس دهنده FTP ارسال می‌گردد سرویس دهنده پاسخ خود را به صورت یک رشته اعلام می‌نماید.
اولین خط این رشته معمولا شامل نام سرویس دهنده و نسخه نرم افزار FTP می‌باشد و در ادامه

Subject:
Year. Month. Date. ( )

می‌توان دستورات GET یا PUT را برای سرویس دهنده ارسال نمود.
سرویس دهنده با ارسال یک پیام وضعیت به درخواست سرویس گیرندگان پاسخ می‌دهد.
کدهای وضعیت برگردانده شده که می‌توان در 5 گروه متفاوت تقسیم نمود:

1xx : کدهای پاسخ اولیه هستند
2xx : درخواست بدون خطا اجرا گردید
3xx : به اطلاعات بیشتری نیاز است
4xx : یک خطای موقت ایجاد شده است
5xx : یک خطای دائمی ایجاد شده است

مفهوم برخی از کدهای متداول:

226 : دستور بدون هیچگونه خطایی اجرا گردید
230 : زمانی این کد نمایش داده می‌شود که یک سرویس گیرنده رمز عبور خود را به درستی درج کرده و عملیات لاگین با موفقیت انجام شده باشد.
231 : این کد نشان دهنده دریافت username ارسالی سرویس گیرنده توسط سرویس دهنده می‌باشد و تاسیدی است بر اعلام وصول username نه صحت آن.
501 : دستور تایپ شده دارای خطای گرامری است و می‌بایست مجدداً دستور تایپ شود
530 : عملیات لاگین با موفقیت انجام نشده است. ممکن است username و یا رمز عبور اشتباه باشد.
550 : فایل مشخص شده در دستور تایپ شده نامعتبر است.

FTP یک پروتکل ارسال فایل است که با استفاده از آن سرویس گیرندگان می‌توانند به سرویس دهندگان متصل شده و صرف نظر از نوع سرویس دهنده اعم از دریافت و یا ارسال فایل نمایند.
پروتکل FTP به منظور ارائه خدمات خود از دو حالت متفاوت استفاده می‌نماید:
Passive Mode و Active Mode.

همانگونه که اشاره کرده بودیم یک ارتباط پروتکل TCP/IP (نسخه شماره 4) شامل دو نقطه مجزا می باشد که هر نقطه از یک آدرس IP و یک شماره پورت استفاده می نماید.

مثال: 192.168.100.12 : 20

$$socket = \begin{cases} \text{آدرس IP}: & 192.168.100.12 \\ \text{شماره پورت}: & 20 \end{cases}$$

آدرس IP و شماره پورت باهم تشکیل سوکت را می دهند.

برقراری ارتباط بین سرویس دهنده و سرویس گیرنده منوط به وجود 4 عنصر است:

1- آدرس سرویس دهنده
2- پورت سرویس دهنده
3- آدرس سرویس گیرنده
4- پورت سرویس گیرنده

در مواردی که الزامی برای شماره پورت وجود ندارد از یک شماره پورت موقتی یا ephermeral استفاده می شود. این نوع پورت ها موقتی بوده و توسط IP stak (یا پشته IP) ماشین مربوط به متقاضیان نسبت داده شده و پس از خاتمه ارتباط پورت آزاد می گردد.

با توجه به اینکه IP stak ها بلافاصله از پورت موقت آزاد شده استفاده نخواهند کرد (تا زمانی که تمام Pool تکمیل نشده باشد)، در صورتی که سرویس گیرنده مجدداً درخواست برقراری یک ارتباط را نماید یک شماره پورت موقتی دیگر به وی تخصیص داده می شود.

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

1- سرویس گیرنده یک ارتباط با پورت 21 سرویس دهنده FTP برقرار می نماید.
پورت 21 پورتی است که سرویس دهنده به آن گوش فرا می دهد تا از صدور فرامین آگاه شود و آنان را به ترتیب پاسخ دهد. سرویس گیرنده برای برقراری ارتباط با سرویس دهنده از یک پورت تصادفی و موقتی (بزرگتر از 1024) استفاده می نماید (پورت x).

Subject:
Year. Month. Date. ( )

۲- سرویس گیرنده شماره پورت لازم برای ارتباط سرویس دهنده با خود را از طریق مسیر دستور PORT N+1 به وی اطلاع می دهد (پورت N+1)

۳- سرویس دهنده یک ارتباط را از طریق پورت 20 خود با پورت مشخص شده سرویس گیرنده (Port N+1) برقرار می نماید.

* - سرویس گیرنده : لطفا من از طریق پورت 1931 برروی آدرس IP : 192.168.1.2 متصل شده و سپس داده را ارسال نمایید.

- سرویس دهنده : تایید دستور

در فرآیند فوق ارتباط توسط سرویس گیرنده آغاز شده و پاسخ به آن توسط سرویس دهنده از طریق پورت N+1 (که توسط سرویس گیرنده مشخص شده) انجام می شود.

در مواردی که سرویس گیرنده از سیستم ها و دستگاه های امنیتی خاصی مثل فایروال استفاده کرده باشد می بایست شرایط لازم به منظور ارتباط کامپیوترهای میزبان راه دور به سرویس گیرنده را پیش بینی کرده تا آنها بتوانند به همه پورت بالاتر از 1024 سرویس گیرنده دسترسی داشته باشند.

بدین منظور لازم است که پورت های اشاره شده برروی ماشین سرویس گیرنده باز یا open باشند.

این موضوع می تواند تحدیدها و چالش های امنیتی متعددی را برای سرویس گیرندگان به دنبال داشته باشد.

۴- Passive Mode :