بسمه تعالی

ارزیابی امنیتی سرویس دهنده های پست الکترونیک

پروتوکل **SMTP** امن بر روی **Transport Layer Security**

فهرست مطالب

۱ مقدمه

بسیاری از سازمان ها از سرویس پست الکترونیک سازمانی مخصوص به خودشان استفاده می کنند. تامین امنیت سرویس های پست الکترونیکی سازمانی یکی از چالش های امنیتی مهم در کسب و کار آن سازمان به حساب می آید. اگر امنیت یک سرویس پست الکترونیکی به خوبی برقرار نشود مورد سوء استفاده بسیاری از هکر ها قرار می گیرد. یکی از این سوء استفاده های که می توان انجام داد، این است که از یک برنامه نامه بر برای ارسال هرزنامه استفاده کرد. یکی دیگر از سوء استفاده های که می توان انجام داد این است که یک فرد خود را به جای یک فرد دیگری قرار دهد و اقدام به ارسال نامه های الکترونیکی از طرف آن فرد کند. این سوء استفاده ها به خاطر این است که اگر برنامه نامه بر به خوبی پیکره بندی نشده باشد، می توان بدون احراز هویت اقدام به ارسال نامه های الکترونیکی نمود.

از دیگر خطراتی که برای میل سرور یک سازمان وجود دارد این است که اگر میل سرور به درستی پیکره بندی نشده باشد، می توان پیام های میان پروتوکل های مختلف یک میل سرور برای مثال بین پروتکل SMTP و پروتکل POP3 را شنود کرد. و با استفاده از شنود این نوع از اطلاعات می توان داده های حساس کاربران میل سرور را شنود کرد. بنابراین باعث می شود که محرمانگی اطلاعات که یکی از مهمترین ویژگی های سیستم های امنیت اطلاعات می باشد به مخاطره افتد.

۲ پست الکترونیک و کاربردها

امروزه مکانیزه و هوشمند سازی فعالیت‌های اداری در سازمان‌ها بسیار حائز اهمیت است. یکی از اجزا و ابزارهای اساسی و لاینفک سامانه‌های اداری در هر اداره و سازمانی پست الکترونیکی می باشد. اهمیت این ابزار به حدی رسیده است که گاه از آن به عنوان ابزاری رده بالا جهت انتقال اطلاعات حساس از جمله نامه‌های محرمانه و ... استفاده می‌شود. با وجود آنکه ابزارهای مختلف و متعدد فناوری اطلاعات جهت بهبود عملیات اداری در سازمان‌ها توسعه داده شده است و پست الکترونیکی از این حیث جزو ابزارهای قدیمی محسوب می‌شود اما این مساله باعث کاهش اهمیت آن نشده است. در زیر برخی از دلایلی را که باعث شده‌است این ابزار همچنان به طور گسترده مورد توجه و کارکرد قرار گیرد، بررسی می‌کنیم:

- پست الکترونیکی ساختاری قابل اعتماد دارد که رسیدن پیام به مخاطب را تا حد زیادی تضمین می‌کند.

- پروتکل پست الکترونیکی یک پروتکل عمومی است که در اختیار همه سازمان‌هاست در نتیجه ارتباط بین سازمانی به راحتی و بدون نیاز به هیچ گونه همگام سازی فناورانه بین سازمان‌های مختلف امکان برقراری ارتباط میان سازمانی را فراهم می‌کند. این مساله دست سازمان را برای استفاده از این ابزار صرفا در سطح سازمانی یا برای ارتباط بین سازمانی باز می‌گذارد.
- پیاده سازی نرم‌افزاری، سخت‌افزاری و نگهداری سامانه‌های پست الکترونیکی ساده و کارآمد است.

مجموعه عوامل و دلایل بالا در کنار برخی دلایل دیگر باعث شده است که با وجود توسعه فناوری‌های جدید و به روزتر همچنان پست الکترونیکی به عنوان یک ابزار سازمانی به کار خود ادامه دهد.

اما اگر بخواهیم کاربردهای پست الکترونیک در سازمان‌ها را بررسی کنیم می‌توان موارد بسیاری را شمرد که برخی از آن‌ها از این قرار هستند:

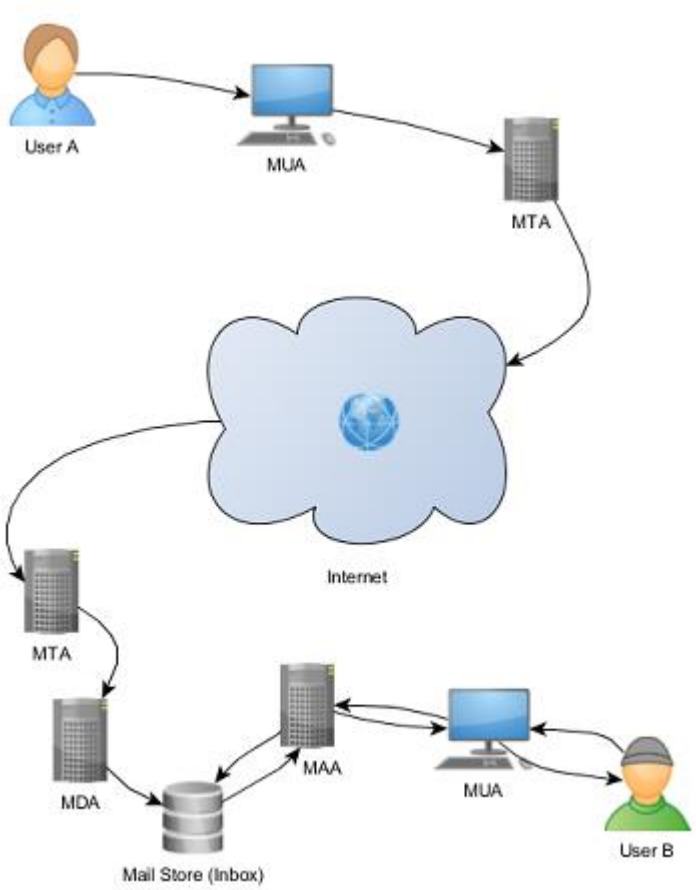
- ارسال اطلاعات و مدارک به صورت عمومی برای تعداد زیادی از افراد
- ارسال اطلاعات و مدارک به صورت خودکار و هوشمند با اتصال سامانه‌های خودکار به سیستم
- استفاده از پروتکل پست الکترونیکی به عنوان زیرساخت سامانه‌های نرم افزاری نظیر اتوماسیون اداری
- استفاده از آدرس پست الکترونیک برای ارسال اطلاعات به عنوان یک امضای تایید هویت

در مورد کاربرد آخر باید این توضیح را ارئه کرد که آدرس پست الکترونیک چه برای افراد و چه برای سازمان‌ها یک ابزار احراز هویت محسوب می‌شود به این معنا که گیرنده، صحت فرستنده پیام را از روی آدرس پست الکترونیکی فرستنده بررسی می‌نماید. این مساله چه در ارتباطات درون سازمانی (نظیر ارسال اطلاعات از طرف یک مدیر بالادست) و چه در ارتباطات بین سازمانی اهمیت به سزایی دارد.

با در نظر گرفتن نقش پررنگی که پست الکترونیکی در سازمان‌ها ایفا می‌کند می‌توان به اهمیت این ابزار پی برد. یکی از ملزومات چنین ابزار مهمی تامین امنیت آن است. یکی از سازمان‌هایی که به سبب کاربرد بالای پست الکترونیکی در آن به تامین سطح بالاتری از امنیت نیاز دارد دانشگاه است. در بخش بعدی پس از معرفی اجمالی در مورد کاربرد پست الکترونیکی در دانشگاه‌ها، اهمیت نقش امنیت و تامین آن در نگهداری و کاربرد سامانه‌های پست الکترونیکی در دانشگاه‌ها را توضیح خواهیم داد.

۳ معماری سرویس دهنده پست الکترونیک

با توجه به شکل زیر عملیات لازم برای فرستادن ایمیل توسط یک کاربر و دریافت آن توسط شخص دیگر به صورت زیر است:



۱. یک عامل کاربر ایمیل MUA[۱] یک برنامه است که به کاربر اجازه ساخت، ارسال و دریافت ایمیل را می دهد. معمولا به یک MUA یک سرویس گیرنده ایمیل[۲] گفته می شود. Microsoft Outlook نمونه ای از

[۱] Mail User Agent
[۲] Mail Client

این برنامه ها هستند ولی اکثر MUA ها بصورت برنامه های مبتنی بر وب پیاده سازی می شوند، مانند آنچه که هنگام ورود به Gmail یا Hotmail دیده می شود.

۲. ایمیل ساخته شده توسط سرویس گیرنده ایمیل به عامل انتقال ایمیل[۳] (MTA) فرستاده می شود. عامل انتقال ایمیل مسئول فرستادن ایمیل به MTA گیرندگان ایمیل می باشد. MTA پیام های پستی را توسط پروتکل SMTP بین دو کامپیوتر انتقال می دهد. Postfix نمونه ای از MTA ها هست.

۳. MTA گیرنده ها، ایمیل را دریافت کرده و آن را به عامل تحویل ایمیل[٤] (MDA) انتقال می دهند. MDA صندوق پست کاربران را مدیریت می کند. Dovecot نمونه ای از یک MDA هست.

٤. علاوه بر MDA از عامل دسترسی ایمیل (MAA[٥]) استفاده می شود که دسترسی راه دور برای خواندن پیام های کاربران را میسر سازد.

٥. گیرنده برای بررسی و دریافت پیغام هایش از MUA استفاده می کند.

۴ پروتکل SMTP

پست الکترونیکی یکی از مهمترین سرویس های اینترنت است که شباهت زیادی به پست معمولی دارد .این سرویس، اتصال غیر هم زمان رابرای افراد پدید می آورد .بدین معنا که افراد هر زمان مایل باشند می توانند اقدام به ارسال و یا مطالعه ی نامه های خود نمایند، بدون این که نیاز باشد این اعمال را با زمان و برنامه ریزی دیگران منطبق کنند .هنگامی که یک نامه ی الکترونیکی ارسال می شود، انتظار این است که سرویس دهنده ی

[۳] Mail Transfer Agent
[٤] Mail Delivery Agent
[٥] Mail Access Agent

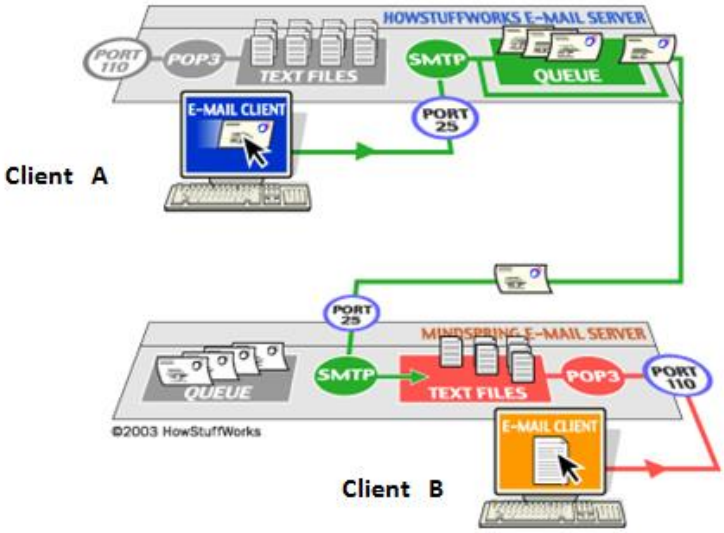
پست الکترونیکی، آن نامه را به درستی به مقصدارسال نماید .مراحل ارسال بدون توجه به سخت افزار و نرم افزار و تنها با استفاده از پروتکل های انتقال پست الکترونیکی انجام می شود.

SMTP مهمترین پروتکل انتقال پست الکترونیکی می باشد. پروتکل SMTP مخفف **SIMPLE MAIL TRANSFER PROTOCOL** بوده که از این پروتکل برای ارسال پیام‌های الکترونیکیE-mail استفاده می‌شود. . تا قبل از آن از پروتکل UUCP(Unix-to-Unix Copy) برای ارسال پیام‌های الکترونیکیE-mail استفاده می‌شد.

این پروتکل دارای ویژگی های بسیار زیادی است که آن را به یکی از مهمترین پروتکلهای اینترنت تبدیل کرده است .اما با این وجود، این پروتکل محدودیت هایی از قبیل محدودکردن بدنه ی نامه های الکترونیکی به هفت بیت کد اسکی را از زمان گذشته با خود به همراه دارد .این محدودیت تا اوایل دهه1980 میلادی که انتقال و ارسال نامه های الکترونیکی بسیار کم و به ندرت بود، مشکلی ایجاد نمی کرد .اما امروزه و در عصر رسانه های چند منظوره، محدودیت هفت بیت کد اسکی دردسرساز است .زیرا نیاز دارد که داد ه های مالتی مدیای باینری، قبل از ارسال از طریق SMTPبه کد اسکی تبدیل شوند و پس از انتقال از طریق این پروتکل از اسکی به باینری برگردانده شوند.

پروتکل smtp به دلیل محدودیت‌هایی در نگهداری نامه‌ها، معمولا با پروتکل‌های POP3 یا (post office protocol3) یا IMAP (internet message access protocol) استفاده می‌شود که برای کاربران امکان ذخیره نامه‌ها را روی یک سرور یا دانلود آنها را از سرور فراهم می‌کند. در حقیقت می‌توان گفت، SMTP برای ارسال نامه‌ها و POP3 یا IMAP برای دریافت نامه‌ها به کار می‌روند. به عبارت ساده‌تر، سرور SMTP، مانند وب سرور یک رایانه است که مانند مسیریاب عمل می‌کند. هنگامی که پیام‌های پست الکترونیکی از کاربران را دریافت می‌کند آنها را به گیرندگان مورد نظر می‌فرستند. SMTPفقط به نام کاربری و دامنه نیاز دارد تا مستقیم پیغام را به سمت گیرنده مسیریابی کند و به طور پیشفرض بر روی پورت ۲۵ قرار دارد. البته مدیران سرور برای افزایش امنیت می توانند پورت آن را تغییر دهند.

سناریوی زیر عملیات پروتکل SMTP را به تصویر میکشد:



فرض کنید client Aمیخواهد یک نامه الکترونیکی ساده را به client B ارسال کند:

- clientA آدرس پست الکترونیکی clientB را در کارگزار کاربر(user agent) خود وارد کرده و پس از نوشتن نامه ی الکترونیکی، آن را ارسال مینماید.
- لازم به ذکر است که کارگزار کاربر (user agent) برنامه ای است که محیطی را برای نوشتن، خواندن، ارسال و دریافت نامه های الکترونیکی فراهم می کند.
- clientA (user agent) نامه را در صف نامه های سرویس دهنده ی پست الکترونیکی وی قرار می دهد.
- سرویس دهنده ی پست الکترونیکی clientA یک اتصالTCP با سرویس دهنده ی پست الکترونیکی clientB ایجاد می کند.
- پس از برقراری اتصال TCP نامه ی clientA از طریق آن اتصال منتقل میگردد.
- نامه ی ارسال شده از طریق سرویس دهنده ی پست الکترونیکی clientB دریافت شده و در فهرست نامه های clientB قرار می گیرد.
- clientB از طریق کارگزار کاربر خود نامه دریافتی را میخواند.

توجه به این نکته ضروری است که پروتکل SMTP برای ارسال نامه های الکترونیکی از سرویس دهندگان پست الکترونیکی میان مبداو مقصد استفاده نمی کند، حتی اگر دو سرویس دهنده ی مذکور در فاصله ی بسیار

دوری از یکدیگر قرار داشته باشند .به عنوان مثال، اگر سرویس دهنده ی پست الکترونیکی clientA در ایران و سرویس دهنده ی پست الکترونیکی clientB درآلمان باشد، اتصال TCP مستقیما بین ایران و آلمان برقرار می گردد منظور از این جمله به طور دقیق تر این است که چنانچه سرویس دهنده ی پست الکترونیکی clientB دردسترس نباشد، نامه در سرویس دهنده ی پست الکترونیکیclientA باقی مانده و این سرویس دهنده سعی در برقراری اتصال مجدد با سرویس دهنده ی باب می نماید و نامه به هیچ وجه در سرویس دهندگان پست الکترونیکی میانی قرار نمی گیرد.

۵ پروتکل TLS

پروتکل TLS در لایه انتقال و نزدیک به پروتکل امنیتی SSL تعریف می‌شود تا ارتباطات شبکه را ایمن نماید. پروتکل‌های TLS, SSL معمولا در لایه انتقال شبکه‌ها مورد استفاده قرار می‌گیرند و در شبکه های سیار و سیمی می‌توانند پیاده سازی شوند.

وظیفه TLS ایمن نمودن تراکنش‌های ارتباطی در لایه کاربرد است. این پروتکل می‌تواند در کنار پروتکل‌های ارتباطی دیگر مانندHTTP،FTP،SMTP، NNTP مورد استفاده قرار گیرد و مکانیزم‌های در نظر گرفته شده در آن به ایجاد محرمانگی، یکپارچگی و تضمین حفظ صحت داده ها در روند انتقال کمک می‌کند.

این پروتکل تایید هویت یک‌طرفه یا دوطرفه را برای دسترسی رمزشده به شبکه‌ها فراهم می‌نماید. بخش‌هایی مانند حفاظت از بسته داده، محدود نمودن و بهینه نمودن اندازه بسته و انتخاب یک الگوریتم سریع هم به استاندارد TLS افزوده شده‌است.

کیفیت ارتباط بین دو طرف بستگی به نوع الگوریتم‌های توافق شده بین آنها دارد. این توافق قبل از اجرای TLS، و با تبادل پیام بین دو طرف بوجود می‌آید. روش انتخابی شبکه و الگوریتم آن هم در پیام ارسالی به اطلاع کاربر می‌رسد و الگوریتم‌ها شامل، الگوریتم‌هایی است که قرار است در محاسبه چکیده پیام (MAC) مورد استفاده قرار گیرند.

۶ تفاوت TLS و SSL

SSL مخفف Secure Sockets Layer می باشد. این پروتکل توسط کمپانی Netscape به عنوان اولین پروتکل امنیتی ابداع شد و بعدها این کمپانی توسط AOL خریداری شد.

TLSمخفف **Transport Layer Security**و به معنای پروتکل امنیتی لایه انتقال می باشد. این نام به منظور جلوگیری از هر گونه مسائل حقوقی با Netscape تغییر یافت، بنابراین این پروتکل می تواند آزاد و رایگان باشد و به عنوان یک RFC که مخفف Request for Comments و به معنای درخواست برای نظرات است، منتشر شود.

TLSاستاندارد ارتباط بسیار نزدیک با SSL رده ۳,۰ دارد و در منابع زیادی از آن به عنوان نام " New SSL " یاد شده و در برخی اوقات به عنوان SSL 3.1 شناخته می شود و بایستی در توسعه های جدید مورد استفاده قرار گیرد. برنامه های کاربردی که نیاز به سطح بالایی از قابلیت همکاری دارند بایستی با SSL 3.0 و TLS پشتیبانی شوند. از آنجایی که این دو پروتکل شباهت بسیار زیادی با هم دارند، تفاوت بین پروتکل TLS و پروتکل SSL 3.0 خیلی مشهود نمی باشد. هر دو روش رمزگذاری کاملا مشابه هستند و در کلیات تفاوت زیادی ندارند با این حال هر کدام یک استاندارد مستقل است و TLS از الگوریتم رمز نگاری قوی تری استفاده می کند، همچنین یکی دیگر از تفاوتهای SSL با TLS پورتهای مورد استفاده می باشد. به طور روزمره بیشترین کاربرد TLS در رمزگذاری ایمیل می باشد هر چند از لحاظ تئوری تفاوتی با SSL ندارد و هر دو پروتکل امنیت را در لایه ۷ application layer مدل OSI تامین می کنند.

۷ اتصال TLS

زمانی که کلاینت و سرور تصمیم گرفتند از اتصال TLS استفاده کنند، به مذاکره با استفاده از روش handshakingمی پردازند. سپس سرور و کلاینت بر روی پارامترهای مختلفی که برای ایجاد امنیت اتصال استفاده می شود به توافق می رسند:

۱. کلاینت اطلاعاتی را که سرور برای برقراری ارتباط با استفاده از SSLبه ان نیاز دارد را ارسال می کند. مانند: شماره نسخه SSL کلاینت، تنظیمات رمزگذاری و سایر اطلاعاتی که سرور ممکن است به آن نیاز داشته باشد.

۲. سرور اطلاعاتی را که کلاینت برای برقراری ارتباط با استفاده از SSL به ان نیاز دارد را برایش ارسال می کند. مانند: شماره نسخه SSL سرور، تنظیمات رمزگذاری و سایر اطلاعاتی که کلاینت به آن نیاز دارد.سرور همچنین گواهینامه خود را برای کلاینت ارسال می کند و اگر کلاینت درخواست منبعی از سرور داشته باشد، کلاینت باید احراز هویت شود و باید گواهینامه کلاینت برای سرور ارسال شود.

۳. با اطلاعات دریافتی از سرور ، کلاینت می تواند سرور را احرازهویت کند. اگر سرور تصدیق نشود، به کاربر هشدار داده می شود که عمل رمزگذاری و تصدیق نمی‌تواند انجام گیرد. اگر سرور به درستی تصدیق شد کلاینت به مرحله بعد می رود.

٤. با استفاده از اطلاعات به دست آمده، کلاینت یک pre-master secret ایجاد کرده و آن را به سرور ارسال می کند.

۵. اگر سرور از کلاینت بخواهد هویتش را ثابت کند، کلاینت کلیه اطلاعات لازم و گواهی خود را برای سرور ارسال می کند.

٦. اگر کلاینت تصدیق نشود، ارتباط قطع می شود اما اگر به درستی تصدیق شود، سرور از کلید خصوصی خود برای یاز کردن pre-master secret استفاده می کند.

۷. کلاینت و سرور از master secret برای تولید کلید جلسات استفاده می کنندکه یک کلید متقارن است و برای رمزگذاری و رمزگشایی اطلاعات مبادله شده استفاده می شود.

۸. وقتی کلاینت پیغامی برای سرور ارسال می کند با استفاده از کلید جلسه آن را رمز می کند.

۹. وقتی سرور پیغامی برای کلاینت ارسال می کند با استفاده از کلید جلسه آن را رمز می کند.

اکنون *SSL* handshakeکامل است و ارتباط شروع می شود. کلاینت و سرور از کلید جلسه برای رمزگذاری و رمزگشایی اطلاعاتی که برای هم می فرستند استفاده می کنند.اگر یکی از قدم های بالا با شکست مواجه شود **TLS**دچار شکست شده و ارتباط برقرار نمی‌شود. در قدم سوم مشتری باید گواهی سرور را به درستی چک کند تا باعث بروز مشکل نشود.

۸ پروتوکل SMTP امن

سرورها و کلاینت های پرتوکل SMTP به طور معمول به روشی غیر از رمزنگاری در برقراری ارتباط از طریق اینترنت مبادرت میکنند. در بسیاری از موارد، این ارتباط از طریق یک یا چند روتر عبورمی کند که تحت

کنترل و یا مورد اعتماد نیست. چنین روتر غیر قابل اطمینان ممکن است اجازه می دهد یک شخص ثالث به نظارت و یا تغییر ارتباطات بین سرور و کلاینت بپردازد.

علاوه بر این، اغلب مطلوب است که دو عامل SMTP قادر به تصدیق هویت یکدیگر باشند. به عنوان مثال، SMTP امن سرور تنها ممکن است اجازه ارتباطات از عامل های SMTPای دهد که آن را می شناسد و یا ممکن است که اعمالی را که انجام می دهد بر روی پیام هایی را که از یک عامل آشنا می گیرد نسبت به پیام هایی که از یک عامل نا آشنا می گیرد کاملا متفاوت باشد.

TLS، یک مکانیسم محبوب برای بهبود ارتباطات TCP با حفظ حریم خصوصی و احراز هویت می باشد. TLS به صورت گسترده با پروتکل HTTP استفاده می شود. همچنین برای اضافه کردن امنیت به بسیاری از پروتکل های رایج دیگر که بر روی TCP اجرا می شوند همانند SMTP مورد استفاده قرار می گیرد.

در ارتباطات SMTP، کلید واژه STARTTLS استفاده می شود تا به کلاینت SMTP اطلاع داده شود که سرور SMTP آماده استفاده از TLS می باشد.

فرمان STARTTLS که به پروتکل SMTP اضافه گردیده است هیچگونه پارامتری نمی گیرد. زمانی که کلاینت SMTP، فرمان STARTTLS را گرفت، سرور با یکی از کدهای زیر پاسخ خواهد داد:

۲۲۰: آماده برای شروع TLS

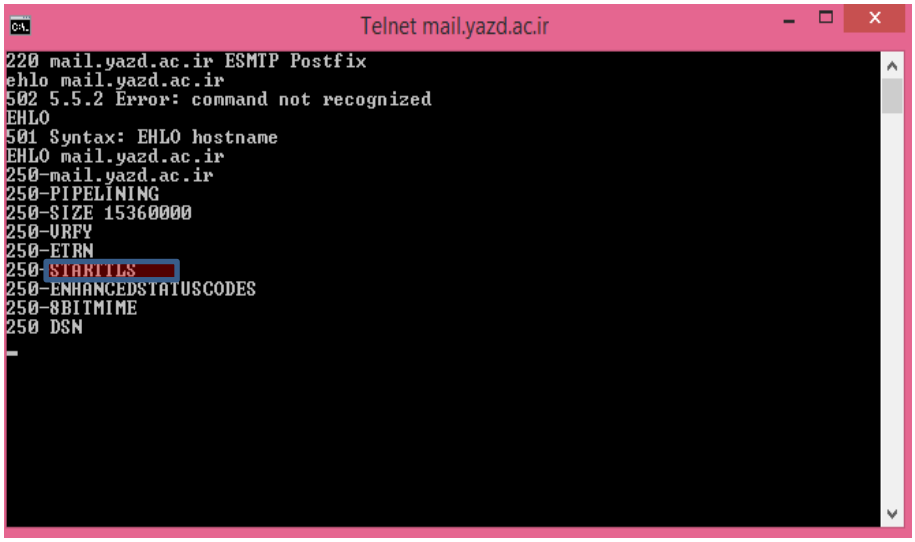
۵۰۱: خطا در استفاده از دستور

٤٥٤: TLS موقتا امکان پذیر نمی باشد.

هنگام کامل شدن TLS handshake، پروتکل SMTP به حالت اولیه ریست خواهد شد. کلاینت باید دستور EHLO را بعنوان اولین دستور بعد از کامل شدن TLS handshake برای سرور بفرستد.

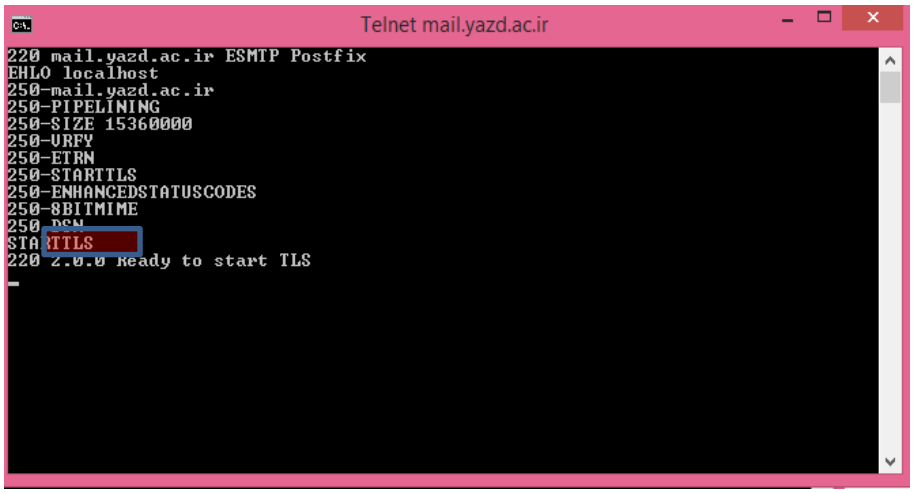
۹ مثال کاربردی

در این قسمت با استفاده از دستور telnet mail.yazd.ac.ir 25 به پروتکل SMTP دانشگاه یزد متصل می شویم و سپس دستور EHLO mail.yazd.ac.ir را صادر می کنیم. شکل زیر خروجی این دستور را نشان می دهد.



همان طور که در بالا نشان داده شده است این ایمیل سرور از STARTTLS پشتیبانی می کند.

مثال زیر نحوه ی استفاده از دستور STARTTLS را نشان می دهد.



بسته به اینکه فرمان EHLO قبل از TLS handshake یا بعد از آن صادرشده باشد، لیست سرویس های SMTP ممکن است تفاوت کند.

۱۰ نوشتن کد مربوطه

برای تست رمزنگاری از قطعه کد زیر استفاده شده است:

```
import smtplib
from optparse import OptionParser
usage = "Usage:output"
parser = OptionParser(usage=usage)
(options, args) = parser.parse_args()
if len(args) != 1:
     parser.print_help()
     parser.error("incorrect number of arguments")
     sys.exit(-1)
```

```
print (str(args[0]))

smtpObj = smtplib.SMTP(args[0])
print(smtpObj.ehlo(args[0]))
if      ('starttls'.lower()in      smtpObj.ehlo(args[0])[1].decode('utf-
8').lower()):
      print ("STARTTLS is supported")
      smtpObj.starttls()
      print(smtpObj.ehlo())
else:
      print ("STARTTLS is not supported")
```

۱۱ جمع بندی

در این گزارش ما به صورت کلی ایمیل سرور ها و به ویژه پروتکل SMTP را توضیح دادیم. درادامه توضیحاتی در مورد پروتکل TLS و چگونگی استفاده آن در پروتکل SMTP را توضیح دادیم. در نهایت کد مربوط به اینکه یک ایمیل سرور از رمزنگاری پشتیبانی می کند یا خیر را ارائه کردیم.