پروژه دوم درس شبکه - Telnet
الهام رازی - 9731019

1. تلنت، پروتکلی است که در سال 1969 معرفی شد و اینترفیسی مبتنی بر متن را برای ارتباط دو طرفه با یک دستگاه یا سرور را فراهم می آورد.
داده‌ی کاربران در این پروتکل(که مربوط به لایه‌ی اپلیکیشن است) با استفاده از پروتکل TCP که در لایه‌ي انتقال است، منتقل می‌شود. معمولا، از تلنت بر روی یک ترمینال برای اجرای توابع از راه دور مورد استفاده قرار می‌گیرد.

   از کاربردهای تلنت، می‌توان به تست کردن میل سرور ها و وب سرورها از راه دور اشاره کرد.

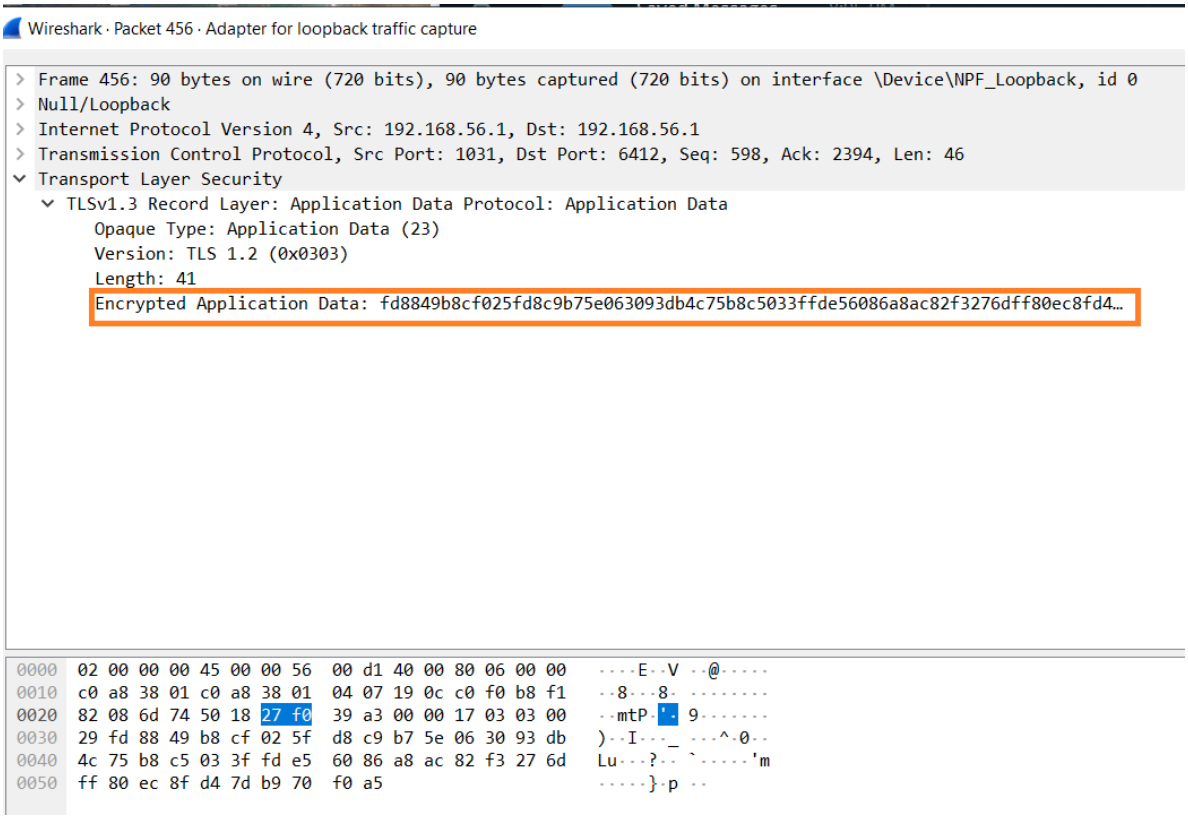
2. این پروتکل پیش از همه گیری اینترنت معرفی شده است، به خودی خود هیچ گونه رمزگذاری ای بر روی داده‌ي منتقل شده انجام نمی دهد و درواقع هیچگونه مسایل امنیتی در آن رعایت نمی‌شود. به همین دلیل، از آن در شبکه های اینترنتی چندان استفاده نمیشود.

3. پروتکل tls، پروتکلی است که با استفاده از رمزگذاری، امنیت end-to-end داده هایی که بین برنامه ها در شبکه رد و بدل می شوند را تامین می‌کند. لازم به ذکر است که این پروتکل، داده ها را در سیستمی که آن را دریافت یا ارسال کرده تضمین نمی‌کند؛ فقط امنیت آن در زمان انتقالش در شبکه توسط پروتکل فراهم می‌شود.
Tls در بالای TCP قرار گرفته و برای رمزگذاری اپلیکیشن هایی مانند HTTP، FTP، SMTP و غیره مورد استفاده قرار می گیرد.
در این پروتکل، از دو روش رمزگذاری متقارن و غیر متقارن استفاده می شود که در روش متقارن، داده با استفاده از یک کلید خصوصی که برای فرستنده و گیرنده شناخته شده است، رمزگذاری و رمزگشایی می‌شود. البته این اشتراک گذاری کلید هم باید به صورت امنی انجام شود.
در روش غیر متقارن، برای رمزگذاری از زوج کلیدهای خصوصی و عمومی استفاده می‌شود. کلید عمومی به صورت ریاضی واری با کلید خصوصی رابطه دارد. به دست آوردن کلید خصوصی از کلید عمومی، چندان راحت نیست. این موضوع به ارسال کننده امکان این را می‌دهد که با استفاده از کلید عمومی دریافت کننده، داده را رمزگذاری کنند. اما این داده، تنها با استفاده از کلید خصوصی دریافت کننده قابل رمزگشایی است.
این روش به نسبت از روش متقارن امنیت بالاتری دارد.

- **TLS HANDSHAKE**

- Client hello message: کلاینت ابتدا با استفاده از ارسال این پیام به سرور، handshake را آغاز می‌کند.
- Server hello meassage: در جواب پیام قبلی کلاینت، سرور یک پیام حاوی ssl certificate و اطلاعات دیگری را هم میفرستد.
- Authentication: کلاینت سرتیفیکت ارسالی سرور را بررسی می کند تا مطمئن باشد که سرور هویت اصلی را دارد.
- Premaster secret: کلاینت رشته رندوم دیگری از بایت را برای سرور ارسال میکند. این رشته با استفاده از کلید عمومی رمزگذاری شده و تنها با استفاده از کلید عمومی توسط سرور رمزگشایی می شود. سرور هم این پیام را رمزگشایی می‌کند.
- Session keys: کلاینت و سرور هر دو session key هایی را از client random، server random و Premaster secret تولید می کنند. هر دو باید به نتیجه مشابهی برسند.
- Client & server are ready: حال کلاینت و سرور یک پیام finished به همراه session key ها برای هم ارسال می کنند.
- Secure Symmetric encryptin achieved: مرحله tls handshake تکمیل شده و حال انتقال داده ها با استفاده از session key ها ادامه می یابد.

در تصویر زیر، میتوان محتوای پیام رمزگذاری شده را مشاهده کرد که قابل خواندن نیست:



در تصویر زیر هم می توان محتوای یک پیام با استفاده از پروتکل تلنت را مشاهده کرد که به صورت متنی ساده و بدون هیچگونه تمهیدات امنیتی قابل خواندن است.