



دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)

دانشکده مهندسی کامپیوتر

درس: شبکه‌های کامپیوتری

گزارش پروژه دوم: تلنت

نگارنده: میلاد اسرافیلیان
شماره دانشجویی: ۹۷۳۱۰۰۷

خرداد ۱۴۰۰

تلنت

تلنت یک پروتکل شبکه است که برای دسترسی مجازی به رایانه و ایجاد کانال ارتباطی دو طرفه ، مشارکتی و متنی بین دو ماشین مورد استفاده قرار می گیرد.

تلنت از دستور کاربر برای ایجاد جلسات از راه دور از پروتکل شبکه TCP/IP پیروی می کند. در وب ، پروتکل انتقال متن (HTTP) و پروتکل انتقال پرونده (FTP) به سادگی کاربران را قادر می سازد تا فایل‌های خاصی را از رایانه های از راه دور درخواست کنند ، در حالی که از طریق تلنت ، کاربران می توانند با دسترسی‌هایی که به برنامه ها و داده ها در آن رایانه به آنها اختصاص داده شده است به عنوان یک کاربر عادی وارد سیستم شوند.

با استفاده از دستور telnet می‌توان به سرور و پورت دلخواه درخواست بدهیم:

telnet aut.ac.ir

نتیجه این درخواست می تواند دعوت به ورود با شناسه کاربری باشد و سپس برنامه از کاربر درخواست رمز عبور می کند. در صورت پذیرش ، به کاربر اجازه دسترسی به میزبان از راه دور داده می شود.

کاربرد تلنت

از تلنت می توان برای فعالیت های مختلف در سرور استفاده کرد ، از جمله ویرایش فایل ها ، اجرای برنامه های مختلف و بررسی ایمیل.

برخی از سرورها برای دسترسی به داده های عمومی برای انجام بازی های ساده یا جستجوی گزارش های هواشناسی، ارتباطات از راه دور را با استفاده از تلنت فعال می کنند. بسیاری از این ویژگی ها برای سرگرمی نوستالژیک یا به دلیل اینکه هنوز با سیستم های قدیمی که نیاز به دسترسی به داده های خاص دارند سازگاری دارد.

کاربران همچنین می توانند از طریق سرورهای وب گرفته تا درگاه ها، از طریق تلنت به هر نرم افزاری که از پروتکل های متنی و رمزگذاری نشده استفاده می کند، متصل شوند.

امنیت تلنت

تلنت یک پروتکل امن نیست و رمزگذاری نشده است. با نظارت بر اتصال کاربر ، هرکسی می تواند به نام کاربری ، رمز ورود و سایر اطلاعات شخصی وی که در جلسه تلنت در متن ساده تایپ می شود ، دسترسی پیدا کند. با استفاده از این اطلاعات می توان به دستگاه کاربر دسترسی پیدا کرد.

منبع: <https://searchnetworking.techtarget.com/definition/Telnet>

پروتکل TLS

Transport Layer Security یا TLS ، یک پروتکل امنیتی است که به طور گسترده ای تصویب شده و برای تسهیل حریم خصوصی و امنیت داده ها برای ارتباطات از طریق اینترنت طراحی شده است. یک مورد اصلی استفاده از TLS رمزگذاری ارتباطات بین برنامه های وب و سرورها است ، مانند مرورگرهای وب که یک وب سایت را بارگیری می کنند. TLS همچنین می تواند برای رمزگذاری ارتباطات دیگر مانند ایمیل ، پیام رسانی و VoIP استفاده شود.

سه مؤلفه اصلی برای دستیابی به پروتکل TLS وجود دارد: رمزگذاری ، احراز هویت و یکپارچگی.

- رمزگذاری: داده های منتقل شده از اشخاص ثالث را پنهان می کند.
- احراز هویت: اطمینان حاصل می کند طرفین تبادل اطلاعات کسانی هستند که ادعا می کنند هستند.
- یکپارچگی: تأیید می کند که داده ها جعل یا دستکاری نشده اند.

منبع: <https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/>