# راهنمای مشکل امنیتی موجود بر روی Telnet


**راهنمای مشکل امنیتی موجود بر روی Telnet**

**تاریخ تنظیم : مرداد ۱۳۹۸**

**گروه شرکت‌های شاتل**

## فهرست مطالب

**Telnet چیست ؟ ( Telecommunication network )**

Telnet یک پروتکل شبکه از طریق با پورت TCP 23 است. به‌وسیله Telnet می‌توانیم از راه دور به تجهیزاتی ازجمله Modem، Router، Switch متصل شد و تنظیمات آن‌ها را تغییر داد.

به دلیل استفاده کم از پهنای باند، سرعت‌بالا، در دسترس بودن همیشگی یک Terminal و عدم نیاز به نصب نرم‌افزار با حجم بالا از این پروتکل برای اتصال از راه دور به Deviceهای موجود در شبکه استفاده می‌شود .به‌طوری‌که در هرکجا که باشیم و دسترسی به اینترنت داشته باشیم و دستگاه موردنظر نیز اینترنت داشته باشد با داشتن نام کاربری و کلمه عبور می‌توانیم تغییرات موردنظرمان را اعمال کنیم

با این حال استفاده از Telnet به‌هیچ‌عنوان راهکار مناسب و توصیه‌شده‌ای به شمار نمی‌آید. چراکه Telnet هیچ‌گونه مکانیزم رمزنگاری ندارد و به این معنی که رمز عبور شما زمانی که از Telnet برای اتصال به دستگاه موردنظر استفاده می‌کنید به‌صورت Clear text بر روی شبکه جابجا می‌شود و یک هکر می‌تواند این رمز عبور را به‌سادگی در شبکه شنود کرده و اطلاعات احراز هویتی شمارا به دست بیاورد. پروتکل Telnet به‌صورت ذاتی برای استفاده در شبکه‌های خصوصی و محرمانه طراحی‌شده است و به همین دلیل تمامی داده‌هایی که توسط این پروتکل منتقل می‌شوند به‌صورت Plain Text یا رمزنگاری نشده منتقل می‌شوند که این شامل تمامی اطلاعات هویتی ازجمله نام کاربری و رمز عبور مورداستفاده نیز می‌شود. گذشته از آن، با باز بودن پورت Telnet و درگاه مدیریت بر روی کل اینترنت دو خطر مهم دیگر نیز شبکه و تجهیزات شمارا تهدید جدی می‌کند. تهدید اول، شبکه‌های سازمان‌یافته که از طریق brute force و با آزمون‌وخطا سعی در پیدا کردن نام کاربری و رمز برای نفوذ به سیستم شما هستند که پس از نفوذ بتوانند از طریق دستگاه‌های شما و با هویت شما به طعمه‌های خود حمله کنند و تهدید دوم اینکه درصورتی‌که یک ضعف ناشناخته در تجهیزات شما بر روی پروتکل TELNET کشف شود، همین گروه‌های سازمان‌یافته بلافاصله از طریق Exploit های منتشرشده نبست به نفوذ به سیستم شما اقدام خواهند کرد و سیستم شما در صف اول دستگاه‌های آسیب‌پذیر قرار می‌گیرد.

**خطرات امنیتی استفاده از Telnet چیست؟**

چند مورد از مشکلاتی که می‌تواند در صورت سوءاستفاده از این پروتکل صورت پذیرد به شرح زیر است:

۱- ترافیک اینترنت شما (گیک مصرفی) بدون اطلاع شما مورداستفاده قرار می‌گیرد.

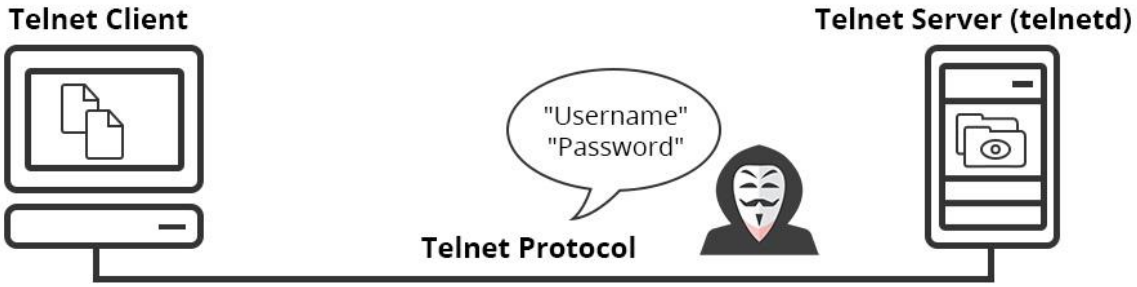
با آلوده شدن شبکه شما امکان برقراری ارتباط با برخی سایت‌ها مهم و معتبر مانند گوگل و یاهو و فیس‌بوک و... را نخواهید داشت چراکه این وب‌سایت‌ها شبکه و IP شمارا رصد می‌کنند و درصورتی‌که مهاجم شناخته شوید شمارا بلاک می‌کنند!

مورد حملات DOS قرار بگیرید.

چند مورد از رایج‌ترین حملات احتمالی در زیر آورده شده است:

**۱-** Sniff کردن ارتباط

Sniff کردن به معنای دریافت تمام اطلاعات ردوبدل شده بین شما و دستگاه موردنظرتان است. با توجه به اینکه این ارتباط یک ارتباط رمزنگاری نشده است فردی با قرار گرفتن در بین این ارتباط می‌تواند اطلاعات مهمی همچون رمز و دستورات واردشده را پیدا کند و ببیند .




شکل ۱

۲- حملات Brute Force

از سری حملات Cracking است به‌این‌ترتیب که یک کامپیوتر قدرتمند، یک ربات و یا حتی یک کامپیوتر شخصی، نام کاربری و رمز عبورهای مختلف را در هر ثانیه روی دستگاه شما امتحان می‌کند و درصورتی‌که موارد امنیتی رعایت نشده باشد امکان نفوذ در شبکه و پیدا کردن نام کاربری و رمز عبور وجود دارد.

۳- حملات DOS (Denial Of Service)

مدتی زیادی است هکرها از این روش استفاده می‌کنند در این حمله تمام پهنای باند موجود شما اشغال‌شده و علاوه بر استفاده از ترافیک سرویس بدون اطلاع شما، باعث ایجاد اختلال در ارتباط شبکه می‌شود به صورتی که همه پهنای باند موجود اشغال می‌شود و ارتباط بسیار کند یا قطع می‌شود.

**راهکارهای مقابله با این تهدیدها**

۱- با مشورت با مسئول شبکه خود در صورت عدم نیاز به این پورت روی دستگاه‌های شبکه این پورت (۲۳) را ببندید. برای بررسی باز یا بسته بودن این پورت در دستگاه‌های شبکه می‌توان از نرم‌افزارهای مختلفی همچون SolarWinds Free Port Scanner و Zenmap و PortCheckers و... که به شما امکان می‌دهد که پورت باز ۲۳ را در دستگاه‌های مختلف بیابید استفاده کنید.

۲- در صورت استفاده و یا نیاز به این پورت راحت‌ترین راه تغییر پورت پیش‌فرض تلنت از ۲۳ به پورت دیگری مانند ۲۳۲۳ است .

۳- تغییر نام کاربری و پسورد و استفاده از کاراکتر و عدد و حرف به‌صورت ترکیبی راه مؤثر دیگر است.

۴- به‌روزرسانی مداوم سیستم‌ها و دستگاه‌ها. چراکه در برخی از به‌روزرسانی‌ها (مانند تجهیزات Cisco) راهکارهای پیش فرضی در نظر گرفته‌شده است.

۵- محدودیت گذاشتن برای پهنای باند مورداستفاده هر دستگاه هم می‌تواند برای بهبود، به ما کمک کند چراکه در زمان ایجاد مشکل روی یکی از دستگاه‌ها تمام شبکه تحت تأثیر قرار نمی‌گیرد.