



راهنمای مشکل امنیتی موجود بر روی **Telnet**



راهنمای مشکل امنیتی موجود بر روی Telnet
تاریخ تنظیم : اردیبهشت ۱۳۹۸
گروه شرکت‌های شاتل

فهرست مطالب

Telnet چیست ؟

خطرات امنیتی استفاده از Telnet چیست ؟

راهکارهای مقابله با این تهدیدها



Telnet چیست؟ (Telecommunication network)

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

به دلیل استفاده کم از پهنای باند، سرعت بالا، در دسترس بودن همیشگی یک Terminal و عدم نیاز به نصب نرم‌افزار با حجم بالا از این پروتکل برای اتصال از راه دور به Device های موجود در شبکه استفاده می‌شود. به طوری که در هر کجا که باشیم و دسترسی به اینترنت داشته باشیم و دستگاه مورد نظر نیز اینترنت داشته باشد با داشتن شناسه و کلمه عبور می‌توانیم تغییرات مورد نظرمان را اعمال کنیم.

با این حال استفاده از Telnet به هیچ‌عنوان 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 مورد نظر استفاده می‌کنید به صورت Clear text بر روی شبکه جابجا می‌شود و یک هکر می‌تواند این رمز عبور را به سادگی در شبکه شنود کرده و اطلاعات احراز هویتی شما را به دست بیاورد. پروتکل Telnet به صورت ذاتی برای استفاده در شبکه‌های خصوصی و محرمانه طراحی شده است و به همین دلیل تمامی داده‌هایی که توسط این پروتکل منتقل می‌شوند به صورت Plain Text یا رمزنگاری نشده منتقل می‌شوند که این شامل تمامی اطلاعات هویتی از جمله نام کاربری و رمز عبور مورد استفاده 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 شما را تهدید جدی می‌کند. تهدید اول، شبکه‌های سازمان‌یافته که از طریق brute force و با آزمون و خطا سعی در پیدا کردن شناسه 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 در صورتی که یک ضعف ناشناخته در تجهیزات شما بر روی پروتکل TELNET کشف شود، همین گروه‌های سازمان‌یافته بلافاصله از طریق Exploit های منتشر شده نسبت به نفوذ به سیستم شما اقدام خواهند کرد و سیستم شما در صف اول دستگاه‌های آسیب‌پذیر قرار می‌گیرد.

خطرات امنیتی استفاده از Telnet چیست؟

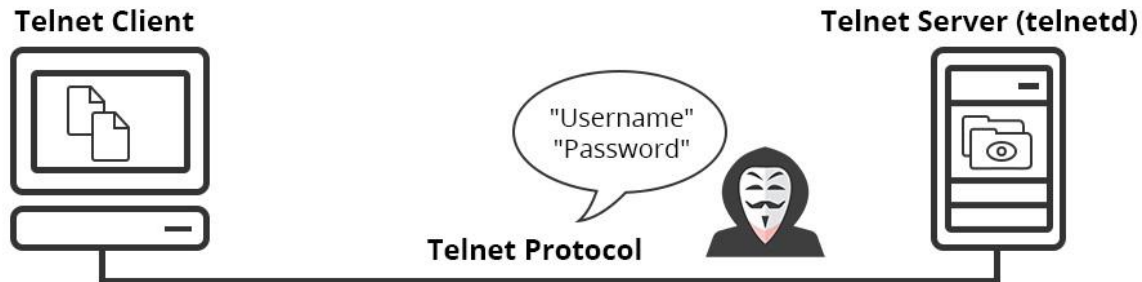
چند مورد از مشکلاتی که می‌تواند در صورت سوءاستفاده از این پروتکل صورت پذیرد به شرح زیر است:

- 1- ترافیک اینترنت شما (گیگ مصرفی) بدون اطلاع شما مورد استفاده قرار می‌گیرد.
- 2- 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 شما را رصد می‌کنند و در صورتی که مهاجم شناخته شوید شما را بلاک می‌کنند!
- 3- مورد حملات DOS قرار بگیرید.

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

- 1- 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 به این ترتیب که یک کامپیوتر قدرتمند، یک ربات و یا حتی یک کامپیوتر شخصی، شناسه و رمز عبورهای مختلف را در هر ثانیه روی دستگاه شما امتحان می‌کند و در صورتی که موارد امنیتی رعایت نشده باشد امکان نفوذ در شبکه و پیدا کردن شناسه 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 اشغال شده 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 این پورت در تمام دستگاه‌های شبکه می‌توان از نرم‌افزارهای مختلفی همچون **SolarWinds Free** و **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 شناسه و پسورد و استفاده از کاراکتر و عدد و حرف به صورت ترکیبی راه مؤثر دیگر است.
- ۴- به‌روزرسانی مداوم سیستم‌ها و دستگاه‌ها. چراکه در برخی از به‌روزرسانی‌ها (مانند تجهیزات **Cisco**) راهکارهای پیش فرضی در نظر گرفته شده است.
- ۵- محدودیت گذاشتن برای پهنای باند مورد استفاده 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.