باسمه تعالی

فعال بودن Telnet و قابل دسترس بودن آن از طریق شبکه اینترنت

پروتکل Telnet

Telnet یکی از پروتکل‌های قدیمی و منسوخ شبکه است که برای ارائه یک ارتباط دوطرفه متنی با استفاده از ترمینال‌های مجازی طراحی شده است (به جای استفاده از رابط کنسول). به‌طور پیش فرض، ارتباط بر بستر IP و روی پورت شماره ۲۳ پروتکل TCP برقرار می‌گردد. ابزارهای متنوعی در سیستم عامل‌های مختلف برای برقراری این نوع ارتباط طراحی و ارائه شده‌اند.

امنیت

به دلیل قدیمی بودن، این پروتکل ذاتاً دارای نقاط ضعف امنیتی جدی می‌باشد. عدم استفاده از روش‌های رمزنگاری، بزرگترین نقطه ضعف امنیتی این پروتکل است. از این‌رو نبایستی از آن برای دسترسی به سیستم‌های راه دور استفاده نمود. مهمترین نقاط ضعف این پروتکل عبارتند از:

- شنود: به دلیل عدم رمز نمودن اطلاعات تبادل شده، به راحتی زمینه شنود و استخراج اطلاعات مبادله شده همچون کلمات عبور فراهم است. از این‌رو استفاده از این پروتکل به‌جز در محیط‌های آزمایشگاهی ایزوله توصیه نمی‌گردد.
- آسیب‌پذیری نسبت به حملات BRUTE FORCE و دیکشنری برای یافتن کلمه عبور
- آسیب‌پذیری نسبت به حمله منع دسترسی (DOS): به راحتی می‌توان با ارسال حجم زیادی درخواست، مانع از اتصال کاربر اصلی به ماشین سرویس‌دهنده شد.
- امکان استخراج اطلاعات: اطلاعات نمایش داده شده در بنر می‌تواند منجر به افشای اطلاعاتی درخصوص سخت‌افزار و نرم‌افزار گردد. این امر می‌تواند روند سوءاستفاده از آسیب‌پذیری‌های موجود را تسریع نماید.

ماشین‌هایی که سرویس Telnet بر روی آن‌ها فعال بوده و از طریق شبکه اینترنت قابل دسترسی هستند، بسیار مورد توجه نفوذگران بوده و به راحتی قابل تسخیر هستند. پس از تسخیر، ماشین قربانی می‌تواند در سناریوهای حمله مختلف همچون DDOS و غیره مورد استفاده قرار گیرد.

توصیه

بررسی‌های انجام گرفته توسط مرکز ماهر نشان می‌دهد که سرویس Telnet بر روی تعدادی از آدرس‌های IP قابل دسترس از طریق اینترنت آن مجموعه فعال است (لیست پیوست). اکیداً توصیه می‌گردد که راهبران شبکه

مطمئن شوند که بر روی هیچ یک از آدرس‌های Valid IP تحت کنترل آن‌ها، سرویس Telnet فعال نمی‌باشد. درصورت لزوم استفاده از ارتباط راه دور متنی، بایستی از سرویس SSH استفاده نمایند که به‌طور امن پیکربندی شده است.