|  |  |  |  |
| --- | --- | --- | --- |
| S02 T01 | | | Importance of Server Hardening |
| Recognizing potential threats | | |
| --- | | Caret Right with solid fill | امنیت سرورهای لینوکس یکی از مهمترین دغدغه‌ها در مدیریت سیستم‌های اطلاعاتی است. سخت‌سازی سرور به معنای اعمال تدابیر و اقدامات امنیتی برای محافظت از سیستم در برابر تهدیدات و حملات مختلف می‌باشد. یکی از بخش‌های اساسی این فرآیند، شناخت تهدیدات احتمالی است. شناخت دقیق و کامل تهدیدات می‌تواند به مدیران سیستم‌ها کمک کند تا تدابیر مناسب‌تری برای محافظت از سرورهای خود اتخاذ کنند. |
| بعد از |
| Understanding types of attacks | | Caret Left with solid fill |
| قبل از |
| راهنمای عملی: خیر | پژوهشی: **بله** | | پیاده سازی عملی: **خیر** |

## شناخت تهدیدات احتمالی در اهمیت سخت‌سازی سرور

امنیت سرورهای لینوکس یکی از مهمترین دغدغه‌ها در مدیریت سیستم‌های اطلاعاتی است. سخت‌سازی سرور به معنای اعمال تدابیر و اقدامات امنیتی برای محافظت از سیستم در برابر تهدیدات و حملات مختلف می‌باشد. یکی از بخش‌های اساسی این فرآیند، شناخت تهدیدات احتمالی است. شناخت دقیق و کامل تهدیدات می‌تواند به مدیران سیستم‌ها کمک کند تا تدابیر مناسب‌تری برای محافظت از سرورهای خود اتخاذ کنند.

### تهدیدات رایج

* حملات بدافزاری: بدافزارها از جمله ویروس‌ها، کرم‌ها، و تروجان‌ها می‌توانند به سیستم‌ها نفوذ کرده و باعث تخریب یا سرقت اطلاعات شوند.
* حملات DDoS: حملات منع سرویس توزیع‌شده که با ارسال ترافیک زیاد به سرور، باعث اختلال در خدمات‌رسانی آن می‌شوند.
* حملات Brute Force: در این نوع حمله، مهاجم با امتحان کردن تمامی ترکیب‌های ممکن برای رمز عبور، سعی در دسترسی به سیستم دارد.
* نقص‌های امنیتی نرم‌افزاری: آسیب‌پذیری‌ها و باگ‌های موجود در نرم‌افزارهای نصب‌شده روی سرور می‌تواند به مهاجمان اجازه دسترسی غیرمجاز به سیستم را بدهد.

ابزارها و برنامه‌های شناسایی تهدیدات

برای شناسایی و مقابله با تهدیدات احتمالی، ابزارها و برنامه‌های مختلفی وجود دارند که به مدیران سیستم کمک می‌کنند تا سرورهای خود را ایمن کنند. برخی از این ابزارها عبارتند از:

* **Snort**: یک سیستم تشخیص نفوذ مبتنی بر شبکه است که قادر است حملات و تهدیدات را شناسایی و گزارش دهد.
* **Fail2Ban**: این برنامه با نظارت بر لاگ‌های سیستم و تشخیص تلاش‌های مشکوک برای ورود، می‌تواند آدرس‌های IP مشکوک را به طور موقت مسدود کند.
* **Lynis** : ابزاری برای ارزیابی امنیتی و حسابرسی لینوکس که به شناسایی مشکلات امنیتی و ارائه توصیه‌های اصلاحی می‌پردازد.
* **Nmap** : ابزاری قدرتمند برای اسکن شبکه که به مدیران سیستم امکان می‌دهد تا پورت‌های باز و خدمات فعال روی سرور را شناسایی کنند.
* **AIDE (Advanced Intrusion Detection Environment)**: ابزاری برای تشخیص تغییرات در فایل‌های سیستم که می‌تواند به شناسایی فعالیت‌های مشکوک کمک کند.

## نتیجه‌گیری

شناخت تهدیدات احتمالی یکی از مراحل حیاتی در فرآیند سخت‌سازی سرور است. با آگاهی از انواع حملات و استفاده از ابزارهای مناسب برای شناسایی و مقابله با آن‌ها، مدیران سیستم می‌توانند گامی مؤثر در جهت حفظ امنیت و پایداری سرورهای خود بردارند. حفظ امنیت سرورها نیازمند تلاش مستمر و بروز نگه‌داشتن اطلاعات امنیتی و ابزارهای مرتبط است.

## منابع و ارجاعات

* <https://roadmap.sh/linux>
* <https://roadmap.sh/r/general-linux-server-hardening>