



Importance of Server Hardening	S02 T03	
	Realizing the risk of unhardened systems	
<p>امنیت سرورها از اهمیت بالایی برخوردار است و یکی از اصلی‌ترین روش‌های افزایش امنیت، سخت‌سازی سرورها است. اما بسیاری از مدیران سیستم ممکن است اهمیت این موضوع را نادیده بگیرند و به همین دلیل سیستم‌های خود را در معرض خطرات جدی قرار دهند. درک ریسک‌های ناشی از سیستم‌های سخت‌سازی نشده به مدیران سیستم کمک می‌کند تا اهمیت این فرآیند را بهتر بفهمند و اقدامات لازم را برای افزایش امنیت سیستم‌های خود انجام دهند.</p>		Understanding types of attacks
	بعد از	
		Appreciating the need for continuous security monitoring
	قبل از	
پیاده سازی عملی: خیر	پژوهشی: بله	راهنمای عملی: خیر

درک ریسک سیستم‌های سخت‌سازی نشده در اهمیت سخت‌سازی سرور

امنیت سرورها از اهمیت بالایی برخوردار است و یکی از اصلی‌ترین روش‌های افزایش امنیت، سخت‌سازی سرورها است. اما بسیاری از مدیران سیستم ممکن است اهمیت این موضوع را نادیده بگیرند و به همین دلیل سیستم‌های خود را در معرض خطرات جدی قرار دهند. درک ریسک‌های ناشی از سیستم‌های سخت‌سازی نشده به مدیران سیستم کمک می‌کند تا اهمیت این فرآیند را بهتر بفهمند و اقدامات لازم را برای افزایش امنیت سیستم‌های خود انجام دهند.

ریسک‌های سیستم‌های سخت‌سازی نشده

- **افزایش آسیب‌پذیری:** سیستم‌های سخت‌سازی نشده به دلیل داشتن پیکربندی‌های پیش‌فرض و تنظیمات ناامن، مستعد به انواع حملات سایبری هستند. این آسیب‌پذیری‌ها می‌توانند به مهاجمان اجازه دهند تا به سیستم دسترسی پیدا کنند و اطلاعات حساس را سرقت کنند.
- **نقص در مدیریت دسترسی:** در سیستم‌های سخت‌سازی نشده، مدیریت دسترسی به منابع و اطلاعات به درستی انجام نمی‌شود. این مسئله می‌تواند به کاربران غیرمجاز اجازه دسترسی به داده‌های حساس را بدهد و منجر به نقض حریم خصوصی شود.
- **احتمال بالای نفوذ:** سیستم‌های بدون سخت‌سازی مستعد به حملات نفوذی هستند. مهاجمان می‌توانند با استفاده از ضعف‌های امنیتی موجود در سیستم به راحتی به آن نفوذ کنند و از آن برای اهداف مخرب خود استفاده کنند.
- **افت عملکرد و قطع خدمات:** حملات DDoS و سایر حملات سایبری می‌توانند باعث افت عملکرد سرور و حتی قطع خدمات شوند. این مسئله می‌تواند به سازمان‌ها ضررهای مالی و اعتباری زیادی وارد کند.
- **جرایم سایبری و نقض قوانین:** عدم سخت‌سازی سرورها می‌تواند منجر به جرایم سایبری و نقض قوانین و مقررات مرتبط با حفظ امنیت داده‌ها شود. این مسئله می‌تواند سازمان‌ها را با جریمه‌های سنگین و دعاوی حقوقی مواجه کند.

ابزارها و برنامه‌های کمک کننده

برای کاهش ریسک‌های سیستم‌های سخت‌سازی نشده، ابزارها و برنامه‌های مختلفی وجود دارند که به مدیران سیستم کمک می‌کنند تا امنیت سرورهای خود را افزایش دهند. برخی از این ابزارها عبارتند از:

- **Bastille Linux**: ابزاری که به سخت‌سازی سیستم‌های لینوکسی کمک می‌کند و توصیه‌های امنیتی را برای افزایش امنیت سیستم ارائه می‌دهد.
- **CIS-CAT (CIS Configuration Assessment Tool)**: ابزاری که با ارزیابی تنظیمات سیستم بر اساس بنچمارک‌های امنیتی CIS، نقاط ضعف و ریسک‌های امنیتی را شناسایی می‌کند.
- **OpenSCAP**: مجموعه‌ای از ابزارهای منبع باز برای ارزیابی آسیب‌پذیری‌ها و سخت‌سازی سیستم‌های لینوکسی که به مدیران سیستم کمک می‌کند تا امنیت سیستم‌های خود را بهبود بخشند.
- **Auditd**: ابزاری برای ثبت و تحلیل لاگ‌های امنیتی که به شناسایی و بررسی فعالیت‌های مشکوک و غیرمجاز کمک می‌کند.

نتیجه‌گیری

درک ریسک‌های ناشی از سیستم‌های سخت‌سازی نشده یکی از مراحل اساسی در افزایش امنیت سرورها است. با شناخت این ریسک‌ها و استفاده از ابزارهای مناسب برای سخت‌سازی سیستم‌ها، مدیران می‌توانند اقدامات مؤثری برای محافظت از سرورهای خود در برابر تهدیدات سایبری انجام دهند. امنیت سرورها نیازمند توجه و تلاش مداوم برای به‌روزرسانی و بهبود تدابیر امنیتی است تا سازمان‌ها بتوانند از داده‌ها و اطلاعات خود به بهترین شکل ممکن محافظت کنند.

منابع و ارجاعات

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

