



Importance of Server Hardening	S02 T02	
	Understanding types of attacks	
<p>در دنیای دیجیتال امروز، امنیت سرورها نقش حیاتی در محافظت از داده‌ها و اطلاعات سازمان‌ها دارد. یکی از مؤلفه‌های اصلی در سخت‌سازی سرورها، درک انواع حملات است. آگاهی از انواع حملاتی که ممکن است بر سرورهای لینوکس انجام شود، به مدیران سیستم کمک می‌کند تا راهکارهای مناسبی برای جلوگیری و مقابله با آنها اتخاذ کنند.</p>		Recognizing potential threats
	بعد از	
		Realizing the risk of unhardened systems
	قبل از	
پیاده سازی عملی: خیر	پژوهشی: بله	راهنمای عملی: خیر

درک انواع حملات در اهمیت سخت‌سازی سرور

در دنیای دیجیتال امروز، امنیت سرورها نقش حیاتی در محافظت از داده‌ها و اطلاعات سازمان‌ها دارد. یکی از مؤلفه‌های اصلی در سخت‌سازی سرورها، درک انواع حملات است. آگاهی از انواع حملاتی که ممکن است بر سرورهای لینوکس انجام شود، به مدیران سیستم کمک می‌کند تا راهکارهای مناسبی برای جلوگیری و مقابله با آن‌ها اتخاذ کنند.

انواع حملات رایج

- **حملات بدافزاری:** این نوع حملات شامل ورود بدافزارها مانند ویروس‌ها، کرم‌ها و تروجان‌ها به سیستم می‌شود که می‌توانند به تخریب داده‌ها، سرقت اطلاعات و یا ایجاد دسترسی غیرمجاز منجر شوند.
- **حملات فیشینگ:** در این حملات، مهاجمان با استفاده از ایمیل‌ها و وب‌سایت‌های جعلی تلاش می‌کنند تا اطلاعات حساس کاربران مانند رمزهای عبور و اطلاعات بانکی را به دست آورند.
- **حملات (Denial of Service) DDoS:** در حملات منع سرویس توزیع‌شده، مهاجمان با ارسال حجم بزرگی از ترافیک به سرور، سعی در ایجاد اختلال در عملکرد سرور و قطع دسترسی کاربران به خدمات دارند.
- **حملات Brute Force:** در این نوع حمله، مهاجم با آزمایش ترکیبات مختلف رمز عبور سعی می‌کند تا به حساب‌های کاربری دسترسی پیدا کند.
- **حملات (Cross-Site Scripting) XSS:** در این حملات، مهاجم کدهای مخرب را در وب‌سایت‌ها تزریق می‌کند تا اطلاعات کاربرانی که از آن سایت بازدید می‌کنند، سرقت شود.
- **حملات SQL Injection:** این حملات با تزریق کدهای SQL مخرب به برنامه‌های وب، مهاجمان را قادر می‌سازد تا به داده‌های پایگاه داده دسترسی غیرمجاز پیدا کنند.

ابزارها و برنامه‌های مقابله با حملات

برای مقابله با حملات مختلف، ابزارها و برنامه‌های متعددی وجود دارند که به مدیران سیستم کمک می‌کنند تا امنیت سرورهای خود را افزایش دهند. برخی از این ابزارها عبارتند از:

- **Suricata**: یک سیستم تشخیص نفوذ پیشرفته است که می‌تواند حملات شبکه‌ای را شناسایی و گزارش دهد.
- **ModSecurity**: یک فایروال برنامه‌های وب (WAF) است که برای محافظت از برنامه‌های وب در برابر حملات مختلف از جمله XSS و SQL Injection استفاده می‌شود.
- **OSSEC**: یک سیستم تشخیص نفوذ مبتنی بر میزبان (HIDS) است که به مانیتورینگ و تحلیل لاگ‌های سیستم برای شناسایی فعالیت‌های مشکوک کمک می‌کند.
- **Tripwire**: ابزاری برای نظارت بر تغییرات فایل‌های سیستم و شناسایی تغییرات مشکوک که می‌تواند به تشخیص نفوذها کمک کند.
- **Wireshark**: یک ابزار تحلیل پروتکل شبکه است که به مدیران سیستم امکان می‌دهد تا ترافیک شبکه را به دقت بررسی کرده و حملات شبکه‌ای را شناسایی کنند.

نتیجه‌گیری

درک انواع حملات یکی از مراحل ضروری در فرآیند سخت‌سازی سرور است. با شناخت دقیق و کامل از انواع حملات و استفاده از ابزارهای مناسب برای مقابله با آن‌ها، مدیران سیستم می‌توانند به طور مؤثرتری از سرورهای خود محافظت کنند. امنیت سرورها نیازمند به‌روزرسانی مداوم دانش امنیتی و استفاده از ابزارهای پیشرفته برای شناسایی و جلوگیری از حملات است.

منابع و ارجاعات

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