# امن کردن کلاینت لینوکسی

# در ۹ گام

**محمدتقی روغنی**

MTRoghani.ir

اردیبهشت ۱۳۹۶



## مقدمه:

این مقاله بر اساس مستندات منتشرشده توسط Linux Foundation جهت امن‌سازی توزیعات مختلف لینوکسی، تهیه شده است.

هرچند هدف مطالب ذکر شده در این مقاله، نسخه‌های کلاینتی لینوکس است؛ ولی شما می‌توانید این موارد را جهت امنیت سرورهای لینوکسی نیز مدنظر قرار دهید.

۹ گام ذکر شده در این مقاله فارغ از نوع توزیع مورد استفاده کلاینت، باید مورد توجه قرار گرفته و اجرا شوند. البته توجه داشته باشید که ممکن است با توجه به شرایط هر کاربر انجام هریک از گام‌ها متفاوت باشد.

در این مقاله، موارد امنیتی در قالب ۹ گام ذکر شده که فقط به معرفی مختصر آن‌ها بسنده شده است. اگر شما برای انجام هریک از گام‌ها نیاز به آگاهی بیشتری داشته باشید، باید بر اساس نوع توزیعی که مورد استفاده قرار می‌دهید اطلاعات بیشتری را جستجو نمایید.

البته بنده با توجه به تعداد درخواست‌ها ممکن است مقالات و یا ویدئوهای آموزشی اختصاصی جهت هریک از موضوعات مطرح شده در این مقاله ارائه نمایم.

راه‌های ارتباطی با بنده در زیر مشخص شده است. منتظر درخواست‌ها، نظرات، پیشنهادات و انتقادات شما عزیزان هستم.

موفق باشید

http://www.MTRoghani.ir
https://t.me/MTRoghani_ir
MTRoghani@Gmail.com
http://www.aparat.com/mtroghani_ir

## گام اول:

### غیرفعال کردن ماژول‌های firewire و thunderbolt

شما باید ماژول‌های firewire و thunderbolt را به صورت کامل غیرفعال نمایید. برای این کار می‌توانید ماژول‌ها را در Black List قرار دهید تا از لود شدن آنها جلوگیری شود.
جهت قرار دادن ماژول‌ها داخل Black List، باید فایل زیر را ادیت نموده و نام ماژول مورد نظر را به فایل اضافه نمایید:

*/etc/modprobe.d/blacklist-dma.conf*:

```
blacklist firewire-core
blacklist thunderbolt
```

## گام دوم:

### بستن تمام پورت‌های ورودی بر روی فایروال

اطمینان حاصل نمایید که فایروال سیستم‌عامل شما تمام پورت‌های ورودی به سیستم را مسدود کرده باشد. البته بسته‌بودن تمام پورت‌ها یک پیشنهاد کلی است و اگر شما اطمینان دارید که باید پورت ورودی خاصی بر روی سیستم شما باز باشد، می‌توانید آن پورت را فعال نمایید.
با توجه به توزیع مورد استفاده، نوع فایروال نیز ممکن است متفاوت باشد. پس لازم است با توجه به فایروال سیستم، آن را چک نمایید که تمام پورت‌های ورودی را غیرفعال کرده باشد و در غیر اینصورت خودتان اقدام به غیر فعال نمودن ورودی‌های فایروال نمایید.

## گام سوم:

### انتقال اطلاعات Root Mail به یک اکانت در دسترس

در اکثر توزیعات لینوکسی، مهمترین اتفاقات روی داده بر روی سیستم برای اکانت root سیستم ایمیل می‌شود. متاسفانه غالب کاربران به ایمیل‌های ارسال شده برای کاربر root که بر روی خود سیستم نیز ذخیره می‌شود، اعتنایی ندارند و هیچ‌گاه توسط آن‌ها خوانده نمی‌شود.
شما برای اطمینان از اینکه این ایمیل‌های مهم خوانده شوند و اطلاعات ارزشمند آن‌ها از دست نرود؛ بهتر است آن‌را به یک اکانت ایمیل دیگر که همواره مورد توجه است، انتقال دهید.
شما برای انتقال ایمل‌های اکانت root، می‌توانید یکی از این روش‌ها را مورد استفاده قرار دهید:

روش اول:
ایجاد یک فایل با نام forward. در داخل home directory کاربر root و نوشتن آدرسهای ایمیل مورد نظر داخل آن:

*/root/.forward*:

```
MTRoghani@Gmail.com
```

روش دوم:
ویرایش فایل زیر و مشخص کردن آدرس ایمیل مورد نظر:

*/etc/aliases*:

```
# Person who should get root’s mail
root:                   MTRoghani@Gmail.com
```

برای اطمینان از عملکرد صحیح forwarding، پس از انجام تنظیمات فوق، از دستور newaliases استفاده نمایید.



توجه داشته باشید، به دلیل تنظیمات سرویس ایمیل و نام دامین، ممکن است که سیستم ایمیل را ارسال نکند و یا در صورت ارسال در هرزنامه‌های گیرنده قرار گیرد.

## گام چهارم:

### تنظیم برنامه به‌روز رسانی خودکار و یا یادآوری به‌روز رسانی

باید تنظیمات برنامه به‌روز رسانی سیستم خود را با دقت انجام داده و آن‌را فعال نمایید؛ تا همواره سیستم منابع معتبر را جهت آپدیت‌های جدید بررسی نموده و اطلاع رسانی نماید. شما می‌توانید تنظیمات را طوری انجام دهید که تمام به‌روز رسانی‌ها به صورت خودکار دانلود و نصب شوند. البته این کار خطرات خاص خود را نیز دارد.
روش دیگر این است که سیستم را تنظیم کنید که ارائه به‌روز رسانی‌ها را به شما اطلاع دهد و سپس خوتان تصمیم به دانلود و نصب آن‌ها بگیرید.
لازم به ذکر است که تلفیق هر دو روش فوق نیز امکانپذیر است. یعنی سیستم Patchهای Critical را به صورت خودکار دانلود و نصب نموده؛ و برای سایر به‌روز رسانی‌ها فقط به یادآوری آن به کاربر، بسنده نماید.

## گام پنجم:

### غیرفعال کردن سرویس sshd

سرویس sshd که فراهم‌کننده دسترسی راه دور است را بر روی سیستم خود غیرفعال نمایید.
همانطور که خیلی بعید است کسی از این سرویس برای دسترسی به سرورهای لینوکسی بهره نبرد؛ به همان میزان نیز بعید به نظر می‌رسد کلاینتی بخواهد با ssh از سیستم خود استفاده کند.
لذا پیشنهاد می‌شود که این سرویس به صورت کامل بر روی سیستم‌عامل کلاینت غیرفعال شده و در موارد خاص و زمان مورد نیاز آن‌را فعال نموده و پس از رفع نیاز، مجدد سرویس را غیر فعال نمایید.
برای غیرفعال کردن سرویس sshd می‌توانید از دستورات زیر استفاده نمایید:

```
systemctl disable sshd.service
systemctl stop sshd.service
```

## گام ششم:

### تنظیم محافظ صفحه نمایش برای قفل کردن سیستم

یکی از کارهای مهمی که کلاینت در زمان ترک سیستم باید انجام دهد، Lock کردن سیستم است. شما باید تنظیمات محافظ صفحه نمایش (Screen Saver) را طوری انجام دهید که در صورت غفلت کاربر، سیستم بعد از مدت زمان مشخصی که در حالت idle می‌ماند به‌صورت خودکار اقدام به قفل نمودن سیستم‌عامل نماید. در اینصورت برای خارج کردن سیستم از حالت Lock، نیاز است که مجددا Password وارد شود.

## گام هفتم:

### تنظیم Logwatch

قاعدتا همه علاقه‌مند هستند تا بدانند چه اتفاقاتی روی سیستمشان رخ داده است. شما برای آگاهی از کارهایی که روی سیستم‌تان انجام گرفته، باید به سراغ لاگ‌های سیستم بروید. البته خواندن لاگ‌های تولید شده توسط سیستم کار سخت و خسته‌کننده‌ای محسوب می‌شود، لذا بهتر است از یک برنامه که به شما در خواندن و طبقه‌بندی لاگ‌ها کمک می‌کند، استفاده نمایید.
توصیه می‌شود برای خوانا شدن لاگ‌ها و همچنین فهم بهتر آن، برنامه Logwatch را بر روی سیستم خود نصب کنید.
علاوه بر طبقه‌بندی لاگ و خواناترشدن اطلاعات، برنامه Logwatch می‌تواند لاگ‌های مورد نظر را بر اساس زمانبندی تعیین شده، برای شما ارسال نماید. ارسال یک نسخه از لاگ‌های مهم به خارج از سیستم می‌تواند کمک قابل توجهی در زمان ردیابی و اشکال‌یابی سیستم‌هایی که لاگ آنها از بین رفته و یا سیستم به‌صورت کلی دچار مشکل شده، به شما نماید.

قبل از استفاده از برنامه‌ای مانند Logwatch، حتما مطمئن شوید توزیع مورد استفاده شما دارای سیستم لاگ‌گیری فعال بوده و فایل‌های مسیر /var/log خالی نباشند.

## گام هشتم:

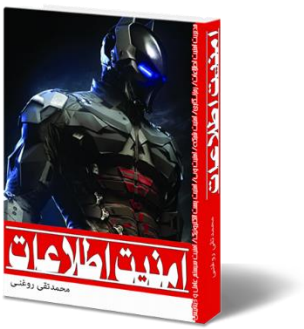
### نصب یک برنامه ضد RootKit

یکی از مهمترین تهدیدات امنیتی برای سیستم‌ها، وجود rootkit است. کدهای مخربی که با نام rootkit نامیده می‌شوند، فراهم کننده دسترسی در سطح کاربر Root برای هکر است.
برای اینکه شما سیستم خود را در مقابل Rootkitها محافظت کنید، توصیه می‌شود که یک برنامه Anti-Rootkit بر روی لینوکس خود نصب نمایید.
یکی از معروفترین برنامه‌های Anti-Rootkit مورد استفاده در سیستم‌های لینوکسی، برنامه RKHunter است. شما باید این برنامه را روی سیستم خود نصب کرده و حداقل روزی یکبار آن را اجرا نمایید.
RKHunter و برنامه‌هایی از این قبیل علاوه بر اینکه از وجود Rootkitهای معمول جلوگیری می‌کند؛ همچنین می تواند شما را از اشتباهات احتمالی کاربری در تنظیمات سیستم، که دسترسی root را در اختیار هکر قرار می‌دهد، آگاه نماید.

## گام نهم:

### نصب یک برنامه تشخیص نفوذ (IDS)

یکی از راه‌های کشف نفوذهای انجام گرفته بر روی سیستم‌عامل، تشخیص تغییرات به‌وجود آمده در فایل‌های سیستمی است.
شما برای جلوگیری از نفوذ هکر به سیستم خود، باید یک سیستم تشخیص نفوذ یا IDS بر روی سیستم‌عامل خود نصب و راه‌اندازی نمایید. این برنامه‌ها با بررسی فایل‌های سیستمی مشخص می‌نمایند که آیا در وضعیت این فایل‌ها نسبت به قبل تغییری به‌وجود آمده است یا نه!
از جمله برنامه‌های مشهوری که به عنوان IDS در سیستم‌عامل لینوکس مورد استفاده قرار می‌گیرند می‌توان به Aide و Tripwire اشاره نمود.




**کتاب امنیت اطلاعات**

**مؤلف: محمدتقی روغنی**

**٤٤٨ صفحه، وزیری**




**کتاب شبکه؛صفرتاصد**

**مؤلف: محمدتقی روغنی**

**٥٤٦ صفحه، وزیری**

اطلاعات بیشتر در:

http://MTRoghani.ir

**کانال تلگرامی کتاب‌ها، مقالات و ویدئوهای آموزشی:**

**https://t.me/mtroghani_ir**