راهنمای جامع امن‌سازی سیستم‌عامل CentOS

1. مقدمه

یکی از اصول پذیرفته شده در حوزه امنیت فضای تبادل اطلاعات، امنیت لایه‌ای یا دفاع در عمق[1] است. براساس این اصل بایستی امنیت را در لایه‌های مختلف شبکه پیاده‌سازی نمود. این امر موجب می‌شود که اگر یک لایه امنیتی با مشکل مواجه شد، هنوز لایه‌های دیگر قادر به تأمین امنیت باشند.

امن‌سازی خود سیستم‌عامل (صرف‌نظر از سایر لایه‌های حفاظتی مانند به‌کارگیری انواع برنامه‌های کاربردی ضد بدافزار، به‌روزرسانی مداوم و ...) یکی از لایه‌های مهم امنیتی است که متأسفانه اغلب مورد فراموشی واقع می‌گردد. بدون تردید یک کامپیوتر با سیستم‌عامل لینوکس بسیار امن‌تر از همان کامپیوتر با سایر سیستم‌عامل‌ها مخصوصاً ویندوز خواهد بود. نکته مهم این است که همیشه برای رسیدن به یک سطح خوب امنیتی حتماً لازم نیست از نرم‌افزارهای امنیتی و تکنیک‌های خاص استفاده گردد. گاهی اوقات آسان ترین راه‌ها برای کسب امنیت، آن‌هایی هستند که به آسانی فراموش می‌شوند.

مستند حاضر، راهنمایی جامع و کاربردی جهت امن‌سازی سیستم‌عامل Cent OS است که در آن به تفصیل و با ذکر جزئیات به موضوع پرداخته شده است. جزئیات امن‌سازی به‌گونه‌ای بیان شده که هم مراحل نصب جدید سیستم‌عامل و هم مراحل امن‌سازی یک سیستم‌عامل نصب شده و در حال کار را پوشش دهد. علاوه‌بر آن، این مستند شامل جزئیات نحوه بررسی وضعیت امنیتی سیستم‌عامل نیز هست.

این مستند با حمایت مرکز ماهر و توسط مرکز تخصصی آپا دانشگاه صنعتی اصفهان تهیه شده و عمدتاً مورد استفاده راهبران شبکه‌ای است که سیستم‌عامل Cent OS در شبکه تحت کنترل آن‌ها وجود دارد. این راهنما

[1] Defense in Depth

برای نسخه 7 این سیستم‌عامل تهیه شده است ولی می‌تواند برای نسخه‌های قدیمی‌تر نیز به‌کار گرفته شود (در قریب به اتفاق موارد سازگار است).

2. نصب به‌روزرسانی‌ها، وصله‌ها و نرم‌افزارهای امنیتی جانبی

2-1. پیکربندی فایل‌های سیستمی

شاخه‌هایی که برای عملکرد سیستم مورد استفاده قرار می‌گیرند را می‌توان با قرار دادن در پارتیشن‌های جداگانه بیشتر محافظت نمود. این کار از خستگی و فرسودگی منابع جلوگیری می‌کند و امکان به‌کارگیری گزینه‌هایی مناسب، برای شاخه‌های در نظر گرفته شده را مهیا می‌سازد. داده‌های کاربر می‌تواند در پارتیشن‌های جداگانه ذخیره گردد.

پارتیشن کاربر به فایل‌سیستمی گفته می‌شود که برای استفاده کاربر ایجاد شده و شامل فایل‌ها و نرم‌افزارهای سیستم‌عامل نمی‌باشد. دستورات این بخش اگر هنگام نصب اولیه سیستم‌عامل اعمال شود آسان‌تر است. در صورتی‌که سیستم‌عامل هم‌اکنون نصب شده است، توصیه می‌گردد قبل از پارتیشن‌بندی مجدد یک نسخه پشتیبان کامل از سیستم گرفته شود.

نکته: اگر تصمیم به پارتیشن‌بندی مجدد سیستم‌عامل نصب‌شده‌ای دارید، اطمینان حاصل کنید که داده‌های مهم به پارتیشن جدید کپی شده و آن پارتیشن unmount شده است. سپس داده‌ها را از شاخه پارتیشن قدیمی حذف کنید در غیر این‌صورت هنوز هم در پارتیشن قدیمی فضا مصرف می‌کند تا زمانی‌که فایل سیستم جدید نصب شود. برای مثال اگر یک سیستم در حالت تک‌کاربره بدون هیچ فایل سیستمی باشد و راهبر سیستم داده‌های زیادی به شاخه /tmp اضافه کند، این داده‌ها هنوز از فضای / استفاده می‌کنند تا زمانی‌که فایل سیستم /tmp نصب شود، مگر اینکه ابتدا حذف شده باشند.

2-1-1. ایجاد پارتیشن مجزا برای tmp/

شاخه tmp/ شاخه‌ای با مجوز همگانی نوشتن است که برای ذخیره فایل‌های temp تمام کاربران و بعضی نرم‌افزارها استفاده می‌گردد.

از آن‌جایی‌که شاخه tmp/ دارای مجوز همگانی نوشتن است، اگر یک پارتیشن جداگانه برایش در نظر گرفته نشود، خطر فرسودگی منابع وجود خواهد داشت. به‌علاوه راهبر سیستم می‌تواند با تنظیم گزینه‌ی noexec، شاخه tmp/ را برای مهاجمانی که می‌خواهند کدهای اجرایی نصب کنند، بی‌استفاده سازد. شاخه ذخیره سازی موقت همانند tmp/ فضای ذخیره‌سازی را برای کارهای اجرایی مخرب فراهم می‌کند به‌طوری‌که مهاجمان، می‌توانند فایل‌های اجرایی را در شاخه tmp/ ذخیره و از فضاهای آن برای اجرای برنامه‌های مخرب استفاده کرده و باعث هک شدن سیستم شوند.

این کار از ایجاد یک hardlink توسط مهاجمان به یک برنامه setuid و انتظار برای به‌روزرسانی آن جلوگیری می‌کند. وقتی یک برنامه به‌روزرسانی می‌شود، hardlink شکسته شده و یک کپی از برنامه در اختیار مهاجم قرار می‌گیرد. اگر برنامه آسیب‌پذیری امنیتی داشته باشد، مهاجم با استفاده از آن نقص به کارش ادامه خواهد داد.

نحوه بررسی صحت پیکربندی امن:

در صورت صحت پیکربندی امن، بایستی پارتیشن tmp/ در فایل etc/fstab/ وجود داشته باشد. برای بررسی این منظور می‌توان از دستور زیر استفاده نمود:

```
# grep "[[:space:]]/tmp[[:space:]]" /etc/fstab
```

نحوه اجرای پیکربندی امن:

هنگام نصب سیستم عامل جدید، بایستی در طول نصب، یک پارتیشن مخصوص برای tmp/ ساخت (تیک زدن باکس "Review and modify partitioning" و ایجاد پارتیشن جدید tmp/).

برای سیستم‌هایی که قبلاً نصب شده‌اند، بایستی از LVM[2] برای ساخت پارتیشن استفاده کرد.

2-1-2. تنظیم گزینه nodev برای پارتیشن tmp/

انتخاب گزینه nodev در هنگام mount شدن فایل‌سیستم مانع از آن می‌گردد که آن فایل‌سیستم شامل دستگاه‌های خاص[3] باشد. از آن‌جایی‌که شاخه tmp/ برای پشتیبانی از دستگاه‌ها در نظر نگرفته شده است، تنظیم گزینه فوق این اطمینان را به‌وجود می‌آورد که کاربران نمی‌توانند اقدام به ایجاد تجهیزات خاص در tmp/ کنند.

نحوه بررسی صحت پیکربندی امن:

با اجرای دستورهای زیر می‌توان مطمئن شد که سیستم به درستی پیکربندی شده است.

```
# grep "[[:space:]]/tmp[[:space:]]" /etc/fstab | grep nodev
# mount | grep "[[:space:]]/tmp[[:space:]]" | grep nodev
```

اگر هیچ یک از دو دستور فوق خروجی نداشته باشند، سیستم به‌صورت امن پیکربندی نشده است.

نحوه اجرای پیکربندی امن:

بایستی فایل /etc/fstab ویرایش شده و nodev به فیلد چهارم (گزینه‌های mounting) اضافه شود.

```
# mount -o remount,nodev /tmp
```

[2] Logical Volume Manager
[3] special devices

2-1-3. تنظیم گزینه nosuid برای پارتیشن /tmp

انتخاب گزینه nosuid مشخص می‌کند که فایل‌سیستم نمی‌تواند شامل مجموعه فایل‌های userid باشد. از آن‌جایی‌که فایل‌سیستم /tmp فقط برای ذخیره فایل‌های temp در نظر گرفته شده است، اعمال این گزینه این اطمینان را به‌وجود می‌آورد که کاربران نمی‌توانند مجموعه فایل‌های userid را در /tmp ایجاد کنند:

```
# mount -o remount,nosuid /tmp
```

نحوه بررسی صحت پیکربندی امن:

با اجرای دستورات زیر می‌توان مطمئن شد که سیستم‌عامل به‌درستی پیکربندی شده است.

```
# grep "[[:space:]]/tmp[[:space:]]" /etc/fstab | grep nosuid
# mount | grep "[[:space:]]/tmp[[:space:]]" | grep nosuid
```

اگر هیچ یک از دو دستور فوق خروجی نداشته باشند، سیستم به‌صورت امن پیکربندی نشده است.

نحوه اجرای پیکربندی امن:

بایستی فایل /etc/fstab ویرایش شده و nosuid به فیلد چهارم (گزینه‌های mounting) اضافه شود. برای اطلاعات بیشتر صفحه راهنمایی fstab (5) مشاهده گردد.

2-1-4. تنظیم گزینه noexec برای پارتیشن /tmp

انتخاب گزینه noexec مشخص می‌کند که آن فایل‌سیستم نمی‌تواند حاوی کدهای دودویی قابل اجرا باشد. از آن‌جایی‌که فایل سیستم /tmp فقط برای ذخیره فایل‌های temp در نظر گرفته شده است، تنظیم این گزینه این اطمینان را به‌وجود می‌آورد که کاربران نمی‌توانند کدهای باینری قابل اجرا را در /tmp اجرا کنند.

نحوه بررسی صحت پیکربندی امن:

با اجرای دستورات زیر می‌توان مطمئن شد که سیستم عامل به‌درستی پیکربندی شده است:

```
# grep "[[:space:]]/tmp[[:space:]]" /etc/fstab | grep noexec
# mount | grep "[[:space:]]/tmp[[:space:]]" | grep noexec
```

اگر هیچ یک از دو دستور فوق خروجی نداشته باشند، سیستم به‌صورت امن پیکربندی نشده است.

نحوه اجرای پیکربندی امن:

بایستی فایل /etc/fstab ویرایش شده و noexec به فیلد چهارم (گزینه‌های mounting) اضافه شود.

```
# mount -o remount,noexec /tmp
```

2-1-5. ایجاد پارتیشن مجزا برای /var

شاخه /var توسط دایمون‌ها و دیگر سرویس‌های سیستمی برای ذخیره داده‌های داینامیک استفاده می‌شوند. بعضی از شاخه‌های ساخته شده به وسیله این فرآیندها ممکن است دارای مجوز همگانی نوشتن باشند. از آن‌جایی‌که شاخه /var ممکن است شامل فایل‌هایی با مجوز همگانی نوشتن باشد، اگر به پارتیشن مجزا تقسیم‌بندی نشده باشد، خطر فرسودگی منابع وجود دارد.

نحوه بررسی صحت پیکربندی امن:

با اجرای دستور زیر می‌توان مطمئن شد که سیستم عامل به‌درستی پیکربندی شده است:

```
# grep "[[:space:]]/var[[:space:]]" /etc/fstab
<volume> /var <fstype> <options>
```

نحوه اجرای پیکربندی امن:

هنگام نصب سیستم عامل جدید، بایستی در طول نصب، یک پارتیشن مخصوص برای var/ ساخت. برای سیستم‌هایی که قبلاً نصب شده‌اند، بایستی از LVM[4] برای ساخت پارتیشن استفاده کرد.

6-1-2. اتصال شاخه var/tmp/ به tmp/

شاخه var/tmp/ به طور معمول یک شاخه مستقل در فایل سیستم var/ است. اتصال var/tmp/ به tmp/ یک لینک غیرقابل شکستن به tmp/ ایجاد می‌کند که حتی توسط کاربر root قابل حذف نیست. همچنین به var/tmp/ اجازه می‌دهد که همان گزینه‌های mount شاخه tmp/ را به ارث ببرد. ضمناً به همان شیوه‌ای از var/tmp/ محافظت می‌گردد که از tmp/ محافظت می‌شود. این کار از پر شدن var/ با فایل‌های موقت var/tmp/ که در واقع در temp/ قرار دارند جلوگیری می‌کند.

همه برنامه‌هایی که از var/tmp/ و tmp/ برای خواندن و نوشتن فایل‌های temp استفاده می‌کنند، همواره در tmp/ نوشته می‌شوند. این امر مانع از آن می‌گردد که فایل سیستم var/ خارج از فضا اجرا شود یا مانع اجرای عملیاتی می‌گردد که در فایل سیستم tmp/ بلوکه شده است.

نحوه بررسی صحت پیکربندی امن:

با اجرای دستورات زیر می‌توان مطمئن شد که سیستم‌عامل به‌درستی پیکربندی شده است:

[4] Logical Volume Manager

```
# grep -e "^/tmp[[:space:]]" /etc/fstab | grep /var/tmp
/tmp /var/tmp none none 0 0
# mount | grep -e "^/tmp[[:space:]]" | grep /var/tmp
/tmp on /var/tmp type none (rw,bind)
```

اگر هیچ یک از دستورات فوق خروجی نداشته باشند، سیستم به‌صورت امن پیکربندی نشده است.

نحوه اجرای پیکربندی امن:

```
# mount --bind /tmp /var/tmp
```

همچنین بایستی /etc/fstab را به‌گونه‌ای ویرایش نمود که شامل سطر زیر باشد:

```
/tmp /var/tmp none bind 0 0
```

2-1-7. ایجاد پارتیشن مجزا برای /var/log

شاخه /var/log به‌وسیله سرویس‌های سیستمی برای ذخیره logها استفاده می‌شود. دو دلیل مهم وجود دارد که بایستی مطمئن شد logهای سیستم در یک پارتیشن جدا ذخیره می‌گردند:

- محافظت در مقابل فرسودگی منابع (logها می‌توانند کاملاً صعودی رشد کنند).
- حفاظت از داده‌های حاصل از بررسی سیستم.

نحوه بررسی صحت پیکربندی امن:

با اجرای دستور زیر می‌توان مطمئن شد که سیستم عامل به‌درستی پیکربندی شده است:

```
# grep "[[:space:]]/var/log[[:space:]]" /etc/fstab
```

```
<volume> /var/log <fstype> <options>
```

نحوه اجرای پیکربندی امن:

هنگام نصب سیستم‌عامل جدید، بایستی در طول نصب، یک پارتیشن مخصوص برای /var/log ساخت. برای سیستم‌هایی که قبلاً نصب شده‌اند، بایستی از LVM برای ساخت پارتیشن استفاده کرد.

8-1-2. ایجاد پارتیشن مجزا برای /var/log/audit

دایمون auditing (auditd)، logها را در شاخه /var/log/audit ذخیره می‌کند. دو دلیل مهم وجود دارد که بایستی مطمئن شد که داده‌های جمع‌آوری شده به‌وسیله auditd در یک پارتیشن جدا ذخیره می‌گردند:

- محافظت در مقابل فرسودگی منابع (فایل‌های audit.log می‌توانند کاملاً صعودی رشد کنند).
- حفاظت از داده‌های جمع‌آوری شده.

دایمون auditing مقدار فضای خالی باقیمانده را محاسبه نموده و بر اساس آن کارها را انجام می‌دهد. اگر سایر پروسه‌ها مانند syslog در همان پارتیشن auditd فضا مصرف کنند، این‌کار مطلوب نمی‌باشد.

نحوه بررسی صحت پیکربندی امن:

با اجرای دستور زیر می‌توان مطمئن شد که سیستم عامل به‌درستی پیکربندی شده است:

```
# grep "[[:space:]]/var/log/audit[[:space:]]" /etc/fstab
<volume> /var/log/audit <fstype> <options>
```

نحوه اجرای پیکربندی امن:

هنگام نصب سیستم عامل جدید، بایستی در طول نصب، یک پارتیشن مخصوص برای /var/log/audit ساخت. برای سیستم‌هایی که قبلاً نصب شده‌اند، بایستی از LVM برای ساخت پارتیشن استفاده نمود.

2-1-9. ایجاد پارتیشن مجزا برای /home

شاخه /home فضایی از حافظه دیسک است که برای استفاده کاربران محلی در نظر گرفته می‌شود. اگر سیستم دارای کاربران محلی است، بایستی یک پارتیشن جداگانه برای /home ایجاد شود تا از فرسودگی منابع جلوگیری شده و نوع فایل‌هایی که می‌توانند در /home ذخیره شوند، محدود گردد.

نحوه بررسی صحت پیکربندی امن:

با اجرای دستور زیر می‌توان مطمئن شد که سیستم‌عامل به‌درستی پیکربندی شده است:

```
# grep "[[:space:]]/home[[:space:]]" /etc/fstab
<volume> /home <fstype> <options>
```

نحوه اجرای پیکربندی امن:

هنگام نصب سیستم‌عامل جدید، بایستی در طول نصب، یک پارتیشن مخصوص برای /home ساخت. برای سیستم‌هایی که قبلاً نصب شده‌اند، بایستی از Logical Volume Manager (LVM) برای ساخت پارتیشن استفاده کرد.

2-1-10. اضافه نمودن گزینه nodev به /home

فعال‌شدن این گزینه برای فایل‌سیستم مانع از تعریف تجهیزات خاص بلوکی و کاراکتری[5] شده و در صورت وجود، مانع از استفاده از آن‌ها به‌صورت تجهیزات خاص بلوکی و کاراکتری می‌گردد. از آن‌جایی که

[5] character and block special devices

پارتیشن‌های اختصاص یافته به کاربران برای پشتیبانی از چنین تجهیزاتی در نظر گرفته نشده است، با تنظیم نمودن این گزینه، این اطمینان حاصل می‌گردد که کاربران نمی‌توانند اقدام به ایجاد آن‌ها نمایند.

نحوه بررسی صحت پیکربندی امن:

با اجرای دستورات زیر می‌توان مطمئن شد که سیستم‌عامل به‌درستی پیکربندی شده است.

```
# grep "[[:space:]]/home[[:space:]]" /etc/fstab
Verify that nodev is an option
# mount | grep /home
<each user partition> on <mount point> type <fstype> (nodev)
```

نکته: ممکن است گزینه‌های لیست شده دیگری برای این فایل‌سیستم وجود داشته باشد.

نحوه اجرای پیکربندی امن:

بایستی فایل /etc/fstab ویرایش شده و nodev به فیلد چهارم (گزینه‌های mounting) اضافه شود. برای اطلاعات بیشتر، صفحه راهنمایی fstab(5) مشاهده گردد.

```
# mount -o remount,nodev /home
```

نکته: مورد ذکر شده در خصوص پارتیشن /home است. در صورت وجود پارتیشن برای سایر کاربران، توصیه می‌گردد که عمل فوق برای تمامی آن‌ها صورت گیرد.

2-1-11. اضافه نمودن گزینه nodev به پارتیشن‌های تجهیزات رسانه‌ای قابل حمل[6]

فعال شدن این گزینه برای تجهیزات قابل حمل مانع از آن می‌گردد که تجهیزات خاص بلوکی و کاراکتری موجود روی این تجهیزات به عنوان فایل‌های دستگاه تلقی شوند.

[6] Removable Media

تجهیزات قابل حمل حاوی تجهیزات خاص بلوکی و کاراکتری می‌توانند برای دور زدن کنترل‌های امنیتی به وسیله کاربران غیر ریشه برای دسترسی به فایل‌های دستگاه‌های حساس (مانند /dev/kmem یا دیسک پارتیشن‌های خام) استفاده شوند.

نحوه بررسی صحت پیکربندی امن:

با اجرای دستور زیر می‌توان مطمئن شد که سیستم عامل به‌درستی پیکربندی شده است:

```
# grep <each removable media mountpoint> /etc/fstab
Verify that nodev is an option
```

نحوه اجرای پیکربندی امن:

بایستی فایل /etc/fstab ویرایش شده و nodev به فیلد چهارم (گزینه‌های mounting) اضافه شود (بایستی به دنبال نوشته‌هایی بود که mount point داشته و حاوی کلماتی مانند cdrom یا floppy باشند). برای اطلاعات بیشتر صفحه راهنمایی fstab (5) مشاهده گردد.

12-1-2. اضافه نمودن گزینه noexec به پارتیشن‌های مربوط به تجهیزات قابل حمل

بایستی برای جلوگیری از اجرای برنامه‌ها توسط تجهیزات قابل حمل، گزینه noexec برای آن‌ها فعال گردد. تنظیم این گزینه در فایل‌سیستم از اجرای برنامه‌های موجود روی این‌گونه تجهیزات توسط کاربران جلوگیری می‌کند. این کار مانع از اجرای برنامه‌های مخرب بالقوه بر روی سیستم می‌شود.

نحوه بررسی صحت پیکربندی امن:

با اجرای دستور زیر می‌توان مطمئن شد که سیستم‌عامل به‌درستی پیکربندی شده است.

```
# grep <each removable media mountpoint> /etc/fstab
```

نکته: بایستی بازبینی صورت گیرد به‌طوریکه noexec یکی از گزینه‌ها باشد.

نحوه اجرای پیکربندی امن:

بایستی فایل /etc/fstab ویرایش شده و noexec به فیلد چهارم (گزینه‌های mounting) اضافه شود. (بایستی به دنبال نوشته‌هایی بود که mount point داشته و حاوی کلماتی مانند cdrom یا floppy باشند). برای کسب اطلاعات بیشتر صفحه راهنمایی fstab (5) مشاهده گردد.

13-1-2. اضافه نمودن گزینه nosuid به پارتیشن‌های مربوط به تجهیزات قابل حمل

بایستی گزینه nosuid برای تجهیزات قابل حمل فعال گردد تا مانع از اجرا شدن فایل‌های اجرایی setuid و setgid ای شود که احیاناً روی این تجهیزات قرار دارند. تنظیم این گزینه بر روی یک فایل‌سیستم مانع از این می‌گردد که برنامه‌های دارای سطح مجوز دسترسی بالا، توسط کاربران غیر ریشه اجرا شوند.

نحوه بررسی صحت پیکربندی امن:

با اجرای دستور زیر می‌توان مطمئن شد که سیستم عامل به‌درستی پیکربندی شده است.

```
# grep <each removable media mountpoint> /etc/fstab
 Verify that nosuid is an option
```

نحوه اجرای پیکربندی امن:

بایستی فایل /etc/fstab ویرایش شده و nosuid به فیلد چهارم (گزینه‌های mounting) اضافه شود. (بایستی به دنبال نوشته‌هایی بود که mount point داشته و حاوی کلماتی مانند cdrom یا floppy باشند).

14-1-2. اضافه نمودن گزینه nodev به پارتیشن /dev/shm

فعال بودن گزینه nodev مشخص می‌کند که /dev/shm (فایل سیستم موقتی که در حافظه ذخیره شده است) نمی‌تواند حاوی تجهیزات خاص بلوکی و کاراکتری باشد. از آن‌جایی‌که فایل‌سیستم /dev/shm برای پشتیبانی deviceها در نظر گرفته نشده است، فعال نمودن این گزینه اطمینان حاصل می‌نماید که کاربران نمی‌توانند اقدام به ایجاد special deviceها در پارتیشن‌های /dev/shm کنند.

نحوه بررسی صحت پیکربندی امن:

با اجرای دستور زیر می‌توان مطمئن شد که سیستم‌عامل به‌درستی پیکربندی شده است.

```
# grep /dev/shm /etc/fstab | grep nodev
# mount | grep /dev/shm | grep nodev
```

اگر هیچ یک از دستورات فوق خروجی نداشته باشند، سیستم به‌صورت امن پیکربندی نشده است.

نحوه اجرای پیکربندی امن:

بایستی فایل /etc/fstab ویرایش شده و nodev به فیلد چهارم (گزینه‌های mounting) اضافه شود بایستی به دنبال نوشته‌هایی بود که mount point داشته و حاوی /dev/shm باشند. برای اطلاعات بیشتر صفحه راهنمایی fstab (5) مشاهده گردد.

```
# mount -o remount,nodev /dev/shm
```

15-1-2. اضافه نمودن گزینه nosuid به پارتیشن /dev/shm

فعال‌بودن گزینه nosuid برای /dev/shm (فایل‌سیستم موقتی که در حافظه ذخیره شده است) مشخص می‌کند که فایل‌های اجرایی تحت عنوان setuid و setgid اجرا نشوند و آن‌ها را با uid و gid کاربری اجرا می‌نماید که برنامه را اجرا کرده است. تنظیم این گزینه بر روی یک فایل‌سیستم مانع از آن می‌گردد که برنامه‌های دارای سطح مجوز دسترسی بالا توسط کاربران غیر ریشه اجرا شوند.

نحوه بررسی صحت پیکربندی امن:

با اجرای دستورهای زیر می‌توان مطمئن شد که سیستم‌عامل به‌درستی پیکربندی شده است.

```
# grep /dev/shm /etc/fstab | grep nosuid
# mount | grep /dev/shm | grep nosuid
```

اگر هیچ یک از دستورات فوق خروجی نداشته باشند، سیستم به‌صورت امن پیکربندی نشده است.

نحوه اجرای پیکربندی امن:

بایستی فایل /etc/fstab ویرایش شده و nosuid به فیلد چهارم (گزینه‌های mounting) اضافه شود. بایستی به دنبال نوشته‌هایی بود که mount point داشته و حاوی /dev/shm باشند. برای اطلاعات بیشتر صفحه راهنمایی fstab (5) مشاهده گردد.

```
# mount -o remount,nosuid /dev/shm
```

16-1-2. افزودن گزینه noexec به پارتیشن /dev/shm

فعال کردن noexec در پارتیشن حافظه اشتراکی از اجرای برنامه‌ها در آن جلوگیری می‌کند. تنظیم این گزینه در سیستم‌فایل از اجرای برنامه‌ها توسط کاربران از حافظه اشتراکی جلوگیری می‌کند. این‌کار مانع از توانایی کاربران برای معرفی برنامه‌های مخرب بالقوه بر روی سیستم می‌شود.

نحوه بررسی صحت پیکربندی امن:

با اجرای دستورهای زیر می‌توان مطمئن شد که سیستم‌عامل به‌درستی پیکربندی شده است.

```
# grep /dev/shm /etc/fstab | grep noexec
# mount | grep /dev/shm | grep noexec
```

اگر هر دو دستور خروجی تولید نمی‌کنند، بنابراین می‌توان گفت، سیستم درست پیکربندی نشده است.

نحوه اجرای پیکربندی امن:

بایستی فایل /etc/fstab ویرایش شده و noexec به فیلد چهارم (گزینه‌های mounting) اضافه شود. بایستی به دنبال نوشته‌هایی بود که mount point داشته و حاوی /dev/shm باشند.

```
# mount -o remount,noexec /dev/shm
```

17-1-2. تنظیم Sticky Bit برروی شاخه‌های با مجوز همگانی نوشتن

تنظیم sticky bit باعث می‌شود که در شاخه‌های با مجوز همگانی نوشتن، از حذف یا تغییر نام فایل‌ها توسط کاربران در شاخه‌ای که صاحب آن نیستند جلوگیری شود.

این ویژگی از حذف یا تغییر نام فایل‌ها در شاخه‌های با مجوز همگانی نوشتن که کاربر دیگری مالک آن است جلوگیری می‌کند.

نحوه بررسی صحت پیکربندی امن:

```
# df --local -P | awk {'if (NR!=1) print $6'} | xargs -I '{}' find '{}' -xdev -type d \( -perm -0002 -a ! -perm -1000 \) 2>/dev/null
```

نحوه اجرای پیکربندی امن:

```
\( -perm -0002 -a ! -perm  # df --local -P | awk {'if (NR!=1) print $6'} | xargs -I '{}' find '{}' -xdev -type d -1000 \) 2>/dev/null | xargs chmod a+t
```

18-1-2. غیرفعال نمودن نصب فایل سیستم‌های cramfs

فایل‌سیستم cramfs نوعی از فایل‌سیستم فشرده و فقط خواندنی لینوکس می‌باشد که در سیستم‌های footprint جاسازی شده است. یک cramfs image را می‌توان بدون آن‌که ابتدا آن را از حالت فشرده خارج ساخت، استفاده کرد.

حذف فایل‌سیستم‌هایی که نیاز به آن‌ها احساس نمی‌گردد، احتمال وقوع حمله‌های محلی را کاهش می‌دهد. بنابراین در صورتی‌که نیازی به این فایل‌سیستم نمی‌باشد، می‌بایست آن را غیرفعال نمود.

نحوه بررسی صحت پیکربندی امن:

```
# /sbin/modprobe -n -v cramfs
 install /bin/true
 # /sbin/lsmod | grep cramfs
 <No output>
```

نحوه اجرای پیکربندی امن:

می‌بایست فایل /etc/modprobe.d/CIS.conf را ویرایش یا ایجاد و سپس سطر زیر را به آن اضافه نمود:

```
install cramfs /bin/true
```

19-1-2. غیرفعال نمودن نصب فایل‌سیستم‌های freevxfs

فایل‌سیستم freevxsf نسخه رایگان سیستم‌فایل Veritas است که یک فایل‌سیستم اصلی برای سیستم‌عامل HP-UX به شمار می‌رود.

حذف نمودن فایل‌سیستم‌هایی که نیازی به آن‌ها نمی‌باشد، احتمال وقوع حمله‌های محلی را پایین می‌آورد. بنابراین در صورت عدم نیاز به این فایل‌سیستم می‌بایست آن‌را غیر فعال نمود.

نحوه بررسی صحت پیکربندی امن:

```
# /sbin/modprobe -n -v freevxfs
 install /bin/true
# /sbin/lsmod | grep freexvfs
 <No output>
```

نحوه اجرای پیکربندی امن:

می‌بایست فایل /etc/modprobe.d/CIS.conf را ویرایش یا ایجاد و سپس سطر زیر را به آن اضافه نمود:

```
install freevxfs /bin/true
```

2-1-20. غیرفعال نمودن نصب فایل‌سیستم‌های jffs2

فایل سیستم jffs2[7] نوعی فایل‌سیستم log-structured است که در فلش مموری‌ها مورد استفاده قرار می‌گیرد.

حذف نمودن فایل‌سیستم‌هایی که نیازی به آن‌ها نمی‌باشد، احتمال وقوع حمله‌های محلی را پایین می‌آورد. بنابراین در صورت عدم نیاز به این فایل‌سیستم می‌بایست آن‌را غیرفعال نمود.

نحوه بررسی صحت پیکربندی امن:

```
# /sbin/modprobe -n -v jffs2
 install /bin/true
 # /sbin/lsmod | grep jffs2
 <No output>
```

نحوه اجرای پیکربندی امن:

می‌بایست فایل /etc/modprobe.d/CIS.conf را ویرایش یا ایجاد و سپس سطر زیر را به آن اضافه نمود:

```
install jffs2 /bin/true
```

2-1-21. غیرفعال نمودن نصب فایل‌سیستم‌های hfs

فایل‌سیستم hfs نوعی فایل‌سیستم سلسله مراتبی است که اجازه نصب فایل‌سیستم‌های مربوط به سیستم عامل مکینتاش[8] را می‌دهد.

حذف نمودن فایل سیستم‌هایی که نیازی به آن‌ها نمی‌باشد، احتمال وقوع حمله‌های محلی را پایین می‌آورد. بنابراین در صورت عدم نیاز به این فایل سیستم می‌بایست آن را غیرفعال نمود.

[7] journaling flash filesystem 2
[8] MAC OS

نحوه بررسی صحت پیکربندی امن:

```
# /sbin/modprobe -n -v hfs
 install /bin/true
# /sbin/lsmod | grep hfs
 <No output>
```

نحوه اجرای پیکربندی امن:

می‌بایست فایل /etc/modprobe.d/CIS.conf را ویرایش یا ایجاد و سپس سطر زیر را به آن اضافه نمود:

```
install hfs /bin/true
```

2-1-22. غیرفعال نمودن نصب فایل‌سیستم‌های hfsplus

فایل‌سیستم hfsplus نوعی فایل‌سیستم سلسله مراتبی است که جایگزین hsf طراحی شده است و اجازه mount نمودن سیستم‌فایل‌های سیستم‌عامل مکینتاش را می‌دهد.

حذف نمودن فایل‌سیستم‌هایی که نیازی به آن‌ها نمی‌باشد، احتمال وقوع حمله‌های محلی را پایین می‌آورد. بنابراین در صورت عدم نیاز به این فایل سیستم می‌بایست آن را غیرفعال نمود.

نحوه بررسی صحت پیکربندی امن:

```
# /sbin/modprobe -n -v hfsplus
 install /bin/true
 # /sbin/lsmod | grep hfsplus
<No output>
```

نحوه اجرای پیکربندی امن:

می‌بایست فایل /etc/modprobe.d/CIS.conf را ویرایش یا ایجاد و سپس سطر زیر را به آن اضافه نمود:

```
install hfsplus /bin/true
```

2-1-23. غیرفعال نمودن نصب فایل‌سیستم‌های squashfs

فایل‌سیستم squashfs نوعی از فایل‌سیستم فشرده و فقط خواندنی لینوکس و جاسازی شده در سیستم‌های footprint کوچک است (شبیه cramfs). یک squashfs image می‌تواند بدون آن‌که ابتدا از حالت فشرده خارج گردد، مورد استفاده قرار گیرد.

حذف نمودن فایل‌سیستم‌هایی که نیازی به آن‌ها نمی‌باشد، احتمال وقوع حمله‌های محلی را پایین می‌آورد. بنابراین در صورت عدم نیاز به این فایل سیستم می‌بایست آن را غیرفعال نمود.

نحوه بررسی صحت پیکربندی امن:

```
# /sbin/modprobe -n -v squashfs
 install /bin/true
# /sbin/lsmod | grep squashfs
 <No output>
```

نحوه اجرای پیکربندی امن:

می‌بایست فایل /etc/modprobe.d/CIS.conf ویرایش یا ایجاد و سپس سطر زیر را به آن اضافه نمود:

```
install squashfs /bin/true
```

2-1-24. غیرفعال نمودن نصب فایل‌سیستم‌های udf

فایل‌سیستم udf[9] نوعی فرمت دیسک جهانی است که برای پیاده‌سازی مشخصات ISO/IEC 13346 و ECMA-167 استفاده می‌شود. udf یک نوع فایل‌سیستم open vendor برای ذخیره داده‌ها روی محدوده وسیعی از رسانه‌هاست. این فایل‌سیستم برای رایت DVDها و دیسک‌های نوری لازم است.

حذف نمودن فایل‌سیستم‌هایی که نیازی به آن‌ها نمی‌باشد، احتمال وقوع حمله‌های محلی را پایین می‌آورد. بنابراین در صورت عدم نیاز به این فایل سیستم می‌بایست آن‌را غیرفعال نمود.

نحوه بررسی صحت پیکربندی امن:

```
# /sbin/modprobe -n -v udf
install /bin/true
 # /sbin/lsmod | grep udf
<No output>
```

نحوه اجرای پیکربندی امن:

می‌بایست فایل /etc/modprobe.d/CIS.conf را ویرایش یا ایجاد و سپس سطر زیر را به آن اضافه نمود:

```
install udf /bin/true
```

[9] universal disk format

2-2. پیکربندی به‌روز رسانی نرم‌افزار

سیستم‌عامل CentOS از دستور yum برای نصب و به‌روزرسانی بسته‌های نرم‌افزاری استفاده می‌کند. روش‌های مدیریت وصله[10] ممکن است بین شرکت‌های مختلف متفاوت باشد. شرکت‌های بزرگ ممکن است یک سرور به‌روزرسانی محلی CentOS را در مکانی راه‌اندازی نمایند که سایر سرورهای CentOS آن‌ها قرار دارد. با این‌حال ممکن است که برخی عمل به‌روزرسانی سرورهای CentOS خود را مستقیماً از سرور اصلی CentOS انجام دهند. به‌روزرسانی‌ها می‌توانند به‌صورت اتوماتیک یا دستی با توجه به سیاست‌های سازمان برای مدیریت وصله انجام شود. بیشتر شرکت‌های بزرگ ترجیح می‌دهند وصله‌ها را ابتدا روی یک سیستم تست کرده بعد روی سیستم‌های اصلی اعمال کنند.

هدف اصلی این بخش از راهنمای امن‌سازی این است که از پیکربندی صحیح و نگهداری درست یک سیستم مدیریت وصله در سازمان اطمینان حاصل گردد. بنابراین جزئیات در مورد روش این به‌روزرسانی در این گزارش ارائه نگردیده است.

2-2-1. بررسی نصب بودن کلید CentOS GPG

سیستم‌عامل CentOS وصله‌ها را توسط روش‌های رمزنگاری و کلید GPG امضاء می‌نماید تا از صحت آن‌ها مطمئن گردد. اطمینان از صحت وصله‌ها مانع از نصب وصله‌های مجعول و درنتیجه نصب انواع بدافزار می‌گردد.

نحوه بررسی صحت پیکربندی امن:

با اجرای دستور زیر اطمینان حاصل می‌گردد که در سیستم کلید GPG به‌درستی نصب شده است :

```
# rpm -q --queryformat "%{SUMMARY}\n" gpg-pubkey
```

[10] Patch Management

نحوه اجرای پیکربندی امن:

کلید GPG را می‌توان با کلید GPG موجود در سایت CentOS به آدرس http://mirror.centos.org/centos/ مقایسه نمود. از دستور زیر می‌توان برای چاپ اثرانگشت[11] کلید نصب شده که در فایل زیر موجود است استفاده کرد.

```
# gpg --quiet --with-fingerprint /etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
```

2-2-2. بررسی به‌طور کامل فعال بودن gpgcheck

گزینه gpgcheck در بخش اصلی فایل /etc/yum.conf وجود دارد که مشخص می‌کند، امضای یک بسته RPM همیشه قبل از نصب چک گردد.

نکته بسیار مهم این است که اطمینان حاصل گردد، امضای یک بسته RPM همیشه قبل از نصب چک شود تا تضمین گردد که نرم‌افزار از منبع درستی به دست آمده است.

نحوه بررسی صحت پیکربندی امن:

برای بررسی اینکه gpgcheck در فایل /etc/yum.conf به مقدار 1 تنظیم شده است، می‌بایست دستور زیر اجرا گردد:

```
# grep gpgcheck /etc/yum.conf
gpgcheck=1
```

[11] fingerprint

نحوه اجرای پیکربندی امن:

می‌بایست فایل /etc/yum.conf ویرایش و gpgcheck به مقدار 1 تنظیم گردد:

```
gpgcheck=1
```

3-2-2. دریافت به‌روزرسانی‌های بسته نرم افزار با yum

ابزار به‌روزرسانی yum، به‌روزرسانی نرم‌افزارها را در کنار تحلیل وابستگی‌ها براساس مخزن متادیتا انجام می‌دهد و می‌تواند به صورت دستی از خط فرمان اجرا شده و یا به صورتی پیکربندی شود که اتوماتیک در فواصل زمانی مشخص اجرا گردد.

ابزار yum برای به‌روزرسانی ارجحیت دارد چون وابستگی‌ها را چک می‌کند و تضمین می‌نماید که نرم‌افزار درست نصب است. برای انجام به‌روزرسانی‌های yum به روند مدیریت‌وصله‌های محلی ارجاع شود.

نحوه بررسی صحت پیکربندی امن:

با اجرای دستور زیر می‌توان بسته‌هایی را که نیاز به به‌روزرسانی دارند مشخص نمود:

```
# yum check-update
```

نحوه اجرای پیکربندی امن:

```
# yum update
```

4-2-2. بررسی صحت بسته با استفاده از RPM

RPM قابلیت بررسی بسته‌های نصب‌شده را به‌وسیله مقایسه فایل‌های نصب شده با اطلاعات فایل ذخیره شده در بسته را دارد.

بررسی بسته‌ها این توانایی را به مدیر سیستم می‌دهد که فایل‌های بسته که تغییر داده شده است را تشخیص دهد (تشخیص آن‌که باینری تروجان روی یک باینری معتبر رونویسی شده باشد).

نحوه بررسی صحت پیکربندی امن:

دستور زیر برای بررسی درستی بسته‌های نصب شده می‌بایست اجرا گردد.

```
# rpm –qVa | awk ‘$2 != “c” { print $0}’
If any output shows up, you may have an integrity issue with that package
```

نکته: فعالیت‌های پیشنهادی در دیگر قسمت‌های این راهنما، مجوزهای دسترسی را در بعضی فایل‌ها برای امن‌تر کردن آن‌ها از حالت پیش‌فرض تغییر می‌دهد که باعث می‌شود بررسی فوق، پیغام عدم تطبیق دهد. خروجی‌های دستور بالا، مجوزهای دسترسی را بررسی نموده و آن دسته از مجوزها که عمداً یا سهواً تغییر نموده‌اند را مشخص می‌نماید.

نحوه اجرای پیکربندی امن:

تناقضات باید با دقت بررسی و در مورد آن‌ها تصمیم‌گیری شود.

2-3. محیط تشخیص نفوذ پیشرفته[12] (AIDE)

AIDE یک ابزار بررسی صحت فایل است (شبیه Tripwire). هرچند که این ابزار نمی‌تواند جلوی نفوذ را بگیرد، اما می‌تواند تغییرات غیرمجاز در فایل‌های پیکربندی را در زمانی‌که فایل‌ها تغییر داده می‌شوند تشخیص داده و سپس هشدار دهد. هنگامی‌که AIDE راه‌اندازی می‌گردد، بایستی سیاست‌های سازمانی درخصوص بررسی صحت فایل‌ها مشخص باشد.

2-3-1. نصب AIDE

در بعضی از نصب‌ها، AIDE به‌طور اتوماتیک نصب نمی‌شود. با نصب AIDE می‌توان بر صحت فایل‌های حساس سیستم و تغییراتاحتمالی آن‌ها نظارت داشت.

نحوه بررسی صحت پیکربندی امن:

با دستور زیر می‌توان از نصب AIDE اطمینان حاصل نمود.

```
Perform the following to determine if AIDE is installed.
# rpm -q aide
aide.<package version>.<hardware platform>
```

نحوه اجرای پیکربندی امن:

برای نصب AIDE از دستور yum استفاده می‌گردد. (گزینه y– برای بله گفتن به همه‌ی اعلان‌ها استفاده می‌شود):

```
yum install aide  #
<Output messages from Yum install>
aide.<hardware platform> <package version> installed
```

[12] Advanced Intrusion Detection Environment

مقداردهی اولیه AIDE :

```
# /usr/sbin/aide --init -B 'database_out=file:/var/lib/aide/aide.db.gz'
```

نکته: ویژگی prelinking می‌تواند با AIDE تداخل پیدا کند چون باینری‌ها را برای افزایش سرعت راه‌اندازی تغییر می‌دهد. در فایل /etc/sysconfig/prelink با تغییر دادن پارامتر PRELINKING=no و اجرای دستور /usr/sbin/prelink –ua ، باینری‌ها به حالت prelinked شان برگردانیده می‌شوند.

2-3-2. پیاده‌سازی اجرای مداوم و دوره‌ای صحت فایل

بایستی بررسی دوره‌ای چک‌کردن صحت فایل‌ها مطابق با سیاست‌های سازمان باشد. چک‌کردن دوره‌ای فایل‌ها به مدیر اجازه می‌دهد تا اگر فایل‌های حساس سیستم به‌صورت غیرمجاز تغییر کردند، این امر مشخص شود.

نحوه بررسی صحت پیکربندی امن:

اجرای دستور زیر مشخص می‌کند که آیا یک کار برنامه‌ریزی شده cron برای اجرای چک نمودن aide وجود دارد یا خیر.

```
# crontab -u root -l | grep aide
0 5 * * * /usr/sbin/aide --check
```

نحوه اجرای پیکربندی امن:

می‌بایست دستور زیر اجرا گردد.

```
# crontab -u root –e
```

می‌بایست سطر زیر به crontab اضافه گردد:

```
0 5 * * * /usr/sbin/aide --check
```

نکته: در این مثال، چک‌کردن هر روز ساعت 5 صبح اتفاق می‌افتد. در صورت لزوم باید زمان و نوع تکرار را مطابق با سیاست‌های سازمان تغییر داد.

4-2. پیکربندی SELinux

SElinux یک سیستم کنترل دسترسی اجباری[13] (MAC) را مهیا می‌کند که تا حد زیادی مدل پیش‌فرض کنترل دسترسی اختیاری[14] (DAC) را تکمیل می‌کند. در SElinux به هر فرآیند و هر شیئی (فایل‌ها، سوکت‌ها، پایپ‌ها) در سیستم یک محتوای امنیتی و یک برچسب تخصیص داده شده است که شامل جزئیات اطلاعات درباره شیئی است. هسته فقط در صورتی‌که دسترسی صریحاً بنا به سیاست‌ها اجازه داده شده باشد، به فرآیندها اجازه می‌دهد به اشیاء دسترسی داشته باشند. در واقع سیاست، چگونگی اجرا را تعریف می‌نماید. بنابراین یک کاربر می‌تواند یک نرم‌افزار را اجرا نماید اما نرم‌افزار می‌تواند در قالبی غیر از کاربر پیش‌فرض اجرا گردد. این امر به‌طور خودکار، آسیبی را که ممکن است برنامه به فایل‌هایی رساند که کاربر بدان دسترسی دارد، کاهش می‌دهد. کاربر نیازی نیست هیچ‌گونه اقدامی برای به دست آوردن این امتیاز انجام دهد. برای رخداد یک عمل، بایستی هم مجوز سنتی DAC و هم قوانین کنترل دسترسی اجباری SELinux برآورده شوند و عدم برآورده شدن هر یک باعث عدم مجوز رخداد عمل می‌شود. درنتیجه قوانین SELinux می‌توانند دسترسی‌های سیستم را محدودتر و امن‌تر نمایند. SELinux نیازمند سیاست‌های پیچیده‌ای است تا اجازه دهد همه کارهای درخواست شده از سیستم در حالت عادی انجام شود. سه نمونه سیاستی که برای CentOS 7 طراحی شده و همراه سیستم وجود دارد در زیر آورده شده است:

- **Targeted** : اکثراً از قوانین نوع اجرا[15] (TE) و همچنین تعداد کمتری از قوانین کنترل دسترسی مبتنی بر نقش[16](RBAC) تشکیل شده است. این سیاست، فعالیت‌های بسیاری از انواع برنامه‌ها را محدود می‌کند اما تعاملات کاربران را تا حد زیادی مجاز می‌شمارد.
- **Strict** : هم از قوانین TE و هم از RBAC استفاده می‌کند اما برنامه‌های بیشتری را پوشش داده و با شدت بیشتری از این قوانین استفاده می‌نماید.

[13] Mandatory Access Control (MAC)
[14] Discretionary Access Control (DAC)
[15] Type Enforcement
[16] Role-Based Access Control

- **Mls** : پیاده‌سازی امنیت چند سطحی[17] یا (MLS) که انواع بیشتری از برچسب‌ها (sensitivity و category) و قوانین حاکم برای دسترسی بر اساس آن‌ها معرفی می‌کند.

2-4-1. اطمینان از فعال بودن SELinux در /boot/grub2/grub.cfg

باید SELinux طوری پیکربندی گردد تا در زمان بوت فعال باشد و بررسی گردد که با پارامترهای grub boot رونویسی[18] نشده باشد. بدین منظور بایستی SELinux در زمان بوت در /boot/grub2/grub.cfg فعال باشد تا اطمینان حاصل گردد که کنترل‌هایی که فراهم می‌کند رونویسی نشده باشد.

نحوه بررسی صحت پیکربندی امن:

برای بررسی اینکه SELinux در زمان بوت فعال است یا نه، می‌بایست دستور زیر اجرا گردد :

```
# grep selinux=0 /boot/grub2/grub.cfg
[no output produced]
# grep enforcing=0 /boot/grub2/grub.cfg
 [no output produced]
```

نحوه اجرای پیکربندی امن:

در فایل /boot/grub2/grub.cfg می‌بایست تمام مواردی که selinux=0 و enforcing=0 هستند، حذف گردند.

2-4-2. تنظیم حالت SELinux

SELinux باید به‌گونه‌ای تنظیم گردد که هنگام بوت سیستم فعال باشد. بایستی SELinux در زمان بوت فعال باشد تا اطمینان حاصل گردد که کنترل‌هایی که فراهم می‌کند در همه زمان‌ها تأثیر می‌گذارند.

[17] implements Multi-Level Security
[18] overwritten

نحوه بررسی صحت پیکربندی امن:

دستور زیر مشخص می‌کند آیا SELinux در زمان بوت فعال است یا خیر.

```
# grep SELINUX=enforcing /etc/selinux/config
SELINUX=enforcing

# /usr/sbin/sestatus

SELinux status: enabled
Current mode: enforcing
Mode from config file: enforcing
Policy from config file: targeted
```

نحوه اجرای پیکربندی امن:

می‌بایست فایل /etc/selinux/config را ویرایش نمود تا پارامترهای SELinux تنظیم گردد:

```
SELINUX=enforcing
```

2-4-3. پیکربندی سیاست SELinux

می‌بایست SELinux به‌گونه‌ای پیکربندی گردد که سیاست سازمانی و حتی فراتر از آن تامین گردد. تنظیمات مورد نیاز امنیتی از یک سازمان به سازمان دیگر متفاوت است. بعضی سازمان‌ها ممکن است یک سیاست سختگیرانه‌تر نسبت به سیاست پیش‌فرض را اجباری کنند که کاملاً قابل قبول است. این بخش به منظور تضمین پیاده‌سازی حداقل توصیه‌های پیش‌فرض تهیه شده است.

نحوه بررسی صحت پیکربندی امن:

دستور زیر مشخص می‌کند که آیا سیاست مورد نظر در فایل /etc/selinux/config انتخاب شده است یا خیر.

```
# grep SELINUXTYPE=targeted /etc/selinux/config
SELINUXTYPE=targeted

# /usr/sbin/sestatus

SELinux status: enabled
Current mode: enforcing
Mode from config file: enforcing
Policy from config file: targeted
```

نکته: اگر سازمان به سیاست‌های سخت‌گیرانه‌تری نیاز دارد، بایستی مطمئن شد که با استفاده از دستور "grep" در فایل /etc/selinux/config انتخاب شده‌اند.

نحوه اجرای پیکربندی امن:

می‌بایست فایل /etc/selinux/config برای تنظیم پارامتر SELINUXTYPE ویرایش گردد.

```
SELINUXTYPE=targeted
```

نکته: اگر سازمان به سیاست‌های سختگیرانه‌تری نیاز دارد، بایستی اطمینان حاصل گردد که آن‌ها به فایل /etc/selinux/config اضافه شده باشند.

4-4-2. حذف SETroubleshoot

سرویس SETroubleshoot به کابران رومیزی از طریق یک رابط کاربرپسند خطاهای SELinux را اطلاع می‌دهد. این سرویس اطلاعات مهمی درباره خطاهای پیکربندی، نفوذ غیرمجاز و خطاهای احتمالی فراهم می‌کند.

از این‌رو سرویس SETroubleshoot یک دایمون غیرضروری است که روی سرور اجرا می‌شود، مخصوصاً اگر X Windows غیرفعال باشد.

نحوه بررسی صحت پیکربندی امن:

```
# rpm -q setroubleshoot
setroubleshoot.<package version>.<hardware platform>
```

نحوه اجرای پیکربندی امن:

```
# yum erase setroubleshoot
```

2-4-5. حذف سرویس ترجمه MCS (mcstrans)

دایمون mcstransd اطلاعات برچسب طبقه‌بندی شده را برای اطلاعات درخواستی فرآیندهای مشتری فراهم می‌کند. ترجمه برچسب در /etc/selinux/targeted/setrans.conf تعریف می‌شود.

به دلیل اینکه این سرویس بیشتر اوقات استفاده نمی‌شود، می‌بایست برای کاهش احتمال سوءاستفاده از آسیب‌پذیری در سیستم در حال اجرا، سرویس را غیرفعال نمود.

نحوه بررسی صحت پیکربندی امن:

برای تشخیص غیرفعال بودن mctrans می‌بایست دستور زیر اجرا گردد.

```
# rpm -q mcstrans
mcstrans.<package version>.<hardware platform>
```

نحوه اجرای پیکربندی امن:

```
# yum erase mcstrans
```

6-4-2. بررسی دایمون‌های پیکربندی نشده

دایمون‌هایی که در سیاست‌های SELinux تعریف نشده‌اند، امنیت فرآیند والدش را به ارث خواهند برد. به‌دلیل اینکه دایمون‌ها از فرآیند init راه‌اندازی می‌شوند، امنیت برچسب initrc_t را به ارث می‌برند. این امر می‌تواند باعث اعطای مجوزی فراتر از آن‌چه شود که فرایند بدان نیاز دارد.

نحوه بررسی صحت پیکربندی امن:

دستور زیر، دایمون‌هایی که در سیستم در حال اجرا هستند و پیکربندی نشده‌اند را مشخص می‌کند:

```
# ps -eZ | egrep "initrc" | egrep -vw "tr|ps|egrep|bash|awk" | tr ':' ' ' | awk '{ print $NF }'
[no output produced]
```

نحوه اجرای پیکربندی امن:

طبق خروجی دستور بالا، می‌بایست تک‌تک دایمون‌های پیکربندی نشده بررسی گردند.

2-5. تنظیمات بوت شدن امن

2-5-1. تنظیم کاربر/گروه مالک بر روی /boot/grub2/grub.cfg

می‌بایست مالک و گروه فایل /boot/grub2/grub.cfg کاربر ریشه[19] تعریف گردد. تنظیم گروه و مالک به کاربر ریشه، از تغییر دادن این فایل توسط کاربران غیر ریشه جلوگیری می‌کند.

نحوه بررسی صحت پیکربندی امن:

انجام دستور زیر تعیین می‌کند که فایل /boot/grun2/grub.cfg دارای مالکیت درستی می‌باشد:

```
# stat -L -c "%u %g" /boot/grub2/grub.cfg | egrep "0 0"
```

اگر دستور بالا خروجی به همراه نداشت، پیکربندی به درستی اعمال نشده است.

نحوه اجرای پیکربندی امن:

```
# chown root:root /boot/grub2/grub.cfg
```

2-5-2. تنظیم مجوزهای دسترسی در /boot/grub2/grub.cfg

بایستی دسترسی فایل /boot/grub2/grub.cfg به‌گونه‌ای تنظیم گردد که فقط کاربر ریشه بتواند در آن بنویسد و یا آن‌را بخواند.

[19] Root

اجازه دسترسی خواندن و نوشتن فقط برای کاربر ریشه از دیدن پارامترهای بوت و تغییر آن توسط کاربران غیرریشه جلوگیری می‌کند. دلیل اتخاذ این توصیه آن است که کاربران غیر ریشه با خواندن این پارامترها ممکن است به ضعف امنیتی سیستم پی ببرند.

نحوه بررسی صحت پیکربندی امن:

انجام دستور زیر تعیین می‌کند که /boot/grub2/grub.cfg اجازه دسترسی درستی داشته باشد:

```
# stat -L -c "%a" /boot/grub2/grub.cfg | egrep ".00"
```

اگر دستور بالا خروجی به همراه نداشت، تنظیمات به درستی اعمال نشده است.

نحوه اجرای پیکربندی امن:

```
# chmod og-rwx /boot/grub2/grub.cfg
```

2-5-3. تنظیم رمز عبور برای Boot Loader

تنظیم رمز عبور برای Boot Loader باعث خواهد شد که هر کسی اقدام به راه‌اندازی مجدد سیستم نماید، درصورتی‌که قصد تنظیم پارامترهای خط فرمان را داشته باشد، مجبور به ورود یک رمز عبور شود. خواستن رمز عبور برای اجرای boot loader از وارد کردن یا تغییر پارامترها یا تغییر دادن بوت پارتیشن توسط کاربران غیرمجاز جلوگیری می‌کند. این کار از تضعیف امنیت توسط کاربران جلوگیری می‌کند (به‌طور مثال غیرفعال نمودن SELinux در زمان راه‌اندازی).

نحوه بررسی صحت پیکربندی امن:

دستور زیر اگر برای تنظیمات خط فرمان بوت رمز عبور خواسته شود را مشخص می‌کند:

```
# grep "^set superusers" /boot/grub2/grub.cfg
set superusers="<user-list>"
# grep "^password" /boot/grub2/grub.cfg
password_pbkdf2 <user> <encrypted password>
```

حداقل یک کاربر مشخص باید به عنوان کاربر برتر[20] باشد و یک رمز عبور به او تخصیص داده شده باشد.

نحوه اجرای پیکربندی امن:

ایجاد رمز عبور رمزگذاری شده توسط grub-md5-crypt که در زیر آمده است:

```
# grub2-mkpasswd-pbkdf2
Enter password: <password>
Reenter password: <password>
Your PBKDF2 is <encrypted-password>
```

می‌بایست متن زیر را به /etc/grub.d/00-header اضافه نمود و یا فایل /etc/grub.d را به‌طور سفارشی پیکربندی نمود:

```
cat <<EOF
set superusers="<user-list>"
password_pbkdf2 <user> <encrypted-password>
EOF
```

درنهایت بایستی با اجرای دستور زیر پیکربندی grub به‌روز رسانی گردد.

```
# grub2-mkconfig -o /boot/grub2/grub.cfg
```

[20] super user

2-6. فرآیندهای اضافی امن‌سازی

2-6-1. محدود نمودن core dump (کپی از هسته)

core dump حافظه‌ی یک برنامه اجرایی است و معمولاً برای تعیین اینکه چرا یک برنامه به صورت غیرعادی بسته شده است مورد استفاده قرار می‌گیرد. همچنین برای جمع‌کردن اطلاعات محرمانه از فایل هسته نیز استفاده می‌گردد. سیستم توانایی soft limit نمودن core dump را دارد اما کاربر می‌تواند آن را بازنویسی کند.

تنظیم نمودن محدودیت به‌صورت hard limit بر core dump از بازنویسی شدن نرم‌افزاری آن جلوگیری می‌کند. در صورتی‌که core dump مورد نیاز است، می‌بایست برای گروه‌های کاربری مورد نظر آن را محدود نمود. همچنین تنظیم متغیر fs.suid_dumpable به 0 از dump شدن هسته توسط برنامه‌های setuid جلوگیری خواهد نمود.

نحوه بررسی صحت پیکربندی امن:

می‌بایست دستور زیر را برای تعیین اینکه آیا core dump محدود شده است یا خیر اجرا نمود.

```
# grep "hard core" /etc/security/limits.conf
* hard core 0
# /sbin/sysctl fs.suid_dumpable
 fs.suid_dumpable = 0
```

نحوه اجرای پیکربندی امن:

می‌بایست سطر زیر به فایل /etc/security/limits.conf اضافه گردد.

```
* hard core 0
```

سطر زیر نیز می‌بایست به فایل /etc/sysctl.conf اضافه گردد.

```
fs.suid_dumpable = 0
```

2-6-2. فعال نمودن محل قرارگیری مکان حافظه مجازی به‌صورت تصادفی

می‌بایست پرچم[21] سیستم طوری تنظیم گردد که محل قرارگیری مکان حافظه مجازی به اجبار تصادفی انتخاب شود. به‌طور تصادفی قرارگرفتن ناحیه حافظه مجازی، سوء استفاده از نوشتن روی صفحه حافظه را مشکل خواهد ساخت.

نحوه بررسی صحت پیکربندی امن:

دستور زیر تعیین می‌کند که آیا حافظه مجازی تصادفی انتخاب می‌شود یا خیر.

```
# /sbin/sysctl kernel.randomize_va_space
kernel.randomize_va_space = 2
```

نحوه اجرای پیکربندی امن:

می‌بایست سطر زیر به فایل /etc/sysctl.conf اضافه گردد:

```
kernel.randomize_va_space = 2
```

[21] Flag

7-2. استفاده از آخرین نسخه سیستم‌عامل منتشر شده

توزیع‌کنندگان سیستم‌عامل CentOS به صورت دوره‌ای به‌روزرسانی‌های خود را منتشر می‌کنند تا هم سخت‌افزارهای جدید را پشتیبانی کرده و هم قابلیت‌های جدیدی ارائه دهند. همچنین به عنوان یک بسته نرم‌افزاری، مجموعه‌ای از وصله‌هایی است که می‌توانند به عنوان یک اصلاحیه واحد اعمال گردند.

به‌روزرسانی‌های جدیدتر ممکن است شامل تمهیدات جدید امنیتی باشند که از طریق فرآیند وصله در دسترس نباشند. در نتیجه توصیه می‌گردد از آخرین به‌روزرسانی سیستم‌عامل CentOS استفاده گردد. از سوی دیگر سازمان‌ها بایستی مطمئن شوند که به‌روزرسانی با نرم‌افزارهای دیگر موجود در سیستم‌هایشان سازگار می‌باشد.

نحوه بررسی صحت پیکربندی امن:

می‌توان از دستور زیر برای تعیین نسخه سیستم‌عامل موجود استفاده نمود:

```
# uname –r
```

یا

```
# cat /etc/centos-release
```

نحوه اجرای پیکربندی امن:

می‌بایست آخرین نسخه CentOS را نصب نمود. با استفاده از آخرین به روزرسانی در هنگام نصب و ارتقاء و یا نصب مجدد آخرین به‌روزرسانی، می‌توان امنیت را در این مورد تأمین نمود.

3. سرویس‌های سیستم‌عامل

در حالی‌که استفاده از به‌روزرسانی سیستم و دریافت وصله برای محافظت از آسیب‌پذیری‌های شناخته شده کمک می‌نمایند، یکی از بهترین راه‌های محافظت در مقابل آسیب‌پذیری‌های گزارش نشده غیرفعال نمودن سرویس‌هایی است که مورد نیاز یک سیستم‌عامل معمولی نیست. این کار مانع بهره‌برداری از آسیب‌پذیری هایی می‌گردد که احتمالاً در آینده کشف خواهند شد، زیرا اگر سرویس غیرفعال باشد، در نتیجه نمی‌تواند مورد سوء استفاده قرار بگیرد. در این قسمت از گزارش برای سرویس‌هایی که می‌توانند تحت هر شرایطی به طور امن غیرفعال گردند و به این ترتیب تا حد زیادی تهدیدات ممکن را در سیستم مورد نظر کاهش می‌دهد، پیشنهادهایی ارائه شده است.

3-1. حذف سرویس‌های قدیمی

توصیه‌های ارائه شده در این بخش به‌گونه‌ای در نظر گرفته شده‌اند تا اطمینان حاصل گردد که در سیستم، سرویس‌های قدیمی نصب نشده است. تعدادی راهنما شامل دستورات غیرفعال یا حذف نمودن سرویس‌ها در ادامه این بخش ارائه شده است. به‌طور کلی دلیلی وجود ندارد که سرویس‌های قدیمی در سیستم وجود داشته باشند، حتی اگر وضعیت آن‌ها غیرفعال باشد.

نکته: توصیه‌های موجود در این بخش، تنها بسته‌های لیست شده در دیتابیس yum و همچنین نصب شده از طریق rpm را بررسی می‌نمایند. درنتیجه درصورتی‌که فردی آن‌ها را به طور جداگانه و با استفاده از روش‌های غیر استاندارد نصب کرده باشد، آن بسته‌ها توسط توصیه‌های بیان شده پوشش داده نخواهند شد. رسیدگی به بسته‌هایی که با استفاده از روش‌های غیراستاندارد نصب و راه‌اندازی شده‌اند، موضوعی فراتر از محدوده این گزارش می‌باشند.

3-1-1. حذف telnet server

بسته telnet-server شامل دایمون telnetd است که ارتباط سایر کاربران از دیگر سیستم‌ها را با استفاده از پروتکل telnet قبول می‌کند.

این پروتکل، نا امن و رمزگذاری نشده است. در نتیجه امکان شنود ترافیک شبکه وجود دارد. بسته SSH یک نشست رمزگذاری شده و امن‌تری را فراهم می‌نماید و در اکثر توزیع‌های لینوکس نیز وجود دارد.

نحوه بررسی صحت پیکربندی امن:

با استفاده از دستور زیر می‌توان مطمئن شد که بسته telnet-server بر روی سیستم نصب نشده باشد.

```
# rpm -q telnet-server
package telnet-server is not installed
```

نحوه اجرای پیکربندی امن:

```
yum erase telnet-server
```

3-1-2. حذف کلاینت‌های telnet

بسته telnet محتوی telnet Client است که توسط آن به کاربران اجازه داده می‌شود که با استفاده از پروتکل telnet به سیستم‌های دیگر متصل گردند. پروتکل telnet نا امن و رمزگذاری نشده است و یک کاربر بدخواه می‌تواند با شنود خط، ترافیک شبکه را سرقت نماید. بسته SSH یک نشست رمزگذاری شده و امن‌تری را فراهم می نماید و در اکثر توزیع‌های لینوکس وجود دارد.

نحوه بررسی صحت پیکربندی امن:

با استفاده از دستور زیر می‌توان مطمئن شد که بسته telnet بر روی سیستم نصب می‌باشد یا خیر.

```
# rpm -q telnet
package telnet is not installed
```

نحوه اجرای پیکربندی امن:

```
# yum erase telnet
```

3-1-3. حذف rsh-server

بسته Berkeley rsh-server (rsh, rlogin, rcp) حاوی سرویس‌های قدیمی است که اعتبارنامه‌ها را در متنی آشکار و رمز نشده تبادل می‌کنند. این سرویس‌های قدیمی مشکلات امنیتی متعددی داشته و با پروتکل امن تر SSH جایگزین شده است.

نحوه بررسی صحت پیکربندی امن:

با استفاده از دستور زیر می‌توان مطمئن شد که سرویس rsh بر روی سیستم نصب می‌باشد یا خیر.

```
# rpm -q rsh-server
package rsh-server is not installed
```

نحوه اجرای پیکربندی امن:

```
# yum erase rsh-server
```

3-1-4. حذف rsh

بسته rsh شامل دستورهای کلاینت برای سرویس‌های rsh است. این سرویس مشکلات امنیتی متعددی دارد و با پروتکل امن‌تر SSH جایگزین شده است.

توصیه می‌گردد که حتی اگر سرویس‌دهنده حذف شده است، برای جلوگیری از اینکه کاربران سهواً از دستورات آن استفاده کنند و اعتبارنامه‌هایشان فاش شود، اطمینان حاصل گردد که کلاینت‌ها نیز حذف شده اند. توجه گردد که حذف بسته rsh، کلاینت‌هایی که برای rcp، rsh و rlogin مورد استفاده قرار می‌گیرد را حذف می‌کند.

نحوه بررسی صحت پیکربندی امن:

با استفاده از دستور زیر می‌توان مطمئن شد که rsh بر روی سیستم نصب می‌باشد یا خیر.

```
# rpm -q rsh
package rsh is not installed
```

نحوه اجرای پیکربندی امن:

```
# yum erase rsh
```

3-1-5. حذف NIS Client

سرویس اطلاعات شبکه[22] یا (NIS) که قبلاً به عنوان Yellow Pages شناخته می‌شد، یک پروتکل سرویس دایرکتوری کلاینت/سرور است که برای توزیع فایل‌های پیکربندی مورد استفاده قرار می‌گیرد. کلاینت NIS (ypbind) برای متصل نمودن[23] یک ماشین به سرویس‌دهنده NIS و دریافت فایل‌های پیکربندی توزیع شده مورد استفاده قرار می‌گیرد.

NIS ذاتاً یک سرویس نا امن است که در مقابل حملات DoS و Buffer Overflows آسیب‌پذیر بوده و احراز هویت ضعیفی[24] برای پرس‌وجوی[25] نقشه‌های NIS دارد. NIS عموماً با پروتکل LDAP[26] جایگزین می‌شود. توصیه می‌شود این سرویس حذف گردد.

نحوه بررسی صحت پیکربندی امن:

با استفاده از دستور زیر می‌توان مطمئن شد که ypbind بر روی سیستم نصب می‌باشد یا خیر.

```
# rpm -q ypbind
package ypbind is not installed
```

نحوه اجرای پیکربندی امن:

```
# yum erase ypbind
```

[22] Network Information Service
[23] bind
[24] Poor Authentication
[25] Querying
[26] Lightweight Directory Access Protocol

3-1-6. حذف NIS Server

سرویس اطلاعات شبکه[۲۷]یا NIS که قبلاً به عنوان Yellow Pages شناخته می‌شد، یک پروتکل سرویس دایرکتوری کلاینت/سرور است که برای توزیع فایل‌های پیکربندی سیستم مورد استفاده قرار می‌گیرد. سرویس‌دهنده NIS یک مجموعه از برنامه‌هایی می‌باشد که اجازه توزیع فایل‌های پیکربندی را می‌دهد.

NIS ذاتاً یک سرویس نا امن است که در مقابل حملات DoS و Buffer Overflows آسیب‌پذیر بوده و احراز هویت ضعیفی[۲۸] برای پرس‌وجوی[۲۹] نقشه‌های NIS دارد. NIS عموماً با پروتکل LDAP[30] جایگزین می‌شود. توصیه می‌شود این سرویس غیرفعال و از سرویس‌های امن‌تر موجود استفاده گردد.

نحوه بررسی صحت پیکربندی امن:

با استفاده از دستور زیر می‌توان مطمئن شد که ypserv بر روی سیستم نصب می‌باشد یا خیر.

```
# rpm -q ypserv
package ypserv is not installed
```

نحوه اجرای پیکربندی امن:

```
# yum erase ypserv
```

[27] Network Information Service
[28] Poor Authentication
[29] Querying
[30] Lightweight Directory Access Protocol

3-1-7. حذف tftp

TFTP[31] یک پروتکل ساده ارسال فایل می‌باشد که عموماً برای فرستادن تنظیمات یا فایل‌های بوت بین ماشین‌ها به طور خودکار مورد استفاده قرار می‌گیرد. TFTP از عملیات احراز هویت پشتیبانی نمی‌کند و می تواند به آسانی هک گردد. بسته tftp یک برنامه کلاینت است که اجازه اتصال به یک سرویس‌دهنده tftp را می‌دهد.

توصیه می‌گردد tftp حذف گردد، مگر اینکه نیاز خاصی برای استفاده از آن وجود داشته باشد (مثل یک سرویس دهنده بوت[32]). در صورت نیاز به سرویس، می‌بایست پیکربندی آن با احتیاط زیاد انجام گردد.

نحوه بررسی صحت پیکربندی امن:

با اجرای دستور زیر می‌توان مطمئن شد که tftp بر روی سیستم نصب می‌باشد یا خیر.

```
# rpm -q tftp
package tftp is not installed
```

نحوه اجرای پیکربندی امن:

```
# yum erase tftp
```

[31] Trivial File Transfer Protocol
[32] Boot Server

3-1-8. حذف tftp-server

TFTPیک پروتکل ساده ارسال فایل است که عموماً برای فرستادن تنظیمات یا فایل‌های بوت بین ماشین‌ها به طور خودکار استفاده می‌شود. بسته tftp-server برای راه‌اندازی یک TFTP سرور استفاده می‌شود.

TFTP از عملیات احراز هویت پشتیبانی نمی‌کند و همچنین نمی‌توان اطمینانی از محرمانه‌بودن و صحت داده‌ها داشت. توصیه می‌گردد tftp حذف گردد، مگر اینکه نیاز خاصی برای استفاده از آن وجود داشته باشد. در صورت نیاز به سرویس، می‌بایست پیکربندی آن با احتیاط زیاد انجام گردد.

نحوه بررسی صحت پیکربندی امن:

با اجرای دستور زیر می‌توان مطمئن شد که سرویس‌های tftp بر روی سیستم نصب می‌باشد یا خیر.

```
# rpm -q tftp-server
package tftp-server is not installed
```

نحوه اجرای پیکربندی امن:

```
# yum erase tftp-server
```

3-1-9. حذف talk

نرم‌افزار talk امکان ارسال و دریافت پیام از طریق ترمینال را مهیا می‌سازد. Talk client به طور پیش‌فرض نصب می‌باشد. این نرم‌افزار یک تهدید امنیتی به حساب می‌آید، چون از پروتکل‌های رمزگذاری برای ارتباطات خود استفاده نمی‌کند.

نحوه بررسی صحت پیکربندی امن:

می‌بایست با دستور زیر اطمینان حاصل گردد که talk بر روی سیستم نصب نشده باشند.

```
# rpm -q talk
 package talk is not installed
```

نحوه اجرای پیکربندی امن:

```
# yum erase talk
```

10-1-3. حذف talk-server

نرم افزار talk امکان ارسال و دریافت پیام از طریق ترمینال را مهیا می‌سازد. talk client به طور پیش‌فرض نصب می‌باشد. این نرم‌افزار یک تهدید امنیتی به حساب می‌آید چون از پروتکل‌های رمزگذاری برای ارتباط استفاده نمی‌کند.

نحوه بررسی صحت پیکربندی امن:

می‌بایست با دستور زیر اطمینان حاصل گردد که talk-server بر روی سیستم نصب نشده باشند.

```
# rpm -q talk-server
package talk-server is not installed
```

نحوه اجرای پیکربندی امن:

```
# yum erase talk-server
```

3-1-11. حذف xinetd

دایمون[33] eXtended InterNET (xinetd) یک دایمون برتر[34] متن باز است که جایگزین دایمون inetd شده است. دایمون Xinetd به سرویس‌های شناخته‌شده گوش می‌کند و دایمون مناسب را برای پاسخ‌دهی مناسب به درخواست آن سرویس‌ها اعزام می‌کند.

توصیه می‌گردد در صورت عدم نیاز به xinetd ، می‌بایست مطمئن شد که از سیستم حذف شده است.

نحوه بررسی صحت پیکربندی امن:

می‌بایست دستور زیر را اجرا نمود، تا مشخص گردد xinetd بر روی سیستم نصب می‌باشد یا خیر.

```
# rpm -q xinetd
package xinetd is not installed
```

نحوه اجرای پیکربندی امن:

```
# yum erase xinetd
```

[33] InterNET Daemon
[34] Super daemon

3-1-12. غیرفعال کردن chargen-dgram

chargen-dgram یک سرویس شبکه‌ای است که هر دیتاگرامی دریافت می‌کند را با کاراکترهای اسکی از 0 تا 512 پاسخ می‌دهد. این سرویس برای اشکال‌زدایی و تست اهداف در نظر گرفته شده است. توصیه می‌شود این سرویس غیرفعال گردد.

غیرفعال نمودن این سرویس، احتمال وقوع این حملات از راه دور را کاهش می‌دهد.

نحوه بررسی صحت پیکربندی امن:

```
# chkconfig --list chargen-dgram
chargen-dgram: off
```

نحوه اجرای پیکربندی امن:

می‌بایست سرویس chargen-dgram را با اجرای دستور زیر غیرفعال نمود:

```
# chkconfig chargen-dgram off
```

3-1-13. غیرفعال‌سازی chargen-stream

chargen-stream یک سرویس شبکه‌ای است که هر ارتباطی که دریافت می‌کند را با کاراکترهای اسکی از 0 تا 512 پاسخ می‌دهد. این سرویس برای اشکال‌زدایی و تست اهداف در نظر گرفته شده است. توصیه می‌شود این سرویس غیرفعال شود.

غیرفعال کردن این سرویس احتمال وقوع حملات از راه دور را کاهش می‌دهد.

نحوه بررسی صحت پیکربندی امن:

```
# chkconfig --list chargen-stream
chargen-stream: off
```

نحوه اجرای پیکربندی امن:

می‌بایست سرویس chargen-stream را با اجرای دستور زیر غیرفعال نمود:

```
# chkconfig chargen-stream off
```

3-1-14. غیر فعال نمودن daytime-dgram

سرویس daytime-dgram یک سرویس شبکه‌ای می‌باشد که تاریخ و ساعت سرورها را اعلام می‌نماید. این سرویس برای اشکال‌زدایی و تست اهداف در نظر گرفته شده است. توصیه می‌شود این سرویس غیرفعال گردد.

غیرفعال کردن این سرویس نیز احتمال وقوع حملات از راه دور را کاهش می‌دهد.

نحوه بررسی صحت پیکربندی امن:

```
# chkconfig --list daytime-dgram
daytime-dgram: off
```

نحوه اجرای پیکربندی امن:

می‌بایست سرویس daytime-dgram را با اجرای دستور زیر غیرفعال نمود :

```
# chkconfig daytime-dgram off
```

3-1-15. غیر فعال نمودن daytime-stream

سرویس daytime-stream یک سرویس شبکه‌ای می‌باشد که تاریخ و ساعت سرورها را اعلام می‌نماید. این سرویس برای اشکال‌زدایی و تست اهداف در نظر گرفته شده است. توصیه می‌شود این سرویس غیرفعال گردد.

غیرفعال کردن این سرویس احتمال وقوع حملات از راه دور را کاهش می‌دهد.

نحوه بررسی صحت پیکربندی امن:

```
# chkconfig --list daytime-stream
daytime-stream: off
```

نحوه اجرای پیکربندی امن:

می‌بایست سرویس daytime-stream را با اجرای دستور زیر غیرفعال نمود:

```
# chkconfig daytime-stream off
```

3-1-16. غیر فعال نمودن echo-dgram

echo-dgram یک سرویس شبکه‌ای است که به کلاینت‌ها با داده‌هایی که به وسیله آن‌ها فرستاده می‌شود، پاسخ می‌دهد. این سرویس برای اشکال‌زدایی و تست اهداف در نظر گرفته شده است. توصیه می‌شود این سرویس غیرفعال گردد.

غیرفعال کردن این سرویس احتمال وقوع حملات از راه دور را کاهش می‌دهد.

نحوه بررسی صحت پیکربندی امن:

```
chkconfig --list echo-dgram
echo-dgram: off
```

نحوه اجرای پیکربندی امن:

می‌بایست سرویس echo-dgram را با اجرای دستور زیر غیرفعال نمود:

```
# chkconfig echo-dgram off
```

3-1-17. غیر فعال نمودن echo-stream

echo-stream یک سرویس شبکه‌ای است که به کلاینت‌ها با داده‌هایی که به وسیله کلاینت‌ها به آن فرستاده می‌شود پاسخ می‌دهد. این سرویس برای اشکال زدایی و تست اهداف در نظر گرفته شده است. توصیه می‌شود این سرویس غیرفعال شود.

غیرفعال کردن این سرویس احتمال وقوع حملات از راه دور را کاهش می‌دهد.

نحوه بررسی صحت پیکربندی امن:

```
# chkconfig --list echo-stream
echo-stream: off
```

نحوه اجرای پیکربندی امن:

می‌بایست سرویس echo-stream را با اجرای دستور زیر غیرفعال نمود:

```
# chkconfig echo-stream off
```

3-1-18. غیرفعال نمودن tcpmux-server

tcpmux-server یک سرویس شبکه‌ای است که به یک کلاینت اجازه می‌دهد به سرویس‌های شبکه‌ای دیگر در حال اجرا بر روی سرور دسترسی داشته باشد. توصیه می‌شود این سرویس غیرفعال گردد.

tcpmux-server می‌تواند برای دور زدن فایروال سرور مورد سوء استفاده قرار گیرد. به‌علاوه، یک مهاجم می‌تواند توسط tcpmux-server اقدام به پویش پورت‌های سرور نماید.

نحوه بررسی صحت پیکربندی امن:

```
# chkconfig --list tcpmux-server
tcpmux-server: off
```

نحوه اجرای پیکربندی امن:

می‌بایست سرویس tcpmux-server را با اجرای دستور زیر غیرفعال نمود :

```
# chkconfig tcpmux-server off
```

4. سرویس‌های برای اهدف خاص

در این بخش سرویس‌هایی شرح داده شده است که بنا به نیاز سازمان، ممکن است نیاز به اجرای این سرویس‌ها وجود داشته باشد. اگر هرکدام از این سرویس‌ها مورد نیاز نمی‌باشد پیشنهاد می‌گردد آن‌را غیرفعال یا حذف نمود تا احتمال وقوع حملات بالقوه و احتمالی کاهش یابد.

4-1. تنظیم دایمون umask

می‌بایست Umask پیش‌فرض را برای تمام فرآیندهای شروع شده در زمان بوت تنظیم نمود. این تنظیمات در umask به‌طور انتخابی مجوز دسترسی پیش‌فرض را زمانی که یک فایل به‌وسیله یک فرآیند دایمون ساخته می‌شود خاموش می‌کند.

تنظیم umask به مقدار 027 اطمینان حاصل می‌نماید که فایل‌های ساخته شده به‌وسیله دایمون‌ها قابل خواندن، نوشتن و قابل اجرا به‌وسیله هر کاربری غیر از مالک و گروه آن فرآیند دایمون نیست و حتی قابل نوشتن توسط گروه آن فرآیند دایمون نیز نیست. در صورتی‌که این فایل‌ها نیاز به مجوز دسترسی اضافه داشته باشند، فرآیند دایمون می‌تواند به‌صورت دستی این تنظیمات را رونویسی کند.

نحوه بررسی صحت پیکربندی امن:

اجرای دستور زیر مشخص می‌کند دایمون umask تنظیم شده است.

```
# grep umask /etc/sysconfig/init
umask 027
```

نحوه اجرای پیکربندی امن:

می‌بایست سطر زیر را به فایل /etc/sysconfig/init اضافه نمود.

```
umask 027
```

2-4. حذف X Windows

سیستم X Window یک رابط گرافیکی (GUI) برای کاربر مهیا می‌کند که کاربران می‌توانند پنجره‌های متعدد داشته باشند و در هرکدام برنامه اجرا کنند و پنجره‌های مختلف اضافه نمایند. سیستم X Window عموماً بر روی desktopی که کاربر لاگین نموده است مورد استفاده قرار می‌گیرد.

در مواردی که سازمان به طورخاص به دسترسی لاگین گرافیکی از طریق X Window نیاز ندارد، می‌بایست آن را حذف نمود تا احتمال وقوع حملات احتمالی و بالقوه کاهش یابد.

نحوه بررسی صحت پیکربندی امن:

اجرای دستور زیر این اطمینان را حاصل می‌نماید که سیستم در مود گرافیکی بوت نمی‌شود.

```
ls -l /etc/systemd/system/default.target | grep graphical.target
```

با اجرای این دستور، نباید خروجی برگردانده شود.

اجرای دستور زیر مشخص می‌نماید که سرویس دهنده X Window بر روی سیستم نصب می‌باشد یا خیر.

```
# rpm -q xorg-x11-server-common
package xorg-x11-server-common is not installed
```

نحوه اجرای پیکربندی امن:

تغییر سطح اجرایی پیش‌فرض به چندین کاربر بدون X :

```
# cd /etc/lib/systemd/system/
# unlink default.target
# ln -s /usr/lib/systemd/system/multi-user.target default.target
```

حذف نمودن سرویس‌دهنده X Window :

```
# yum remove xorg-x11-server-common
```

3-4. غیرفعال نمودن Avahi Server

Avahi یک پیاده‌سازی رایگان از zeroconf است که شامل سیستمی جهت کشف سرویس چند پخشی DNS/DNS-SD است. Avahi به برنامه‌ها اجازه انتشار و کشف سرویس‌ها و میزبان‌های در حال اجرا بر روی شبکه محلی را بدون هیچ‌گونه تنظیمات خاصی می‌دهد. برای مثال یک کاربر می‌تواند یک کامپیوتر را به شبکه اضافه کند و Avahi به‌طور خودکار پرینتر، کاربران، فایل‌ها و سرویس‌های شبکه در حال اجرا بر روی کامپیوتر را پیدا می‌کند.

از آنجایی‌که معمولاً از سرورها برای پرینت استفاده نمی‌شود، بنابراین به این سرویس نیازی نیست. دراین صورت می‌بایست این سرویس را برای کاهش احتمال وقوع حملات احتمالی و بالقوه غیرفعال نمود.

نحوه بررسی صحت پیکربندی امن:

اجرای دستور زیر مشخص می‌کند که Avahi غیرفعال شده است یا خیر.

```
# systemctl is-enabled avahi-daemon
```

طبق خروجی به‌دست آمده از دستور بالا از غیرفعال بودن Avahi اطمینان حاصل می‌گردد.

نحوه اجرای پیکربندی امن:

```
# systemctl disable avahi-daemon
```

4-4. غیرفعال نمودن سرویس دهنده چاپ CUPS

سیستم چاپ عادی یونیکس[35](CUPS) امکان چاپ محلی و شبکه‌ای را فراهم نموده است. سیستمی که در آن CUPS در حال اجراست، می‌تواند سفارش چاپ را از سیستم‌های دور قبول کند و آن‌ها را در چاپگر محلی چاپ نماید. همچنین قابلیت مدیریت از راه دور مبتنی بر وب را نیز فراهم می‌آورد.

اگر در سیستمی نیازی به کارهای چاپی و قبول چاپ از سیستم‌های دوردست نیست، پیشنهاد می‌گردد CUPS را برای کاهش احتمال وقوع حملات بالقوه غیرفعال نمود.

نحوه بررسی صحت پیکربندی امن:

اجرای دستور زیر مشخص می‌کند که CUPS غیرفعال می‌باشد.

```
# systemctl is-enabled cups
disabled
```

[35] Common Unix Print System

نحوه اجرای پیکربندی امن:

```
# systemctl disabled cups
```

4-5. حذف DHCP Server

سرویس DHCP[36] به ماشین‌ها به صورت پویا آدرس IP تخصیص می‌دهد.

پیشنهاد می‌گردد که این سرویس برای کاهش احتمال وقوع حملات بالقوه حذف گردد مگر اینکه سرویس دهنده به طور خاص به‌عنوان سرویس‌دهنده DHCP راه‌اندازی شود.

نحوه بررسی صحت پیکربندی امن:

اجرای دستور زیر مشخص می‌کند که DHCP بر روی سیستم فعال یا غیرفعال می‌باشد.

```
# rpm -q dhcp
package dhcp is not installed
```

نحوه اجرای پیکربندی امن:

```
# yum erase dhcp
```

[36] Dynamic Host Configuration Protocol

6-4. پیکربندی NTP

پروتکل زمان شبکه‌ای NTP[37] برای همگام‌سازی ساعت انواع مختلف سیستم‌ها استفاده می‌شود و از یک منبع بسیار دقیق استفاده می‌نماید. NTP می‌تواند به عنوان یک کلاینت و یا یک سرویس‌دهنده پیکربندی گردد.

توصیه می‌گردد سیستم‌های فیزیکی و مجازی که به طور مستقیم به ساعت میزبان دسترسی ندارند، به عنوان NTP Client پیکربندی شوند تا ساعت‌هایشان همگام‌سازی گردند (به خصوص برای پشتیبانی زمان در مکانیزم‌های حساس به زمان شبیه Kerberos). این کار تضمین می‌کند فایل‌های log ای که در یک شرکت ثبت می‌شوند، زمان ثبت آن‌ها با هم سازگار است که این مورد به تحقیقات جرم‌شناسی کمک بزرگی می نماید.

نحوه بررسی صحت پیکربندی امن:

اسکریپت زیر صحیح بودن پارامترها در restrict default و restrict -6 default را چک می‌کند:

```
# grep "restrict default" /etc/ntp.conf
restrict default kod nomodify notrap nopeer noquery
# grep "restrict -6 default" /etc/ntp.conf
restrict -6 default kod nomodify notrap nopeer noquery
```

در صورتی‌که سیستم به‌گونه‌ای پیکربندی شده باشد که از یک سرویس دهنده NTP استفاده نماید و دایمون ntp توسط کاربر غیرممتاز[38] اجرا شده باشد، دستور زیر آن را مشخص می‌کند.

```
# grep "^server" /etc/ntp.conf
  server
# grep "ntp:ntp" /etc/sysconfig/ntpd
OPTIONS="-u ntp:ntp -p /var/run/ntpd.pid"
```

[37] Network Time Protocl
[38] Unprivileged user

نحوه اجرای پیکربندی امن:

می‌بایست در فایل /etc/ntp.conf پارامترها به شکل زیر محدود گردند:

```
restrict default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer noquery
```

همچنین باید اطمینان حاصل گردد که در /etc/ntp.conf یک سرور NTP مشخص شده است.

```
server <ntp-server>
```

نکته: سرویس‌دهنده NTP، آدرس IP یا نام میزبان سرور زمانی مورد اعتماد است. نحوه پیکربندی یک سرویس‌دهنده NTP خارج از اهداف این گزارش است.

می‌بایست اطمینان حاصل گردد که در فایل /etc/sysconfig/ntpd گزینه OPTIONS برابر u ntp:ntp– است:

```
OPTIONS="-u ntp:ntp"
```

7-4. حذف LDAP

پروتکل LDAP[39] به‌عنوان جایگزینی برای پروتکل NIS/YP معرفی شده است. این سرویس یک روش برای جستجوی اطلاعات در پایگاه‌داده مرکزی فراهم کرده است. نرم‌افزار پیش‌فرض کلاینت/سرویس‌دهنده LDAP برای سیستم‌عامل CentOS، برنامه کاربردی OpenLDAP است.

در صورتی‌که سرویس‌دهنده به فعالیت LDAP احتیاج ندارد، توصیه می‌گردد این سرویس برای کاهش احتمال وقوع حملات بالقوه غیرفعال گردد.

نحوه بررسی صحت پیکربندی امن:

دستور زیر مشخص می‌کند LDAP بر روی سیستم در حال اجرا است یا خیر.

```
# rpm -q openldap-servers
package openldap-servers is not installed
# rpm -q openldap-clients
package openldap-clients is not installed
```

نحوه اجرای پیکربندی امن:

اگر LDAP روی سیستم در حال اجرا می‌باشد و نیازی به آن احساس نمی‌شود، می‌بایست آن را توسط دستورات زیر حذف نمود:

```
# yum erase openldap-servers
# yum erase openldap-clients
```

[39] Lightweight Directory Access Protocol

8-4. غیرفعال نمودن NFS و RPC

فایل‌سیستم شبکه[40] (NFS) یکی از اولین و گسترده‌ترین فایل‌سیستم‌های محیط یونیکس است و توانایی سوار نمودن[41] فایل‌سیستم‌های دیگر سرورها از طریق شبکه را مهیا می‌کند.

در صورتی‌که به آن احتیاجی نیست، توصیه می‌گردد برای کاهش احتمال وقوع حملات بالقوه غیرفعال گردد.

نحوه بررسی صحت پیکربندی امن:

اجرای دستورات زیر مشخص می‌کنند که NFS بر روی سیستم غیرفعال شده است.

```
# systemctl is-enabled nfslock
# systemctl is-enabled rpcgssd
# systemctl is-enabled rpcbind
# systemctl is-enabled rpcidmapd
# systemctl is-enabled rpcsvcgssd
```

نحوه اجرای پیکربندی امن:

```
# systemctl disable nfslock
# systemctl disable rpcgssd
# systemctl disable rpcbind
# systemctl disable rpcidmapd
# systemctl disable rpcsvcgssd
```

[40] Network File System
[41] mount

4-9. حذف DNS Server

سیستم نام دامنه[42] (DNS)، سیستم نامگذاری سلسله مراتبی است که نام‌ها را به آدرس‌های IP برای کامپیوترها، سرویس‌ها و منابع دیگری که به شبکه وصل شده‌اند تبدیل می‌کند.

پیشنهاد می‌گردد که این سرویس برای کاهش احتمال وقوع حملات بالقوه حذف گردد مگر اینکه سرویس دهنده به‌طورخاص به عنوان سرویس‌دهنده DNS راه‌اندازی شود.

نحوه بررسی صحت پیکربندی امن:

اجرای دستور زیر مشخص می‌کند که آیا DNF بر روی سیستم غیرفعال شده است یا خیر.

```
# rpm -q bind
package bind is not installed
```

نحوه اجرای پیکربندی امن:

```
# yum erase bind
```

4-10. حذف FTP Server

پروتکل انتقال فایل[43] (FTP) توانایی ارسال فایل را برای کامپیوترها در سطح شبکه فراهم می‌آورد.

[42] Domain Name System
[43] File Transfer Protocol

FTP از محرمانه‌بودن داده‌ها یا اطلاعات احراز هویت ردوبدل شده محافظت نمی‌کند و پیشنهاد می‌گردد به جای آن از SFTP برای ارسال استفاده گردد.

درصورتی‌که به اجرای سیستم به‌عنوان یک سرویس‌دهنده FTP نیازی نیست (به عنوان مثال برای دانلود ناشناس)، توصیه می‌گردد که این پروتکل برای کاهش احتمال وقوع حملات بالقوه غیرفعال گردد.

نحوه بررسی صحت پیکربندی امن:

اجرای دستور زیر مشخص می‌کند که FTP بر روی سیستم غیرفعال شده است یا خیر.

```
# rpm -q vsftpd
package vsftpd is not installed
```

نحوه اجرای پیکربندی امن:

```
# yum erase vsftpd
```

11-4. حذف سرویس‌دهنده HTTP

پروتکل HTTP که به‌عنوان سرویس‌دهنده وب مورد استفاده قرار می‌گیرد، توانایی میزبانی محتوای وب را فراهم می‌آورد. سرویس‌دهنده HTTP پیش‌فرض در سیستم‌عامل CentOS آپاچی می‌باشد.

پیشنهاد می‌گردد که این سرویس را برای کاهش احتمال وقوع حملات بالقوه حذف نمود مگر اینکه سرویس دهنده به طور خاص و مجزا به‌عنوان وب‌سرور راه‌اندازی گردد.

نحوه بررسی صحت پیکربندی امن:

اجرای دستور زیر مشخص می‌کند که آپاچی بر روی سیستم غیرفعال می‌باشد یا خیر.

```
rpm -q httpd
package httpd is not installed
```

نحوه اجرای پیکربندی امن:

```
# yum erase httpd
```

12-4. حذف Dovecot (IMAP and POP3 services)

Dovecot یک سرویس‌دهنده IMAP و POP3 متن‌باز برای سیستم‌های بر پایه‌ی لینوکس است.

پیشنهاد می‌گردد که این سرویس برای کاهش احتمال وقوع حملات بالقوه حذف گردد مگر در مواردی که سرورهای POP3 و IMAP برای سرویس‌دهنده‌ای لازم باشند.

نحوه بررسی صحت پیکربندی امن:

اجرای دستور زیر مشخص می‌کند که dovecot بر روی سیستم نصب می‌باشد یا خیر.

```
# rpm -q dovecot
package dovecot is not installed
```

نحوه اجرای پیکربندی امن:

```
# yum erase dovecot
```

13-4. حذف Samba

دایمون Samba به مدیران سیستم اجازه می‌دهد که سیستم‌های لینوکس خود را طوری تنظیم نمایند که فایل سیستم و شاخه‌های خود را با سیستم‌های ویندوز به اشتراک گذارند. Samba فایل‌ها و دایرکتوری‌ها را از طریق پروتکل SMB[44] تبلیغ می‌کند. کاربران ویندوز قادر خواهند بود این فایل‌ها و دایرکتوری‌ها را در یکی از درایورهای سیستم خود سوار نمایند.

در صورتی‌که نیازی به Samba احساس نمی‌شود، پیشنهاد می‌گردد که برای کاهش احتمال وقوع حملات بالقوه از سیستم حذف گردد.

نحوه بررسی صحت پیکربندی امن:

اجرای دستور زیر مشخص می‌کند samba بر روی سیستم نصب می‌باشد یا خیر.

```
# rpm -q samba
package samba is not installed
```

نحوه اجرای پیکربندی امن:

```
# yum erase samba
```

[44] Small Message Block

4-14. حذف سرویس‌دهنده پروکسی HTTP

Squid بسته پیش‌فرض HTTP proxy است که با CentOS روانه بازار شده است.

در صورت عدم نیاز به poroxy server ، توصیه می‌گردد که squid برای کاهش احتمال وقوع حملات بالقوه حذف گردد.

نحوه بررسی صحت پیکربندی امن:

اجرای دستور زیر مشخص می‌کند squid بر روی سیستم نصب می‌باشد یا خیر.

```
# rpm -q squid
package squid is not installed
```

نحوه اجرای پیکربندی امن:

```
# yum erase squid
```

4-15. حذف سرویس‌دهنده SNMP

سرویس‌دهنده SNMP[45] برای گوش‌کردن به دستورات SNMP از یک سیستم مدیریت SNMP، اجرای دستورات و جمع‌آوری اطلاعات و ارسال نتایج به سیستم درخواست کننده مورد استفاده قرار می‌گیرد.

اگر سرویس‌دهنده SNMP از SNMPv1 استفاده کند، برای انتقال اطلاعات و اجرای دستورات، احراز هویت انجام نمی‌گیرد.

[45] Simple Network Management Protocol

توصیه می‌گردد که در صورت ضرورت از این سرویس استفاده گردد. در غیر این‌صورت توصیه می‌گردد که این سرویس مورد استفاده قرار نگیرد.

نحوه بررسی صحت پیکربندی امن:

اجرای دستور زیر مشخص می‌کند که net-snmp بر روی سیستم نصب می‌باشد یا خیر.

```
# rpm -q net-snmp
package net-snmp is not installed
```

نحوه اجرای پیکربندی امن:

```
# yum erase net-snmp
```

16-4. پیکربندی MTA در حالت Local-Only

از ایستگاه انتقال پست‌الکترونیکی MTA[46]، برای دریافت و ارسال ایمیل به یک کاربر یا سرویس‌دهنده پست الکترونیکی استفاده می‌شود.

اگر سیستمی برای میل‌سرور بودن در نظر گرفته نشده است، توصیه می‌گردد که MTA طوری تنظیم گردد که فقط ایمیل‌های محلی را پردازش کند.

[46] Mail Transfer Agents

نرم‌افزارهای موجود در بازار برای همه‌ی MTAها پیچیده بوده و مشکلات امنیتی زیادی دارند. مهم این است که اطمینان حاصل گردد که سیستم می‌تواند پیغام‌های پست الکترونیکی محلی را پردازش کند و لازم نیست یک دایمون MTA داشته باشد که به پورت گوش کند، مگر اینکه به عنوان یک میل‌سرور در نظر گرفته شده باشد که از سیستم‌های دیگر نامه دریافت کند.

نحوه بررسی صحت پیکربندی امن:

با انجام دستور زیر اطمینان حاصل می‌گردد که MTA آدرس loopback (127.0.0.1) را گوش می‌کند:

```
# netstat -an | grep LIST | grep ":25[[:space:]]"
tcp 0 0 127.0.0.1:25 0.0.0.0:* LISTEN
```

نحوه اجرای پیکربندی امن:

می‌بایست فایل /etc/postfix/main.cf ویرایش گردد و سطر زیر به بخش RECEIVING MAIL اضافه گردد. در صورتی‌که این سطر وجود دارد، می‌بایست آن‌را به شکل زیر تغییر داد:

```
inet_interfaces = localhost
# Execute the following command to restart postfix
# service postfix restart
```

1 5. پیکربندی شبکه و فایروال‌ها

این بخش راهنمایی برای پیکربندی امنیت‌شبکه و فایروال است.

5-1. اصلاح پارامترهای شبکه (Host Only)

پارامترهای شبکه که در ادامه توضیح داده خواهند شد مشخص می‌کنند که یک سیستم به مانند یک میزبان تنها[47] عمل می‌کند. یک سیستم در صورتی به‌عنوان یک میزبان‌تنها شناخته می‌شود که یک اینترفیس شبکه داشته باشد یا اگر سیستم دارای دو یا چندین اینترفیس شبکه بود، مانند یک روتر تنظیم نشده باشد.

5-1-1. غیرفعال نمودن IP Forwarding

پرچم net.ipv4.ip_forward به سرور می‌گوید که آیا می‌تواند بسته را هدایت کند یا خیر. در صورتی‌که سرور وظیفه مسیریابی را برعهده ندارد، بایستی پرچم را برابر 0 در نظر گرفت.

مقداردهی پرچم با مقدار صفر این اطمینان را ایجاد می‌نماید که سرور با اینترفیس‌های چندگانه، هیچ‌وقت نمی‌تواند بسته را هدایت نماید و بنابراین هیچ وقت نمی‌تواند مثل یک روتر خدمت کند.

نحوه بررسی صحت پیکربندی امن:

اجرای دستور زیر مشخص می‌کند که net.ipv4.ip_forward بر روی سیستم نصب می‌باشد یا خیر.

```
# /sbin/sysctl net.ipv4.ip_forward
 net.ipv4.ip_forward = 0
```

نحوه اجرای پیکربندی امن:

[47] Host Only

در فایل /etc/sysctl.conf، می‌بایست پارامتر net.ipv4.ip_forward به 0 تنظیم گردد:

```
net.ipv4.ip_forward=0
```

اصلاح پارامترهای فعال هسته مطابق:

```
forward=0  # /sbin/sysctl -w net.ipv4.ip
# /sbin/sysctl -w net.ipv4.route.flush=1
```

5-1-2. غیرفعال نمودن تغییر مسیر ارسال بسته

پیغام ICMP مبتنی بر تغییر مسیر[۴۸]، برای ارسال اطلاعات مسیریابی به دیگر میزبان‌ها مورد استفاده قرار می گیرد. یک میزبان تنها به مانند یک روتر عمل نمی‌کند و در این صورت هیچ احتیاجی به ارسال تغییر مسیر وجود ندارد.

یک حمله‌کننده می‌تواند میزبان را با ارسال پیغام ICMP مبتنی بر تغییر مسیر نامعتبر به دیگر تجهیزات مسیریابی به خطا بیاندازد و دسترسی نامعتبری به سیستم پیدا کند.

نحوه بررسی صحت پیکربندی امن:

در صورتی‌که تغییر مسیر ارسال بسته غیرفعال باشد به صورت زیر مشخص می‌گردد:

```
# /sbin/sysctl net.ipv4.conf.all.send redirects
net.ipv4.conf.all.send redirects = 0
# /sbin/sysctl net.ipv4.conf.default.send redirects
net.ipv4.conf.default.send_redirects = 0
```

[48] ICMP redirect

نحوه اجرای پیکربندی امن:

می‌بایست پارامترهای net.ipv4.conf.all.send_redirects و net.ipv4.conf.default.send_redirects در فایل /etc/sysctl.conf به 0 تغییر یابند:

```
net.ipv4.conf.all.send_redirects=0
net.ipv4.conf.default.send_redirects=0
```

پارامترهای هسته فعال نیز بایستی مطابق زیر تغییر یابند:

```
# /sbin/sysctl -w net.ipv4.conf.all.send_redirects=0
# /sbin/sysctl -w net.ipv4.default.all.send_redirects=0
# /sbin/sysctl -w net.ipv4.route.flush=1
```

5-2. اصلاح پارامترهای شبکه (میزبان و مسیریاب)

پارامترهای شبکه‌ای زیر تعیین می‌کنند که سیستم به‌مانند یک مسیریاب عمل کند. یک سیستم هنگامی می‌تواند مشابه یک مسیریاب عمل کند که حداقل دو اینترفیس شبکه[49] داشته باشد و برای مسیریابی نیز پیکربندی شده باشد.

5-2-1 غیرفعال نمودن پذیرش بسته‌های Source Routed

در شبکه، source routing به فرستنده اجازه می‌دهد که به طور کامل یا جزئی مسیر بسته‌ها را در شبکه تعیین کند. در مقابل بسته‌های non-source routed مسیری که توسط روترها در شبکه تعیین شده را طی می‌کنند. در بعضی موارد ممکن است سیستم‌ها از بعضی مکان‌ها قابل دسترس یا مسیردهی نباشند (مثل

[49] interfaces

آدرس‌های خصوصی[50] در برابر مسیریابی اینترنت) و بنابراین بایستی از بسته‌های source routed استفاده شود.

اگر net.ipv4.conf.all.accept_source_route و net.ipv4.conf.default.accept_source_route به مقدار 0 تنظیم گردند، سیستم بسته‌های source routed را دریافت نمی‌نماید. فرض بر این است که سرور قادر است بسته‌ها را مابین اینترفیس متصل به شبکه اینترنت (آدرس‌های عمومی) و شبکه متصل به شبکه داخلی (آدرس‌های خصوصی) مسیریابی نماید.

در ضمن آدرس‌های خصوصی نباید به اینترنت مسیریابی شوند. در شرایط نرمال، یک مهاجم از یک آدرس قابل مسیریابی اینترنت نمی‌تواند برای دستیابی به آدرس خصوصی سرورها استفاده کند مگر اینکه source routed packet اجازه این کار را دهد. در این‌صورت آن‌ها می‌توانند به سیستم‌های با آدرس خصوصی دستیبابی داشته باشند درصورتی‌که پروتکل‌های مسیریابی اجازه این کار را نخواهند داد.

نحوه بررسی صحت پیکربندی امن:

دستورات زیر مشخص می‌نماید که آیا پذیرش بسته‌های source routed بر روی سیستم غیرفعال است یا فعال.

```
# /sbin/sysctl net.ipv4.conf.all.accept_source_route
net.ipv4.conf.all.accept_source_route = 0
# /sbin/sysctl net.ipv4.conf.default.accept_source_route
net.ipv4.conf.default.accept_source_route = 0
```

نحوه اجرای پیکربندی امن:

[50] private

در فایل /etc/sysctl.conf پارامترهای net.ipv4.conf.all.accept_source_route و net.ipv4.conf.default.accept_source_route به 0 تنظیم گردند.

```
net.ipv4.conf.all.accept_source_route=0
net.ipv4.conf.default.accept_source_route=0
```

پارامترهای هسته فعال نیز بایستی مطابق زیر تغییر داده شوند:

```
route=0 source # /sbin/sysctl -w net.ipv4.conf.all.accept
# /sbin/sysctl -w net.ipv4.conf.default.accept_source_route=0
# /sbin/sysctl -w net.ipv4.route.flush=1
```

5-2-2. غیرفعال نمودن پذیرش پیغام‌های ICMP مبتنی بر تغییر مسیر

پیغام‌های ICMP مبتنی‌بر تغییر مسیر، بسته‌هایی هستند که اطلاعات مسیریابی را انتقال می‌دهند و می‌گویند میزبان‌های موجود (که به مانند یک روتر رفتار می‌کنند)، بسته‌ها را به یک مسیر جایگزین بفرستند. این‌کار اجازه می‌دهد که یک دستگاه مسیریاب خارجی جدول‌های مسیریابی سیستم را به‌روز کند.

با تنظیم net.ipv4.conf.all.accept_redirects به 0، سیستم پیغام‌های ICMP مبتنی‌بر تغییر مسیر را قبول نمی‌کند و بنابراین به افراد خارجی اجازه به‌روز رسانی جدول مسیریابی سیستم را نمی‌دهد.

حمله‌کنندگان می‌توانند با ارسال پیغام‌های ICMP مبتنی بر تغییر مسیر ساختگی، جدول مسیریابی را تغییر داده و بسته‌ها را به شبکه دیگری فرستاده و ممکن است آن‌ها را به سرقت برند.

نحوه بررسی صحت پیکربندی امن:

با اجرای دستور زیر مشخص می‌گردد که آیا پیغام‌های ICMP مبتنی‌بر تغییر مسیر پذیرفته می‌شوند یا خیر.

```
redirects  # /sbin/sysctl net.ipv4.conf.all.accept
net.ipv4.conf.all.accept_redirects = 0
redirects  # /sbin/sysctl net.ipv4.conf.default.accept
net.ipv4.conf.default.accept_redirects = 0
```

نحوه اجرای پیکربندی امن:

بایستی پارامترهای net.ipv4.conf.all.accept_redirect و net.ipv4.conf.default.accept_redirects در فایل /etc/sysctl.conf به 0 تغییر داده شوند:

```
redirects=0  net.ipv4.conf.all.accept
net.ipv4.conf.default.accept_redirects=0
```

پارامترهای هسته فعال نیز بایستی مطابق زیر تغییر یابد:

```
# /sbin/sysctl -w net.ipv4.conf.all.accept  redirects=0
# /sbin/sysctl -w net.ipv4.conf.default.accept  redirects=0
# /sbin/sysctl -w net.ipv4.route.flush=1
```

5-2-3. غیرفعال نمودن پذیرش پیغام‌های ICMP مبتنی‌بر تغییر مسیر امن

پیغام‌های ICMP مبتنی‌بر تغییر مسیر امن همان ICMP redirect ها هستند که فقط از gatewayهای لیست شده در لیست gatewayهای پیش‌فرض می‌آیند. فرض شده است این‌gatewayها برای سیستم شناخته شده اند و به احتمال زیاد امن شده‌اند.

البته هنوز هم احتمال به خطر افتادن حتی gatewayهای شناخته شده وجود دارد. می‌بایست پارامتر net.ipv4.conf.all.secure_redirects به 0 تغییر یابد تا سیستم از به‌روزرسانی جدول مسیریابی به وسیله gatewayهای امن شناخته شده (ولی تسخیر شده) نیز محافظت شود.

نحوه بررسی صحت پیکربندی امن:

اجرای دستور زیر مشخص می‌نماید که پیغام‌های ICMP مبتنی‌بر تغییر مسیر از طرف gatewayهای شناخته شده پذیرفته می‌شوند یا خیر.

```
redirects   # /sbin/sysctl net.ipv4.conf.all.secure
net.ipv4.conf.all.secure_redirects = 0
redirects   # /sbin/sysctl net.ipv4.conf.default.secure
net.ipv4.conf.default.secure_redirects = 0
```

نحوه اجرای پیکربندی امن:

می‌بایست در فایل /etc/sysctl.conf پارامترهای net.ipv4.conf.all.secure_redirects و net.ipv4.conf.default.secure_redirects به 0 تغییر یابند:

```
net.ipv4.conf.all.secure  redirects=0
net.ipv4.conf.default.secure_redirects=0
```

پارامترهای هسته فعال نیز بایستی مطابق زیر تغییر یابند:

```
# /sbin/sysctl -w net.ipv4.conf.all.secure  redirects=0
# /sbin/sysctl -w net.ipv4.conf.default.secure  redirects=0
# /sbin/sysctl -w net.ipv4.route.flush=1
```

4-2-5. ثبت بسته‌های مشکوک

وقتی این ویژگی فعال است، بسته‌ها با آدرس‌های منبع غیرقابل مسیریابی در kernel log ثبت می‌شوند.

فعال‌سازی این ویژگی و ثبت این بسته‌ها به مدیر اجازه می‌دهد که اگر یک مهاجم بسته جعلی به سرور ارسال کند، آن را مورد بررسی قرار دهد.

نحوه بررسی صحت پیکربندی امن:

با اجرای دستورات زیر، مشخص می‌گردد که آیا بسته‌های مشکوک ثبت می‌شوند یا خیر.

```
# /sbin/sysctl net.ipv4.conf.all.log_martians
net.ipv4.conf.all.log  martians = 1
# /sbin/sysctl net.ipv4.conf.default.log  martians
 net.ipv4.conf.default.log_martians = 1
```

نحوه اجرای پیکربندی امن:

در فایل /etc/sysctl.conf می‌بایست پارامترهای net.ipv4.conf.all.log_martians و net.ipv4.conf.default.log_martians به 1 تغییر مقدار داده شوند:

```
net.ipv4.conf.all.log_martians=1
net.ipv4.conf.default.log_martians=1
```

پارامترهای هسته فعال بایستی مطابق زیر تغییر یابند:

```
# /sbin/sysctl -w net.ipv4.conf.all.log_martians=1
# /sbin/sysctl -w net.ipv4.conf.default.log  martians=1
```

```
# /sbin/sysctl -w net.ipv4.route.flush=1
```

5-2-5. فعال نمودن عدم پذیرش درخواست‌های همه‌پخشی

می‌بایست net.ipv4.icmp_echo_ignore_broadcasts به 1 تغییر داده شود تا سیستم تمام درخواست‌های ICMP echo و timestamp همه‌پخشی[51] و یا چندپخشی[52] را حذف کند.

پذیرش درخواست‌های ICMP echo و timestamp با مقاصد همه‌پخشی یا چندپخشی برای شبکه می‌تواند زمینه‌ساز حمله smurf باشد. در حمله smurf، حمله‌کننده مقدار زیادی پیام ICMP همه‌پخشی با آدرس منبع جعلی می‌فرستد و اگر بسیاری از میزبان‌ها جواب این پیام‌ها را دهند، ترافیک شبکه چندین برابر می‌شود.

نحوه بررسی صحت پیکربندی امن:

اجرای دستور زیر مشخص می‌کند که سیستم تمام ICMO echo و درخواست‌های timestamp همه‌پخشی و چندپخشی را رد کند.

```
# /sbin/sysctl net.ipv4.icmp_echo_ignore_broadcasts
net.ipv4.icmp_echo_ignore_broadcasts = 1
```

نحوه اجرای پیکربندی امن:

بایستی در فایل /etc/sysctl.conf پارامتر net.ipv4.icmp_echo_ignore_broadcasts به 1 تغییر داده شود:

```
net.ipv4.icmp_echo_ignore_broadcasts=1
```

[51] Broadcast
[52] Multicast

پارامترهای هسته فعال بایستی مطابق زیر تغییر یابند:

```
broadcasts=1  ignore echo # /sbin/sysctl -w net.ipv4.icmp
# /sbin/sysctl -w net.ipv4.route.flush=1
```

5-2-6. فعال نمودن Bad Error Message Protection

می‌بایست icmp_ignore_bogus_error_responses به مقدار 1 تنظیم گردد تا هسته از ثبت کردن پاسخ‌های جعلی (غیر منطبق بر RFC-1122) اجتناب نموده و جلوی پرشدن فایل سیستم با پیام‌های log بی فایده جلوگیری شود.

بعضی روترها (و بعضی مهاجمان) پاسخ‌هایی که منطبق بر RFC-1122 نبوده ارسال می‌کنند و درنتیجه log سیستم را با پیام‌های بی فایده پر می‌کنند.

نحوه بررسی صحت پیکربندی امن:

اجرای دستور زیر مشخص می‌کند که آیا در سیستم پیغام‌های غیرمنطبق با استاندارد[53] پذیرفته می‌شوند یا خیر.

```
responses  error bogus ignore # /sbin/sysctl net.ipv4.icmp
net.ipv4.icmp_ignore_bogus_error_responses = 1
```

نحوه اجرای پیکربندی امن:

[53] bogus

می‌بایست در فایل /etc/sysctl.conf پارامتر net.ipv4.icmp_ignore_bogus_error_responses به 1 تنظیم گردد:

```
net.ipv4.icmp_ignore_bogus_error_responses=1
```

پارامترهای هسته فعال نیز بایستی مطابق زیر تغییر یابند:

```
# /sbin/sysctl -w net.ipv4.icmp_ignore_bogus_error_responses=1
# /sbin/sysctl -w net.ipv4.route.flush=1
```

5-2-7. فعال کردن RFC-recommended Source Route Validation

باید پارامترهای net.ipv4.conf.all.rp_filter و net.ipv4.conf.default.rp_filter به 1 تغییر داده شوند تا هسته لینوکس مجبور به استفاده از فیلترینگ عکس مسیر[54] بسته دریافتی برای تعیین اعتبار بسته شود. اگر بسته برگشت‌شده از همان اینترفیسی که بسته اولیه دریافت شده برنگردد، بسته حذف خواهد شد.

تنظیم این پرچم‌ها راه خوبی برای جلوگیری از فرستادن بسته‌های ساختگی توسط مهاجم‌ها است که نمی‌توان پاسخ آن‌ها را داد. البته بایستی توجه داشت که درصورت استفاده از مسیریابی نامتقارن، این قابلیت اشکال ایجاد خواهد نمود. این امر زمان استفاده از پروتکل‌های مسیریابی پویا[55] همچون BGP، OSPF و ... در سیستم رخ می‌دهد. اگر از مسیریابی نامتقارن بر روی سرویس‌دهنده استفاده می‌گردد، نمی‌توان این ویژگی را فعال نمود.

[54] reverse path filtering
[55] Dynamic Routing

نحوه بررسی صحت پیکربندی امن:

با اجرای دستور زیر مشخص می‌گردد که ویژگی RFC-recommended source route validation فعال است یا خیر.

```
filter  # /sbin/sysctl net.ipv4.conf.all.rp
net.ipv4.conf.all.rp_filter = 1
filter  # /sbin/sysctl net.ipv4.conf.default.rp
net.ipv4.conf.default.rp_filter = 1
```

نحوه اجرای پیکربندی امن:

می‌بایست در فایل /etc/sysctl.conf پارامترهای net.ipv4.conf.all.rp_filter و net.ipv4.conf.default.rp_filter به 1 تنظیم گردند:

```
filter=1  net.ipv4.conf.all.rp
net.ipv4.conf.default.rp_filter=1
```

پارامترهای هسته فعال نیز بایستی مطابق زیر تغییر یابند:

```
# /sbin/sysctl -w net.ipv4.conf.all.rp_filter=1
filter=1  # /sbin/sysctl -w net.ipv4.conf.default.rp
# /sbin/sysctl -w net.ipv4.route.flush=1
```

5-2-8. فعال نمودن کوکی‌های TCP SYN

زمانی‌که tcp_syncookie تنظیم می‌شود، هسته به‌صورت عادی به بسته‌های TCP SYN رسیدگی می‌کند تا زمانی‌که صف ارتباطات نیمه‌باز پر شود. در این زمان قابلیت کوکی SYN وارد عمل می‌شود. کوکی‌های SYN

بدون استفاده از صف SYN در همه‌حال کار می‌کنند. به جای آن، هسته به‌آسانی با SYN|ACK جواب SYN را می‌دهد ولی از یک شماره ترتیب مجعول TCP استفاده می‌کند که حاوی مقدار کد شده آدرس IP مبدأ، مقصد و شماره پورت و زمان بسته ارسال شده است. یک ارتباط درست، بسته ACK را مطابق روش three way handshake با شماره ترتیب مجعول می‌فرستد. این امر به سرور اجازه می‌دهد که تأیید نماید یک جواب معتبر برای کوکی SYN دریافت کرده و اجازه برقراری ارتباط را می‌دهد حتی اگر SYN مربوطه در صف وجود نداشته باشد.

مهاجمان از SYN flood برای اجرای حمله DOS استفاده می‌کنند و در طی آن سرویس مورد حمله قرار گرفته در سرور را با فرستادن تعداد زیادی بسته SYN بدون کامل کردن three way handshake متوقف می‌کنند. این بسته‌ها سریعاً صف ارتباطات نیمه‌باز هسته را پر نموده و نمی‌گذارند که ارتباط جدیدی شکل بگیرد. در این حالت کوکی SYN به سرور اجازه می‌دهد که ارتباط‌های معتبر جدید را قبول کند حتی اگر تحت حمله DOS قرار گرفته باشد.

نحوه بررسی صحت پیکربندی امن:

برای بررسی اینکه TCP SYN Cookies فعال است یا خیر می‌بایست دستور زیر اجرا گردد.

```
syncookies  # /sbin/sysctl net.ipv4.tcp
net.ipv4.tcp_syncookies = 1
```

نحوه اجرای پیکربندی امن:

در فایل /etc/sysctl.conf می‌بایست پارامتر net.ipv4.tcp_syncookies به 1 تنظیم گردد:

```
net.ipv4.tcp_syncookies=1
```

پارامترهای هسته فعال نیز بایستی مطابق زیر تغییر یابند:

```
syncookies=1  # /sbin/sysctl -w net.ipv4.tcp
# /sbin/sysctl -w net.ipv4.route.flush=1
```

5-3. شبکه‌های بی‌سیم

5-3-1. غیرفعال نمودن اینترفیس‌های بی‌سیم

شبکه‌های بی‌سیم زمانی‌که شبکه‌های سیمی در دسترس نیستند استفاده می‌شوند. CentOS شاملیک کیت ابزار بی‌سیم[56] است که به مدیران سیستم اجازه می‌دهد شبکه‌های بی‌سیم را پیکربندی و مورد استفاده قرار دهند.

اگر از ارتباط بی‌سیم استفاده نمی‌شود، توصیه می‌گردد برای کاهش احتمال وقوع حملات بالقوه این ابزار غیرفعال گردد.

نحوه بررسی صحت پیکربندی امن:

دستور زیر مشخص می‌کند که اینترفیس‌های بی‌سیم فعال می‌باشد یا خیر (می‌بایست تأیید گردد که همه‌ی اینترفیس‌های بی‌سیم قطع می‌باشند):

```
# ip link show
```

نحوه اجرای پیکربندی امن:

برای نمایش لیست اینترفیس‌ها و تجهیزات بی‌سیم از دستورات زیر استفاده می‌گردد. پس از شناسایی آن‌ها می‌بایست اینترفیس خاموش و یا حذف گردد.

```
# ip link show
# iw list
```

[56] Wireless tool kit

```
# ip link set <interface> down
# rm /etc/sysconfig/network-scripts/ifcfg-<interface>
```

5-4. پیکربندی IPv6

پروتکل شبکه‌ای IPv6 جانشین پروتکل IPv4 شده است و دارای آدرس‌های قابل مسیریابی بیشتر بوده و دارای امنیت بیشتری نسبت به IPv4 می‌باشد.

5-4-1. پیکربندی IPv6

اگر درشبکه از IPv6 استفاده می‌گردد، می‌بایست این بخش از گزارش برای پیکربندی IPv6 دنبال گردد.

5-4-1-1. غیرفعال نمودن تبلیغات مسیریابی IPv6

این تنظیمات توانایی پذیرش تبلیغات مسیریابی را غیرفعال می‌کند.

توصیه می‌شود سیستم، تبلیغات مسیریابی را قبول نکند زیرا که می‌تواند فریبی برای هدایت ترافیک به سوی سیستم مخربی باشد. تنظیمHard routes برای سیستم آن را در مقابل مسیرهای اشتباه محافظت می‌کند (معمولاً یک مسیر پیش‌فرض به یک روتر قابل اعتماد).

نحوه بررسی صحت پیکربندی امن:

برای بررسی اینکه پذیرش تبلیغات مسیریابی غیرفعال است، از دستورات زیر استفاده می‌گردد.

```
# /sbin/sysctl net.ipv6.conf.all.accept ra
net.ipv6.conf.all.accept ra = 0
# /sbin/sysctl net.ipv6.conf.default.accept_ra
net.ipv6.conf.default.accept_ra = 0
```

نحوه اجرای پیکربندی امن:

می‌بایست در فایل /etc/sysctl.conf پارامترهای net.ipv6.conf.all.accept_ra و net.ipv6.conf.default.accept_ra به 0 تنظیم گردند:

```
net.ipv6.conf.all.accept_ra=0
net.ipv6.conf.default.accept_ra=0
```

پارامترهای هسته فعال نیز بایستی مطابق زیر تغییر یابند:

```
ra=0  # /sbin/sysctl -w net.ipv6.conf.all.accept
ra=0 # /sbin/sysctl -w net.ipv6.conf.default.accept
# /sbin/sysctl -w net.ipv6.route.flush=1
```

5-4-1-2. غیرفعال نمودن پذیرش تغییر مسیر IPv6

این تنظیمات سیستم را از پذیرش پیغام تغییر مسیر مبتنی بر ICMP منع می‌کند. پیغام تغییر مسیر مبتنی بر ICMP ، به سیستم درباره مسیرهای جایگزین برای ارسال ترافیک اطلاع‌رسانی می‌کند.

توصیه می‌شود که سیستم، پیغام تغییر مسیر مبتنی بر ICMP را قبول نکند زیرا می‌تواند فریبی برای هدایت ترافیک به سوی سیستم مخرب باشد. تنظیم Hard routes برای سیستم آن را در مقابل مسیرهای اشتباه محافظت می‌کند (معمولاً یک مسیر پیش‌فرض به یک روتر قابل اعتماد).

نحوه بررسی صحت پیکربندی امن:

برای بررسی غیرفعال بودن IPv6 redirects از دستورات زیر استفاده می‌گردد.

```
# /sbin/sysctl net.ipv6.conf.all.accept redirects
net.ipv6.conf.all.accept_redirect = 0
# /sbin/sysctl net.ipv6.conf.default.accept redirects
net.ipv6.conf.default.accept_redirect = 0
```

نحوه اجرای پیکربندی امن:

در فایل /etc/sysctl.conf می‌بایست پارامترهای net.ipv6.conf.all.accept_redirects و net.ipv6.conf.default.accept_redirects به 0 تنظیم گردند:

```
net.ipv6.conf.all.accept redirects=0
net.ipv6.conf.default.accept_redirects=0
```

پارامترهای هسته فعال نیز بایستی مطابق زیر تغییر یابند:

```
# /sbin/sysctl -w net.ipv6.conf.all.accept redirects=0
# /sbin/sysctl -w net.ipv6.conf.default.accept redirects=0
# /sbin/sysctl -w net.ipv6.route.flush=1
```

5-4-2. غیرفعال نمودن IPv6

گرچه IPv6 امتیازات بسیار بیشتری نسبت به IPv4 دارد ولی تعداد کمی‌از سازمان‌ها IPv6 را پیاده‌سازی نموده‌اند.

در صورت عدم استفاده از IPv6، توصیه می‌شود برای کاهش احتمال وقوع حملات این نسخه غیرفعال گردد.

نحوه بررسی صحت پیکربندی امن:

دستورات زیر برای بررسی فعال‌بودن IPv6 به‌کار می‌روند.

```
# grep net.ipv6.conf.all.disable_ipv6 /etc/sysctl.conf
```

```
net.ipv6.conf.all.disable_ipv6=1
# /sbin/sysctl net.ipv6.conf.all.disable_ipv6
net.ipv6.conf.all.disable_ipv6=1
```

نحوه اجرای پیکربندی امن:

می‌بایست اطمینان حاصل گردد net.ipv6.conf.all.disable_ipv6 در فایل /etc/sysctl.conf به 1 تنظیم شده است.

```
net.ipv6.conf.all.disable_ipv6=1
```

پارامترهای هسته فعال نیز بایستی مطابق زیر تغییر یابند:

```
# /sbin/sysctl net.ipv6.conf.all.disable_ipv6=1
```

5-5. نصب TCP Wrappers

5-5-1. نصب TCP Wrappers

TCP Wrappers یک لیست‌دسترسی ساده بوده و روش ثبت استانداردی برای سرویس‌هایی که می‌توانند آن را پشتیبانی کنند، فراهم آورده است. در گذشته، سرویس‌هایی که inetd و xinetd نامیده می‌شدند استفاده از tcp wrapper را پشتیبانی می‌کردند. از زمانی‌که دیگر از inetd و xinetd استفاده نشد، به هر سرویسی که می‌تواند tcp wrapper را پشتیبانی کند، کتابخانه libwrap.so اضافه گردیده است.

TCP Wrappers یک مکانیزم لیست دسترسی ساده و مناسب را در اختیار سرویس‌هایی قرار می‌دهد که که ممکن است آن را در خود نداشته باشند. توصیه می‌شود که تمام سرویس‌هایی که می‌توانند TCP Wrappers را پشتیبانی کنند، از آن استفاده کنند.

نحوه بررسی صحت پیکربندی امن:

دستور زیر را برای اطمینان از اینکه TCP Wrapper فعال است می‌بایست اجرا نمود:

```
# yum list tcp wrappers
tcp_wrappers.<hardware platform>   <release>   <installed>
```

نحوه اجرای پیکربندی امن:

```
# yum install tcp_wrappers
```

برای بررسی اینکه یک سرویس از TCP Wrappers پشتیبانی می‌کند، می‌بایست دستور زیر را اجرا نمود:

```
# ldd <path-to-daemon> | grep libwrap.so
```

اگر دستور فوق خروجی به همراه داشت، نشان می‌دهد که سرویس TCP Wrappers را پشتیبانی می‌نماید.

5-5-2. ایجاد فایل /etc/hosts.allow

فایل /etc/hosts.allow مشخص می‌کند که کدام آدرس IP مجاز به وصل‌شدن به میزبان است. این فایل به همراه فایل /etc/hosts.deny استفاده می‌شود.

فایل /etc/hosts.allow کنترل دسترسی به وسیله IP را مهیا می‌کند و این اطمینان را به‌وجود می‌آورد که فقط سیستم مجاز می‌تواند به سرور وصل شود.

نحوه بررسی صحت پیکربندی امن:

می‌بایست دستور زیر را برای بررسی محتویات فایل /etc/hosts.allow اجرا نمود.

```
# cat /etc/hosts.allow
[contents will vary, depending on your network configuration]
```

نحوه اجرای پیکربندی امن:

می‌بایست فایل /etc/hosts.allow ایجاد گردد:

```
# echo "ALL: <net>/<mask>, <net>/<mask>, …" >/etc/hosts.allow
```

هر ترکیب <net>/<mask> (برای مثال "192.168.1.0/255.255.255.0") نشان می‌دهد که کدام بلوک شبکه که در استفاده سازمان می‌باشد، نیاز به اتصال به این سیستم دارد.

5-5-3. بررسی مجوز دسترسی به فایل /etc/hosts.allow

فایل /etc/hosts.allow شامل اطلاعات شبکه‌ای است که مورد استفاده بسیاری از نرم‌افزارها قرار می‌گیرد و بنابراین باید برای این نرم‌افزارها قابل خواندن باشد.

ضروری است مطمئن شویم که فایل /etc/hosts.allow دارای مجوز نوشتن توسط افراد غیرمجاز نیست. هرچند که این فایل به‌طور پیش‌فرض محافظت شده است، اما اجازه دسترسی می‌تواند سهواً یا از طریق نرم افزارهای مخرب تغییر کند.

نحوه بررسی صحت پیکربندی امن:

برای دیدن مجوز دسترسی فایل /etc/hosts.allow می‌بایست دستور زیر اجرا گردد.

```
# /bin/ls -l /etc/hosts.allow
-rw-r--r-- 1 root root 2055 Jan 30 16:30 /etc/hosts.allow
```

نحوه اجرای پیکربندی امن:

اگر اجازه دسترسی فایل/etc/hosts.allow اشتباه است، می‌بایست با اجرای دستور زیر آن را تصحیح نمود:

```
# /bin/chmod 644 /etc/hosts.allow
```

5-5-4. ایجاد فایل /etc/hosts.deny

فایل /etc/hosts.deny مشخص می‌کند که کدام آدرس IP مجاز به وصل شدن به میزبان نیست. این فایل به همراه فایل /etc/hosts.allow مورد استفاده قرار می‌گیرد.

فایل /etc/hosts.deny حالت جلوگیری از خطا داشته و اگر میزبانی در لیست فایل /etc/hosts.allow نباشد، اجازه دسترسی به سرور به وی داده نخواهد شد.

نحوه بررسی صحت پیکربندی امن:

بررسی اینکه فایل /etc/hosts.deny وجود دارد و به‌گونه‌ای پیکربندی شده است که تمام میزبانی‌هایی که صریحاً در /etc/hosts.allow لیست نشده است را نمی‌پذیرد:

```
# grep "ALL: ALL" /etc/hosts.deny
ALL: ALL
```

نحوه اجرای پیکربندی امن:

می‌بایست فایل /etc/hosts.deny ایجاد گردد:

```
# echo "ALL: ALL" >> /etc/hosts.deny
```

5-5-5. بررسی مجوز دسترسی به فایل /etc/hosts.deny

فایل /etc/hosts.deny شامل اطلاعات شبکه‌ای است که به‌وسیله بسیاری از نرم‌افزارها مورد استفاده قرار می‌گیرد و بنابراین باید برای این نرم افزارها قابل خواندن باشد.

ضروری است مطمئن شویم که فایل /etc/hosts.deny دارای مجوز نوشتن توسط افراد غیرمجاز نیست. هرچند که این فایل به‌طور پیش‌فرض محافظت شده است، اما اجازه دسترسی می‌تواند سهواً یا از طریق نرم افزارهای مخرب تغییر کند.

نحوه بررسی صحت پیکربندی امن:

برای دیدن دسترسی فایل /etc/hosts.deny می‌بایست دستور زیر اجرا گردد:

```
# /bin/ls -l /etc/hosts.deny
-rw-r--r-- 1 root root 2055 Jan 30 16:30 /etc/hosts.deny
```

نحوه اجرای پیکربندی امن:

اگر اجازه دسترسی فایل /etc/hosts.deny اشتباه است، می‌بایست با اجرای دستور زیر آن را تصحیح نمود:

```
# /bin/chmod 644 /etc/hosts.deny
```

5-6. پروتکل‌های شبکه‌ای غیر رایج

لینوکس CentOS چندین پروتکل شبکه‌ای که استفاده از آن‌ها رایج نیست را پشتیبانی می‌کند. در صورتی‌که به این پروتکل‌ها نیازی نمی‌باشد، پیشنهاد می‌گردد که آن‌ها غیرفعال گردند.

5-6-1. غیرفعال نمودن DCCP

پروتکل DCCP[57] در لایه انتقال[58] کار کرده و از جریان چندرسانه‌ای و تلفنی پشتیبانی می‌کند. DCCP راهی برای کنترل ازدحام است بدون آن‌که کاری به لایه‌ی کاربرد[59] داشته باشد، اما ترتیب تحویل بسته‌ها را رعایت نمی‌کند.

[57] Datagram Congestion Control Protocol
[58] Transport layer
[59] Application layer

در صورتی‌که این پروتکل مورد نیاز نمی باشد، پیشنهاد می‌گردد برای کاهش احتمال وقوع حملات بالقوه بر روی سیستم، درایور آن نصب نباشد.

نحوه بررسی صحت پیکربندی امن:

دستور زیر تعیین می‌کند که DCCP بر روی سیستم فعال است یا غیرفعال.

```
# grep "install dccp /bin/true" /etc/modprobe.d/CIS.conf
install dccp /bin/true
```

نحوه اجرای پیکربندی امن:

```
# echo "install dccp /bin/true" >> /etc/modprobe.d/CIS.conf
```

5-6-2. غیرفعال نمودن SCTP

پروتکل SCTP[60] یک پروتکل لایه انتقال است که برای پشتیبانی از ارتباطات پیامی (به‌صورت چند جریان از پیام‌ها در یک ارتباط) مورد استفاده قرار می‌گیرد. این پروتکل عملکردی شبیه TCP و UDP با ترکیبی از ویژگی‌های هر دو دارد (پیام‌گرا[61] بودن شبیه UDP و رعایت ترتیب پیام‌ها و پیاده‌سازی کنترل ازدحام شبیه TCP).

[60] Stream Control Transmission Protocol
[61] Message-oriented

اگر از این پروتکل استفاده نمی‌شود، توصیه می‌گردد که ماژول هسته آن بارگزاری نشود و این سرویس برای کاهش احتمال وقوع حملات بالقوه غیرفعال گردد.

نحوه بررسی صحت پیکربندی امن:

دستور زیر مشخص می‌کند که آیا SCTP بر روی سیستم غیرفعال است یا خیر.

```
# grep "install sctp /bin/true" /etc/modprobe.d/CIS.conf
install sctp /bin/true
```

نحوه اجرای پیکربندی امن:

```
# echo "install sctp /bin/true" >> /etc/modprobe.d/CIS.conf
```

3-6-5. غیرفعال نمودن RDS

پروتکل RDS[62] یک پروتکل لایه انتقال است که برای مهیا کردن زمان تأخیر کم و ارتباطات پهن باند بین cluster nodeها طراحی شده است. این پروتکل توسط شرکت اوراکل توسعه داده شده است.

اگر از این پروتکل استفاده نمی‌شود، توصیه می‌گردد که ماژول هسته بارگزاری نشود و این سرویس برای کاهش احتمال وقوع حملات بالقوه غیرفعال گردد.

نحوه بررسی صحت پیکربندی امن:

دستور زیر تعیین می‌کند که RDS بر روی سیستم غیرفعال است یا خیر.

[62] Reliable Datagram Sockets

```
# grep "install rds /bin/true" /etc/modprobe.d/CIS.conf
install rds /bin/true
```

نحوه اجرای پیکربندی امن:

```
# echo "install rds /bin/true" >> /etc/modprobe.d/CIS.conf
```

5-6-4. غیرفعال نمودن TIPC

پروتکل TIPC[۶۳] برای مهیا کردن ارتباطات بین cluster nodeها طراحی شده است.

اگر از این پروتکل استفاده نمی‌شود، توصیه می‌گردد که ماژول هسته بارگزاری نشود و برای کاهش احتمال وقوع حملات بالقوه غیرفعال گردد.

نحوه بررسی صحت پیکربندی امن:

دستور زیر تعیین می‌کند که TIPC بر روی سیستم غیرفعال است یا خیر.

```
# grep "install tipc /bin/true" /etc/modprobe.d/CIS.conf
install tipc /bin/true
```

نحوه اجرای پیکربندی امن:

```
# echo "install tipc /bin/true" >> /etc/modprobe.d/CIS.conf
```

[63] Transparent Inter-Process Communication

7-5. فعال نمودن firewalld

IPtables یک برنامه کاربردی است که به مدیر سیستم اجازه می‌دهد جدول‌های IP، زنجیره و قوانین مهیا شده توسط فایروال هسته لینوکس را پیکربندی نماید.

سرویس firewalld یک فایروال پویا می‌باشد که امکان اجازه تغییرات را در هر زمان بدون ایجاد اختلال در سرویس‌دهی، با بارگیری مجدد خود می‌دهد.

یک فایروال، حفاظت و امنیت بیشتری را به وسیله محدود کردن ارتباطات در داخل و خارج آدرس‌ها و پورت‌های مشخص شده برای سیستم لینوکس مهیا می‌کند.

نحوه بررسی صحت پیکربندی امن:

اجرای دستور زیر مشخص می‌کند که firewalld بر روی سیستم فعال می‌باشد یا خیر:

```
# systemctl is-enabled firewalld
 enabled
```

نحوه اجرای پیکربندی امن:

```
# systemctl enable firewalld
```

2

3

4

6. نظارت و ثبت وقایع

مواردی که در این بخش توصیف می‌شود، نحوه پیکربندی ثبت وقایع و نظارت بر وقایع ثبت شده با استفاده از ابزارهایی است که در CentOS 7 وجود دارد.

توصیه می‌شود که برای ثبت وقایع از rsyslog (همراه با logwatch که امکان نظارت را فراهم می‌آورد) و برای نظارت از audits (همراه با aureport که امکان نظارت را فراهم می‌آورد) استفاده شود تا به طور خودکار وقایع ثبت شده را برای تشخیص نفوذ و رفتار مشکوک سیستم‌ها مانیتور کند.

علاوه بر فایل‌های ثبت وقایع محلی که بنا به توصیه‌های این بخش تولید می‌شوند، توصیه می‌گردد که کپی فایل‌های ثبت وقایع از طریق یک ارتباط رمزگذاری شده به یک سرور مرکزی امن منتقل شوند. ثبت وقایع در یک مکان متمرکز، امکان همبسته‌سازی وقایع مختلف را فراهم ساخته و درنتیجه به تشخیص بهتر حوادث کمک می‌کند. در ضمن داشتن یک کپی دوم از اطلاعات ثبت وقایع این اطمینان را به‌وجود می‌آورد که در صورت تسخیر سیستم و تخریب فایل‌های ثبت وقایع توسط نفوذگر، همچنان این فایل‌ها وجود دارند.

از آن‌جایی‌که همبسته‌سازی فایل‌های ثبت وقایع نیازمند سنکرون بودن ساعت‌های تجهیزات مختلفی است که فایل ثبت وقایع تولید می‌کنند، توصیه می‌شود که زمان سیستم‌ها و تجهیزاتی که به شبکه محلی متصل هستند همگام‌سازی گردد. پروتکل استاندارد این‌کار Network Time Protocol (NTP) است که به وسیله بیشتر دستگاه‌ها پشتیبانی می‌شود.

6-1. پیکربندی rsyslog

نرم‌افزار rsyslog به عنوان جایگزینی برای دایمون syslogd پیشنهاد می‌گردد. این نرم‌افزار نسبت به syslogd توانایی‌های بیشتری از جمله ارسال اتصال‌گرای logها، فرمت پایگاه‌داده log انتخابی و امکان رمزگذاری داده‌های log در طول مسیر برای ورود به سرور مرکزی دارد.

6-1-1. نصب بسته rsyslog

بسته rsyslog یک افزونه‌ی جدید سیستم‌عامل است که قابلیت‌های بیشتری نسبت به syslog دارد. به عنوان مثال، ارتباط چند نخی، ارتباط TCP، امکان فیلتر پیام‌ها و پشتیبانی از پایگاه‌داده را فراهم می‌آورد.

پیشرفت‌های امنیتی rsyslog که در بخش قبلی بدان اشاره شد، نصب و پیکربندی این نرم‌افزار را توجیه می‌کند.

نحوه بررسی صحت پیکربندی امن:

برای بررسی نصب بودن rsyslog دستور زیر به‌کار می‌رود.

```
# rpm -q rsyslog
rsyslog.<package version>.<hardware platform>
```

نحوه اجرای پیکربندی امن:

```
# yum install rsyslog
```

6-1-2. فعال نمودن سرویس rsyslog

می‌توان از دستور systemctl برای اطمینان از اینکه سرویس rsyslog فعال است استفاده نمود.

اگر سرویس rsyslog غیرفعال است، در واقع سیستم سرویس syslog در حال اجرا ندارد.

نحوه بررسی صحت پیکربندی امن:

اجرای دستور زیر مشخص می‌کند که آیا rsyslog فعال می‌باشد یا خیر.

```
# systemctl is-enabled rsyslog
enabled
```

نحوه اجرای پیکربندی امن:

```
# systemctl enable rsyslog
```

3-1-6. پیکربندی /etc/rsyslog.conf

فایل /etc/rsyslog.conf قوانین ثبت وقایع و فایل‌هایی که بایستی برای ثبت وقایع کلاس‌های خاصی از پیام‌ها مورد استفاده قرار گیرند را مشخص می‌کند.

مقدار زیادی از اطلاعات مهم امنیتی از طریق rsyslog ارسال می‌شود (مثل تلاش موفق یا ناموفق برای su، تلاش‌های برای ورود ناموفق، تلاش‌های ورود در سطح کاربر ریشه و ...).

نحوه بررسی صحت پیکربندی امن:

برای اطمینان از اینکه قوانین ثبت وقایع به صورت مناسب تنظیم شده است، می‌بایست محتوای فایل /etc/rsyslog.conf بررسی گردد. به‌علاوه با اجرای دستور زیر از اینکه فایل‌های log اطلاعات را ثبت می‌کنند اطمینان حاصل می‌گردد:

```
# ls -l /var/log/
```

نحوه اجرای پیکربندی امن:

می‌بایست در فایل /etc/rsyslog.conf خطوط زیر به‌طور مناسب برای سیستم ویرایش گردند:

```
auth,user.* /var/log/messages
kern.* /var/log/kern.log
daemon.* /var/log/daemon.log
syslog.* /var/log/syslog
lpr,news,uucp,local0,local1,local2,local3,local4,local5,local6.* /var/log/unused.log

# Execute the following command to restart rsyslogd
# pkill -HUP rsyslogd
```

6-1-4. ایجاد و تنظیم سطح دسترسی برای فایل‌های ثبت وقایع rsyslog

بایستی یک فایل log وجود داشته باشد تا rsyslog بتواند داخل آن بنویسد.

بنابراین مهم است که از وجود فایل و همچنین مجوزهای صحیح دسترسی بدان فایل اطمینان حاصل گردد تا مطمئن بود که داده‌های rsyslog حساس، آرشیو شده و از آن محافظت می‌گردد.

نحوه بررسی صحت پیکربندی امن:

برای هر logfile که در فایل /etc/rsyslog.conf لیست شده است، می‌بایست دستور زیر اجرا گردد و بررسی شود که <owner>:<group> به‌صورت root:root و مجوز دسترسی 0600 (برای سازمان‌هایی که یک گروه امنیتی تعریف نکرده‌اند) و root:securegrp با مجوز دسترسی 0640 (برای سازمان‌هایی که یک گروه امنیتی تعریف کرده‌اند) می‌باشد:

```
# ls -l <logfile>
```

نحوه اجرای پیکربندی امن:

- برای سازمان‌هایی که یک گروه مدیریت امنیتی تعریف نکرده‌اند، پوشه /var/log/ ایجاد گردد و برای هر <logfile> که در فایل /etc/rsyslog.conf لیست شده است، دستورات زیر اجرا گردد:

```
touch <logfile>
# chown root:root <logfile>
# chmod og-rwx <logfile>
```

- برای سازمان‌هایی که یک گروه مدیریت امنیتی تعریف کرده‌اند، پوشه /var/log/ ایجاد گردد و برای هر <logfile> که در فایل /etc/rsyslog.conf لیست شده‌اند، دستورات زیر اجرا گردد (با نام گروه امنیتی تعریف شده):

```
# touch <logfile>
# chown root:<securegrp> <logfile>
# chmod g-wx,o-rwx<logfile>
```

6-1-5. تنظیم rsyslog برای ارسال logها به یک میزبان ثبت‌وقایع راه‌دور[۶۴]

[64] remote log host

ابزار rsyslog توانایی فرستادن logهای جمع‌آوری شده به یک میزبان ثبت‌وقایع راه‌دور را دارد که syslogd(8) را اجرا می‌کند. همچنین توانایی دریافت پیام‌ها از میزبان‌های راه دور را داشته که این امر سربار راهبری[۶۵] را کاهش می‌دهد.

ذخیره‌ی داده‌های log بر روی یک میزبان راه‌دور از یکپارچگی و صحت log در مقابل حملات محلی محافظت می‌کند. اگر یک مهاجم دسترسی کاربر ریشه به سیستم محلی را به‌دست آورد، می‌تواند logهایی که درسیستم محلی ذخیره شده است را دست‌کاری نموده یا حذف کند.

نحوه بررسی صحت پیکربندی امن:

فایل /etc/rsyslog.conf می‌بایست مرور و بررسی گردد، به‌طوری‌که اطمینان حاصل گردد که logها به سوی میزبان مرکزی فرستاده می‌شوند (که در آن logfile.example.com نام میزبان ثبت وقایع مرکزی می‌باشد):

```
# grep "^*.*[^I][^I]*@" /etc/rsyslog.conf
*.* @@loghost.example.com
```

نحوه اجرای پیکربندی امن:

می‌بایست فایل /etc/rsyslog.conf ویرایش و سطر زیر به آن اضافه گردد (که در آن logfile.example.com نام میزبان ثبت وقایع مرکزی می‌باشد):

```
*.* @@loghost.example.com
# Execute the following command to restart rsyslogd
# pkill -HUP rsyslogd
```

[65] administrative

نکته: علامت (@@)، rsyslog را به استفاده از TCP برای فرستادن logها به سوی سرور هدایت می‌کند که نسبت به UDP از اطمینان بیشتری برخوردار است.

6-1-6. قبول پیام‌های از راه‌دور rsyslog فقط از میزبان‌های ثبت‌وقایع معرفی شده

در حالت پیش‌فرض، rsyslog پیام‌هایی که از سیستم‌های راه‌دور می‌آیند را نمی‌پذیرد. ModLoad به rsyslog می‌گوید که ماژول imtcp.so بارگیری گردد تا بتواند در شبکه پیام‌های TCP را بشنود. گزینه‌ی "InputTCPServerRun" به rsyslog دستور می‌دهد که به پورت خاصی گوش کند.

توضیحات در این بخش تضمین می‌کند که میزبان ثبت‌وقایع راه‌دور به‌گونه‌ای پیکربندی شده است که فقط داده‌های rsyslog را از میزبان(های) مشخص شده قبول کند و هیچ پیام rsyslog ای را از سوی میزبان‌های تعریف نشده قبول نکند. این‌کار جلوی دریافت logهای جعلی را گرفته و تضمین می‌کند که مدیران سیستم داده‌های syslog نسبتاً کاملی را در محل مرکزی بررسی می‌کنند.

نحوه بررسی صحت پیکربندی امن:

در صورتی‌که rsyslog به پیام‌های از راه‌دور گوش کند، توسط دستورات زیر مشخص می‌گردد:

```
# grep '$ModLoad imtcp.so' /etc/rsyslog.conf
$ModLoad imtcp.so
# grep '$InputTCPServerRun' /etc/rsyslog.conf
$InputTCPServerRun 514
```

نحوه اجرای پیکربندی امن:

برای میزبان‌هایی که بایستی log آن‌ها دریافت گردد، می‌بایست فایل /etc/rsyslog.conf ویرایش و خطوط زیر در آن از حالت توضیحات خارج گردند:

```
$ModLoad imtcp.so
```

```
$InputTCPServerRun 514
```

نکته: برای میزبان‌هایی که نبایستی log آن‌ها دریافت گردد، این خطوط باید به‌صورت توضیحات در نظر گرفته شوند.

دستور زیر می‌بایست برای راه‌اندازی دوباره rsyslogd اجرا گردد:

```
# pkill -HUP rsyslogd
```

6-2. پیکربندی سیستم حسابرسی یا Accounting

حسابرسی[66] سیستم به‌وسیله auditd به مدیران سیستم اجازه می‌دهد تا سیستم‌های خود را مانیتور کرده و دسترسی‌های غیرمجاز و تغییر فایل‌ها را تشخیص دهند. به‌صورت پیش‌فرض، رویدادها در /var/log/audit/audit.log ذخیره می‌شوند. ذخیره این رویدادها حجم متوسطی از فضای هارد دیسک را استفاده می‌کند. درنتیجه درنظر گرفتن حجم مناسبی فضای ذخیره داده بدین منظور الزامی است.

6-2-1. پیکربندی نگهداری داده‌ها

تنظیم مقدار فضای مناسب برای ذخیره audit logs بسیار مهم است. به‌طور پیش‌فرض auditd نتایج را در فایلی با سایز ماکزیمم 5MB ذخیره نموده و فقط 4 کپی از نسخه‌های قدیمی را نگه می‌دارد. درصورت پر شدن این فضا، مقداری از audit logهای قدیمی از بین می‌رود. از این‌رو می‌بایست مقدار فضای لازم را به درستی محاسبه نمود.

[66] Auditing

6-2-1-1. پیکربندی سایز مخزن نگهداری logهای حسابرسی

حداکثر سایز فایل audit log را می‌بایست تنظیم نمود. وقتی فایل log به حداکثر سایز خود برسد، لاگ‌های جدید در یک فایل جدید شروع به ذخیره شدن خواهد کرد.

تعیین سایز مناسب برای ذخیره فایل‌های log بسیار مهم است (برای اینکه روی سیستم تاثیر منفی نگذاشته و داده‌ای گم نشود).

نحوه بررسی صحت پیکربندی امن:

برای تعیین حداکثر سایز فایل‌های audit log می‌بایست دستور زیر اجرا گردد:

```
# grep max log file /etc/audit/auditd.conf
max_log_file = <MB>
```

نحوه اجرای پیکربندی امن:

در فایل /etc/audit/auditd.conf می‌بایست پارامتر max_log_file تنظیم گردد:

```
max_log_file = <MB>
```

نکته: MB عددی است که نشان‌دهنده حجم فایل براساس مگابایت می‌باشد.

6-2-1-2. غیرفعال نمودن سیستم هنگام پر شدن logهای بررسی

دایمون auditd می‌تواند به گونه‌ای تنظیم گردد تا زمانی‌که فایل audit logها به‌صورت کامل پر شد، سیستم متوقف گردد.

در صورت نیاز به سطح بالای امنیت، مولفه‌های امنیتی تشخیص دسترسی غیرمجاز و عدم انکار بیش از مولفه دسترس‌پذیری سیستم دارای اهمیت است.

نحوه بررسی صحت پیکربندی امن:

اگر Auditd به‌گونه‌ای پیکربندی شده باشد که وقتی فایل audit logها پر شود، به مدیر هشدار دهد و سیستم را متوقف[۶۷] کند، دستورات زیر این موضوع را مشخص می‌نمایند:

```
# grep space_left_action /etc/audit/auditd.conf
space left action = email
# grep action mail acct /etc/audit/auditd.conf
action mail acct = root
 # grep admin_space_left_action /etc/audit/auditd.conf
admin_space_left_action = halt
```

نحوه اجرای پیکربندی امن:

می‌بایست خطوط زیر به فایل /etc/audit/auditd.conf اضافه گردند:

```
space left action = email
action mail acct = root
admin_space_left_action = halt
```

6-2-1-3. نگهداری همه‌ی اطلاعات حسابرسی

معمولاً auditd، چهار log آخر ذخیره شده (که هر یک بزرگترین سایز پیکربندی شده را دارند) را نگهداری نموده و با ایجاد فایل جدید، قدیمی‌ترین فایل را حذف می‌کند.

[67] halt

در صورت نیاز به سطح بالای امنیت، می‌توان تعداد بیشتری از فایل‌های قدیمی را نگهداری نمود. گاهی ارزش این فایل‌ها بسیار بیشتر از هزینه خرید فضای ذخیره‌سازی اضافی است.

نحوه بررسی صحت پیکربندی امن:

برای تعیین وضعیت نگهداری audit logها می‌بایست دستور زیر اجرا گردد:

```
# grep max log file action /etc/audit/auditd.conf
max_log_file_action = keep_logs
```

نحوه اجرای پیکربندی امن:

خطوط زیر می‌بایست به فایل /etc/audit/auditd.conf اضافه گردد:

```
max_log_file_action = keep_logs
```

6-2-2. فعال نمودن سرویس auditd

بایستی دایمون auditd برای ذخیره رویدادهای سیستم نصب و فعال گردد.

ثبت رویدادهای سیستم به مدیران سیستم اجازه می‌دهد که متوجه دسترسی‌های غیر مجاز به سیستم شوند.

نحوه بررسی صحت پیکربندی امن:

با اجرای دستور زیر اطمینان حاصل می‌گردد که auditd بر روی سیستم فعال می‌باشد.

```
# systemctl is-enabled auditd
enabled
```

نحوه اجرای پیکربندی امن:

```
# systemctl enable auditd
```

6-2-3. فعال نمودن حسابرسی فرآیندهایی که قبل از auditd شروع می‌شوند

می‌بایست Grub طوری پیکربندی گردد که پردازش‌هایی که امکان حسابرسی شدن داشته ولی قبل از راه اندازی auditd راه‌اندازی می‌شوند نیز حسابرسی شوند. درنتیجه احتمال عدم تشخیص فعالیت‌های مخرب کاهش خواهد یافت.

نحوه بررسی صحت پیکربندی امن:

با استفاده از دستور زیر می‌توان مطمئن شد که پیکربندی /boot/grub2/grub.cfg مناسب بوده و وقایع پروسه‌هایی که قبل از auditd شروع می‌شوند نیز ثبت می‌گردد:

```
# grep "linux" /boot/grub2/grub.cfg
```

بایستی اطمینان حاصل گردد که هرخطی که با Linux شروع می‌شود، دارای پارامتر audit=1 است.

نحوه اجرای پیکربندی امن:

می‌بایست در شاخه /etc/default/grub بخش GRUB_CMDLINE_LINUX مقدار audit=1 تنظیم گردد.

```
GRUB_CMDLINE_LINUX="audit=1"
```

و سپس با استفاده از دستور زیر پیکربندی grub به روزرسانی گردد:

```
# grub2-mkconfig -o /boot/grub2/grub.cfg
```

6-2-4. ثبت رویدادهایی که تاریخ و زمان را تغییر می‌دهند

بایستی رویدادهایی که تاریخ و زمان سیستم را تغییر می‌دهند، ثبت شوند. در این بخش پارامترهایی تنظیم می‌شوند تا درصورتی‌که adjtimex (تنظیم ساعت هسته)، settimeofday (تنظیم ساعت، با استفاده از timeval و ساختارهای محدوده زمانی)، stime (با استفاده از ثانیه از سال 1/1/1970) یا clock_settime (اکه جازه تنظیم چند ساعت و تایمر داخلی را می‌دهد) اجرا شوند، رخداد مربوطه در قالب یک رکورد حسابرسی در فایل /var/log/audit.log ذخیره شود و به آن برچسب "time-change" زده شود.

تغییرات غیرمنتظره در تاریخ و یا زمان سیستم می‌تواند نشانه فعالیت‌های مخرب در سیستم باشد.

نحوه بررسی صحت پیکربندی امن:

دستورات زیر مشخص می‌کنند که آیا رویدادهایی که زمان و تاریخ سیستم را تغییر می‌دهند، ثبت می‌شوند یا خیر.

در سیستم‌های 64بیتی، دستور زیر می‌بایست اجرا گردد و مطمئن شد که خروجی نشان داده می‌شود.

نکته: "-a always,exit" ممکن است به صورت "-a exit,always" مشخص گردد.

```
change /etc/audit/audit.rules-# grep time
 -a always,exit -F arch=b64 -S adjtimex -S settimeofday -k time-change
 -a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-change
 -a always,exit -F arch=b64 -S clock_settime -k time-change
 -a always,exit -F arch=b32 -S clock_settime -k time-change
 -w /etc/localtime -p wa -k time-change
```

در سیستم‌های 32بیتی، می‌بایست دستور زیر اجرا گردد و مطمئن شد که خروجی نشان داده می‌شود.

نکته: "-a always,exit" ممکن است به صورت "-a exit,always" مشخص شود.

```
change /etc/audit/audit.rules -# grep time
-a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-change
-a always,exit -F arch=b32 -S clock_settime -k time-change
-w /etc/localtime -p wa -k time-change
```

نحوه اجرای پیکربندی امن:

برای سیستم‌های 64 بیتی، می‌بایست خطوط زیر در فایل /etc/audit/audit.rules اضافه گردد.

```
-a always,exit -F arch=b64 -S adjtimex -S settimeofday -k time-change
-a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-change
-a always,exit -F arch=b64 -S clock_settime -k time-change
-a always,exit -F arch=b32 -S clock_settime -k time-change
 -w /etc/localtime -p wa -k time-change

# Execute the following command to restart auditd
-HUP auditd # pkill -P 1
```

برای سیستم‌های 32 بیتی، می‌بایست خطوط زیر در فایل /etc/audit/audit.rules اضافه گردد.

```
-a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-change
 -a always,exit -F arch=b32 -S clock_settime -k time-change
-w /etc/localtime -p wa -k time-change

# Execute the following command to restart auditd
# pkill -P 1-HUP auditd
```

6-2-5. ثبت رویدادهایی که اطلاعات کاربر/گروه را تغییر می‌دهند

بایستی رویدادهایی که بر فایل‌های passwd , group (شناسه کاربری)،shadow و gshadow (رمزعبور) یا /etc/security/opasswd (پسوردهای قدیمی بر پایه‌ی یادآوری پارامترها در تنظیمات PAM) تأثیر می‌گذارد، ثبت گردند. پارامترهای موجود در این بخش، فایل‌هایی که برای نوشتن باز می‌شوند یا مشخصات آن‌ها تغییر می‌کنند (مانند مجوزهای دسترسی) را نظارت کرده و با افزودن برچسب "identity" آن‌ها را در فایل audit log مشخص می‌کنند.

تغییرات غیرمنتظره این فایل‌ها می‌تواند نشانه این باشد که سیستم تسخیر شده و یک کاربر غیر مجاز سعی در پنهان‌کردن فعالیت‌هایش داشته و یا حساب‌های کاربری خطرناک را اضافه می‌کند.

نحوه بررسی صحت پیکربندی امن:

در صورتی‌که رویدادهایی که اطلاعات کاربر/گروه را تغییر می‌دهند ثبت شوند، دستور زیر این موضوع را مشخص می‌نماید.

```
# grep identity /etc/audit/audit.rules
-w /etc/group -p wa -k identity
-w /etc/passwd -p wa -k identity
-w /etc/gshadow -p wa -k identity
-w /etc/shadow -p wa -k identity
-w /etc/security/opasswd -p wa -k identity
```

نحوه اجرای پیکربندی امن:

خطوط زیر می‌بایست به فایل /etc/audit/audit.rules اضافه گردد.

```
-w /etc/group -p wa -k identity
-w /etc/passwd -p wa -k identity
-w /etc/gshadow -p wa -k identity
```

```
-w /etc/shadow -p wa -k identity
-w /etc/security/opasswd -p wa -k identity

# Execute the following command to restart auditd
# pkill -P 1-HUP auditd
```

6-2-6. ثبت رویدادهایی که تنظیمات شبکه سیستم را تغییر می‌دهند

بایستی تغییرات فایل‌های شبکه یا فراخوانی سیستم ذخیره شوند. پارامترهای زیر بر فراخوانی‌های سیستمی sethostname(تنظیم نام سیستم‌های میزبان) و setdomainname (تنظیم نام دامنه سیستم‌ها) نظارت می‌کنند و در هنگام خروج از فراخوان، رویداد رخ داده را ذخیره می‌کنند. دیگر پارامترها بر فایل‌های /etc/issue و /etc/issue.net (پیام‌هایی که قبل از ورود به سیستم نمایش داده می‌شوند)، /etc/hosts (فایل شامل نام میزبان و آدرس‌های IP مرتبط) و /etc/sysconfig/network (پوشه شامل اسکریپت‌های اینترفیس شبکه و تنظیمات) نظارت می‌کنند.

نظارت بر sethostname و setdomainname تغییرات غیرمجاز احتمالی در نام میزبان و نام دامنه سیستم را مشخص می‌کند. تغییرات این نام‌ها موجب بی‌اثر شدن آن دسته از پارامترهای امنیتی می‌شود که برپایه‌ی آن نام‌ها تنظیم شده‌اند.

تغییرات در فایل /etc/hosts می‌تواند نشان دهد که یک کاربر غیرمجاز تلاش می‌کند تا کاربران و پروسه‌های ماشین را فریب داده تا به ماشین‌های اشتباهی متصل شوند. نظارت بر /etc/issue و /etc/issue.net مهم است، زیرا مهاجمان می‌توانند اطلاعات گمراه‌کننده در آن فایل‌ها قرار دهند و کاربران را برای تهیه‌ی اطلاعات به سوی خود هدایت نمایند.

نظارت بر /etc/sysconfig/network نیز مهم است زیرا تغییر این فایل می‌تواند موجب تسخیر یا غیرقابل دسترس شدن ماشین گردد.

تمام رکوردهای audit شده در این بخش با برچسب "system-locale" ذخیره می‌شوند.

نحوه بررسی صحت پیکربندی امن:

در سیستم‌های 64 بیتی، می‌بایست دستور زیر اجرا شده و اطمینان حاصل گردد که خروجی نمایش داده شده مطابق آن چیزی است که در خروجی نمایش داده شده است.

نکته: "-a always,exit" ممکن است به صورت "-a exit,always" مشخص شود.

```
# grep system-locale /etc/audit/audit.rules
-a exit,always -F arch=b64 -S sethostname -S setdomainname -k system-locale
-a exit,always -F arch=b32 -S sethostname -S setdomainname -k system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/sysconfig/network -p wa -k system-locale
```

در سیستم‌های 32 بیتی، می‌بایست دستور زیر اجرا شده و اطمینان حاصل گردد که خروجی نمایش داده شده مطابق آن چیزی است که در خروجی نمایش داده شده است.

نکته: "-a always,exit" ممکن است به صورت "-a exit,always" مشخص شود.

```
# grep system-locale /etc/audit/audit.rules
-a exit,always -F arch=b32 -S sethostname -S setdomainname -k system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/sysconfig/network -p wa -k system-locale
```

نحوه اجرای پیکربندی امن:

برای سیستم‌های 64 بیتی، می‌بایست سطر زیر به فایل /etc/audit/audit.rules اضافه گردد:

```
-a exit,always -F arch=b64 -S sethostname -S setdomainname -k system-locale
-a exit,always -F arch=b32 -S sethostname -S setdomainname -k system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/sysconfig/network -p wa -k system-locale

# Execute the following command to restart auditd
# pkill -P 1-HUP auditd
```

برای سیستم‌های 32 بیتی، می‌بایست سطر زیر به فایل /etc/audit/audit.rules اضافه گردد:

```
-a exit,always -F arch=b32 -S sethostname -S setdomainname -k system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
w /etc/hosts -p wa -k system-locale -
-w /etc/sysconfig/network -p wa -k system-locale

# Execute the following command to restart auditd
# pkill -P 1-HUP auditd
```

6-2-7. ثبت رویدادهایی که سیستم کنترل دسترسی اجباری[۶۸] را تغییر می‌دهند

می‌بایست بر سیستم کنترل دسترسی اجباری SELinux نظارت گردد. پارامترهای زیر هر دسترسی نوشتنی یا تغییر مشخصات در شاخه /etc/selinux را مانیتور می‌کنند.

تغییر فایل‌ها در این پوشه می‌تواند نشان دهد که یک کاربر غیرمجاز برای تغییر کنترل‌های دسترسی تلاش می‌کند و محتواهای امنیتی را تغییر می‌دهد.

نحوه بررسی صحت پیکربندی امن:

در صورتی‌که رویدادهایی که سیستم کنترل دسترسی اجباری را تغییر می‌دهند ثبت شوند، توسط دستور زیر مشخص می‌گردد.

```
# grep MAC-policy /etc/audit/audit.rules
-w /etc/selinux/ -p wa -k MAC-policy
```

نحوه اجرای پیکربندی امن:

می‌بایست سطر زیر به فایل /etc/audit/audit.rules اضافه گردد:

```
-w /etc/selinux/ -p wa -k MAC-policy
```

اجرای دستور زیر باعث راه اندازی دوباره auditd خواهد شد:

```
# pkill -P 1-HUP auditd
```

[68] Mandatory Access Controls (MAC)

8-2-6. جمع‌آوری رویدادهای ورود و خروج به/از سیستم

بایستی بر رویدادهای ورود به سیستم و خروج از سیستم نظارت صورت گیرد. پارامترهای زیر تغییرات فایل‌های مرتبط با ورود و خروج را پیگیری می‌کنند. فایل /var/log/faillog ورود به سیستم‌های ناموفق را پیگیری می‌کند. فایل /var/log/lastlog شامل رکوردهایی می‌باشد که آخرین بار یک کاربر، موفق به ورود به سیستم گردیده است. فایل /var/log/btmp رد ورود به سیستم‌های ناموفق را نگه می‌دارد و با وارد کردن دستور /usr/bin/last -f /var/log/btmp خوانده می‌شود.

تمامی رکوردهای این بخش با برچسب "logins" ذخیره می‌شوند.

نظارت بر رویدادهای ورود و خروج می‌تواند به مدیر سیستم در تشخیص حملاتی همچون اجرای حملات brute force کمک نماید.

نحوه بررسی صحت پیکربندی امن:

در صورتی‌که رویدادهای ورود و خروج ثبت شوند، دستور زیر آن‌را مشخص می‌نماید.

```
# grep logins /etc/audit/audit.rules
-w /var/log/faillog -p wa -k logins
-w /var/log/lastlog -p wa -k logins
-w /var/log/tallylog -p wa -k logins
```

نحوه اجرای پیکربندی امن:

خطوط زیر می‌بایست به فایل /etc/audit/audit.rules اضافه گردند.

```
-w /var/log/faillog -p wa -k logins
-w /var/log/lastlog -p wa -k logins
-w /var/log/tallylog -p wa -k logins

# Execute the following command to restart auditd
# pkill -HUP -P 1 auditd
```

6-2-9. جمع‌آوری اطلاعات شروع نشست

بایستی رویدادهای شروع نشست[۶۹] نظارت گردند. پارامترهای این بخش تغییرات مربوط به فایل‌های مرتبط با رویدادهای نشست را پیگیری می‌کنند. فایل /var/run/utmp تمام کاربرانی که در حال حاضر به سیستم وارد شده‌اند را پیگیری می‌نماید.

فایل /var/log/wtmp رویدادهای ورودها، خروج‌ها، خاموش کردن و ریستارت کردن را پیگیری می‌کند.

همه‌ی رکوردهای حسابرسی با برچسب "session" ذخیره می‌شوند.

نظارت بر تغییر این فایل‌ها می‌تواند به مدیر سیستم برای ورود در زمان نامعمول هشدار دهد.

نحوه بررسی صحت پیکربندی امن:

اگر جمع‌آوری اطلاعات شروع نشست انجام گیرد، توسط دستور زیر مشخص می‌گردد.

```
# grep session /etc/audit/audit.rules
-w /var/run/utmp -p wa -k session
-w /var/log/wtmp -p wa -k session
-w /var/log/btmp -p wa -k session
```

[69] session initiation

نحوه اجرای پیکربندی امن:

می‌بایست خطوط زیر به فایل /etc/audit/audit.rules اضافه گردند:

```
-w /var/run/utmp -p wa -k session
-w /var/log/wtmp -p wa -k session
-w /var/log/btmp -p wa -k session
# Execute the following command to restart auditd
# pkill -HUP -P 1 audit
```

6-2-10. جمع‌آوری رویدادهای تغییر مجوز کنترل دسترسی اختیاری

می‌بایست بر تغییر دسترسی به فایل‌ها، ویژگی‌ها، مالکیت و گروه فایل نظارت صورت پذیرد. پارامترهای بیان شده در این بخش، بر فراخوانی‌های سیستمی که بر روی دسترسی‌ها و ویژگی‌های فایل تاثیر می‌گذارند نظارت می‌کنند. فراخوانی‌های سیستمی chmod , fchmod و fchmodat بر روی سطح دسترسی یک فایل تأثیر می‌گذارند. فراخوانی‌های سیستمی Chown , fchown , fchownat و lchown روی مالکیت و گروه فایل تأثیر می‌گذارند. Setxattr , lsetxattr , fsetxattr (تنظیم ویژگی‌های فایل گسترش یافته) و , removexattr lremovexattr , fremovexattr (حذف ویژگی‌های فایل گسترش یافته) ویژگی‌های فایل گسترش‌یافته را کنترل می‌کنند. در همه موارد، رکورد حسابرسی فقط برای کاربران غیرسیستمی (auid>=1000) نوشته می‌شود و رویدادهای دایمون نادیده گرفته می‌شوند (auid=4294967295).

همه‌ی رکوردهای حسابرسی مربوط به این بخش با برچسب "perm_mod" ذخیره می‌شوند.

نظارت بر تغییر این فایل‌ها می‌تواند به مدیر سیستم درباره فعالیت‌های افراد مهاجم یا مموارد نقض سیاست هشدار دهد.

نحوه بررسی صحت پیکربندی امن:

در سیستم‌های 64 بیتی، می‌بایست دستور زیر اجرا گردد و به‌وسیله خروجی نمایش داده شده اطمینان حاصل گردد که تغییرات سطح دسترسی ثبت می‌شوند.

نکته: "-a always,exit" ممکن است به صورت "-a exit,always" مشخص شود.

```
# grep perm mod /etc/audit/audit.rules
-a always,exit -F arch=b64 -S chmod -S fchmod -S fchmodat -F auid>=1000 \
-F auid!=4294967295 -k perm mod
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 \
-F auid!=4294967295 -k perm mod
-a always,exit -F arch=b64 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 \
-F auid!=4294967295 -k perm mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 \
-F auid!=4294967295 -k perm mod
-a always,exit -F arch=b64 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S \
lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S \
lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm mod
```

در سیستم‌های 32 بیتی، می‌بایست دستور زیر اجرا گردد و به‌وسیله خروجی نمایش داده شده اطمینان حاصل گردد که تغییرات سطح دسترسی ثبت می‌شوند.

نکته: "-a always,exit" ممکن است به صورت "-a exit,always" مشخص شود.

```
# grep perm_mod /etc/audit/audit.rules
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 \
-F auid!=4294967295 -k perm mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 \
-F auid!=4294967295 -k perm mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S \ lremovexattr -S
fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod
```

نحوه اجرای پیکربندی امن:

برای سیستم‌های 64 بیتی، می‌بایست خطوط زیر به فایل /etc/audit/audit.rules اضافه گردد:

```
-a always,exit -F arch=b64 -S chmod -S fchmod -S fchmodat -F auid>=1000 \
-F auid!=4294967295 -k perm mod
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 \
-F auid!=4294967295 -k perm mod
-a always,exit -F arch=b64 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 \
-F auid!=4294967295 -k perm mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 \
-F auid!=4294967295 -k perm mod
-a always,exit -F arch=b64 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S \
lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S \
 lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm mod

# Execute the following command to restart auditd
# pkill -HUP -P 1 auditd
```

برای سیستم‌های 32 بیتی، می‌بایست خطوط زیر به فایل /etc/audit/audit.rules اضافه گردند:

```
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 \
-F auid!=4294967295 -k perm mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 \
-F auid!=4294967295 -k perm mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S \
 lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod
# Execute the following command to restart auditd
 # pkill -HUP -P 1 auditd
```

6-2-11. جمع‌آوری دسترسی غیرمجاز ناموفق به فایل‌ها

می‌بایست بر تلاش‌های غیرمجاز ناموفق برای دسترسی به فایل‌ها نظارت انجام گیرد. پارامترهای زیر با فراخوانی‌های سیستمی که ساختن (creat)، بازکردن (open,openat) و جابجا کردن (truncate,ftruncate) فایل‌ها را کنترل می‌کنند، در ارتباط هستند. یک رکورد log حسابرسی فقط هنگامی ثبت می‌گردد که کاربر

ممتاز نبوده (auid>=1000) یا یک رویداد دایمون نباشد (auid=4294967295) یا جواب فراخوانی از سیستم یکی از حالات EAACCES (عدم اجازه دسترسی به فایل) یا EPERM (بعضی دیگر از خطاهای دائمی مرتبط با فراخوانی‌های سیستمی خاص) نباشد.

همه‌ی رکوردهای حسابرسی فوق با برچسب "access" ذخیره می‌شوند.

عدم موفقیت در تلاش برای باز کردن، ساختن یا جابجا کردن فایل‌ها می‌تواند نشانه‌ای باشد که شخص یا فرآیندی تلاش برای دسترسی غیرمجاز به فایل داشته است.

نحوه بررسی صحت پیکربندی امن:

در سیستم‌های 64 بیتی، می‌بایست دستور زیر اجرا گردد و توسط خروجی نمایش داده شده اطمینان حاصل گردد که تلاش‌های ناموفق برای دسترسی به فایل‌ها جمع‌آوری می‌شود.

نکته: "-a always,exit" ممکن است به صورت "-a exit,always" مشخص شود.

```
# grep access /etc/audit/audit.rules
-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S ftruncate \
-F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate \
-F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S ftruncate \
-F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate \
-F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access
```

در سیستم‌های 32 بیتی، می‌بایست دستور زیر اجرا گردد و توسط خروجی نمایش داده شده اطمینان حاصل گردد که تلاش‌های ناموفق برای دسترسی به فایل‌ها جمع‌آوری می‌شود.

نکته: "-a always,exit" ممکن است به صورت "-a exit,always" مشخص شود.

```
# grep access /etc/audit/audit.rules
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate \
-F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate \
-F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access
```

نحوه اجرای پیکربندی امن:

در سیستم‌های 64 بیتی، می‌بایست خطوط زیر به فایل /etc/audit/audit.rules اضافه گردد.

```
-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S ftruncate \
-F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate \
-F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S ftruncate \
-F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate \
-F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access
 # Execute the following command to restart auditd
# pkill -HUP -P 1 auditd
```

در سیستم‌های 32 بیتی، می‌بایست خطوط زیر به فایل /etc/audit/audit.rules اضافه گردند.

```
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate \
-F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate \
-F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access
 # Execute the following command to restart auditd
# pkill -HUP -P 1 auditd
```

6-2-12. جمع‌آوری دستورهای ممتاز مورد استفاده

می‌بایست برنامه‌های ممتاز مانیتور گردند (آن‌هایی که بیت setuid یا setgid آن‌ها در هنگام اجرا ست شده است) و در صورتی‌که یک کاربر غیرممتاز این دستورها را اجرا نموده است، اطلاع داده شود.

اجرای دستورات ممتاز توسط کاربران غیر ممتاز می‌تواند نشانه این باشد که شخصی سعی در دسترسی غیرمجاز به سیستم دارد.

نحوه بررسی صحت پیکربندی امن:

بایستی بررسی کرد که یک سطر حسابرسی برای هر برنامه setuid/setgid در دستور find مشخص شده است که دارای ویژگی‌های بیان شده است.

نحوه اجرای پیکربندی امن:

برای حل این مشکل، مدیر سیستم بایستی یک دستور جستجو برای پیدا نمودن برنامه‌های ممتاز اجرا کند و سپس یک سطر حسابرسی برای هرکدام از آن‌ها اضافه نماید. پارامترهای حسابرسی مرتبط عبارتند از:

- -F path=" $1 " : هر نام فایل که از طریق دستور find گذاشته می‌شود و با awkپردازش می‌شود.
- -F perm=x : اگر فایل اجرا شده باشد، یک رکورد حسابرسی نوشته می‌شود.
- -F auid>=1000 : اگر کاربر غیر ممتازی دستوری را اجرا کند، یک رکورد نوشته می‌شود.
- -F auid!= 4294967295 : رویدادهای دایمون را نادیده می‌گیرد.

همه ی رکوردهای حسابرسی با برچسب "privileged" ذخیره می‌شوند.

```
# find PART -xdev \( -perm -4000 -o -perm -2000 \) -type f | awk '{print \
"-a always,exit -F path=" $1 " -F perm=x -F auid>=500 -F auid!=4294967295 \
-k privileged" }'
```

سپس این خطوط می‌بایست به فایل /etc/audit/audit.rules اضافه گردند.

6-2-13. جمع‌آوری mountهای موفق فایل سیستم‌ها

می‌بایست استفاده از فراخوان‌های سیستمیmount مانیتور گردند. فراخوان‌های سیستمی mount و unmount، سوار شدن و پیاده شدن فایل سیستم‌ها را کنترل می‌کنند. پارامترهای زیر، زمانی‌که فراخوان‌های سیستمی mount به‌وسیله کاربران غیرممتاز استفاده می‌شود، یک رکورد حسابرسی ثبت می‌کنند.

اکثر مواقع mount نمودن فایل‌سیستم‌ها توسط کاربر غیرممتاز، غیر معمول است. هرچند که پیگیری دستور mount به مدیر سیستم نشان می‌دهد که مدیایی خارجی ممکن است mount شده باشد، اما دقیقاً داده‌هایی که به مدیا صادر[70] شده است را نشان نمی‌دهد. مدیران سیستم مایل هستند بدانند که آیا داده‌ای به مدیا صادر شده است یا خیر. فراخوانی‌های سیستمی open ,create و truncate نیاز به دسترسی نوشتنی به فایل مدیا خارجی دارند. این امر می‌تواند نشانه خوبی باشد که عمل نوشتن اتفاق افتاده است. تنها راهی که می‌تواند واقعاً این موضوع را به اثبات برساند این است که عملیات نوشتن روی مدیای خارجی موفقیت‌آمیز باشد. ثبت فراخوان‌های سیستمی نوشتن می‌تواند سریعاً audit log را پر کند و به‌طور کلی این امر پیشنهاد نمی‌گردد. توصیه‌هایی برای پیکربندی گزینه‌های ثبت موفقیت‌آمیز بودن صدور داده به مدیا وجود دارد که از هدف این توصیه‌نامه خارج است.

نحوه بررسی صحت پیکربندی امن:

برای سیستم‌های 64 بیتی، می‌بایست دستور زیر اجرا گردد و توسط خروجی که نشان داده می‌شود اطمینان حاصل گردد که mount فایل‌سیستم‌ها ثبت می‌گردد.

[70] Export

نکته: "-a always,exit" ممکن است به صورت "-a exit,always" مشخص شود.

```
# grep mounts /etc/audit/audit.rules
-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=4294967295 -k mounts
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=4294967295 -k mounts
```

برای سیستم‌های 32 بیتی، می‌بایست دستور زیر اجرا گردد و توسط خروجی که نشان داده می‌شود اطمینان حاصل گردد، آیا mount فایل‌سیستم‌ها ثبت می‌شوند یا خیر.

نکته: "-a always,exit" ممکن است به صورت "-a exit,always" مشخص شود.

```
# grep mounts /etc/audit/audit.rules
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=4294967295 -k mounts
```

نحوه اجرای پیکربندی امن:

در سیستم‌های 64 بیتی می‌بایست سطر زیر به فایل /etc/audit/audit.rules اضافه گردد.

```
-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=4294967295 -k mounts
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=4294967295 -k mounts
# Execute the following command to restart auditd
# pkill -HUP -P 1 auditd
```

در سیستم‌های 32 بیتی می‌بایست سطر زیر به فایل /etc/audit/audit.rules اضافه گردد.

```
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=4294967295 -k mounts
# Execute the following command to restart auditd
# pkill -HUP -P 1 auditd
```

6-2-14. جمع‌آوری رویدادهای حذف فایل توسط کاربر

می‌بایست فراخوان‌های مرتبط با حذف یا تغییر نام فایل‌ها یا تغییر ویژگی فایل‌ها مانیتور گردند. این تنظیمات فراخوان‌های سیستمی unlink (حذف یک فایل) ، unlinkat (حذف ویژگی یک فایل)، rename (تغییر نام یک فایل) و renameat (تغییر نام یک ویژگی فایل) را مانیتور کرده و آن‌ها را با برچسب "delete" ذخیره می‌کنند.

مانیتورکردن این فراخوانی‌ها توسط کاربران غیرممتاز می‌تواند برای مدیر سیستم نشانه‌ای باشد که فایلی حذف و یا تغییراتی در فایل‌های محافظت شده اتفاق افتاده است.

نحوه بررسی صحت پیکربندی امن:

برای سیستم‌های 64 بیتی، می‌بایست دستور زیر اجرا گردد و توسط خروجی که نشان داده می‌شود اطمینان حاصل گردد که اگر فایلی توسط کاربر حذف می‌شود، در سیستم ثبت می‌گردد.

```
# grep delete /etc/audit/audit.rules
-a always,exit -F arch=b64 -S unlink -S unlinkat -S rename -S renameat -F auid>=1000 \
-F auid!=4294967295 -k delete
-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F auid>=1000 \
-F auid!=4294967295 -k delete
```

برای سیستم‌های 32 بیتی، می‌بایست دستور زیر اجرا گردد و توسط خروجی که نشان داده می‌شود اطمینان حاصل گردد که اگر فایلی توسط کاربر حذف گردد، در سیستم ثبت می‌شود.

```
# grep delete /etc/audit/audit.rules
-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F auid>=1000 \
-F auid!=4294967295 -k delete
```

نحوه اجرای پیکربندی امن:

حداقل بایستی پیکربندی سیستم حسابرسی به‌گونه‌ای باشد که رویدادهای حذف شدن فایل توسط کلیه کاربران از جمله کاربر ریشه ثبت گردد.

در سیستم‌های 64 بیتی می‌بایست متن زیر به فایل /etc/audit/audit.rules اضافه گردد.

```
-a always,exit -F arch=b64 -S unlink -S unlinkat -S rename -S renameat -F auid>=1000 \
-F auid!=4294967295 -k delete
-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F auid>=1000 \
-F auid!=4294967295 -k delete
# Execute the following command to restart auditd
# pkill -HUP -P 1 auditd
```

در سیستم‌های 32 بیتی می‌بایست متن زیر به فایل /etc/audit/audit.rules اضافه گردد.

```
-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F auid>=1000 \
-F auid!=4294967295 -k delete
# Execute the following command to restart auditd
# pkill -P 1-HUP auditd
```

6-2-15. جمع‌آوری تغییرات در حوزه مدیریت سیستم

می‌بایست تغییرات حوزه مدیریت سیستم مانیتور گردد. اگر سیستم به‌طور صحیح پیکربندی شده باشد، مدیران سیستم اول وارد سیستم شده و بعد از دستور sudo برای دسترسی ممتاز استفاده می‌کنند. در این حالت امکان مانیتور کردن تغییرات در حوزه مدیریت وجود دارد.

زمانی‌که فایل یا ویژگی‌های آن تغییر یابد، در فایل /etc/sudoers نوشته می‌شود. رکوردهای حسابرسی این بخش با برچسب "scope" ذخیره می‌شوند.

تغییر در فایل /etc/sudoers می‌تواند نشان دهد که حوزه فعالیت مدیریت سیستم تغییر نموده است.

نحوه بررسی صحت پیکربندی امن:

با اجرای دستور زیر مشخص می‌گردد که تغییرات در /etc/sudoers ذخیره می‌گردد.

```
# grep scope /etc/audit/audit.rules
-w /etc/sudoers -p wa -k scope
```

نحوه اجرای پیکربندی امن:

خطوط زیر می‌بایست به فایل /etc/audit/audit.rules اضافه گردند.

```
-w /etc/sudoers -p wa -k scope
# Execute the following command to restart auditd
# pkill -HUP -P 1 auditd
```

6-2-16. جمع‌آوری فعالیت‌های مدیر سیستم (sudolog)

می‌بایست فایل ثبت وقایع sudo مانیتور گردد. اگر سیستم درست پیکربندی شده باشد و استفاده از دستور su غیرفعال شده باشد، همه‌ی مدیران سیستم مجبور می‌شوند که اول وارد شوند و سپس از sudo برای اجرای دستورات ممتاز استفاده کنند. درنتیجه همه‌ی دستورات مدیران در /var/log/sudo.log ثبت می‌شود. هر زمانی‌که یک دستور اجرا می‌شود، یک رویداد حسابرسی در فایل /var/log/sudo.log نوشته می‌شود.

تغییر در فایل /var/log/sudo.log نشان می‌دهد که مدیر سیستم یک دستور اجرا کرده یا فایل log خودش دستکاری شده است. مدیر می‌تواند رویدادهای نوشته شده در دنباله حسابرسی را با رکورد نوشته شده در /var/log/sudo.log بررسی نموده و به اجرا شدن دستورهای غیرمجاز پی برد.

نحوه بررسی صحت پیکربندی امن:

با دستور زیر مشخص می‌گردد که آیا فعالیت‌های مدیر ثبت می‌شوند یا خیر.

```
# grep actions /etc/audit/audit.rules
-w /var/log/sudo.log -p wa -k actions
```

نحوه اجرای پیکربندی امن:

می‌بایست خطوط زیر به فایل /etc/audit/audit.rules اضافه گردند.

```
-w /var/log/sudo.log -p wa -k actions
# Execute the following command to restart auditd
# pkill -HUP -P 1 auditd
```

6-2-17. جمع‌آوری بارگذاری[71] و تخلیه[72] ماژول هسته

بارگذاری و تخلیه ماژول هسته می‌بایست مانیتور گردد. برنامه‌های insmod (نصب یک ماژول هسته)، rmmod (حذف یک ماژول هسته) و modprobe (یک برنامه پیچیده‌تر برای بارگذاری و تخلیه ماژول‌ها و بعضی ویژگی‌های دیگر)، بارگذاری و تخلیه ماژول‌ها را کنترل می‌کنند. فراخوان‌های سیستمی Init_module (بارگذاری یک ماژول) و delete_module (حذف یک ماژول) بارگذاری و تخلیه ماژول‌ها را کنترل می‌کنند.

تمامی اجراهای برنامه یا فراخوانی سیستمی از بارگذاری و تخلیه ماژول یک رکورد حسابرسی با برچسب"modules" ذخیره می‌کند.

مانیتور کردن insmod، rmmod و modprobe مورد استفاده می‌تواند برای مدیر سیستم نشانه‌ای باشد که کاربران غیرمجاز یک ماژول هسته را بارگذاری یا تخلیه کرده‌اند و امکان به خطر افتادن امنیت سیستم وجود دارد. نظارت بر فراخوان‌های سیستمی init_module و delete_module نشانه‌ای از آن است که یک کاربر غیر مجاز تلاش به استفاده از یک برنامه متفاوت برای بارگذاری و تخلیه ماژول دارد.

نحوه بررسی صحت پیکربندی امن:

اجرای دستور زیر مشخص می‌کند که آیا بارگذاری و تخلیه ماژول هسته ثبت می‌شود یا خیر.

نکته: "-a always,exit" ممکن است به صورت "-a exit,always" مشخص شود.

```
# grep modules /etc/audit/audit.rules
-w /sbin/insmod -p x -k modules
-w /sbin/rmmod -p x -k modules
-w /sbin/modprobe -p x -k modules
```

[71] Loading
[72] Unloading

```
For 32 bit systems
-a always,exit -F arch=b32 -S init_module -S delete_module -k modules
For 64 bit systems
-a always,exit -F arch=b64 -S init_module -S delete_module -k modules
```

نحوه اجرای پیکربندی امن:

خطوط زیر را می‌بایست به فایل /etc/audit/audit.rules اضافه گردد.

```
-w /sbin/insmod -p x -k modules
-w /sbin/rmmod -p x -k modules
-w /sbin/modprobe -p x -k modules
For 32 bit systems, add
-a always,exit -F arch=b32 -S init_module -S delete_module -k modules
For 64 bit systems, add
-a always,exit -F arch=b64 -S init_module -S delete_module -k modules
```

6-2-18. تغییرناپذیر نمودن پیکربندی audit

بایستی سیستم حسابرسی طوری پیکربندی شود که نتوان قوانین حسابرسی را با auditctl تغییر داد. تنظیم پرچم "2 e-" حسابرس را مجبور می‌کند که به حالت تغییرناپذیر برود. تغییر audit تنها می‌تواند در هنگام راه‌اندازی مجدد سیستم اعمال گردد.

در حالت غیرقابل تغییر، کاربران غیرمجاز نمی‌توانند با استفاده از auditctl تغییراتی در سیستم حسابرسی اعمال نموده و فعالیت‌های مخرب خود را پنهان نمایند.

در حالت غیرقابل تغییر، تغییر پیکربندی با بازنشانی سیستم همراه است و درنتیجه مدیران سیستم به احتمال زیاد متوجه ریبوت شدن سیستم می‌شوند.

نحوه بررسی صحت پیکربندی امن:

اجرای دستور زیرمشخص می‌کند که آیا تنظیمات audit تغییرناپذیر است یا خیر.

```
# grep "^-e 2" /etc/audit/audit.rules
-e 2
```

نحوه اجرای پیکربندی امن:

سطر زیر می‌بایست به فایل /etc/audit/audit.rules اضافه گردد.

```
-e 2
```

نکته: این سطر باید آخرین سطر در فایل /etc/audit/audit.rules/ باشد.

3-6. پیکربندی logrotate

سیستم با قابلیت rotating log فایل‌ها، به طور مرتب از پر شدن سیستم با logها یا ساختن logهای غیرقابل مدیریت بزرگ جلوگیری می‌کند. فایل /etc/logrotate.d/syslog ، فایل پیکربندی برای فایل‌های rotate logاست و به وسیله rsyslog یا syslog ساخته می‌شود. این فایل‌ها به صورت هفتگی با برنامه cron، rotate می‌شوند و حداکثر تا چهار هفته نگهداری می‌شوند.

با کوچک و قابل مدیریت نگه داشتن فایل‌های log، یک مدیر سیستم می‌تواند به سادگی این فایل‌ها را در سیستم‌های دیگر آرشیو کند و زمان کمتری نسبت به فایل‌های بزرگ صرف می‌کند.

نحوه بررسی صحت پیکربندی امن:

با دستور زیر مشخص می‌گردد که توانایی logrotate به صورت مناسب پیکربندی شده است یا خیر.

```
# grep '{' /etc/logrotate.d/syslog
/var/log/messages /var/log/secure /var/log/maillog /var/log/spooler /var/log/boot.log /var/log/cron {
```

نحوه اجرای پیکربندی امن:

می‌بایست فایل /etc/logrotate.d/syslog جهت داشتن سیستم log مناسب ویرایش گردد.

```
/var/log/messages /var/log/secure /var/log/maillog /var/log/spooler /var/log/boot.log /var/log/cron {
```