بسمه تعالی

امن‌سازی پایه زیرساخت شبکه

بخش دوم: مدیریت دسترسی

همگان بر این باورند که امن‌سازی تجهیزات زیرساخت شبکه شامل مسیریاب‌ها، سوییچ‌ها، سرورها و دیگر تجهیزات زیرساخت یکی از مؤلفه‌های کلیدی برای تامین امنیت کل شبکه محسوب می‌شود. یکی از مهمترین بخش‌های تامین چنین امنیتی، امنیت مدیریت دسترسی به این تجهیزات می‌باشد. اگر دسترسی به تجهیزات زیرساخت از کنترل خارج شود و به خطر بیافتد، دراین صورت مدیریت کل شبکه می تواند در خطر افتد. در نتیجه برقراری کنترل‌های مناسب برای جلوگیری از دسترسی‌های غیر مجاز به تجهیزات زیرساخت شبکه بسیار حساس می‌باشد.

برای دسترسی به تجهیزات زیرساخت شبکه می‌توان از روش‌های مختلفی از جمله استفاده از کنسول و ارتباطات غیر سنکرون و همچنین دسترسی از راه دور از طریق telnet، rlogin، http و ssh استفاده کرد.

برای برخی مکانیزم‌های دسترسی که به طور پیش‌فرض فعال هستند، حداقل امنیت در نظر گرفته شده است. برای مثال در پلتفرم‌های مبتنی بر نرم‌افزار IOS سیسکو، دسترسی از طریق کنسول و مودم به طور پیش‌فرض فعال است. به همین دلیل هر تجهیز موجود در زیرساخت باید به طور دقیق راه‌اندازی و پیکربندی شود و فقط مکانیزم‌های دسترسی پشتیبانی‌شده روی آن‌ها فعال و به طور کامل امن‌سازی شده باشد.

گام های کلیدی به منظور تامین امنیت دسترسی‌های تعاملی و مدیریتی به یک تجهیز زیرساخت به‌صورت زیر قابل بیان است:

- محدود کردن دسترسی به تجهیز: محدود کردن دسترسی به پورت ها، منحصر کردن افراد مجاز و محدود ساختن روش‌های دسترسی مجاز
- ارائه اخطارهای مناسب
- اعتبارسنجی دسترسی: اطمینان از اینکه دسترسی به افراد، گروه‌ها و سرویس‌های احراز اصالت شده اعطا شود.

- فعالیت‌های مجاز : محدود کردن فعالیت‌های مجاز قابل انجام توسط کاربران، گروه‌ها و سرویس‌های مشخص
- اطمینان از حفظ محرمانگی داده ها: حفاظت از داده های حساس که به صورت محلی ذخیره شده‌اند (عدم توانایی مشاهده و کپی آن‌ها). این داده های حساس در حین تبادل از طریق کانال ارتباطی ممکن است در معرض حملاتی همچون sniffing، session hijacking و MITM[1] قرار گیرند.
- ثبت وقایع و حساب‌ها برای همه دسترسی‌ها: ثبت این که چه کسی، چه موقع به تجهیز دسترسی داشته و چه فعالیتی انجام داده است.

توجه: به منظور بررسی دسترسی‌ها و تعیین هرگونه دسترسی غیرمجاز، بایستی وقایع ثبت شده به طور مرتب بازبینی شوند.

مدیریت دسترسی از دید متدولوژی CSF[2]

خلاصه نتایج به دست آمده از اعمال CSF در حوزه امنیت دسترسی به تجهیزات زیرساخت شبکه در جدول زیر نمایش داده شده است.

جدول ۱- مدیریت دسترسی از دید متودولوژی CSF

➢ AAA Enforcement • Centralized AAA and local fallback • Administrator access • Privileged level access ➢ SNMP Accounts • Community strings or auth/privacy policy ➢ AAA server definitions ➢ Device Management Best Common Practices • Strong password policy • Per-user accounts • Remove default accounts and passwords	➢ Logging • Syslog • SNMP • AAA Server Based Accounting • Configuration change notification and logging

[1] man in the middle
[2] Cisco Security Framework

محدودکردن امکان مدیریت تجهیزات موجود در زیرساخت

اولین قدم برای امن‌سازی دسترسی به تجهیزات موجود در زیرساخت، محدود کردن امکان دسترسی بـه آن-هاست.

موارد قابل توجه در این زمینه در ادامه بیان شده‌اند:

- محدودکردن دسترسی تنها به ترمینال‌ها و پورت‌های مدیریتی مجاز
- محدودکردن دسترسی تنها به سرویس‌ها و پروتکل‌های دارای مجوز
- محدودکردن دسترسی تنها به سرویس‌ها و پروتکل‌های مجاز
- محدودکردن تعداد دفعات دسترسی به سرویس‌های مجاز توسط کاربران مجاز
- اعطای مجوز دسترسی تنها به کاربران احراز اصالت شده
- اعطای کمترین سطح دسترسی به کاربران مجاز
- اجبار مدیریت نشست[۳]
- محدودکردن آسیب‌پذیری‌ها به حملات دیکشنری و DOS

ایده کلی برای مدیریت دسترسی آن است که امکان دسترسی به تجهیزات به صورت پیش فرض نباید فراهم شود، مگر برای آن دسته از کاربران و سرویس‌ها که نیاز آن‌ها کاملاً ضروری است.

[3] session management

توجه: اکثر تجهیزات موجود در زیرساخت، از طریق چندین ترمینال و پورت مدیریتی، چندین سرویس و پروتکل گوناگون (که برخی از آن ها بصورت پیش فرض فعال هستند) قابلیت دسترسی دارند. بنابراین همه مکانیزم‌های مدیریت دسترسی ممکن باید بررسی و امن‌سازی شوند.

پایانه‌ها و خطوط دسترسی تجهیزات سیسکو

تجهیزات سیسکو معمولاً از طریق خطوط و پورت‌های زیر قابل دسترسی هستند:

- خطوط TTY: پورت‌های غیر سنکرون شامل:
  - AUX
  - کنسول
- خطوط VTY: خطوط TTY مجازی برای دسترسی از راه دور استفاده می‌شوند مانند :
  - Telnet
  - SSH
  - rlogin

توجه: دسترسی گرافیکی از طریق وب و دسترسی SNMP در بخش‌های بعدی توضیح داده خواهد شد.

پورت AUX

این پورت برای اتصال به یک مودم خارجی استفاده می‌شود. دسترسی از طریق پورت AUX به طور عادی برای دسترسی dial-in وdial-out به دستگاه مورد استفاده قرار می گیرد. در صورتی که این پورت نیاز نباشد، باید غیرفعال گردد تا احتمال دسترسی‌های غیرمجاز کاهش یابد.

پورت کنسول

دسترسی از طریق پورت کنسول به طور مستقیم برای کاربران محلی قابل دسترسی است و دسترسی از راه دور از طریق استفاده از ترمینال و سرور کنسول قابل انجام است. اگر دسترسی از طریق پورت کنسول درخواست شده باشد، خط ارتباطی باید به منظور محافظت در برابر دسترسی‌های غیر مجاز ایمن شود.

خط VTY

دسترسی از طریق خط VTY معمول‌ترین روش برای مدیریت از راه دور یک تجهیز است. اگر دسترسی VTY نیاز باشد، خطوط باید به طور مناسب برای جلوگیری از دسترسی غیر مجاز امن شوند.

توجه: هر مسیریاب به طور معمول شامل ۵ خط (از ۰ تا ۴) است. البته ممکن است تعداد بیشتری را نیز پشتیبانی نماید. نکته قابل توجه این است که تمامی این خطوط باید به طور دقیق امن‌سازی شده باشند.

غیر فعال‌کردن پورت‌ها و ترمینال‌های دسترسی غیرضروری تجهیزات

برخی از پورت‌ها و ترمینال‌های تجهیزات زیرساخت شبکه به صورت پیش فرض فعال در نظر گرفته شده‌اند. این مسئله یک تهدید امنیتی محسوب می‌شود. بدین منظور پیشنهاد می‌گردد تمامی ترمینال‌ها، پورت‌ها و اینترفیس‌هایی که مورد نیاز نیستند، غیرفعال شوند.

در تجهیزات Cisco ترمینال و پورت‌های مدیریتی به طور معمول شامل خطوط TTY و VTY هستند. این پورت‌ها همانطور که در زیر نشان داده شده است، با استفاده از دستور no exec غیر فعال می‌شود:

```
! Disable access to VTY
line vty 1
login
no exec
!
! Disable access to Console
line con 0
no exec
```

محدود ساختن دسترسی تجهیزات، تنها به سرویس‌ها و پروتکل‌های مجاز

در برخی از تجهیزات زیرساخت شبکه، سرویس‌ها و پروتکل‌هایی برای دسترسی به مدیریت تجهیز به صورت پیش‌فرض فعال است. در این حالت شبکه با ریسک‌های امنیتی مختلفی مواجه می‌باشد. بدین منظور توصیه می‌شود سرویس‌ها و پروتکل‌هایی که مورد نیاز نیستند، غیرفعال گردند.

سرویس‌ها و پروتکل‌های دسترسی در تجهیزات Cisco عبارتند از:

- Telnet , SSH و ...
- HTTP , HTTPS
- SNMP

دسترسی تعاملی از طریق خطوط TTY و VTY در تجهیزات Cisco باید تنها برای سرویس‌ها و پروتکل‌های مورد نیاز و دارای مجوز فراهم شده باشد. این محدودیت باید بر روی هر دو نوع ارتباطات درونی و بیرونی لحاظ گردد. این کار بر روی خطوط TTYو VTY با استفاده از دستور transport اجرا می‌گردد. در جدول زیر چند مثال در این مورد ارائه شده است.

جدول ۲- مثال‌هایی از محدود کردن ارتباطات ورودی و خروجی

transport input none	هیچ ارتباط ورودی وجود ندارد.
transport output none	هیچ ارتباط خروجی وجود ندارد.
transport input ssh	فقط به SSH برای برقراری ارتباط ورودی اجازه داده می‌شود.
transport input telnet	فقط به telnet برای برقراری ارتباط ورودی اجازه داده می‌شود.
transport input telnet ssh	به SSH و telnet برای برقراری ارتباط ورودی اجازه داده می‌شود.
transport output ssh	فقط به SSH برای برقراری ارتباط خروجی اجازه داده می‌شود.
transport preferred none	پروتکل لایه انتقال باید در بسته درخواست دسترسی مشخص شده باشد.

در بین پروتکل‌های دسترسی، توصیه می‌شود از پروتکل‌های دسترسی رمزشده مانند SSH استفاده شود.

محدود کردن دسترسی به سرویس‌ها تنها توسط افراد مجاز

تنها افراد مجاز باید توانایی دسترسی به تجهیزات و سرویس‌هایی که استفاده از آن‌ها برایشان مجاز در نظرگرفته شده است را داشته باشند. در این صورت می‌توان اطمینان داشت که درخواست‌های دسترسی تنها به سرویس‌های دارای مجوز صورت می‌گیرد و توسط منابع با آدرس IP معتبر امکان دسترسی خواهند داشت. در این صورت ریسک دسترسی غیرمجاز و حملات مرتبط با آن بسیار کاهش می‌یابد. نمونه‌هایی از این حملات می‌تواند شامل حملات brute force، DOS وdictionary باشد.

در تجهیزات سیسکو، از ACL های نوع استاندارد می توان برای محدود کردن دسترسی به تجهیزات مدیریتی استفاده کرد و در این حالت دسترسی تنها برای افراد مجاز امکان پذیر است. همچنین ACL های نوع extended برای محدود کردن دسترسی به سرویس‌های مجاز می‌تواند استفاده شود.

بدیهی است که هرچه محدودیت بیشتری توسط ACL ها ایجاد شود، در این حالت محدودیت‌های بیشتری برای دسترسی به صورت غیرمجاز خواهد بود. با این وجود هرچه محدودیت‌های تعیین شده توسط ACL بیشتر باشد، باعث ایجاد سربار در شبکه می‌شود و می‌تواند دسترسی به شبکه را تحت‌الشعاع قرار دهد. به عنوان نمونه اگر یک محدودیت خاص برای یک سیستم تعریف شده باشد، مثلاً برای یکی از سیستم‌های NOC، و ارتباط شبکه برای آن محدوده خاص قطع شده باشد، این امر می‌تواند قابلیت دسترسی مدیر شبکه به آن سیستم به منظور عیب‌یابی را کاهش دهد. به همین دلیل باید یک تعادل بین تعریف محدودیت‌ها و دسترسی‌پذیری به شبکه در نظر گرفته شود. یکی از مواردی که باید تعریف شود اعمال محدودیت دسترسی تنها به آدرسIP های داخلی است.

ACL های نوع استاندارد

ACL های نوع استاندارد می‌توانند براساس آدرس IP مبدأ (ویا یک رنج از آدرس IP های مبدأ) محدودیت ایجاد کنند.

```
access-list 10 permit <NOCsubnet> <inverse-mask>
access-list 10 deny any any
```

ACL های نوع extended

این ACL ها توانایی ایجاد محدودیت بر اساس آدرس‌های IP مبدأ وپروتکل مورد نظر را دارا می‌باشند:

```
access-list <xACL#> permit tcp <NOCsubnet1> <inverse-mask> any eq <TCP port>
access-list <xACL#> permit tcp <NOCsubnet2> <inverse-mask> any eq <TCP port>
access-list <xACL#> deny ip any any log-input
```

البته رعایت ترتیب تنظیمات موجود در ACL الزامی است. چون تنظیمات نوشته شده در ACL خط به خط و به همان ترتیب اجرا می‌شوند. در مثال زیر، چگونگی اعمال یک ACL بر روی خطوط VTY بیان شده است:

```
line vty 0 4
access-class <ACL#> in
```

توجه: می توان از ACL برای خطوط VTY استفاده کرد که در این صورت می‌تواند از دسترسی به خطوط VTY در حین حمله DOS جلوگیری کند.

احراز اصالت با استفاده از AAA

دسترسی به تمام پورت‌های تجهیزات موجود در زیرساخت باید احراز اصالت شوند. این کار منجر به محدودیت دسترسی تنها برای کاربران مجاز خواهد شد. توصیه می‌شود که یک سرور AAA به منظور احرازاصالت کلیه کاربران به صورت مجزا درنظر گرفته شود. این عمل بر روی تمام پورت‌ها و ترمینال‌های تجهیزات قابل اعمال است.

در سیستم‌عامل نرم‌افزاری سیسکو، دسترسی با سطح مدیر شبکه به تجهیزات به عنوان نشست EXEC عنوان می‌شود و از طریق خطوط VTY یا TTY انجام می‌شود. احراز اصالت این نشست‌ها[۴] بر مبنای AAA و با اعمال تنظیمات مشخص بر روی خطوط TTY و VTY انجام می‌شود.

در زیر نمونه‌ای از اعمال تنظیمات احراز اصالت AAA برای نشست EXEC بر روی خطوط کنسول و VTY نشان داده شده است:

```
aaa authentication login adminAuthen-list group adminAAAgroup local-case
!
line con 0
login authentication adminAuthen-list
!
line vty 0 4
login authentication adminAuthen-list
```

[4] sessions

اجرای بررسی مجوزهای ورود به دستگاه با استفاده از AAA

در ابتدای کار بایستی کمترین سطح دسترسی برای کاربران احراز اصالت شده با توجه به نیازمندی‌های آن‌ها در نظر گرفته شود. در تجهیزات سیسکو قابلیت کنترل دسترسی کاربران احراز اصالت شده به محیط CLI با استفاده از دستور aaa authorization exec قابل انجام است. با استفاده از AAA می‌توان برای گروه‌های مختلف از کاربران، سطح دسترسی‌های گوناگونی تعریف کرد.

در زیر نمونه‌ای از تنظیمات مربوط به تعیین سطح دسترسی بر اساس AAA بر روی خط VTY نشان داده شده است. سطح دسترسی متناسب با کاربر در صورتی به آن داده می‌شود که قبل از آن احراز اصالت شده باشد.

```
aaa authorization exec adminAuthor-list group adminAAAgroup if-authenticated
line vty 0 4
authorization exec adminAuthor-list
```

نکته: برای اینکه بتوان سطح دسترسی نشست EXEC را به کاربر مورد نظر داد، باید در تنظیمات مربوط به سرور AAA ، ویژگی Service-Type در حالت EXEC قرار داده شده باشد.

اجرای بررسی مجوزها بر اساس سطح دسترسی

نکته مهم در تنظیمات AAA این است که کاربری که قرار است سطح دسترسی مدیر به آن داده شود، باید به خوبی احراز اصالت شده باشد. دسترسی بر اساس سطوح مشخص بدین معنی است که هر سطح دسترسی توانایی انجام چه تنظیماتی بر روی تجهیزات زیر ساخت را دارد. سطح دسترسی Privilege این امکان را به کاربر می‌دهد که بتواند بر روی تجهیز سیسکو تنظیمات مورد نظرش را انجام دهد.

کسب سطح دسترسی EXEC بر روی تجهیزات سیسکو با استفاده از دستور enable قابل حصول است، یا می‌تواند به صورت اتوماتیک به عنوان نتیجه بررسی مجوز توسط RADIUS یا TACACS+ داده شود.

برای اینکه دسترسی enable با استفاده از عملیات احراز اصالت توسط سرور AAA و با توجه بـه enable secret تعریف شده از قبل داده شود، باید لیست پیش‌فرض AAA برای احراز اصالت دسترسی enable تعیین شود.

aaa authentication enable default group adminAAAgroup enable

توصیه می‌شود که به‌جای استفاده از enable password از enable secret استفاده شود. به ایـن خـاطر کـه enable secret از رمزنگاری type 5 که غیرقابل رمزگشایی است، استفاده می‌کند.

اجرای مدیریت نشست‌ها

نشست‌های دسترسی به تجهیزات با توجه به نکات زیر باید مدیریت شوند:

- نشست‌های معطل (آماده به کار)
- نشست‌های معلق

نشست‌های معطل

نشست‌های معطل نباید اجازه استفاده از ترمینال یا پورت‌های مدیریتی برای زمان نامحدود و طولانی را داشته باشند. این کار به افزایش دسترسی‌پذیری ترمینال‌ها و پورت‌ها و کاهش دزدیده شدن نشست‌ها کمک می‌کند.

در سیستم‌عامل نرم‌افزاری سیسکو می‌توان یک وقفه خالی از طریق دستور session-timeout بر روی خطوط VTY یا TTY تعریف کرد. به طور پیش فرض یک نشست VTY یک وقفه ۱۰ دقیقه‌ای دارد:

[seconds] Router(config-line)# session-timeout <minutes>

اعمال دستور session-timeout بر روی VTY اندکی با اعمال آن بر روی پورت کنسول، AUX و TTY تفاوت دارد. هنگامی که روی VTY وقفه اتفاق می‌افتد، کاربر به محیط EXEC باز می‌گردد . این درحالی است که وقتی وقفه‌ای در خطوط فیزیکی اتفاق می‌افتد، کاربر از سیستم خارج می‌شود و خط به حالت معطل در می‌آید.

می‌توان از ترکیبی از دستورات exec-timeout و session-timeout و قرار دادن مقادیر تقریباً یکسان برای آن‌ها استفاده نمود و درنتیجه رفتار خطوط مجازی و فیزیکی هنگامی که session-timeout اتفاق می‌افتد مشابه هم خواهد بود.

در IOS سیسکو به طور پیش فرض یک نشست VTY دارای وقفه ۱۰ دقیقه‌ای است:

```
Router(config-line)# session-timeout <minutes>
```

نشست‌های معلق

اگر با استفاده از یک سیستم از راه دور با یک تجهیز ارتباط برقرار شده باشد و در این حال سیستم دچار اشکال شود و ارتباط قطع گردد، نشستی که از آن استفاده می‌شد ممکن است همچنان باز باقی بماند و در برابر حملات آسیب‌پذیر باشد. بنابراین تشخیص نشست‌های معلق و بستن آن‌ها امری ضروری است. این کار به افزایش دسترسی‌پذیری ترمینال‌ها و پورت‌ها و کاهش دزدیده شدن نشست‌ها کمک می‌کند.

در IOS سیسکو می‌توان نشست‌های معطل روی خطوط VTY را از طریق دستور service tcp-keepalives-in تشخیص داد و مسدود نمود. با استفاده از این دستور پیغام‌هایی برای connection های فعلی ارسال می‌شود و اگر پاسخی بازگردانده نشود، نشست بسته می‌شود:

```
Router(config)# service tcp-keepalives-in
```

محدودکردن آسیب‌پذیری تجهیزات در برابر حملات Dictionary و DoS

آسیب‌پذیری تجهیزات موجود در شبکه هنگام دسترسی به آن‌ها نسبت به حملات DoS و Dictionary می‌تواند با اعمال نکات زیر کاهش یابد:

- اجبار به استفاده از رمزهای عبور قوی
- محدودکردن تعداد تلاش‌ها برای ورود به تجهیزات

- محدودکردن تلاش مجدد برای وارد شدن به دستگاه بعد از تلاش‌های ناموفق با اعمال یک تاخیر زمانی
- رزرو یک ترمینال و یا پورت

اجبار به استفاده از رمزهای عبور قوی

در مورد حمله Dictionary استفاده از رمز عبور قوی می‌تواند در کاهش موفقیت این حمله بسیار مؤثر باشد، در صورتی که رمز عبور انتخاب شده به صورت ساده و یکی از کلمات دیکشنری نباشد. اگر از یک سرور AAA برای احراز اصالت استفاده شده باشد، این سرور می‌تواند بر اساس سیاست‌های امنیتی تعریف شده، کاربران را مجبور به استفاده از رمزهای عبور قوی کند. اگر یک سرور AAA برای اجبار به استفاده از رمزهای قوی موجود نباشد، باید با استفاده از ویژگی‌های تجهیزات موجود و اعمال آن‌ها تأثیر حملات مذکور را کاهش داد.

اگر هیچ ویژگی و قابلیتی برای کاهش اثر حمله دیکشنری وجود نداشته باشد، اجبار به استفاده از رمزهای عبور با طول حداقل به عنوان یک ویژگی پایه قابل اعمال است. البته این ویژگی باعث جلوگیری مستقیم از حمله دیکشنری نمی‌شود بلکه می‌تواند از حدس زدن رمزهای عبور ساده که به طور معمول استفاده می‌شوند، مانند cisco یا lab ، جلوگیری کند.

ویژگی کمترین طول پسورد در IOS سیسکو

IOS سیسکو توانایی اجبار به استفاده از رمزهای عبور با حداقل طول برای کاربران را دارد. این سیاست قابل اعمال به رمزهای عبور زیر می‌باشد:

- user password
- enable password
- enable secret
- line password

این ویژگی از طریق دستور زیر می‌تواند به کار گرفته شود:

```
Router(config)# security passwords min-length length
```

وقتی این دستور اجرا شود، هر پسوردی با طول کمتر از مقداری که در این دستور در نظرگرفته شده، مردود می‌باشد.

توجه: این ویژگی نمیتواند هیچ محافظتی در برابر حمله دیکشنری انجام دهد.

محدود کردن تعداد دفعات ورود

برای مقابله با حمله دیکشنری می‌توان یک تأخیر بین هر دو درخواست ورود تعریف کرد. این کار باعث کاهش سرعت حمله، افزایش زمان مورد نیاز برای موفقیت حمله و افزایش بازه زمانی برای تشخیص رفتارهای غیرعادی می‌شود.

در IOS سیسکو برای اعمال تاخیر بین درخواست‌های ورود پی در پی می‌توان از دستور login delay استفاده کرد. به طور پیش‌فرض یک ثانیه تأخیر برای این منظور در نظر گرفته شده است:

Router(config)# login delay <seconds>

محدود کردن تعداد دفعات ورود ناموفق در یک بازه زمانی مشخص

برای مقابله با حمله دیکشنری می‌توان تعداد دفعات درخواست‌های ورود ناموفق به تجهیز را در یک بازه زمانی معین، محدود کرد. این کار باعث کاهش سرعت حمله، افزایش زمان مورد نیاز برای موفقیت حمله و افزایش بازه زمانی برای تشخیص رفتارهای غیرعادی می‌شود.

اگر از سرور AAA برای احراز اصالت درخواست‌های ورود به سیستم استفاده شده باشد، این سرور به طور معمول دارای این ویژگی است که اگر تعداد مشخصی درخواست ورود ناموفق انجام شده باشد، سیستم برای یک بازه زمانی مشخص قفل می‌شود و در این بازه امکان ورود به سیستم وجود نخواهد داشت. اگر از سرور AAA استفاده نشده باشد، باید از ویژگی‌های سیستم عامل نرم‌افزاری سیسکو بهره برد.

در IOS سیسکو برای تعریف حداکثر تعداد دفعات تلاش برای ورود به دستگاه در یک بازه زمانی مشخص، به طوری که بعد از آن دستگاه برای یک زمان معین اجازه وارد شدن را ندهد، از دستور زیر می‌توان استفاده کرد:

```
Router(config)# login block-for seconds attempts tries within seconds
```

همچنین در سیستم عامل نرم‌افزاری سیسکو می‌توان یک ACL استثناء برای سیستم‌ها و شبکه‌های مورد اعتماد و مجاز، با استفاده از دستور زیر تعیین کرد:

```
Router (config)# login quiet-mode access-class
```

در مثال زیر روتر به گونه‌ای پیکربندی شده است که اگر در بازه زمانی ۱۰۰ ثانیه تعداد دفعات تلاش برای وارد شدن به تجهیز از ۱۵ مرتبه تجاوز کند، دستگاه برای یک بازه زمانی ۱۰۰ ثانیه‌ای اجازه هیچ‌گونه وارد شدن به دستگاه مگر برای سیستم‌هایی که در ACL 10 تعریف شده‌اند را نمی‌دهد:

```
Router(config)# access-list 10 permit host 172.26.150.206
Router(config)# login block-for 100 attempts 15 within 100
Router(config)# login quiet-mode access-class 10
```

رزرو یک ترمینال و یا پورت

هدف یک حمله DoS به تجهیزات موجود در زیر ساخت می‌تواند ترمینال و یا پورت‌ها باشد. این نوع از حمله به این حقیقت اشاره دارد که تعداد محدودی از ترمینال‌ها و یا پورت‌ها در دسترس هستند و اگر تمام پورت-ها مورد استفاده قرار گیرند، حتی اگر ارتباطی احراز اصالت نشده باشد، امکان ایجاد هیچ ارتباط جدیدی وجود ندارد.

تجهیزات سیسکو (مبتنی بر سیستم عامل IOS) دارای تعداد محدودی خطوط VTY هستند که به طور معمول این تعداد ۵ خط می‌باشد. زمانی که تمام این خطوط VTY مورد استفاده قرار می‌گیرند، هیچ ارتباط از راه دوری نمی‌تواند برقرار گردد. با توجه به این موضوع شرایط برای انجام یک حمله DOS می‌تواند فراهم شود. اگر حمله‌کننده بتواند تمامی خطوط VTY را از راه دور اشغال کند، دیگر کاربران مجاز نمی‌توانند به سیستم دسترسی داشته باشند. حمله‌کننده نیازی به وارد شدن به تجهیز برای عملی کردن حمله خود ندارد و پس از وارد شدن به صفحه login ، نشست را رها می‌کند. استفاده از AAA نمی‌تواند از وقوع این حمله

جلوگیری کند چون حمله‌کننده اصلاً نیازی به تلاش برای وارد شدن به تجهیز ندارد و تنها کاری که برای انجام حمله باید انجام دهد این است که یک ارتباط با پورت مورد نظر برقرار نماید، بنابراین این پورت برای دیگر کاربران قابل استفاده نخواهد بود.

یکی از روش‌های مقابله با این نوع حمله، اعمال محدودیت دسترسی قوی برای یک ترمینال یا پورت مشخص می‌باشد، به طور مثال برای یک پورت می‌توان این‌گونه تعریف کرد که فقط از یکی از سیستم‌های NoC قابل دسترسی باشد.

در IOS سیسکو این موضوع با استفاده از اعمال ACL های محدودکننده قوی بر روی آخرین VTY صورت می‌گیرد. آخرین VTY که معمولاً VTY4 می‌باشد، می‌تواند تنها به برقراری ارتباط از سوی یک سیستم معین و مشخص محدود شود و بقیه VTY ها بتوانند به درخواست‌های ارتباط از سوی هر آدرسی پاسخ دهند:

```
access-list 10 permit <NOCsubnet> <inverse-mask>
access-list 20 permit host <NOC-Host>
line vty 0 3
access-class 10 in
line vty 4
access-class 20 in
```

بنرهای مجاز اطلاع‌رسانی

توصیه می‌شود که بر روی تمام session های ارتباطی، یک بنر به منظور اطلاع‌رسانی سیاست‌های امنیتی که کاربر ملزم به رعایت آن‌ها می‌باشد، ایجاد شود.

این اطلاعات شامل مواردی همچون تعیین کاربران مجاز و دسترسی آن‌ها و یا اخطار به کاربران غیر مجاز و عواقب دسترسی غیرمجاز آن‌ها می‌تواند باشد.

اگر از دیدگاه امنیتی به قضیه نگاه شود، دراین صورت در بنرها نباید هیچگونه اطلاعات خاصی درباره تجهیز از جمله نام، مدل، نرم افزار، محل قرارگیری، اپراتور و یا صاحب آن ذکر شود، به این دلیل که این نوع اطلاعات ممکن است برای حمله کننده مفید واقع شود .

در IOS سیسکو تنظیمات معینی برای نمایش این هشدارها در دسترس است. این موارد شامل banner motd ، banner login ، banner incoming و banner exec می‌باشند.

زمانی که یک کاربر به یک تجهیز سیسکو مبتنی بر IOS متصل می‌شود، یک پیغام MOTD[5] ، اگر تنظیم شده باشد، ظاهر می‌شود. پس از آن بنر مربوط به login (در صورت تنظیم بودن) نشان داده خواهد. پس از ورود موفق کاربر به تجهیز، اگر این ورود با استفاده از telnet صورت گرفته باشد، بنر ورودی و اگر به روش‌های دیگری به تجهیز متصل شده باشد بنر EXEC نشان داده خواهد شد. توصیه می‌شود که یکی از دو بنر MOTD و یا Login در تجهیز فعال شود. در این صورت بر روی تمام session ها هنگام برقراری ارتباط با تجهیز و قبل از نمایش login promt اطلاعات مربوط به بنر نشان داده خواهد شد.

سرویس‌های AAA

مروری بر AAA: در واقع AAA یک چارچوب معماری برای پیکربندی سه اصل امنیتی مجزا از هم در کنار یکدیگر به روش ماژولار می‌باشد. این اصول در زیر آورده شده‌اند:

- Authentication : احراز اصالت کاربر قبل از اینکه بتواند به شبکه و یا سرویس‌های آن دسترسی داشته باشد.
- Authorization : تعیین سطح دسترسی برای کاربری که احراز اصالت شده است.
- Accounting : توانایی پیگیری دسترسی‌های کاربر که می‌تواند شامل مشخصات، زمان شروع و پایان اتصال، دستورات اجرا شده، تعداد بسته‌ها و یا بایت‌های ارسالی و دریافتی توسط وی باشد.

AAA روش توصیه شده برای کنترل دسترسی است. IOS سیسکو برای تسهیل کنترل دسترسی ویژگی‌هایی از جمله احراز اصالت محلی نام کاربری[6] و احراز اصالت رمز عبور خطوط[7] در اختیار می‌گذارد. در هر صورت

[5] Message Of The Day
[6] Local username authentication
[7] Line password authentication

این ویژگی‌ها قابل مقایسه با سطح کنترل دسترسی که AAA در اختیار می‌گذارد نیست و استفاده از آن‌ها توصیه نمی‌شود. اگر یک سرور مجزا برای تنظیمات AAA در دسترس نباشد، باید آن را بر روی دیتابیس محلی خود دستگاه پیکربندی کرد. سه متد مربوط به AAA با اعمال آن‌ها بر روی اینترفیس‌ها فعال می‌شود.

AAA از پروتکل‌هایی از جمله RADIUS, TACACS+ و یا Kerbros برای تامین امنیت استفاده می‌کند.

متمرکزسازی AAA

روش پیشنهادی برای پیاده‌سازی AAA ، متمرکزسازی آن بر روی یک سرور به همراه یک رمزعبور برای حالت جایگزین می‌باشد. از این رمز عبور مواقعی استفاده می‌شود که عملیات احراز اصالت توسط سرور AAA امکان‌پذیر نباشد. مهمترین مزایای متمرکزسازی سرور AAA شامل موارد زیر است:

مدیریت : نام کاربری و رمز ورود به طور جداگانه در یک محل مرکزی ذخیره می‌شوند که می‌توانند به صورت مستقل توسط تجهیزات مختلف استفاده شوند.

مقیاس‌پذیری: مقیاس سرورهای AAA می‌توانند به طور مستقل بر حسب اندازه دیتابیس مربوط به کاربران و تعداد تراکنش‌های انجام شده در ثانیه تغییر یابد.

امنیت : رمزهای عبور می‌توانند در یک روتر به صورت رمزشده و با در یک دیتابیس ذخیره شوند. ولی حتی اگر آن‌ها رمزشده هم باشند، باز هم قابل رمزگشایی هستند.

توانایی حسابرسی : از تمامی دسترسی‌ها و session های مجازبه طور مستقل گزارش‌گیری می‌شود.

پیشنهاد می‌شود به‌جای استفاده از مکانیزم‌های موجود در سیستم‌عامل نرم‌افزاری سیسکو برای احراز اصالت، از AAA استفاده شود. در این صورت می‌توان به‌جای استفاده از یک نام کاربری و رمزعبور برای همه کاربران، برای هر کدام از آن‌ها رمزعبور جداگانه در نظر گرفت.

گروه‌های سرور AAA

در IOS سیسکو یک گروه سرور AAA در واقع یک لیست از سرورهای AAA هم‌نوع است، مثلاً RADIUS یا +TACACS که برای اجرای AAA مورد نیاز است. استفاده از گروه سرور AAA به‌جای استفاده از سرورهای AAA برای هر هدف مشخص، قابلیت انعطاف‌پذیری بیشتری را فراهم می‌کند. برای مثال می‌توان از سرورهای AAA مختلف برای سرویس‌های گوناگون AAA به منظور جداسازی دسترسی کاربران به تجهیزات استفاده کرد. مثلاً احرازاصالت برای دسترسی به تجهیزات زیرساخت از طریق سرور +TACACS و احراز اصالت کاربران عادی از طریق سرور RADIUS انجام شود:

```
aaa group server tacacs+ adminAAAgroup
server TAC+server1
server TAC+server2
!
 aaa group server radius enduserAAAgroup
server RADserver1
 server RADserver2
```

لیست روش‌های AAA

AAA از طریق اعمال لیست‌های تعیین شده بر روی اینترفیس‌های مشخص اجرا می‌شود. این لیست‌ها شامل روش‌های احراز اصالت و تعیین سطح دسترسی مشخصی می‌باشند که باید بر روی اینترفیس‌ها اعمال شوند. این لیست‌ها می‌توانند بر اساس یک یا چندین پروتکل امنیتی برای عملیات احراز اصالت و یا تعیین سطح دسترسی عمل کنند.

IOS سیسکو به این ترتیب عمل می‌کند که ابتدا اولین خط لیست مربوط به AAA را بررسی می‌کند، اگر ارتباط با بررسی این خط ایجاد نشود، خط دوم از لیست بررسی می‌شود. این کار ادامه پیدا می‌کند تا اینکه با بررسی یکی از خطوط لیست ارتباط برقرار شود و یا اینکه لیست تمام شود، که در این صورت هیچ ارتباطی شکل نمی‌گیرد.

یک نمونه از این لیست‌ها که با نام adminAuthen-list مشخص شده است، در زیر نشان داده شده است.

اولین متد از این لیست سعی در انجام احراز اصالت از طریق سرور +TACACS دراد که در گروه سرور adminAAAgroup است. اگر احراز اصالت از طریق این متد انجام نشود، احراز اصالت به صورت محلی انجام می‌گیرد.

```
aaa authentication login adminAuthen-list group adminAAAgroup local-case
aaa group server tacacs+ adminAAAgroup
server TAC+server1
```

server TAC+server2

این لیست‌ها برای اجرا شدن باید بر روی یک اینترفیس اعمال شوند. تنها استثنا در این حالت، لیست پیش-فرض AAA با نام default می‌باشد. این لیست‌ها به صورت خودکار بر روی تمام اینترفیس‌ها فعال می‌شوند، البته اگر لیستی قبلاً اعمال نشده باشد. همچنین با اعمال یک لیست روی اینترفیس، این لیست بر روی لیست پیش‌فرض بازنویسی می‌شود.

aaa authentication login default group enduserAAAgroup local-case
aaa group server radius enduserAAAgroup
server RADserver1

برقراری امنیت ارتباط سرور AAA

ارتباط بین احراز اصالت کننده[8] (یا همان NAS[9]) و سرور AAA به طور معمول از طریق RADIUS یا TACACS+ انجام می‌گیرد. امنیت این ارتباط به طور خلاصه در زیر آورده شده است:

- تراکنش‌ها و تعاملات RADIUS و TACACS+ از طریق یک کلید ثابت و مشترک احراز اصالت می‌شوند. این کلید بر اساس نام تجهیز یا آدرس IP آن می‌باشد و هرگز بر روی بستر شبکه ارسال نمی‌شود.
- RADIUS طبق استاندارد تنها قسمت رمزعبور کاربر را رمزنگاری می‌کند. بقیه قسمت‌های بسته به صورت فاش ارسال می‌شود که در این صورت در برابر شنود آسیب‌پذیر می‌باشد.
- TACACS+ کل محتوای بسته را رمز می‌کند. در این روش اگر چه محرمانگی اطلاعات حفظ می-شود ولی الگوریتم رمزنگاری استفاده شده در آن خیلی قوی نمی‌باشد.

[8] authenticator
[9] Network Access Server

راهنمای کلی برای امن کردن ارتباط AAA به صورت زیر است:

- استفاده از کلیدهای قوی به منظور انجام عملیات احراز اصالت برای سرور AAA و NAS
- تغییر کلید استفاده شده برای احراز اصالت سرور AAA و NAS به طور منظم
- محدود کردن ارتباطات AAA با تعدادی از سرورهای مجاز AAA و پورت‌های ارتباطی AAA با استفاده از ACL های نوع extended
- از آنجایی که RADIUS یا TACACS+ از رمزنگاری و عملیات احراز اصالت قوی پشتیبانی نمی-کنند، توصیه می‌شود که از OOB[10] یا IPSec برای حفاظت از تراکنش‌ها و تعاملات سرور AAA در برابر حملات استفاده شود.

سرویس‌های حسابداری مبتنی بر AAA

موضوع مهمی که باید در نظر گرفته شود، ثبت دسترسی‌هایی است که به یک تجهیز صورت می‌گیرد. یکی از روش‌های ثبت گزارش دسترسی به تجهیزات استفاده از سرویس‌های AAA می‌باشد. با استفاده از این مکانیزم می‌توان سرویس‌هایی که کاربران به آن‌ها دسترسی دارند و یا میزان ترافیک مصرفی آن‌ها را پیگیری کرد. با فعال‌شدن سرویس‌های حسابداری مبتنی بر AAA ، تجهیزات زیرساخت فعالیت‌های صورت گرفته توسط کاربران را به سرور AAA ارسال می‌کنند.

IOS سیسکو از ۵ روش مختلف برای عملیات حسابداری پشتیبانی می‌کند:

Network Accounting : حسابداری شبکه اطلاعاتی در مورد نشست‌های PPP ، SLIP و ARAP در اختیار می‌گذارد که شامل شمارش تعداد بسته‌ها و همچنین تعداد بایت‌ها می‌باشد.

[10] Out of band

Connection Accounting : این قسمت اطلاعاتی در مورد تمام connection های برقرار شده از سرور به سمت بیرون مثل Telnet ، local-area transport(LAT) ، TN3270 ، packet assembly-disassembly(PAD) در اختیار می‌گذارد.

EXEC Accounting : در این قسمت اطلاعاتی در مورد نشست‌های کاربران که در حالت EXEC به سرور متصل شده‌اند، شامل نام کاربری، تاریخ، زمان شروع و پایان، آدرس IP و شماره تلفن در صورتی که کاربر به صورت dial-up متصل شده باشد، در دسترس خواهد بود.

Command Accounting : اطلاعاتی که در این حالت می‌توان بدست آورد شامل دستورات محیط EXEC می‌باشد که برای یک سطح دسترسی خاص بر روی سرور اجرا می‌شود. هر دستور به همراه تاریخ و زمان اجرای آن و کاربری که آن را اجرا کرده است، گزارش‌گیری می‌شود.

System Accounting : در این قسمت اطلاعاتی در مورد تمام رخدادهای سطح سیستم (برای مثال زمانی که سیستم reboot می‌شود) در دسترس خواهد بود.

مباحث پایه امنیت شبکه بر روی امن‌سازی زیرساخت شبکه و سرویس‌های مهم تمرکز می‌کند. در نتیجه، حسابداری مبتنی بر AAA با توجه به مباحث پایه امنیتی شبکه شامل موارد زیر است:

- EXEC Accounting
- Command Accounting
- System Accounting

پروتکل SSH

SSH پروتکلی برای دسترسی امن از راه دور به تجهیز و انتقال فایل است. این پروتکل دارای مکانیزم رمزنگاری و احراز اصالت قوی می‌باشد. به همین دلیل استفاده از آن به‌جای بهره بردن از Telnet و یا rlogin توصیه می‌شود.

معمولاً دو نسخه از SSH وجود دارد: SSHv1 و SSHv2 . در SSHv2 ضعف‌های امنیتی نسخه اول برطرف شده است. البته نسخه دوم از این پروتکل روی بعضی از تجهیزات پشتیبانی نمی‌شود ولی IOS سیسکو از هر دو نسخه پشتیبانی می‌کند.

مکانیزم احراز اصالت در SSH از بسیاری پروتکل‌ها مثل TACACS+ ، RADIUS و احراز اصالت RSA پشتیبانی می‌کند. همچنین SSH از الگوریتم‌های رمزنگاری مانند DES ، 3DES ، IDEA ، RC4-128 و دیگر الگوریتم‌ها پشتیبانی می‌کند.

برای فعال کردن SSH بر روی تجهیزات سیسکو باید مراحل زیر طی شوند:

- گام اول: تعیین hostname و پیکربندی دامنه DNS برای روتر
- گام دوم: تولید یک جفت کلید RSA
- گام سوم: به طور اختیاری می‌توان یک time-out و محدودیتی برای تعداد تلاش‌های ورود به تجهیز قرار داد. به طور پیش فرض time-out برابر ۱۲۰ ثانیه و تعداد تلاش‌ها برای احراز اصالت پی‌درپی، ۳ مرتبه در نظر گرفته شده است.
- گام چهارم: محدود کردن دسترسی VTY ها فقط از طریق SSH . اکیداً توصیه می‌شود این مرحله بر روی تجهیز انجام شود.
- گام پنجم: محدود کردن دسترسی از طریق SSH فقط برای کاربران یا شبکه‌های مجاز

در مثال زیر نحوه پیکربندی SSH بر روی یک تجهیز سیسکو نشان داده شده است:

```
---!Step 1: Configure a hostname and domain name
Router(config)# hostname router
Router (config)# ip domain-name nyc.cisco.com
---!Step 2: Generate an RSA key pair, automatically enabling SSH.
Router (config)# cry key generate rsa
---!Step 3: Configure time-out and number of authentication retries.
Router (config)# ip ssh time-out 60
Router (config)# ip ssh authentication-retries 2
---!Step 4: Configure VTYs to only accept SSH .
```

```
Router (config)# line vty 0 4
Router (config-line)# transport input ssh
 ---!Step 5: Allow SSH connections only originated from the management network.
Router (config)# access-list 111 remark ACL for SSH
Router (config)# access-list 111 permit tcp 172.26.0.0 0.0.255.255 any eq 22
Router (config)# access-list 111 deny ip any any log-input
Router (config)# line vty 0 4
Router (config-line)# access-class 111 in
```

دسترسی گرافیکی به تجهیز مبتنی بر وب

امروزه تقریباً تمام محصولات شبکه را می‌توان از طریق محیط گرافیکی مبتنی بر وب پیکربندی کرد. این روش به‌خاطر سهولت استفاده از آن بسیار پر استفاده می‌باشد. در این روش تنها به یک مرورگر وب نیاز داریم.

به هر حال ممکن است بعضی از این محیط‌های گرافیکی مبتنی بر وب از پروتکل‌های نا امنی مثل HTTP استفاده کنند. پروتکل HTTP اطلاعات را به صورت فاش در شبکه ارسال می‌کند. ازاین‌رو HTTP در برابر شنود و دیگر حمله‌ها آسیب‌پذیر است. توصیه می‌شود که دسترسی از طریق این پروتکل غیرفعال و به‌جای آن از HTTPS استفاده شود. HTTPS از SSL و TLS برای رمزنگاری اطلاعات و احراز اصالت استفاده می‌کند.

پروتکل HTTP

در IOS سیسکو به طور پیش فرض http غیرفعال است. HTTP از طریق دستور زیر می‌تواند غیر فعال شود:

```
Router(config)# no ip http server
```

برای حالت‌هایی که استفاده از پروتکل HTTPS مقدور نمی‌باشد و حتماً باید از پروتکل HTTP استفاده کرد، اعمال راهنمای استفاده بیان شده در جدول ۲ ضروری می‌باشد.

(جدول ۶) راه اندازی HTTP

نحوه پیکربندی در IOS سیسکو	راهنمای امنیتی http
ip http authentication aaa login-authentication <aaa-listname>	احراز اصالت کاربران توسط AAA
ip http authentication aaa exec-authorization <aaa-listname>	بررسی مجوز دستورهای http وارد شده در محیط exec توسط AAA
ip http access-class <ACL#> access-list <ACL#> permit host 10.0.0.1	محدود ساختن دسترسی‌های http تنها توسط کاربران مجاز
ip http max-connections 3	محدود ساختن تعداد ارتباطات همزمان http

در IOS سیسکو برای فعال کردن احراز اصالت از طریق پروتکل HTTP بایستی از دستور زیر استفاده کرد. در مثال زیر نحوه انجام تنظیمات احراز اصالت بر اساس HTTP که از پروتکل TACTACS+ استفاده می‌کند، نشان داده شده است.

```
username adminuser privilege 15 password <mypassword>
aaa new-model
aaa authentication login default group adminAAAgroup local-case
aaa authorization exec default group adminAAAgroup local
aaa accounting exec default start-stop group adminAAAgroup
!
ip http server
ip http authentication aaa
!
!HTTP access requires telnet service being accepted at the VTY
line vty 0 4
transport input telnet
```

پروتکل HTTPS

در IOS سیسکو برای فعال‌کردن سرویس HTTPS از دستور زیر باید استفاده کرد:

```
Router(config)# ip http secure-server
```

پروتکل SNMP

SNMP مشهورترین پروتکل برای مدیریت شبکه است و تقریباً تمامی دستگاه‌های شبکه از آن پشتیبانی می‌کنند.

سه نسخه از SNMP وجود دارد :

- نسخه 1 ، قدیمی‌ترین نسخه آن است که هنوز هم البته به طور اندک در حال استفاده می‌باشد.

- نسخه c2 ،که بیشترین استفاده از این نسخه می‌باشد.
- نسخه 3 ، این نسخه استاندارد IETF می‌باشد که دارای امنیت بالایی است.

SNMP نسخه 1 و c2 از نظر امنیتی ضعیف می‌باشند. در این دو نسخه فقط دسترسی‌های احراز اصالت شده به دیتابیس MIB از community string استفاده می‌کنند. علاوه بر این تمام اطلاعات به صورت فاش ارسال می‌شوند. ضمن اینکه هیچ کدام از این دو نسخه از رمزنگاری پشتیبانی نمی‌کنند.
در SNMP v3 این مشکلات امنیتی با استفاده از مکانیزم‌هایی از جمله احراز اصالت، بررسی صحت پیام، کنترل دسترسی و رمزنگاری رفع شده است. در این نسخه با استفاده از الگوریتم رمزنگاری DES تمامی اطلاعات رمز می‌شوند. با توجه به ویژگی‌های SNMPv3 توصیه می‌شود که از این نسخه استفاده شود.

راهنمای کلی برای امن‌سازی SNMP در زیر آمده است. در صورت نیاز نداشتن به این پروتکل، باید آن را غیرفعال کرد:

- فقط از ویژگی‌های مورد نیاز SNMP استفاده کنید.
- باید این ویژگی‌ها فقط اجازه خوانده شدن داشته باشند.
- بایستی از درخواست‌هایی که می‌خواهند کل جدول مسیریابی و جدول ARP را با استفاده از SNMP دانلود کنند، جلوگیری شود.
- بایستی به community string ها همانند رمز عبور مدیر شبکه نگاه کرد.
- بایستی community string های پیش‌فرض پاک شوند.
- بایستی از community string های قوی استفاده کرد.
- بایستی تعداد سیستم‌هایی که از آن‌ها بتوان به تجهیز دسترسی SNMP داشت، محدود شوند. این کار با استفاده از ACL های extended و محدود کردن پورت‌هایی انجام می‌شود که پروتکل SNMP از آن‌ها استفاده می‌کند (UDP 161,162).

- بایستی اعمالی که در مورد SNMP توسط سیستم‌های مجاز می‌توان انجام داد، با استفاده از community string های متفاوت محدود شود.
- اگر فقط از نسخه ۳ استفاده می‌شود، باید از فعال بودن این نسخه و غیرفعال بودن دیگر نسخه‌ها اطمینان حاصل شود.
- بایستی تنها trap های مهم فعال شوند.
- بایستی هنگامی که عملیات احراز اصالت community name با موفقیت انجام نمی‌شود، یک trap ارسال شود.
- بایستی نظارت منظم بر SNMP trap ها صورت پذیرد.
- اگر نیاز به استفاده از نسخه‌های ۱ و۲ وجود داشته باشد، توصیه می‌شود که حتماً با استفاده از IPSec تعاملات SNMP در برابر حملات امن شوند.

محافظت از اطلاعات محلی ذخیره شده

تجهیزات سیسکو بعضی از اطلاعات حساس مانند رمزهای عبور و یا کلیدهای رمزنگاری را به صورت محلی ذخیره می‌کنند. تمامی رمزهای عبور باید توسط یک سرور مرکزی AAA کنترل و نگهداری شوند. مزیت این روش می‌تواند به مدیریت امن رمزهای عبور، توانایی اجبار به استفاده از رمزهای عبور قوی، قفل شدن حساب کاربری بعد از تعداد مشخصی ورود ناموفق، اجبار کاربران به تغییر رمزهای عبور به صورت دوره‌ای و بسیاری مزایای دیگر منجر شود. علاوه بر این در این حالت رمزهای عبور در مکان امن ذخیره می‌شوند و امکان تهیه نسخه پشتیبان از آن‌ها نیز وجود دارد.

با این وجود حتی اگر یک سرور AAA مرکزی ایجاد شود تعدادی از پسوردهای محلی برای حالت‌های خاصی ذخیره می‌گردند، مثلاً در حالتی که سرورهای AAA در دسترس نباشد.

البته در صورتی که یک سرورمرکزی AAA نیز وجود داشته باشد، به دلیل اینکه ممکن است مواقعی این سرور در دسترس نباشد، باز هم باید تعدادی رمزعبور که به صورت محلی ذخیره شده‌اند، وجود داشته باشد.

IOS سیسکو برای ذخیره امن اطلاعات، ویژگی‌های زیر را در اختیار می‌گذارد:

- Global passeord encryption
- Local user password encryption
- Ecable secret

رمزنگاری اطلاعات حساس شامل رمزهای عبور به دلیل حفظ محرمانگی آن‌ها هنگام مشاهده و یا هنگام ارسال اطلاعات می‌باشد.

- Global password encryption: در فایل تنظیمات سیسکو به طور پیش‌فرض رمزهای عبور به صورت فاش ذخیره شده‌اند. برای حفاظت از آن‌ها می‌توان با استفاده از دستور زیر اطلاعات حساس را رمز کرد:

Router(config)# service password-encryption

با این حال الگوریتم استفاده شده در این دستور امن نمی‌باشد و اطلاعات رمز شده توسط آن به سادگی قابل رمزگشایی هستند. در نتیجه این دستور فقط برای حالتی مناسب است که فرد در حال مشاهده تنظیمات تجهیز بوده و همکار فرد نیز در همین حال آن‌ها را مشاهده می‌کند ولی قادر به تشخیص رمزهای عبور نمی‌تواند باشد.

البته تمام اطلاعات حساس موجود در فایل تنظیمات با استفاده از این دستور رمز نمی‌شوند و باید از کل این فایل که حاوی اطلاعات حساسی است به طور مؤثر محافظت شود.

البته IOS سیسکو از رمزنگاری قوی‌تری نیز برای محافظت از رمزهای عبور که به صورت محلی ذخیره شده‌اند، پشتیبانی می‌کند. این کار با استفاده از enable secret به‌جای استفاده از enable password می‌تواند انجام می‌شود.

- Local User Password Encryption: نام‌های کاربری و رمزهای عبور باید در امن‌ترین فضای تجهیز ذخیره شوند. از این حساب‌های کاربری فقط باید در حالتی استفاده شود که احراز اصالت از طریق سرور AAA امکان پذیر نمی‌باشد.

در IOS سیسکو، رمزهای عبور مربوط به نام‌های کاربری که به صورت محلی ذخیره شده‌اند، می‌توانند با استفاده از الگوریتم رمز قوی MD5 با استفاده از دستور زیر رمزنگاری شوند.

Router(config)# username <name> secret <strongpassword>

نکته قابل توجه این است که رمزنگاری MD5 برگشت‌پذیر نمی‌باشد و نمی‌تواند همراه پروتکل‌هایی که نیاز به استفاده از رمزهای عبور به صورت فاش دارند، مثل CHAP ، استفاده گردد.

- Enable Secret: در IOS سیسکو می‌توان با استفاده از دستور enable به محیط EXEC دسترسی داشت. توصیه می‌شود به منظور ایجاد رمز عبور برای این محیط، به‌جای استفاده از دستور enable password از دستور enable secret استفاده شود. enable secret از الگوریتم رمز MD5 استفاده می کند.

Router(config)# enable secret <strongpassword>

اگر enable password نیز ایجاد شده باشد، باید با استفاده از دستور زیر آن را غیرفعال کرد.

Router(config)# no enable password

البته با انجام این مراحل، همچنان آسیب‌پذیری نسبت به حلمه dictionary باقی می‌ماند.

ثبت گزارش دسترسی به تجهیزات زیرساخت

بایستی دسترسی به تجهیزات زیرساخت و تغییراتی که در فایل تنظیمات انجام می‌شود، طبق موارد زیر گزارش‌گیری شود:

- چه کسی به وسیله دسترسی داشته است.
- چه موقع یک کاربر وارد شده است.
- کاربر چه فعالیتی انجام داده است.
- چه موقع کاربر خارج شده است.
- تلاش‌های ناموفق برای وارد شدن به تجهیز
- درخواست‌های ناموفق احراز اصالت
- درخواست‌های ناموفق کسب مجوز دسترسی

ثبت گزارش‌های مربوط به محیط EXEC بر اساس AAA

در این قسمت اطلاعاتی در مورد تمام کاربران محیط EXEC مربوط به تجهیزات زیرساخت شبکه شامل نام کاربری، تاریخ، زمان شروع و پایان، آدرس IP تجهیز و آدرس IP مبدأ مربوط به کاربر در دسترس می‌باشد. برای فعال کردن AAA EXEC Accounting بایستی از دستورهای زیر استفاده کرد. در این مثال یک پیکربندی نمونه از اعمال این سرویس بر روی خطوط VTY نشان داده شده است.

```
aaa accounting exec account-exec-list start-stop group adminAAAgroup
line vty 0 4
accounting exec account-exec-list
```

ثبت گزارش‌های احراز اصالت‌های ناموفق

برای اینکه بتوان گزارش‌های مربوط به احراز اصالت‌های ناموفق برای ورود به تجهیز یا عدم برقراری ارتباط PPP برای کاربرانی که به طور موفق احراز اصالت شده‌اند را ثبت کرد، از دستور زیر باید استفاده کرد:

```
Router (config)# aaa accounting send stop-record authentication failure
```

ثبت گزارش‌های مربوط به دستورهای وارد شده

این ویژگی تنها زمانی قابل اجرا می‌باشد که از TACACS+ استفاده شده باشد و اطلاعاتی در مورد دستوراتی که در محیط EXEC یک تجهیز زیرساخت، تحت یک سطح دسترسی خاص وارد شده‌اند، در اختیار قرار می‌دهد. جزئیات این اطلاعات شامل تاریخ، زمان و کاربری است که دستور مربوطه را اجرا کرده است.

برای استفاده از این سرویس از دستورات زیر باید استفاده کرد.

```
aaa accounting exec
 aaa accounting commands 15 account-exec-list start-stop group tacacs-group
 line vty 0 4
accounting commands 15 account-exec-list
```

هنگامی که از این سرویس استفاده می‌شود، تمامی دستورهایی که در حالت enable وارد می‌شوند، از آن‌ها گزارش گرفته می‌شود. در نتیجه هرگونه تغییر در اطلاعات حساس تجهیز مانند enable secret نباید در محیط CLI اعمال شوند مگر اینکه این سرویس به طور موقت غیرفعال شده باشد. راه حل پیشنهادی این

است که تغییرات مورد نظر به صورت آفلاین انجام شوند و پس از آن این فایل به طور امن به تجهیز انتقال داده شود.

ثبت گزارش‌های سیستم

برای فعال کردن این سرویس در یک تجهیز سیسکو از دستورات زیر استفاده می‌شود:

```
aaa accounting system
Router (config)# aaa accounting system default start-stop group tacacs-group
```

ثبت گزارش‌های دسترسی به دستگاه

IOS سیسکو توانایی ارسال یک syslog trap برای ورودهای موفق یا ناموفق به دستگاه را دارد. با استفاده از دستورات زیر می‌توان از این ویژگی استفاده کرد:

```
Router(config)# login on-success log
Router(config)# login on-failure log
```

اطلاع‌رسانی و ثبت گزارش‌های تغییر تنظیمات

در IOS سیسکو هر تغییری که در پیکربندی تجهیز صورت بگیرد به صورت مناسب به کاربر اطلاع رسانی و ثبت می‌شوند. این گزارش‌های شامل موارد زیر است:

- دستوری که اجرا شده است.
- محیط و سطح دسترسی که دستور در آن اجرا شده است.
- کاربری که دستور را اجرا کرده است.
- زمان اجرای دستور

برای فعال کردن ثبت گزارش‌ها از دستورات زیر استفاده می‌شود:

```
 Enter archive mode
Router(config)# archive
!
 !Enter the archive configuration change logger configuration mode
Router(config-archive)# log config
!
```

```
!Enable configuration change logging
Router(config-archive-log-config)# logging enable
!
!Set the maximum number of configuration change log entries as 200
Router(config-archive-log-config)# logging size 200
!
!Prevent passwords from being displayed in the configuration log
Router(config-archive-log-config)# hidekeys
!
!Enable configuration change messages to be sent to a syslog server
Router(config-archive-log-config)# notify syslog
```

نمایش گزارش‌های ثبت‌شده در مورد تغییر پیکربندی‌ها

گزارش‌های ثبت شده در تجهیز را می‌توان با استفاده از دستور زیر مشاهده کرد:

```
Router# show archive log config all
```

برای مقایسه خط به خط یک فایل پیکربندی با پیکربندی فعلی تجهیز می‌توان از دستور زیر استفاده کرد:

```
Router# show archive config incremental-diffs nvram:startup-config
```

همچنین برای مقایسه دو فایل پیکربندی و تعیین تفاوت‌های آن‌ها می‌توان از دستور زیر استفاده کرد:

```
Router# show archive config differences nvram:startup-config
```

پروتکل‌های انتقال فایل

برای انتقال فایل در طول شبکه می‌توان از پروتکل‌های زیر استفاده کرد:

- File Transfer Protocol (FTP)
- Trivial File Transfer Protocol (TFTP)
- Srcure Copy (SCP)

FTP و TFTP دارای کمترین امنیت می‌باشند و اطلاعات را به صورت فاش در طول شبکه ارسال می‌کنند. در حالی که SCP از SSH برای احراز اصالت و رمزنگاری استفاده می‌کند. پروتکل TFTP دارای مکانیزم احراز

اصالت نمی‌باشد در صورتی که FTP با استفاده از درخواست نام کاربری و رمزعبور، کاربران را احراز اصالت می‌کند.

توصیه می‌شود که از پروتکل SCP برای انتقال فایل استفاده شود. البته برای استفاده از این پروتکل باید قبلاً SSH به طور صحیح بر روی تجهیز پیکربندی شده باشد. با استفاده از دستور زیر می‌توان پروتکل SCP را بر روی یک تجهیز سیسکو فعال کرد:

```
Router(config)# ip scp server enable
```

همچنین برای حصول اطمینان از دسترسی تنها کاربران احراز اصالت شده و مجاز به SCP باید تنظیمات لازم در AAA انجام شود.

```
!AAA authentication and authorization must be configured properly for SCP to work.
aaa new-model
aaa authorization exec default group tacacs-group local
aaa authorization exec default group tacacs-group local
username <admin-user> privilege 15 password <password>
!SSH must be configured and functioning properly.
ip ssh time-out 120
ip ssh authentication-retries 3
```

تاییدیه نرم‌افزار

برای بررسی IOS فعلی یک تجهیز سیسکو و اطمینان از معتبر بودن آن، باید از دستورات زیر استفاده کرد. این کار در واقع با مقایسه مقدار MD5 سیستم عامل فعلی با مقدار اصلی که باید داشته باشد، انجام می‌گیرد.

برای بررسی خودکار معتبر بودن IOS سیسکو از دستورات زیر باید استفاده کرد:

```
Router(config)# file verify auto
```

و برای انجام این کار به صورت دستی از دستور زیر استفاده می‌شود:

```
Router# verify location://image
```