بسمه تعالی

مرکز مدیریت راهبردی افتا

عنوان

دستورالعمل پیکربندی امن مسیریاب

گروه زیر ساخت امن

تیرماه ۱۳۹۳

فهرست

۱. مقدمه

امنیت مسیریاب[۱] شامل محافظت خود شبکه به وسیله‌ی مقاوم یا امن کردن مسیریاب‌ها می‌باشد. به طور خاص امن‌سازی مسیریاب از فعالیت مهاجمین در موارد زیر جلوگیری می‌کند:

- بکارگیری مسیریاب‌ها جهت بدست آوردن اطلاعات در مورد شبکه و استفاده از این اطلاعات در برآوردن یک حمله (نشتی اطلاعات)
- از کار انداختن مسیریاب‌ها و در نتیجه شبکه
- پیکربندی مجدد مسیریاب‌ها
- بکارگیری مسیریاب‌ها جهت انجام حمله‌های داخلی
- بکارگیری مسیریاب‌ها جهت انجام حمله‌های خارجی

وظیفه‌ی اصلی مسیریاب‌ها هدایت بسته‌های IP می‌باشد. هر شبکه‌ای که به اینترنت متصل است، اتصالش از طریق یک مسیریاب می‌باشد. برخی از آن‌ها ممکن است سیستم‌عامل‌های لینوکس باشند که نقش مسیریاب را بازی می‌کنند و برخی دیگر ممکن است دیواره‌های آتشی باشند که مسیریابی هم انجام می‌دهند، اما اغلب آن‌ها مسیریاب‌های اختصاصی سیسکو می‌باشند. آمارهای کنونی نشان می‌دهند که ۸۰ درصد اینترنت از طریق تجهیزات سیسکو اجرا می‌شود.

مسیریاب‌ها صرفا بنیان و اساس اینترنت نیستند؛ آن‌ها اساس چگونگی ارتباطات داخلی و خارجی شرکت شما نیز می‌باشند. علاوه بر این، در حال حاضر گرایش زیادی به سمت ادغام صدا، داده، و حتی تصویر متحرک (ویدئو) بر روی شبکه‌ای که IP را اجرا می‌کند وجود دارد. با این شرایط، مسیریاب‌ها در حال تبدیل شدن به بنیانی برای ارتباطات داده، صدا و تصویر متحرک می‌باشند. با این همگرایی، اغلب اطلاعات یک شرکت از طریق مسیریاب‌ها گذر خواهد کرد که موجب می‌گردد مسیریاب‌ها به هدف‌های بی‌نهایت جذابی تبدیل شوند.

---

[۱] Router

قبل از مطالعه و اجرای این سند، نکات زیر باید مورد توجه قرار گیرد:

- از آن‌جا که ممکن است تنظیمات امن‌سازی، کارکردهای سیستم را مختل یا غیرفعال کند، لازم است قبل از اجرای تنظیمات، یک نسخه پشتیبان از پیکربندی سیستم تهیه شود.
- برای اجرای الزامات تعیین شده در این سند، اولویت با خط‌مشی‌های سازمان است. به عبارت دیگر اگر برخی از الزامات بیان شده در این سند، با خط‌مشی‌های سازمان تداخل یا تضاد داشت، اولویت با خط‌مشی‌های سازمان است.
- در تهیه این سند، سعی شده است که حداکثر الزامات مرتبط با حوزه‌ی سند، پوشش داده شود. اما این بدان معنا نیست که پس از اجرای این الزامات، سیستم به صورت صد در صد امن خواهد بود. الزامات بیان شده در این سند، حداقل انتظارات برای امن‌سازی در حوزه‌ی تعریف شده در این مستند است.

۱,۱ تهدیدات

قبل از هر حمله‌ای، مهاجمین تا جایی که امکان دارد در مورد یک شرکت، شبکه و مسیریاب‌هایش اطلاعات جمع‌آوری می‌کنند. هر چه اطلاعاتی که یک مهاجم بتواند جمع‌آوری کند بیشتر باشد، راحت‌تر می‌تواند یک سایت[۲] را در معرض خطر قرار دهد. به این نوع جمع‌آوری اطلاعات، یافتن‌ردپا[۳] اطلاق می‌شود و به هنگام یافتن-ردپا، به طور معمول از مسیریاب‌ها بهره گرفته می‌شود. با پیکربندی‌های پیش‌فرض[۴]، یک مهاجم می‌تواند مسیریاب‌ها را جستجو کرده و نقشه کل شبکه اعم از زیرشبکه‌ها[۵]، الگوهای آدرس‌دهی[۶] و مسیرهای افزونه[۷] را به دست‌آورد.

---

[۲] Site
[۳] Footprinting
[۴] Default
[۵] Subnets
[۶] Addressing Schemes
[۷] Redundant Paths

همه سازمان‌های متصل به شبکه همواره در حال نبرد جهت محافظت منابع و اطلاعاتشان می‌باشند. ارتباط امن برای بقای یک سازمان به اندازه‌ی یک ارتباط امن در یک جنگ نظامی اهمیت دارد. از طرفی مسیریاب‌ها رسانه-های ارتباطی در سازمان‌ها می‌باشند. از اینرو عواقب به خطر افتادن مسیریاب‌ها می‌تواند مهلک و خطرناک باشد. در نتیجه‌ی به خطر افتادن مسیریاب‌های یک سازمان مهاجم می‌تواند:

۱,۱,۱ ناتوان‌سازی شبکه‌ی داخلی

مهاجمین می‌توانند از طریق جمع‌آوری اطلاعات، متوجه از دست رفتن بهره‌وری شبکه شده و از این موضوع بهره برند. تصور کنید اگر مهاجمین توانایی ترمیم[۸] پسورد را از بین برده، پسوردهای مسیریاب‌ها را تغییر داده و پیکربندی‌ها را حذف کنند، چه مدت زمان جهت تعمیر شبکه طول خواهد کشید.

۲,۱,۱ بکارگیری مسیریاب‌ها جهت حمله به سامانه‌های داخلی

مسیریاب‌ها می‌توانند یک جای‌پا[۹] داخل شبکه به مهاجمین بدهند. به سبب آن، با گرفتن کنترل مسیریاب‌ها مهاجمین اغلب از سامانه‌های تشخیص نفوذ عبور کرده، مسیریاب‌ها را جهت دسترسی به شبکه بکار بسته و از هر گونه ورود به سیستم و نظارت بر شبکه جلوگیری می‌کنند.

۳,۱,۱ بکارگیری مسیریاب‌ها جهت حمله به سایت‌های دیگر

هکرها معمولا خواهان پنهان‌سازی مسیر خود هستند. از اینرو مسیر خود را به چندین سامانه‌ی متصل به شبکه-ی دیگر شکسته و از آن سامانه‌ها جهت راه‌اندازی حمله‌های دیگر استفاده می‌کند. دنبال کردن حمله‌ها وقتی از شش یا هفت سرور بگذرد دشوار می‌شود. علاوه بر آن از آنجایی که مسیریاب‌ها حفاظت و ورود کمتری نسبت به

---

[۸] Recovery

[۹] Foothold

سرورها دارند حمله از طریق شش یا هفت مسیریاب به شدت سخت و بررسی آن پرهزینه است. برای سازمان-هایی با مسیریاب‌های ناامن و بدون نظارت، مهاجم یا به میزان کم یا اصلا دنبال نمی‌شود.

۴,۱,۱ تغییر مسیر همه‌ی ترافیک ورودی و خروجی شبکه

مسیریاب‌های قربانی، اجازه‌ی تغییر مسیر ترافیک را به مهاجم می‌دهند. سپس مهاجم می‌تواند ترافیک تغییر مسیر داده شده را مشاهده، ثبت و اصلاح کند.

۲,۱ دامنه

در این متن هدف بررسی عوامل به خطر انداختن مسیریاب‌های شبکه و به موجب آن تهدیدات ایجاد شده برای شبکه، پرداخته می‌شود. در این راستا در ادامه پیشنهادات امنیتی جهت امن‌سازی مسیریاب‌های شبکه ارائه شده است.

۳,۱ اصطلاحات

مهمترین اصطلاحاتی که در این مستند استفاده شده اند عبارتند از:

۱,۳,۱ AAA (Authentication, Authorization, Accounting)

تأیید هویت، مجوز دسترسی، حساب‌رسی : چارچوب سرویسی‌های امنیتی سیسکو است که روشی را برای شناسایی کاربران (تأیید هویت) به منظور کنترل دسترسی (مجوز دسترسی) و جمع‌آوری و ارسال اطلاعات سرور امنیتی برای صدور صورت‌حساب، ممیزی و گزارش‌گیری (حساب‌رسی) تأمین می‌نماید.

۲,۳,۱ ACL (Access Control List)

لیست کنترل دسترسی : فیلتری است بر روی یک سیستم شبکه، که مشخص می‌کند یک ارتباط شبکه اجازه عبور دارد یا خیر.

۳,۳,۱ ARP (Address Resolution Protocol)

پروتکل تفکیک آدرس: یک پروتکل TCP/IP است که برای بدست آوردن آدرس فیزیکی یک نود استفاده می‌شود.

۴,۳,۱ CDP (Cisco Discovery Protocol)

پروتکل کشف سیسکو: یک پروتکل لایه دو است که بر روی اغلب محصولات سیسکو (مانند مسیریاب‌ها، سوئیچ‌ها و سرورهای دسترسی) اجرا می‌شود و مدیر شبکه با استفاده از آن می‌تواند اطلاعات تمام سیستم‌های سیسکو بر روی یک زیرشبکه داده شده را مشاهده کند.

۵,۳,۱ DNS (Domain Name System)

سیستم نام دامنه: پروتکلی است که نام‌های دامنه را به آدرس‌های IP ترجمه می‌کند.

۶,۳,۱ IOS (Internetworking Operating System)

سیستم‌عاملی است که بر روی بسیاری از مسیریاب‌ها و سوئیچ‌های سیسکو مورد استفاده قرار می‌گیرد.

۷,۳,۱ LAN (Local Area Network)

شبکه محلی: یک شبکه کامپیوتری است که منطقه نسبتاً کوچکی را دربرمی‌گیرد.

(Message Digest algorithm 5) MD5 ۸,۳,۱

الگوریتم چکیده پیام: الگوریتم کنترلی رمزنگاری که به طور گسترده‌ای مورد استفاده قرار می‌گیرد.

(Network Time Protocol) NTP ۹,۳,۱

پروتکل زمان شبکه: پروتکلی است که برای همزمان‌سازی کلاک یک کامپیوتر با یک سرور زمانی مورد اعتماد استفاده می‌شود.

(Remote Authentication Dial-in User Service) RADIUS ۱۰,۳,۱

یک سیستم کلاینت/سرور توزیع شده است که شبکه‌ها را در مقابل دسترسی‌های غیرمجاز امن می‌کند.

(Terminal Access Controller Access Control System +) TACACS+ ۱۱,۳,۱

یک پروتکل امنیتی برای تأیید هویت است که مکانیسم متمرکز AAA را برای کاربری که می‌خواهد به یک روتر یا سرور دسترسی پیدا کند، فراهم می‌نماید.

(Simple Network Management Protocol) SNMP ۱۲,۳,۱

پروتکل آسان مدیریت شبکه: پروتکل لایه کاربرد است که امکان تبادل اطلاعات مدیریتی را بین عناصر شبکه ایجاد می‌کند و در واقع قسمتی از پروتکل TCP/IP است. این پروتکل توانایی مدیریت و پیدا کردن مشکلات و حل آن‌ها را در شبکه برای مدیران فراهم می‌نماید و بطور گسترده برای کنترل و مانیتورینگ شبکه مورد استفاده قرار می‌گیرد.

(Secure Shell) SSH ۱۳,۳,۱

شِل امن: پروتکل و رابطی بر مبنای خط فرمان یونیکس است که یک دسترسی امن به سیستم را از راه دور میسر می‌سازد.

Syslog ۱۴,۳,۱

یک پروتکل UDP ساده که توسط سیستم‌های مبتنی بر یونیکس و مسیریاب‌های سیسکو برای عملیات لاگ‌گیری مورد استفاده قرار می‌گیرد.

(Unicast Reverse Packet Forwarding) URPF ۱۵,۳,۱

ارسال معکوس بسته‌ها بصورت تک‌پخشی: ویژگی است که توسط شرکت سیسکو طراحی شده است تا عملیات ضدجعل بر روی مسیریاب‌ها را، راحت‌تر مدیریت و نظارت نماید و از حملات جعل جلوگیری کند.

(Virtual TeletYpe) VTY ۱۶,۳,۱

رابطی است بر روی یک میزبان یا مسیریاب که سرویس‌های تعاملی یک ترمینال را فراهم می‌کند.

۲. امن‌سازی مسیریاب

در این بخش به روش‌های گوناگون امن سازی زیرساخت شبکه پرداخته می‌شود.

۱,۲ امن سازی سیستم‌عامل مسیریاب

لازم است تا مسیریاب از آخرین نسخه سیستم‌عامل (IOS) موجود استفاده و کاربر از صحت این سیستم عامل اطمینان حاصل نماید. همچنین کاربر باید از آخرین آسیب‌پذیری‌های گزارش شده در مورد سیستم‌عامل موجود بر روی مسیریاب خود اطلاع پیدا کرده و اقدامات لازم برای رفع آن‌ها را انجام دهد.

۲,۲ اعمال کنترل دسترسی‌های اولیه

مسیریاب مکانیزم‌های کنترل دسترسی گوناگونی در اختیار مدیر شبکه جهت مدیریت مسیریاب قرار می‌دهد. در این زمینه لازم است تا در گام اول دسترسی فیزیکی به مسیریاب، دسترسی به قابلیت پیکربندی تجهیز و دسترسی از طریق کنسول امن گردیده و همچنین دسترسی از طریق پورت AUX و VTY امن و یا غیرفعال شود. روشهای امن نمودن موجود معمولا فعال‌سازی، تعریف نام‌کاربری و کلمه عبور می‌باشد.

- در مسیریاب لازم است ذخیره‌سازی کلمات عبور بصورت رمز شده بوده و در صورتی که در سازمانی مدیران مختلف اجازه تغییر پیکربندی مسیریاب را داشته باشند، برای هر کدام نام کاربری و کلمه عبور مجزا تعریف شود.
- در مسیریاب لازم است مکانیزم مدیریت احراز هویت TACACS استفاده نشود.
- مسیریاب نباید قابلیت بارکردن اتوماتیک پیکربندی از طریق TFTP را داشته و نیز به عنوان TFTP Server پیکربندی شود.
- در صورت امکان دسترسی از طریق dial-up، لازم است پورت‌های مودم و AUX به وسیله کلمه عبور حفاظت شده و نیز callback security پیکربندی شود.
- لازم به ذکر است هرگز مودم به پورت کنسول وصل نشود.

- در ارتباطات از راه دور لازم است، پس از مدت زمانی غیر فعال بودن این ارتباط قطع شده و محدوده آدرس‌های افرادی که حق پیکربندی از راه دور از طریق ssh و یا http را دارند مشخص و پیکربندی شوند.
- لازم است بر روی خطوط VTY، Telnet غیرفعال و از SSH استفاده شود. (Telnet معکوس بر روی تمامی پورت‌های فیزیکی غیرفعال شود.)
- بهتر است دسترسی HTTP به مسیریاب غیرفعال شود. اما در صورت نیاز دسترسی HTTP به مسیریاب، لازم است استفاده از آن و دسترسی آن از طریق ACLها به تعداد اندکی IP امن محدود و فقط در بستر IPSec استفاده شود.
- لازم است روش تأیید هویت HTTP از کلمه عبور enable پیش‌فرض تغییر کند.

۳,۲ کلمه عبور

- در تمامی مسیریاب‌ها سرویس رمزنگاری کلمه عبور (service password-encryption) را فعال نمایید.
- فایل‌های پیکربندی پشتیبان را رمز کنید و در یک سرور امن نگهداری نمایید.
- باید از پسوردهای پیچیده استفاده شود به نحوی که حدس زدن آن‌ها مشکل باشد.
- مطمئن شوید که هر مسیریاب کلمه عبور متفاوتی برای enable و کاربر داشته باشد.
- فقط از طریق یک سیستم امن و مطمئن به مسیریاب‌ها دسترسی پیدا کنید.
- در سازمان‌های بزرگ که تعداد زیادی از کارمندها به مسیریاب دسترسی دارند، برای محدود کردن دسترسی به فرامین غیرضروری از سطوح دسترسی اضافه‌تر (Privilege Level : 2-14) استفاده کنید.

۴,۲ AAA (Authentication, Authorization, Accounting)

- اگر از پروتکل AAA استفاده شود لازم است هر زمان که امکان داشت به جای سایر روش‌ها از روش +TACACS استفاده و اگر از +TACACS یا RADIUS استفاده می‌شود، فایل‌های پیکربندی امن نگه داشته شود.
- اگر از تأیید هویت AAA استفاده شود، لازم است روش پشتیبان برای تأیید هویت نام‌های کاربری پیکربندی شده محلی یا کلمه عبور پیش‌فرض Privilege تنظیم شود.
- اگر از تأیید مجوز AAA استفاده شود لازم است امنیت از متوسط به پایین و روش پشتیبان برای تأیید مجوز if-authenticated (برای اجتناب از تحریم شدن توسط مسیریاب) و اگر سطح بالاتری از امنیت نیاز است، لازم است روش پشتیبان برای تأیید مجوز وجود نداشته باشد.
- لازم است دسترسی HTTP غیرفعال شود. اما اگر باید از HTTP استفاده شود، به جای آن از +TACACS یا RADIUS استفاده شود و کلمه عبور Privilege برای تأیید هویت در حالت پیش‌فرض قرار نگیرد. در ضمن در سازمان‌های بزرگ که کنترل دسترسی دو عامله نیاز است، لازم است سرورهای +TACACS یا RADIUS مسیریاب برای استفاده در کنترل دسترسی‌های مبتنی بر توکن پیکربندی شوند.

۵,۲ پیغام‌های هشدار

لازم است که هر مسیریاب پیغام‌های هشدار متناسب شامل عبارت‌های زیر داشته باشد:

- The router is for authorized personnel only (مسیریاب فقط برای کارمندها مجاز است)
- The router is for official use only (مسیریاب فقط برای استفاده رسمی است)
- Users have no expectations of privacy (کاربران انتظارات خصوصی ندارند)

- All access and use may (not will) be monitored and/or recorded (تمامی دسترسی‌ها و کاربری‌ها ممکن است مانیتور و یا ثبت شوند)
- Monitoring and/or recording may be turned over to the appropriate authorities (ممکن است مانیتورینگ و ثبت به متصدیان مقتضی برگردانده شود.)
- Use of the system implies consent to the previously mentioned conditions (استفاده از سیستم دلالت بر موافقت با شرایط مذکور اخیر دارد)

لازم است پیغام‌های هشدار در هیچ کجا عبارت خوش‌آمدید را بیان نکرده، شامل هیچ یک از اطلاعات شناسایی مرتبط با مسیریاب، مدیران یا سازمان بکاربرنده مسیریاب نباشند و نیز با بررسی الزامات قانونی محلی مطمئنا شامل تمامی زبان و محتویات مورد نیاز باشند.

بهتر است از دستور banner login برای نمایش پیغام تلاش یک کابر زمانی که می‌خواهد به سیستم ورود کند و از دستور banner exec برای نمایش پیغام بار دوم هر زمان که یک کابر یک فایل اجرایی یا shell را اجرا می‌کند، استفاده شود.

۶,۲ سرویس‌ها و پروتکل‌های غیرضروری

لازم است سرویس‌های زیر بر روی همه واسط‌های کاربری در تمام مسیریاب‌ها غیرفعال شود:

- ICMP redirects
- ICMP broadcasts
- ICMP mask replies
- ICMP unreachables
- Proxy ARP
- CDP
- source routing
- small services

- Finger

سرویس‌های متفرقه از قبیل موارد زیر و نیز دسترسی به HTTP و SNMP لازم است غیرفعال شود:

- BOOTP
- PAD
- configuration auto loading
- DNS

شایان ذکر است بهتر است بسته‌های ورودی ICMP با استفاده از ACL مناسب محدود شود.

SNMP ۷,۲

درصورتیکه SNMP لازم نباشد و نیز دسترسی خواندن و نوشتن SNMP جز در موارد کاملاً ضروری، غیرفعال شود. اگر دسترسی خواندن و نوشتن SNMP پیکربندی شده است، از دستور snmp-server tftp-server-list برای محدود ساختن انتقالات SNMP و TFTP استفاده شود. در ضمن بهتر است تمام سرورهای مدیریت SNMP امن شود.

در صورت امکان از دنباله‌های تأیید هویت متفاوت برای هر مسیریاب استفاده شود. در ضمن کلمه‌های عبور به طور مناسب انتخاب شده و به راحتی حدس زده نشوند.

لازم است تمام دسترسی‌های SNMP به هاست‌های ویژه از طریق ACLها و نیز تمام خروجی‌های SNMP از طریق استفاده از viewها محدود شود.

زمانیکه SNMP v3 وجود دارد، لازم است SNMP v1 و SNMP v2c غیرفعال شود و نکات زیر در مورد SNMP v3مورد توجه قرار گیرد:

- اطمینان از غیرفعال بودن SNMP v1 و SNMP v2c .
- لزوم استفاده از هر دو پارامتر رمزنگاری و تأیید هویت بر روی مسیریاب‌ها.
- استفاده از viewها برای محدود کردن دسترسی SNMP به اطلاعات.

۸,۲ پروتکل مسیریابی و ضدجعل

در مرز هر مسیریاب با یک شبکه خارجی لازم است اقدامات ضدجعل زیر انجام شود:

- ip verify unicast reverse-path (مسیر معکوس تک‌پخشی تأیید ip) در تمامی رابطهایی که به شبکه‌های خارجی متصل می‌شوند و شامل مسیریابی نامتقارن نمی‌باشند، فعال شود.
- اگر نمی‌شود از uRPF استفاده شود، لیست‌های کنترل دسترسی ورود و خروج ضدجعل به تمام رابط‌های متصل به یک شبکه خارجی، اعمال شود.
- اگر شبکه بسیار کوچک است و یا به امنیت بیشتری نیاز دارد، از مسیریابی استاتیک استفاده شود.

به هنگام استفاده از یک پروتکل مسیریابی، انتخاب یکی از موارد زیر که فرآیند تأیید هویت بر روی تمام مسیریاب‌های شبکه را پشتیبانی و فعال می‌نماید لازم است:

- کلمه عبور مناسب برای تأیید هویت انتخاب و اطمینان حاصل شود که کنترل‌ها در جایی به منظور امنیت کلمات عبور تأیید هویت، نگهداری می‌شوند.
- از پروتکل‌های توابع درهم‌ساز امن مانند MD5 برای تأیید هویت استفاده شود.

به منظور جلوگیری از تزریق اطلاعات غلط مسیریابی به شبکه، در مرزهای شبکه که توسط افراد دیگری کنترل می‌شوند، از فیلترهای مسیریاب استفاده شود.

NTP ۹,۲

تمامی مسیریاب‌ها لازم است از پروتکل NTP برای همزمان‌سازی استفاده کرده و نیز لیست‌های کنترل دسترسی که از تبدیل شدن آن‌ها به سرورهای عمومی همگام‌سازی زمان جلوگیری می‌کند داشته باشند.

با توجه به این که در شبکه‌های بزرگتر زمان دقیق‌تری لازم است، برای جلوگیری از یک نقطه شکست مشترک، برای چندین سرور از سرورهای زمانی افزونه و همزمان کردن مسیریاب‌ها استفاده شود.

فقط زمانیکه همگام‌سازی زمان خارجی امکان‌پذیر نیست از دستور ntp master (مثلاً در شبکه‌هایی که به اینترنت وصل نمی‌شوند) و نیز بین کلاینت‌ها، سرورها و جفت‌های مشابه از تأیید هویت NTP استفاده شود تا اطمینان حاصل شود که فقط برای سرورهای تأیید شده، همزمان‌سازی انجام شده است.

۱۰,۲ لاگ کردن

در این قسمت ابتدا لازم است تمامی لاگ‌هایی که دلالت بر حملات، پیکربندی‌های اشتباه و خرابی‌ها دارند بطور فعال مانیتور و برچسب‌های زمانی لاگ‌ها طوری که دربردارنده میلی‌ثانیه‌ها باشد پیکربندی شود.

در فرایند لاگ کردن لازم است RAM buffer logging و logging sequence numbers فعال شوند.

جهت حفظ پیام‌ها مسیریاب‌ها برای ارسال لاگ‌ها به سرور syslog پیکربندی می‌شوند. در این راستا اطمینان از ارسال لاگ‌های مسیریاب به چندین سرور syslog به منظور حفظ افزونگی در سایت‌هایی که سطوح بالاتری از امنیت و قابلیت ممیزی را احتیاج دارند و نیز فیلتر کردن پیام‌های syslog سیستم‌های خارجی از طریق لیست‌های کنترل دسترسی، در مرز شبکه خود یا از طریق خود سرور syslog لازم می‌باشد.

به منظور ثبت تخلفات دسترسی لازم است لیست‌های کنترل دسترسی کلید پیکربندی شود. لیست کنترل دسترسی پیشنهادی شامل موارد زیر می‌باشد:

- تخلفات ضد جعل
- تلاش‌های دسترسی به VTY
- تلاش‌های دسترسی به HTTP
- تلاش‌های دسترسی به SNMP

- تخلفات فیلتر مسیریابی
- تخلفات ICMP

در محیط‌هایی که امنیت بیشتری مورد نیاز است لازم است از AAA استفاده و بخش حساب‌رسی آن فعال شود. در این راستا لزوم پیکربندی EXEC، سیستم، ارتباط و حساب‌رسی شبکه برای ثبت اطلاعات رخدادهای سیستم و نشست‌های کاربر و نیز بخش حساب‌رسی AAA برای ثبت خطاهای تأیید هویت مشهود است. در ضمن اگر لازم بود یک رکورد از هر دستور اجرا شده بر روی مسیریاب ثبت شود، بخش حساب‌رسی دستور پیکربندی شود.

۳. چک لیست

در این بخش به ارائه چک لیست پیکربندی امن مسیریاب سیسکو پرداخته می‌شود.

بند	توصیه امنیتی	√
امن‌سازی سیستم‌عامل مسیریاب		
۱	بایستی مسیریاب‌ها از آخرین نسخه IOS موجود استفاده کنند.	
۲	بایستی کاربر از صحت سیستم عامل اطمینان حاصل نماید.	
۳	بایستی اقدامات لازم برای رفع آخرین آسیب‌پذیری‌های گزارش شده بر روی نسخه IOS موجود انجام شود.	
اعمال کنترل دسترسی		
۴	لازم است ذخیره‌سازی کلمات در مسیریاب عبور بصورت رمز شده باشد.	
۵	لازم است مکانیزم مدیریت احراز هویت TACACS در مسیریاب استفاده نشود.	
۶	مسیریاب نباید قابلیت بارکردن اتوماتیک پیکربندی از طریق TFTP را داشته باشد.	
۷	مسیریاب نباید به عنوان TFTP Server پیکربندی شود.	
۸	در صورت امکان دسترسی از طریق dial-up، لازم است پورت‌های مودم و AUX به وسیله کلمه عبور حفاظت شده و نیز callback security پیکربندی شود.	
۹	نباید مودم به پورت کنسول وصل شود.	

۱۰	در ارتباطات از راه دور بایستی، پس از مدت زمانی غیر فعال بودن این ارتباط قطع شود.	
۱۱	محدوده آدرس‌های افرادی که حق پیکربندی از راه دور از طریق ssh و یا http را دارند بایستی مشخص و پیکربندی شود.	
۱۲	لازم است بر روی خطوط VTY، Telnet غیرفعال و از SSH استفاده شود.	
۱۳	بایستی دسترسی HTTP به مسیریاب غیرفعال شود. اما در صورت نیاز دسترسی HTTP به مسیریاب، لازم است استفاده از آن و دسترسی آن از طریق ACLها به تعداد اندکی IP امن محدود و فقط در بستر IPSec استفاده شود.	
۱۴	لازم است روش تأیید هویت HTTP از کلمه عبور enable پیش‌فرض تغییر کند.	
کلمه عبور		
۱۵	لازم است در تمامی مسیریاب‌ها سرویس رمزنگاری کلمه عبور (service password-encryption) فعال شود.	
۱۶	فایل‌های پیکربندی پشتیبان بایستی رمز و در یک سرور امن نگهداری شود.	
۱۷	باید از پسوردهای پیچیده استفاده شود به نحوی که حدس زدن آن‌ها مشکل باشد.	
۱۸	بایستی هر مسیریاب کلمه عبور متفاوتی برای enable و کاربر داشته باشد.	
۱۹	بایستی فقط از طریق یک سیستم امن و مطمئن به مسیریاب‌ها دسترسی داشت.	

۲۰	لازم است برای محدود کردن دسترسی به فرامین غیرضروری از سطوح دسترسی اضافه‌تر استفاده شود.	
AAA		
۲۱	اگر از پروتکل AAA استفاده شود لازم است هر زمان که امکان داشت به جای سایر روش‌ها از روش +TACACS استفاده و اگر از +TACACS یا RADIUS استفاده می‌شود، فایل‌های پیکربندی امن نگه داشته شود.	
۲۲	اگر از تأیید هویت AAA استفاده شود، لازم است روش پشتیبان برای تأیید هویت نام‌های کاربری پیکربندی شده محلی یا کلمه عبور پیش‌فرض Privilege تنظیم شود.	
۲۳	اگر از تأیید مجوز AAA استفاده شود لازم است امنیت از متوسط به پایین و روش پشتیبان برای تأیید مجوز if-authenticated وجود داشته باشد.	
۲۴	در سازمان‌های بزرگ که کنترل دسترسی دو عامله نیاز است، لازم است سرورهای +TACACSیا RADIUS مسیریاب برای استفاده در کنترل دسترسی‌های مبتنی بر توکن پیکربندی شوند.	
پیغام‌های هشدار		
۲۵	لازم است که هر مسیریاب پیغام‌های هشدار متناسب داشته باشد.	
۲۶	لازم است پیغام‌های هشدار شامل هیچ یک از اطلاعات شناسایی مرتبط با مسیریاب، مدیران یا سازمان بکاربرنده مسیریاب نباشند.	

۲۷	لازم است پیغام‌های هشدار با بررسی الزامات قانونی محلی شامل تمامی زبان و محتویات مورد نیاز باشند.	
۲۸	بایستی از دستور banner login برای نمایش پیغام تلاش یک کابر زمانی که می‌خواهد به سیستم ورود کند، استفاده شود.	
۲۹	بایستی از دستور banner exec برای نمایش پیغام بار دوم هر زمان که یک کابر یک فایل اجرایی یا shell را اجرا می‌کند، استفاده شود.	
سرویس‌ها و پروتکل‌های غیرضروری		
۳۰	لازم است سرویس‌های ICMP broadcasts، ICMP mask replies، ICMP unreachables، Proxy ARP، CDP، source routing، small services، Finger بر روی همه واسط‌های کاربری در تمام مسیریاب‌ها غیرفعال شود.	
۳۱	دسترسی به HTTP و SNMP بایستی غیرفعال شود.	
SNMP		
۳۲	درصورتیکه SNMP لازم نباشد و دسترسی خواندن و نوشتن SNMP ، جز در موارد کاملاً ضروری، بایستی غیرفعال شود.	
۳۳	اگر دسترسی خواندن و نوشتن SNMP پیکربندی شده است، بایستی از دستور snmp-server tftp-server-list برای محدود ساختن انتقالات SNMP و TFTP استفاده شود.	

۳۴	لازم است تمام سرورهای مدیریت SNMP امن شود.	
۳۵	لازم است تمام دسترسی‌های SNMP به هاست‌های ویژه از طریق ACLها و نیز تمام خروجی‌های SNMP از طریق استفاده از viewها محدود شود.	
۳۶	زمانیکه SNMP v3 وجود دارد، لازم است SNMP v1 و SNMP v2c غیرفعال شود.	
۳۷	زمانیکه SNMP v3 وجود دارد، لازم است از هر دو پارامتر رمزنگاری و تأیید هویت بر روی مسیریاب‌ها استفاده شود.	
۳۸	زمانیکه SNMP v3 وجود دارد، لازم است از viewها برای محدود کردن دسترسی SNMP به اطلاعات استفاده شود.	
پروتکل‌های مسیریابی و ضدجعل		
۳۹	لازم است ip verify unicast reverse-path در تمامی رابط‌هایی که به شبکه‌های خارجی متصل می‌شوند و شامل مسیریابی نامتقارن نمی‌باشند، فعال شود.	
۴۰	اگر نمی‌شود از uRPF استفاده شود، بایستی لیست‌های کنترل دسترسی ورود و خروج ضدجعل به تمام رابط‌های متصل به یک شبکه خارجی، اعمال شود.	
۴۱	اگر شبکه بسیار کوچک است و یا به امنیت بیشتری نیاز دارد، بایستی از مسیریابی استاتیک استفاده شود.	

۴۲	به هنگام استفاده از یک پروتکل مسیریابی، لازم است کلمه عبور مناسب برای تأیید هویت انتخاب و کنترل‌ها در جایی به منظور امنیت کلمات عبور تأیید هویت، نگهداری شوند.	
۴۳	به هنگام استفاده از یک پروتکل مسیریابی، لازم است از پروتکل‌های توابع درهم‌ساز امن مانند MD5 برای تأیید هویت استفاده شود.	
۴۴	به منظور جلوگیری از تزریق اطلاعات غلط مسیریابی به شبکه، لازم است در مرزهای شبکه که توسط افراد دیگری کنترل می‌شوند، از فیلترهای مسیریاب استفاده شود.	
NTP		
۴۵	لازم است مسیریاب‌ها از پروتکل NTP برای همزمان‌سازی استفاده کنند.	
۴۶	لازم است مسیریاب‌ها لیست‌های کنترل دسترسی که از تبدیل شدن آن‌ها به سرورهای عمومی همگام‌سازی زمان جلوگیری می‌کند داشته باشند.	
۴۷	برای جلوگیری از یک نقطه شکست مشترک، بایستی برای چندین سرور از سرورهای زمانی افزونه و همزمان کردن مسیریاب‌ها استفاده شود.	
۴۸	لازم است فقط زمانیکه همگام‌سازی زمان خارجی امکان‌پذیر نیست از دستور ntp master و نیز بین کلاینت‌ها، سرورها و جفت‌های مشابه از تأیید هویت NTP استفاده شود تا اطمینان حاصل شود که فقط برای سرورهای تأیید شده، همزمان‌سازی انجام شده است.	
لاگ کردن		

۴۹	لازم است تمامی لاگ‌هایی که دلالت بر حملات، پیکربندی‌های اشتباه و خرابی‌ها دارند بطور فعال مانیتور و برچسب‌های زمانی لاگ‌ها پیکربندی شود.	
۵۰	لازم است RAM buffer logging و logging sequence numbers فعال شوند.	
۵۱	جهت حفظ پیام‌ها بایستی مسیریاب‌ها برای ارسال لاگ‌ها به سرور syslog پیکربندی شوند.	
۵۲	اطمینان از ارسال لاگ‌های مسیریاب به چندین سرور syslog به منظور حفظ افزونگی در سایت‌هایی که سطوح بالاتری از امنیت و قابلیت ممیزی را احتیاج دارند لازم است.	
۵۳	فیلتر کردن پیام‌های syslog سیستم‌های خارجی از طریق لیست‌های کنترل دسترسی، در مرز شبکه خود یا از طریق خود سرور syslog لازم می‌باشد.	