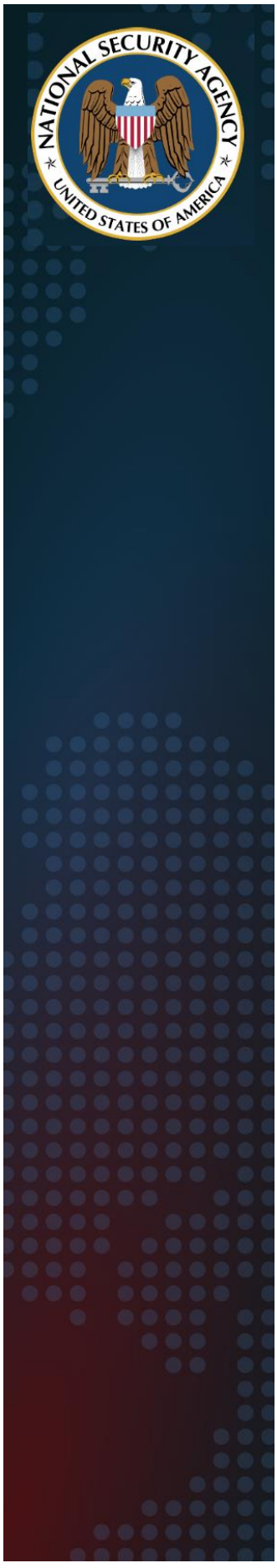

آژانس امنیت ملی ایالات متحده امریکا

گزارش فنی امنیت سایبری

راهنمای امنیت زیرساخت شبکه

ترجمه نیما نادریان

ماه مارچ - ۲۰۲۲

PP-22-0266

Version 1.0

هدف

این سند به منظور پیشبرد ماموریت های امنیت سایبری سازمان امنیت ملی تهیه شده است که شامل مسئولیت‌های آن برای شناسایی و انتشار تهدیدات، علیه سیستم‌های امنیت ملی، سیستم‌های اطلاعاتی وزارت دفاع و پایگاه های صنعتی دفاعی و توسعه و صدور مشخصات و اقدامات منجر به کاهش امنیت سایبری می باشد. این اطلاعات ممکن است به طور گسترده برای دستیابی به همه ذینفعان مرتبط به اشتراک گذاشته شود.

اطلاعات و نظرات موجود در این سند "همانطور که هست" و بدون هیچ گونه تضمینی ارائه شده است. ارجاع به هر یک از محصولات تجاری، فرآیند یا خدمات خاص با نام تجاری، علامت تجاری، سازنده یا موارد دیگر، لزوماً به منزله تأیید، توصیه یا حمایت از آن توسط دولت ایالات متحده نیست و این راهنما نباید برای اهداف تبلیغاتی یا تایید محصول مورد استفاده قرار بگیرد.

فهرست

۱. معرفی

راهنمایی برای ایمن سازی شبکه ها همچنان در حال تکامل است، زیرا آسیب پذیری های جدید توسط دشمنان مورد سوء استفاده قرار می گیرند، ویژگی های امنیتی جدید پیاده سازی می شوند، و روش های جدید ایمن سازی دستگاه ها شناسایی می شوند . پیکربندی نامناسب، مدیریت نادرست پیکربندی‌ها و کلیدهای رمزگذاری ضعیف می‌تواند آسیب‌پذیری‌ها را در کل شبکه آشکار کند . همه شبکه ها در معرض خطر قرار دارند، به خصوص اگر دستگاه ها به درستی پیکربندی و نگهداری نشوند . نقش مدیر برای ایمن سازی شبکه در برابر تکنیک های متخاصم حیاتی است و به افراد متخصص نیاز است تا دستگاه ها، برنامه ها و اطلاعات موجود در شبکه را ایمن کنند .

این گزارش بهترین روش‌ها را برای امنیت کلی شبکه و حفاظت از تجهیزات ارائه می‌کند و به مدیران در جلوگیری از سوء استفاده از شبکه آنها توسط دشمن کمک می‌کند . در حالی که راهنمایی ارائه شده در اینجا عمومی است و می تواند برای بسیاری از انواع دستگاه های شبکه اعمال شود، دستورات نمونه برای دستگاه های دارای سیستم عامل اینترنت ورک سیسکو (IOS) ارائه شده است که می تواند برای پیاده سازی توصیه ها اجرا شود .

۱,۱ در مورد اعتماد صفر (Zero Trust)

Zero Trust یک مدل امنیتی، مجموعه‌ای از اصول طراحی سیستم و یک استراتژی هماهنگ امنیت سایبری و مدیریت سیستم است که بر اساس اذعان به وجود تهدیدها در داخل و خارج از مرزهای شبکه سنتی تعریف شده است .آژانس امنیت ملی (NSA) به طور کامل از مدل امنیتی Zero Trust پشتیبانی می‌کند و بسیاری از راهنمایی‌های این گزارش را می‌توان در مرزهای مختلف همانطور که در راهنمای Zero Trustتوصیه می‌شود، اعمال کرد .با این حال، این گزارش بر ارائه راهنمایی برای کاهش آسیب‌پذیری‌ها و ضعف‌های رایج در شبکه‌های موجود تمرکز دارد .از آنجایی که صاحبان سیستم طرح‌های شبکه جدیدی را معرفی می‌کنند که برای دستیابی به اصول کامل‌تر Zero Trust طراحی شده‌اند، این راهنمایی ممکن است نیاز به اصلاح داشته باشد.

۲. معماری و طراحی شبکه

طراحی شبکه ایمن که طی چندین لایه دفاعی پیاده سازی شده باشد برای دفاع در برابر تهدیدات و حفاظت از منابع درون شبکه بسیار مهم است .طراحی باید از بهترین شیوه‌های امنیتی و مدل‌سازی اصول Zero Trust ، هم برای محیط شبکه و هم برای دستگاه‌های داخلی، پیروی کند.

۲,۱ نصب تجهیزات دفاعی محیطی و داخلی

شبکه به یک استراتژی دفاعی اساسی نیاز دارد تا از اجزای جداگانه و اطلاعاتی که در آنها وجود دارد محافظت کند .برای محافظت در برابر تهدیدات خارجی و نظارت و محدود کردن ترافیک ورودی و خروجی باید چندین لایه دفاعی در محیط شبکه اجرا شود.

NSA پیکربندی و نصب دستگاه های امنیتی در محیط شبکه را با توجه به بهترین شیوه های امنیتی توصیه می کند:

- یک روتر مرزی برای تسهیل اتصال به شبکه خارجی مانند یک ارائه دهنده خدمات اینترنتی (ISP) نصب کنید .

- اجرای چندین لایه از فایروال های نسل بعدی در سراسر شبکه برای محدود کردن ترافیک ورودی، محدود کردن ترافیک خروجی، و بررسی تمام فعالیت های داخلی بین مناطق مختلف شبکه. که هر لایه باید از فروشندگان مختلف برای محافظت در برابر دشمنی که از همان آسیب‌پذیری اصلاح نشده در تلاش برای دسترسی به شبکه داخلی سوء استفاده می‌کند، استفاده کند .سیستم‌های قابل دسترسی عمومی و پراکسی‌های خروجی را در بین لایه‌های فایروال در یک یا چند زیرشبکه منطقه غیرنظامی (DMZ) قرار دهید، جایی که می‌توان دسترسی را بین دستگاه‌های خارجی، دستگاه‌های DMZ و سیستم‌های داخلی به طور مناسب کنترل کرد .یک راه حل نظارت بر شبکه برای ثبت و ردیابی ترافیک ورودی و خروجی، مانند سیستم تشخیص نفوذ شبکه(NIDS) ، بازرس ترافیک، یا دستگاه کپچر کامل پکت، مستقر کنید .

- استقرار چندین سرور ثبت لاگ از راه دور اختصاصی برای فعال کردن همبستگی فعالیت بین تجهیزات

- برای اطمینان از در دسترس بودن، دستگاه‌های اضافی را در نواحی اصلی پیاده‌سازی کنید، که می‌توانند برای افزایش توان شبکه و کاهش تأخیر با بار متعادل شوند.

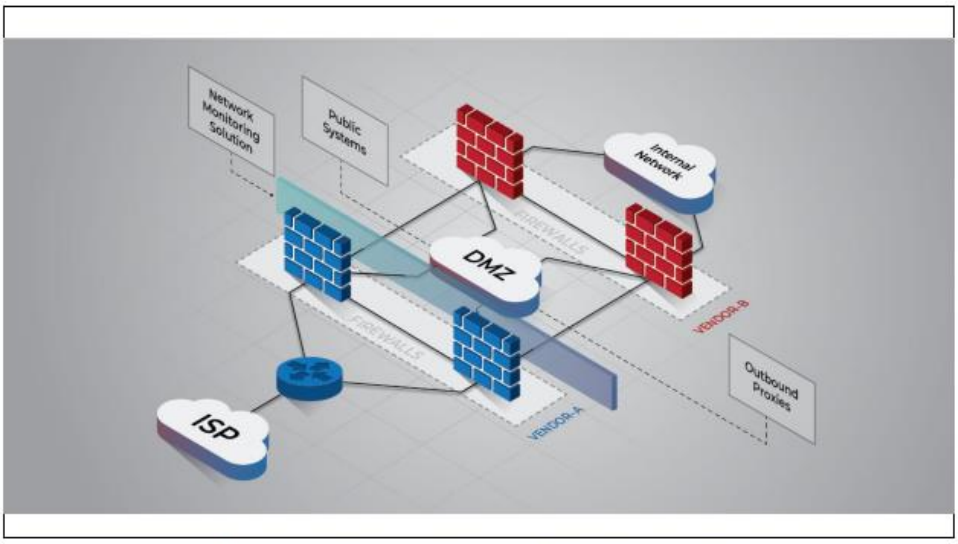

Figure 1: Network perimeter with firewalls and a DMZ

۲,۲ گروه بندی سیستم های شبکه مشابه

سیستم های مشابه در یک شبکه باید به طور منطقی با هم گروه بندی شوند تا در برابر نفوذ از جانب انواع دیگر سیستم ها محافظت شوند .دشمنان سیستم‌هایی را که به راحتی قابل بهره‌برداری هستند، مانند چاپگرها، هدف قرار می‌دهند و از این دسترسی اولیه برای انتشار بیشتر به سیستم‌های دیگر در شبکه استفاده می‌کنند .تقسیم بندی مناسب شبکه به طور قابل توجهی توانایی یک دشمن برای دسترسی و بهره برداری از این سیستم های دیگر را کاهش می دهد. علاوه بر این، این محدودیت‌های دسترسی بین انواع مختلف سیستم‌ها اگر به طور منطقی انجام شود، مدیریت، کنترل و نظارت آسان تر خواهد بود.

NSA توصیه می‌کند سیستم‌های مشابه را در زیرشبکه‌های مختلف یا شبکه‌های محلی مجازی (VLAN) تفکیک کنید، یا زیرشبکه‌های مختلف را از طریق فایروال‌ها یا مسیریاب‌های فیلترکننده جداسازی کنید. کلاینت ها، سرورها، چاپگرها، سیستم های مخابراتی و سایر تجهیزات جانبی شبکه باید از یکدیگر جدا باشند. فناوری عملیاتی، مانند سیستم های کنترل صنعتی، معمولاً باید از سایر فناوری اطلاعات و شبکه های پرخطر مانند اینترنت جدا شود. این جداسازی فیزیکی حفاظت قوی‌تری را فراهم می‌کند زیرا دستگاه میانی بین زیرشبکه‌ها باید به خطر بیفتد تا نفوذگر محدودیت‌های دسترسی را دور بزند. محدودیت‌های دسترسی را روی روترها، سوئیچ‌ها یا فایروال‌های داخلی اعمال کنید تا فقط به پورت‌ها و پروتکل‌هایی اجازه داده شود که برای عملیات شبکه یا نیازهای عملیاتی معتبر مورد نیاز هستند. لیست‌های کنترل دسترسی (ACL) ممکن است نیاز به تکرار داشته باشند و مستقیماً روی سوئیچ‌ها اعمال شوند تا دسترسی بین VLAN ها محدود شود، یا می‌توان آنها را در مسیریاب‌های اصلی که در آن مسیریابی بین زیرشبکه‌های داخلی انجام می‌شود، اعمال کرد.

۲,۳ اتصالات Backdoor را حذف کنید

یک اتصال Backdoor، اتصالی بین دو یا چند دستگاه واقع در مناطق مختلف شبکه است که عموماً تنوع داده و الزامات امنیتی متفاوتی دارد .اگر یک دستگاه در معرض خطر قرار گیرد، دشمن می تواند از این اتصال برای دور زدن محدودیت های دسترسی و دسترسی به سایر مناطق شبکه استفاده کند .نمونه ای از اتصال شبکه Backdoor، روتر لبه شبکه است که به ISP متصل است و مستقیماً به شبکه های داخلی یا مدیریتی نیز متصل است .دشمنی که بتواند این روتر مرز خارجی را به خطر بیاندازد، احتمالاً به شبکه داخلی دسترسی خواهد داشت و تمام فایروال ها را دور می زند. NSA توصیه می کند که تمام اتصالات Backdoor را حذف کنید و هنگام اتصال دستگاه هایی با بیش از یک رابط شبکه، احتیاط کنید . بررسی کنید که تمام رابط های شبکه یک دستگاه در سطوح امنیتی مشابهی هستند یا اینکه یک دستگاه میانی، هم جداسازی منطقی و هم فیزیکی را بین مناطق مختلف شبکه فراهم می کند.

۲,۴ از کنترل های دسترسی محیطی دقیق استفاده کنید

دستگاه‌های محیطی شبکه عناصر ضروری در یک مدل امنیتی هستند و باید به گونه‌ای پیکربندی شوند که با اجرای ACL برای تنظیم ورودی و خروجی ترافیک شبکه، یکدیگر را تکمیل کنند .این قوانین کنترل دسترسی باید به گونه‌ای پیکربندی شوند که به طور صریح فقط به سرویس‌ها و سیستم‌هایی اجازه دهند که برای پشتیبانی از ماموریت شبکه مورد نیاز هستند .اگر فایروال‌ها و مسیریاب‌های محیطی با سیاست‌های امنیتی شبکه کافی پیکربندی نشده باشند، امکان دسترسی غیرضروری به یا از شبکه داخلی را فراهم می‌کند و خطر آسیب شبکه و جمع‌آوری اطلاعات را افزایش می‌دهد. NSA توصیه می‌کند به دقت در نظر بگیرید که کدام اتصال‌ها مجاز هستند، و قوانینی ایجاد کنید که فقط بر اجازه دادن به موارد مجاز و انکار هر چیز دیگری تمرکز کنند .این روش به یک قانون اجازه می دهد تا چندین نوع اتصال را رد کند، به جای اینکه نیاز به ایجاد یک قانون

جداگانه برای هر اتصال مسدود شده باشد . اگر برای جلوگیری از تکمیل یا ادامه تلاش‌ها بهره‌برداری لازم است به‌صورت پویا قوانین محیطی اضافی اعمال شود، NSA استفاده از یک سیستم پیشگیری از نفوذ (IPS) را توصیه می‌کند.

۲,۵ راه حل کنترل دسترسی به شبکه (NAC) را پیاده سازی کنید

نفوذگری که مایل به دسترسی داخلی به یک شبکه است باید یا راهی را از طریق محیط خارجی شبکه بیابد یا از داخل شبکه دسترسی داشته باشد. راه حل NAC از اتصالات فیزیکی غیرمجاز جلوگیری می کند و اتصالات فیزیکی مجاز را در شبکه نظارت می کند. NSA اجرای یک راه حل NAC را توصیه می کند که دستگاه های منحصر به فرد متصل به شبکه را شناسایی و احراز هویت می کند. امنیت پورت مکانیزمی است که می تواند روی سوئیچ ها اجرا شود تا تشخیص دهد که دستگاه های غیرمجاز از طریق آدرس کنترل دسترسی رسانه (MAC) دستگاه به شبکه متصل می شوند. با این حال، مدیریت امنیت پورت ممکن است دشوار باشد. به عنوان مثال، به دلیل درگاه های شبکه مسدود شده معتبر (به عنوان مثال، دستگاه های متصل که اغلب تغییر می کنند، مانند اتاق های کنفرانس) تعداد تیکت پشتیبانی را افزایش می دهد. علاوه بر این، دشمنانی که می توانند آدرس MAC را جعل کنند، می توانند آن را نیز دور بزنند. یک راه حل قوی تر از 802.1x استفاده می کند که دستگاه ها را بر اساس گواهی دیجیتال قابل اعتماد نصب شده بر روی دستگاه احراز هویت می کند. در حالی که پیاده سازی آن دشوارتر است، به دلیل تولید و نصب گواهینامه ها، مدیریت آن آسان تر از امنیت پورت است و سطح بالاتری از اطمینان را ارائه می دهد.

۲,۶ شبکه های خصوصی مجازی (VPN) را محدود و رمزگذاری کنید

گیت وی های VPN معمولاً از طریق اینترنت قابل دسترسی و مستعد اسکن شبکه، تلاش‌های brute force و آسیب‌پذیری‌های روز صفر هستند . برای کاهش بسیاری از این آسیب‌پذیری‌ها، مدیران باید همه ویژگی‌های غیرضروری را غیرفعال کنند و قوانین سخت‌گیرانه فیلتر ترافیک را برای جریان ترافیک به سمت گیت وی های VPN اجرا کنند. NSA توصیه می‌کند دسترسی گیت وی VPN را به پورت ۵۰۰ پروتکل دیتاگرام کاربر (UDP)، پورت UDP۴۵۰۰ ، محفظه بار امنیتی (ESP) و سایر پورت‌های مناسب محدود کنید .در صورت امکان، ترافیک پذیرفته شده را به آدرس های پروتکل اینترنت همتا (IP) شناخته شده VPN محدود کنید .اگر آدرس IP همتا از راه دور ناشناخته باشد، VPNهای دسترسی از راه دور را نمی توان به یک قانون فیلتر ثابت اضافه کرد .اگر ترافیک را نمی توان به آدرس های IP خاصی فیلتر کرد، از یک IPS در جلوی گیت وی VPN برای نظارت بر ترافیک نادرست IP Security (IPsec) استفاده کنید و مذاکرات سشن IPsec را بررسی کنید.

همه پیکربندی‌های IPsec VPN به یک خط‌مشی IPsec و یک خط‌مشی تبادل کلید اینترنت (IKE) نیاز دارند .این خط‌مشی‌ها تعیین می‌کنند که چگونه در هنگام ایجاد تونل IPsec در هر مرحله مذاکره صورت خواهد پذیرفت. اگر هر یک از فازها به گونه ای پیکربندی شده باشد که رمزنگاری ضعیف را مجاز کند، ممکن است کل VPN در خطر باشد و محرمانه بودن داده ها از بین برود .هر خط مشی IKE شامل حداقل سه جزء کلیدی است:

۱. الگوریتم/گروه دیفی-هلمن
۲. الگوریتم رمزگذاری
۳. الگوریتم هش

موارد زیر حداقل تنظیمات توصیه شده برای کمیته سیاست سیستم های امنیت ملی 15 (CNSSP) است:

* گروه دیفی هلمن: ۱۶ با توان مدولار ۴۰۹۶ بیتی(MODP)

* گروه دیفی هلمن: ۲۰ با گروه منحنی بیضوی ۳۸۴ بیتی (ECP)

❋ رمزگذاری: استاندارد رمزگذاری پیشرفته 256-(AES)

❋ هش: الگوریتم هش ایمن 384-(SHA)

Diffie-Hellman Group 15 نیز بر اساس حداقل الزامات CNSSP 15 قابل قبول است، اما گروه ۱۵ به دلیل مسائل مربوط به قابلیت همکاری که رعایت شده است توصیه نمی شود .یک تونل VPN را می توان بین دو نقطه پایانی ایجاد کرد تا یک کانال ارتباطی رمزگذاری شده را از طریق یک شبکه نامعتبر مانند اینترنت فراهم کند .هنگام ایجاد یک پیشنهاد، خط مشی، یا مجموعه تبدیلVPN ، مطمئن شوید که از توصیه های CNSSP 15پیروی می کند.

برای اطمینان از عدم استفاده سهوی از آنها، سیاست‌ها و پیشنهادات پیش‌فرض برای انجمن امنیت اینترنت و پروتکل مدیریت کلید (ISAKMP) و IKEv2 را با دستورات پیکربندی زیر غیرفعال کنید:

```
no crypto isakmp default policy
no crypto ikev2 policy default
no crypto ikev2 proposal default
no crypto ipsec transform-set default
```

توجه: اگر خط‌مشی‌های پیش‌فرض غیرفعال باشند، فقط از خط‌مشی‌هایی که صریحاً پیکربندی شده‌اند استفاده می‌شود.

یک پیشنهاد، خط مشی و پروفایل IKEv2 را با دستورات پیکربندی مثال زیر ایجاد کنید:

```
crypto ikev2 proposal <IKEV2_PROPOSAL_NAME>
encryption aes-gcm-256
group [16|20]
crypto ikev2 policy <IKEV2_POLICY_NAME>
proposal <IKEV2_PROPOSAL_NAME>
crypto ikev2 profile <IKEV2_PROFILE_NAME>
match identity remote ...
authentication remote ...
authentication local ...
```

پیکربندی پروفایل به شبکه ای که برای آن پیکربندی شده است بستگی دارد و باید دارای روش های احراز هویت محلی و راه دور و یک match statement باشد .همچنین می‌توان یک keyring جداگانه ایجاد کرد و برای چندین کلید از قبل مشترک روی پروفایل اعمال کرد .

یک مجموعه تبدیل IPsec را با دستورات پیکربندی مثال زیر ایجاد کنید:

```
crypto ipsec transform-set <IPSEC_TRANSFORM_NAME> esp-gcm 256 mode tunnel
```

یک پروفایل Ipsec که پروفایل IKEv2 و مجموعه تبدیل IPsec بالا استفاده می کند ، با دستورات پیکربندی مثال زیر ایجاد کنید :

```
crypto ipsec profile <IPSEC_PROFILE_NAME>
set transform-set <IPSEC_TRANSFORM_NAME>
set pfs group16
set ikev2-profile <IKEV2_PROFILE_NAME>
```

پروفایل Ipsec می بایستی که مطابق دستورات پیکربندی زیر بر روی اینترفیس تانل اعمال گردد.

```
interface <TUNNEL_INTERFACE_NAME>
tunnel protection ipsec profile <IPSEC_PROFILE_NAME>
no shutdown
```

۳. نگهداری امنیتی

سخت‌افزار و نرم‌افزار قدیمی ممکن است حاوی آسیب‌پذیری‌های شناخته‌شده عمومی باشد و مکانیزم آسانی برای سوء استفاده از شبکه برای دشمنان فراهم کند .این آسیب‌پذیری‌ها با ارتقای منظم سخت‌افزار و نرم‌افزار به نسخه‌های جدیدتر که توسط فروشنده پشتیبانی می‌شوند، کاهش می‌یابد . علاوه بر این، یکپارچگی نرم افزار دانلود شده باید قبل و در حین استفاده تأیید شود .تعمیر و نگهداری امنیتی باید به طور منظم انجام شود تا اطمینان حاصل شود که دستگاه ها به طور ایمن به کار خود ادامه می دهند.

۳,۱یکپارچگی نرم افزار و پیکربندی را بررسی کنید

دشمن می‌تواند با تغییر فایل‌های سیستم‌عامل، کد اجرایی در حال اجرا در حافظه، یا سفت‌افزار یا بوت‌لودری که سیستم‌عامل یک دستگاه شبکه را بارگیری می‌کند، نرم‌افزار مخرب را وارد دستگاه‌های شبکه کند .نرم افزاری که به طور مخرب در یک دستگاه شبکه تغییر یافته است می تواند توسط دشمن برای نقض یکپارچگی داده ها، استخراج اطلاعات حساس و ایجاد انکار سرویس (DoS) استفاده شود.

NSA توصیه می کند یکپارچگی فایل های سیستم عامل نصب شده و در حال اجرا بر روی دستگاه ها را با مقایسه هش رمزنگاری شده فایل با هش معتبر شناخته شده منتشر شده توسط فروشنده تأیید کنید. هنگام ارتقاء فایل‌های سیستم‌عامل، قبل و بعد از نصب، تایید یکپارچگی فایل‌ها را انجام دهید تا مطمئن شوید هیچ تغییری ایجاد نشده است .یک هش آنلاین اولیه را می توان بر روی یک فایل تصویری سیستم عامل با دستور execزیر محاسبه کرد:

```
verify /sha512 <PATH:filename>
```

دستگاه‌های قدیمی‌تر ممکن است فقط از هش Message Digest 5 (MD5) پشتیبانی کنند که می‌تواند با دستور exec زیر محاسبه شود:

```
verify /md5 <PATH:filename>
```

ممکن است دشمن به سادگی تنظیمات را تغییر دهد .تغییرات پیکربندی می تواند نشانه ای باشد که یک دستگاه در معرض خطر قرار گرفته است. NSA همچنین اجرای یک فرآیند کنترل تغییر پیکربندی را توصیه می کند که به طور ایمن پشتیبان های پیکربندی دستگاه را برای شناسایی تغییرات مخرب ایجاد می کند .هنگامی که نیاز به تغییر پیکربندی است، تغییر را مستند کنید و مجوز، هدف و توجیه عملیات را درج کنید .با مقایسه پیکربندی‌های فعلی دستگاه با جدیدترین نسخه‌های پشتیبان، به‌صورت دوره‌ای تأیید کنید که تغییرات اعمال نشده‌اند .اگر تغییرات مشکوکی مشاهده شد، تأیید کنید که تغییر مجاز است.

۳,۲سیستم فایل و مدیریت بوت مناسب را حفظ کنید

بسیاری از تجهیزات شبکه حداقل دو پیکربندی مختلف دارند، یکی یا چند مورد در فضای ذخیره‌سازی دائمی ذخیره شده و یک نسخه فعال در حافظه اجرا می‌شود .در صورت راه اندازی مجدد یا قطع برق، تغییرات دائمی در پیکربندی باید ذخیره شود تا از تناقضات پیکربندی جلوگیری شود .تغییرات پیکربندی را می توان با دستور exec زیر در دستگاه ذخیره کرد:

```
copy running-config startup-config
```

اگر قرار است تغییرات موقتی باشد، NSA توصیه می‌کند تا کامنت هایی را قبل از خطوط پیکربندی به‌روز شده درج کنید و دلیل ایجاد و زمان حذف آن را ذکر کنید. اگر دستگاه از کامنت پشتیبانی نمی کند، کامنت ها را در یک نسخه پشتیبان از پیکربندی وارد کنید تا با نسخه موجود در دستگاه مقایسه شود .هنگام کپی کردن تنظیمات از راه دور، از پروتکل رمزگذاری شده ، مانند پروتکل انتقال فایل امن (SFTP) یا پروتکل کپی ایمن(SCP) استفاده کنید .این مکانیسم برای پشتیبان گیری یا بایگانی تنظیمات، باید از دسترسی غیرمجاز محافظت شود.

NSA همچنین توصیه می کند فایل های استفاده نشده یا غیر ضروری را در هر دستگاه بررسی کنید و با دستورات exec زیر آنها را حذف کنید:

```
dir /recursive all-filesystems
delete <PATH:filename>
```

فایل های قدیمی سیستم عامل یا فایل های پیکربندی پشتیبان قدیمی ذخیره شده در دستگاه به احتمال زیاد غیر ضروری هستند و باید حذف شوند .ذخیره چندین نسخه نرم افزار این فرصت را برای دشمن فراهم می کند تا نرم افزار قدیمی را بارگیری مجدد کند و آسیب پذیری های اصلاح شده در نسخه های جدیدتر سیستم عامل را دوباره برقرار کند.

۳,۳نرم افزار و سیستم عامل را به روز نگهدارید

حفظ سیستم عامل‌ها و نرم افزارها در حالت به‌روز ،شبکه را از آسیب‌پذیری‌های حیاتی و مسائل امنیتی که در نسخه‌های جدیدتر شناسایی و رفع شده‌اند، محافظت می‌کند .دستگاه‌هایی که سیستم‌عامل‌های قدیمی یا نرم‌افزارهای آسیب‌پذیر را اجرا می‌کنند، در معرض آسیب‌پذیری‌های مختلف منتشر شده هستند، و بهره‌برداری از این دستگاه ها یک تکنیک رایج است که توسط دشمنان برای به خطر انداختن شبکه استفاده می‌شود. NSA توصیه می کند سیستم عامل و نرم افزار را در همه دستگاه ها به آخرین نسخه پایدار موجود از فروشنده ارتقا دهید .ارتقاء سیستم عامل ممکن است به ارتقاء سخت افزار یا حافظه اضافی نیاز داشته باشد و دریافت نسخه نرم افزاری جدید ممکن است به قرارداد تعمیر و نگهداری یا پشتیبانی با فروشنده نیاز داشته باشد .اکثر دستگاه‌های زیرساخت شبکه از ویژگی به‌روزرسانی خودکار پشتیبانی نمی‌کنند، بنابراین لازم است فرآیند درخواست و نصب آخرین نرم‌افزار با همکاری فروشنده اجرا شود.

۳,۴سخت افزار پشتیبانی شده توسط فروشنده را به روز نگهدارید

فروشندگان در نهایت پشتیبانی از پلتفرم‌های سخت‌افزاری خاص را متوقف می‌کنند و در صورت بروز نقص، این دستگاه تا پایان عمر نمی‌توانند سرویس شوند .علاوه بر بی ثباتی دستگاه و نگرانی ها در مورد نیاز به ارتقا حافظه، به دلیل عدم به روز رسانی نرم افزار برای رفع آسیب پذیری های شناخته شده، خطر سوء استفاده دشمن از دستگاه افزایش می یابد .پلتفرم‌های سخت‌افزاری جدیدتر که توسط فروشنده پشتیبانی می‌شوند، ویژگی‌های امنیتی را بهبود بخشیده‌اند، از جمله محافظت در برابر آسیب‌پذیری‌های شناخته شده .هنگامی که یک فروشنده اعلامیه پایان عمر دستگاه خود را منتشر می کند یا اعلام می کند که دستگاه دیگر پشتیبانی نمی شود، NSAتوصیه می کند طبق توصیه های فروشنده، طرحی برای ارتقا یا جایگزینی دستگاه های آسیب دیده با تجهیزات جدیدتر ایجاد کنید .دستگاه های قدیمی یا پشتیبانی نشده باید فورا ارتقا یافته یا جایگزین شوند تا از در دسترس بودن خدمات شبکه و پشتیبانی امنیتی اطمینان حاصل شود گردد.

۴. احراز هویت، مجوز، و حساب کاربری (AAA)

سرورهای متمرکز AAA مکانیزم یکپارچه ای را برای مدیریت دسترسی به دستگاه ها ارائه می دهند و حساب های ایجاد شده برای دشمن چالش برانگیزتر است زیرا سرتیفیکیت ها مستقیماً در دستگاه ها ذخیره نمی شوند .پیکربندی صحیح این سرورها منبع معتبری برای مدیریت و نظارت بر دسترسی فراهم می کند، ثبات کنترل دسترسی را بهبود می بخشد، نگهداری پیکربندی را کاهش می دهد و هزینه های اداری را کاهش می دهد . همه دستگاه‌ها ابتدا باید برای استفاده از سرویس‌های مدرن AAA با دستور پیکربندی مثال زیر برای دستگاه‌های Cisco IOS پیکربندی شوند:

```
aaa new-model
```

اعمال پیکربندی بالا تضمین می‌کند که دستگاه از روش‌های احراز هویت و مجوز قدیمی استفاده نمی‌کند.

۴,۱ پیاده سازی سرورهای متمرکز

همه دستگاه ها باید برای استفاده از سرورهای AAA متمرکز پیکربندی شوند. NSA توصیه می کند حداقل دو سرور AAA را در شبکه برای اطمینان از در دسترس بودن و کمک به شناسایی و پیشگیری از فعالیت های دشمن پیاده سازی کنید .اگر یک سرور به دلیل نگهداری برنامه ریزی شده یا به دلایل دیگر در دسترس نباشد، سرورهای باقی مانده به ارائه خدمات متمرکز AAA ادامه خواهند داد . سرورها باید:

* برای احراز هویت دستگاه ها با یک preshared-key منحصر به فرد و پیچیده برای اطمینان از اینکه فقط دستگاه های مجاز می توانند از خدمات AAA استفاده کنند پیکربندی شده باشند .

* برای استفاده از پروتکل یکسان مانند TACACS+ ، RADIUS، یا LDAP پیکربندی شده است .

* همگام سازی با یکدیگر برای اطمینان از سازگاری سرتیفیکیت کاربر و کنترل های دسترسی.

یک گروه سرور با چندین سرور AAA را می توان با دستورات پیکربندی زیر پیکربندی کرد:

```
aaa group server {tacacs+ | radius | ldap} <GROUP_NAME>
server-private <IP_ADDRESS_1> key <KEY_1>
```

server-private <*IP_ADDRESS_2*> key <*KEY_2*>

برخی از دستگاه های قدیمی ممکن است از کلمات کلیدی tacacs-server و radius-server در پیکربندی استفاده کنند که از اختصاص یک کلید منحصر به فرد به هر سرور جلوگیری می کند.

۴.۲ احراز هویت را پیکربندی کنید

احراز هویت، هویت یک شخص یا نهاد را تأیید می کند .همه دستگاه‌ها باید به گونه‌ای پیکربندی شوند که ابتدا از سرورهای متمرکز برای سرویس‌های AAA استفاده کنند و حساب‌های Local Administrator تنها در صورتی که همه سرورهای متمرکز در دسترس نباشند، به عنوان روش پشتیبان‌گیری مورد استفاده قرار گیرند . همین امر در مورد احراز هویت سطح ممتاز (privileged level) نیز صدق می کند . دستگاه‌ها فقط باید در صورتی از رمز عبور Local Administrator استفاده کنند که همه سرورهای متمرکز در دسترس نباشند .این ترتیب اولویت از ورود دشمنی که اعتبار Local Administrator را به دست آورده است به دستگاه ها جلوگیری می کند زیرا دسترسی معمولاً توسط سرورهای AAA کنترل می شود.

NSA توصیه می کند که حتما احراز هویت متمرکز را برای ورود به سیستم پیکربندی کنید و دسترسی (ممتاز) را همانطور که در دستورات پیکربندی زیر نشان داده شده است به عنوان روش اصلی فعال کنید :

aaa authentication login default group <*GROUP_NAME*> local

aaa authentication enable default group <*GROUP_NAME*> enable

استفاده از کلمه کلیدی default تضمین می‌کند که پیکربندی در تمام مواردی که فهرست احراز هویت صریح مشخص نشده است، به صورت سراسری اعمال می‌شود .اگر به جای آن از یک لیست با نام سفارشی استفاده می شود، لازم است این لیست به صراحت در همه مواردی که AAAاستفاده می شود اعمال شود و به طور بالقوه برخی از سرویس های مدیریتی به درستی پیکربندی نشده و در معرض خطر قرار گیرند . لیست default همیشه زمانی اعمال می شود که یک لیست با نام سفارشی به صراحت اعمال نشده باشد.

<GROUP_NAME> باید نام سفارشی گروه سرور AAA (قبلا تعریف شده) باشد که شامل آدرس های IP سرورهای AAA متمرکز و کلیدهای مرتبط با آنها می شود.

کلمه کلیدی Line نباید استفاده شود زیرا این رمزهای عبور به طور ایمن در پیکربندی ذخیره نمی شوند.

کلمه کلیدی none هرگز نباید استفاده شود زیرا احراز هویت را غیرفعال می کند.

۴.۳ پیکربندی مجوز

مجوز تأیید می کند که یک شخص یا نهاد، مجوز دسترسی به یک منبع خاص یا انجام یک عمل خاص را داشته باشد . سازمان، موقعیت و هدف دستگاه دستورات را دیکته می کند. NSA توصیه می کند که به اندازه کافی آنچه را که ادمین های قانونی مجاز به اجرای آن هستند محدود کنید تا از انجام اقدامات غیرمجاز با یک حساب کاربری در معرض خطر توسط دشمن جلوگیری شود .اکثر ادمین ها از privilege level سطح ۱ برای دسترسی در سطح کاربر و از privilege level سطح ۱۵ برای دسترسی سطح ممتاز استفاده می کنند .مجوز باید برای هر دو این سطوح و هر سطح امتیاز دیگری که توسط مدیران با دستورات پیکربندی زیر استفاده می شود اعمال شود:

aaa authorization exec default group <*GROUP_NAME*> local

aaa authorization commands 1 group <*GROUP_NAME*> local

aaa authorization commands 15 group <*GROUP_NAME*> local

aaa authorization config-commands

لیست default باید برای اطمینان از اعمال پیکربندی در همه جا استفاده شود.

<GROUP_NAME> باید نام سفارشی گروه سرور AAA (قبلا تعریف شده است) باشد که شامل آدرس های IP سرورهای AAA متمرکز و کلیدهای مرتبط با آنها می شود.

در صورت تمایل، کلمه کلیدی if-authenticated را می توان بعد از کلمه کلیدی local اعمال کرد .اگر یک مدیر با موفقیت وارد سیستم شود و همه سرورهای AAA متمرکز در دسترس نباشند، دیگر مجاز به اجرای دستورات نخواهند بود .کلمه کلیدی if-authenticated تضمین می کند که کاربر احراز هویت شده همچنان مجاز به اجرای دستورات است .با این حال، در مورد این کلمه کلیدی محتاط باشید، زیرا به طور بالقوه می تواند به مدیر دسترسی فراتر از آنچه در سرورهای AAA متمرکز پیکربندی شده است، بدهد.

کلمه کلیدی none هرگز نباید استفاده شود زیرا مجوز را غیرفعال می کند.

۴.۴ پیکربندی حساب کاربری

مدیریت حساب کاربری سوابق تمام منابع مرتبط با دسترسی یا اقدامات انجام شده را نگه می داشته و مدیران را مسئول نگه می دارد . سوابق حسابداری را می توان برای چندین نوع رویداد دیگر جمع آوری کرد، اما بستگی به سازمان و هدف دستگاه دارد NSA .توصیه می کند که تغییرات پیکربندی سیستم به صورت مرکزی ثبت شود و فرآیندی برای بررسی دوره ای این سوابق برای شناسایی فعالیت های مخرب احتمالی اجرا شود .حداقل، سوابق حسابداری باید هنگام شروع و توقف یک جلسه exec (shell) و هنگامی که دستورات Shell شروع و متوقف می شوند، جمع آوری شوند .مانند مجوز، حسابداری commands باید با دستورات پیکربندی زیر برای تمام سطوح امتیاز administrator اعمال شود:

aaa accounting exec default start-stop group <*GROUP_NAME*>
aaa accounting commands 1 default start-stop group <*GROUP_NAME*>
aaa accounting commands 15 default start-stop group <*GROUP_NAME*>

۴.۵ اعمال اصل کمترین دسترسی

اصل کمترین دسترسی یک مفهوم امنیتی است که اجازه دسترسی به یک شخص یا نهاد را در پایین ترین سطح امتیاز لازم برای انجام وظایف مجاز می دهد .بسیاری از کارهای رایج به دسترسی سطح ممتاز نیاز ندارند، مانند مشاهده وضعیت رابط های شبکه یا بررسی جداول مسیریابی . برای اجرای حداقل امتیاز، مدیران ابتدا باید با کمترین سطح امتیاز لازم وارد سیستم شوند .این یک لایه امنیتی اضافی را فراهم می کند که یک دشمن باید برای به خطر انداختن کامل یک دستگاه ، آن را دور بزند .همچنین از ایجاد ناخواسته تغییرات پیکربندی در دستگاه توسط مدیران جلوگیری می کند .

NSA توصیه می‌کند که همه حساب‌ها با سطح امتیاز ۱ یا ۰ پیکربندی شوند و مدیران را ملزم می‌کند که سرتیفیکیت های بیشتری را وارد کنند تا به سطح امتیاز بالاتری برای انجام وظایف مورد نیاز ارتقا یابد .سطوح امتیاز باید به صورت دوره‌ای بازبینی شوند و دسترسی‌های غیرضروری حذف شوند تا از استفاده ناخواسته از دستورات سطح ممتاز در سطوح امتیاز پایین‌تر جلوگیری شود.

سطح امتیاز حساب های local فردی را می توان با کلمه کلیدی امتیاز تغییر داد .با دستور پیکربندی زیر، حساب های محلی را به سطح امتیاز ۱ اختصاص دهید:

username <*USER_NAME*> privilege 1

همه حساب‌های administrator که در سطح امتیاز ۱ وارد می‌شوند بایستی تا دستور enable را اجرا و سرتیفیکیت اضافی برای ارتقا به سطح امتیاز بالاتر ارائه نمایند. علاوه بر بررسی تمام حساب‌های local administratorl و اطمینان از تخصیص کمترین سطح امتیاز، لازم است همه حساب‌های پیکربندی شده روی سرورهای AAA متمرکز نیز بررسی شوند.

به طور مشابه، همین مفهوم باید برای خطوط کنسول(CON) ، کمکی (AUX) و تله تایپ مجازی (VTY) اعمال شود .وقتی مجوز AAA به درستی پیکربندی شده باشد، نباید به پیکربندی خطوط وابسته باشد .با این حال، بهترین روش برای اطمینان از پیکربندی خطوط به حداقل

line con 0 privilege level 1
line aux 0 privilege level 1
line vty 0 4 privilege level 1
line vty 5 15 privilege level 1

بسته به دستگاه، ممکن است لازم باشد پیکربندی مشابهی برای خطوط دیگر نیز اعمال شود .اگر خطوط VTY 5 تا 15 در دستگاه خاصی وجود نداشته باشد، اجرای آن دستورات ضروری نیست.

۴.۵ محدود کردن تلاش برای احراز هویت

محدود کردن تعداد تلاش‌های احراز هویت و ایجاد تاخیر در ورود، مانع از آن می‌شود که حریف در تلاش برای دستیابی به دسترسی، شکستن رمز عبور brute force را علیه دستگاه انجام دهد لذا NSA توصیه می‌کند که تلاش‌های مدیریت از راه دور ناموفق را به حداکثر سه یا کمتر با دستور پیکربندی زیر برای دستگاه‌های Cisco IOS محدود کنید:

aaa authentication attempts login 3

به طور مشابه، همان مفهوم سه یا کمتر تلاش ناموفق باید برای جلسات Secure Shell (SSH) با دستور پیکربندی زیر اعمال شود:

ip ssh authentication-retries 3

NSA همچنین توصیه می‌کند با دستور پیکربندی زیر حداقل یک ثانیه تاخیر بین تلاش‌های ورود به سیستم برای کاهش قابل توجه تلاش‌های brute forceایجاد کنید:

```
login delay 1
```

۵. حساب های مدیر و رمزهای عبور

حساب های local برای مدیریت دستگاه های شبکه حیاتی هستند .اگر احراز هویت متمرکز ناموفق باشد، حساب‌های local دسترسی مدیران را به دستگاه‌های شبکه برای عیب‌یابی و تشخیص مشکلات شبکه فراهم می‌کنند.

حساب‌های local باید منحصربه‌فرد باشند، با یک رمز عبور منحصربه‌فرد و پیچیده احراز هویت شوند و مسئولیت‌پذیری را برای مدیران فراهم کنند .اگر خط مشی رمز عبور برای سازمان وجود ندارد، یک خط مشی جدید ایجاد و اجرا کنید .در صورت لزوم، خط مشی را به صورت دوره ای بررسی و بازنگری کنید.

این بخش عمدتاً بر روی حساب ها و رمزهای عبور local تمرکز دارد .دستگاه‌های شبکه سنتی از روش‌های قدیمی برای مدیریت حساب‌های local استفاده می‌کنند و ممکن است از مکانیسم‌های توصیه‌شده برای نوشتن، تغییر و تأیید رمز عبور پشتیبانی نکنند .ماهیت ساده این حساب‌های local مستلزم اعمال توصیه‌های متفاوت است .این برخلاف سرورهای متمرکز AAA است که در آن احراز هویت چند عاملی، پیچیدگی رمز عبور، مقایسه رمز عبور قبلی و سایر مفاهیم به درستی قابل پیاده سازی هستند.

۵,۱ از نام های کاربری منحصر به فرد و تنظیمات حساب استفاده کنید

اکثر دستگاه‌ها دارای سرتیفیکیت های مدیریتی پیش‌فرض هستند که برای عموم ارائه می‌شوند، و اغلب به یک دستگاه دسترسی کامل مدیریتی می‌دهند .حفظ این تنظیمات به دشمن امکان ورود آسان به شبکه را برای اتصال و به طور بالقوه دسترسی سطح ممتاز برای نظارت ناشناس یا پیکربندی مجدد دستگاه می دهد.

NSA توصیه می کند تمام تنظیمات پیش فرض را حذف کنید و هر دستگاه را با یک حساب منحصر به فرد و امن برای هر مدیر پیکربندی مجدد کنید .بدون تغییر تنظیمات پیش فرض مدیریتی و حساب های کاربری، هیچ دستگاه جدیدی را وارد شبکه نکنید .توجه داشته باشید که حساب کاربری پیش فرض در برخی از دستگاه ها قابل حذف نیست.

۵,۲ رمزهای عبور پیش فرض را تغییر دهید

به اکثر دستگاه‌ها یک رمز عبور پیش‌فرض، یا گاهی اوقات بدون رمز عبور اختصاص داده می‌شود تا به Administrator اجازه دسترسی آسان قبل از پیکربندی اولیه را بدهد .بسیاری از این رمزهای عبور عمومی هستند و معمولاً برای عملکرد صحیح دستگاه نیازی به تغییر ندارند .آنها اهداف اصلی برای اسکنرهای خودکار مخرب (بات نت) برای بهره برداری هستند، زیرا اعتبارنامه های پیش فرض دسترسی سطح ممتازی را به دستگاه ارائه می دهند.

NSA توصیه می کند همه رمزهای عبور پیش فرض را حذف کنید و یک رمز عبور منحصر به فرد، پیچیده و ایمن را به همه سطوح دسترسی، از جمله سطوح کاربری و سطوح ممتاز، اختصاص دهید .علاوه بر این، هنگام معرفی دستگاه های جدید به شبکه، قبل از اتصال دستگاه به شبکه، گذرواژه کاربری پیش فرض و سطح ممتاز را تغییر دهید.

۵,۳ حساب های غیر ضروری را حذف کنید

برخی از دستگاه ها دارای حساب هایی هستند که مورد نیاز نیستند .از آنجایی که ممکن است به ندرت از آنها استفاده شود یا اصلاً استفاده نشود، حفظ امنیت آنها اغلب نادیده گرفته می شود .در صورت امکان، نام حساب های پیش فرضی را که با یک سرپرست خاص مرتبط نیستند، تغییر دهید یا حذف کنید.

NSA توصیه می‌کند که تعداد حساب‌های مجاز برای ورود به دستگاه‌ها باید به آنچه ضروری است محدود شود .بقیه باید حذف شوند وقتی یک Admin سازمان را ترک می‌کند یا نقش‌هایش را تغییر می‌دهد، حساب‌های مرتبط باید غیرفعال یا حذف شوند .در دستگاه‌های سیسکو IOS، یک حساب local را با دستور پیکربندی زیر حذف کنید:

no username <*NAME*>

۵,۴ از حساب های فردی استفاده کنید

حساب ها را می توان توسط مدیران فردی استفاده کرد یا بین یک گروه به اشتراک گذاشت. با این حال، اگر چندین Admin از یک حساب گروهی برای دسترسی به دستگاه استفاده کنند، مسئولیت پذیری نمی تواند اعمال شود زیرا تغییرات پیکربندی به یک فرد خاص مرتبط نمی شود. به همین دلیل، دشمنان حساب های گروه را هدف قرار می دهند تا دسترسی غیرمجاز به دستگاه ها داشته باشند.

NSA توصیه می‌کند که همه حساب‌های admin مشترک یا گروهی را غیرفعال کنید و از یک حساب منحصر به فرد برای هر admin برای ایجاد دسترسی برای تغییرات پیکربندی و اطمینان از پاسخگویی در هر دستگاه استفاده کنید. اگر حساب‌های گروهی ضروری است، NSA توصیه می‌کند این حساب‌ها را برای شناسایی هر گونه فعالیت مشکوک نظارت کنید. ممکن است ایجاد یک حساب محلی پشتیبان برای هر مدیر امکان پذیر نباشد، اما یک حساب گروهی منفرد که برای هر مدیری شناخته شده است، پاسخگویی فردی را فراهم نمی کند.

NSA همچنین توصیه می‌کند که حساب‌های local فقط در شرایط اضطراری زمانی که سرورهای AAA متمرکز در دسترس نیستند، استفاده شوند. در طول چنین رویدادی، گذرواژه‌های حساب اضطراری local منحصر به فرد باید توسط یک فرد مورد اعتماد که دسترسی مستقیم به دستگاه‌ها ندارد، نگهداری شود. مدیران می توانند حساب local و رمز عبور را درخواست کنند و پس از پایان وضعیت اضطراری، فرد مورد اعتماد می تواند رمز عبور را تغییر دهد. این از استفاده مجدد رمز عبور جلوگیری می کند و مسئولیت پذیری را تضمین می کند. سایر درخواست های احراز هویت باید از طریق سرورهای AAA متمرکز انجام شوند.

۵,۵ ذخیره رمزهای عبور با الگوریتم های امن

گذرواژه ها معمولاً در پیکربندی یک دستگاه یا در یک پایگاه داده local، به صورت clear text، رمزگذاری شده یا هش یک طرفه ذخیره می شوند .هرگز نباید از clear text استفاده کرد، همچنین برخی از توابع رمزگذاری یا هش، ضعیف در نظر گرفته می‌شوند و به راحتی می‌توانند با استفاده از ابزارهای در دسترس عموم شکسته شوند .یک دشمن می‌تواند با استفاده از یک تحلیلگر شبکه یا با به خطر انداختن یک سیستم مدیریت مرکزی که فایل‌های پیکربندی را ذخیره می‌کند، گذرواژه‌ها یا هش‌ها را از پیکربندی یا پایگاه داده local جمع‌آوری کند. clear text و رمزهای عبور الگوریتم ضعیف را می توان به راحتی شکسته و برای دسترسی کاربر یا سطح ممتاز به یک دستگاه استفاده کرد Cisco IOS .انواع هش یک طرفه و رمزگذاری شده زیر را پشتیبانی می کند:

- رمزهای عبور تایپ ۰ نباید استفاده شوند زیرا clear text ذخیره می شوند
- هش رمز عبور تایپ ۴ نباید استفاده شود زیرا به راحتی می توان آنها را شکست
- از هش رمز عبور نوع ۵ (MD5) باید اجتناب شود مگر در سیستم عامل های قدیمی که از تایپ های ۶، ۸ یا ۹ پشتیبانی نمی کنند

• رمزهای تایپ ۶ با AES رمزگذاری شده‌اند و فقط باید برای گذرواژه‌هایی استفاده شوند که به جای هش کردن نیاز به رمزگذاری دارند (مانند کلیدهای VPN)، یا در سیستم‌هایی که از تایپ ۸ پشتیبانی نمی‌کنند (که معمولاً نشان می‌دهد که تایپ ۹ نیز در دسترس نیست.

•رمزهای عبور تایپ ۷ نباید استفاده شوند زیرا به راحتی قابل برگشت هستند، حتی اگر رمزگذاری شده باشند

•استفاده از هش رمز عبور تایپ ۸ (SHA-256 PBKDF2) توصیه می شود

•هش رمز عبور تایپ ۹ (Scrypt) توسط موسسه ملی استاندارد و فناوری (NIST) تایید نشده است.

NSA توصیه می کند که همه رمزهای عبور روی یک دستگاه با استفاده از امن ترین الگوریتم موجود ذخیره شوند و هرگز به صورت clear-text ذخیره نشوند .الگوریتم های هش یک طرفه برگشت ناپذیر هستند و معمولاً باید برای ذخیره رمزهای عبور استفاده شوند .با این حال، اگر الگوریتم‌های هش یک طرفه در دسترس نباشند، رمزهای عبور باید با یک کلید منحصر به فرد قوی رمزگذاری شوند .هنگام ایجاد یک حساب کاربری یا اختصاص رمز عبور، برخی از دستگاه ها نیاز به تعیین الگوریتم دارند .لذا بایستی تا توجه ویژه ای به حساب‌های سطح ممتاز معطوف شود، اما این راهنمایی در مورد حساب‌های کاربری، پورت‌های مدیریت، پروتکل‌های مسیریابی تأیید شده، کلیدهای VPN و هر مکانی که ممکن است رمز عبور در پیکربندی دستگاه مشخص شود نیز اعمال می‌شود.

با دستور پیکربندی زیر از استفاده از رمز clear-text جلوگیری کنید:

```
service password-encryption
```

یک هش رمز عبور تایپ ۸ را برای یک حساب local با دستور پیکربندی زیر ذخیره کنید:

```
username <NAME> algorithm-type sha256 secret <PASSWORD>
```

اگر به گذرواژه‌های رمزگذاری‌شده برگشت‌پذیر نیاز دارید مانند کلیدهای(VPN) ، به جای گذرواژه‌های تایپ ۷ با دستورات پیکربندی زیر از تایپ ۶ AES استفاده کنید:

```
password encryption aes
key config-key password-encrypt <KEY>
```

<KEY>باید یک رمز عبور منحصر به فرد و پیچیده باشد که برای ایجاد کلید رمزگذاری رمزهای عبور تایپ ۶ استفاده می شود .این رمز عبور نباید یک رمز عبور پیش فرض، ضعیف یا به راحتی قابل حدس زدن باشد و نباید در جای دیگری از پیکربندی مجدداً استفاده شود .دشمنی که این کلید را حدس می‌زند می‌تواند از آن برای رمزگشایی تمام رمزهای عبور تایپ ۶ ذخیره شده در پیکربندی استفاده کند .وقتی این کلید تنظیم شد، معمولاً نیازی به نگه داشتن آن نیست.

از آنجایی که نیازی به حفظ آن نیست، NSA استفاده از یک کلید منحصر به فرد را برای هر دستگاهی توصیه می کند که مانع از استفاده دشمن از همان کلید برای رمزگشایی رمزهای عبور تایپ ۶ در همه دستگاه ها می شود .توجه داشته باشید که اگر کلید تغییر کند، رمزهای عبور رمزگذاری شده تایپ ۶ باید دوباره به صورت دستی تنظیم شوند.

۵,۶ ایجاد رمزهای عبور قوی

دستگاهی که با یک رمز عبور ضعیف پیکربندی شده است، توانایی دشمن را در به خطر انداختن آن دستگاه افزایش می دهد .دشمن ممکن است بتواند به راحتی رمز عبور ضعیف را حدس بزند یا با استفاده از ابزارهای شکستن رمز عبور در دسترس عموم (به عنوان مثال، dictionary یا brute force attempts) آن را بشکند .هنگامی که دسترسی سطح ممتاز به دست آمد، دشمن می تواند تغییراتی در پیکربندی ایجاد کند که به طور بالقوه دستگاه های دیگر را در شبکه به خطر می اندازد. NSA توصیه می کند که یک رمز عبور منحصر به فرد و پیچیده را به تمام سطوح دسترسی، از جمله دسترسی های کاربر و سطح ممتاز، اختصاص دهید .رمزهای عبور منحصر به فرد و پیچیده همچنین باید برای احراز هویت مسیریابی، همگام‌سازی زمان، تونل‌هایVPN ، SNMP و هر جای دیگری که گذرواژه‌ها در پیکربندی ذخیره می‌شوند استفاده شوند .گذرواژه ها باید شرایط پیچیدگی زیر را داشته باشند:

- از تمام کلاس های کاراکترهای مختلف (حروف بزرگ، کوچک، اعداد و کاراکترهای خاص) استفاده کنید .
- حداقل پانزده کاراکتر باشد
- بر اساس کلمات اختصاری یا کلمات اصلاح نشده نیست
- منطبق بر الگوی پیاده روی بر روی صفحه کلید نیست
- مشابه نام کاربری نیست
- با شبکه، سازمان، مکان، تیم ورزشی محلی، یا سایر شناسه های عملیاتی مرتبط نیست
- با آخرین رمز عبور یا رمزهای عبور اختصاص داده شده در جای دیگر یکسان یا مشابه نباشد
- رمز عبور پیش فرض، خالی یا شناخته شده عمومی نیست

خط مشی رمز عبور یک سازمان ممکن است نیازی به گذرواژه های مدیریت شده از طریق سرورهای AAA متمرکز برای رعایت همه این توصیه ها نداشته باشد، به خصوص زمانی که با احراز هویت چند عاملی و سایر اصول همراه باشد .دستورالعمل فوق حداقل باید برای حساب‌های local و سایر گذرواژه‌هایی که در پیکربندی یک دستگاه شبکه ذخیره می‌شوند، اعمال شود، جایی که کنترل‌های امنیتی متمرکز نمی‌توانند اعمال شوند.

دشمنی که از شبکه، مکان، برنامه‌ها و غیره آگاهی داشته باشد، می‌تواند به راحتی این عبارات را حدس بزند (یا بداند)، بنابراین به آنها در شکستن رمزهای عبور کمک می‌کند. NSA همچنین توصیه می کند برای اجرای سیاست رمز عبور سازمان، به طور منظم رمزهای عبور ضعیف را بررسی کنید .پیچیدگی رمز عبور باید قبل از تنظیم رمز عبور جدید بررسی شود و مدیران شبکه باید به طور دوره‌ای تنظیمات دستگاه شبکه را برای شناسایی استفاده از الگوریتم‌های رمز عبور ضعیف بررسی کنند.

۵,۷ استفاده از رمزهای عبور منحصر به فرد

تخصیص رمز عبور یکسان به چندین حساب یا چندین سطح دسترسی می تواند بر مسئولیت پذیری و مجوز تأثیر بگذارد. اگر یک مدیر از طریق یک پروتکل رمزگذاری نشده به دستگاه دسترسی پیدا کند، یک دشمن می تواند از یک تحلیلگر شبکه برای جمع آوری رمز عبور از ترافیک شبکه استفاده کند. چنانچه دشمن به سطح کاربری دسترسی پیدا کند، می‌تواند به طور بالقوه از همان رمز عبور برای دسترسی به سطح ممتاز استفاده مجدد کند .تخصیص رمز عبور یکسان به چندین دستگاه به دشمن اجازه می دهد تا دستگاه های متعددی را به طور همزمان و بدون هیچ تلاش اضافی به خطر بیاندازد. اگر رمز عبور یکسانی به اکثر دستگاه‌ها اختصاص داده می‌شد، حریف تنها باید یک رمز عبور واحد را به خطر بیاندازد تا دسترسی سطح ممتاز به همه آن دستگاه‌ها را داشته باشد. NSA توصیه می کند برای هر حساب و سطح ممتاز در هر دستگاه یک رمز عبور منحصر به فرد، پیچیده و ایمن اختصاص دهید. NSA همچنین توصیه می‌کند استفاده مجدد از رمز عبور را در چندین حساب و سطوح دسترسی و در چندین دستگاه بررسی کنید. هش های یکسان می تواند نشانه ای از استفاده مجدد از رمز عبور باشد.

۵,۸ در صورت لزوم رمزهای عبور را تغییر دهید

تغییر دوره‌ای گذرواژه‌ها از لحاظ تاریخی منجر به استفاده از گذرواژه‌های ضعیف‌تر شده است و اگر کاربران از دستورالعمل‌های ۵,۶ ایجاد رمزهای عبور قوی پیروی کنند، ممکن است اجرای این خط‌مشی ضروری نباشد. ایجاد اولیه رمزهای عبور قوی روش موثرتری برای کاهش خطرات موفقیت آمیز رمز عبور است. NSA توصیه می کند در صورتی که رمز عبور یا هش رمز عبور به خطر افتاده است فوراً رمز عبور را تغییر دهید و آن را همانطور که در رمز بند ۵,۵ با الگوریتم های ایمن توضیح داده شده است، به صورت ایمن ذخیره کنید.

با توجه به زمان و منابع کافی، هر رمز عبور را می‌توان حدس زد یا با brute force شکست. گذرواژه‌های به خطر افتاده که تغییر نکرده‌اند به حریف زمان بیشتری برای استفاده از این تکنیک‌ها می‌دهند. علاوه بر این، اگر دشمن در نهایت رمز عبور قدیمی را شکست، ممکن است به تلاش برای تغییر ادامه دهد و اگر رمز عبور فعلی بر اساس رمز عبور قبلی باشد،آن را حدس بزند. متأسفانه، تشخیص اینکه چه زمانی یک رمز عبور به خطر افتاده است، به خصوص رمزهای عبور local ذخیره شده در پیکربندی، ممکن است دشوار باشد. دستگاه‌های شبکه سنتی در نحوه ذخیره و انتقال پیکربندی که شامل رمزهای عبور و هش رمز عبور است، بسیار ساده‌تر هستند. علاوه بر این، ارسال ایمیل پیکربندی‌های دستگاه شبکه یا ذخیره آن‌ها در اشتراک‌گذاری فایل‌های محافظت‌نشده می‌تواند منجر به افشا شود، زیرا گذرواژه‌ها و هش‌های رمز عبور ذخیره‌شده در پیکربندی‌ها بدون محافظت رها می‌شوند. علاوه بر این، رمزهای عبور ذخیره شده با یک الگوریتم ضعیف باید به خطر افتاده در نظر گرفته شوند، زیرا شکستن آنها بسیار آسان تر است.

اگر محرمانه بودن گذرواژه‌ها قابل حفظ نباشد یا سازمان بخواهد به طور منظم تلاش کند تا عواملی را که ممکن است رمزهای عبور را به خطر انداخته‌اند بدون شناسایی، اخراج کند، NSA توصیه می‌کند یک خط‌مشی قدیمی ایجاد شود که شامل تغییر رمزهای عبور به طور منظم باشد . تغییر گذرواژه‌های local می‌تواند به‌طور قابل‌توجهی دشوارتر از رمزهای عبور متمرکز باشد، بنابراین لازم است چارچوب زمانی ای را انتخاب کنید که برای مدیران شبکه عملی باشد و در عین حال مدت زمانی را که دشمن می‌تواند از رمز عبور احتمالی در معرض خطر استفاده کند، کاهش می‌دهد .اگر دستگاه از گذرواژه‌های طولانی پشتیبانی نمی‌کند، توصیه می‌شود برای جلوگیری از شکستن رمز عبوری که هنوز استفاده می‌شود، گذرواژه‌ها را بیشتر تغییر دهید.

توجه: اگر رمز عبور با استفاده از یک رمز پیچیده تایپ ۹ ذخیره شود که در آن هش رمز عبور با 14 شروع می شود، نشان می دهد که رمز عبور اخیراً تغییر نکرده است .

۶. ثبت و نظارت از راه دور

Logging مکانیزم مهمی برای ثبت فعالیت‌های دستگاه و ردیابی رویدادهای امنیتی شبکه است که به مدیران این امکان را می‌دهد تا گزارش‌ها را برای فعالیت‌های مشکوک و حوادث بررسی کنند .پیکربندی ناقص گزارش‌گیری در یک دستگاه می‌تواند منجر به گم شدن یا نادرست بودن اطلاعات و مشکل در ارتباط رویدادهایی شود که در دستگاه یا شبکه رخ داده‌اند .ثبت گزارش مناسب شامل ارسال گزارش‌ها به چندین سرور گزارش راه دور، همگام‌سازی ساعت با چندین منبع زمانی تأیید شده و اجرای سیاست‌ها و رویه‌های مدیریت گزارش است .سیستم اطلاعات امنیتی و مدیریت رویداد (SIEM) می تواند برای جمع آوری و تجزیه و تحلیل گزارش های دریافتی توسط سرورهای گزارش راه دور استفاده شود.

۶,۱ سیستم ثبت لاگ را فعال کنید

پیام‌های لاگ تنها زمانی در دستگاه‌های شبکه ایجاد می‌شوند که سیستم لاگینگ فعال باشد .دستگاه‌ها باید به گونه‌ای پیکربندی شوند که پیام‌های لاگ را به یک بافر گزارش local و سرورهای گزارش مرکزی به طور همزمان ارسال کنند. NSA توصیه می کند که سیستم ثبت لاگ را فعال کنید، بافر گزارش local را روی ۱۶ مگابایت یا بیشتر تنظیم کنید، و رویه ای برای تأیید دریافت و بازبینی گزارش ها به طور منظم ایجاد کنید .اکثر دستگاه‌ها باید اندازه بافر بزرگ‌تری را پشتیبانی کنند، اما اگر حافظه کافی وجود نداشته باشد، می‌توان آن را برای دستگاه خاصی کاهش داد .مطمئن شوید که ثبت سیستم ثبت لاگ با دستور پیکربندی زیر فعال است:

```
logging on
```

با دستورحداکثر زیر بافر لاگlocal را با دستور پیکربندی زیر افزایش دهید:

```
logging buffered 16777216 informational
```

توجه: با این کار سطح ثبت نیز به informational تغییر می کند، زیرا هر دو مقدار باید به طور همزمان تنظیم شوند.

۶,۲ ایجاد سرورهای متمرکز ثبت لاگ از راه دور

پیام‌های لاگ ارسال شده به سرورهای لاگینگ راه دور کمتر در معرض خطر یا پاک کردن قرار دارند و این اطمینان حاصل می شود که در صورت آسیب‌دیدگی، راه‌اندازی مجدد یا پر شدن بافر گزارش local، پیام‌ها تحت تأثیر قرار نخواهند گرفت. NSA توصیه می‌کند حداقل دو سرور لاگینگ راه دور و متمرکز ایجاد کنید تا از نظارت، افزونگی و در دسترس بودن پیام‌های لاگ دستگاه اطمینان حاصل شود .در صورت پشتیبانی، مطمئن شوید که پیام‌های لاگ در حین انتقال رمزگذاری شده‌اند تا از افشای غیرمجاز اطلاعات حساس جلوگیری شود.

حداقل دو سرور لاگینگ راه دور را با دستورات پیکربندی زیر پیکربندی کنید:

```
logging host <IP_ADDRESS_1>
logging host <IP_ADDRESS_2>
```

۶,۳ اطلاعات لاگ ضروری را ذخیره کنید

دستگاه‌هایی که با اطلاعات کافی پیرامون لاگ ها پیکربندی شده‌اند، اطلاعاتی را که مدیران برای تجزیه و تحلیل رویدادهای مربوط به یک حادثه نیاز دارند، از جمله مرتبط کردن چندین رویداد یا رویدادهای رخ داده در دستگاه‌های دیگر، در اختیار مدیران قرار می‌دهند .توصیه می‌شود برای جمع‌آوری تمام اطلاعات لازم، سطوح ثبت trap و بافر را در هر دستگاه حداقل روی سطح informational (کد ۶) تنظیم کنید .دستگاه ها را روی سطح Debugging نیز پیکربندی کرد (کد ۷)، اما افزایش تعداد لاگ های تولید شده ممکن است روند بررسی گزارش را کُند کند . با دستورات پیکربندی زیر، هر دو سطح ثبت tarp و بافر را روی سطحinformational تنظیم کنید:

```
logging trap informational
logging buffered 16777216 informational
```

Logging را نیز می توان در خطوط کنسول و VTY به ترتیب با کلمات کلیدی console و monitor فعال کرد .این روش‌ها بلافاصله به مدیرانی که وارد سیستم شده‌اند هشدار می‌دهند، اما لاگ ها حفظ نمی‌شوند .لازم نیست برای این روش ها لاگ را فعال کنید مگر اینکه توسط مدیران خواسته شود . می توان با دستورات پیکربندی زیر این تنظیمات را غیرفعال کرد:

```
no logging console
no logging monitor
```

NSA همچنین استفاده از زمان جهانی هماهنگ (UTC) را برای منطقه زمانی توصیه می‌کند، به خصوص اگر شبکه چندین منطقه زمانی را در بر بگیرد .همه لاگ های گزارش باید حاوی یک مهر زمانی با پیکربندی مناسب با تاریخ کامل شامل سال، زمان شامل ثانیه و میلی‌ثانیه و منطقه زمانی باشد .اطمینان حاصل کنید که منطقه زمانی به درستی تنظیم شده است و تمام ویژگی های ذکر شده در بالا را با دستورات پیکربندی زیر فعال کنید:

```
clock timezone UTC 0 0
service timestamps log datetime msec localtime show-timezone year
service timestamps debug datetime msec localtime show-timezone year
```

در نهایت، NSA همچنین توصیه می‌کند پیام‌های لاگینگ را فعال کنید تا نشان دهند کاربر در ورود به سیستم موفق یا ناموفق بوده است . حتی اگر زمانی که کنترل حساب ها و کاربری ها به درستی پیکربندی شده باشد، این رویدادها در سرورهای AAA متمرکز ثبت می‌شوند، این اطلاعات در بافر محلی ثبت نمی‌شوند .مطمئن شوید که این رویدادها با دستورات پیکربندی زیر ثبت شده اند:

```
login on-failure log
login on-success log
```

۶,۴ همگام سازی ساعت ها

پروتکل زمان شبکه (NTP) برای همگام‌سازی ساعت دستگاه های در سراسر جهان و اطمینان از دقیق بودن مهرهای زمانی همراه با پیام‌های لاگ استفاده می‌شود. برای ارائه این قابلیت به شکل مطمئن، هر دستگاه باید حداقل با دو منبع زمانی قابل اعتماد همگام شود. این دقت برای اطمینان از اینکه مهرهای زمانی مربوط به پیام لاگ را می‌توان به راحتی در مناطق زمانی پراکنده جغرافیایی مرتبط کرد و برای ردیابی جمعی یک حادثه شبکه از یک دستگاه به دستگاه دیگر استفاده کرد، بسیار مهم است . توصیه شده است که که هر دستگاه و سرورهای گزارش راه دور

از حداقل دو سرور زمان قابل اعتماد برای اطمینان از صحت و در دسترس بودن اطلاعات استفاده کنند. سرورهای زمانی داخلی باید به عنوان منبع اصلی برای همه دستگاه‌ها ایجاد شوند، که متعاقباً باید با منابع معتبر خارجی همگام شوند. این طراحی تعداد درخواست‌های خارجی را کاهش می‌دهد و از یکنواختی مهرهای زمانی اطمینان می‌دهد. هنگام استقرار سرورهای زمان در شبکه، مدیران باید تأیید کنند که دستگاه‌ها می‌توانند به سرورهای زمان دسترسی داشته باشند و ساعت‌ها پس از اعمال پیکربندی همگام‌سازی می‌شوند. NSA همچنین توصیه می‌کند برای جلوگیری از دستکاری ساعت، احراز هویت NTP را در همه دستگاه‌ها فعال کنید و کلیدهای احراز هویت قوی و منحصر به فرد NTP را بین دستگاه‌ها و منبع زمانی مشخص‌شده‌شان پیکربندی کنید .کلیدهای NTP قابل اعتماد را ایجاد کنید و احراز هویت NTP را با دستورات پیکربندی زیر فعال کنید:

```
ntp authentication-key <#1> md5 <KEY>
ntp trusted-key <#1>
ntp authentication-key <#2> md5 <KEY>
ntp trusted-key <#2>
ntp authenticate
```

هر تعداد کلید قابل اعتماد را می توان ایجاد کرد .توجه داشته باشید که کلیدهای احراز هویت NTP در پیکربندی به عنوان رمز عبور تایپ ۷ ذخیره می شوند .گذرواژه های رمزگذاری شده با AES تایپ ۶ برای احراز هویت NTP پشتیبانی نمی شوند.

دستگاه را با حداقل دو سرور NTP مختلف با دستورات پیکربندی زیر همگام کنید:

```
ntp server <IP_ADDRESS_1> key <#1>
ntp server <IP_ADDRESS_2> key <#2>
```

توجه: شماره در انتهای هر دستور، کلید NTP قابل اعتماد است که برای احراز هویت آن سرور خاص استفاده می شود .پس از انتظار برای همگام سازی ساعت، همگام سازی و وضعیت سرورهای NTP را با دستورات اجرایی زیر بررسی کنید:

```
show ntp status
show ntp associations
```

توجه: لازم است همگام سازی ساعت را پس از هر تغییر پیکربندی NTP تأیید کنید و ممکن است چندین ساعت طول بکشد تا همگام سازی صحیح انجام شود.

۷. مدیریت از راه دور و خدمات شبکه

تجهیزات شبکه را می توان از راه دور و توسط ادمین های متفاوت از طریق سرویس های مختلف مدیریت کرد . برخی از خدمات رایج شبکه عبارتند ازSSH ، پروتکل انتقال ابرمتن(HTTP) ، SNMP و پروتکل انتقال فایل(FTP) . این سرویس ها برای مدیران مفید هستند، اما آنها همچنین توسط دشمنان برای سوء استفاده و دسترسی سطح ممتاز به یک دستگاه مورد هدف قرار می گیرند. همه آنها باید به درستی پیکربندی شوند تا احتمال نفوذ کاهش یابد.

۷,۱ سرویس های مدیریتی clear text را غیرفعال کنید

پروتکل‌های clear text ترافیک را در سراسر شبکه (بدون رمزگذاری) منتقل می‌کنند و قبل از استفاده گسترده از رمزگذاری طراحی شده‌اند . بنابراین، استفاده از این پروتکل‌ها برای مدیریت از راه دور دستگاه‌های حیاتی ممکن است منجر به افشای اطلاعاتی شود که می‌تواند بر امنیت دستگاه و شبکه تأثیر منفی بگذارد .دشمن می‌تواند شبکه را به خطر بیاندازد، نام‌های کاربری، گذرواژه‌ها، اطلاعات پیکربندی و سایر داده‌های حساس را از طریق تکنیک‌های رایج بازیابی اطلاعات (مانند تحلیلگر شبکه یا ابزار ضبط بسته) جمع‌آوری کند. NSA استفاده از سرویس‌های رمزگذاری‌شده را برای محافظت از ارتباطات شبکه و غیرفعال کردن همه سرویس‌های مدیریت clear text مانندTelnet ، HTTP، FTP، SNMP 1/2 توصیه می‌کند .این تضمین می‌کند که اطلاعات حساس نمی‌توانند به راحتی توسط دشمنی که ترافیک شبکه را کپچر می‌کند افشا شود.

اگر دستگاهی از پروتکل های رمزگذاری شده پشتیبانی نمی کند، سیستم مدیریتی را مستقیماً به کنسول یا پورت مدیریت متصل کنید یا یک شبکه مدیریت اختصاصی خارج از شبکه پروداکشن ایجاد کنید تا توانایی دشمن در کپچر پروتکل های clear text را کاهش دهید .سرویس Telnetرا با دستورات پیکربندی زیر غیرفعال کنید :

```
line vty 0 4
transport input none

line vty 5 15
transport input none
```

بسته به دستگاه، ممکن است لازم باشد پیکربندی مشابهی برای خطوط دیگر نیز اعمال شود .اگر خطوط VTY 5 تا 15 در دستگاه خاصی وجود نداشته باشد، اجرای آن دستورات ضروری نیست .توجه داشته باشید که این دستورات ممکن است سرویس های دیگری که به طور پیش فرض روی خطوط فعال هستند، از جمله SSH را نیز غیرفعال کنند.

سرویس HTTP را با دستور پیکربندی زیر غیرفعال کنید:

```
no ip http server
```

نسخه‌های 1 و 2c سرویس‌های SNMP و SNMP trap را با حذف Community string های پیکربندی شده با دستورات زیر غیرفعال کنید:

```
no snmp-server community <COMMUNITY_STRING>
no snmp-server host <HOSTNAME_OR_IP_ADDRESS> <COMMUNITY_STRING>
```

پروتکل TFTP را با دستورات زیر غیر فعال کنید:

```
no ip ftp username
no ip ftp password
```

۷,۲ از قدرت رمزگذاری کافی اطمینان حاصل کنید

برخی از سرویس های رمزگذاری شده نیاز دارند که یک جفت کلید عمومی و خصوصی ایجاد شود تا مشتریان بتوانند به سرور متصل شده و احراز هویت کنند. علاوه بر این، سرویس گیرنده و سرور یک اتصال رمزگذاری شده ممکن است در مجموع یک کلید جلسه خصوصی برای هر اتصال منحصر به فرد ایجاد کنند. شکستن کلید جلسه خصوصی و رمزگشایی تمام داده‌های منتقل شده در اتصالات رمزگذاری شده که از الگوریتم‌های ضعیف یا تعداد کمی بیت استفاده می‌کنند، برای دشمن آسان‌تر است. NSA توصیه می کند که ۳۰۷۲ بیت یا بالاتر برای تولید کلید نامتقارن (عمومی و خصوصی)، ۳۸۴ بیت برای کلیدهای رمزنگاری منحنی (ECC)و ۲۵۶ بیت برای کلیدهای رمزگذاری متقارن استفاده شود. برخی از سیستم ها ممکن است ۳۰۷۲ بیت را پشتیبانی نکنند، بنابراین ممکن است به جای آن از ۴۰۹۶ بیت استفاده شود. برای هر دستگاهی که اندازه کلید کوچک‌تری دارد، یک جفت کلید جدید را بازسازی کنید و پروتکل‌های رمزگذاری شده را پیکربندی کنید تا فقط از الگوریتم‌های تایید شده استفاده کند. اندازه کلید بزرگتر ممکن است زمان اتصال به سرویس را افزایش دهد (به دلیل محاسبات اضافی)، اما در اکثر دستگاه ها ناچیز است.

۷,۳ از پروتکل های امن استفاده کنید

اغلب سرویس های مدیریتی رایج پروتکل هایی را پیاده سازی می کنند که حاوی نقص هایی در پیاده سازی و تبادل اطلاعات است که می تواند توسط دشمن مورد سوء استفاده قرار گیرد .برخی از پروتکل ها مانند SSH را می توان به گونه ای پیکربندی کرد که سازگار با گذشته باشد و پروتکل های ناامن قدیمی را به همراه پروتکل های جدیدتر بپذیرند .پروتکل‌های قدیمی‌تر تابع تکنیک‌های Man-in-the-Middle هستند که می‌توانند کلاینت‌ها و سرورها را مجبور به مذاکره با الگوریتم‌های ضعیف‌تر، احتمالاً بدون آگاهی کاربر، کنند. NSA توصیه می کند اطمینان حاصل شود که سرویس های مدیریتی از آخرین نسخه پروتکل ها استفاده می کنند و تنظیمات امنیتی مناسب به اندازه کافی فعال هستند. SSH نسخه ۲ روش ترجیحی برای دسترسی از راه دور به دستگاه ها است .سرورهای HTTP رمزگذاری شده باید طوری پیکربندی شوند که فقط امنیت لایه انتقال (TLS) نسخه ۱,۲ یا بالاتر را بپذیرند.

۷,۴ دسترسی به سرورها را محدود کنید

چنانچه تعداد زیادی از دستگاه ها مجاز به اتصال به سرویسهای مدیریتی باشند در برابر بهره برداری نیز آسیب پذیرتر هستند. NSA توصیه می‌کندACL ها را به گونه‌ای پیکربندی کنید که فقط سیستم‌های ادمین ها بتوانند برای مدیریت از راه دور به دستگاه‌ها متصل شوند. دستگاه هایی که قابلیت پشتیبانی از ACL را ندارند باید در یک بخش مدیریت شبکه جداگانه مانند VLAN قرار گیرند. ممکن است لازم باشد که یک فایروال جداگانه در مقابل بخش های حیاتی شبکه پیاده سازی شود تا سیستم هایی که می توانند به آن VLAN متصل شوند محدود شود. جایگزینی برای استفاده از پروتکل (DHCP) در نظر بگیرید. برای سیستم های مدیر از آدرس های IP ثابت استفاده کنید یا از مجموعه کوچکتری از آدرس ها استفاده کنید. آدرس‌های استاتیک، تعریف ACL را آسان‌تر کرده و دسترسی مدیر به خدمات مدیریت را محدود می‌کند . اکثر سرویس های مدیریتی فقط ACL های استاندارد را می پذیرند. بیش از یک دستگاه یا شبکه را می توان در خطوط اضافی با کلمه کلیدی مجوز فهرست کرد. حتی اگر هر ACL یک عبارت انکار در پایان دارد، بهترین روش این است که صریحاً آن را درج کنید تا تلاش‌های رد شده لاگ شوند. یک ACL استاندارد ایجاد کنید تا فقط آدرس های IP مورد استفاده مدیران را با دستورات پیکربندی زیر مجاز کند:

access-list <*ACL#*> permit <*NETWORK*> <*WILDCARD_MASK*> log
access-list <*ACL#*> deny any log

NSA همچنین توصیه می‌کندACL های استفاده نشده را از پیکربندی حذف کنید زیرا می‌توانند مدیر را گیج کنند که فکر کند به درستی اعمال می‌شوند در حالی که نیستند .پس از تأیید عدم اعمال ACL استاندارد، آن را با دستور پیکربندی زیر حذف کنید:

```
no access-list <ACL#>
```

۷,۵ بازه زمانی قابل قبول تعیین کنید

تنظیم یک بازه زمانی برای اتصالات آیدل به سشن ها اجازه می‌دهد پس از یک زمان تعیین‌شده برای عدم فعالیت بسته شوند .زمانی که دوره های وقفه تنظیم نشده یا خیلی طولانی تنظیم شده باشد، ممکن است اتصالات بیکار به طور نامحدود ادامه یابند یا حتی اگر اتصالات همزمان محدودی روی دستگاه تنظیم شده باشد، DoS ایجاد شود. این DoS تا زمانی که مدت زمان آیدل به پایان برسد ادامه خواهد داشت، که در صورت غیرفعال شدن مهلت زمانی غیرفعال می تواند نامحدود باشد .یک بازه زمانی طولانی‌تر به حریف زمان بیشتری برای کپچر یک سشن در حالی که بی‌کار است، می‌دهد. NSA توصیه می کند که زمان پایان جلسه برای اتصالات مدیریتی را روی پنج دقیقه یا کمتر در تمام دستگاه های راه دور تنظیم کنید. به عنوان مثال، exec-timeoutدر خطوط VTY ، SSH، کنسول و پورت های آگزیلاری .(مدت زمان وقفه را روی صفر قرار ندهید، زیرا اکثر دستگاه‌ها با این تنظیم عملکرد وقفه را غیرفعال می‌کنند).

۷.۶ فعال نگه داشتن پروتکل کنترل انتقال (TCP)

پیام‌های TCP keep-alive ارسال و دریافت شده از یک دستگاه به آن اجازه می‌دهد وضعیت اتصال را زمانی که هیچ فعالیتی در یک بازه زمانی مشخص رخ نداده است ارزیابی کند .از این پیام ها می توان برای تشخیص فقدان سهوی در اتصال و کاهش خطرات احتمالی شبکه استفاده کرد .در برخی از دستگاه‌ها، فقدان سرویس TCP keep-alive باعث می‌شود که اتصالات TCP برقرار شده پس از قطع اتصال سهوی در یک طرف باز باقی بمانند و سشن را در معرض سرقت قرار دهد .علاوه بر این، احراز هویت ممکن است حتی برای اتصالات رمزگذاری نشده مورد نیاز نباشد، و حریف می تواند به سادگی سشن را از سر بگیرد و احتمالاً دسترسی سطح ممتازی به دست آورد. NSA توصیه می کند که تنظیمات TCP keep-alive را برای پیام های ورودی و خروجی برای همه اتصالات TCP با دستورات پیکربندی زیر فعال کنید:

```
service tcp-keepalives-in
service tcp-keepalives-out
```

۷,۷ کانکشن های خروجی را غیرفعال کنید

پس از احراز هویت به یک دستگاه از طریق یک پورت مدیریتی، کاربر معمولاً توانایی اتصال از راه دور به سایر سیستم‌های موجود در شبکه را از طریق پروتکل‌های پشتیبانی‌شده مانند Telnet و SSH دارد .اگر دشمنی بتواند دستگاه را به خطر بیاندازد یا از یک حساب ادمین برای دسترسی در سطح کاربر استفاده کند، این اتصال خروجی به طور بالقوه می تواند برای پیشروی از طریق شبکه استفاده شود .بررسی صحیح تنظیمات دستگاه و استفاده از ACL ها می تواند از دسترسی سیستم های غیرمجاز به منابع شبکه جلوگیری کند. NSA توصیه می کند کانکشن های خروجی را غیرفعال کنید تا حرکات دشمن را از طریق شبکه با دستورات پیکربندی زیر محدود کنید:

```
line con 0

transport output none

line vty 0 4
```

transport output none

line vty 5 15

transport output none

بسته به دستگاه، ممکن است لازم باشد پیکربندی مشابهی برای خطوط دیگر نیز اعمال شود .اگر خطوط VTY 5 تا 15 در دستگاه خاصی وجود نداشته باشد، اجرای آن دستورات ضروری نیست .توجه به این نکته ضروری است که این ویژگی باید به صراحت در خط کنسول غیرفعال شود . اگر اتصالات خروجی برای کپی کردن فایل‌ها به یا از دستگاه‌ها برای تأیید تعمیر و نگهداری یا یکپارچگی لازم است، آن را فقط به SSH محدود کنید و تعداد دستگاه‌هایی را که می‌توان از طریقACL های خروجی به آنها دسترسی داشت محدود کنید .پس از اتمام کار به پیکربندی بالا مراجعه کنید.

۷,۸ کانکشن های خروجی را غیرفعال کنید

یک read-write community string نسخه ۱ یا ۲ SNMP شبیه رمز عبور است و می تواند برای دسترسی یا تغییر پیکربندی های دستگاه و فایل های سیستم عامل استفاده شود .این اقدامات معمولاً با یک read community string قابل انجام نیستند .از آنجایی که read-write community string در قالب clear text ارسال می شوند، می توانند توسط یک دشمن برای به دست آوردن کنترل کامل یک دستگاه شبکه مورد سوء استفاده قرار گیرند. NSA توصیه می‌کند که تمام read-write community string ها را حذف کنید و با رمزگذاری و احراز هویت به SNMP نسخه ۳ ارتقا دهید .اگر یک read-write community string نسخه ۱ یا ۲ SNMP برای مدیریت از راه دور مورد نیاز است و نمی توان آن را حذف کرد، توصیه می شود که read-write community string به طور قابل توجهی متفاوت از سایر read-write community string ها باشد تا از حدس زدن توسط دشمن جلوگیری شود .تمام read-write community string SNMP های نسخه ۱ و ۲ c را می توان با دستور exec زیر فهرست کرد:

show running-config | include snmp-server community

و دستور مربوط به غیرفعال کردن :

no snmp-server community <*COMMUNITY_STRING*>

۷,۹ سرویس های غیر ضروری شبکه را غیرفعال کنید

در طول نصب اولیه دستگاه‌ها، چندین سرویس TCP و UDP به طور پیش‌فرض فعال می‌شوند، این سرویس‌ها می‌توانند سطح امنیت شبکه را کاهش دهند و به دشمن نقاط دسترسی اضافی برای سوءاستفاده از یک دستگاه ارائه دهند و آن را در معرض نظارت غیرمجاز، جمع‌آوری اطلاعات و در معرض خطر قرار دهند .به عنوان مثال، Cisco Smart Install اغلب غیر ضروری است، اما وقتی فعال باقی بماند، یک دشمن می‌تواند از این سرویس برای دریافت فایل پیکربندی دستگاه، آپلود پیکربندی یا فایل ایمیج سیستم عامل جدید یا اجبار به راه‌اندازی مجدد استفاده کند.

NSA توصیه می کند هر سرویس غیر ضروری را در هر دستگاهی غیرفعال کنید .اگر آن سرویس مورد نیاز است و می‌تواند رمز عبور و ACL را پشتیبانی کند، یک رمز عبور براساس راهنمایی رمز عبور قوی ایجاد کنید (به ۵,۶ ایجاد رمزهای عبور قوی مراجعه کنید) و یک ACL را اعمال کنید تا فقط سیستم‌های مورد نیاز به سرویس متصل شوند .اگر دستگاهی از ACL پشتیبانی نمی کند، می توان آن را به

یک VLAN جداگانه منتقل کرد و یک ACL را می توان به VLAN اعمال کرد. NSA همچنین توصیه می کند که بلافاصله سرویس Cisco Smart Installرا در همه دستگاه ها با دستور پیکربندی زیر غیرفعال کنید:

```
no vstack
```

اگرچه این سرویس برای سوئیچ‌ها طراحی شده است، روترها را می‌توان به‌عنوان مدیر نصب هوشمند Cisco نیز پیکربندی کرد .بنابراین، باید صراحتاً در همه دستگاه‌ها غیرفعال شود، به خصوص زمانی که برای اولین بار پیکربندی می‌شوند .سایر سرویس های TCP و UDP غیر ضروری را با دستورات پیکربندی زیر غیرفعال کنید:

```
no service tcp-small-servers
no service udp-small-servers
no service finger
```

۷,۱۰ غیرفعال کردن پروتکل های دیسکاوری بر روی اینترفیس های خاص

Cisco Discovery Protocol (CDP) و Link Layer Discovery Protocol (LLDP) پروتکل های برادکست هستند که به طور دوره ای توپولوژی شبکه و اطلاعات دستگاه را برای دستگاه های همسایه که از این پروتکل پشتیبانی می کنند و بسته ها را گوش می دهند تبلیغ می کنند. این عملکرد به طور پیش فرض فعال است و می تواند برای مدیران برای به دست آوردن اطلاعات در مورد شبکه مفید باشد، اما همچنین برای دشمنی که می تواند اطلاعات پیکربندی شبکه را بطور غیر فعال جمع آوری کند بسیار مفید است. دشمنی که قادر به استقرار snifferدر یک شبکه است می‌تواند شماره مدل دستگاه، نسخه‌های سیستم عامل، اطلاعات VLAN و آدرس‌های فیزیکی و منطقی را جمع‌آوری کند و اطلاعات ارزشمندی را برای بهره‌برداری از دستگاه‌های موجود در شبکه به دست آورد. NSA توصیه می کند CDP و LLDPرا در تمام دستگاه هایی که قادر به استفاده از این خدمات هستند غیرفعال کنید. اگر سرویسی برای ارتباطات شبکه مناسب مورد نیاز است به عنوان مثال، برخی از تلفن های سیسکو(Voice-over-IP (VoIP ، آن را فقط در پیوندهای پوینت به پوینت بین دستگاه هایی که به پروتکل نیاز دارند یا در پورت های های فعال صوتی فعال کنید. CDP و LLDP را می توان با دستورات پیکربندی زیر به صورت سراسری غیرفعال کرد:

```
no cdp run
no lldp run
```

اگر CDP روی اینترفیس‌های خاص مورد نیاز است، باید به صورت سراسری فعال شود اما در تمام اینترفیس های دیگر غیرفعال شود، همانطور که در دستورات پیکربندی زیر برای یک اینترفیس نشان داده شده است:

```
interface <INTERFACE>
no cdp enable
```

۷,۱۱ تنظیمات سرویس شبکه

این بخش نحوه فعال کردن صحیح خدمات مدیریت شبکه از راه دور را توضیح می دهد.

SSH ۷,۱۱,۱

اتصالات SSH ورودی را با دستورات پیکربندی زیر مجاز کنید:

```
line vty 0 4
transport input ssh
line vty 5 15
transport input ssh
```

ترنسپرت ورودی مجاز را می توان با دستور exec زیر تأیید کرد:

```
show line <LINE> <LINE_NUMBER>
```

اتصالات SSH نسخه ۱ را غیرفعال کنید و فقط نسخه ۲ پروتکل را با دستور پیکربندی زیر مجاز کنید

```
ip ssh version 2
```

یک جفت کلید نامتقارن جدید Rivest-Shamir-Adleman (RSA) برای SSH با دستور پیکربندی زیر ایجاد کنید :

```
crypto key generate rsa modulus 3072
```

توجه: این دستور یک جفت کلید RSA موجود را بازنویسی می کند .

یک جفت کلید ECC نامتقارن جدید برای SSH با دستور پیکربندی زیر ایجاد کنید :

```
crypto key generate ec keysize 384
```

توجه: این دستور یک جفت کلید ECC موجود را بازنویسی می کند.
با دستور پیکربندی زیر حداقل اندازه کلید Diffie-Hellman را روی ۴۰۹۶ بیت تنظیم کنید :

```
ip ssh dh min 4096
```

الگوریتم‌های رمزگذاری، تبادل کلید (KEX) و کد احراز هویت پیام که توسط پروتکل SSH پذیرفته شده‌اند را می‌توان با دستورات پیکربندی زیر مشخص کرد :

```
ip ssh server algorithm encryption <ALGORITHM> [<ALGORITHM> ...]
ip ssh server algorithm kex <ALGORITHM> [<ALGORITHM> ...]
ip ssh server algorithm mac <ALGORITHM> [<ALGORITHM> ...]
```

پیکربندی سرویس SSH را می توان با دستور exec زیر تأیید کرد:

```
show ip ssh
```

یک ACL استاندارد را اعمال کنید تا فقط آدرس های IP مورد استفاده مدیران را با دستورات پیکربندی زیر مجاز کند:

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

line vty 5 15
access-class <ACL#> in
```

اگر خطوط VTY 5 تا 15 در دستگاه خاصی وجود نداشته باشد، اجرای آن دستورات ضروری نیست .توجه داشته باشید که اگر این ACL در لاین ها فعال باشد، برای Telnet نیز اعمال می شود .بسته به دستگاه، ممکن است لازم باشد پیکربندی مشابهی برای لاین های دیگر نیز اعمال شود.

با دستورات پیکربندی زیر، انقضای جلسه را روی ۵ دقیقه یا کمتر تنظیم کنید:

```
line con 0
exec-timeout 5 0

line vty 0 4
exec-timeout 5 0

line vty 5 15
exec-timeout 5 0
```

اگر خطوط VTY 5 تا 15 در دستگاه خاصی وجود نداشته باشد، اجرای آن دستورات ضروری نیست .توجه داشته باشید که اگر روی لاین ها فعال باشد، این مورد برای Telnet نیز صدق می کند .بسته به دستگاه، ممکن است لازم باشد پیکربندی مشابهی برای لاین های دیگر نیز اعمال شود.

HTTP ۷,۱۱,۲

اگر از HTTP برای اهداف مدیریتی استفاده می شود، HTTPرا از طریق TLS با دستور پیکربندی زیر فعال کنید:

```
ip http secure-server
```

TLS نسخه ۱,۲ را فقط با دستور پیکربندی زیر بپذیرید:

```
ip http tls-version TLSv1.2
```

مجموعه های رمز پذیرفته شده توسط سرویس HTTP رمزگذاری شده را می توان با دستور پیکربندی زیر مشخص کرد :

ip http secure-ciphersuite <*CIPHERSUITE*> [<*CIPHERSUITE*> ...]

یک ACL استاندارد را اعمال کنید تا فقط آدرس های IP مورد استفاده مدیران را با دستور پیکربندی زیر مجاز کند:

ip http access-class <*ACL#*>

مدت زمان پیش‌فرض آیدل اتصال سرور HTTP 180 ثانیه (سه دقیقه) است، بنابراین نیازی به تغییر این مقدار نیست.

SNMP ۷,۱۱,۲

اگر از SNMP برای مدیریت استفاده می شود، SNMP نسخه ۳ را با احراز هویت و حریم خصوصی (رمزگذاری) با دستورات پیکربندی زیر فعال کنید:

snmp-server group <*SNMPv3_GROUP*> v3 priv access <*ACL#*>
snmp-server user <*USER*> <*SNMPv3_GROUP*> v3 auth sha <*AUTH_PASSWORD*> priv aes 256 <*PRIV_PASSWORD*> access <*ACL#*>

ابتدا باید یک گروه تعریف شود که در آن کلمه کلیدی priv معادل authPriv باشد (هم احراز هویت و هم حریم خصوصی) .یک یا چند کاربر باید تعریف و به یک گروه اختصاص داده شوند .علاوه بر پارامترهای احراز هویت و رمزگذاری، باید دو رمز عبور مختلف برای هر کاربر ارائه شود، یکی برای احراز هویت و دیگری برای حفظ حریم خصوصی .مشکلاتی با AES-192 و AES-256 مشاهده شده است، بنابراین ممکن است لازم باشد از AES-128 برای رمزگذاری به جای AES-256 از کلمات کلیدی aes 128 استفاده شود .همانطور که در بالا نشان داده شد، یک ACL را می توان هم برای گروه و هم برای هر کاربر جداگانه با مشخص کردن آن به عنوان یک گزینه جداگانه در انتهای هر دستور با کلمه کلیدی access اعمال کرد.

پیکربندی SNMP فوق را می توان از یک سیستم لینوکس با دستور شل زیر آزمایش کرد:

snmpget -v 3 -u <*USER*> -a sha -l authPriv -A '<*AUTH_PASSWORD*>' -x AES \ -X '<*PRIV_PASSWORD*>' <*IP_ADDRESS*> 1.3.6.1.2.1.1.5.0

۸. مسیریابی (Routing)

روترها بسته های داده را بین شبکه های کامپیوتری ارسال می کنند .هنگامی که روتر بسته ای را دریافت می کند، از جدول مسیریابی و اطلاعات آدرس شبکه بسته برای تعیین جهش بعدی برای رسیدن به مقصد استفاده می کند .پیکربندی نامناسب خود روتر یا پروتکل‌های مسیریابی پویا که برای پر کردن جدول مسیریابی استفاده می‌شوند، می‌تواند به دشمن اجازه دهد تا بسته‌ها را به مقصد دیگری هدایت کند و امکان جمع‌آوری، دستکاری یا دور انداختن داده‌های حساس را فراهم کند که این امر محرمانه، یکپارچگی یا ناقض دسترسی خواهد بود.

۸,۱ IP source routing را غیرفعال کنید.

IP source routing یک ویژگی به ندرت مورد استفاده است که فرستنده بسته را قادر می سازد به جای استفاده از جدول مسیریابی داخلی برای تصمیم گیری، لیست از پیش تعیین شده ای از گره های میانی را مشخص کند که باید در آنجا ارسال شود. با استفاده از این تنظیمات، یک دشمن می‌تواند بسته‌ها را از طریق مسیری که انتخاب می‌کند، انتقال دهد. همراه با جعل آدرسIP ، دشمن می تواند از ویژگی مسیریابی منبع IP برای دور زدن موفقیت آمیز ACL ها و سایر محدودیت های شبکه استفاده کند و اساسا مسیر شبکه خود را انتخاب کند. اگرچه این آسیب‌پذیری با روترها و نحوه مسیریابی بسته‌ها مرتبط است، اما می‌توان از این قابلیت در سوئیچ‌ها نیز سوء استفاده کرد. NSA توصیه می کند مسیریابی منبع IP را در همه دستگاه ها غیرفعال کنید، نه فقط روترها، زیرا این ویژگی برای عملیات عادی شبکه مورد نیاز نیست. یک ویژگی مشابه در IPv6 نیزموجود است و باید جداگانه غیرفعال شود. IP source routing را با دستورات پیکربندی زیر غیرفعال کنید:

```
no ip source-route
no ipv6 source-route
```

۸,۲ unicast reverse-path forwarding (uRPF) را فعال کنید.

uRPFروشی برای محافظت در برابر جعل IP است که به روتر دستور می دهد آدرس مبدا و مقصد را در بسته بررسی کند .هنگامی که یک بسته در یک اینترفیس دریافت می شود، آدرس منبع با ورودی های جدول مسیریابی مقایسه می شود و اگر مسیر برگشت با جایی که بسته دریافت شده مطابقت داشته باشد، ارسال می شود .در غیر این صورت، به دلیل نگرانی مبنی بر جعلی بودن آدرس منبع در بسته حذف می شود .اگر uRPF فعال نباشد، دشمن ممکن است بتواند با موفقیت آدرس منبع بسته های IP ارسال شده به شبکه را جعل کند.

NSAتوصیه می کند که uRPF را در اینترفیس های خارجی روترهای محیطی فعال کنید .در روترها، لازم است که Cisco Express Forwarding (CEF)، که جستجوهای بهینه‌سازی شده برای ارسال کارآمد بسته‌ها را فراهم می‌کند، قبل از uRPF فعال شود .توجه داشته باشید که uRPF نباید در اینترفیس های داخلی یا مسیریاب‌هایی که مسیریابی نامتقارن دارند (که ممکن است دو یا چند مسیر بازگشت برای یک آدرس منبع مشخص وجود داشته باشد) فعال شود، زیرا این وضعیت می‌تواند باعث حذف بسته‌های قانونی شود.

uRPF را در یک اینترفیس با دستورات پیکربندی زیر فعال کنید:

```
ip cef

interface <INTERFACE

 ip verify unicast reverse-path
```

۸,۳ احراز هویت مسیریابی را فعال کنید.

پروتکل های مسیریابی پویا، برای توزیع اطلاعات به دستگاه های همسایه و ارائه مسیرهایی برای دسترسی به شبکه های دیگر استفاده می شوند. دستگاه های شبکه از این اطلاعات برای پر کردن جدول مسیریابی خود استفاده می کنند، و سپس برای تعیین جهش بعدی برای ارسال یک بسته به مقصد درخواستی استفاده می شود. برای کنترل جریان ترافیک، یک حریف ممکن است اطلاعات مسیریابی ارسال و دریافت شده توسط دستگاه های همسایه را تزریق، اصلاح یا خراب کند. برای جلوگیری از دستکاری مسیر، احراز هویت مسیریابی باید فعال شود تا اطمینان حاصل شود که اطلاعات مسیریابی دریافتی از دستگاه های همسایه توسط یک منبع نامعتبر دستکاری نشده اس.

NSA توصیه می‌کند که احراز هویت مسیریابی را در پروتکل‌های مسیریابی پویا که به‌روزرسانی‌های مسیریابی را از سایر دستگاه‌های موجود در شبکه دریافت می‌کنند، فعال کنید. با فعال کردن آن در فرآیند OSPF برای هر ناحیه و اعمال کلید احراز هویت برای هر اینترفیس مرتبط با آن فرآیند با دستورات پیکربندی زیر، احراز هویت مسیریابی (OSPF) را فعال کنید:

key chain <*KEY_CHAIN_NAME*>
key <*KEY_NUMBER*>
key-string <*KEY*>
cryptographic-algorithm hmac-sha-512

interface <*INTERFACE*>

ip ospf authentication key-chain <*KEY_CHAIN_NAME*>

NSAهمچنین توصیه می کند به جای استفاده از کلید احراز هویت یکسان برای همه اینترفیس ها در همه دستگاه ها، از یک کلید منحصر به فرد بین همه همسایگان استفاده کنید .اگر کلیدها متفاوت باشند، دشمن نمی تواند از یک کلید در معرض خطر از یک شبکه برای تزریق یک مسیر مخرب به شبکه دیگر استفاده کند.

احراز هویت مسیریابی پروتکل (BGP)را با اعمال یک کلید رمز عبور منحصر به فرد برای هر همتای مجزا با دستورات پیکربندی زیر فعال کنید:

router bgp <*AS_NUMBER*>

peer <*IP_ADDRESS_1*> password <*KEY*>

با ایجاد یک زنجیره کلید و اعمال آن بر روی هر اینترفیس با دستورات پیکربندی زیر، احراز هویت پروتکل مسیریابی (EIGRP) را فعال کنید:

key chain <*KEY_CHAIN_NAME*>
key <*KEY_NUMBER*>
key-string <*KEY*>
cryptographic-algorithm hmac-sha-512

interface <*INTERFACE*>

ip authentication key-chain eigrp <*AS_NUMBER*> <*KEY_CHAIN_NAME*>

از پروتکل مسیریابی (RIP) استفاده نکنید. زیرا به کندی همگرا می شود و RIP نسخه ۱ را نمی توان برای احراز هویت روترهای مجاور پیکربندی کرد، و این امر سوء استفاده از پروتکل را برای دشمن آسان می کند .دستگاه‌هایی که فقط RIP را پشتیبانی می‌کنند باید از استاتیک روت یا دیفالت روت به سایر دستگاه‌هایی که از پروتکل‌های مسیریابی مدرن با احراز هویت پشتیبانی می‌کنند استفاده کنند.

۹. پورت های اینترفیس

پورت های اینترفیس سوئیچ های شبکه به طور فیزیکی ایستگاه های کاری، سرورها و سایر دستگاه ها را به شبکه متصل می کنند، در حالی که اتصالات بین روترها و سوئیچ ها نحوه ارتباط سیستم ها در سراسر شبکه را مشخص می کند .دشمن ابتدا باید برای اتصال یک سیستم غیرمجاز به شبکه دسترسی فیزیکی داشته باشد یا از سیستمی که قبلاً در شبکه ایجاد شده است برای سوء استفاده از اتصال موجود استفاده کند .پورت های اینترفیس با پیکربندی مناسب می توانند مانع از انجام تلاش های سوء استفاده از سوی دشمن علیه شبکه شوند.

۹,۱ ترانکینگ پویا را فعال کنید.

ترانک یک ارتباط پوینت به پوینت بین دو دستگاه است که فریم های کپسوله شده VLAN را مبادله می کند .بسته به ترافیکی که از طریق پیوند ارسال می شود، این امکان وجود دارد که یک پورت اینترفیس به صورت پویا خود را به عنوان یک ترانک یا یک پورت دسترسی پیکربندی کند .دشمنی که به یک پورت پویا متصل است می تواند به آن دستور دهد تا به یک پورت ترانک تبدیل شود و به طور بالقوه بدون توجه به جداسازی VLAN به ترافیک شبکه دسترسی پیدا کند. NSA توصیه می‌کند که ترانکینگ پویا را غیرفعال کنید، زیرا لازم نیست یک پورت اینترفیس به صورت پویا خود را پیکربندی کند .هنگامی که دستگاهی به شبکه اضافه می شود، اطمینان حاصل کنید که تمام پورت های اینترفیس به طور صریح به عنوان پورت ترانک یا پورت اکسس پیکربندی شده اند .سیستم‌هایی که فریم‌های کپسوله‌شده VLAN را مدیریت نمی‌کنند باید به پورتی متصل شوند که فقط برای مود اکسس پیکربندی شده است .فقط با دستورات پیکربندی زیر یک پورت اینترفیس را برای دسترسی استاتیک پیکربندی کنید:

```
interface <INTERFACE>
switchport mode access
```

با دستورات پیکربندی زیر، یک پورت اینترفیس را به صورت یک ترانک پیکربندی کنید:

```
interface <INTERFACE>
switchport mode trunk
```

۹,۲ Port security را فعال کنید.

پورت های اینترفیس فیزیکی دستگاه ها اغلب آخرین خط دفاعی و ابزار اصلی محدود کردن دسترسی به شبکه هستند. امنیت پورت تعداد آدرس‌های MAC معتبر مجاز برای اتصال به یک سوئیچ پورت را محدود می‌کند و اتصال را فقط به افراد مجاز محدود می‌کند. یک سوئیچ پورت پیکربندی نشده برای اعمال امنیت پورت می تواند به یک دشمن با دسترسی فیزیکی اجازه دهد تا یک سیستم غیرمجاز را متصل کند. سپس دشمن می‌تواند به عنوان یک سیستم قابل اعتماد عمل کند و محدودیت‌های امنیتی موجود را دور بزند، اطلاعات شبکه را جمع‌آوری کند، به عمق شبکه وارد شود یا سیستم‌های داخلی را به خطر بیندازد. NSA توصیه می‌کند که port security را در تمام سوئیچ‌پورت‌های فعال یک دستگاه فعال کنید و حداکثر تعداد آدرس‌های MAC مجاز را برای هر پورت دقیقاً یک یا دو تنظیم کنید، اگر از قابلیت‌های VoIP استفاده

می‌شود. Port security جایگزینی برایNAC ، مانند ۸۰۲,۱ Xنیست، اما باید زمانی استفاده شود که NAC قابل اجرا نباشد. در صورت امکان، یک آدرس MAC ثابت به هر سوئیچ پورت که به یک سیستم شناخته شده متصل است اختصاص دهید، و هر سوئیچ پورت را به گونه ای پیکربندی کنید که در صورت بروز نقض امنیت پورت، یک پیام SNMP trap ارسال شود. Port security را می توان در رابط های ترانک فعال کرد. با این حال، توصیه نمی شود، زیرا نیاز به دانستن تعداد دستگاه هایی دارد که دارای ترافیک هستند. یک سوئیچ پورت پویا نمی تواند port security را به طور همزمان فعال کند و ابتدا باید برای دسترسی ایستا پیکربندی شود تا port security فعال شود.

با دستورات پیکربندی زیر، port security را در یک اینترفیس با مود اکسس ایستا با حداکثر یک آدرس MAC فعال کنید:

```
interface <INTERFACE>
switchport mode access
switchport port-security
switchport port-security maximum 1
switchport port-security violation shutdown
switchport port-security mac-address sticky
```

کلمه کلیدی sticky به دستگاه این امکان را می دهد که پس از اتصال اولین سیستم مجاز به آن پورت، آدرس MAC را در پیکربندی وارد کند .توجه داشته باشید که برای حفظ اطلاعات پس از راه‌اندازی مجدد، پیکربندی باید ذخیره شود .اگر خاموش کردن یک پورت به دلیل نگرانی‌های مربوط به در دسترس بودن، اقدام قابل قبولی نیست، کلمه کلیدی shutdown را می‌توان با restrict جایگزین کرد تا از برقراری ارتباط هر گونه آدرس MAC اضافی در آن پورت جلوگیری شود.

۹,۳ VLAN پیشفرض را غیر فعال کنید.

اکثر سوئیچ ها از VLAN 1 به عنوان پیش فرض استفاده می کنند، از جمله پورت های مدیریت، که ممکن است دسترسی مستقیم به سوئیچ را برای مدیریت فراهم کند. علاوه بر این، برخی از پروتکل های لایه ۲ (به عنوان مثال، دیسکاوری یا ترانکینگ) باید روی یک VLAN خاص در لینک های ترانک ارسال شوند و VLAN 1 به طور کلی به عنوان پیش فرض انتخاب می شود. اگر اقدامات میتیگیشن انجام نشود، VLAN پیش‌فرض ممکن است کل شبکه را در بر گیرد و دستگاه‌های مورد اعتماد را در معرض خطر امنیتی بالاتری قرار دهد که توسط دستگاه‌های غیرقابل اعتمادی که دسترسی دارند، مورد بهره‌برداری قرار گیرند. NSA توصیه می‌کند که تمام ترافیک مدیریتی و عملیاتی را بهVLAN های مختلف (نه پیش‌فرض) منتقل کنید که ترافیک مدیریت را از داده‌های کاربر و ترافیک پروتکل جدا می‌کند و همچنین از سوئیچ‌های متعدد برای جداسازی سطوح امنیتی مختلف ترافیک شبکه استفاده کنید. VLAN پیش‌فرض همچنین باید منطقاً در همه ترانک‌ها و پورت‌های دسترسی که به آن نیازی ندارند (از جمله درگاه‌های قطع شده و خاموش) غیرمجاز باشد تا اطمینان حاصل شود که پخش غیرضروری، چندپخشی و ترافیک مقصد ناشناخته را منتقل نمی‌کند .فریم هایی که در پورت های ترانک ارسال و دریافت می شوند معمولا با شناسه VLAN مرتبط با فریم برچسب گذاری می شوند. هر فریم دریافتی که برچسب گذاری نشده باشد به طور خودکار در VLAN ترانکینگ بومی مرتبط با آن پورت قرار می گیرد. ترانکینگ بومی VLAN باید در هر دو انتهای یک پیوند ترانک یکسان تخصیص داده شود. به طور مشابه، فریم هایی که در پورت های دسترسی ارسال و دریافت می شوند، به دسترسی VLAN مرتبط با آن پورت اختصاص داده می شوند. همه سوئیچ پورت ها به یک VLAN دسترسی و یک VLAN ترانکینگ بومی اختصاص داده می شوند، صرف نظر از اینکه آنها پورت ترانک یا دسترسی هستند. NSA توصیه می کند که تمام پورت های ترانک را به یک VLAN ترانکینگ بومی منحصر به فرد اختصاص دهید که فقط به پورت های ترانک اختصاص داده شده

است و VLAN دسترسی را به یک VLAN استفاده نشده و غیرفعال اختصاص دهید. به طور مشابه، NSAتوصیه می‌کند که تمام پورت‌های اکسس را به VLAN دسترسی مناسب اختصاص دهید، و VLAN ترانکینگ بومی را به VLAN استفاده نشده و غیرفعال دیگری، متفاوت از پورت‌های استفاده شده توسط پورت‌های ترانک، اختصاص دهید. این پیکربندی مانع از پرش دشمن بین VLAN های فعال با برچسب گذاری عمدی ترافیکی می شود که در غیر این صورت برچسب گذاری نمی شود.

۹,۴ پورت های استفاده نشده را غیر فعال کنید.

فعال کردن پورت‌های بلااستفاده در دستگاه به دشمن اجازه می‌دهد یک دستگاه مخرب را به شبکه متصل کند و جمع‌آوری اطلاعات انجام دهد یا تلاش‌هایی را برای ایجاد خطر در شبکه آغاز کند .همه پورت های استفاده نشده باید غیرفعال شوند و در یک VLAN استفاده نشده ، که پیش فرض نیست قرار گیرند. .این کار به جلوگیری از دسترسی به شبکه، حتی اگر پورت‌ها فعال شوند، منجر خواهد شد .قبل از غیرفعال کردن یک پورت، باید بررسی کنید که واقعاً استفاده نشده است و به هیچ چیز متصل نیست .اگر دستگاه متصل به پورت خاموش باشد، ممکن است به نظر برسد که درگاه سوئیچ استفاده نشده است .تمام اینترفیس های استفاده نشده را خاموش کنید و با دستورات پیکربندی مثال زیر، VLANهای اکسس و ترانکینگ بومی را به VLAN های استفاده نشده و غیرفعال اختصاص دهید:

```
vlan 999
name UNUSED-DISABLED
shutdown

interface <INTERFACE>
switchport mode access
switchport access vlan 999
switchport trunk native vlan 998
no switchport voice vlan
shutdown
```

۹,۵ پورت مانیتورینگ را غیر فعال کنید.

پورت مانیتورینگ در یک سوئیچ شبکه برای ارسال یک کپی از بسته های شبکه مشاهده شده در یک سوئیچ پورت به یک اتصال نظارت بر شبکه در یک سوئیچ پورت دیگر استفاده می شود. دستگاهی که دارای یک یا چند سشن مانیتورینگ پورت تعریف شده است، اجازه می دهد مجموعه ای از پورت های مبدا توسط یک پورت مقصد مشخص نظارت شود و تمام ترافیک ارسال شده به یا از پورت های مبدا نیز به پورت مقصد ارسال می شود. پورت مانیتورینگ معمولاً برای اتصالNIDS ، تشخیص مشکل یا استفاده از تحلیلگر شبکه برای نظارت بر شبکه استفاده می‌شود. بسته به فروشنده، پورت مانیتورینگ همچنین به عنوان "Port mirroring" یا "Port spanning" شناخته می شود. یک دشمن متصل به پورت مقصد روی یک سشن نظارت پورت می‌تواند ترافیک شبکه ارسال شده از طریق تمام پورت‌های مبدأ مشخص شده توسط سشن را جمع‌آوری کند. NSA توصیه می کند که تمام سشن های نظارت بر پورت غیرفعال در یک دستگاه را غیرفعال کنید. پورت مانیتورینگ فقط باید برای آن پورت‌هایی فعال شود که ضروری است، و زمانی که دیگر مورد نیاز نیستند، باید غیرفعال شود. نمونه هایی از این ضرورت NIDS یا یک مدیر نظارت بر شبکه است .

سشن های مانیتورینگ تعریف شده در پیکربندی را با دستور exec زیر فهرست کنید:

```
show monitor session [1|2|all]
```

یک سشن مانیتورینگ تعریف شده را با دستور پیکربندی زیر را حذف کنید:

```
no monitor session <SESSION#>
```

۹,۶ Proxy ARP را غیر فعال کنید.

Proxy ARP تکنیکی است که در آن یک سرور پراکسی در یک شبکه به درخواست های ARP برای یک آدرس IP که در آن شبکه نیست پاسخ می دهد .این موضوع به دستگاه های موجود در یک زیرشبکه کمک می کند تا به زیرشبکه های راه دور دسترسی پیدا کنند، بدون اینکه مسیریابی را در یک دیفالت گیت وی پیکربندی کند .این مورد می تواند سودمند باشد زیرا می تواند بدون پردازش جداول مسیریابی از شبکه های دیگر به یک روتر اضافه شود، اما باید توجه داشت که فقط در بین بخش های شبکه محلی قابل اعتماد (LAN) ایمن است .این تکنیک آسیب‌پذیری‌ها را وارد شبکه می‌کند زیرا دشمنان می‌توانند یک سیستم قابل اعتماد را جعل کنند و بسته‌ها را رهگیری کنند. NSA توصیه می‌کند ARP پروکسی را در همه اینترفیس ها غیرفعال کنید، مگر اینکه دستگاه به عنوان بریج LAN استفاده شود یا اجازه ترجمه آدرس شبکه ورودی (NAT) را برای چندین آدرس IP مقصد بدهد .

با دستور exec زیر اینترفیس هایی را که ARP پروکسی دارند پیدا کنید:

```
show ip interface
```

Proxy ARP را در یک اینترفیس شخصی با دستورات پیکربندی زیر غیرفعال کنید:

```
interface <INTERFACE>
no ip proxy-arp
```

۱۰. بنرهای اطلاع رسانی

توصیه های فنی ارائه شده در این سند می تواند احتمال سوء استفاده دشمن از یک آسیب پذیری در شبکه را به میزان قابل توجهی کاهش دهد . متأسفانه، یک دشمن یا خودی ممکن است همچنان بتواند نقطه ضعفی برای خرابکاری، دور زدن یا مختل کردن شبکه پیدا کند .داشتن یک بنر اعلان می تواند روشن کند که چه چیزی برای هرکسی که به سیستم دسترسی دارد مجاز است و هرگونه اخطار و سلب مسئولیت لازم را اضافه می کند.

۱۰,۱ ارائه یک بنر اطلاع رسانی

بسته به نیاز سازمان، یک بنر اعلان می‌تواند به کاربران اطلاع دهد که اتصال به دستگاه تحت شبکه فقط برای استفاده مجاز است و هرگونه استفاده از سیستم منوط به نظارت برای هر هدف مجاز می باشد. یک بنر قانونی کافی تضمین می کند که مالک شبکه و سایرین، از جمله دولت،

می توانند اقدامات لازم را برای نظارت و ایمن سازی شبکه انجام دهند. با این حال، الزامات دقیق برای چنین بنری بسته به سازمان و حوزه قضایی متفاوت است.

NSA توصیه می کند که هر دستگاه به گونه ای پیکربندی شود که هر زمان که کاربر به سیستم اطلاعاتی وارد می شود یا به هر سرویس راه دور متصل می شود، بنر اعلان کامل را ارائه دهد .دستگاه های سیسکو IOS دو نوع بنر دارند. بنر ورود به سیستم قبل از ورود کاربر نمایش داده می شود و پس از احراز هویت کاربر "پیام روز" نمایش داده می شود. حداقل، بنر اعلان باید برای کاربران مجاز و غیرمجاز که قصد ورود به سیستم را دارند نمایش داده شود. در صورت تمایل، می‌توان همان اطلاعات یا اطلاعات اضافی را پس از ورود به سیستم در اختیار کاربران تأیید شده قرار داد با دستور پیکربندی زیر قبل از اینکه کاربران وارد سیستم شوند، یک بنر اعلان اضافه کنید :

```
banner login ^
INSERT NOTIFICATION BANNER HERE
^
```

همان بنر اعلان یا اطلاعات اضافی را برای کاربران مجاز که با موفقیت احراز هویت کرده اند با دستور پیکربندی زیر اضافه کنید:

```
banner motd ^
INSERT NOTIFICATION BANNER HERE ADDITIONAL INFORMATION
^
```

۱۱. نتیجه گیری

راهنمایی های موجود در این گزارش نشات گرفته از عمق و وسعت تجربه در کمک به مشتریان NSA در ارزیابی شبکه‌هایشان و ارائه توصیه‌هایی برای هاردنینگ فوری دستگاه‌های شبکه می باشد همراه با عملکردهای تعمیر و نگهداری ضروری، مدیران نقش مهمی در دفاع از شبکه ها در برابر تهدیدات متخاصم ایفا می کنند .پیروی از این راهنما به این مدافعان شبکه کمک می‌کند تا بهترین شیوه‌های امنیت سایبری را به اجرا درآورند، ریسک در برابر خرابکاری را کاهش داده و شبکه ای امن‌تر و محافظت‌شده‌تر را تضمین کنند.

۱۲. منابع

[1] Cybersecurity and Infrastructure Security Agency (2022), Layering Network Security Through Segmentation. Available at: https://www.cisa.gov/sites/default/files/publications/layering-network-security-segmentation_infographic_508_0.pdf

[2] National Security Agency (2019), Segment Networks and Deploy Application-aware Defenses. Available at: https://www.nsa.gov/cybersecurity-guidance

[3] National Security Agency (2021), Selecting and Hardening Remote Access VPN Solutions. Available at: https://www.nsa.gov/cybersecurity-guidance

[4] Committee on National Security Systems (2016), CNSS Policy 15. Available at: https://www.cnss.gov/CNSS/issuances/Policies.cfm

[5] Corcoran, Jenkins, NSA (2021), Commercial National Security Algorithm (CNSA) Suite Cryptography for Internet Protocol Security (IPsec). Available at: https://datatracker.ietf.org/doc/html/draft-corcoran-cnsa-ipsec-profile

[6] National Security Agency (2020), Configuring IPsec Virtual Private Networks. Available at: https://www.nsa.gov/cybersecurity-guidance

[7] National Security Agency (2019), Mitigating Recent VPN Vulnerabilities. Available at: https://www.nsa.gov/cybersecurity-guidance

[8] National Security Agency (2021), Eliminating Obsolete Transport Layer Security (TLS) Protocol Configurations. Available at: https://www.nsa.gov/cybersecurity-guidance

[9] Cisco Systems, Inc. (2022), Support & Downloads. Available at: https://www.cisco.com/c/en/us/support/index.html

[10] National Security Agency (2016), Network Device Integrity (NDI) Methodology. Available at: https://www.iad.gov/iad/library/reports/network-device-integrity-methodology.cfm

[11] National Security Agency (2016), Network Device Integrity (NDI) on Cisco IOS devices. Available at: https://www.iad.gov/iad/library/reports/network-device-integrity-ndi-cisco-ios-devices.cfm

[12] National Security Agency (2016), Validate Integrity of Hardware and Software. Available at: https://www.iad.gov/iad/library/ia-guidance/security-tips/validate-integrity-of-hardware-and-software.cfm

[13] National Security Agency (2022), Cisco Password Types: Best Practices. Available at: https://www.nsa.gov/cybersecurity-guidance

[14] Office of Management and Budget (2021), Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents. Available at: https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf

[15] Cooley, D, NSA (2021), Commercial National Security Algorithm (CNSA) Suite Profile for TLS and DTLS 1.2 and 1.3. Available at: https://datatracker.ietf.org/doc/html/draft-cooley-cnsa-dtls-tlsprofile

[16] Gajcowski, Jenkins, NSA (2021), Commercial National Security Algorithm (CNSA) Suite Cryptography for Secure Shell (SSH). Available at: https://datatracker.ietf.org/doc/html/draft-gajcowski-cnsa-ssh-profile

[17] National Institute for Standards and Technology (2020), Special Publication 800-52 Rev. 2: Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations. Available at: https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final

[18] Cisco Systems, Inc. (2017), Cisco Smart Install Protocol Misuse. Available at: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170214-smi

[19] National Security Agency (2017), Cisco Smart Install Protocol Misuse. Available at: https://www.nsa.gov/cybersecurity-guidance

[20] Cybersecurity and Infrastructure Security Agency (2022), Guidance on Consent Banners. Available at: https://www.cisa.gov/publication/guidance-consent-banners

 National Institute of Standards and Technology (2020), Special Publication 800-207: Zero Trust Architecture. Available at: https://www.nist.gov/publications/zero-trust-architecture

 Defense Information Systems Agency (DISA) and National Security Agency (NSA) Zero Trust Engineering Team (2021), Department of Defense (DOD) Zero Trust Reference Architecture. Available at: https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v1.1(U)_Mar21.pdf

 National Institute for Standards and Technology (2020), Special Publication 800-63B: Digital Identity Guidelines - Authentication and Lifecycle Management. Available at: https://pages.nist.gov/800-63-3/sp800-63b.html

 National Security Agency (2019), Continuously Hunt for Network Intrusions. Available at: https://www.nsa.gov/cybersecurity-guidance

 National Security Agency (2021), Embracing a Zero Trust Security Model. Available at: https://www.nsa.gov/cybersecurity-guidance

 National Security Agency (2020), Hardening Network Devices. Available at: https://www.nsa.gov/cybersecurity-guidance