تسلط بر مفاهیم پایه شبکه منطبق با استانداردهای بین‌المللی

آموزش رایگان دوره نتورک‌پلاس (Network+) (بخش 60)

در شماره گذشته آموزش نتورک‌پلاس با استانداردهای امنیتی WPA، WPA2، پروتکل احراز هویت توسعه پذیر،EAP EAP-TLS، Protected EAP، تأیید هویت انعطاف‌پذیر EAP از طریق تونل زدن امن و ابزارهای مانیتورینگ آشنا شدیم. در این شماره مبحث فوق را ادامه خواهیم داد.

برای مطالعه بخش پنجاه و نهم آموزش رایگان و جامع نتورک پلاس (Network+) اینجا کلیک کنید

ابزارهای نظارت بر شبکه می‌توانند حداقل قابلیت‌های زیر را ارائه می‌کنند:

• تنظیم کارت شبکه برای کار در حالت بی قاعده برای هدایت تمامی ترافیک شبکه به سمت نرم‌افزار نظارتی

• نظارت مستمر روی ترافیک متعلق به یک بخش شبکه

• ضبط اطلاعات انتقال پیدا کرده روی یک بخش از شبکه

• ضبط فریم‌های ارسال شده یا دریافت شده از سوی یک گره خاص.

• بازطراحی مجدد وضعیت شبکه با انتخاب حجم و نوع داده‌ها

• آماده‌سازی اطلاعات آماری در ارتباط با فعالیت شبکه (به‌طور مثال، چند درصد از کل فریم‌های منتقل شده در یک بخش خاص فریم‌های پخشی بوده‌اند.)

برخی از ابزارهای نظارت بر شبکه ضمن ارائه قابلیت‌هایی که به آن‌ها اشاره شد، قابلیت‌های زیر را نیز ارائه می‌کنند:

• شناسایی تمامی گره‌های شبکه که روی یک بخش قرار دارند.

• ایجاد یک خط پایه با هدف ارزیابی عملکرد، میزان بهره وری و...

• پیگیری وضعیت استفاده از منابع شبکه (مانند پهنای باند و فضای ذخیره‌سازی) و منابع حساس (همچون پردازنده یا استفاده از حافظه) و ارائه این اطلاعات به صورت نمودار، جدول یا چارت.

• ذخیره‌سازی اطلاعات ترافیکی و گزارش‌های تولید شده.

• ضبط و نمایش هشدارها زمانی که وضعیت ترافیک شبکه در آستانه بحرانی شدن قرار می‌گیرد. (به‌طور مثال، اگر مصرف بیش از 60 درصد ظرفیت شده است.)

• شناسایی ناهنجاری‌ها در زمان استفاده از منابع (میزبان‌هایی که مقدار زیادی از اطلاعات را ارسال می‌کنند) یا پورت‌ها یا دستگاه‌هایی که میزبان زیادی از داده‌ها را دریافت می‌کنند.

برای آن‌که بتوانید منبع بروز مشکل در شبکه‌ای را شناسایی کنید به ابزارهای درستی نیاز دارید. ابزارهای نظارتی، داده‌هایی در اختیارتان قرار می‌دهند که برای تجزیه‌وتحلیل ترافیک (**traffic analysis**) مفید بوده و اجازه می‌دهند جریان ترافیک شبکه را برای بررسی الگوها و حالت‌های خاص بررسی کنید. به‌طور مثال، تجزیه‌وتحلیل ترافیک باعث آشکار شدن مکان‌هایی می‌شود که باعث بروز تنگنا در شبکه شده‌اند، یک دستگاه قدیمی که باید جایگزین شود یا یک سرویس شبکه که نیازمند منابع بیشتری است از جمله این موارد است. با این حال، یک پروتکل تحلیل‌گر اطلاعات می‌تواند با تحلیل بسته‌ها اطلاعات عمیق‌تری در ارتباط با بسته‌های خاص ارائه کرده و پروتکل‌ها، خطاها و پیکربندی‌های اشتباه را آشکار کند. هر دو ابزار اطلاعات مفیدی در اختیارتان قرار می‌دهند، با این حال باید ابزاری که مناسب‌تر بوده و منبع بروز مشکل را سریع‌تر مشخص می‌کند را انتخاب کنید. استفاده دقیق و درست از ابزارهای نظارت بر شبکه می‌تواند از بروز مشکلات زیر پیشگیری کند: (دقت کنید بهتر است اصطلاحات تخصصی هر یک از تعاریف زیر را حفظ کنید تا در آزمون **نتورک‌پلاس** مشکلی پیدا نکنید.)

• runts- به بسته‌هایی که اندازه‌ای کمتر از مقدار مشخص شده دارند اشاره دارد. به‌طور مثال، هر بسته اترنت که اندازه‌ای کمتر از 64 بایت دارد یک runts نامیده می‌شود.

• giants- به بسته‌هایی اشاره دارد که اندازه آن‌ها فراتر از حداکثر اندازه رسانه است. به‌طور مثال، یک بسته اترنت بزرگ‌تر از 1518 بایت (یا 1522 بایت برای بسته‌های VLAN) یک gaint نامیده می‌شوند.

• jabber- دستگاهی است که سیگنال‌های الکتریکی را به‌طور نامناسبی مدیریت می‌کند که باعث می‌شود عملکرد سایر بخش‌های شبکه با مشکل روبرو شود.

• ghosts- فریم‌هایی که در حقیقت فریم‌های داده‌ای نیستند، اما به واسطه تعریف اشتباهی که از ولتاژها روی یک سیم ارائه می‌کنند باعث خرابی دستگاه‌ها می‌شوند. بر خلاف فریم‌های داده‌ای واقعی، ghosts یک الگوی نامعتبر در ابتدای الگوی فریم خود دارند.

• packet loss- بسته‌هایی هستند که به دلیل وجود یک پروتکل ناشناخته، پورت ناشناخته یا یک وضعیت غیرعادی از دست رفته‌اند و در عمل باعث ایجاد نویز در شبکه یا سایر ناهنجاری‌ها می‌شوند. بسته‌های از دست رفته هرگز به مقصد خود نمی‌رسند.

• discarded packets- بسته‌هایی هستند که به مقصد خود می‌رسند، اما پس از دریافت دور ریخته شده و گم می‌شوند، زیرا مسائلی مانند سرریز بافر، زمان تأخیر، تنگناها و سایر مشکلات تراکمی را برای شبکه به وجود می‌آورند. بسته‌ای که حذف می‌شود اغلب دور انداخته می‌شود.

• interface resets- بازنشانی مجدد اتصال، مشکلی که باعث کاهش کیفیت می‌شود. این مشکل عمدتا به دلیل پیکربندی اشتباه رخ می‌دهد.

هر یک از مشکلاتی که به آن‌ها اشاره شد، باعث می‌شوند تا هشدار یا پیغام خطایی در سیستم ثبت شود. بسته به پیکربندی سیستم، هشدار می‌تواند از طریق پیام کوتاه، ایمیل یا پیامک برای مدیر شبکه ارسال شوند. البته هشدارها به شکل خودکار در یک سیستم ثبت شده و در بخش گزارش‌های مربوط به رخدادادها ثبت می‌شوند. بیشتر دستگاه‌های شبکه شبیه به روترها، سوییچ‌ها، سرورها و ایستگاه‌های کاری همراه با ابزارهای گزارش‌گیری که به شکل داخلی درون دستگاه‌ها قرار گرفته‌اند و قادر هستند گزارش‌ها را درون سامانه‌ها نگه‌داری کنند به بازار عرضه می‌شوند. سایر ابزارها هشدارهایی که دستگاه‌های متصل به شبکه تولید می‌کنند را جمع‌آوری می‌کنند. اجازه دهید به قابلیت‌ها هر دو ابزار نگاهی داشته باشیم.

System and Event Logs

سیستم‌عامل‌ها تقریبا هرگونه رخدادی که شناسایی کنند را ثبت و ضبط می‌کنند. این اطلاعات عمدتا درون فایل‌های گزارش ثبت می‌شوند. به‌طور مثال، هر بار که کامپیوتر شما یک آدرس IP از DHCP درخواست می‌کند و پاسخی دریافت نمی‌کند، این رویداد در قالب یک رخداد هشداری در سیستم ثبت می‌شود. به همین ترتیب، زمانی که یک میزبان تلاش می‌کند به میزبان دیگری متصل شود و دیوارآتش مانع از انجام این‌کار می‌شود رخداد مربوطه درون سیستم ثبت می‌شود. سیستم‌عامل‌های مختلف به‌طور پیش‌فرض رویدادهای مختلفی را ثبت و ضبط می‌کنند. علاوه بر این، مدیران شبکه می‌توانند با تعریف یکسری قواعد، زمانی که ورودی‌های جدیدی به شبکه وارد می‌شوند گزارش‌های سفارشی را دریافت کنند. به‌طور مثال، یک مهندس شبکه در نظر دارد هر زمان رطوبت نسبی مرکز داده بیش از 60 درصد شد گزارشی در این خصوص دریافت کند. در چنین شرایطی اگر یک دستگاه بتواند این اطلاعات نظارتی را به دست آورده و به شکل بلادرنگ برای کامپیوتری ارسال کند، اطلاعات فوق در قالب یک ورودی توسط سیستم ثبت خواهد شد. در رایانه‌های مبتنی بر ویندوز، چنین ورودی به نام event log شناخته شده و به سادگی توسط ابزار **Event Viewer** قابل مشاهده است. برای آشنایی با ابزار فوق و شیوه به‌کارگیری آن به مقاله **راهنمای جامع به‌کارگیری Event Viewer برای شناسایی مشکلات سیستم (بخش اول)** مراجعه کنید.

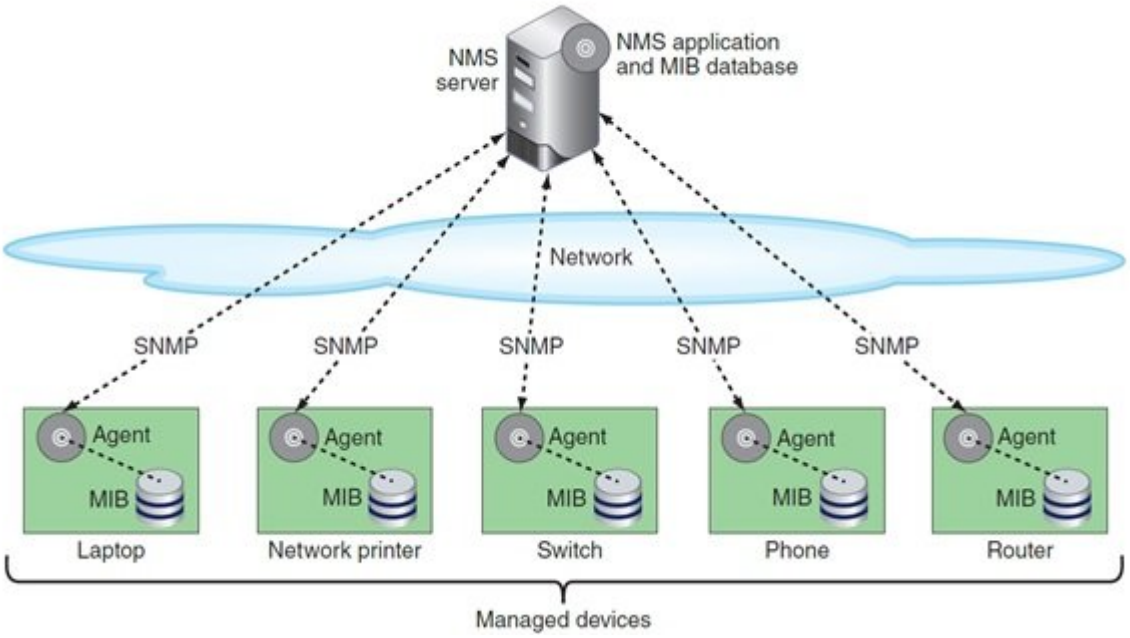
مشابه چنین اطلاعاتی در کامپیوترهایی که لینوکس یا یونیکس روی آن‌ها اجرا می‌شود از طریق ابزار **syslog** قابل مشاهده است. Syslog سرنام system log استانداردی برای تولید، ذخیره‌سازی و پردازش پیام‌هایی در ارتباط با رویدادهایی است که درون یک سیستم ثبت شده‌اند. استاندارد فوق روش‌هایی برای تشخیص و گزارش‌گیری از رویدادها و تعیین قالب و محتوایی برای پیام‌ها ارائه می‌کند. شکل زیر مکان گزارش‌های سیستمی در برخی از توزیع‌های لینوکس و یونیکس را نشان می‌دهد.

Version type	System log location
Newer versions of Linux	/var/log/messages
Older versions of UNIX	/var/log/syslog/
Solaris versions of UNIX	var/adm/messages

برای پیدا کردن مکانی که گزارش‌های سامانه‌های لینوکسی و یونیکس درون آن‌ها ذخیره می‌شود به etc/syslog مراجعه کنید. فایل conf در برخی از سامانه‌ها به صورت etc/rsyslog.conf ثبت می‌شود، فایل فوق مکانی است که می‌توانید پیکربندی انواع مخلفی از رویدادهای متعلق به گزارش‌ها و سطح اولویت اختصاص داده شده به هر رویداد را در آن مشاهده کنید. توجه داشته باشید که ابزار syslog هشداری در ارتباط با هرگونه مشکل در سیستم نشان نمی‌دهد، بلکه تنها تاریخچه‌ای از پیام‌های ثبت شده در سیستم را نگه‌داری می‌کند. در نتیجه این وظیفه شما است که گزارش‌های سیستم در ارتباط با خطاها را بررسی کرده یا برای داده‌ها یا بسته‌های شبکه که قرار است رصد شوند و در زمان اشکال‌زدایی یا بررسی الگوهایی که در تشخیص مشکلات راهگشا هستند فیلترهایی را مشخص کنید.

SNMP Logs

سازمان‌ها اغلب از سامانه‌های مدیریت شبکه در مقیاس سازمانی برای انجام کارهایی همچون گزارش‌گیری از کل شبکه استفاده می‌کنند. در یک سازمان بزرگ صدها ابزار این چنینی وجود دارد که همه آن‌ها بر مبنای معماری یکسانی کار می‌کنند. شکل زیر نشان می‌دهد که چگونه این نهادها درون یک شبکه با یکدیگر کار می‌کنند:



جزییات هر یک از مولفه‌های موجود در شکل بالا به شرح زیر است:

• سرور NMS (سیستم مدیریت شبکه) – در پایین‌ترین سطح یک کنسول مدیریت شبکه است که ممکن است یک سرور یا ایستگاه کاری باشد. بسته به اندازه شبکه، داده‌ها را از چند دستگاه مدیریت شده در فواصل منظم در یک فرآیند که polling نام دارد جمع‌آوری می‌کند.

• managed device- هر گره شبکه زیر نظارت یک سامانه NMS قرار دارد. هر دستگاه مدیریت شده تحت شبکه ممکن است شامل اشیا مختلفی باشد که هر یک از ویژگی‌های آن‌ها همچون پردازنده، حافظه، هارددیسک، کارت شبکه یا عملکردها زیر نظر سرور سیستم مدیریت شبکه رصد می‌شود. به هر شیء مدیریت شده یک شی شناسه هویتی OID سرنام object identifier تخصیص داده می‌شود.

• network management agent- هر دستگاه مدیریتی یک عامل مدیریت شبکه را اجرا می‌کند که یک پروسه نرم‌افزاری است که اطلاعاتی در مورد عملکرد دستگاه‌ها جمع آوری می‌کند و آن‌را به سامانه مدیریت شبکه تحویل می‌دهد. به‌طور مثال، در یک سرور، یک عامل می‌تواند برای اندازه‌گیری این مسئله که چه تعداد کاربر به سرور متصل شده‌اند یا چه مقدار از منابع پردازنده در هر زمان معینی استفاده می‌شوند به‌کارگرفته شود. برای آن‌که عملکرد شبکه در چنین حالتی کاهش پیدا نکند، عامل‌ها از حداقل منابع پردازشی استفاده می‌کنند.

• MIB سرنام Management Information Base –اشیا مدیریت شده با سرور NMS را فهرست کرده و همچنین توصیفی برای این اشیاء درون پایگاه اطلاعات مدیریتی خود نگه‌داری می‌کند. MIB همچنین اطلاعاتی در ارتباط با عملکرد اشیا در فرمت خاص بانک اطلاعاتی دارد که می‌توانند برای تجزیه‌وتحلیل استخراج شوند.

عامل‌ها اطلاعات مربوط به دستگاه‌های مدیریت شده را از طریق هر یک از پروتکل‌های لایه کاربرد انتقال می‌دهند. در شبکه‌های مدرن، اکثر عامل‌ها از پروتکل SNMP (سرنام Simple Network Management Protocol بخشی از مجموعه پروتکل‌های TCP / IP است و به‌طور معمول روی پروتکل UDP و از طریق پورت‌های 161 و 162 اجرا می‌شود) استفاده می‌کنند. سه نسخه از پروتکل SNMP به شرح زیر وجود دارد:

• SNMPv1 این نسخه اولیه در سال 1988 منتشر شد. به دلیل ویژگی‌های محدودی که دارد امروزه به ندرت در شبکه‌های مدرن از آن استفاده می‌شود.

• SNMPv2 این نسخه با هدف افزایش عملکرد و امنیت SNMPv1 و همچنین ویرایش برخی دیگر از قابلیت‌ها طراحی شد.

• SNMPv3 این نسخه شبیه به SNMPv2 است، اما احراز هویت، اعتبارسنجی و رمزگذاری را برای پیام‌های مبادله شده بین دستگاه‌های مدیریت شده و کنسول مدیریت شبکه اضافه کرد. SNMPv3 امن‌ترین نسخه این پروتکل است. با این حال، برخی از مدیران تمایل به ارتقاء به SNMPv3 ندارند، زیرا به تنظیمات پیچیده‌ای نیاز دارد. بنابراین، SNMPv2 هنوز به‌طور گسترده استفاده می‌شود. اکثر، اما نه همه، برنامه‌های کاربردی مدیریت شبکه از نسخه‌های مختلف SNMP پشتیبانی می‌کنند. در این‌جا یکسری پیام‌های کلیدی SNMP برای برقرار ارتباط میان دستگاه‌های مدیریت شده و NMS وجود دارد که از مهم‌ترین این پیام‌ها به موارد زیر می‌توان اشاره کرد:

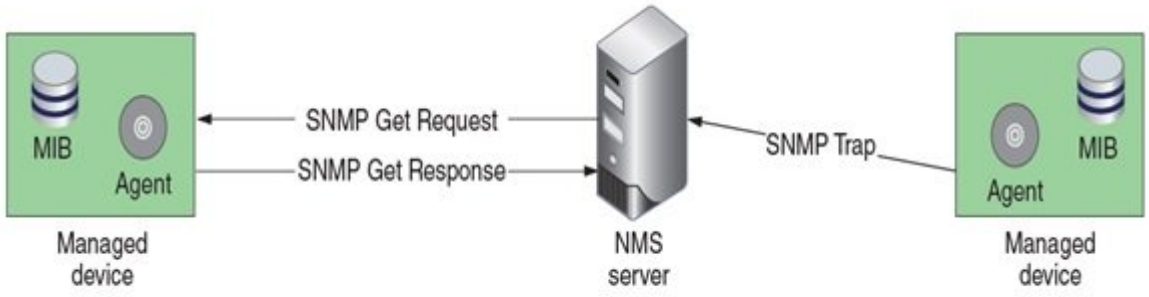
• NMS - SNMP Get Request درخواست دریافت داده‌ها را برای عاملی که روی یک دستگاه مدیریتی قرار دارد ارسال می‌کند. این موضوع در سمت چپ شکل زیر نشان داده شده است.

• SNMP Get Response - عامل پاسخی که شامل اطلاعات درخواستی است ارسال می‌کند.

• SNMP Get Next - پس از دریافت پاسخ، NMS ممکن است درخواستی مبنی بر دسترسی به ردیف بعدی داده‌ها در پایگاه داده MIB را ارسال کند.

• SNMP Walk-با استفاده از فرمان فوق، NMS می‌تواند معادل یک دنباله از پیام‌های SNMP Get Next را برای دریافت ردیف‌های متوالی در پایگاه داده MIB ارسال کند.

• SNMP Trap عاملی است که می‌تواند برنامه‌ریزی شده باشد تا شرایط غیرطبیعی را تشخیص داده و یک پیام SNMP Trap را تولید کند. این مسئله در سمت راست تصویر زیر نشان داده شده است. به‌طور مثال، در یک سرور سیسکو، شما می‌توانید با استفاده از دستور **snmp trap link-status** برای کمک به عامل SNMP برای ارسال یک هشدار زمانی که رابط از کار افتاده است استفاده کنید. trap در ادامه می‌تواند با فرمان **no snmp trap link-status** غیر فعال شود. پیام‌های SNMP trap می‌توانند به مدیران شبکه در ارتباط با سرویس‌ها یا دستگاه‌هایی که پاسخ‌گو نیستند، مسائل مربوط به منبع تغذیه، درجه حرارت بالا و قطع مدارات مختلف هشدار دهد تا تکنسین‌ها بتوانند به سرعت و به احتمال زیاد قبل از بروز یک مشکلی جدی خرابی‌های را برطرف کنند. به‌طور مثال، یک سرویس غیرپاسخگو همچون DHCP می‌تواند از راه دور دوباره راه‌اندازی شود.



نکته امتحانی: هنگام استفاده از UDP، عامل‌های SNMP درخواست‌های ارائه شده از سوی NMS را در پورت 161 دریافت می‌کنند. NMS نیز پاسخ‌های ارائه شده از سوی یک عامل و traps را روی پورت 162 دریافت می‌کند. پیام‌های SNMP را می‌توان با TLS ایمن کرد، در این صورت عامل‌ها درخواست‌ها را در پورت 10161 دریافت می‌کنند و NMS نیز پاسخ‌ها و traps را روی پورت 10162 دریافت می‌کند.

پس از جمع‌آوری داده‌ها، برنامه مدیریت شبکه می‌تواند از طریق به‌کارگیری روش‌های مختلفی اطلاعات و تحلیل‌های انجام شده را در اختیار مدیر قرار دهد. به‌طور مثال، یک روش بسیار رایج برای تجزیه و تحلیل داده‌ها استفاده از یک گراف خطی است. زمانی که صحبت از نظارت بر عملکرد شبکه به میان می‌آید، ایجاد داده‌ها ساده‌ترین بخش داستان است. چالش اصلی در ارتباط با تحلیل موثر و مفید داده‌های به دست آمده است که شماره آینده این موضوع را بررسی خواهیم کرد.

در شماره آینده آموزش **نتورک‌پلاس** مبحث فوق را ادامه خواهیم داد.

تاریخ انتشار:

20 خرداد 1398

نشانی منبع:
https://www.shabakeh-mag.com/tricks/network-tricks/15516/%D8%A2%D9%85%D9%88%D8%B2%D8%B4-%D8%B1%D8%A7%DB%8C%DA%AF%D8%A7%D9%86-%D8%AF%D9%88%D8%B1%D9%87-%D9%86%D8%AA%D9%88%D8%B1%DA%A9%E2%80%8C%D9%BE%D9%84%D8%A7%D8%B3-network-%D8%A8%D8%AE%D8%B4-60