FORTINET
NSE Training Institute

NSE 2 Network Access Control Scripts—Spanish Version

¡Hola! En esta clase, presentaremos el control de acceso a la red, <pausa> NAC, y explicaremos cómo ha evolucionado.

El NAC es una herramienta o máquina virtual que controla el acceso de los dispositivos a la red. Al principio, era un método de autenticación y autorización para incorporar dispositivos a la red, según los estándares IEEE 802.1X. La autenticación constaba de tres elementos:

el dispositivo del cliente <ícono>

el autenticador <ícono>

el servidor de autenticación <ícono>

El autenticador podía ser un conmutador de red o un punto de acceso inalámbrico que diferenciaba una red protegida de una que no lo estaba. El cliente proveía credenciales, como un nombre de usuario y una contraseña o un certificado digital al autenticador, que a su vez las enviaba al servidor. Según el resultado de la autenticación, el autenticador podía bloquear el dispositivo o permitirle el acceso a la red. Otro método para controlar el acceso a la red, especialmente a una red pública, es el portal cautivo. Si usted alguna vez se conectó a la red de un aeropuerto, un hotel o una cafetería, puede que recuerde haber interactuado con una página web que le solicitaba su conformidad con los términos legales antes de acceder.

Más tarde, el control de acceso a la red evolucionó e incluyó lo siguiente:

acceso de invitados <ícono>

la tendencia "traiga su propio dispositivo", <pausa> o BYOD <ícono>

y la internet de las cosas, <pausa> o IoT <ícono>

Por dos motivos, tanto la tendencia BYOD como la internet de las cosas presentaron nuevos retos de seguridad. En primer lugar, los dispositivos individuales son de propiedad personal, no son recursos de una empresa. Por esa razón, el sistema de información de gestión (MIS) no controla lo que se ejecuta en ellos, por ejemplo, programas antivirus o aplicaciones inseguras. En segundo lugar, la internet de las cosas consta de hardware con un sensor que transmite datos por internet, de un lugar a otro, lo que amplía de manera considerable la superficie expuesta a ataques. Las empresas adquieren dispositivos habilitados para IoT a través de proveedores externos. Los dispositivos se conectan a la red del proveedor para obtener información acerca del uso del producto y su mantenimiento. Las empresas aceptan esta situación porque estos dispositivos permiten ahorrar tiempo y dinero. Por ejemplo, si una impresora tiene poca tinta, el proveedor puede notificar al administrador de la red por correo electrónico o, incluso, entregar cartuchos de tinta nuevos de manera automática. En un hogar inteligente, la internet de las cosas regula la temperatura y la humedad, verifica que las puertas estén cerradas con llave, lleva un control de lo que hay en el refrigerador o, incluso, ayuda con la lista de compras.

La conveniencia obvia de estos dispositivos los ha hecho extremadamente populares y numerosos. Sin embargo, debido a su diversidad, a la falta de estándares y a la imposibilidad de protegerlos, son un medio de contagio potencial que puede acceder a la red. Muchos dispositivos de internet de las cosas no cuentan con los ciclos de CPU o la memoria suficientes para alojar software de autenticación y seguridad. Se identifican mediante un secreto compartido o un número de serie único que se introduce durante la fabricación. Pero este esquema de autenticación es muy limitado: si el secreto se hace público, probablemente no haya forma de restablecerlo. Además, como no es posible instalar un software de seguridad, los dispositivos son poco visibles. Afortunadamente, el control de acceso a la red ha evolucionado y solucionado estos problemas.

Cuando un sistema de información de gestión incorpora el control de acceso a una red, en primer lugar el control de acceso a la red crea perfiles de todos los dispositivos conectados. Luego, habilita el acceso a los recursos de la red de acuerdo con el perfil del dispositivo, que se define

por su función. Es algo similar a cuando a una persona se le otorga permiso para acceder a información confidencial según lo que necesite saber. Por ejemplo, el control de acceso a la red permite conectar una cámara IP al servidor de una grabadora de video en red (NVR), pero no a un servidor con información financiera. Por su perfil, una grabadora de video en red no necesita conectarse a un servidor financiero. Con este tipo de permiso de acceso, la red se segmenta de acuerdo con la función de los dispositivos. Si alguno resulta vulnerable, un malware solo puede infectar los objetos a los que el dispositivo se puede conectar. Así, en el ejemplo anterior, si la cámara IP es vulnerable, puede infectar el servidor de la grabadora de video en red pero no el financiero.

Si bien se comprobó que el control de acceso a la red es muy efectivo para administrar numerosos dispositivos sin protección, presentó algunas falencias en su evolución. Algunas soluciones de este tipo se diseñaron para la incorporación (*onboarding*) de dispositivos personales (BYOD) en redes inalámbricas, pero su desempeño era muy pobre en la parte cableada de la red. Otras soluciones, que se desarrollaron para trabajar dentro del entorno de un proveedor único, no eran capaces de crear automáticamente perfiles de dispositivos de terceros. Algunas brindaban una buena visibilidad en redes pequeñas y simples, pero no escalaban bien en redes distribuidas y de mayor tamaño.

Actualmente, la mayoría de las soluciones de control de acceso a la red han superado estas limitaciones. Aportan una visibilidad completa de la red y son más efectivas para categorizar dispositivos de manera automática. Tienen un buen rendimiento tanto en redes Ethernet como en redes inalámbricas. Muchas de estas soluciones tienen una arquitectura centralizada que mejora el control de dispositivos en redes multisitio y de gran tamaño. Fundamentalmente, el control de acceso a la red debe estar integrado en el marco de seguridad. Así, cuando detecta una vulneración, puede responder para notificar automáticamente al centro de operaciones de seguridad (SOC) y coordinar con otros dispositivos de seguridad para neutralizar la amenaza.

Fortinet ofrece una solución de control de acceso a la red, conocida como FortiNAC™. Incluye todas las características mencionadas en esta clase.

Gracias por su tiempo, y no olvide responder el cuestionario a continuación.