Lectura 5

Lectura 5 - Port-Based Authentication Concepts

Redes

Preguntas

1. ¿Como funciona el Port-Based Authentication?
   Funciona como un sistema de control de acceso que verifia la identidad y las credenciales de un usuario o dispositivo y en base a estas darle acceso a la red o no darle el permiso. Uno de los estándar utilizados es el 802.1X en las redes LAN. Este proceso involucra componentes que se mencionaran mas adelante como por ejemplo:
   - Supplicant que pide permiso de conexión al authenticator
   - El authenticator bloque el acceso del supplicant hasta que esté autorizado.
   - El servidor de autenticación verifica las credenciales mediante el EAP.
   - Luego se da el acceso a la red o se lo niega.
     En la lectura aparece una analogía que explica muy bien el funcionamiento, esta lo hace mediante la Casa Blanca como ejemplo:
     Esta analogía muestra cómo funciona la autenticación 802.1X:
   - El **supplicant** (Terry) intenta acceder a la red.
   - El **authenticator** (el guardia) actúa como filtro y no permite el acceso hasta recibir confirmación.
   - El **servidor de autenticación** (Eva) verifica las credenciales (como el pasaporte) y decide si la persona debe tener acceso.
   - Si las credenciales son válidas, el puerto se “abre” y el usuario entra a la red.
2. Defina los componentes principales de 802-1x

- **Supplicant:** Es el dispositivo del cliente que necesita ser autenticado para darle permiso de acceso a la red. Una forma de mas simple de verlo, es como usuarios desconocidos o no identificados. Para considerar un supplicant valido, se necesita implementar 802.1X y un método específico EAP. El supplicant se conecta con el server de autenticación mediante este EAP.
- **Authenticator:** Es el dispositivo intermediario, como un switch Ethernet o un punto de acceso inalámbrico, que controla el acceso al puerto. Este actúa como un guardia de seguridad, bloqueando el acceso hasta recibir autorización del servidor de autenticación.

Una vez el sistema autentica el supplicant, el authenticator abre el puerto para que el supplicant ingrese a la red protegida.

- **Authentication Server:** Este en algún momento va a solicitar las credenciales del supplicant. Generalmente es un servidor RADIUS, que valida las credenciales del supplicant y decide si se le permite o no el acceso a la red.

3. ¿Por qué considera que este tipo de autenticación es relevante?
   Este tiempo de autenticación es importante, ya que, mantiene a los usuarios y las dispositivos no autorizados del acceso a recursos protegidos en la red. Sin un sistema de autenticación, un hacker podría acceder fácilmente al LAN conectando la computadora a un puerto Ethernet o el punto de acceso en una red inalámbrica. Una vez el hacker esta dentro, conectado a la red, este puede explotar cualquier fallo o vulnerabilidad en la seguridad. Existen muchas herramientas que puede utilizar un hacker para realizar el ataque dentro de la red y obtener información protegida y confidencial, por ejemplo: TCP scanner, de esta forma se puede tener la IP de usuarios conectados y otros datos. Además, de proteger la red de ataques de hacker y de acceso de usuarios no identificados, brinda otros servicios utiles para las empresas en cuanto seguridad. Por ejemplo: Seguimiento de ubicación del usuario, control de acceso basado en políticas y perfiles personalizados,