INSTITUTO TECNOLÓGICO DE CELAYA

MATERIA:
TÓPICOS AVANZADOS DE SEGURIDAD EN REDES CONVERGENTES

ALUMNA:
SANTANA DE LOS RÍOS CAROLINA

NÚMERO DE CONTROL:
13030622

TÍTULO:
NESSUS

FECHA DE ENTREGA:
07 DE NOVIEMBRE DEL 2017

INTRODUCCIÓN

Nessus es un programa de escaneo de vulnerabilidades para diversos sistemas operativos. Básicamente consiste en un demonio (nessusd) que realiza el escaneo en el sistema objetivo y otro demonio llamado nessus que muestra el avance e informa sobre el estado de los escaneos realizados.

Nessus comenzó en 1998, cuando Renaud Deraison decidió que la comunidad de Internet debería tener un escáner remoto de seguridad gratuito. Actualmente existen cuentas gratuitas y de paga.

NESSUS

Herramienta para realizar distintos análisis de vulnerabilidades sobre los equipos de red, similar al proceso de auditoría para una red.

El proceso de instalación para este software es sencillo sobre un SO Ubuntu 10.10. Básicamente consiste en realizar los siguientes pasos:

1. Descargar el instalador
2. Instalar la herramienta
3. Crear una cuenta en el sitio oficial de Nessus y obtener una clave de activación
4. Crear un usuario desde la consola de Ubuntu especificando su nombre y contraseña
5. Registrar el usuario desde la consola de Ubuntu, especificando la clave de activación obtenida en el paso 3.

Después de realizar estos pasos, ya solo queda ejecutar el servicio y verificar que todo esté funcionando bien comprobando que los números de puerto son correctos, por defecto Nessus escucha el puerto 1241 y su interfaz el 8834.

Para acceder a la consola web de administración, se realizan los siguientes pasos:

- Abrir un navegador web
- Ingresar alguna de las siguientes URL
    - https://localhost:8834
    - https://ip_servidor:8834
- Ingresar el usuario y contraseña configurados durante el proceso de instalación

Una vez que se ha autenticado al usuario y se tiene pleno acceso a la consola web de administración, es posible realizar varias acciones, desde crear más usuarios y asignarles distintos tipos de roles, hasta crear políticas y comenzar a configurar distintos tipos de escaneos.

Una política en Nessus es un conjunto de reglas y plugins que se ejecutan durante el proceso de un escaneo. Un plugin representa los tipos de ataques o pruebas que se realizarán sobre los dispositivos o redes que se analizarán. Nessus viene con algunas políticas ya configuradas y el administrador de red puede crear nuevas.

Para comenzar con un proceso de escaneo, es necesario tener ya configurada una política, debido a que ésta será ejecutada durante todo el proceso de análisis.

Nessus también permite especificar una hora o momento específico para ejecutar dicho análisis, así como los hosts o redes objetivos para el proceso.

Durante el escaneo, esta herramienta nos permite observar información detallada de cada host, puerto y vulnerabilidad encontrados. Es interesante la cantidad de información que puede obtenerse desde un simple análisis. Además, la GUI de Nessus es muy sencilla y amigable al usuario, por lo que es fácil de entender y utilizar.

Al finalizar cada análisis, se genera un reporte que contiene la siguiente información:

- Total de Hosts encontrados
- Total de vulnerabilidades encontradas
- Nivel de severidad por cada vulnerabilidad
- Total de puertos abiertos

Se debe tener en cuenta que varias vulnerabilidades encontradas por Nessus pueden representar un falso positivo, es decir, realmente la vulnerabilidad no existe o no representa un riesgo muy grande para el correcto funcionamiento de la red.

Los reportes son visualizados en una tabla sencilla de entender, pero también es posible ver los datos de manera más cómoda mediante gráficas de pastel, las cuales muestran los 10 tipos de vulnerabilidades más encontradas dentro del tráfico de red. Cada reporte puede ser descargado, exportado e importado para poder visualizarlo desde otro servidor Nessus.

Éstas son las operaciones básicas que se pueden realizar con Nessus. Sin embargo, existen ciertas características que se pueden ejecutar dependiendo del tipo de cuenta que se haya registrado durante el proceso de instalación. Los tres tipos de cuentas disponibles son: Home, Professional y Manager.

Las características de Nessus Home son las siguientes:

- Escaneo límite a 16 direcciones IP
- Alta velocidad de escaneo
- Evaluaciones acertadas con miles de verificaciones
- Disponible para un solo usuario

Nessus profesional cuenta con las siguientes características:

- Permite la creación de más de 20,000 usuarios
- Escaneo de un número ilimitado de direcciones IP
- Disponible para un solo usuario

Las características de Nessus Manager son las siguientes:

- Disponible para múltiples usuarios
- Escaneos basados en agentes
- Soporte multi escaneo
- Gestión de usuario
- Gestión de recursos
- Tableros de control

Características que los tres tipos de cuentas comparten:

- Auditoría de configuración
- Verificación de cumplimiento
- Detección de Virus
- Escaneo de aplicaciones web
- Búsqueda de datos sensibles
- Auditoría en sistemas de control
- Escaneo de redes múltiples
- Programación de escaneos

Además de las características anteriormente listadas, Nessus cuenta con varias ventajas que lo convierten en una opción muy viable, entre ellas se encuentran las siguientes:

- Nessus es una plataforma integrada que ofrece en una misma licencia la más extensa cobertura para la Gestión de Vulnerabilidades, verificación de configuraciones, plugins y actualizaciones.
- Multiplataforma
- Puede detectar en un día lo que a otras soluciones pueden tomarles meses.
- Cuenta con sus propios agentes de soporte local para el escaneo de vulnerabilidades, cumplimiento y auditoría local.
- Detecta eficazmente una amplia gama de amenazas como virus, malware, backdoors y servidores conectados a sistemas infectados con botnets.
- Muestra reportes que también sugieren soluciones

- La versión Professional garantiza la detección de más de 60,000 amenazas.

Teniendo todos estos aspectos en consideración, es posible encontrar varios beneficios de usar Nessus dentro de una empresa. Lo más seguro es que una empresa no implementará la cuenta tipo Home, sino más bien Professional o Manager, debido a la gran cantidad de ventajas que tienen en comparación con otras soluciones, las cuales están listadas en puntos anteriormente mostrados. Esto es, hablando de empresas medianas o grandes.

En cuanto a empresas pequeñas, posiblemente sea suficiente la opción Home, dependiendo del número de host que se encuentren en la red. Es de gran utilidad que este tipo de cuenta sea gratuita para que así la organización se ahorra algunos gastos en otras soluciones de paga. Además, aunque sea una versión gratuita aún proporciona ciertas características que soluciones de paga también ofrecen, por lo que puede considerarse como una buena opción para realizar el análisis del tráfico de red.

Los usuarios que no pertenecen a una empresa o que simplemente quieren implementar esta herramienta, solo requieren de conocimientos de redes para hacerlo, ya que se habla de protocolos y otros temas relacionados con la administración y seguridad en redes. El usuario puede implementar Nessus para verificar si existe algún problema en su red, por ejemplo, alguna aplicación que esté abarcando mucha bandwith en comparación con todo el tráfico de red.

Un usuario incluso puede implementar esta herramienta con fines educativos, puede utilizarla para practicar los temas teóricos de redes, entre ellos los puertos, protocolos, entre otros. También puede aprender sobre las soluciones recomendadas en cada reporte obtenido después de cada escaneo.

CONCLUSIÓN

Nessus es una herramienta tanto gratuita como de paga, dependiendo del tipo de cuenta seleccionada para trabajar. Puede ser implementada por grandes, medianas y pequeñas empresas, incluso por usuarios comunes con ciertos conocimientos de redes.

Es fácil de instalar, además de ser multiplataforma, por lo que puede ser implementado en distintos sistemas operativos. Incluye una GUI amigable al usuario, lo cual mejora la experiencia con el uso de esta herramienta. Me sorprendió la facilidad que hay para gestionar las políticas y los escaneos, me agradó mucho el poder agendar los escaneos y poder relacionarlo a una política ya configurada con varias vulnerabilidades o pruebas a realizar durante el mismo.

Los datos que pueden ser listados durante y al final de cada escaneo son muy completos, con Nessus es posible ver información sobre los hosts, puertos y protocolos. Además cada reporte incluye una sinopsis explicando un poco sobre el mismo y una recomendación para llegar a mitigar las vulnerabilidades encontradas.

Me parece una herramienta muy completa, muy útil y muy recomendable para realizar escaneos y análisis de redes.

REFERENCIAS

[1] Es.wikipedia.org. (2017). *Nessus*. [online] Available at: https://es.wikipedia.org/wiki/Nessus [Accessed 7 Nov. 2017].

[2] Informática, S. (2017). *NESSUS TUTORIAL*. [online] Seguridadcallosa2013.blogspot.mx. Available at: http://seguridadcallosa2013.blogspot.mx/2013/05/nessus-tutorial.html [Accessed 7 Nov. 2017].

[3] López, L. (2017). *Nessus de Tenable Vs. Nexpose de Rapid7*. [online] GB Advisors. Available at: http://www.gb-advisors.com/es/blog/nessus-de-tenable-vs-nexpose-rapid7/ [Accessed 7 Nov. 2017].

[4] Nessus Cloud, Manager & Professional. (2017). *Características Principales de la familia Nessus*. [online] Available at: http://nessus.gb-advisors.com/es/nessus-family-features/ [Accessed 7 Nov. 2017].

[5] Tenable™. (2017). *Tenable™ - The Cyber Exposure Company*. [online] Available at: https://www.tenable.com/ [Accessed 7 Nov. 2017].

[6] *Uso básico de Nessus*. (2011). [video] Youtube: Hotfixed.