ESCÁNER DE VULNERABILIDADES APLICANDO NESSUS

*S*antos Ireneo Juchasara Colque
sijucol@homail.com, sijucol@gmail.com

Docente Ingeniería Informática
Universidad Nacional Siglo XX
Llallagua, Bolivia

Resumen – *El ser humano invento la internet y tanto fue su desarrollo que en la actualidad se convirtió no solo en una necesidad sino un derecho, es así que en esta red de redes fluye gran cantidad de información de toda índole desde texto simple hasta información e audio video.*

Sin margo la preocupación es si la información que viaja por la red es segura o no, si es interceptado por ciertas personas que se dedican a atacar o apoderarse de dicha información, debido a los protocolos de comunicación es que muchos atacantes se infiltran en la red para sacar o extraer información de forma ilícita. Sin embargo es tanto el avance tecnológico que nos provee de ciertas herramientas para poder resguardar la información dentro una organización, dicha herramienta que se aplicó es nada menos que nessus, una herramienta libre para poder realizar un escáner de vulnerabilidades y de esta manera tomar los recaudos necesarios para proteger los datos que es de vital importancia en una organización.

Palabras Claves – *Seguridad informática; nessus; nessusd; nmap; vulnerabilidad; internet;*

Abstract – *The human being invented the internet and its development was so great that today it has become not only a necessity but a right, that is why in this network of networks a large amount of information of all kinds flows from simple text to information and audio Video.*

However, the concern is if the information that travels through the network is secure or not, if it is intercepted by certain people who are dedicated to attacking or seizing said information, due to the communication protocols is that many attackers infiltrate the network to extract or extract information illegally. However, there is so much technological advance that provides us with certain tools to be able to protect the information within an organization, said tool that was applied is nothing less than nessus, a free tool to be able to perform a vulnerability scanner and in this way take precautions necessary to protect the data that is of vital importance in an organization.

Keywords – *Computer security; nessus; nessusd; nmap; vulnerability; Internet;*

I. INTRODUCCIÓN

Con la aparición del Internet considerado como la autopista de la información, se publica cada vez más miles de datos relacionados a una empresa o institución ya sea estatal o privada. Que para el acceso a la información lo realizamos mediante un navegador web, sin embargo toda página o aplicación web viene hospedada en un servidor lo cual atiende las peticiones del cliente.

Esto hace que muchos usuarios visiten cotidianamente sitios web, lamentablemente se tiene un desconocimiento sobre la procedencia de los usuarios (como ser nombre, la máquina de la cual accede, etc.) que interaccionan con las aplicaciones web publicada en la autopista de la información, muchas veces esta información es interceptada por personas o usuarios

malintencionados con el fin de apoderarse de los datos capturados. Es decir el sistema informático es atacando por un intruso burlando la seguridad.

En el proceso de comunicación cliente servidor se manejan los protocolos de comunicación lo cual no es más que partes o acuerdos para poder intercambiar información en la red, esto hace que se utilicen muchos protocolos las mismas carecen de seguridad . Sea cual sea el ataque, por lo general cada una de estas intrusiones implica muchas veces en importantes pérdidas económicas para las empresas, además de la imagen negativa y poco confiable que esta daría ante los usuarios.

En la actualidad los incidentes relacionados con la seguridad en los sistemas de información de las empresas aumentan de manera periódica, comprometiendo uno de los recursos más valiosos que es la INFORMACIÓN.

Se puede decir que la información es uno de los pilares más trascendentales a la hora de toma de decisiones en una entidad. De allí el valor que tiene para estos entes la protección y prevención de los sistemas de información.

De ahí que nace la urgente necesidad de proteger resguardar la integridad de la información dentro las instituciones públicas y/o privadas. Afortunadamente existen herramientas que facilitan la tarea de encontrar vulnerabilidades en nuestros sistemas.

Y es por esta razón que en el presente documento se realiza un análisis respecto a una de las muchas herramientas para el escaneo de vulnerabilidades llamado NESSUS que permita conocer las amenazas frente a los intrusos que quieran apoderarse de la información útil

Nessus llega ser un programa de escaneo de vulnerabilidades en diversos sistemas operativos. Es una potente aplicación de detección de vulnerabilidades muy usada tanto por los hackers, como por los expertos en seguridad informática cuando tienen que realizar auditorías.

Es así que en el presente artículo vamos abordar sobre esta herramienta tan imprescindible para la seguridad informática, hemos de ver la forma de instalación y configuraciones, entre otros aspectos que atingen a la seguridad dentro una organización o empresa con o sin fines de lucro.

II. DESARROLLO

Seguridad Informática:

La seguridad informática es una forma de proteger los recursos computacionales que implica hardware y software y todos los componentes relacionados a esta. La seguridad informática debe establecer normas políticas en la cual minimicen aquellos riesgos a la información o infraestructura informática. En cuanto estas normas podemos mencionar como: aquellos horarios de funcionamiento, restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo lo necesario que permita un buen nivel de seguridad informática. (Herrera Joancomartí, y otros, 2004)

A continuación se describe de manera breve:

- **Infraestructura computacional**: Velar que los equipos funcionen adecuadamente y anticiparse en caso de fallas, robos, incendios, boicot, desastres naturales, fallas en el suministro eléctrico y cualquier otro factor que atente contra la infraestructura informática.
- **Los usuarios**: Debe protegerse el sistema en general para que el uso por parte de ellos no pueda poner en entredicho la seguridad de la información y tampoco que la información que manejan o almacenan sea vulnerable.
- **La información**: Ésta es el principal activo. Utiliza y reside en la infraestructura computacional y es utilizada por los usuarios.

Vulnerabilidad:

Son errores que permiten realizar desde afuera actos sin permiso del administrador del equipo, incluso se puede suplantar al usuario, actualmente, ya hay muchas amenazas que tratan de acceder remotamente a los

ordenadores, ya sea para hacerlos servidores ilegales de Spam o para robar información.

Vulnerabilidades de un sistema informático

Los sistemas de informáticos tienen un recurso muy importante y lo cual amerita proteger dicho recurso, hablamos de los datos (información) los cuales cuentas con los siguientes componentes:

- **Hardware**: elementos físicos del sistema informático, tales como procesadores, electrónica y cableado de red, medios de almacenamiento (cabinas, discos, cintas, DVDs,...).
- **Software**: elementos lógicos o programas que se ejecutan sobre el hardware, tanto si es el propio sistema operativo como las aplicaciones.
- **Datos**: comprenden la información lógica que procesa el software haciendo uso del hardware. En general serán informaciones estructuradas en bases de datos o paquetes de información que viajan por la red.
- **Otros**: fungibles, personas, infraestructuras,.. aquellos que se 'usan y gastan' como puede ser la tinta y papel en las impresoras, los soportes tipo DVD o incluso cintas si las copias se hacen en ese medio, etc.

De ellos los más críticos son los datos, el hardware y el software. Es decir, los datos que están almacenados en el hardware y que son procesados por las aplicaciones software.

Vulnerabilidades conocidas:

- Vulnerabilidad de desbordamiento de buffer: Si un programa no controla la cantidad de datos que se copian en buffer, puede llegar un momento en que se sobrepase la capacidad del buffer y los bytes que sobran se almacenan en zonas de memoria adyacentes.

  En esta situación se puede aprovechar para ejecutar código que nos de privilegios de administrador.

- Vulnerabilidad de condición de carrera (race condition): Si varios procesos acceden al mismo tiempo a un recurso compartido puede producirse este tipo de vulnerabilidad. Es el caso típico de una variable, que cambia su estado y puede obtener de esta forma un valor no esperado.

- Vulnerabilidad de Cross Site Scripting (XSS): Es una vulnerabilidad de las aplicaciones web, que permite inyectar código VBSript o JavaScript en páginas web vistas por el usuario. El phishing es una aplicación de esta vulnerabilidad. En el phishing la víctima cree que está accediendo a una URL (la ve en la barra de direcciones), pero en realidad está accediendo a otro sitio diferente. Si el usuario introduce sus credenciales en este sitio se las está enviando al atacante.

- Vulnerabilidad de denegación del servicio: La denegación de servicio hace que un servicio o recurso no esté disponible para los usuarios. Suele provocar la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos informáticos del sistema de la víctima.

- Vulnerabilidad de ventanas engañosas (Window Spoofing): Las ventanas engañosas son las que dicen que eres el ganador de tal o cual cosa, lo cual es mentira y lo único que quieren es que el usuario de información. Hay otro tipo de ventanas que si las sigues obtienen datos del ordenador para luego realizar un ataque. (Mënalkiawn, 2013)

Herramientas para escáner de vulnerabilidades:

En la actualidad existen varias herramientas para realizar el escaneo de vulnerabilidades en los diferentes sistemas operativos. Las más conocidas son como sigue:

Metasploit Framework, DVL – DVWA, NMAP, existe una distribución muy avanzada Kali Linux, OpenVAS, nessus y entre otras herramientas.

En el presente ariculo vamos hablar y describir los pasos a realizar con la herramienta en el ámbito Linux con NESSUS.

Nessus:

Nessus llega ser una aplicación o un programa de escaneo de vulnerabilidades en diversos sistemas operativos. Consiste en un daemon (proceso informático no interactivo, es decir, que se ejecuta en segundo plano en vez de ser controlado directamente por el usuario), aquel proceso que realiza el escaneo en el sistema objetivo, cuenta con un lado cliente (basado en consola o gráfico) que muestra el avance e informa sobre el estado de los escaneos. Desde consola nessus puede ser programado para hacer escaneos programados con cron. (Tenable, 2016)

Sin embargo es necesario aclarar y hacer comparación frente a otras herramientas tal es el caso de OpenVAS, es una mejora de Nessus de código abierto, mientras que Nessus a partir de la versión 3 es una herramienta de código cerrado que ofrece una versión gratuita para uso personal, es así que en esta oportunidad se hará uso de la versión personal o Home.

III. RESULTADOS

En este apartado vamos a realizar la instalación y configuración de Nessus, para lo cual necesitamos tener instalado una distribución GNU/Linux en este caso vamos a utilizar Ubuntu 15.10, una HP 15 core i5 cuarta generación.

Lo primero es descargar la última versión nessus desde la página oficial de la misma: www.tenable.com

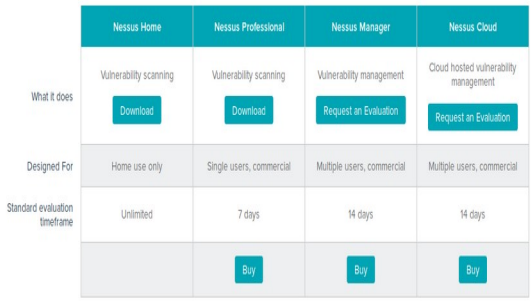

Figura 1: Página oficial de descarga nessus.
Fuente: Elaboración propia.

Como se puede apreciar en la figura anterior hay cuatro tipos de versiones, tres de ellos son de pago, en esta oportunidad vamos a descargar la versión Home que llega ser gratuito.

Lo que se hizo fue descargar la última versión para ubuntu la cual llega a ser Nessus-6.7.0-ubuntu1110_amd64.deb, este archivo descargado se puede instalar utilizando el gestor de paquetes desde la terminal de ubuntu. A continuación se describen los pasos para su instalación:

Instalación de nessus desde la terminal de linux.
santos@HP-15:~$ sudo dpkg -i Nessus-6.7.0-ubuntu1110_i386.deb

Una vez terminado la instalación ejecutamos el demonio nessusd que está ubicado en el directorio donde radican los daemon de Linux en este caso en /etc/init.d/, en caso contrario si en caso salga algún error de instalación como algunas dependencias ejecutar la instrucción siguiente desde la consola para subsanar dichos errores o dependencias.
santos@HP-15:~$sudo aptitude -f install

Ejecutar el daemon nessusd desde el directorio init.d
santos@HP-15:~$sudo /etc/init.d/nessusd start

Posterior a la ejecución del procreso anterior nos dirigimos al navegador web y colocamos en la URL la siguiente dirección https://localhost:8834/

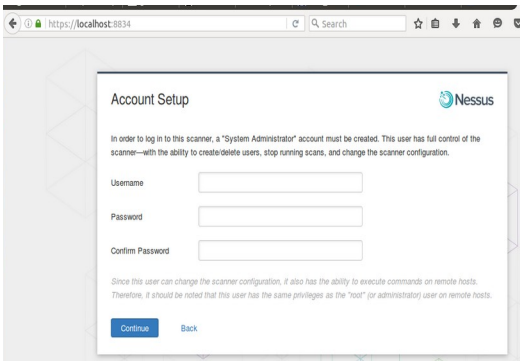

Figura 2: Pantalla de registro de usuario en nessus.
Fuente: Elaboración propia

Una vez registrado los datos que nos solicitan seguidamente nos solicita el código de activación para nessus, en este caso nos dirigimos a la página de http://www.tenable.com/products/nessus/nessus-plugins/obtain-an-activation-code, donde con solo un registro gratuito nos enviara al correo electrónico mencionado código de activación. Una vez activada se procederá con una actualización del Plug-in de manera automática.

Suele fallar la actualización del plugin, en caso de salir un error de actualización ejecutar desde consola la siguiente instrucción.
santos@HP-15:~$sudo ./nessuscli update
Una vez terminada la actualización del Plug-in detener el daemon nessusd con la siguiente instrucción desde la terminal linux.
santos@HP-15:~$sudo /etc/init.d/nessusd stop

Posterior a esta volver a levantar el demonio con la orden;
santos@HP-15:~$sudo /etc/init.d/nessusd start

Tras el levantamiento dbe,os entrar nuevante a la direccion https://localhost:8834/

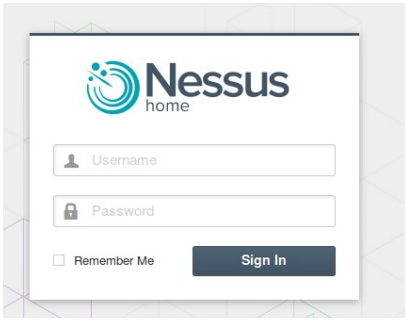

Figura 3: Ingreso a nessus con la cuenta creada en el anterior punto.
Fuente: Elaboración propia.

Tras la autentificación ingresamos al panel de control de nessus

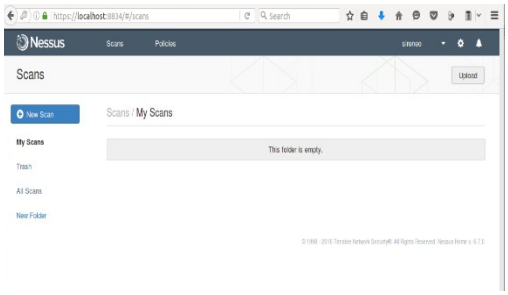

Figura 4: Panel de control nessus
Fuente: Elaboración propia.

El siguiente paso es realizar un primer escaner básico a la red.

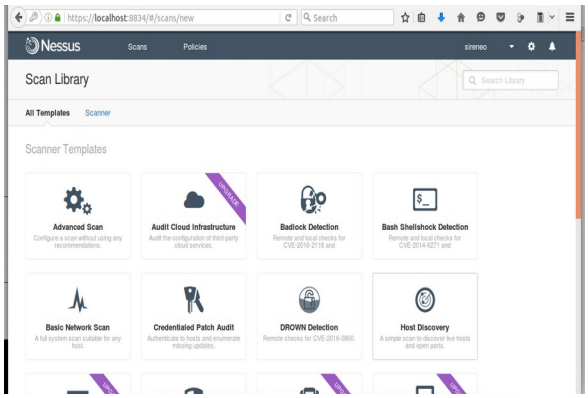

Figura 5: Escaner básico de la red.

Fuente: Elaboración propia.

A continuación un ecaneo de vulnerabilidades a un router con una ip 192.168.1.1

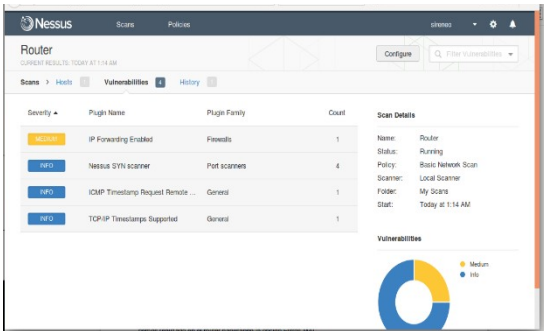

Figura 6: Escaner de vulnerabilidades con nessus
Fuente: Elaboración propia.

Si pulsamos sobre las vulnerabilidades saldrán de una en una, con su nivel de seguridad y un título explicativo.

Nessus es una sencilla herramienta que nos permite escanear vulnerabilidades dentro nuestro sistema integrado, de esta manera escanea los puertos, DHCP, SSL, etc. a partir de aquí podemos tomar decisiones en cuanto al aseguramiento de nuestros datos que son de vital importancia.

IV. CONCLUSIÓN

La seguridad informática es muy importante ya que depende de esta la difusión confiable y oportuna de los datos.

En la actualidad fluye mucha información en el Internet, estas tienden a ser capturados por los famosos llamados hacker.

Sin embargo tanto es el avance científico tecnológico que nos proporciona herramientas que permite escanear vulnerabilidades dentro una máquina, precisamente para el resguardo de la información dentro una organización.

Hemos hecho una introducción a esta herramienta software libre nessus es un poderoso y sencillo software para el escaneo de vulnerabilidades, en los resultados hemos visto que se pudo evidenciar las vulnerabilidades del router a la cual hemos escaneado.

Por su puesto a manera de concluir no es la única herramienta existen muchas herramientas que pertenecen a la categoría de software libre, además mencionar que existen distribuciones Linux específicamente para seguridad informática, los cuales son: Wifislax, Kali Linux, etc.

V. BIBLIOGRAFÍA

Benchimol, Daniel . 2011. *Hacking desde Cero.* Buenos Aires : s.n., 2011.

Chica, José Luis y Vila, Jose. 2012. *GUÍA AVANZADA DE NMAP.* 2012.

Debish. 2012. *Debian Hackers Elementals.* 2012.

Herrera Joancomartí, Jordi , García Alfaro, Joaquín y Perramón Tornil, Xavier . 2004. *Aspectos avanzados de seguridad en redes.* Barcelona : s.n., 2004.

Mënalkiawn. 2013. *MANUAL BÁSICO DE SEGURIDAD INFORMÁTICA PARA ACTIVISTAS.* Barcelona : Klinamen), 2013.

Tenable. 2016. *Nessus 6.4 Installation and Configuration Guide.* 2016.

wikipedia. *Wikipedia. [En línea] [Citado el: 30 de mayo de 2016.]* https://es.wikipedia.org/wiki/Nessus.