*Revista Nexos Científicos* *ISSN: 2773-7489*
*Enero –Junio 2019 pp. 35-41* *Correo: editor@istvidanueva.edu.ec*
*Volumen 3, Número 1* *URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index*
*Fecha de recepción: abril 2019* *Fecha de aceptación: mayo 2019*

# Metodología abierta de testeo en Seguridad NESSUS

**Chicaiza Verónica**[1]

[1] *Universidad Tecnológica Israel-Departamento de Ciencias de la Ingeniería –Carrera de Sistemas, Quito, Ecuador, vnchm25@hotmail.com*

**Resumen:** La metodología Abierta de Testeo de Seguridad (OSSTMM) el cual nos permitirá destacar las áreas donde se puedan concentrar la mayoría de los ataques a la red y así pueden crear las bases correctivas y las acciones preventivas para evitar esos ataques, por otro lado hemos rescatado una herramienta de seguridad informática "NESSUS", esta selección se ha realizado debido a que es un analizador de seguridad de redes potente y fácil de usar, con una amplia base de datos que nos permite hacer pruebas y determinar si nuestra red o equipo tiene fallos de seguridad, el cual no solo nos informara que vulnerabilidades de seguridad existen y el nivel de riesgo (alto, medio, bajo) de cada una de ellas, sino que también nos notificara sobre como mitigarlas ofreciendo soluciones.

**Palabras clave:** Seguridad Informática, Ataques a Redes de Datos

## *Open NESSUS Security Testing Methodology*

**Abstract:** The Open Security Testing Methodology (OSSTMM) which will allow us to highlight the areas where most attacks on the network can be concentrated and thus can create the corrective bases and preventive actions to prevent such attacks, on the other hand we have rescued a computer security tool "NESSUS", this selection has been made because it is a powerful and easy to use network security analyzer, with a comprehensive database that allows us to test and determine if our network or equipment has security flaws, which will not only inform us what security vulnerabilities exist and the level of risk (high, medium, low) of each of them, but will also notify us about how to mitigate them by offering solutions.

**Keywords**: Computer Security, Attacks on Data Networks

## 1. INTRODUCCIÓN

Por vulnerabilidad entendemos la exposición latente a un riesgo. En el área de informática, existen varios riesgos tales como: ataques malintencionados (virus, gusanos, troyano) y hackers; no obstante, con la adopción de Internet como instrumento de comunicación y colaboración, los riesgos han evolucionado y, ahora, las organizaciones deben enfrentar ataques de negación de servicio y amenazas combinadas; es decir, la integración de herramientas automáticas de "hackeo", accesos no autorizados a los sistemas y capacidad de identificar y explotar las vulnerabilidades de los sistemas operativos o aplicaciones para dañar los recursos informáticos. Los riesgos de ataques a la información surgen a partir de las debilidades de las redes de Datos y de los sistemas, estos ataques ya sea internos o externos pueden dejar inoperables ciertos servicios y recursos de hardware y software generando pérdidas económicas y exponiendo nuestra información.

Los análisis de vulnerabilidades inicialmente son capaces de descubrir y definir una guía para el aseguramiento de los datos; el escaneo periódico provee información actualizada acerca de la administración de las vulnerabilidades.

1. Estudiante de Sistemas de Información, vnchm25@hotmail.com

*Revista Nexos Científicos* *ISSN: 2773-7489*
*Enero –Junio 2019 pp. 35-41* *Correo: editor@istvidanueva.edu.ec*
*Volumen 3, Número 1* *URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index*
*Fecha de recepción: abril 2019* *Fecha de aceptación: mayo 2019*

```
$ wget -c --limit-rate=100k
http://mirror.jmu.edu/pub/linuxmint/ima
ges//stable/14/linuxmint-14.1-mate-dvd-
64bit.iso
```

Nessus es un programa de escaneo de vulnerabilidades en diversos sistemas operativos. Consiste en un demonio o diablo, nessusd, que realiza el escaneo en el sistema objetivo, y nessus, el 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. Thacker, B. H., Riha, D. S., Fitch, S. H., Huyse, L. J., & Pleming, J. B. (2006).

En operación normal, nessus comienza escaneando los puertos con nmap o con su propio escaneador de puertos para buscar puertos abiertos y después intentar varios exploits para atacarlo. Las pruebas de vulnerabilidad, disponibles como una larga lista de plugins, son escritos en NASL (Nessus Attack Scripting Language, Lenguaje de Scripting de Ataque Nessus por sus siglas en inglés), un lenguaje scripting optimizado para interacciones personalizadas en redes.

Opcionalmente, los resultados del escaneo pueden ser exportados como informes en varios formatos, como texto plano, XML, HTML, y LaTeX. Los resultados también pueden ser guardados en una base de conocimiento para referencia en futuros escaneos de vulnerabilidades. Anderson, H. (2003).

Nessus es un escáner de seguridad que se arrastra a través de una red, buscando
para vulnerabilidades bien conocidas y configuraciones incorrectas comunes.

Tiene un conjunto único de características, incluido el descubrimiento automático de SSL,
reconocimiento de servicios (por lo que capturará, por ejemplo, un servidor FTP
ejecutándose en un puerto diferente de 21) y su propio lenguaje de script.

El Nessus Security Scanner se lanza bajo el público en general de GNU
Licencia y pretende ser fácil de usar y extremadamente potente.

Estas incluyen organizaciones que usan
Nessus y compre el feed directo para cada escáner y organizaciones que compran
Centro de seguridad de Tenable (anteriormente Lightning Console).
Tenable también proporciona soporte comercial por correo electrónico a clientes de feeds de complementos directos que están
utilizando Nessus 3. La alimentación directa también incluye un conjunto de comprobaciones de cumplimiento basadas en host para
UNIX y Windows, que es muy útil al realizar auditorías SOX o FISMA. Rogers, R. (Ed.). (2011)

## 2. METODOLOGÍA

Las metodologías más usadas en el Ethical Hacking son las siguientes:

- OSSTMM (FUENTE ABIERTA DE SEGURIDAD MANUAL DE MÉTODOS DE PRUEBA)
- ISSAF (MARCO DE EVALUACIÓN EN SISTEMAS DE INFORMACIÓN DE SEGURIDAD)
- OWASP (SOLICITUD DEL PROYECTO DE SEGURIDAD OPEN WEB)
- CEH (ETHICAL HACKING CERTIFICADO)
- OFFENSIVE SECURITY

Es muy delgada la línea entre un hacker de sombrero blanco y un hacker de sombrero negro, a nivel de conocimientos ambos tienen la capacidad de reconocer vulnerabilidades y/o fallos en el área informática, para sacar provecho de la situación, el hacker ético tiene como misión explotar estas vulnerabilidades y reportar las mismas, el fin nunca es el sacar provecho económico de la situación, por lo contrario el objetivo es hacer recomendaciones y/o diseñar controles para la mejora del sistema.

## 3. RESULTADOS Y DISCUSIÓN

### CICLO DE VIDA DE LA INFORMACIÓN


### 3.1 Vulnerabilidad

Define la Vulnerabilidad como debilidad de cualquier tipo que compromete la seguridad del

sistema informático. Las vulnerabilidades de los sistemas informáticos las podemos agrupar.

### 3.2 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.

### 3.3 Vulnerabilidad de condición de carrera

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

### 3.4 Vulnerabilidad de Cross Site Scripting

Es una vulnerabilidad de las aplicaciones web, que permite inyectar código VBScript 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.

### 3.5 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.

### 3.6 Vulnerabilidad de ventanas engañosas

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.

## 4. Herramientas

En el caso de servidores Linux/Unix para hacer el análisis de vulnerabilidades se suele utilizar el programa 'Nessus'. Nessus es de arquitectura cliente-servidor OpenSource, dispone de una base de datos de patrones de ataques para lanzar contra una máquina o conjunto de máquinas con el objetivo de localizar sus vulnerabilidades. Existe software comercial que utiliza Nessus como motor para el análisis. Por ejemplo está Catbird (www.catbird.com) que usa un portal para la gestión centralizada de las vulnerabilidades, analiza externamente e internamente la red teniendo en cuenta los accesos inalámbricos. Además hace monitoreo de servicios de red como el DNS y la disponibilidad de los portales web de las organizaciones.

## 5. Concepto de amenaza

Entendemos la amenaza como el escenario en el que una acción o suceso, ya sea o no deliberado, compromete la seguridad de un elemento del sistema informático.

Integrando estos conceptos podemos decir que “un evento producido en el sistema informático que constituye una amenaza, asociada a una vulnerabilidad del sistema.

## 6. Firewall Lógico

En la actualidad el software firewall Shorewall, es una herramienta de alto nivel para la configuración de Netfilter y permite la configuración de un firewall de host, de un servidor, un firewall enrutador, y lograr manejar complejas configuraciones. Esta herramienta cuenta con soporte para IPV4 e IPV6.

## 7. Seguridad Informática

La seguridad informática se enfoca en la protección y la privatización de sus sistemas y en esta se pueden encontrar dos tipos: La seguridad lógica que se

*Revista Nexos Científicos*
*Enero –Junio 2019 pp. 35-41*
*Volumen 3, Número 1*
*Fecha de recepción: abril 2019*
*ISSN: 2773-7489*
*Correo: editor@istvidanueva.edu.ec*
*URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index*
*Fecha de aceptación: mayo 2019*

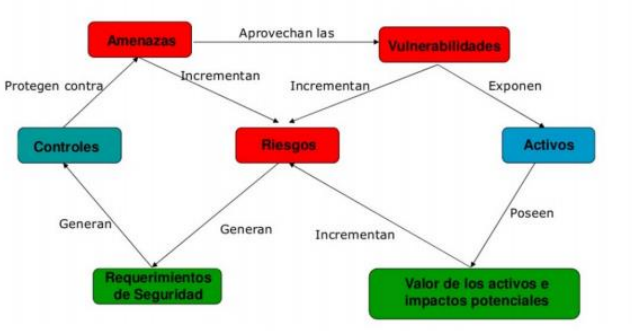
enfoca en la protección de los contenidos y su información y la seguridad física aplicada a los equipos como tal, ya que el ataque no es estrictamente al software y también al hardware y también la infraestructura informática es una parte fundamental para la preservación del activo más valioso que es la información, así mismo se busca mantener la confidencialidad, integridad, autenticidad, y disponibilidad que son los datos recordando símbolos que representan hechos, situaciones, condiciones o información es el resultado de procesar o transformar los datos la información es significativa para el usuario.

## 8. Características

En el análisis de riesgo es importante reconocer que cada proceso de riesgo tiene características, tales como:

Activos: Elementos que forman parte de los sistemas informáticos y redes de comunicación:

- Amenazas: Todo tipo de circunstancias que puede suceder a los sistemas y redes de comunicación.
- Las amenazas pueden ser de carácter físico como por ejemplo un incendio o lógico como por ejemplo acceso no autorizado a una base de datos.
- Probabilidad: Establecer la probabilidad de ocurrencia que puede realizarse de manera cuantitativa o cualitativa, pero siempre considerando que la medida no debe contemplar la existencia de ninguna acción paliativa, o sea, debe considerarse en cada caso qué posibilidades existen que la amenaza se presente independientemente del hecho que sea o no contrarrestada.
- Vulnerabilidades: Agujeros de seguridad, debilidad de los activos que son aprovechadas por las amenazas para dañar un activo.
- Impacto: Consecuencia de la materialización de una amenaza sobre un activo.
- Controles: Mecanismos que permiten reducir las vulnerabilidades de equipos y sistemas informático.

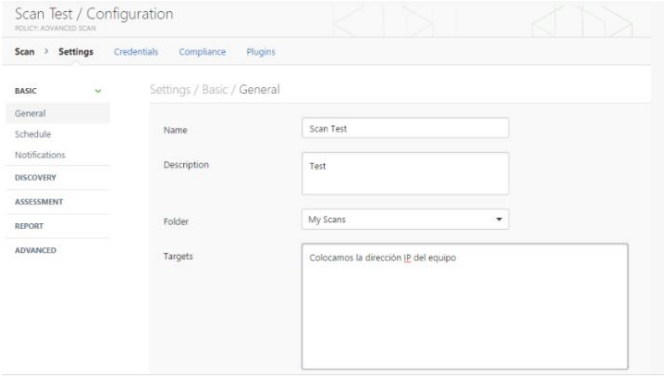



Elementos del Análisis de Riesgo Informático

## 9. Verificación del análisis

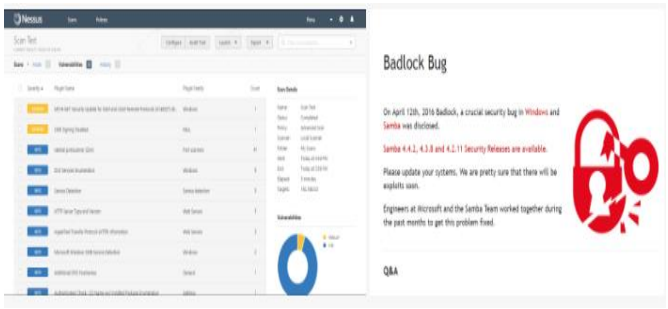
asignamos un usuario y clave para ingresar por el cliente web.


Configuramos un nuevo **SCANEO**



*Revista Nexos Científicos* *ISSN: 2773-7489*
*Enero –Junio 2019 pp. 35-41* *Correo: editor@istvidanueva.edu.ec*
*Volumen 3, Número 1* *URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index*
*Fecha de recepción: abril 2019* *Fecha de aceptación: mayo 2019*

Una vez ejecutada la tarea, nos arrojara un informe similar al siguiente.




Puede utilizar secuencias de comandos o cualquier solución de gestión de parches, como SCCM. A continuación, se incluyen los comandos de Nessus Agents que pueden utilizarse en secuencias para automatizar la implementación/agrupación de agentes.

```
Redhat
Linux: /opt/nessus_agent/sbin/nessuscli
agent link --key=apikey --groups="Red
Hat linux" --host=hostname --port=8834
```

```
Amazon
Linux: /opt/nessus_agent/sbin/nessuscli
agent link --key=apikey --
groups="Amazon linux" --host=hostname -
-port=8834
```

```
Windows Member Server: msiexec /i
NessusAgent-<version number>-x64.msi
NESSUS_GROUPS="Windows, Windows Member
Servers" NESSUS_SERVER="hostname:8834"
NESSUS_KEY=apikey /qn
```

## 10. EL ESCÁNER DE VULNERABILIDADES

Nessus es el estándar mundial para la prevención de ataques de red, identificación de vulnerabilidades y detección de problemas de configuración que utilizan los hackers para entrar en la red. Nessus se ha utilizado por más de 1 millón los usuarios en todo el mundo, por lo que es el líder mundial de evaluación de la vulnerabilidad, configuración de seguridad y cumplimiento de las normas de seguridad.

## 11. VERIFICACIONES DE CUMPLIMIENTO

Las verificaciones de cumplimiento se redactan con base en las guías de mejores prácticas de la comunidad y las políticas de seguridad, como CIS Benchmarks. Para los sistemas Windows, las auditorías de cumplimiento pueden verificar la complejidad de las contraseñas, la configuración del sistema, los valores del registro y la mayoría de las configuraciones que puedan describirse en un archivo de política de Windows. En el caso de los sistemas Unix, las auditorías de cumplimiento comprueban los procesos en ejecución, la política de seguridad del usuario, la configuración a nivel del sistema y los valores dentro de los archivos de configuración de aplicaciones.

## 12. APLICACIONES DE ALTO RIESGO.

Las organizaciones industriales y gubernamentales son las que poseen más usuarios de aplicaciones de alto riesgo. “Hay casos donde el uso de algunas de estas aplicaciones tiene un uso legítimo, por ejemplo, el uso de herramientas de administración remota para mesa de ayuda”. Por todo lo expuesto, el uso de este tipo de aplicaciones debe ser monitoreado constantemente.

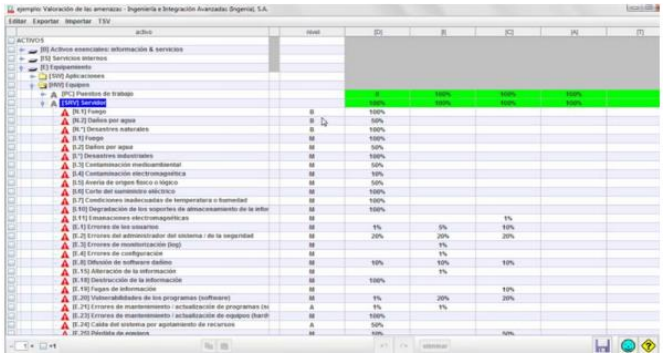
## 13. BÚSQUEDA Y VERIFICACIÓN DE VULNERABILIDADES

El objetivo de esto es en sí poder identificar, verificar y comprender las debilidades, los fallos que se encuentran en la configuración y sobre todo la vulnerabilidad que se encuentra en una red ya sea local o externa del servidor o en el mismo. La búsqueda de vulnerabilidades utilizando herramientas automáticas, como Zenmap en Windows, o Nmap en Kali Linux, es una manera eficaz de poder determinar inseguridades, sabe que estos escáneres actúan tanto en el mercado laboral como en el mundo Hacker, es importante que la persona encargada de realizar el hackeo, identificar y poner en las pruebas los scripts y exploits que se

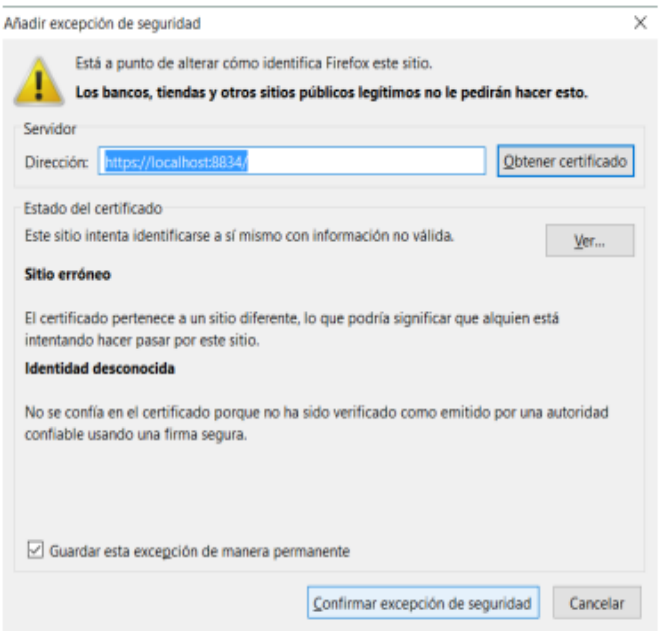
*Revista Nexos Científicos*
*Enero –Junio 2019 pp. 35-41*
*Volumen 3, Número 1*
*Fecha de recepción: abril 2019*
*ISSN: 2773-7489*
*Correo: editor@istvidanueva.edu.ec*
*URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index*
*Fecha de aceptación: mayo 2019*

utilizan para hackear. Como ya se ha insistido en pasos anteriores, es importante siempre verificar los falsos positivos y aumentar el conocimiento sobre hackeo, descubrir vulnerabilidades depende mucho de la experiencia y la creatividad de la persona que va a realizar el Hackeo.

Es importante integrar en las pruebas los programas de escaneo que se hayan usado, las herramientas, usar al menos dos tipos diferentes de escáneres para obtener más información o verificar la ya obtenida. Pode encontrar todas las vulnerabilidades o fallos con similitudes en las aplicaciones, sistemas operativos o sistemas los cuales son similares y pueda de una manera perjudicar al sistema objetivo en general.



Nessus y confirmar la excepción de seguridad




## 14. IMPLEMENTACIÓN DEL ESCENARIO VIRTUAL.

Para la comunicación entre los equipos virtuales fue necesario configurar los adaptadores de red respectivos tomando en consideración que cada tarjeta de red tiene las siguientes opciones de configuración: Modo Bridge en donde se le asigna a la tarjeta de red de la máquina virtual una dirección ip real visible desde la red. Modo Nat en donde la maquina real actuará como un router NAT convirtiendo las direcciones internas en direcciones compatibles con el resto de red real.

## 15. TESTEO DE CONTROL DE ACCESO

El Firewall es el que controla el flujo de tráfico de red, en la propia empresa, DMZ y también en la Internet. Su funcionalidad es la de seguridad y usa ACL´s (Listas de Control de Acceso). Lo que se hace es asegurar que el Firewall permita el ingreso solo a aquello que puede ser aceptado dentro de la red, lo demás debe ser negado. La mejor forma de verificar todo esto, es viendo si el Firewall está correctamente ocupándose del filtrado del tráfico de la red local hacia afuera, también esta debe mostrar si está detectando las direcciones de orígenes falsos. Es importante probar las capacidades externas del Firewall desde el interior de la Red

## 16. TESTEO DE MEDIDAS DE CONTINGENCIA

Se trata acerca de lo que es fácilmente atravesable y como saber manejarlo, se refiere a programas maliciosos y a emergencias, medir en lo posible los recursos mínimos necesarios como el Firewall que utiliza la empresa y antivirus que se encuentren instalados en los ordenadores.

## 4. CONCLUSIONES

– Se puede ver que es diferente a cualquier otra amenaza a la seguridad de una corporación. De esta manera se evitan las tecnologías puestas en su lugar para proteger y detectar la actividad maliciosa. Es una amenaza que siempre existirá, y que no puede ser contenida por software,

antivirus, parches completos, firewalls y sistemas de detección de intrusiones. Sólo se necesita de una persona no consciente para hacer un ataque de ingeniería social con éxito. Con la formación adecuada y las políticas establecidas, el riesgo de la ingeniería social puede ser mitigado eficazmente.

- La seguridad informática cumple un rol importante, que consiste en la 118 protección de datos, en los tiempos actuales en donde toda información se traslada a través de Internet, por lo que es primordial proteger el flujo de datos, con esto se da a entender el lugar tan importante que ocupa la seguridad informática.

- El momento en que se evalúa y configura las herramientas, se las hace en base al estudio previo que se hizo a la infraestructura de TI de la empresa y al mapa de Red que esta tiene rastro de un inconveniente al momento de realizar la configuración.

- Prestar mucha atención y cuidado al momento de modificar los parámetros en los archivos de configuración ya que los mismos son del tipo texto que no permite una validación previa de su contenido.

## REFERENCIAS

Thacker, B. H., Riha, D. S., Fitch, S. H., Huyse, L. J., & Pleming, J. B. (2006). Probabilistic engineering analysis using the NESSUS software. Structural Safety, 28(1-2), 83-107.

Rogers, R. (Ed.). (2011). Nessus network auditing. Elsevier.

Anderson, H. (2003). Introduction to nessus. SecurityFocus. Saatavilla wwwosoitteessa< http://www. securityfocus. com/infocus/1741.