ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría en Seguridad Informática Aplicada

"ANÁLISIS DE LAS VULNERABILIDADES DEL SITIO WEB DE LA UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO"

EXAMEN DE GRADO (COMPLEXIVO)

PREVIO A LA OBTENCIÓN DEL GRADO DE:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

JUAN CARLOS ENRIQUE ORTEGA ACOSTA

GUAYAQUIL – ECUADOR

AÑO: 2016

AGRADECIMIENTO

Agradezco a Dios por haberme dado la vida y por la oportunidad de haberme dado un padre, hoy convertido en ángel y una madre que siempre me han brindado el apoyo necesario en todas las etapas de mi vida y me han motivado a seguir adelante en cada tropiezo que se me ha presentado a lo largo de mi carrera.

DEDICATORIA

A mi padre convertido en ángel Juan Santiago, y mi madre Luz María por ser mis principales pilares de apoyo y comprensión en este camino. A mi hermanita Lorenita. A mi esposa Ninfa, por haberme dado su apoyo para alcanzar esta meta, A mi hija Carlita y mi hijo Juan Santiago por haberme complementado en esta vida.

TRIBUNAL DE SUSTENTACIÓN

_____

Ing. Lenin Freire MSG.

DIRECTOR DEL MSIA

_____

Ing. Juan Carlos García MSG.

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA

_____

Ing. Lenin Freire MSG

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA

RESUMEN

En la actualidad la seguridad informática es un pilar fundamental en todas organizaciones, debido al crecimiento de Internet ha generado el aumento de flujo de datos con información muy importante para las organizaciones.

Esto motiva que las organizaciones cada vez contraten más personal capacitado en seguridad informática para mitigar las posibles vulnerabilidades en su infraestructura.

El presente trabajo propone realizar un análisis de las vulnerabilidades del sitio web de la Universidad Técnica Estatal de Quevedo ***académico.uteq.edu.ec***, ya que en el pasado este sitio fue blanco de varios ataques.

Luego de realizar el análisis se propondrá una solución viable para estos focos de inseguridad en la infraestructura del sitio web.

Estos análisis aportaran en mejorar la seguridad de la institución, para que en el futuro la institución esté preparada para posibles ataques informáticos.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍAS

UTEQ	UNIVERSIDAD TECNICA ESTATAL DE QUEVEDO
CBC	CIPHER BLOCK CHAINING MODE
CTR	COUNTER MODE
DOS	Denegación de servicio
http	Protocolo de navegación internet
Host	Equipos de usuarios finales
PC	Computadora personal

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

En este documento se explica el análisis de las vulnerabilidades del sitio web de la Universidad Técnica Estatal de Quevedo.

Luego que se el análisis de las vulnerabilidades se propones las posibles soluciones que se debe de implementar para corregir estos focos de inseguridad.

Finalmente se describe los resultados que la institución adquiere al momento implementar las medidas de seguridad planteadas como solución para que la institución esté presto al momento que se le presentes estas situaciones de inseguridad.

CAPÍTULO 1

GENERALIDADES

La Universidad Técnica Estatal de Quevedo como toda institución de prestigio del ecuador, está al tanto con las soluciones informáticas para administrar mejor sus recursos educativos.

Entonces cuenta con una infraestructura de servidores web para agilitar estos procesos educativos, en el pasado fue producto de un ataque informático, por eso se pensó en realizar este proyecto en uno de los servidores.

Esperando que esto proyecto sea de gran ayuda para mitigar posibles ataque en el futuro.

1.1. DESCRIPCIÓN DEL PROBLEMA

La universidad Técnica Estatal de Quevedo cuenta con su propio sistema informático que son, un sitio de matrículas y notas llamado sicau.uteq.edu.ec, y otro que es para gestionar las tareas en línea de los estudiantes **académico.uteq.edu.ec**, y cuenta con un sitio web informativo llamado www.uteq.edu.ec. El cual ya ha sido atacado varias veces mandando abajo este sitio informativo.

Debido a que nunca se ha hecho un análisis de las posibles vulnerabilidades del sitio web, se plantea en este proyecto realizarlo para minimizar los riesgos de un ataque al sitio **académico.uteq.edu.ec.**

1.2. SOLUCIÓN PROPUESTA

Debido a que los sitios web están expuestos a los ataques informáticos y en la actualidad no se han tomado medidas de corrección a los ataques que hubo en el pasado a este sitio web de la Universidad.

Por medio de una herramienta de análisis de vulnerabilidades se realizara un escaneo al sitio web de la universidad para escoger los

puntos más críticos, analizarlos, y darle solución a estos focos de inseguridad.

Proponiendo una solución viable y efectiva para corregir estos focos de inseguridad del sitio.

CAPÍTULO 2

METODOLOGÍA DE DESARROLLO DEL ESCENARIO

2.1 ALCANCE

El presente trabajo describe el análisis de las vulnerabilidades del sitio web de la Universidad Técnica Estatal de Quevedo, luego de esto se plantea las soluciones a estos focos de inseguridad.

2.2. ORGANIZACIÓN

La Universidad Técnica Estatal de Quevedo (UTEQ), localizada en la ciudad de Quevedo, Provincia de Los Ríos.

Iniciando sus actividades académicas el 22 de enero 1976. Poco a poco la institución se ha actualizado tecnológicamente para estar a la par con las mejores universidades del país, por ese motivo la Universidad Técnica Estatal de Quevedo creo su departamento informático con su cuarto de servidores para almacenar y administrar todos los recursos académicos por medio de la tecnología.

2.3. DESCRIPCIÓN DEL ESCENARIO

Para la ejecución del escenario se hizo un análisis externo de caja gris, que se la realizo desde la red doméstica del ejecutor.

2.3.1. ESCENARIO

Para realizar este escenario haremos uso del reconocimiento activo, ya que conocemos el nombre de la organización y el nombre del servidor al que queremos realizar el análisis de las vulnerabilidades.

Para esto se utilizó un PC con Windows 8, la cual tiene instalado NESSUS un analizador de vulnerabilidades, y una máquina virtual con el Sistema Operativo KALI que tiene varias

herramientas de reconocimiento, escaneo y análisis de vulnerabilidad.

Tabla 1 Lista de equipos que conforman el escenario

Sistema Operativo	Función
Windows 8	Sistema Operativo de donde se realizara el análisis de vulnerabilidades con la herramienta NESSUS
Kali Linux	Sistema Operativo de donde se intentara tener acceso al servidor de la Universidad, y se realizara el escaneo de puertos.
CentOS	Sistema Operativo donde se aloja la página de la Universidad

A continuación en la figura 2.1 se muestra una imagen del escenario planteado anteriormente.

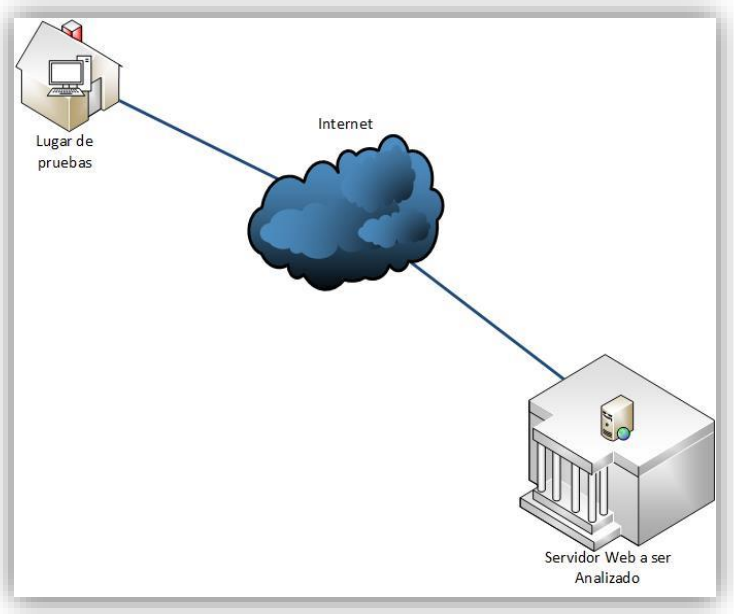


Figura 2. 1 Esquema del escenario planteado

2.4. DETALLE DE HERRAMIENTAS Y PROCEDIMIENTOS UTILIZADOS

2.4.1. HERRAMIENTAS DE ESCANEOS

Nmap: ("Network Mapper") es una fuente libre y abierta para la detección de redes y auditoría de seguridad. A muchos sistemas y administradores de red también les resulta útil para tareas como el inventario de la red, los horarios de actualización de servicio de gestión y monitoreo de host o servicio de tiempo de actividad. Nmap utiliza paquetes IP puros en formas novedosas para determinar qué servicios están disponibles en la red, ¿qué servicios (nombre de la aplicación y la versión) están ofreciendo,

qué sistemas operativos (y versiones del sistema operativo) que se están ejecutando, qué tipo de filtros de paquetes / cortafuegos están en uso, y docenas de otras características. Fue diseñado para escanear rápidamente grandes redes, pero funciona bien contra los host individuales. Nmap se ejecuta en todos los principales sistemas operativos y paquetes binarios oficiales están disponibles para Linux, Windows y Mac OS X. Además de la clásica línea de comandos Nmap ejecutable, la suite Nmap incluye un visor de interfaz gráfica de usuario avanzada y resultados (Zenmap), una transferencia de datos flexible, redirección y herramienta de depuración (Ncat), una utilidad para comparar los resultados del análisis (Ndiff), y una herramienta de análisis de generación de paquetes y la respuesta (Nping). [1]

2.4.2. HERRAMIENTAS DE ANÁLISIS DE VULNERABILIDAD

Los analizadores facilitan la labor del auditor porque permiten ejecutar desde una sola interfaz escaneos y enumeraciones sobre el objetivo, a la vez que identifican las vulnerabilidades presentes en dichos sistemas y las clasifican de acuerdo al nivel de riesgo presente. La identificación se realiza de acuerdo a la versión del sistema operativo y de los servicios y aplicaciones detectados comparándolos contra una base de datos de

vulnerabilidades que se actualiza frecuentemente conforme nuevos huecos de seguridad son descubiertos. [2]

Los niveles de riesgo se clasifican usualmente en: bajo, medio y alto, conforme a la siguiente escala:

Riesgo Alto: el equipo tiene una o más vulnerabilidades críticas que podrían ser explotadas fácilmente por un atacante y que podrían conllevar a tomar control total del sistema o comprometer la seguridad de la información de la organización. Los equipos con este nivel de riesgo requieren acciones correctivas inmediatas. [2]

Riesgo Medio: el equipo tiene una o más vulnerabilidades severas que requieren una mayor complejidad para poder ser explotadas y que podrían no brindar el mismo nivel de acceso al sistema afectado. Los equipos con riesgos severos requieren atención a corto plazo. [2]

Riesgo Bajo: el equipo tiene una o más vulnerabilidades moderadas que podrían brindar información a un atacante, la cual podría utilizarse para realizar ataques posteriores. Estos

riesgos deben ser mitigados adecuadamente, pero no tienen un nivel de urgencia alto. [2]

Aunque para el análisis de vulnerabilidad al sitio web de la universidad será mediante **NESSUS**, igual se detalla los analizadores de vulnerabilidad más populares:

OpenVas: Sistema de Evaluación de Vulnerabilidad Open (OpenVAS) es un framework de diversos servicios y herramientas que ofrecen una solución completa y potente de análisis de vulnerabilidades y gestión de vulnerabilidades. [3]

El escáner de seguridad real se acompaña con una alimentación diaria actualizada de pruebas de vulnerabilidades de red, más de 35.000 en total (a partir de abril de 2014). [3]

Todos los productos OpenVAS son Software Libre. La mayoría de los componentes están licenciados bajo la Licencia Pública General de GNU (GNU GPL). [3]

Nexpose: es un escáner de vulnerabilidades que tiene como objetivo apoyar a todo el ciclo de vida de gestión de vulnerabilidades, incluyendo el descubrimiento, la detección, verificación, clasificación de riesgo, análisis de impacto, la presentación de informes y la mitigación. Se integra con Metasploit de Rapid7 para la explotación de la vulnerabilidad. Se vende como software independiente, máquina virtual, o como un servicio gestionado o de despliegue de nube privada. La interacción del usuario es a través de un navegador web. Hay una versión gratuita pero limitada, así como versiones comerciales que comienzan en $ 2.000 por usuario al año. [4]

Nessus: Analizador popular y uno de los más antiguos, es patrocinado por la empresa Tenable Network Security. [2]

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. [5]

Retina: este analizador fue diseñado por la empresa E-Eye Digital Security (https://www.eeye.com/), recientemente adquirida por Beyond Trust (http://www.beyondtrust.com/) y presenta varias versiones, una de ellas de código abierto llamada Retina Community. [2]

2.5. ANÁLISIS DE VULNERABILIDADES DEL SITIO WEB

Efectuando un análisis de vulnerabilidad mediante la herramienta NESSUS se pudo obtener los siguientes resultados.

Luego de hacer Login en NESSUS como se muestra en la figura 2.2, pasamos a configurar el escaneo al sitio web, en el campo Name escribimos el alias del análisis, y en Targets escribimos la IP del sitio web, para este caso 186.46.90.120 como se muestra en la figura 2.3.

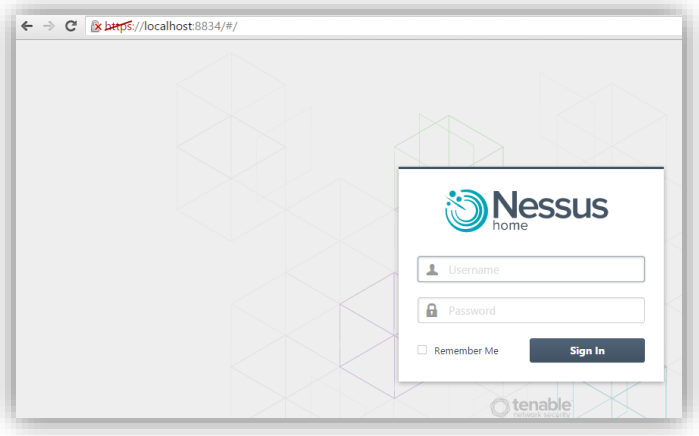


Figura 2. 2 Pantalla de inicio de sesión del NESSUS

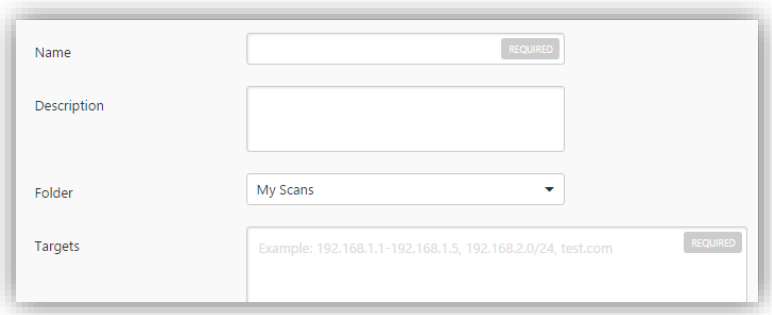


Figura 2. 3 Pantalla de configuración del análisis de vulnerabilidad de NESSUS

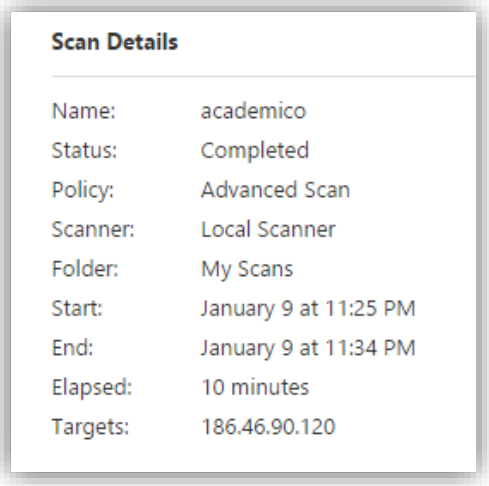


Figura 2. 4 Detalle del escaneo

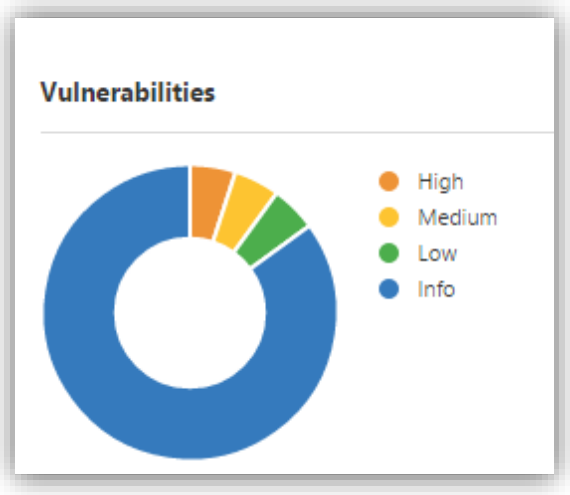


Figura 2. 5 Niveles de riesgos de vulnerabilidades encontrados

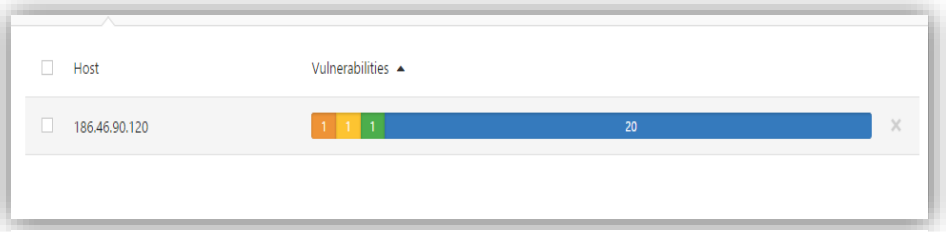
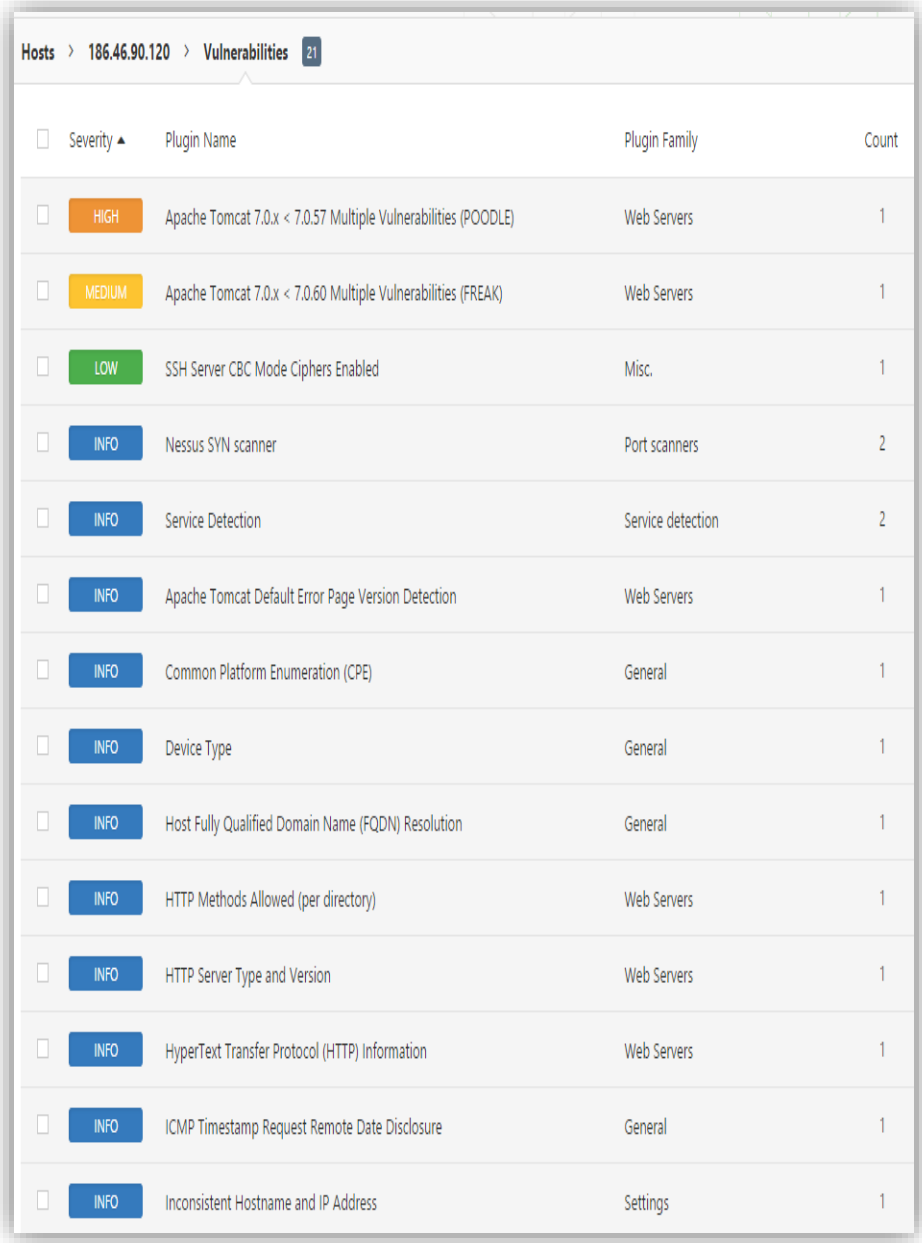


Figura 2. 6 Vulnerabilidades encontradas

En la figura 2.7 se ve con más detalle las vulnerabilidades del sitio, las de Alto, medio y bajo riesgo. Y las de tipo informativos. El análisis se lo hizo con la herramienta NESSUS.

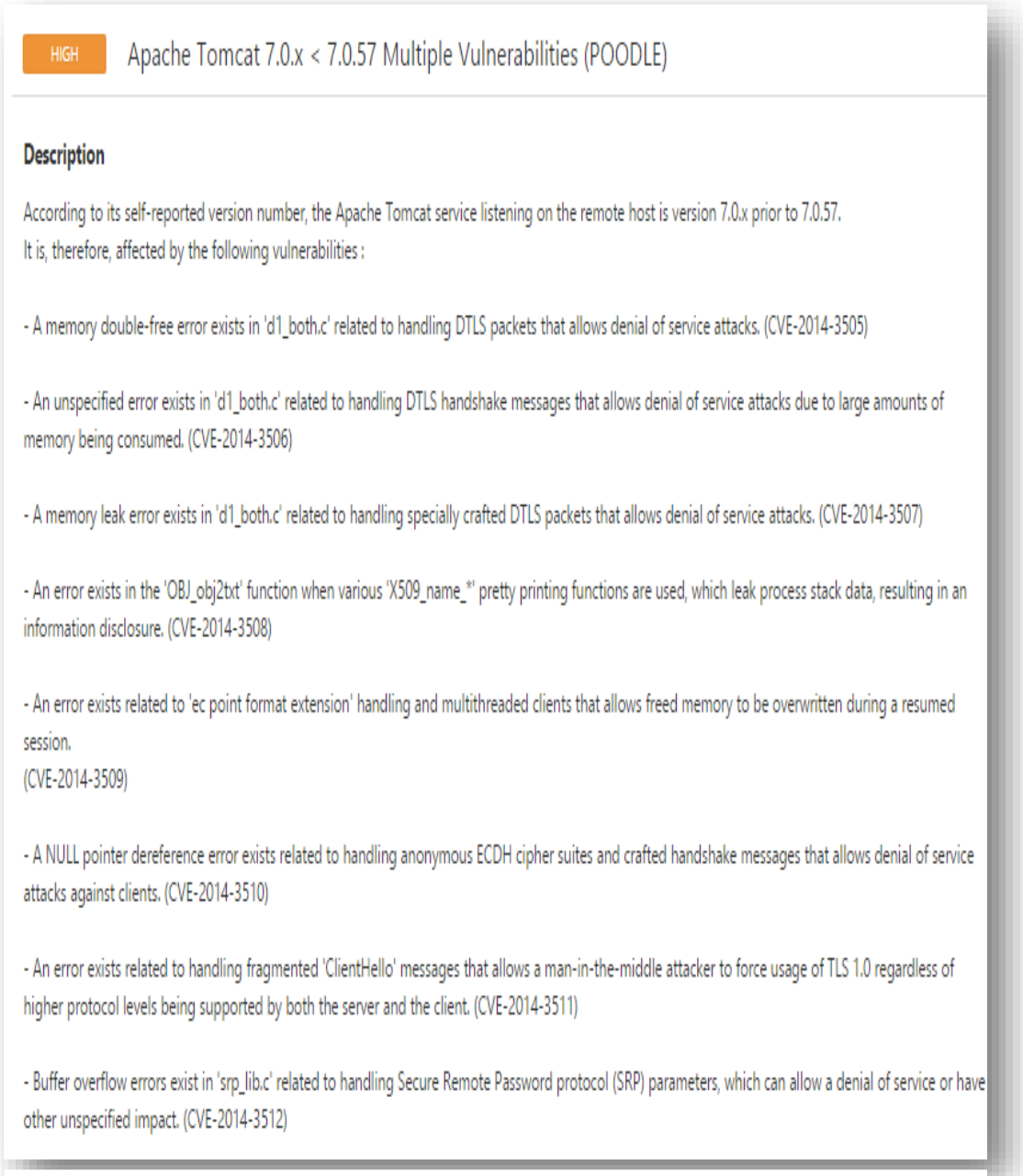


Hosts › 186.46.90.120 › Vulnerabilities 21

Severity ▲	Plugin Name	Plugin Family	Count
HIGH	Apache Tomcat 7.0.x < 7.0.57 Multiple Vulnerabilities (POODLE)	Web Servers	1
MEDIUM	Apache Tomcat 7.0.x < 7.0.60 Multiple Vulnerabilities (FREAK)	Web Servers	1
LOW	SSH Server CBC Mode Ciphers Enabled	Misc.	1
INFO	Nessus SYN scanner	Port scanners	2
INFO	Service Detection	Service detection	2
INFO	Apache Tomcat Default Error Page Version Detection	Web Servers	1
INFO	Common Platform Enumeration (CPE)	General	1
INFO	Device Type	General	1
INFO	Host Fully Qualified Domain Name (FQDN) Resolution	General	1
INFO	HTTP Methods Allowed (per directory)	Web Servers	1
INFO	HTTP Server Type and Version	Web Servers	1
INFO	HyperText Transfer Protocol (HTTP) Information	Web Servers	1
INFO	ICMP Timestamp Request Remote Date Disclosure	General	1
INFO	Inconsistent Hostname and IP Address	Settings	1

Figura 2. 7 Detalle de las vulnerabilidades encontradas con la herramienta NESSUS

A continuación detallaremos las vulnerabilidades de alto riesgo encontradas:



HIGH Apache Tomcat 7.0.x < 7.0.57 Multiple Vulnerabilities (POODLE)

Description

According to its self-reported version number, the Apache Tomcat service listening on the remote host is version 7.0.x prior to 7.0.57.
It is, therefore, affected by the following vulnerabilities :

- A memory double-free error exists in 'd1_both.c' related to handling DTLS packets that allows denial of service attacks. (CVE-2014-3505)

- An unspecified error exists in 'd1_both.c' related to handling DTLS handshake messages that allows denial of service attacks due to large amounts of memory being consumed. (CVE-2014-3506)

- A memory leak error exists in 'd1_both.c' related to handling specially crafted DTLS packets that allows denial of service attacks. (CVE-2014-3507)

- An error exists in the 'OBJ_obj2txt' function when various 'X509_name_*' pretty printing functions are used, which leak process stack data, resulting in an information disclosure. (CVE-2014-3508)

- An error exists related to 'ec point format extension' handling and multithreaded clients that allows freed memory to be overwritten during a resumed session.
(CVE-2014-3509)

- A NULL pointer dereference error exists related to handling anonymous ECDH cipher suites and crafted handshake messages that allows denial of service attacks against clients. (CVE-2014-3510)

- An error exists related to handling fragmented 'ClientHello' messages that allows a man-in-the-middle attacker to force usage of TLS 1.0 regardless of higher protocol levels being supported by both the server and the client. (CVE-2014-3511)

- Buffer overflow errors exist in 'srp_lib.c' related to handling Secure Remote Password protocol (SRP) parameters, which can allow a denial of service or have other unspecified impact. (CVE-2014-3512)

Figura 2. 8 Vulnerabilidad de riesgo Alto

Con este análisis se identificó que el sitio es vulnerable a ataques de denegación de servicios como se muestra en la figura 2.8.

A continuación se detalla las vulnerabilidades de medio riesgo:

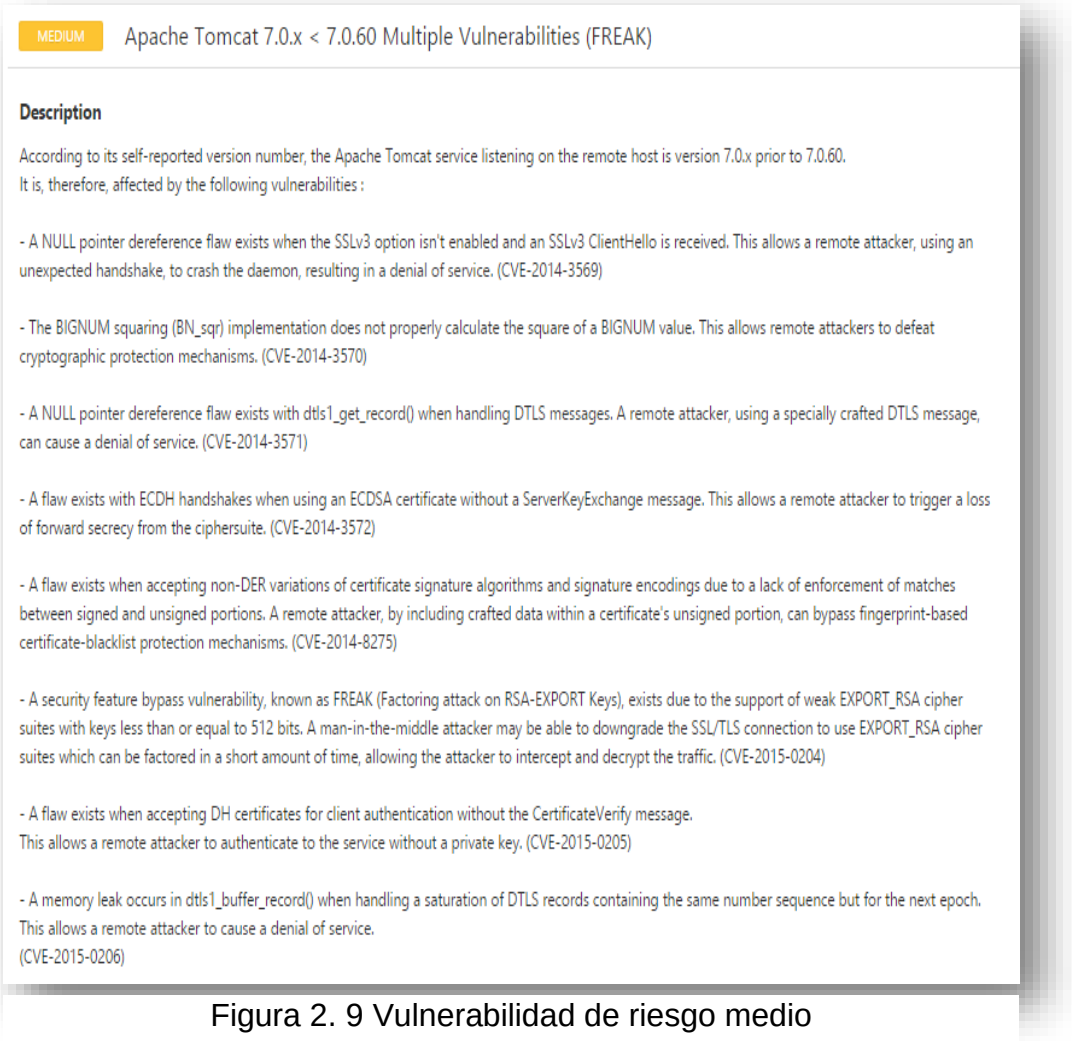


Figura 2. 9 Vulnerabilidad de riesgo medio

Con este análisis se identificó que el sitio es vulnerable a ataques de denegación de servicios.

A continuación se detalla las vulnerabilidades de bajo riesgo.

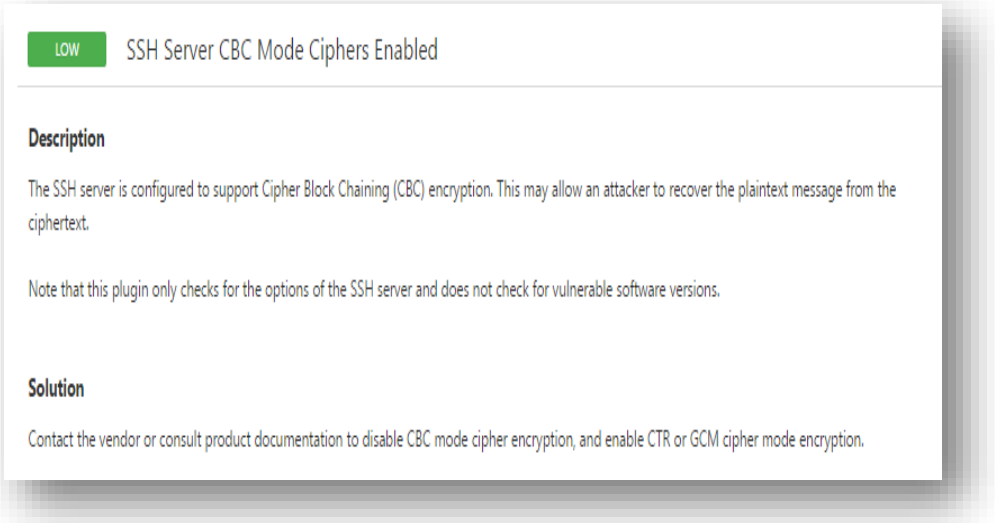


Figura 2. 10 Vulnerabilidad de riesgo bajo encontrados con la herramienta NESSUS

Con este análisis se identificó que un atacante podría recuperar texto plano de esta conexión, debido a que el encriptado se lo hace con CBC, el cual con la técnica adecuada permitiría a un atacante sustraer información.

CAPÍTULO 3

ANÁLISIS DE RESULTADOS

3.1 DENEGACIÓN DE SERVICIO

Con el análisis que se hizo con la herramienta de análisis de vulnerabilidad NESSUS se pudo deducir que el sitio web universitario es vulnerable a los ataque DoS, este ataque lo vamos hacer mediante un script llamado slowloris.pl usando Kali Linux.

Al ejecutar el script vemos que el sitio web deja de funcionar en unos cuantos segundos. Como se muestra en las figura y en video que se presentara durante la sustentación.

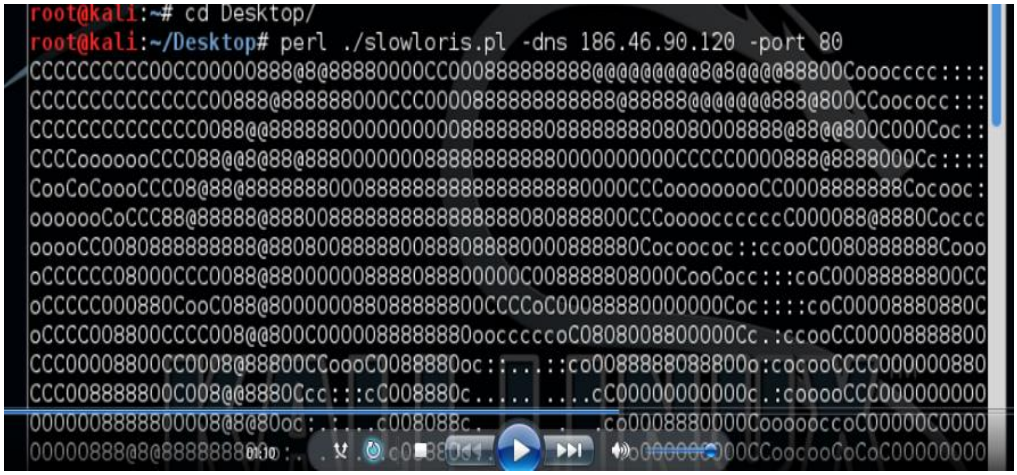


Figura 2. 11 Ejecución de ataque DoS

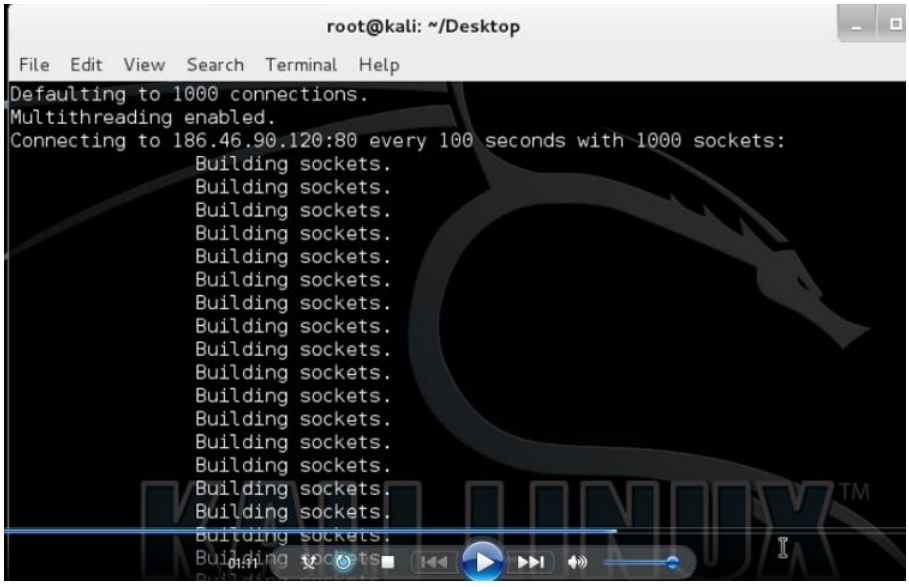


Figura 2. 12 Ejecución exitosa del ataque DoS

Este Ataque es era uno de los Riesgos más altos que nos mostró la herramienta de análisis de vulnerabilidad NESSUS, por lo tanto es algo que hay que tener muy presente ya que con esto la universidad se podría meter en problemas al momento que sean los días de subir las notas al sistema académico. Como se muestra en la figura 2.13.

Por eso se recomienda que se actualice a Apache Tomcat versión 7.0.60 o superior.

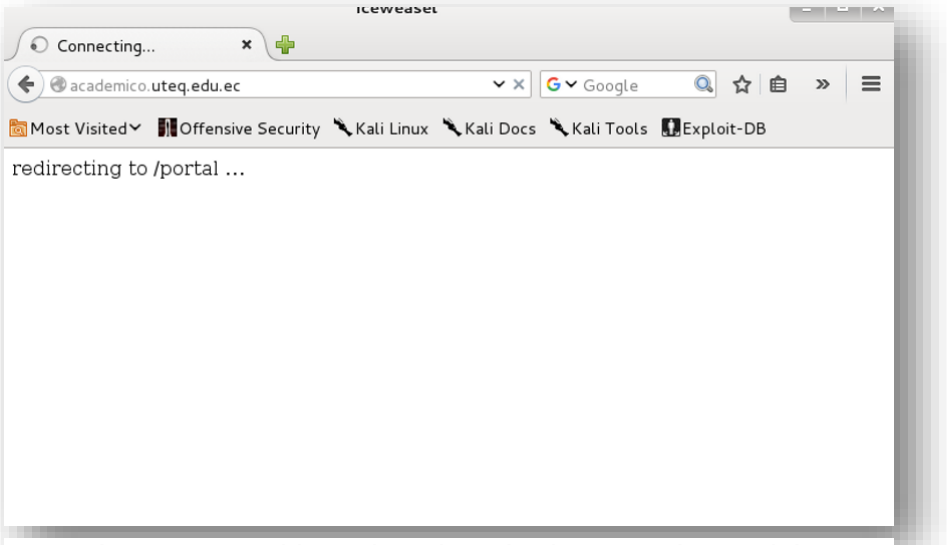


Figura 2. 13 Sitio web Universitario fuera de servicio

3.2. VULNERABILIDADES BAJAS

Unas de las vulnerabilidades bajas que logro detectar el analizador de vulnerabilidades NESSUS, es decir que el servidor SSH está configurado para admitir el cifrado Cipher Block Chaining (CBC). Esto podría permitir a un atacante recuperar un mensaje de texto plano a partir del texto cifrado. La solución para esto es deshabilitar el cifrado CBC, y permitir cifrado CTR , que hace que los paquetes de texto plano no cifren en forma de bloques sino que se cifren de manera de un flujo de bloque, esto hace que recuperar texto plano de este cifrado sea casi imposible.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. Luego de los ataques efectuados al sitio web universitario hace un año, se tomaron medidas para corregir estos focos de inseguridad, pero vemos en la realización de este proyecto que aún hay vulnerabilidades en el sitio.
2. Se debe de tomar medidas para poder mitigar un ataque DoS.
3. Vemos que tiene un cifrado SSH pero la herramienta de vulnerabilidad nos muestra que a pesar de estar cifrado podría ser producto de un ataque informático.

RECOMENDACIONES

1. Hay que tomar seriamente el tema de la seguridad informática en todas las organizaciones, en especial cuando se trata de instituciones como las universidades que manejan datos muy importantes como los registros académicos de los estudiantes de años de estudios.
2. Realizar análisis de vulnerabilidad continuamente con expertos en el tema para poder siempre estar un paso delante de los ataques informáticos.

BIBLIOGRAFÍA

[1] G. Lyon, «http://www.hamirayane.com,» 2014. [En línea]. Available: http://www.hamirayane.com/es/download/download_Nmap/.

[2] K. Astudillo, Hacking Ético 101, Guayaquil, 2013.

[3] «http://www.openvas.org,» 2015. [En línea]. Available: http://www.openvas.org/about.html.

[4] «http://sectools.org/,» [En línea]. Available: http://sectools.org/tool/nexpose/.

[5] «http://www.gb-advisors.com/,» [En línea]. Available: http://www.gb-advisors.com/es/digital-security/nessus-vulnerability-scanner/?gclid=CNP99OmRrMoCFVEIkQodt6oIwQ.