Metodología para detectar riesgos en seguridad informática en la universidad autónoma de zacatecas basada en pruebas de penetración

Methodology for detecting computer security risks at the autonomous university of zacatecas based on penetration tests

DOI: 10.46932/sfjdv3n6-030

Received in: October 24th, 2022
Accepted in: November 25th, 2022

Pedro Morales González
Máster en Ciencias de la Ingeniería
Institución: Universidad Autónoma de Zacatecas - Campus Siglo XXI, Edificio de Ingeniera de Software
Dirección: Carr. Zacatecas-Guadalajara, Km 6, C.P. 98160, Zacatecas, Zac., México
Correo electrónico: 27800748@uaz.edu.mx

Sodel Vázquez Reyes
Doctorado en Informática
Institución: Universidad Autónoma de Zacatecas - Campus Siglo XXI, Edificio de Ingeniera de Software
Dirección: Carr. Zacatecas-Guadalajara, Km 6, C.P. 98160, Zacatecas, Zac., México
Correo electrónico: vazquezs@uaz.edu.mx

Santiago Villagrana Barraza
Máster en Ciencias de la Ingeniería
Institución: Universidad Autónoma de Zacatecas - Campus Siglo XXI, Edificio de Ingeniera de Software
Dirección: Carr. Zacatecas-Guadalajara, Km 6, C.P. 98160, Zacatecas, Zac., México
Correo electrónico: svillagrana@uaz.edu.mx

Perla Velasco Elizondo
Doctorado en Informática
Institución: Universidad Autónoma de Zacatecas - Campus Siglo XXI, Edificio de Ingeniera de Software
Dirección: Carr. Zacatecas-Guadalajara, Km 6, C.P. 98160, Zacatecas, Zac., México
Correo electrónico: pvelasco@uaz.edu.mx

Carlos H. Castañeda Ramírez
Máster en Ciencias de la Ingeniería
Institución: Universidad Autónoma de Zacatecas - Campus Siglo XXI, Edificio de Ingeniera de Software
Dirección: Carr. Zacatecas-Guadalajara, Km 6, C.P. 98160, Zacatecas, Zac., México
Correo electrónico: castr@uaz.edu.mx

Alejandro Mauricio González
Doctorado en Educación
Institución: Universidad Autónoma de Zacatecas - Campus Siglo XXI, Edificio de Ingeniera de Software
Dirección: Carr. Zacatecas-Guadalajara, Km 6, C.P. 98160, Zacatecas, Zac., México
Correo electrónico: amgdark@uaz.edu.mx

RESUMEN
El propósito de este artículo es mostrar algunas vulnerabilidades con las que se cuentan en la Universidad Autónoma de Zacatecas después de aplicar pruebas de penetración a los activos informáticos como lo son servidores, aplicaciones web y equipo de cómputo, mostrando puntos críticos que puedan comprometer el funcionamiento o información privada de la misma, exponiendo datos de alumnos, profesores y áreas administrativas. El hecho de que las universidades no contemplen los activos informáticos como un factor que pueda detener su funcionamiento resulta un gran problema, según datos de la Asociación Nacional de Universidades e instituciones de Educación Superior solo 46 universidades de 140 hacen auditorías a sus sistemas(ANUIES, 2016), por lo que esta prueba se realizó de forma interna en la universidad aplicando la metodología de penetración estándar ya que esta se adapta a los recursos y capacidades de TI con las que la universidad cuenta. Obteniendo como resultado un reporte de algunas vulnerabilidades de seguridad existentes.

Palabras clave: seguridad, virus, infraestructura, vulnerabilidades, ataques, metodologías, herramientas, detección de vulnerabilidades.

ABSTRACT
The purpose of this article is to show some vulnerabilities in the Universidad Autónoma de Zacatecas after applying penetration tests to computer assets such as servers, web applications and computer equipment, showing critical points that can compromise the operation or private information of the same, exposing data of students, teachers and administrative areas. The fact that universities do not contemplate IT assets as a factor that can stop their operation is a big problem, according to data from the National Association of Universities and Higher Education Institutions only 46 universities out of 140 make audits to their systems(ANUIES, 2016), so this test was performed internally at the university applying the standard penetration methodology since this is adapted to the IT resources and capabilities with which the university has. Obtaining as a result a report of some existing security vulnerabilities.

Keywords: security, virus, infrastructure, vulnerabilities, attacks, methodologies, tools, vulnerability detection.

1 INTRODUCCIÓN

Existe un creciente número de ataques cibernéticos hacia las organizaciónes,especificamente a su información y/o procesos, con el fin de bajar la reputación de la empresa, vandalimo, robo, dañar propiedad intelectual o generar perida de ingresos. Cualquiera de los casos impidiende su optimo funcionamiento, por lo que las se ha tenido que adoptar medidas contra esto, implementando diferentes tipos de acciones sean políticas, software y/o hardware especializado para contrarrestar estos ataques, existen métodos como ISSAF,cadena de eliminación cibernetica o PTES por mencionar algunos, elaborados con el fin de ayudar a detectar gran parte de las vulnerabilidades dentro de una organización.

La Universidad Autónoma de Zacatecas como organización publica cuenta en sus sistemas con datos de información del personal como nombres, telefonos, correos, etc; trabajos de docentes y estudiantes, al igual que datos financieros. Perder esta información es crítico para cualquier organización, como lo mencionamos los motivos pueden ser multifactoriales y dan como resultado un tema que para muchos pasa desapercibido o simplemente se le da poca importancia. La Ciberseguridad cuya definición es: “Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, se almacena y se transporta mediante los sistemas de información que se encuentran interconectados”(Morales, 2016).

Por lo tanto, la seguridad de la información es el estado de “confianza” donde se mantiene baja o tolerable la posibilidad de robo, manipulación y destrucción de la información y servicios, esto por el hecho de que realmente nunca se esta seguro en su totalidad, por tal motivo se busca tener un nivel en el que almenos no existan vulnerabilidades ya documentadas.

Normalmente este tema se considera poco atractivo para una inversión económica pero el costo de un ataque a la seguridad podría ser mayor a reemplazar los dispositivos involucrados en el ataque. En caso de pérdidas de información la organización es responsable de comunicarse con todas las personas afectadas y en el peor de los casos prepararse para un proceso jurídico.

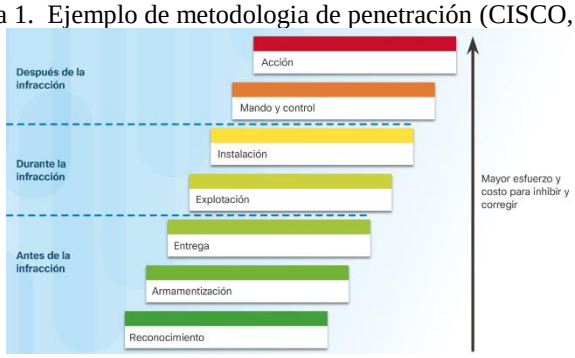
La seguridad de la información debe cuidar tres puntos importantes:

- Confidencialidad. Garantía que la información se accesible solo a quien tiene la autorización de acceder a ella.
- Integridad. La confiabilidad del dato o recurso en términos de prevenir el cambio incorrecto o no autorizado.
- Disponibilidad. Garantía que la información estara disponible cuando se requiera.

De los mecanismos que existen para comprobar la seguirdad se encuentras las pruebas de penetración la cual nos puede servir como apoyo para tomar medidas ante las vulnerabilidades detectadas.

Existen varias metodologias para realizar pruebras de penetración que varian según la granualidad de sus fases,como ya se ha mencionado ocupan de recurso humano normalmente especializado en el tema o almenos para tenerlo destinado para estas funciones, recurso humano con el que la universidad no cuenta, por lo que implementar una metodologia extensa se vuelve complicado.

Figura 1. Ejemplo de metodologia de penetración (CISCO, 2017)



En la figura 1 se muestra un ejemplo de metodologia para penetración la cual cuenta con fases/capas ,existen muchas otras con mas o menos fases dependiendo el nivel de detalle que se quiera tener, no por ello implica que las que menos tienen sean menos efectivas.

Cuadro 1.Comparativa de fases entre metodologias de penetración

Proceso	Color
Fase 1	
Fase 2	
Fase 3	
Fase 4	
Fase 5	
Fase 6	
Fase 7	

Metodología	Planeación y preparación	Recolección de información	Mapeo de la red de trabajo	Identificación de vulnerabilidades	Penetración	Ganar acceso y escalar privilegios	Mapeo con acceso	Comprometer acceso remoto	Mantener Acceso	Cubrir ataque	Reporte
ISSAF											
Cadena de Eliminación Cibernetica											
Prueba de penetración estandar											

2 DESCRIPCIÓN DEL MÉTODO

La metodoliga que se uso para esta prueba se basa en “la cadena de Eliminación cibernetica”, si bien esta no contempla una fase de planeación y preparación, se tubieron juntas para delimitar el area a probar y se brindo un acceso total a la infraestructura de la red por lo que la fase de mapeo con acceso se hace con el mapeo de la red de trabajo de la fase 1, otro punto que se agrega a esta prueba es el reporte ya que era necesario para la universidad concocer sus vulnerabilidades en estas areas, como erremienta para la prueba se utilizo el sistema operativo Kali Linux ya que este cuenta con exploits ya difundidos, como se mencionó es importante almenos estar protegidos ante vulnerabilidades ya existentes, de igual forma al utilizar software libre evitamos el uso de licencias.

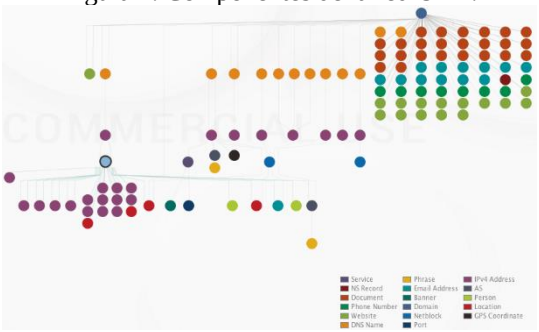
2.1 RECOLECCIÓN DE INFORMACIÓN(FASE 1)

En este punto uilizaremos diferentes herramientas como motores de busqueda,ingenieria social, etc. para conocer la postura de la seguiridad de forma externa, de igual forma podremos reducir el area de trabajo obteniendo registros DNS y Rangos de IP que la componen, de igual forma algunos datos relevantes que permitan identificar algunas vulnerabilidades y poder dimencionar el area de trabajo.

La Universidad Autónoma de Zacatecas al momento de realizar la prueba cuenta con AXTEL-1 AXTEL S.A DE C.V como provedor de internet,12 correos de docentes y 15 sitios web relacionados al

nodo inicio con dominio uaz.edu.mx aproximadamente montado en un servidor web Apache-Coyote/1.1 desde el 19 de octubre del 2013,con un sistema operativo HP-UX;Se encuentra localizada en la ciudad de Zacatecas,Zac. Latitud 22,7833 y longitud -102,5833 codigo postal 98024.

Figura 2. Componentes de la red UAZ.



En la cuadro 2 se osbserva parte de la red que compone a la universidad, se utiliza el donimio uaz.edu.mx para empezar a realizar la busqueda, en la que pudimos obtenter, números de telefono, correos asociados a este domino de docentes y encargados, de igual forma DNS,algunos se muestran en la figura 4.

Cuadro 2.Muestra de los DNS de la UAZ

Nombres de DNS	IPS
virtual.uaz.edu.mx	192.169.215.204
intranet.uaz.edu.mx	148.217.18.15
portal.uaz.edu.mx	148.217.18.32
siiaf.uaz.edu.mx	148.217.18.36
www2.escolar.uaz.edu.mx	148.217.18.34
www.uaz.edu.mx	148.217.50.5
escolar.uaz.edu.mx	148.217.18.17

Una vez obtenidos los DNS podemos ir recopilando mas información de cada nodo, mas telefonos, correos, aplicaciónes web, etc. para este segmento se encontraron los bloques de red que se muestran en la cuadro 3.

Cuadro 3.Rangos de direcciones de la UAZ

Bloques de red	
Inicia	Termina
148.217.18.0	148.217.18.255
192.169.215.0	192.169.215.255
148.217.50.0	148.217.50.255

2.2 MAPEDO DE LA RED DE TRABAJO (FASE 1)

En este punto escanearemos la red de forma interna en la universidad para identificar los servidores, puertos y servios con los que se cuenta, en este caso mostraremos como se realizó el escaneo a uno de los programas con los que se cuenta en la universidad.

Unidad academica: Ingenieria en computación.

IPS(Privadas) :10.2.48-50.1/24.

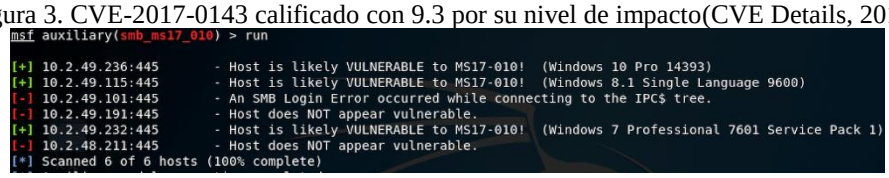
Se utiliza nmap con los los puertos TCP: 21-23,53,80,134,etc. y los puertos UDP:123,135,137,161,etc. por mencionar algunos, los puertos a evaluar se identificaron como los top en vulnerabilidades(ISC,2017)al mencionar puertos vulnerables hacemos referencia al servicio que este corre por defecto.

Despues de realizar dicha funcion se optiene un reconocimiento de 768 IPS con 533 maquinas activas.

2.3 IDENTIFICACIÓN DE VULNERABILIDADES (FASE 2)

En la figura 3 se muestra como se ulitza el auxiliar smb_ms17_010 para comprobar si son vulnerables en el puerto 445.

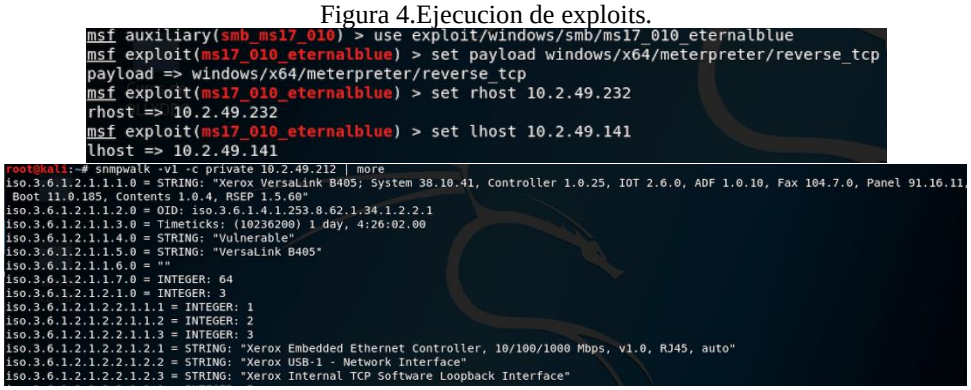
Figura 3. CVE-2017-0143 calificado con 9.3 por su nivel de impacto(CVE Details, 2017).



2.4 PENETRACIÓN (FASE 3 Y 4)

Una vez comprobado que existen vulnerabilidades se ejecuta la penetración, muchas de las vulnerabilidades conocidas se encuentran la base de datos de Kali Linux por lo que solo bastaria encontrar el exploit indicado,ejemplo de esto tenemos el eternalblue como se muestra en la figura 4. Seleccionamos la maquina con la ip 10.2.49.232 con sistema operativo Windows 7 Professional y para la IP 10.2.49.212 el snmpwalk la cual es una impresora Xerox.

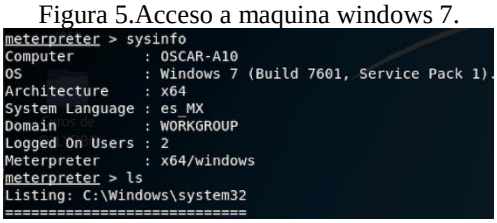
Figura 4.Ejecucion de exploits.



2.5 GANAR ACCESO Y ESCALAR PRIVILEGIOS (FASE 5)

Para los dos casos se tienen acceso de forma remota y se cuenta con derecho de escritura y lectura por lo que no fue necesario escalar privilegios.

Figura 5.Acceso a maquina windows 7.



2.6 MANTENER ACCESO (FASE 6)

Una vez teniendo acceso se cuentan con exploit post ataque o bien se puede realizar un backdor que se ejecute cada que se inicie la maquina, perminitiendonos accceso a ella cada que se ocupe, siempre y cuando no se detecte el dicho malware.

2.7 REPORTE (FASE 7)

En la figura podemos observar el numero de servidores según el puerto abierto, el nivel de impacto,entiéndace como bajo con existencia de vulnerabilidad, medio con riesgo a tener acceso según el nivel de conocimiento del aatacante y crítico acceso con bajo conocimiento del atacante la descripcion de este puerto.

Cuadro 4.Repote ante vulnerabilidades por puertos.

Nivel	Conocimiento del atacante	Impacto
Bajo	Bajo	Bajo
Medio	Alto	Alto
Crítico	bajo	Alto

Puertos/Protocolo	Nombre	N.Hosts	Bajo	Medio	Crítico	Descripción
21/tcp	Ftp	2	2			Protocolo de transferencia.
22/tcp	Ssh	8		8		SSH,SFTP.
23/tcp	telnet	4		2	2	Manejo remoto de equipo.
53/udp	DNS	2	2			Nombre del dominio.
80/tcp	http	11	9	2		Prot. De trans. De Hip.Text.
123/udp	NTP	492	492			Prot. De sincr. de Tiempo.
135/udp	epmap	482	482			Epmap.
139/tcp	netbios-ns	480	480			Servicio de sesiones.
161/udp	netbios-ssn	486	485		1	SNMP.
443/tcp	https	8				Trans. Segura de pág. Web.
445/tcp	Protocolo smb	6	3		3	Compartir archivos.
3306/tcp		5	2	3		MySQL.
8000/tcp		1	1			Sustituo erroneo de 8080.

El escaneo a dicha unidad de la universidad nos muestra 5 host con nivel crítico, los dos ejemplo que se muestran demuestran el acceso a información personal de los docentes y alumnos, la impresona nos dio conocimiento de las ip de la maquina del direcctor del progama e igual forma de la secretaria, las que posteriormente se les dio un tratamiento especial para la obtencion de datos por el nivel de información que se cuentran en ellas.

3 COMENTARIOS FINALES

3.1 RESUMEN DE RESULTADOS

En este artículo se realizo una prueba de penetración a la Universidad Autónoma de zacatecas, Los resultados de la prueba se muestran en la tabla de reporte en el que se observa el numero de servidores, tipos de puertos evaluados y el nivel que la vulnerabilidad que se llega a tener.

4 CONCLUSIONES

El presente trabajo ayuda a reforzar la necesidad de que la universidad inicie con la implementación de un programa de seguridad de la información que permita evaluar los riesgos y establecer los mecanísmos de control necesarios, lo cual implica inversión en diferentes estraterías sea software, hardware o capacitación, para brindar una mejor protección de los activos de información de la institución. No cabe duda que es indispensable el uso de tecnologías de la información como apoyo a los proceso educativo, ya que le facilita e incrementa la productividad de docentes, administrativos y alumnos. Sin embargo, es necesario valorar los riesgos, ya que como se puedo demostrar, existen activos

vulnerables a ataques internos y externos, los cuales podrían representar pérdidas económicas y/o intelectuales para la continuidad de la universidad.

RECOMENDACIONES

Cabe destacar que existen gran variedad herramientas capaces de ejecutar automáticamente una prueba de penetración, se sugiere que se haga manualmente ya que solo así podremos saber si son realmente vulnerables o solo son falsos positivos. El pentester o auditor, al hacerlo de forma manual debe recurrir al uso de su conocimiento y de la información en internet ya que nuevas vulnerabilidades pondrían salir durante el proceso, de igual forma existen múltiples herramientas que le permitirán realizar un test preciso sobre el sistema para obtener buenos resultados.

REFERENCIAS

ANUIES. (2016). *Estado actual de las Tecnologías de la Información y las Comunicaciones en las Instituciones de Educación Superior en México* (Primera Ed).

CISCO. (2017). Introducción a la Ciberseguridad. Retrieved September 19, 2017, from https://static-course-assets.s3.amazonaws.com/CyberSec2/es/index.html#4.2.2.1

CVE Details. (2017). CVE-2017-0143 : The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows. Retrieved September 27, 2017, from https://www.cvedetails.com/cve-details.php?t=1&cve_id=cve-2017-0143

Morales. (2016). ¿Qué es la Administración de Riesgos? Retrieved May 21, 2017, from https://www.auditool.org/blog/control-interno/700-administracion-de-riesgos-conceptos-fundamentales-parte-1

ISC. (2017). Top 10 reportes. Retrieved September 26,2017, from https://isc.sans.edu/top10.html