Esquema de Seguridad de la Capa de Distribución para Redes de Datos en Instituciones Educativas de Nivel Superior basadas en el Modelo Jerárquico.

A. Calvillo, C. Hernández

***Abstract*|—Se presentan los principales resultados y observaciones presentadas de una evaluación de ciberseguridad en una entidad educativa en Montemorelos, Nuevo León, México basados en la metodología OSSTMM. El fin del estudio es proponer un esquema a la institución con el fin de evaluar los riesgos dentro de la infraestructura de red.**

***Keywords*— Ciberseguridad, Evaluación de Riesgos, OSSTMM, Modelo jerárquico, Vulnerabilidades.**

I. Introducción

La seguridad de la información es todavía un desafío severo para frustrar las amenazas debido a la falta de control sobre las brechas de seguridad y la conciencia en la sociedad [1]. Dentro de la Universidad de Montemorelos, la entidad por auditar, no existe un esquema definido para la implementación de la estructura de la red, muchos problemas puede surgir a partir de esto, tales como:

- Escaso nivel del aseguramiento de la calidad en el servicio.
- Limitaciones a la hora de monitorear dispositivo con fallas.
- Entornos pocos seguros dentro de la LAN
- Dificultad a la hora de expandir las necesidades del servicio.

En los últimos años se han descubierto ciertos ataques de seguridad en el sector educativos [2], demostrando que esta área no estaba totalmente exenta. Durante esta investigación se buscó esquematizar un modelo seguro para para la capa de distribución a manera de objetivo principal, para esto, se desarrollaron diferentes un par de objetivos específicos los cuales buscaban establecer pautas para la evaluación del riesgo, además de realizar una base de datos con las vulnerabilidades dentro de la Universidad de Montemorelos.

En diferentes entidades se han desarrollado estudios similares con el fin de evaluar y establecer propuestas a los encargados de la infraestructura de red, un ejemplo es descrito en ministerio de gobierno chileno [3] donde se realizaron estudios de valoración de riesgo a partir de un estudio de vulnerabilidades. Durante dicho estudio, se tomó como base la metodología OSSTMM (Manual de la Metodología Abierta de Testeo de Seguridad, por sus siglas en inglés), el fin de esta metodología es realizar un análisis de la seguridad, evitando la subjetividad del auditor y estableciendo métricas cuantitativas objetivas.

II. Metodología

Para encontrar vulnerabilidades en la capa 2 y 3 de la red en la Universidad de Montemorelos se utilizó la distribución basada en el GNU/Linux Kali ya que esta provee una gran cantidad de herramientas con el fin de evaluar diferentes sistemas.

Basándose en las metodologías del EC-Council Certified Ethical Hacking se utilizaron dos de las cinco etapas que el material propone [4], ya que, el fin del estudio fue solo encontrar vulnerabilidades en la infraestructura de la red sin explotarlas. Estas etapas fueron usadas con el fin de encontrar posibles vulnerabilidades en los dispositivos conectados a la red de la entidad educativa.

A. Fase de Reconocimiento

Durante la fase de reconocimiento se utilizaron diferentes herramientas para obtener información general de la red que nos facilite el acceso al entorno [5] como:

- Who.is: Sitio que provee información general tomando como argumentos un nombre de dominio.
- Nslookup: Es una aplicación incluida en sistemas Windows para verificar los problemas de DNS de una conexión.

B. Fase de Escaneo

El propósito de esta fase es revisar todos los dispositivos que se puedan encontrar, aplicaciones utilizadas, credenciales de fácil acceso por medio de diferentes herramientas.

- Fing: Permite hacer un escaneo de dispositivos activos que se encuentran dentro de la red a la cual se está conectada, además de proveer información como: Dirrección IP, MAC y nombre del host.

- OpenVAS: Es una herramienta que permite hacer una búsqueda automatizada de las vulnerabilidades de un dispositivo especifico dada su dirección IP como argumento. Las vulnerabilidades son comparadas con la base de datos de CVE. [6]

C. Evaluación de los riesgos.

Para la propuesta de evaluación de riesgos se decidió optar por la metodología OSSTMM [7] ya que, basados en un estudio de literatura, esta propone ciertas ventajas sobre algunos otros modelos como el uso de métricas cuantificables, denominadas *ravs (Risk Assessment Value)*, con el fin de evaluar el riesgo de manera objetiva.

El primer paso para la realización de la metodología está denominado como seguridad operacional, la cual está conformada por tres parámetros que necesitan ser cuantificados para obtener un resultado definido. Las tres medidas serán descritas a continuación:

1) Visibilidad: Cuantificar el número objetivos que serán auditados. Todos los canales que vayan a ser verificados deben ser incluidos en este parámetro.
2) Accesos: Corroborar los puntos de acceso que interactúen con el canal, es decir, si se tiene una dirección IP, además de 2 puertos activos, se dice que existen 3 accesos.
3) Confianza: Contar cada punto de confianza. Un ejemplo podría ser la redirección de puertos.

La segunda categoría es denominada “Controles”, en esta sección se visualizarán algunas formas de protección.

4) Autenticación: Verificar las instancias para acceder. Cada forma de autenticación tendrá el valor de 1.
5) Indemnización: Hacer un conteo de los dispositivos que cuentan con una compensación en caso de sufrir daños.
6) Resistencia: Se tiene control de la seguridad aún en caso de desastre.
7) Subyugación: Se hace un conteo donde las comunicaciones pueden realizarse de forma segura, un ejemplo podría ser el uso del protocolo HTTPS.
8) Continuidad: Comprobar la redundancia que los objetivos tienen y corroborar si existe una metodología en caso de interrupción.
9) No repudio: Comprobar si existen formas de determinar si existió alguna interacción con el sistema. Un ejemplo puede ser un sistema de logs.
10) Confidencialidad: Verificar si existe alguna forma para evitar que la información sea revelada a un usuario malintencionado.
11) Privacidad: Corroborar que las conexiones en los enlaces sean privadas.
12) Integridad: Establecer mecanismos para corroborar que la información que viaja no sea modificada por usuarios malintencionados.
13) Alarma: Establecer pautas para el monitoreo de equipos y la generación de una notificación en dado caso de presentarse un suceso no previsto.

Por último las limitaciones, se describen como errores o fallas

14) Vulnerabilidad: Cuantificar las fallas que pudieran resultar en el acceso no autorizado de terceros.
15) Debilidad: Verificar la legitimidad en los controles de interacción: autenticación, indemnización, resistencia, subyugación y continuidad.
16) Preocupación: Corroborar las fallas en los controles de: no repudio, confidencialidad, privacidad, integridad y alarma. Un ejemplo podría ser la generación de datos erróneos en los logs.
17) Exposición: Contar acciones no justificadas que provean información de los objetivos.
18) Anomalía: Verificar los elementos desconocidos que no pueden ser clasificados.

Todos estos valores son expuestos para entender qué es lo que se está midiendo, sin embargo, dentro del sitio web de ISECOM es posible descargar una plantilla donde el analista pueda ingresar los datos y obtener automáticamente los valores de los ravs.

III. RESULTADOS

Durante el estudio, se realizaron escaneos de red con el fin de encontrar dispositivos con los que se pudieran interactuar y se encontró que existían 10 dispositivos que cumplían la función de switcheo y enrutamiento .

Dentro del escaneo es importante comentar que se descubrieron:

- 1 Firewall de Nueva Generación.
- 5 switches Cisco.
- 2 switches capa 3 Brocade.
- 2 controladoras virtuales (Aruba y Ruckus).

Ya con las direcciones IP de los dispositivos en nuestro poder, se procedió a realizar un análisis de vulnerabilidades y amenazas para los equipos encontrados con la aplicación OpenVAS. Dentro de los 10 dispositivos encontrados que presentaban riesgos altos, medios y bajos como se puede observar en la figura 1. Además, en la Figura 2 se puede

observar, de manera breve, el título de cada una de las vulnerabilidades encontradas.

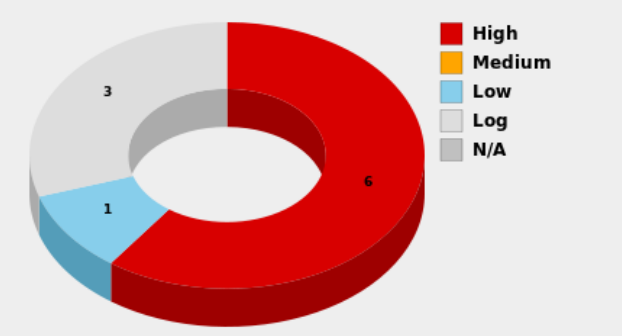

Fig. 1. Grafico de los riesgos de los dispositivos.

IV. Discusión

Tras el estudio, se encontró que el nivel actual de la seguridad (74.83) se encontraba dentro de los límites de lo aceptable como se puede observar en la figura 3, sin embargo, si se desea aumentar el nivel de seguridad en el entorno se debería hacer énfasis en el aumento de controles.

A manera de propuesta, se realizó un esquema que pudiera explicar al encargado de la red la manera de gestionar los riesgos y medir el nivel de seguridad de la red basados en el esquema de la figura 4.

La metodología OSSTMM ya ha propuesto un diagrama, sin embargo, a diferencia del propuesto en esta investigación, el modelo presentado en la metodología se presenta de manera genérica para la realización de auditorías en diferentes entornos como: inalámbrico, telecomunicaciones, físicos.

Algunas ventajas del esquema propuesto son las siguientes:

- Facilitación de análisis de riesgos en redes de datos.
- Terminología técnica específica para un administrador de red.

V. Conclusión

En base al estudio realizado se comprobó el nivel de la seguridad actual en la institución auditada.

Los objetivos propuestos que fueron cumplidos son los siguientes:
Esquematizar un esquema seguro para la capa de distribución para complementar el estudio previo “Esquema seguro para la red inalámbrica de la Universidad de Montemorelos.”, además se cumplió con los objetivos específicos como la realización pautas para la realización de medición de riesgos y una base de datos con la vulnerabilidades que encontradas.

Cumplido el objetivo principal, se comprobó la hipótesis que se planteó.

Por último se propone al administrador de la red de la institución auditada que evalúe los controles que afectan al nivel de la seguridad del entorno.

VI. Referencias

[1] G. R. Jidiga and P. Sammulal, “The need of awareness in cyber security with a case study,” in *2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT)*, pp. 1–7.
[2] 2008 DATA BREACH INVESTIGATIONS REPORT: Four Years of Forensic Research More than 500 cases,” 2008.
[3] F. Flores, R. Paredes, and F. Meza, “Procedures for mitigating Cybersecurity risk in a Chilean Government Ministry,” IEEE Latin Am. Trans., vol. 14, no. 6, pp. 2947–2950, 2016.
[4] K. Graves, CEH: Official certified ethical hacker review guide. Indianapolis Ind.: Wiley Pub, 2007.
[5] J. M. Ortega, Footprinting for security auditors. [Online] Available: https://fosdem.org/2017/schedule/event/footprinting/
[6] S. Özkan, Vulnerabilites by year. [Online] Available: http://www.cvedchietails.com/browse-by-date.php.
[7] P. Herzog. OSSTMM 3 The Open Source Security Testing Methodology Manual. Contemporary Security Testing and Analysis. Institute for Security and Open Methodologies, 2010

Vulnerability	Severity	QoD	Host	Location
HP Power Manager Management Web Server Login Remote Code Execution Vulnerability	10.0 (High)	98%	10.4.230.67	443/tcp
HP Power Manager Management Web Server Login Remote Code Execution Vulnerability	10.0 (High)	98%	10.4.230.67	80/tcp
Dropbear SSH Multiple Vulnerabilities	10.0 (High)	80%	172.16.4.1	22/tcp
Dropbear SSH Multiple Vulnerabilities	10.0 (High)	80%	172.16.4.254	22/tcp
HP Power Manager Management Web Server Login Remote Code Execution Vulnerability	10.0 (High)	98%	172.16.3.6	443/tcp
HP Power Manager Management Web Server Login Remote Code Execution Vulnerability	10.0 (High)	98%	172.16.3.111	443/tcp
LiteServe URL Decoding DoS	9.3 (High)	99%	172.16.3.4	443/tcp
Header overflow against HTTP proxy	7.5 (High)	99%	172.16.3.4	443/tcp
Header overflow against HTTP proxy	7.5 (High)	99%	172.16.3.111	80/tcp
CERN httpd CGI name heap overflow	7.5 (High)	99%	172.16.3.111	80/tcp
Format string on HTTP method name	6.9 (Medium)	99%	172.16.3.4	443/tcp
Format string on HTTP header name	6.9 (Medium)	99%	172.16.3.4	443/tcp
Format string on HTTP method name	6.9 (Medium)	99%	172.16.3.6	443/tcp
Format string on HTTP header name	6.9 (Medium)	99%	172.16.3.6	443/tcp
Format string on HTTP header name	6.9 (Medium)	99%	172.16.3.111	443/tcp
Format string on HTTP method name	6.9 (Medium)	99%	172.16.3.111	80/tcp
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	6.8 (Medium)	70%	172.16.4.254	9998/tcp
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	6.8 (Medium)	70%	172.16.4.254	443/tcp
Check for Anonymous FTP Login	6.4 (Medium)	80%	172.16.4.254	21/tcp
Dropbear SSH CRLF Injection Vulnerability	5.5 (Medium)	80%	172.16.4.1	22/tcp
Dropbear SSH CRLF Injection Vulnerability	5.5 (Medium)	80%	172.16.4.254	22/tcp
SSL/TLS: Certificate Expired	5.0 (Medium)	98%	172.16.3.111	443/tcp
HTTP negative Content-Length DoS	5.0 (Medium)	99%	172.16.3.6	80/tcp
Jigsaw webserver MS/DOS device DoS	5.0 (Medium)	99%	172.16.3.111	443/tcp
HTTP 1.1 header overflow	5.0 (Medium)	99%	172.16.3.6	443/tcp
Polycom ViaVideo denial of service	5.0 (Medium)	99%	172.16.3.6	443/tcp
BadBlue invalid GET DoS	5.0 (Medium)	99%	172.16.3.111	443/tcp
SSH Weak Encryption Algorithms Supported	4.3 (Medium)	95%	172.16.4.1	22/tcp
SSH Weak Encryption Algorithms Supported	4.3 (Medium)	95%	172.16.4.254	22/tcp
SSL/TLS: Report Weak Cipher Suites	4.3 (Medium)	98%	172.16.4.254	9998/tcp
SSL/TLS: Report Weak Cipher Suites	4.3 (Medium)	98%	172.16.4.254	443/tcp
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	4.0 (Medium)	80%	172.16.4.254	9998/tcp
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	4.0 (Medium)	80%	172.16.4.254	443/tcp
TCP timestamps	2.6 (Low)	80%	172.16.4.1	general/tcp
TCP timestamps	2.6 (Low)	80%	172.16.4.254	general/tcp
SSH Weak MAC Algorithms Supported	2.6 (Low)	95%	172.16.4.254	22/tcp
TCP timestamps	2.6 (Low)	80%	172.16.254.1	general/tcp

Fig. 2. Base de datos con las vulnerabilidades encontradas

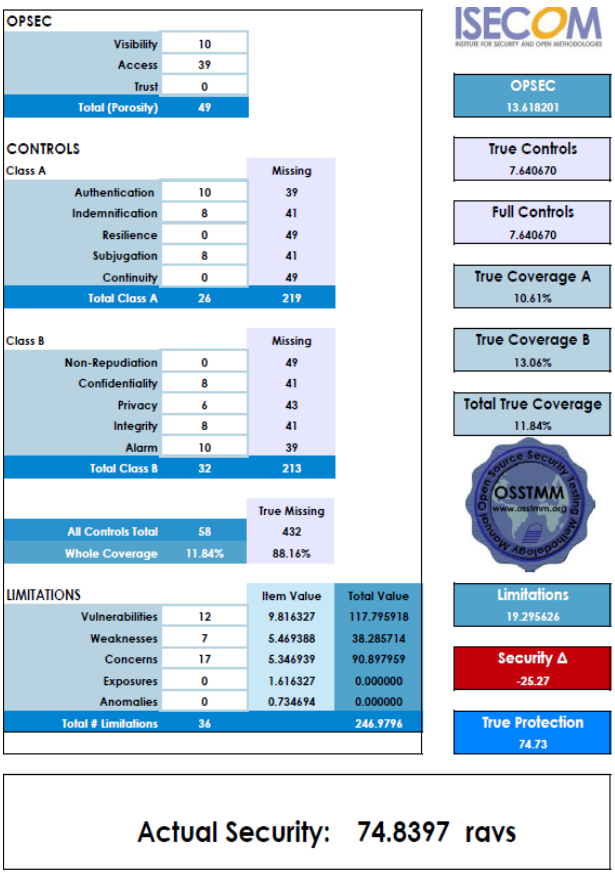

Fig. 3. Cálculo del nivel seguridad de la red auditada.

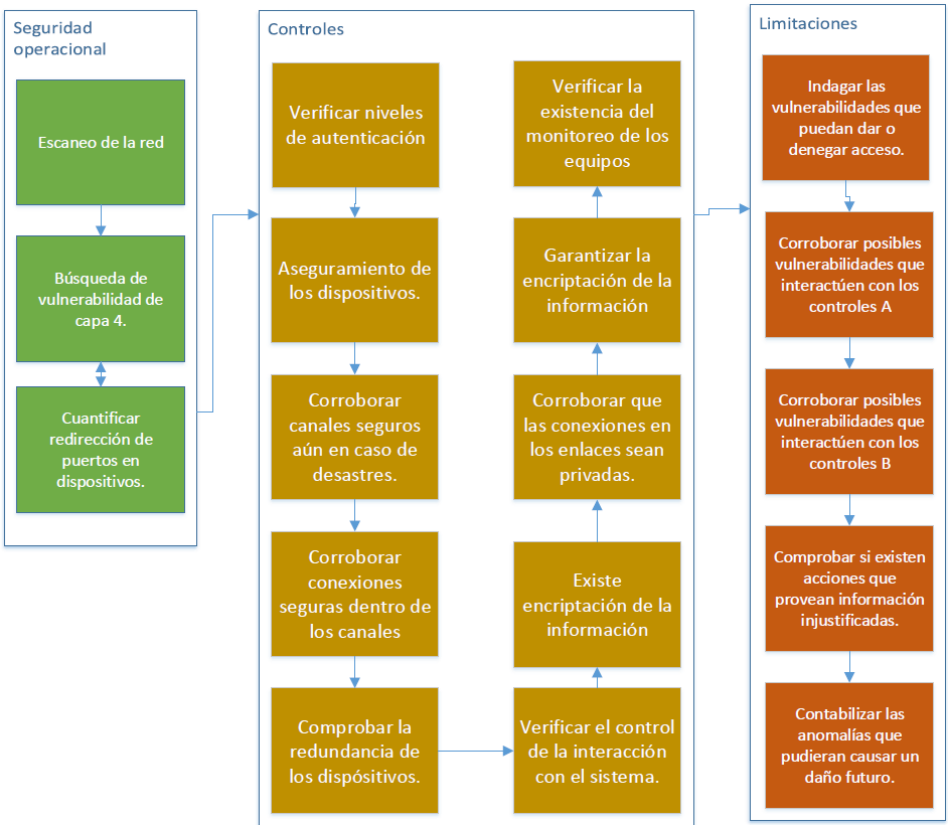

Fig. 4. Esquema de evaluación del riesgo en una red de datos.