Metodología para la Ejecución de Evaluación de Ciber-Vulnerabilidades en los Sistemas ICS- SCADA de los Agentes del Sistema Interconectado Nacional

Medina Becerra Fabián Andrés[1]
Tirano Vargas Jesús Alberto[2]
Vargas Barrera Diego Alexander[3]

Resumen—Se realiza un análisis comparativo de las metodologías NIST SP 800-115 y OSSTMM, buscando establecer una metodología adecuada para la ejecución de evaluación de ciber vulnerabilidades en un sistema ICS-SCADA de una infraestructura critica. Se eligió la metodología OSSTMM por cumplir criterios que ofrecen una evaluación completa de ciber vulnerabilidades y gracias a su métrica permite definir en qué nivel seguridad tiene. Al aplicarla se le da cumplimento a la normatividad establecida por el gobierno nacional. Ante la protección de los ciber-activos críticos de los agentes del sistema interconectado nacional. Para llegar al resultado se definieron los criterios bajo los cuales se evaluarían las dos metodologías, luego se analizaron las fases de ejecución de cada una para así compararlas con base los criterios establecidos anteriormente.

Palabras clave— Ciber-vulnerabilidades, infraestructura critica,
OSSTMM, NIST, ICS-SCADA.

Abstract— A comparative analysis of the NIST SP 800-115 and OSSTMM methodologies is made, in the sense of a critical vulnerability in an ICS-SCADA system of a critical infrastructure. The OSSTMM methodology was chosen to comply with a complete vulnerability assessment and, thanks to its metric, it allows defining the level of security it has. When applied in compliance with the regulations established by the national government. The protection of the active agents of the agents of the national interco nnected system. To obtain the result, the criteria were defined under which the methodologies were evaluated, then the phases of the execution of each of them were analyzed.

Keywords— Cyber-vulnerabilities, critical infrastructure,
OSSTMM, NIST, ICS-SCADA.

[1] Especialización en Telecomunicaciones. Universidad Pedagógica y Tecnológica de Colombia, Calle 4 Sur No. 15-134 Sogamoso, Colombia. fabian.medina@uptc.edu.co
[2] Especialización en Telecomunicaciones. Universidad Pedagógica y Tecnológica de Colombia, Calle 4 Sur No. 15-134 Sogamoso, Colombia. jesus.tirano@uptc.edu.co
[3] Especialización en Telecomunicaciones. Universidad Pedagógica y Tecnológica de Colombia, Calle 4 Sur No. 15-134 Sogamoso, Colombia. diegoalexander.vargas@uptc.edu.co

I. INTRODUCCION

Las infraestructuras criticas como: instalaciones nucleares, instalaciones químicas, centrales eléctricas, petroleras, fábricas de alimentos y servicios masivos de transporte, dentro de su planta física cuentan con "sistemas y activos físicos tan vitales que la incapacidad o destrucción de tales sistemas y activos tendrían un impacto debilitante sobre la seguridad, la seguridad económica nacional, salud pública o cualquier combinación de estos asuntos"[1]. Dentro los Sistemas de Control Industrial (ICS) de las infraestructuras críticas se encuentran las redes SCADA, las cuales requieren protección contra ciber-amenazas, debido a que la conectividad a internet (TCP/IP), ha llevado a una mayor exposición a ataques de explotación de sus vulnerabilidades y manipulación maliciosa de los protocolos de comunicación industrial, tales como: CIP, MODBUS, DNP3, Profibus, Profinet, Powerlink Ethernet, OPC y EtherCAT, entre otras razones, porque algunos de estos no fueron diseñados para ser utilizados mediante internet [2], al compartir este servicio con la red corporativa, la red SCADA queda expuesta a la explotación de sus vulnerabilidades por esta vía. En la figura 1 se pueden observar los ataques más relevantes a los ICS a nivel mundial.

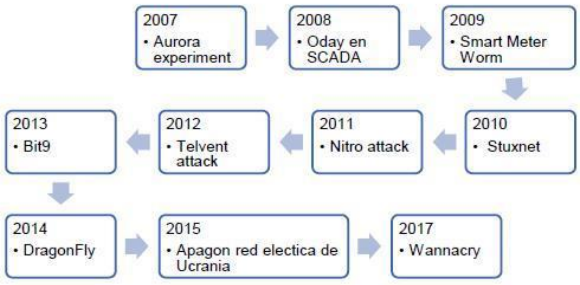

Fig. 1. Ataques a sistemas ICS en los últimos años.

Según el ICS-CERT una vulnerabilidad es "una característica física o atributo operacional que hace a un sistema abierto a una explotación o susceptible a un peligro" [1]. Para identificar las vulnerabilidades presentes en un sistema, se pueden hacer pruebas pasivas, estas tienen que ver con características propias del sistema como, por ejemplo, versión de su sistema operativo y software. También están las pruebas activas, que buscan identificar vulnerabilidades relacionadas con exploración de puertos, negación de servicio, desbordamiento de memoria, comprobación de inyecciones SQL y HTML. En el estudio realizado en la universidad de Arizona[2], aplicaron técnicas pasivas y activas, para este fin utilizaron la base de datos National Vulnerability Database (NVD) y el buscador de dispositivos conectados a internet Shodan, y así, identificar de forma pasiva las vulnerabilidades de dispositivos de las principales marcas utilizadas en las redes SCADA. Para las pruebas activas, mediante el software NESSUS implementaron filtros para escanear una muestra de dispositivos, sin ocasionar daños a los sistemas durante la identificación de sus vulnerabilidades. Otra

técnica desarrollada es CySeMol que es un lenguaje de modelado de seguridad cibernética a partir de la arquitectura de red específica. Esta herramienta utiliza métodos racionales probabilísticos (PRM), para encontrar rutas de posibles ataques, tiene problemas de escalabilidad y es recomendado utilizarlo en las organizaciones que no cuentan con un experto en seguridad [3]. En la universidad Khalifa, de los Emiratos Árabes Unidos se realizó un estudio para evaluar la seguridad del protocolo Modbus, generando tráfico malicioso sobre el protocolo mediante Scapy y monitoreando la susceptibilidad de Modbus con los software Snort y Wireshark[4]. Aunque existen diferentes herramientas para la identificación de ciber- vulnerabilidades, es necesario aplicar una metodología que proporcione directrices a las organizaciones para la planificación y realización de pruebas de seguridad de la información. Institutos dedicados a temas relacionados con ciber-amenazas han desarrollado algunas metodologías como por ejemplo: NIST SP800-115, OWASP, OSSTMM, PTES, EC-Council y la Guía Metodológica de Pruebas de Efectividad diseñada por el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia[5].

La investigación busca identificar los criterios, bajo los cuales se selecciona una metodología para aplicar evaluaciones de vulnerabilidades en una infraestructura critica, según el ingeniero Roberto López Santoyo de la de universidad autónoma de Madrid[6], al aplicar una metodología se debe garantizar un orden adecuado para las pruebas, cubrir toda la variedad de pruebas que se deben realizar, facilitar la tarea del analista y la presentación de los resultados se expone al cliente de una forma más organizada y ordenada. Después de las consideraciones anteriores, se analizaron ventajas y desventajas de dos metodologías de auditoria de seguridad más reconocidas, por ofrecer un amplio enfoque en seguridad informática, para este fin, se consideraron las metodologías NIST SP 800-115 y OSSTMM, y bajo los criterios definidos, se eligió la metodología OSSTMM, para ser aplicada en los sistemas ICS-SCADA de los Agentes del Sistema Interconectado Nacional.

II. MARCO NORMATIVO

El gobierno colombiano a través del documento CONPES 3701[7], [8], establece lineamientos de política para ciber- seguridad y ciber-defensa, buscando que las entidades públicas y privadas generen los mecanismos que les permitan garantizar su seguridad, teniendo en cuenta normas técnicas y estándares nacionales e internacionales sobre la protección de infraestructuras críticas como por ejemplo, la norma publicada por la NERC (North American Electric Relibility Corporation) y compuesta por los estándares de Protección de Infraestructura Critica (CIP) para tecnologías de activos críticos [8], [9]. Con respecto a esto, el Consejo Nacional de Operación mediante el acuerdo 788 [10], aprueba la Guía de Ciber-seguridad en donde de manera específica invita a los miembros del Sistema Interconectado Nacional a identificar sus activos críticos, ciber-activos críticos, riesgos, vulnerabilidades y nivel de gestión de su ciber-seguridad.

III. CRITERIOS

Para ejecutar una evaluación de ciber-vulnerabilidades en los sistemas ICS-SCADA de una infraestructura critica, se tienen en cuenta criterios que debe abordar la metodología seleccionada para garantizar la fiabilidad, disponibilidad e integridad de dicho sistema, algunos de estos tienen relación con: el ámbito digital, ámbito físico, ámbito social, métricas, e informes. En el ámbito digital se considera, que debe de haber medios para rastrear o monitorizar sensores, antivirus gestión de actualizaciones, gestión de políticas de software y las trazas del operador en la consola del sistema en tiempo real, por ejemplo, al entrar en una aplicación o autenticarse en el sistema operativo, en el ámbito físico se encuentra la protección del hardware y los soportes de datos e instalaciones. En el ámbito social se halla la ingeniería social, así lo indica AEI Seguridad [11]. Los resultados de cada evaluación de ciber-vulnerabilidades deben ser expresados en un formato de desempeño contra un conjunto de métricas predefinidas apropiadas que muestren el nivel de seguridad conseguido y las pautas a seguir dadas se deben incluir en el informe.

IV. METODOLOGIAS ANALIZADAS

A. NIST SP800-115

La metodología NIST SP800-115[12] tiene como finalidad proporcionar recomendaciones para realizar de forma adecuada un análisis de vulnerabilidades a un sistema ICS y consta de cuatro etapas o fases; fase de planificación, fase de descubrimiento, fase de ataque y fase de reporte las cuales siguen un ciclo, como se muestra en la figura 2. En La fase de planificación se establecen los objetivos y reglamentación para realizar la prueba de vulnerabilidad, allí, se especifican detalles para asegurar que todas la partes sean conscientes de los que está autorizado o no, bajo políticas de la guía, y que se espera como resultado de la prueba, es la fase más importante porque encamina el proceso hacia un resultado satisfactorio, la siguiente fase, “fase de descubrimiento” se divide a su vez en dos partes; la cuales constan de recopilación de la información, que puede ser obtenida mediante la dirección IP de la organización, realizar sniffing a la red, o, escaneos pasivos y activos. La “fase de ataque” consiste en explotar las vulnerabilidades encontradas, conseguir el acceso a la red y a los sistemas del ICS, para luego, al finalizar la fase, dejar los sistemas funcionales como estaban antes de la prueba, en dado caso que la prueba ocasione algún fallo al sistema. Por último, la fase de reporte, es la entrega del informe de los resultados obtenidos de la evaluación realizada.

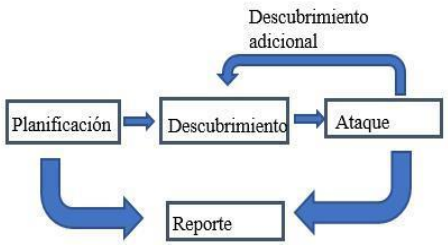

Fig. 2. fases de ejecución metodología NIST 800-115.

B. OSSTMM

Esta metodología fue desarrollada por el Instituto de Seguridad y Metodologías Abiertas (ISECOM). ISECOM basa su investigación en seguridad informática. Su principal metodología es el Manual de la Metodología Abierta de Testeo de Seguridad (OSSTMM) [13], esta metodología tiene una visión amplia de la seguridad y la evalúa desde diferentes puntos de vista o clases como: Seguridad Física (PHISSEC), Seguridad de Espectro (SPECSEC) y Seguridad de Comunicaciones (COMSEC), estas a su vez se dividen en canales como se puede ver en la tabla 1. Adicionalmente para evaluar la seguridad divide su metodología en cuatro fases: inducción, interacción, investigación e intervención

En referencia a la clasificación anterior se aplican diecisiete módulos con el fin de definir tareas a realizar en cada canal en cuanto a operaciones, controles y limitaciones, el mapeo de estos se puede observar en la tabla 2.

Tabla 1: Clases y canales en un ámbito.

Clases	**Canales**
Seguridad Física (PHISSEC)	Humano
	Físico
Seguridad de Espectro (SPECSEC)	Comunicaciones Inalámbricas
Seguridad de Comunicaciones (COMSEC)	Telecomunicaciones
	Redes de Datos

Tabla 2: Mapeo de los controles operaciones y limitaciones.

Categoría		**Seguridad operativa**	**Limitaciones**
Operaciones		Visibilidad	Exposición
		Acceso	Vulnerabilidad
		Confianza	
Controles	Clase A - Interactivo	Autenticación	Debilidad
		Indemnización	
		Resistencia	
		Sometimiento	
		Continuidad	
	Clase B- Proceso	No repudio	Preocupación
		Confidencialidad	
		Privacidad	
		Integridad	
		Alarma	

V. CATERGORIZACION Y ELECCION DE LA METODOLOGIA.

La categorización se realizó mediante la comparación de las dos metodologías bajo los criterios definidos previamente. En la tabla 3, se presenta el resultado obtenido, y como se puede observar, OSSTMM cumple con los criterios requeridos para la aplicación de una evaluación de ciber-vulnerabilidades en un sistema ICS-SCADA. La principal ventaja de frente a NIST SP 800-115 es que ofrece métricas que son indispensables para la gestión de la seguridad de la información identificando si la organización tiene un nivel de seguridad aceptable o si está protegido de forma adecuada, y a diferencia de la otra metodología examinada, esta incluye el ámbito físico y humano [14].

Tabla 3. Comparación entre OSSTMM y NIST SP 800-115

Metodología Criterio	OSSTMM	NIST SP 800-115
Ámbito Digital	●	●
Ámbito Físico	●	
Ámbito Social	●	●
Métricas	●	
Informes	●	●

VI. CONCLUSION

OSSTMM al enfocarse en evaluar de la seguridad en el espectro y comunicaciones, cubre los escenarios en los que se encuentran las ciber-vulnerabilidades. Además, opera dentro de la ley de la ubicación física de los ICS-SCADA, cumple las normas y leyes que regulan la ubicación de la evaluación. Por estas razones OSSTMM es metodología que se debe seguir para la ejecución de evaluación de ciber- vulnerabilidades. En los sistemas ICS-SCADA de los agentes del sistema interconectado nacional.

REFERENCIAS

[1] C. Management, C. I. Owners, C. I. Partner, and C. Incident, “Common Cyber Security Language,” Estados Unidos, 2013.

[2] S. Samtani, S. Yu, H. Zhu, M. Patton, and H. Chen, “Identifying SCADA Vulnerabilities Using Passive and Active Vulnerability Assessment Techniques,” pp. 25–30, 2016.

[3] T. Sommestad, M. Ekstedt, and H. Holm, “The Cyber Security Modeling Language : A Tool for Assessing the Vulnerability of Enterprise System Architectures,” vol. 7, no. 3, pp. 363–373, 2013.

[4] R. Al-dalky, O. Abduljaleel, K. Salah, H. Otrok, and M. Al-qutayri, "A Modbus Traffic Generator for Evaluating the Security of SCADA Systems," pp. 809– 814, 2014.

[5] Roberto Lopez Santoyo, "Propuesta de implementación de una metodología de auditoría de seguridad informática," Universidad Autonoma de Madrid, 2015.

[6] MINTIC, *Guía Metodológica de Pruebas de Efectividad*, no. 1. Colombia, 2016.

[7] M. D. R. Exteriores and M. D. D. Nacional, *Conpes*. Colombia, 2011.

[8] W. Ñustes, and S. Rivera, "Colombia territorio de inversión en fuentes no convencionales de energía renovable para la generación eléctrica*,"Revista Ingeniería, Investigación y Desarrollo*, vol 17 no. 1 pp. 37-48, Enero 2017.

DOI: https://doi.org/10.19053/1900771X.v17.n1.2017.5954

[9] A. Introduction, *CIP-010-2 — Cyber Security — Configuration Change Management and Vulnerability Assessments*. EEUU, 2106.

[10] Consejo Nacional de Operacion CNO, "acuerdo788," Bogota D.C, 05-Sep-2015.

[11] AEI Seguridad, *Protección de infraestructuras críticas guía para la elaboración de planes de seguridad del...*, no. June. 2012, 2017.

[12] K. Scarfone and A. Orebaugh, *Technical Guide to Information Security Testing and Assessment Recommendations of the National Institute of Standards and Technology*. EEUU, 2008.

[13] ISECOM, *The Open Source Security Testing Methodology Manual*. EEUU, 2010.

[14] G. Fonseca, E. Avendaño, and A. Araque, "Supervisión de ph redox y turbidez en una plata de tratamiento de agua utilizando wsn (Wireless sensor networks) con tecnología zigbee," Revista Ingeniería, Investigación y Desarrollo, vol. 14 no. 1, pp. 17-21, Enero 2014. DOI:https://doi.org/10.19053/1900771X.4046