Herramientas DNP3 pentesting para redes de infraestructura critica

M. Sánchez
Escuela Superior de Guerra, Bogotá
sanchezm@esdegue.mil.co

M. Santander
Escuela Superior de Guerra, Bogotá
manuel.santander@esdegue.edu.co

(Tipo de Artículo: Investigación Científica y Tecnológica. Recibido el 22/06/2016. Aprobado el 24/06/2016)

Resumen. Este artículo presenta un conjunto de herramientas de software que son capaces de realizar actividades Pentesting en la infraestructura crítica del sector eléctrico mediante el protocolo DNP3. Las herramientas son capaces de comprobar la capacidad de los controles de seguridad cibernética en el interior del perímetro de la red para evitar cualquier comando sensible falsificado pueda llegar a cualquier controlador de subestación

Palabras clave. Ciberseguridad, DNP3, pentesting, comunicación industrial, herramientas de software.

DNP3 pentesting tools for critical infrastructure networks

Abstract. *This paper presents a set of free software tools that are able to perform pentesting activities in the electrical sector critical infrastructure using DNP3 protocol. The tools are able to check the ability of the cybersecurity controls inside the network perimeter to avoid any spoofed sensitive command to arrive at any substation controller.*

Keywords. *Cybersecurity, DNP3, pentesting, industrial communications, software tools.*

1. Introducción.

La infraestructura crítica se ha convertido en un elemento relevante en la protección de los países, pues la afectación de cualquiera de sus componentes puede llevar a situaciones de afectación a la sociedad, la economía y el funcionamiento en general de un país. Teniendo en cuenta que la gran mayoría de estos sistemas están haciendo una transición al mundo IP, el nivel de riesgo está en aumento al tener estos sistemas interconectados a las redes corporativas de los negocios e incluso internet. Este nivel se incrementa por problemas como los siguientes [1]:

- Vida útil de la infraestructura: Si bien en el mundo de las tecnologías de información (TI) es normal que un sistema operativo o un equipo de comunicaciones es renovado cuando el fabricante publica un aviso de fin de vida, en el mundo de las tecnologías de operación (TO) esto no es una realidad, pues los dispositivos de control y el software asociado que operan un proceso industrial tienen tiempos de vida útil superiores y los fabricantes otorgan tiempos de soporte hasta de 15 años.
- Controles de seguridad: Las variables de operación de los sistemas industriales están asociadas a la disponibilidad y fiabilidad del servicio, en donde la transmisión en tiempo real es fundamental y no es tolerable cualquier posibilidad de lentitud en el procesamiento de información o las comunicaciones de los distintos componentes. Por lo anterior, soluciones convencionales de seguridad de la información como antimalware de endpoint y Host IPS están descartadas, debido al consumo de procesador y retardo en las comunicaciones que ocasionan respectivamente en los componentes de la infraestructura de gestión del proceso industrial.
- Vulnerabilidades en seguridad: Las soluciones que involucran infraestructuras críticas vienen aprobadas por los fabricantes con versiones y configuraciones específicas para cada uno de sus componentes. Para que el fabricante pueda aprobar algún tipo de configuración adicional en cualquiera de sus componentes que involucre componentes de seguridad tales como parches a software de sistema operativo o aplicaciones y configuraciones de seguridad de cualquiera de sus componentes, se hace necesario que el fabricante efectúe la realización de pruebas exhaustivas que permitan asegurar el desempeño del sistema en las variables críticas para el funcionamiento adecuado del proceso industrial. Por lo anterior, se ha constituido como una práctica difundida conservar las configuraciones iniciales realizadas por el fabricante, conservando con esto todas las posibles vulnerabilidades de seguridad existentes en el software base y las aplicaciones del sistema.
- Vulnerabilidades en los protocolos: Los distintos protocolos especializados para control industrial fueron diseñados para ser simples y muy rápidos. No fueron tenidos en cuenta consideraciones previas de seguridad, lo cual los hace vulnerables a ataques de suplantación y replay.

¿Bajo qué modelo es posible asegurar la infraestructura crítica? La Purdue Enterprise Reference Architecture (PERA) [2] es el modelo más difundido

para el aseguramiento en redes basadas en el proceso industrial, el cual se basa en los siguientes principios (Figura 1):

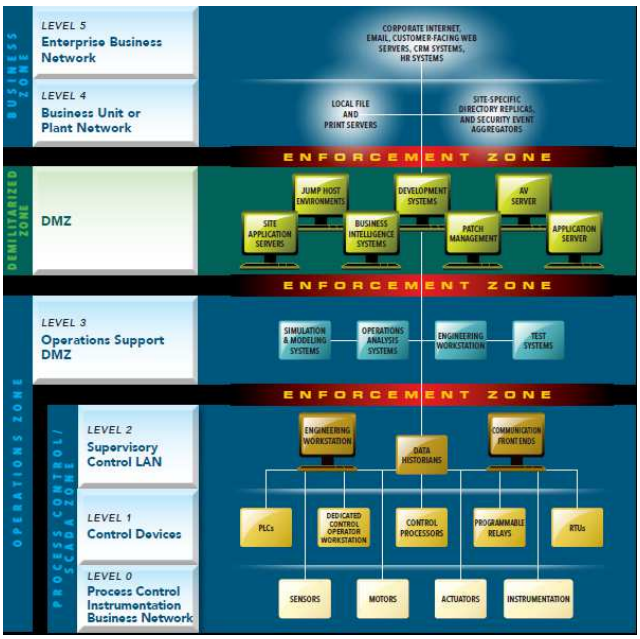

Figura 1. Diagrama explicativo modelo PERA [2]

– Delimitación de zonas: Se establece la creación de las siguientes zonas:

  Zona de negocio: Compuesta por los niveles 5 (red corporativa empresarial), la cual contiene todos los sistemas utilizados en el mundo de TI y el nivel 4 (unidad de negocio y red de la planta), el cual contiene todos los equipos de la planta a los que se les permite el uso de cualquiera de los componentes de la red de TI.

  Zona desmilitarizada: Compuesta por todos aquellos equipos que permiten el intercambio de información entre la zona de negocio y la zona de operaciones.

  Zona de operaciones: Compuesta por los niveles 3 (soporte de operaciones), 2 (LAN de supervisión y control), 1 (Dispositivos de control) y 0 (red de bus para la instrumentación de control de procesos).

– Establecimiento de zonas de control: El modelo establece la creación de zonas de control para el paso de tráfico entre la zona de negocios, zona desmilitarizada, y al interior de la zona de operaciones entre los niveles 3 y 2, 1 y 0, el cual deberá regular las comunicaciones permitidas entre los distintos dispositivos que conforman la infraestructura crítica.

¿Cuál es el esquema prototipo de un sistema de infraestructura crítica para distribución de energía? [1].

En los esquemas descritos en las Figuras 2 y 3 no se describen las zonas de negocio y desmilitarizadas por motivos de simplicidad. Para la zona de operación, se hace necesario la existencia de dispositivos de seguridad perimetral que controlen el flujo del tráfico de la red de los centros de control con las redes de datos de las distintas subestaciones.

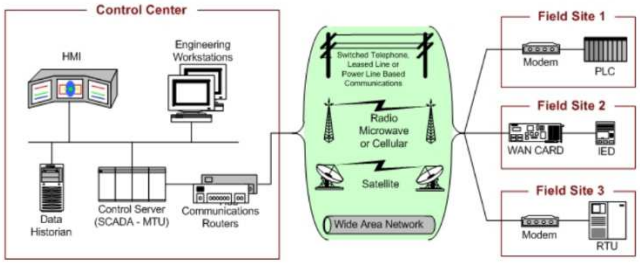

Figura 2. Modelo general de sistemas SCADA [1].

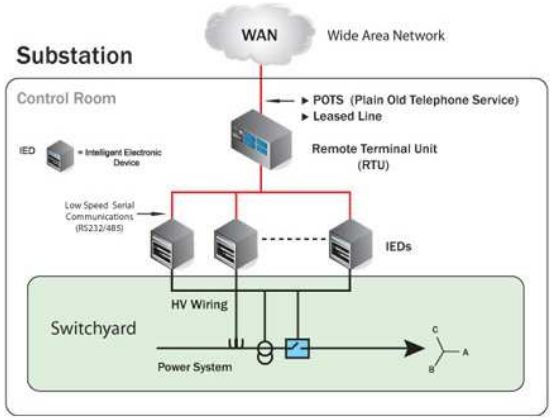

Figura 3. Modelo general de subestación con RTU [1].

La práctica del pentesting es universalmente aceptada como ejercicio de auditoría para determinar si los controles existentes en la infraestructura cumplen con criterios de seguridad específicos. Teniendo en cuenta que a la fecha no existen herramientas especializadas que permitan comprobar si las vulnerabilidades de los protocolos industriales se encuentran minimizadas en una instalación específica, este trabajo se enfoca en mostrar un conjunto de herramientas que puede ser utilizado en la verificación de la adecuada configuración de los dispositivos de seguridad en la minimización de vulnerabilidades del protocolo DNP3.

La organización del trabajo es la siguiente: en la sección II se ilustra la motivación para la creación de las herramientas de network protocol exploitation para DNP3. En la sección III se ilustra las generalidades del protocolo DNP3. La sección IV muestra los riesgos de ciberseguridad del protocolo DNP3 para una subestación de energía. La sección V ilustra las herramientas construidas que aprovechan los riesgos de ciberseguridad descritos y finalmente la sección VI ilustra las conclusiones.

2. Realización proceso pentesting en ambientes de control industrial

La realización de pentesting en un ambiente industrial no puede utilizar herramientas ni procedimientos como los realizados en cualquier ambiente de TI, pues labores tan simples como la utilización de una herramienta para escaneo de puertos puede causar una denegación de servicio [3]. Es sabido también que el ciclo de de vida para los parches en ambientes de TI no es el mismo que para sistemas SCADA[4], lo cual hace que la utilización de herramientas de explotación como metasploit tenga una rata de éxito considerablemente alta pero se quede corto con los resultados finales, pues este software permite el escalamiento de privilegios y toma de control de los respectivos HMI y dispositivos de control pero sin mayores posibilidades para influir en la ejecución del proceso industrial que gobierna el sistema. De igual manera, el funcionamiento del sistema SCADA puede verse afectado por el uso de estas herramientas [5]. Al realizar una revisión bibliográfica detallada en la Association for Computer Machinery (ACM), International Society of Automation (ISA), SANS, ENISA e Information Systems Audit and Control Association (ISACA), European Union Agency for Network and Information Security (ENISA) y el Electric Power Research Institute (EPRI), se encuentra que la única metodología oficial disponible para sistemas SCADA es la NESCOR Guide to Penetration Testing for Electric Utilities [6], la cual plantea los pasos descritos en la Figura 4:

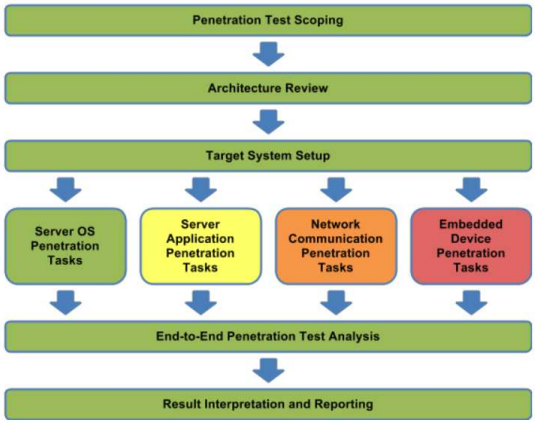

Figura 4. Modelo NESCOR para penetration testing [6].

- Penetration test scoping: Se debe definir el alcance para el penetration testing en la plataforma industrial, sea el conjunto completo de dispositivos que conforman el ambiente de control industrial o sólo una sección de los mismos.
- Architecture review: El Penetration testing debe iniciar con una revisión de arquitectura para ayudar al equipo de trabajo a tener un entendimiento profundo del sistema a revisar. Esto ayudará al equipo a comprender el funcionamiento del sistema objetivo, la postura de seguridad requerida desde la arquitectura y los riesgos de seguridad que una vulnerabilidad pudiera tener para la organización
- Target system setup: El penetration testing debe ser realizado en sistemas no productivos con dispositivos que sean de la misma referencia y el mismo esquema de conectividad que el productivo.
- Server OS Penetration Tasks: Las tareas que se realizan son análogas a las que se desarrollan en la metodología OSSTMM [6]:

  Information Gathering: En este paso se recopila información del servidor, su configuración, tráfico de red, puertos abiertos y demás información pertinente para el análisis que pudiera determinar algún tipo de vulnerabilidad.

  Vulnerability analysis: En este paso se hace una revisión detallada de todos los componentes detallados en el paso anterior y se utilizan herramientas que permitan determinar posibles vulnerabilidades existentes.

  Exploitation: Se realizan pruebas de concepto que permitan determinar riesgos en la infraestructura que pudieran ser claramente materializados por un atacante.

- Server Application Penetration Tasks: Para este caso, las tareas que se realizan son análogas a las que se desarrolla en la metodología OWASP Testing Guide[7]:

  Application Mapping: En este paso se recopila información del servidor web, la interfaz de la aplicación y demás información pertinente para el análisis que pudiera determinar algún tipo de vulnerabilidad.

  Application Discovery: Esta etapa se focaliza en la identificación de vulnerabilidades en las interfaces de usuario o en los servicios web.

  Application Exploitation: Esta etapa se focaliza en la explotación de las vulnerabilidades encontradas en el paso anterior.

- Network Communication Penetration tasks: No se evidenció semejanza de este apartado con otros tipos de metodología para la realización de penetration testing. Se realizan las siguientes tareas:

  RF Packet Analysis: Esta etapa pretende la realización de análisis a todas las comunicaciones RF de bajo nivel, tales como salto de frecuencia, modulación, multiplexación y codificación de datos en la capa física y de acceso a la red (PHY/MAC) del modelo OSI.

  Network Protocol Analysis: Esta etapa pretende la elaboración de ataques dirigidos a afectar el proceso

industrial a partir de fallas encontradas en los protocolos de red que lo controlan.

- Embedded Device Penetration Tasks: Al igual que el anterior ítem, no se evidenció semejanza de este apartado con otros tipos de metodología para la realización de penetration testing. Se realizan las siguientes tareas:

  Electronic Component Analysis: Esta etapa se focaliza en la identificación de vulnerabilidades en el diseño de los componentes electrónicos que conforman los dispositivos de automatización del proceso industrial.

  Field Technian Interface Analysis: Esta etapa se focaliza en la revisión de las vulnerabilidades presentes en las interfaces seriales de administración provistas para la administración de los dispositivos por parte de los técnicos en campo.

  Firmware Binary Analysis: Esta etapa se focaliza en la revisión de vulnerabilidades en el firmware binario de los dispositivos embebidos que son parte del proceso industrial.

- End-to-end Penetration Test Analysis: Esta etapa pretende la revisión de las comunicaciones de los distintos tipos de equipos que hacen parte del proceso industrial de principio a fin. No se evidenció semejanza de este apartado con otros tipos de metodología.
- Result Interpretation and Reporting: Esta etapa se focalice en el reporte de las vulnerabilidades que se encuentran, el procedimiento utilizado para materializarlas y su posible solución.

En las etapas de Server OS Penetration Tasks y Server Application Penetration Tasks existen herramientas ya probadas ampliamente en el mercado que cumplen adecuadamente el objetivo allí planteado, tales como Nexpose, metasploit, Vega Security Scanner, OpenVAS, entre otros, las cuales se encuentran disponibles en Internet. Sin embargo, no existen herramientas actualmente que permitan trabajar la etapa Network Communication Penetration Tasks, específicamente en lo correspondiente a Network Protocol Exploitation que permita tomar ventaja de las vulnerabilidades presentes en los protocolos SCADA y realizar acciones que puedan causar daños o acciones anormales en el proceso industrial, tales como habilitar conexiones eléctricas suspendidas, daños en los transformadores de las subestaciones de transmisión, interrupción de las líneas de tranmisión de energía, entre otros.

3. Generalidades del protocolo dnp3

El protocolo DNP3 fue construido para la transmisión eficiente de datos en tiempo real desde las estaciones de proceso hacia el centro de control y el envío de comandos desde el centro de control a cualquiera de las estaciones de campo que conforman el proceso industrial. Para efectos del sector eléctrico, el protocolo permite la lectura de dispositivos análogos y dispositivos digitales, tales como medidores y de envío de comandos a dispositivos digitales o análogos, tales como los interruptores, sincrofasores y transformadores. La descripción del protocolo DNP3 es la siguiente [8] (Figura 5 y 6):

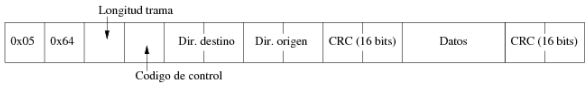

Figura 5. Descripción del frame para el protocolo DNP3 [8]

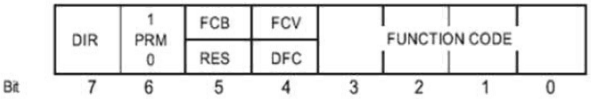

Figura 6. Descripción del código de control para el protocolo DNP3 [8]

- 2 bytes de encabezado, cuyo valor constante es 0x0564.
- 1 byte para el tamaño del paquete. Este valor no tiene en cuenta ni la cabecera, ni los CRC.
- 1 byte para el código de control, que permite fijar aspectos como los servicios del nivel de enlace, el sentido del flujo, entre otros.
- 2 bytes para la dirección de destino, codificada en little endian.
- 2 bytes para la dirección de origen, codificada en little endian.
- 2 bytes para el código de redundancia cíclica (CRC).

Las operaciones que el protocolo puede efectuar son las siguientes (Figura 7):

Requests (Hex)			
0	Confirm	11	Start application
1	Read	12	Stop application
2	Write	13	Save configuration
3	Select	14	Enable unsolicited
4	Operate	15	Disable unsolicited
5	Dir operate	16	Assign class
6	Dir operate – No Ack	17	Delay measurement
7	Freeze	18	Record current time
8	Freeze – No Ack	19	Open file
9	Freeze clear	1A	Close file
A	Freeze clear – No Ack	1B	Delete file
B	Freeze at time	1C	Get file information
C	Freeze at time – No Ack	1D	Authenticate file
D	Cold restart	1E	Abort file
E	Warm restart	1F	Activate config
F	Initialize data	20	Authentication request
10	Initialize application	21	Authentication request – No acknowledgment

Figura 7. Códigos de función para DNP3

Los siguientes son los objetos sobre los cuales se efectúan las operaciones[14]

- Objeto 1 - Digital Input: Este objeto hace referencia a las entradas digitales. Permite la lectura de las mismas, mediante el código de función read, o la asignación de clase mediante el código de función assign class.
- Objeto 2 - Digital Input Event: Este objeto permite referenciar los eventos de las entradas digitales.
- Objeto 12 - Digital Output: este objeto hace referencia a los controles digitales. Mediante los códigos de función de select, operate, select and operate y direct operate, se podrán realizar estas operaciones sobre los elementos especificados bajo este objeto.
- Objeto 20 - Counter: Mediante este objeto, el protocolo permite la lectura o manipulación (congelación, reseteo, etc.) de contadores.
- Objeto 22 - Counter events: Este objeto es utilizado para agrupar la información relativa a eventos generados por contadores (objeto 20).
- Objeto 30 - Analog Input: los valores analógicos se agrupan bajo este objeto.
- Objeto 32 - Analog Input Event: Este es el objeto utilizado para los eventos de las entradas analógicas del objeto 30.
- Objeto 41 - Analog Output: este es el objeto utilizado para ejecutar mandos analógicos o Set Points. Admite las mismas funciones para el objeto 12.
- Objeto 50 - Time and Date: Este objeto permite al HMI sincronizar la hora en la estación controlada.
- Objeto 60 - Class: Este objeto hace alusión a una serie de servicios del nivel de aplicación, el cual es específico del dispositivo que implementa el protocolo.

4. Riesgos de ciberseguridad para el protocolo DNP3

El riesgo de ciberseguridad de mayor impacto en la infraestructura crítica es la suplantación del HMI, con lo cual es posible ejecutar comandos a los distintos dispositivos DNP3 que hacen parte del proceso, lo cual podría desencadenar en interrupciones en la ejecución del mismo e incluso posibles desastres, tales como apagones masivos por accionar los interruptores, daño masivo en dispositivos electrónicos por aumento en los voltajes, explosión en los transformadores por corto circuito, entre otros. Este riesgo puede ser evidenciado en las actividades de Network Protocol Exploitation de la metodología NESCOR.

La suplantación del HMI debe ser minimizada en las zonas de control establecidas en el modelo PERA. Específicamente, debe monitorearse cualquier tránsito de comandos con códigos de función desde un lugar distinto al segmento de red donde se encuentran localizados los HMI. Los siguientes códigos de función establecidos en el protocolo DNP3 son los más riesgosos y pueden ser utilizados en ataques:

- Warm restart: Cuando este paquete es recibido por la estación remota y su remitente es reconocido como el HMI, el dispositivo realiza un reinicio parcial luego de completar la secuencia de comunicación. Si este paquete se recibe varias veces por segundo, el IED se experimenta una denegación de servicio y no será capaz de realizar acciones para el proceso industrial, enviar eventos al panel o recibir comandos desde el HMI.
- Cold restart: Cuando este paquete es recibido por la estación remota y su remitente es reconocido como el HMI, el dispositivo realiza un reinicio completo luego de completar la secuencia de comunicación. Al igual que el anterior, si este paquete se recibe varias veces por segundo, el IED se experimenta una denegación de servicio y no será capaz de realizar acciones para el proceso industrial, enviar eventos al panel o recibir comandos desde el HMI
- Write: Esta función permite ordenar escritura de datos en diversos objetos del dispositivo DNP3:

  Contadores: Permite cambiar los valores de los distintos contadores. Si el proceso se encuentra monitoreando una o más variables a través de un contador, el programa puede tomar decisiones a partir del mismo para la continuidad del proceso industrial, lo cual puede poner en riesgo la disponibilidad del mismo. Un ejemplo claro es un contador de kilovatios/hora transmitidos a través de la subestación, número de veces que la corriente ha sobrepasado un límite específico. Puede saberse el número de contadores existentes cuando se ejecuta el comando de read sobre todos los contadores.

  Fecha y hora: Permite cambiar el valor de la fecha y la hora así que las órdenes recibidas con fecha y hora específica no se ejecutarán y los registros serán colocados en otros lugares diferentes para que el operador no puede ver en tiempo real

- Select: Este código de función permite seleccionar un objeto Digital Output o Analog output y programar la operación a realizar. La operación se confirma con el código de función operate. Las posibles operaciones son las siguientes:

  Latch: Permite accionar un interruptor en un dispositivo físico. Las opciones son on y off

  Pulse: Permite accionar un pulso en un dispositivo análogo. Las opciones son on y off.

- Operate: Este código de función permite hacer efectivas las operaciones seleccionadas con el código de función Select. Deben seleccionarse las mismas operaciones.

– Direct Operate: Este código de función permite operar directamente un objeto Digital Output o Analog Output sin efectuar un código de función Select previo.

5. Herramientas para pentesting

Al no existir herramientas que permitan efectuar network protocol exploitation en DNP3, se hace importante contar con un conjunto de herramientas que permitan suplantar de manera efectiva los comandos enviados por la estación HMI administradora. Para los responsables de ciberseguridad de las plataformas de infraestructura crítica en DNP3, se hace importante que la ejecución de cualquiera de las herramientas descritas no produzca resultado alguno, lo cual indicará que la configuración de los dispositivos de seguridad perimetral se realizó adecuadamente.

Las pruebas descritas a continuación se realizaron bajo el siguiente diagrama de red (Figura 8):

Figura 8. Diagrama de red utilizado para las pruebas

Para efectos de las pruebas que se realizan a continuación, se procedió a codificar la IP de dicha estación a 192.168.0.105. Se desarrollaron las siguientes herramientas para verificar la posibilidad de materialización de los códigos de función riesgosos, lo cual permite ejecutar Network Protocol Exploitation establecido en la metodología NESCOR para sistemas SCADA utilizando el protocolo DNP3:

– dnp3restart: Esta herramienta permite la ejecución de las dos modalidades de reinicio para un dispositivo DNP3: warm y cold.
– dnp3read:Permite leer el estado de contadores y variables del dispositivo DNP3
– dnp3write: Esta herramienta permite la ejecución de escritura de valores en los contadores y el día y la hora de un dispositivo DNP3.
– dnp3operate: Esta herramienta permite realizar operaciones sobre cualquier objeto Digital Output o Analog Output, de acuerdo con lo descrito en la sección anterior para los códigos Select, Operate y Direct Operate.

La herramienta dnp3restart permite crear un ciclo infinito para el envío de los códigos de función Cold Restart o Warm Restart. Para ejecutar la herramienta, se utilizan los argumentos crestart (Cold Restart) o wrestart (Warm Restart). A continuación se procede a ejecutar un cold restart contra 192.168.0.111 (Figura 9):

```
MSANTAND@MSANTAND10 /tmp
$ ./dnp3restart 192.168.0.111 crestart
```

Figura 9. Ejecución herramienta dnp3restart para efectuar un Cold Restart

Esto ocasiona que el dispositivo DNP3 no acepte órdenes adicionales mientras la herramienta se encuentre activa, lo cual ocasiona una negación de servicio que puede implicar en la disrupción del proceso industrial

La herramienta dnp3read permite leer contadores y variables del dispositivo DNP3. A continuación se observa la salida de la herramienta al ejecutarla para indagar sobre los valores y el estado de los contadores del dispositivo 192.168.0.111 (Figura 10):

```
MSANTAND@MSANTAND10 /tmp
$ ./dnp3read 192.168.0.111 counters
Host 192.168.0.111 reports 5 counters.Values are:

Counter 0: Value: 1 Status: online
Counter 1: Value: 2 Status: online
Counter 2: Value: 3 Status: online
Counter 3: Value: 4 Status: online
Counter 4: Value: 5 Status: online
```

Figura 10. Resultado ejecución herramienta DNP3 para lectura de contadores

Esto permite al atacante revisar el estado de variables específicas en el proceso industrial controlado por el dispositivo DNP3.

En la ejecución de la herramienta dp3read se observó la existencia de 5 contadores, los cuales tienen el valor respectivo del 1 al 5. Los dispositivos DNP3 toman decisiones con base en los valores presentes en los contadores y proceden a ordenar acciones en los distintos equipos que controlan. Para cambiar el valor de los contadores en el dispositivo DNP3 se utiliza la herramienta dnp3write. En la siguiente figura es posible observar el estado inicial de los contadores del dispositivo DNP3 implementado por el simulador XSlave, el cual confirma la salida observada por la herramienta dnp3read (Figura 11):

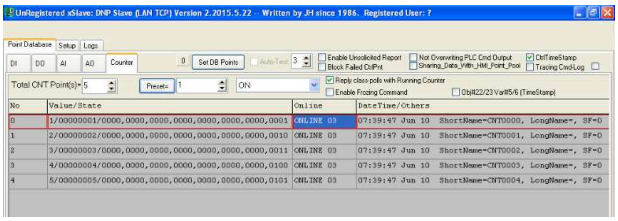

Figura 11. Estado inicial de contadores en el simulador DNP3

Se procede a cambiar el estado del contador 0 a offline (Figura 12):

```
MSANTAND@MSANTAND10 /tmp
$ ./dnp3write 192.168.0.111 counters 0 status offline
```

Figura 12. Ejecución herramienta dnp3write para cambio de estado de contadores

Al revisar resultado en el dispositivo DNP3, se obtiene el resultado esperado (Figura 13):

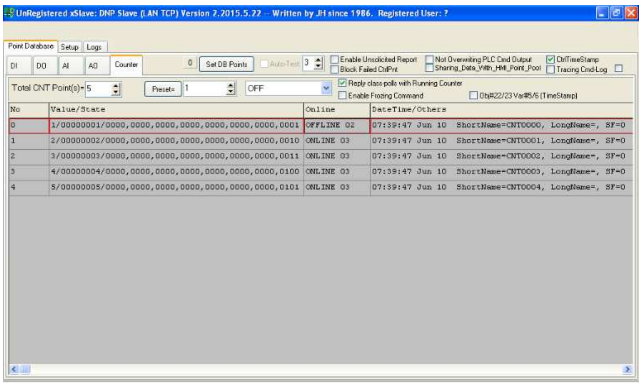

Figura 13. Resultado ejecución herramienta para cambio de estado del contador 0 en el simulador DNP3

Este cambio de contadores tiene efectos prácticos en el proceso industrial como abrir un circuito de una línea de transmisión de energía dejando sin servicio a sectores de la población o regular el nivel de voltaje que circula a través de un transformador. Si se cambia con gran rapidez, puede ocasionar daños en los interruptores, teleprotecciones y transformadores involucrados, lo cual llevaría a interrupciones del fluido eléctrico por meses o, en el peor de los casos, explosiones que ocasionen daños físicos al área circundante de la subestación.

Para mostrar el cambio del valor del contador, se procederá a reiniciar el estado de los contadores, de acuerdo con la figura 9. A continuación, se procede a continuación a utilizar la herramienta para cambiar el valor del contador 0 a 300 en el dispositivo DNP3 (Figura 14):

```
MSANTAND@MSANTAND10 /tmp
$ ./dnp3write 192.168.0.111 counters 0 300
```

Figura 14. Ejecución herramienta dnp3write para cambio de valor del contador 0 a 300

Al revisar resultado en el dispositivo DNP3, se obtiene el resultado esperado (Figura 15):

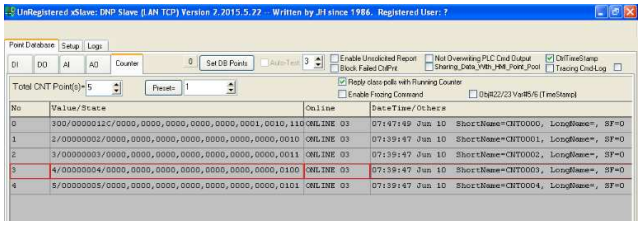

Figura 15. Resultado ejecución herramienta para cambio de valor de contador en el simulador DNP3

Otro uso posible de la herramienta es el cambio de la fecha y hora de un dispositivo DNP3. Antes de ejecutar la herramienta, tenemos la siguiente fecha y hora en el dispositivo DNP3 (Figura 16):

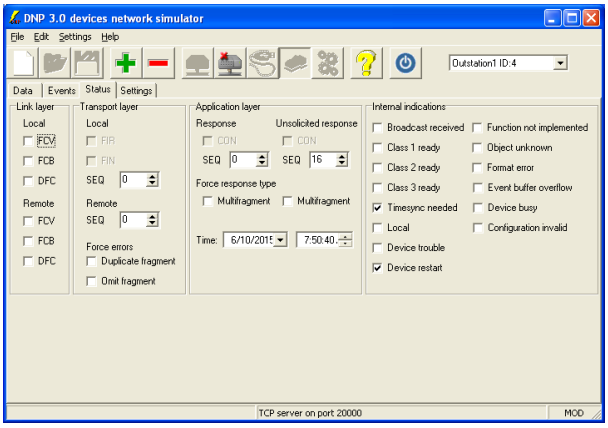

Figura 16. Hora inicial en el simulador DNP3

Se procede a utilizar la herramienta, dirigida a cambiar la hora del dispositivo DNP3 (Figura 17):

```
MSANTAND@MSANTAND10 /tmp
$ ./dnp3write 192.168.0.111 time 2015-06-15-11-56-16
```

Figura 17. Comando para cambiar la hora

Al revisar el simulador DNP3, se obtiene el resultado esperado (Figura 18):

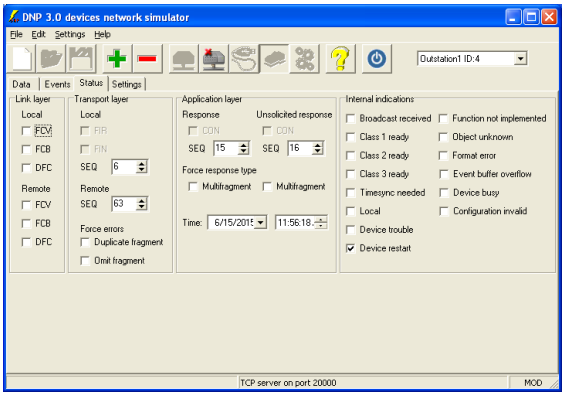

Figura 18. Resultado cambio de hora en el simulador DNP3

Antes de mostrar los resultados con la herramienta dno3operate, en la siguiente figura es posible observar el estado inicial de los Digital Output en el simulador DNP3 (Figura 19):

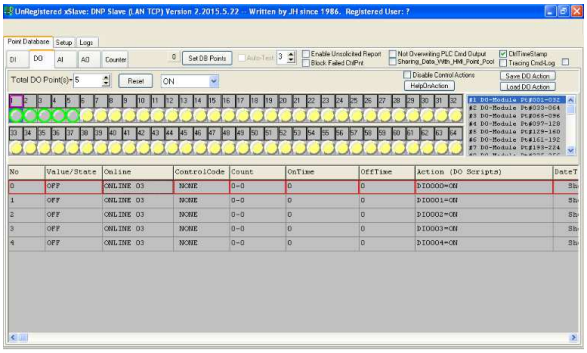

Figura 19. Estado inicial de los objetos Digital Output en el simulador DNP3

El simulador DNP3 soporta el código de función Direct Operate. Se procede a utilizar la herramienta dnp3operate para efectuar un latch on utilizando este código de función (Figura 20):

```
MSANTAND@MSANTAND10 /tmp
$ ./dnp3operate 192.168.0.111 doperate 0 latchon
```

Figura 20. Comando para operar Latch ON el DO 0

Al revisar el simulador DNP3, se obtiene el resultado esperado (Figura 21):

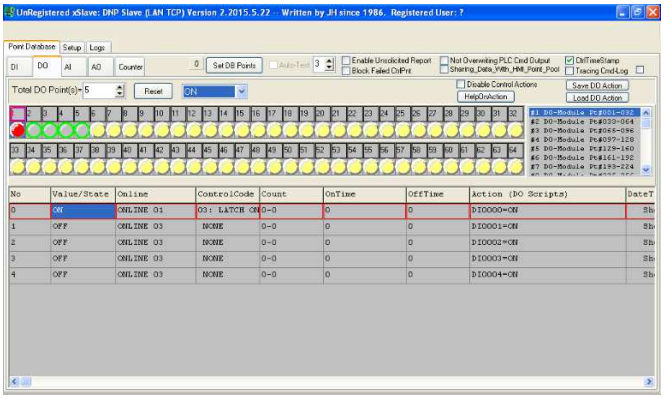

Figura 21. Resultado ejecución operación Latch ON en el DO 0 del simulador DNP3

Se procede a utilizar la herramienta dnp3operate para efectuar un latch off con el mismo código de función (Figura 22):

```
MSANTAND@MSANTAND10 /tmp
$ ./dnp3operate 192.168.0.111 doperate 0 latchoff
```

Figura 22. Comando para operar Latch OFF en DO 0

Al revisar el simulador DNP3, se obtiene el resultado esperado

6. Conclusiones

Este conjunto de herramientas permite que los responsables de ciberseguridad en infraestructura crítica bajo el protocolo DNP3 puedan realizar la verificación de las configuraciones de los dispositivos de seguridad perimetral (Firewalls, IPS, Application Control, entre otros) y líneas base de seguridad de la red de control, con el fin de minimizar la probabilidad de ocurrencia y factibilidad de la suplantación de la estación HMI administradora hacia los dispositivos localizados en el nivel de supervisión y control, lo cual permitirá constatar que los atacantes no podrán cambiar los contadores, DO, AO y fecha y hora de la infraestructura.

7. Referencias

[1] K. Stouffer, J. Falco and K. Scarfone, *Guide to Industrial Control Systems (ICS) Security*. Gaithersburg, MD: National Institute of Standards and Technology, pp 2, 19. 2011

[2] T. J. Williams, *The Purdue Enterprise Reference Architecture and Methodology (PERA)*. Information Infrastructure Systems for Manufacturing II. John Mills and Fumihiko Kimura, eds. 1998

[3] G. Weidman, *Penetration Testing: a Hands-On Introduction to Hacking*, No Starch Press, pp131, 2014.

[4] A. Pauna, K. Moulinos, *Window of exposure … a real problem for SCADA Systems?*. European Union Agency for Network and Information Security, pp 1. 2013,

[5] J. Searle, *NESCOR Guide to Penetration Testing for Electric Utilities*, National Electric Sector Cybersecurity Organization Resource, pp 8, 51

[6] M. Barceló, P. Herzog, *The Open Source Security Testing Methology Manual*, ISECOM, pp 35, 47. 2002

[7] M. Meucci, A. Muller, *OWASP Testing Guide V. 4.0*, Open Web Application Security Project, pp 30, 36.

[8] D. Reynders, S. Mackay, E. Wright, *Practical Industrial Data Communications*, Newnes, pp 149-181, 2005