Proyecto de la asignatura

Detección de intrusiones en redes de control

1. Objetivos

El proyecto propuesto se orienta a aplicar e integrar, con un cierto grado de autonomía, los conocimientos adquiridos para la resolución de un problema de importancia en el ámbito de los sistemas de control.

Dicho problema es la **configuración y prueba de un sistema de detección de intrusos con reglas específicas** para sistemas de control y del sistema asociado para la **monitorización de los eventos** que genera.

Se propone la realización de este proyecto de forma individual o en un grupo pequeño (de dos personas).

Para ello, en primer lugar, será necesario seleccionar un sistema de detección de intrusiones para el que existan reglas o filtros específicos de protocolos de sistemas de control, propios o de terceros. Las principales alternativas en este caso son Snort, Suricata y Zeek.

El sistema IDS vigilará tráfico representativo de la comunicación entre al menos dos elementos del sistema de control, entre los que podrían encontrarse la estación de ingeniería encargada de configurar/programar los elementos de control, un PLC o una plataforma SCADA. En la medida de lo posible, sería conveniente no contar únicamente con tráfico que sea etiquetable como normal.

Se da libertad a los estudiantes para definir dichos elementos y sus características (como los protocolos que se utilizan). También para decidir cómo se emulan dichos elementos, para lo cual se podrían utilizar:

- aplicaciones de programación de autómatas, SoftPLC y SCADA/HMI públicamente accesibles, como las que se verán a lo largo de la asignatura
- repeticiones o variaciones de capturas de tráfico previamente obtenidas de un sistema real, de las cuales existen también ejemplos públicamente accesibles

Finalmente, se configurará adecuadamente una plataforma SIEM que permita visualizar los eventos generados por el IDS.

Los estudiantes deberán realizar una memoria explicativa del trabajo realizado, explicando la estructura propuesta, los detalles de su configuración e implementación y los resultados obtenidos como respuesta al tráfico generado por los elementos simulados de la red de automatización. Dicho trabajo deberá ser también presentado en una sesión al final de la asignatura.

En los siguientes apartados se explican en mayor detalle tanto las herramientas potencialmente útiles para el desarrollo del proyecto como los resultados esperados del mismo.

No obstante, no se debe entender este proyecto como una tarea independiente al resto de contenidos prácticos, ya que a lo largo de la asignatura se verán aspectos relativos a la generación y análisis de tráfico de red de control que resultarán de utilidad para la resolución de la misma. Asimismo, se planteará una sesión intermedia centrada este mismo problema, que puede ser útil para la elaboración del trabajo.

2. Herramientas

Las tres opciones más conocidas en el ámbito de los sistemas de detección de intrusos (IDS) y monitorización de la seguridad de la red (NSM) son las plataformas Snort, Suricata y Zeek. Aunque con orientaciones diferentes, que las hacen apropiadas para escenarios diferentes y conllevan diferentes grados de dificultad en su configuración, todas ellas contienen al menos unas pocas reglas o plug-ins relativos a protocolos del ámbito de la automatización como Modbus TCP, Ethernet/IP, DNP3, etc. Además de las reglas disponibles por defecto, a menudo se pueden encontrar otras desarrolladas por terceros que cubren protocolos o condiciones adicionales. A continuación, se indican estas herramientas y las reglas disponibles:

- Snort: https://www.snort.org/ Tiene un triple modelo de reglas, dependiendo de que el usuario esté o no registrado y/o pague una suscripción. Centrándonos en las opciones gratuitas, los usuarios no registrados tendrían disponibles las *Community Rules*, que no incluyen ninguna regla específica para sistemas de control, mientras que los usuarios registrados tendrían disponibles reglas antiguas del *Snort Subscriber Rule Set*, que si incluye multitud de ellas. Adicionalmente, se podría utilizar también el conjunto de reglas desarrollado por Digital Bond (Quickdraw).
- Suricata: https://suricata-ids.org/ Utiliza un conjunto de reglas gratuitas (Emerging Threats) que contiene un pequeño subconjunto de reglas para sistemas de control. No obstante, la mayor parte de reglas de Snort serían también compatibles y existen algunas bases de reglas de terceros (Quickdraw y ProfinetMOD).
- Zeek (antiguo Bro): https://zeek.org/ Tiene soporte nativo para analizar Modbus, DNP3, MQTT y de terceros para Ethernet/IP, Profinet, el protocolo propietario de Siemens y Bacnet, que se deberían utilizar en este caso para crear scripts.

En lo relativo a los correladores de eventos o sistemas SIEM (gestión de eventos e información de seguridad), existen diversas opciones de código abierto disponibles como OSSIM, u2platform u OSSEC, que en términos generales son las versiones gratuitas y sin soporte por parte del fabricante de otras herramientas y, por tanto, presentan una cierta necesidad de configuración manual. Adicionalmente, es relativamente habitual también hacer uso para este propósito de la pila ELK (ElasticSearch, Logstash/Beats y Kibana), que tiene un uso más amplio en el ámbito de la supervisión.

Para facilitar la configuración conjunta del IDS y el SIEM se puede utilizar, no obstante, la distribución Security Onion orientada a facilitar la configuración de la monitorización de los sistemas de detección de intrusiones y que ya contiene algunas de las herramientas previamente descritas.

En lo relativo a la generación de tráfico simulado para ser analizado por la plataforma IDS, existen esencialmente dos opciones:

- La utilización de herramientas para editar y reproducir capturas de tráfico públicamente disponibles, entre las que se podría destacar Tcpreplay. En este caso, se podrían utilizar bases de datos de PCAPs como las siguientes: ICS-Security-Tools, Netresec, ICS-Pcap o PCAPr.

- La simulación de elementos de control y supervisión, para lo cual a su vez podríamos establecer otras dos opciones. En primer lugar, podríamos limitarnos a utilizar herramientas que meramente simulan los protocolos. Otra opción más flexible será utilizar software de uso común en la industria para el que existan versiones de prueba, como por ejemplo el software de programación de autómatas Codesys y su runtime de PLC sobre Linux o el SCADA Vijeo Citect, que generalmente presentan alguna limitación temporal. Esta opción, obviamente, requerirá más recursos desde un punto de vista computacional.

Cabe destacar que la selección de herramientas a utilizar es importante para evitar que el esfuerzo requerido supere lo razonable en un trabajo de una asignatura.

3. Resultados

Se enviarán mediante la plataforma Ágora, en la forma y plazos allí determinados, y posteriormente se presentará en clase.

Los resultados a aportar serán una **memoria** que exponga los siguientes puntos:

- La estructura propuesta para el proyecto, incluyendo tanto la de la subred simulada que es objeto de monitorización como la del conjunto IDS-SIEM que se hayan utilizado.
- Las posibilidades que permiten el IDS y SIEM seleccionados y las ventajas y desventajas que presentan en relación a la adecuación a este ámbito.
- De forma general, los pasos seguidos para la configuración y puesta en marcha del sistema, destacando las dificultades encontradas.
- Los resultados de la detección de intrusiones ante el tráfico simulado, mostrando capturas del SIEM e interpretándolos en el contexto de la red simulada.
- Conclusiones.

Adicionalmente, podrían incluirse los ficheros de configuración que se entiendan útiles para replicar la experiencia.

Finalmente, se realizará una **exposición** de los resultados de la actividad, centrada en los contenidos incluidos en la memoria.