Published on *Revista .Seguridad* (https://revista.seguridad.unam.mx)

Frameworks para monitoreo, forense y auditoría de tráfico de red - I

Javier Ulises Santillán Arenas

redes
SEM
SIEM
tráfico de red
numero-24

Frameworks

Actualmente existen diversas técnicas y tecnologías para el monitoreo del tráfico de red. Las redes de datos manejan información con protocolos y aplicaciones cada vez más complejas. Esto, combinado con la gran cantidad de información que se transfiere y la migración paulatina a modelos de comunicación codificados o cifrados, ha hecho también del monitoreo una tarea cada vez más compleja.

En los últimos años se han desarrollado tecnologías de análisis de datos como los SIEM (Security Information and Event Management), SIM (Security Information Management), SEM (Security Event Management), NSM (Network Security Monitoring), PNA (Passive Network Audit), etcétera. Estas tecnologías han ido madurando a través de la adición de nuevos modelos de análisis de información e incluso de nuevos mecanismos de detección e identificación de patrones, usando el aprendizaje de máquina o *machine learning*. En este contexto, existen también diversas técnicas y herramientas que pueden ayudar a los administradores a desarrollar o elegir un modelo de monitoreo, detección y auditoría que mejore el nivel de seguridad de sus organizaciones.

Frameworks de monitoreo

Ciertas técnicas podrían ser más efectivas, dependiendo del contexto del monitoreo y tomando en cuenta sus características, ventajas y enfoque. La Figura 1 presenta un panorama general sobre la relación entre los modelos de monitoreo y detección que se abordan en este artículo y que proveen lineamientos para desarrollar o implementar *frameworks* usando diversas tecnologías.

Figura 1. Panorama general de los modelos de monitoreo y análisis (Santillan, 2014)

Network Security Monitoring (NSM)

Es un modelo de análisis de tráfico de red que proporciona lineamientos para desarrollar un *framework* que incluya técnicas y herramientas para monitoreo, detección y retención de evidencia sobre incidentes de seguridad. Este modelo está basado en el análisis de datos generados por herramientas de seguridad como los IDS (Intrusion Detection Systems), analizadores de flujos, entre otros. NSM hace énfasis en las técnicas a seguir

para poder alcanzar una mejor detección, es decir, no solamente describe qué herramientas pueden ser utilizadas, también cómo, cuándo y dónde utilizarlas dentro del contexto de la red, así como las consideraciones de implementación, zonas y puntos de monitoreo. Una de las herramientas más conocidas y utilizadas en este tipo de *framework* es Sguil[1], un *front-end* para el análisis de datos extraídos del IDS Snort[2] y el analizador de flujos Argus[3], entre otras herramientas.

Panorama general de los procesos de monitoreo y análisis

Figura 2. Proceso de atención de incidentes de red (Network Incident Response Process)[4]

Dentro del proceso de atención a incidentes de red (Network Incident Response Process) mostrado en la Figura 2, NSM está involucrado en la fase de Detección (Detect), específicamente en dos de sus procesos*:* Contención Pronta del Incidente (Short Term Incident Containment), donde se tiene información sobre el incidente detectado; y en Emergencia (Emergency), donde se identifica y provee evidencia del incidente. Asimismo, NSM describe el llamado *Modelo de Referencia de Intrusiones (Reference Intrusion Model)*[5] el cual define cuatro tipos de datos:

- Datos de contenido completo: captura *bit-a-bit.*
- Datos de sesión: Distribución de protocolos y acumulación de tráfico.
- Datos estadísticos: Registro de conversaciones entre dispositivos.
- Datos de alerta: Información extraída de IDS.

En relación a NSM y la detección de intrusos, algunos debates[6] mencionan que los desarrolladores de IDS buscan una “detección inmaculada”, es decir, detección precisa; mientras que los practicantes de NSM buscan una “colección de datos inmaculada”, es decir, captura de evidencia tanto como sea posible.

Security Information and Event Management (SIEM)

La *minería de datos* es un proceso de extracción de modelos descriptivos a partir de grandes cantidades de datos, mediante el uso de modelos de análisis estadísticos, *machine learning*, entre otros. En el contexto de la seguridad en TI, la minería de datos se aplica en los llamados SIEM (Security Information and Event Management) para la identificación de patrones con propósitos de detección, auditoría e interpretación de información. Las fuentes de datos a analizar pueden ser herramientas como IPS (Intrusion Prevention Systems o Sistemas de Prevención de Intrusiones), IDS, *firewalls*, *routers*, bitácoras de sistemas, etcétera. Como se muestra en la Figura 3, a partir de estos datos se lleva a cabo una correlación (*correlation*) con el objetivo de filtrar información (*reduction*) para identificación e interpretación de eventos específicos relacionados, por ejemplo, con incidentes de seguridad.

Los SIEM combinan características de los SIM (Security Information Manager) y de los SEM (Security Event Manager), cuyos enfoques en términos generales son el análisis en tiempo real (SIM) y almacenamiento a largo plazo de registros de eventos (SEM).

Proceso general de los SIEM

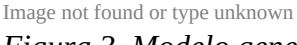

Figura 3. Modelo general de los SIEM [7]

Entre las características principales que los SIEM proporcionan están:

- Acumulación de datos (*data aggregation)*: Datos de diferentes fuentes alimentan un motor de análisis centralizado.
- Correlación: Identifican relaciones y se crean interpretaciones significativas.
- Alertas.
- Cumplimiento: Identificar si ciertas políticas se cumplen.
- Retención: Almacenamiento de datos históricos.
- Análisis forense: Creación de líneas de tiempo para reconstrucción de eventos.
- Inteligencia: Descripción del contexto de seguridad para efectos de toma de decisiones.

Actualmente existen herramientas SIEM *open source* tales como OSSIM de Alien Vault[8]. También existen opciones comerciales que integran algunas características adicionales, sin embargo el fundamento base es proveer características de un SIEM. Algunas de ellas son Alien Vault USM[9], Tenable SIEM [10], Splunk[11], entre otros.

Auditoría Pasiva de Tráfico de Red

De manera similar a los SIEM, la Auditoría Pasiva de Tráfico de Red (Passive Network Audit) involucra el análisis de bitácoras y correlación de datos, sin embargo, lo que define a PNA como un modelo de análisis independiente a los SIEM es el uso de tráfico de red como su fuente ***principal y única*** para la obtención de información y generación de reportes. A su vez, PNA implica solamente la utilización de herramientas pasivas para la extracción de información, es decir, ninguna acción llevada a cabo durante el proceso de análisis altera o interviene en la operación de la red que se analiza.

Mientras los SIEM se basan en acumulación de datos (*data aggregation*) de diversas fuentes como *firewalls,* bitácoras de sistemas, IDS, IPS, *routers*, etcétera, PNA se enfoca al tráfico de red como fuente de información. Como se aprecia en la Figura 4, la acumulación de datos ("*Multiple data aggregation"*) se hace de manera interna, ya que involucra un proceso adicional que es el procesamiento y decodificación previa de datos ("*Pre-processing & decoding"*) para generación de "bitácoras" o datos que normalmente serían la fuente de información inicial para un SIEM, sin embargo, en este caso son obtenidos sólo a partir del tráfico de red y son en realidad una "*aproximación"* a bitácoras reales. Esto quiere decir que en realidad dicha extracción implica una interpretación y en ciertos casos una extrapolación de información a partir de datos que representen una "firma" sobre determinada actividad o sistema (por ejemplo, el tráfico de *headers* HTTP puede contener datos para generar información similar que normalmente se obtendría a partir de una bitácora de un servidor web como Apache, etcétera). Así, a partir de este preprocesamiento es posible entonces identificar y decodificar protocolos, versiones de software, dominios, alertas de IDS, flujos, etcétera que comúnmente serían tomados de bitácoras de sistemas u otros dispositivos, con la ventaja de que todo el proceso se desarrolla de manera pasiva y únicamente a partir de tráfico de red.

Diagrama de auditoría pasiva de tráfico de red

Figura 4. Diagrama de auditoría pasiva de tráfico de red

PNA también se conoce como Identificación Pasiva de Red (Passive Network Discovery) y algunas fuentes[12] la describen como una tecnología para responder a las preguntas *¿Quién y qué hay en la red de la organización? y ¿Qué se está haciendo en la red de la organización?*, mediante identificación de utilización de la red, análisis forense de eventos, identificación de vulnerabilidades y perfiles de activos (equipos, servidores, entre otros).

Una desventaja de PNA es que el análisis puede ser limitado y no muy preciso debido a que el tráfico de red puede no contener datos suficientes para identificar y generar información confiable sobre la seguridad y el

estado de la red.

Prototipo de Auditoría Pasiva: PNAF

A continuación se presenta una introducción al prototipo de un *framework* de PNA llamado **Passive Network Audit Framework (PNAF)** (Santillan, 2014). Este *framework* define un modelo de análisis (Figura 5) para auditoría de tráfico de red a través de la utilización de diversas herramientas las cuales se conjuntan en una implementación de software libre. En este artículo se presenta una breve introducción sobre las características del *framework*, sin embargo en el próximo número se presentará una prueba de concepto con detalles sobre instalación, configuración y análisis de una muestra de tráfico de red.

Las principales características de PNAF son:

- Diseño modular con tres principales fases: (1) captura/lectura de tráfico, (2) procesamiento y (3) visualización (Figura 5).
- Provee un resumen del nivel de seguridad de la red basado en análisis de activos identificados en el tráfico de red.
- Identificación de actividades anómalas.
- Auditoría de políticas de seguridad.
- Análisis de impacto de vulnerabilidades basado en CVE (Common Vulnerabilities and Exposures) de NVD (National Vulnerability Database)[13].
- Recopilación de evidencia.

Modelo de análisis de Passive Network Audit Framework

Image not found or type unknown

Figura 5. Modelo de análisis de Passive Network Audit Framework (PNAF)

La siguiente tabla presenta un panorama general de algunas de las herramientas que pueden ser utilizadas dentro de PNAF. Cada una de ellas tiene un propósito específico de modo que la información se correlaciona para la identificación de activos y la determinación del contexto de la red.

Herramienta	**Propósito**	**Datos generados**	**Observaciones**
Enumeración e identificación de activos (*Profiling and Enumeration*)			
P0f	Enumeración de red y servicios.	Tipos de conexión (Capa 1), versiones de software y plataformas, roles de equipos.	Detección mediante múltiples métodos: firmas y comportamiento.
Snort Open AppId	Identificación de aplicaciones.	Tipos de aplicaciones usadas en la red.	Identificación mediante análisis de protocolos y no mediante número de puerto.
Prads	Enumeración de red y servicios.	Tipos de conexión (Capa 1), VLAN, versiones de software y plataformas.	Detección mediante múltiples métodos.
Motores de detección de intrusos (*IDS Engines*)			

Suricata	Motor IDS, decodificador de capa de aplicación, captura en tiempo real.	Alertas basadas en firmas, datos de HTTP, TLS, DNS, SSH, extracción de archivos transferidos.	Detección flexible por firmas (*signatures*), *parsers* de capa de aplicación y captura de alto rendimiento.
Snort IDS	Motor IDS.	Alertas basadas en firmas.	Detección flexible por firmas (*signatures*).
Bro IDS	Motor IDS, decodificador de protocolos y verificador de políticas.	Alertas de IDS, datos decodificados de capa de aplicación como HTTP, TLS, DNS, SSH.	Conjunto de *parsers* de capa de aplicación.
Análisis de flujos de tráfico de red (*Network Flow Analysis*)			
Cxtracker	Análisis de flujos.	Estadísticas de tráfico de red.	Análisis de gran cantidad de tráfico.
Argus	Análisis de flujos.	Estadísticas de flujos de tráfico de red, protocolos y decodificación de paquetes.	Método eficiente para análisis de grandes cantidades de tráfico.
Silk	Análisis de flujos.	Estadísticas de tráfico de red.	Análisis de gran cantidad de tráfico.
Tcpflow	Reensamblado de sesiones TCP y decodificación HTTP.	Datos HTTP.	Análisis de *payloads*.
Tcpdstat	Identificación de protocolos.	Estadísticas de protocolos.	Clasificación por capas de protocolos.
Inspección profunda de paquetes (*Deep Packet Inspection*)			
Chaosreader	Decodificación de capa de aplicación.	Datos HTTP, DNS, FTP, SMTP.	Análisis de *payloads*.
PassiveDNS	Análisis pasivo de DNS.	Estadísticas de DNS.	Identificación de *malware* basado en DNS (como Fastflux).
Tcpxtract	Extracción de archivos transferidos.	Lista de archivos transferidos.	Útil para identificación de *malware* y violación de políticas.
TcpExtract	Extracción de archivos transferidos.	Lista de archivos transferidos.	Basado en Python.
Httpry	Decodificación de protocolo HTTP.	Datos de HTTP y *payloads*.	Análisis a fondo de HTTP.
Xplico	Extracción de datos de capa de aplicación.	Datos HTTP, archivos, información de protocolos.	Tiene su propia interfaz web.
Nftracker	Extracción de archivos transferidos.	Lista de archivos transferidos.	Útil para identificación de *malware* y violación de políticas.
Ssldump	Extracción de información de protocolos SSLv3/SSL.	Información de certificados.	Útil en análisis de cadenas de confianza (basadas en PKI) mediante certificados.

Tabla 1. Herramientas de análisis de tráfico de red

PNAF puede ser utilizado sobre entornos GNU/Linux y su utilización es mediante la línea de comandos (CLI , *Command Line Interface*). El *framework* se alimenta de tráfico de red, el cual es analizado usando las herramientas mencionadas en la tabla anterior de modo que el administrador puede visualizar un resumen de una auditoría básica de tráfico de red.

Opciones de ejecución en PNAF

Image not found or type unknown

Figura 6. Opciones de ejecución en PNAF

Para mayor información y actualizaciones de PNAF se pueden consultar los siguientes sitios web.

- *http://www.github.com/jusafing/*
- *http://sec.jusanet.org/*

Referencias

- Passive Network Audit Framework, Master thesis. Santillan, Javier. Eindhoven University of Technology. The Netherlands, 2014.
- The Tao of network security monitoring: beyond intrusion detection. Richard Bejtlich. Pearson Education, 2004.
- The Practice of Network Security Monitoring: Understanding Incident Detection and Response. Richard Bejtlich No Starch Press, 2013.
- Demystifying the myth of passive network discovery and monitoring systems. Ofir Arkin. InsightiX McAfee, 2012.

---

[1] http://bammv.github.io/sguil/index.html

[2] http://www.snort.org

[3] http://qosient.com/argus/

[4] Richard Bejtlich. The Tao of network security monitoring: beyond intrusion detection. Pearson Education, 2004.

[5] Richard Bejtlich. The Practice of Network Security Monitoring: Understanding Incident Detection and Response. No Starch Press, 2013.

[6] Post by Richard Bejtlich's on TaoSecurity blog. http://taosecurity.blogspot.nl/2007/03/ nsm-and-intrusion-detection-differences.html

[7] http://www.cybervally.com/2012/10/siem-technology/

[8] https://www.alienvault.com/open-threat-exchange/projects

[9] https://www.alienvault.com/open-threat-exchange

[10] http://www.tenable.com/solutions/log-management-siem

[11] http://www.splunk.com/

[12] Ofir Arkin. Demystifying the myth of passive network discovery and monitoring systems. http://www.mcafee.com/us/resources/white-papers/wp-demystifying-passive-network-discovery.pdf

[13] https://nvd.nist.gov/
