Entregable D3. Diseño del entorno de experimentación

Investigador Responsable: Pedro García Teodoro
Grupo de trabajo (% dedicación): PGT (50), JCP (25), GMF (25), RRG (100)
Requisitos previos: D1.
Riesgos y contingencia: R1 – C1.a y/o C1.b
Duración: 3 meses
Intensidad de trabajo (hombre-mes): 6,00
Objetivo Específico (IP Responsable): OE5 (Gabriel Maciá Fernández)
Entregables: D3.

Índice:

1. Preliminares

Para abordar adecuadamente la definición de la tarea objeto de discusión, hemos de partir necesariamente de los **objetivos técnicos principales del proyecto** global:

- Reducción de dimensionalidad basada en PCA para detección de anomalías.
- Arquitectura lógica jerárquica de los elementos sensores y de detección.

Para alcanzar los objetivos anteriores y así validar nuestras hipótesis, dos son las **tareas últimas a realizar**:

1. Evaluación de una detección de anomalías 'plana', donde todas las fuentes de información se analicen por parte de una misma entidad detectora.
2. Evaluación y comparación de una detección de anomalías jerárquica PCA, donde las fuentes y detectores se organicen siguiendo esta estructura alternativa.

Como es evidente, las evaluaciones aludidas precisan de un entorno experimental adecuado que permita el despliegue de distintos escenarios y consecuentes desarrollos. Para ello, varios son los **aspectos a considerar en la definición y despliegue del entorno**:

- Funcionales, relacionados con el tipo de máquinas/nodos a considerar (*p.ej.*, sistemas Windows *vs.* Linux, servidores *vs.* clientes, ...).
- Topológicos, relativos al número y tipo de dispositivos (*p.ej.*, estaciones finales *vs. routers*, cortafuegos, …) y sus interconexiones (*p.ej.*, disposición en subredes, DMZ, etc.).
- Fuentes de información, relacionados con las herramientas de adquisición de datos para la monitorización del entorno y subsiguiente detección de anomalías (*p.ej.*, escaneo de puertos, *IDS logs*, *firewall logs*, *netflow*, antivirus, etc.).

- Bases de datos, necesarias para llevar a cabo pruebas de detección que permitan concluir de forma definitiva la validez de la experimentación. En ellas se deberá disponer tanto de instancias de ataque como legítimas, 'normales'.

A fin de alcanzar unos resultados y conclusiones realmente válidos, es preciso que el entorno a considerar sea tan realista como sea posible. En este sentido, es de indicar como primer hecho reseñable que un **entorno de simulación** no resultaría adecuado por cuanto que no existe actividad alguna en el entorno más allá de la propia relativa a los potenciales ataques ejecutados, lo cual conlleva la ausencia de instancias legítimas (*véase* Bases de datos antes). Es más, muchos de los ataques podrían no ser posibles por cuanto que su ejecución precisa de un entorno en producción, con usuarios reales haciendo uso de servicios y sistemas e interaccionando entre sí.

Así pues, el potencial empleo de entornos virtuales, sin duda de interés en diversas situaciones, quedará relegado aquí a situaciones específicas donde se requiera testar algún aspecto puntual de los desarrollos pretendidos. Para tales casos, cabe mencionar algunos recursos de posible interés:

- VirtualBoxes: *http://virtualboxes.org/*
- Virtual Machine image Repository & Catalog (VMRC), UPV: *http://www.grycap.upv.es/vmrc/index.php*
- VM Depot, MS Open Tech: *https://msopentech.com/opentech-projects/vm-depot-from-ms-open-tech/*

Frente al uso, pues, de entornos de simulación, se tratará de hacer uso en la medida de lo posible de **escenarios reales**. Habida cuenta de la participación del Grupo Trevenque en VERITAS, se tratará de disponer de escenarios dentro de su red.

Seguidamente se discuten las características que ha de tener el escenario real pretendido, y ello en base a cada uno de los cuatro tipos de aspectos anteriormente mencionados: funcionales, topológicos, fuentes de información y bases de datos.

2. Aspectos funcionales

Por lo que respecta a la tipología de equipos a considerar en el entorno, los tres siguientes serán los principales:

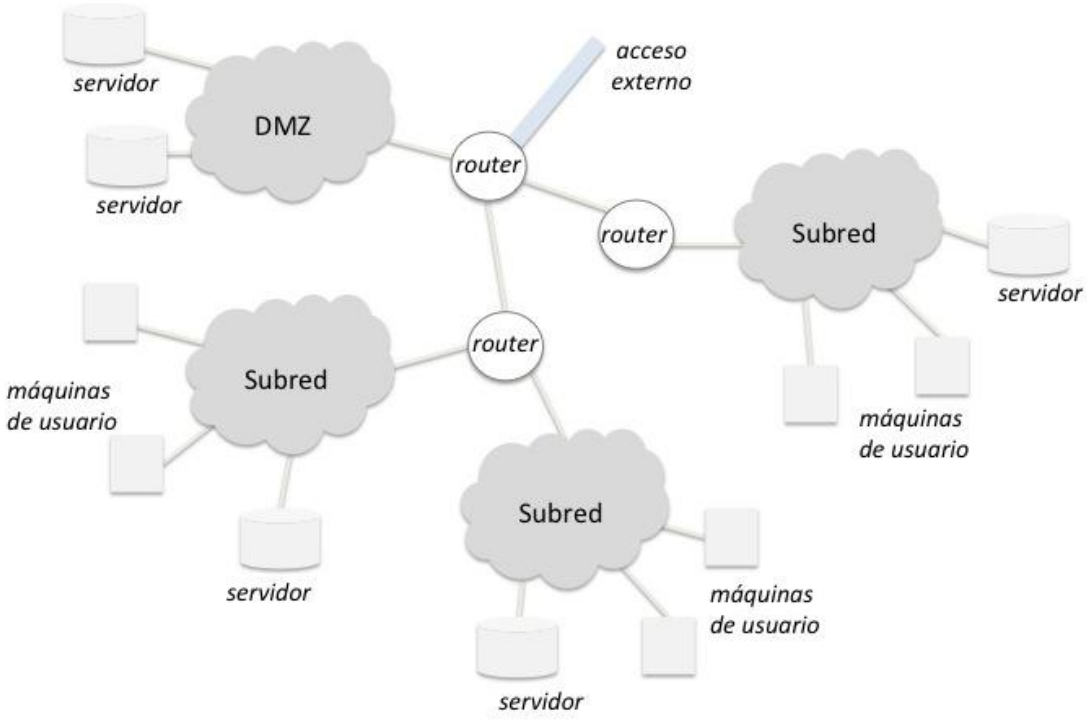
- ***Máquinas de usuario***, por cuanto que estas constituyen el objetivo y fin último de toda red: la interacción con y entre usuarios finales. Además, estos constituyen habitualmente la principal fuente de infección en un entorno de redes y comunicaciones.

  Aunque existen diversas posibilidades de SO para dichas máquinas, se aceptarán tanto de tipo ***Windows*** como de tipo ***Linux***.
- ***Servidores***, como elementos principales en los que se sustenta la provisión de servicios. Si bien son varios los tipos de servicios a proporcionar en un entorno de red, sería deseable contar en el escenario de trabajo con los tres siguientes tipos de servidores: ***DNS, mail*** y ***web***, pudiendo considerarse también la posibilidad de contar con servidores de ***ficheros***.
- ***Routers***, al ser los elementos clave que permiten la interconexión y acceso a redes y sistemas. Además de ello, gran parte de los esquemas de monitorización y seguridad actuales se basan en el seguimiento de la actividad en este tipo de dispositivos.

Si bien podría considerarse importante también el medio físico último que soporta el transporte de la información (WiFi, ADSL, Ethernet, …), consideramos ello secundario por lo que respecta a los objetivos en este proyecto perseguidos. Más allá de este hecho, es obvia la necesidad de contar con dicho/s medio/s.

3. Aspectos topológicos

Partiendo de la existencia de los elementos anteriormente citados, la disposición específica de estos en el escenario ha de ser tal que permita abordar los objetivos pretendidos. Considerando como hecho principal la organización jerárquica, la propuesta topológica base sería algo del siguiente estilo:



En esta disposición se observan algunos elementos constitutivos básicos:

- **Subred**, donde están dispuestas las máquinas de los usuarios (en número de alrededor de 10 como mínimo), además de algún servidor tipo ficheros o similar.
- **DMZ**, conformada por servidores típicos como DNS, mail o HTTP.
- Interconexión a través de ***routers***, con un mínimo de 2 **niveles de profundidad**. En caso de necesidad, esta podría aumentarse a valores mayores sin más que repetir algunos de los elementos ya mencionados.

4. Fuentes de información

Tras una revisión bibliográfica acerca de las fuentes de información más habituales consideradas en un sistema SIEM, las que serán objeto de estudio y posible despliegue en el entorno considerado son las siguientes:

- ***Syslog traces***, para llevar a cabo el registro de eventos de un sistema dado. Esta herramienta se dispondría en todas y cada una de las máquinas (de usuario, servidor o *router*) existente en el entorno.
- ***Firewall traces***, para monitorizar la operación de los cortafuegos. Esta herramienta se dispondrá en cada uno de los cortafuegos dispuestos en la topología.
- ***Netflow***, para trazas de red. Esta herramienta se dispondría en cada una de las subredes de la topología.
- ***IDS***, para intrusiones. Esta herramienta se dispondrá en cada una de las subredes de la topología.
- ***Nmap***, para monitorizar puertos demandados. Esta herramienta se dispondría en una o varias de las máquinas finales de usuario para cada subred, así como en los servidores dispuestos en el entorno.
- ***Antivirus***, para detectar gran variedad de *malware*. Esta herramienta se dispondría en una o varias de las máquinas finales de usuario para cada subred.

Todas estas herramientas son de carácter estándar y no suponen en modo alguno una adecuación ad hoc a los objetivos perseguidos, más allá del necesario despliegue de disposición específicos de monitorización (y detección) que hagan uso de ellas.

5. Bases de datos

Es evidente que para llevar a cabo la evaluación de un sistema de detección como el aquí propuesto, es precisa la recolección de datos procedentes a las herramientas anteriormente citadas en base a una experimentación extensa, donde se alternen situaciones de normalidad con otras en las que tengan lugar eventos maliciosos o ataques orientados a transgredir la seguridad del sistema monitorizado en uno o más aspectos. Será a partir de toda esta información que podamos determinar la eficacia y eficiencia de nuestras propuestas.

La disposición de **eventos legítimos** (o normales, no de ataque) es fundamental de cara a la potencial extracción de modelos de comportamiento en los que sustentar la detección. Adicionalmente, una actividad de operación normal en el entorno resulta también importante por cuanto que sirve de ocultación de los ataques reales y permitirá determinar un parámetro de alta relevancia en todo sistema de detección, la *tasa de falsos positivos*. Es por todo ello que al inicio se ha concluido que un entorno de simulación no resulta adecuado para la experimentación, al no existir actividad 'normal' subyacente.

Adicionalmente a la actividad normal, es evidente que será precisa la disposición de **eventos de ataque**, objetivo último de un sistema de detección, para poder determinar las capacidades reales de detección (en términos de *accuracy*) de los desarrollos realizados. Para poder contrastar la bondad de las propuestas, hemos de ser conscientes de la naturaleza maliciosa de los ataques puestos en marcha[1]. Para ello, lo que haremos será llevar a cabo la inyección

[1] El conocimiento preciso de los eventos legítimos y maliciosos es lo que se conoce como *groundtruth*.

controlada de ciertos ataques en el entorno a monitorizar. Algunos de los ataques a ejecutar son los siguientes, considerados los de mayor impacto en 2015 (http://www.calyptix.com/top-threats/top-7-network-attack-types-in-2015-so-far/):

- Denegación de servicio a servidores, orientado a anular estos.
- Fuerza bruta, para conseguir las claves de acceso a un sistema.
- Ataques a navegadores, orientados a la descarga de *malware*.
- Ataques de puerta trasera, orientados a conseguir acceso a un sistema de forma remota.
- *Botnet*, ideado para llevar a cabo el control remoto de un equipo, haciendo que este realice las acciones ordenadas desde el *botmaster*.

Todos estos ataques serán puestos en marcha a través del despliegue de software específico existente al efecto.

6. Conclusiones

En este documento se ha tratado de perfilar el entorno de experimentación a considerar en la evaluación de los desarrollos pretendidos para el proyecto VERITAS. En este estudio se han discutidos aspectos funcionales, topológicos, de fuentes de información y bases de datos; todo ello en relación a un entorno real en producción que permita la validación adecuada de los desarrollos y realizaciones pretendidos.