Implantación de una plataforma de monitorización de la seguridad informática con Security Onion

David COMPANY ESTALL
david.company@cttc.es

¿Qué es el CTTC?

- Centre Tecnològic de Telecomunicacions de Catalunya: Fundación sin ánimo de lucro dedicada a la investigación en tecnologías y sistemas de comunicaciones y geomática.
- 5G, Smart Grids, Optical networks, SDN, DSP, M2M, satélites, sistemas de navegación
- Infraestructuras TI
  - Varios data-centers y testbeds, repartidos en dos edificios
  - 120 usuarios
  - 40 Servidores físicos/ virtuales: email, servidores web, servidores de ficheros, simulaciones,...
  - Red ethernet y red wireless

Plataforma de monitorización de la seguridad

Funciones:

- Detección de intrusiones -> monitorización de eventos en red y equipos informáticos en busca de incidentes de seguridad
  - Capturas de paquetes
  - Datos de sesión y transacciones de datos
  - Genera alertas de seguridad de Host y de red
- Análisis de logs -> detectar ataques usando logs
  - Recepción, parseo, filtrado y agregación de eventos y logs
  - Almacenamiento: compresión, normalización, indexación

Plataforma permite gestionar

- Correlación de eventos, gestión de alertas e incidentes, generación de informes, investigación forense

Security Onion

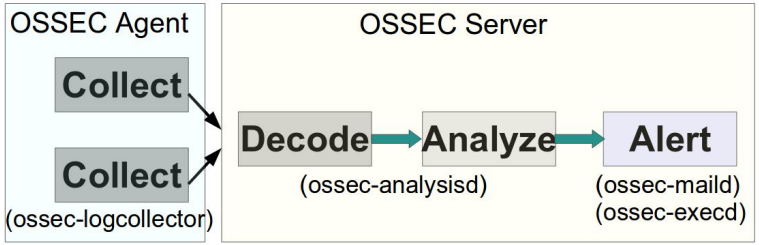
- Distribución Linux basada en Ubuntu que contiene varias herramientas de seguridad: Snort, Suricata, Bro, OSSEC, Sguil, Squert, CapMe, NetworkMiner, WireShark, ELSA (ahora logstash + Kibana), etc.
- Todas las herramientas están integradas
  - complementadas y es sencillo pivotar de una a otra
  - sencillo de instalar y poner en marcha
- Permite la detección de intrusiones y monitorización de red y la gestión de eventos de seguridad.

https://securityonion.net

OSSEC - HIDS

Sistema de detección de intrusiones de host Open-Source

- Análisis automático de logs del host -> basado en reglas
- Verificación de la integridad de los ficheros
- Detección de rootkits
- Respuesta activa y envío de avisos en tiempo real
- Arquitectura basada en un servidor + agentes en los servidores a monitorizar



Snort - NIDS

Network IDS Open-source

- Funcionamiento
  - Sensores que capturan paquetes de red
  - Se realiza un preprocesado i normalización del tráfico
  - El resultado es comparado con patrones y reglas definidos internamente
  - Detecta amenazas o ataques y generar alertas
- Motor de detección basado en reglas se actualizan automáticamente mediante la funcionalidad pulled-pork des de repositorios gratuitos o de pago (ET)
- Se puede escoger Suricata

Bro Network Security Monitor

Framework de Monitorización de red

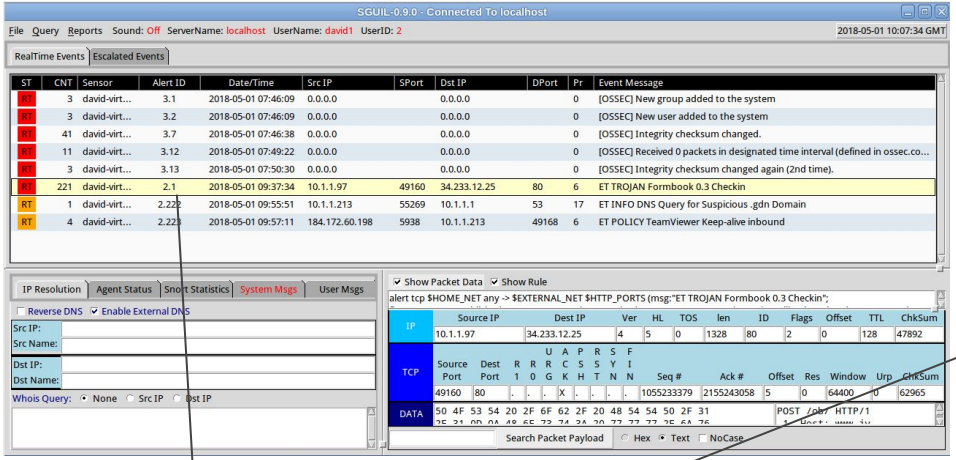
- Monitoriza la actividad de red y genera logs de las conexiones TCP/UDP, peticiones DNS, servicios de red y software detectados, actividad HTTP, FTP, IRC, SMTP, SSH, SSL, etc.
- Bro incluye analizadores para los protocolos más comunes
- La información se recoge en una base de datos y se puede consultar mediante ELSA o Logstash y Kibana-> complemento con información de contexto a la hora de analizar alertas.

Sguil

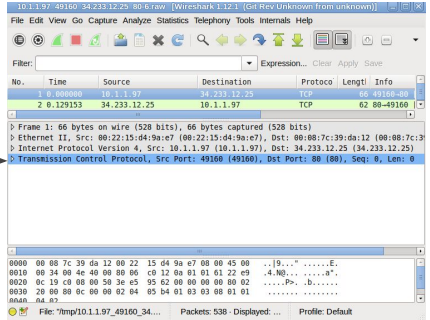
Consola de analista de seguridad.

- Interfaz gráfica intuitiva con la que acceder a las alertas de seguridad, los datos de sesión y las capturas de datos.
- Toda esta información se almacena en una base de datos a la que sguil accede
- Herramientas integradas CapMe, Wireshark y Network Miner
- No solo tenemos acceso a la alerta, sino también al contexto en que se ha producido

Sguil (II)



Event History
Transcript
Transcript (force new)
Wireshark
Wireshark (force new)
NetworkMiner
NetworkMiner (force new)
Bro
Bro (force new)

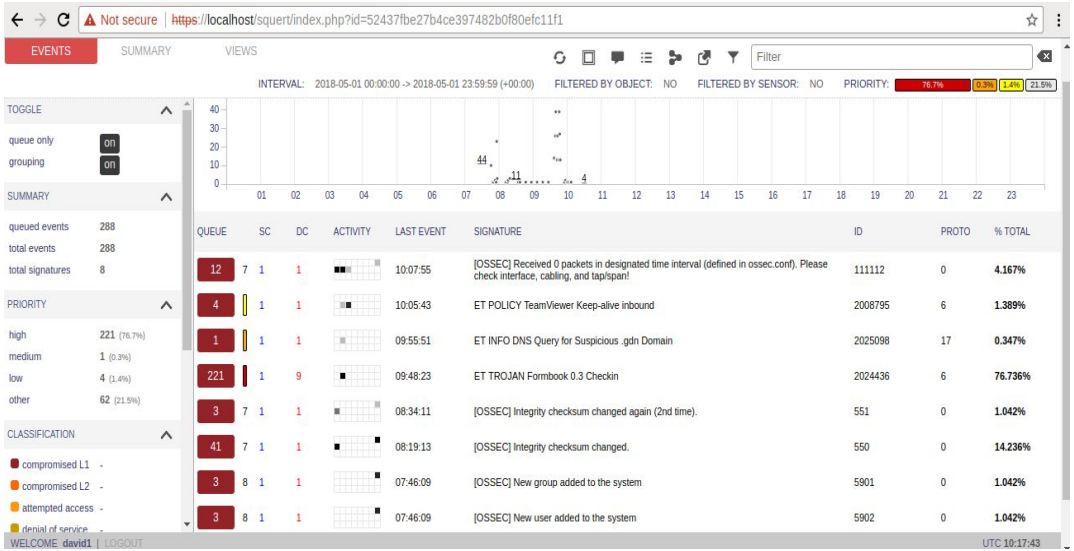


Squert

the squertproject

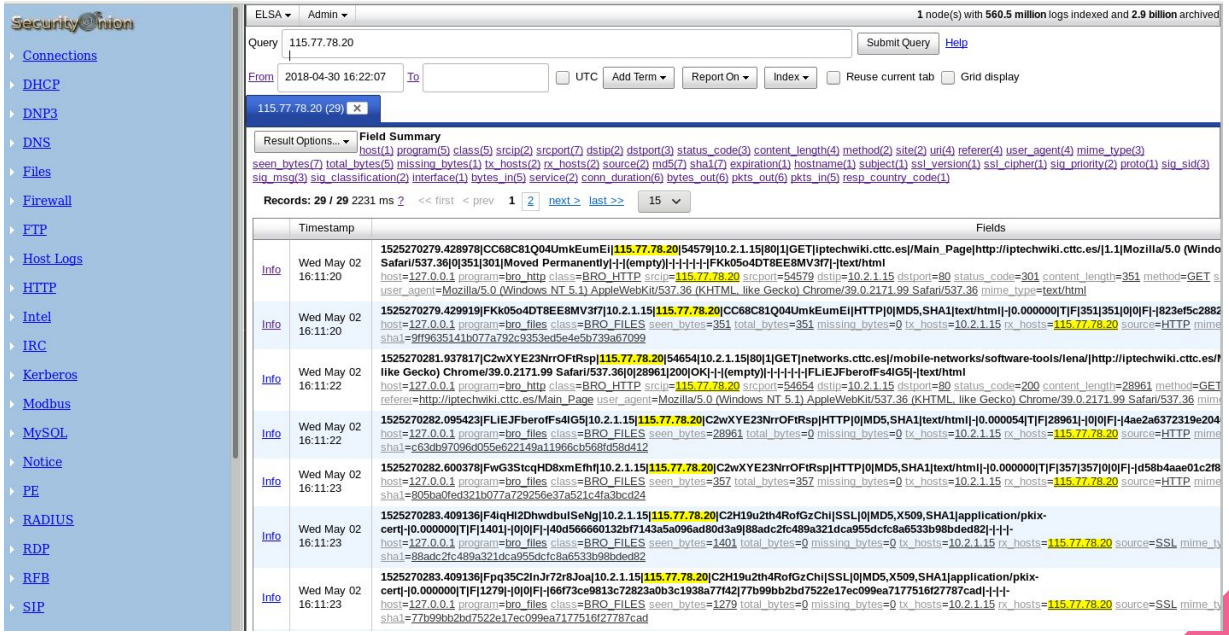
Aplicación web de visualización de los eventos:

- Consola de analista complementaria de sguil
- Aporta información de contexto, agrupación de eventos, timeline
- Consulta la base de datos de sguil -> se basa en los mismos datos pero los muestra de manera diferente



ELSA

Plataforma de registro y visualización de logs -> Interfaz web para poder hacer búsquedas en los datos y logs recogidos en la plataforma (ahora logstatsh y Kibana)



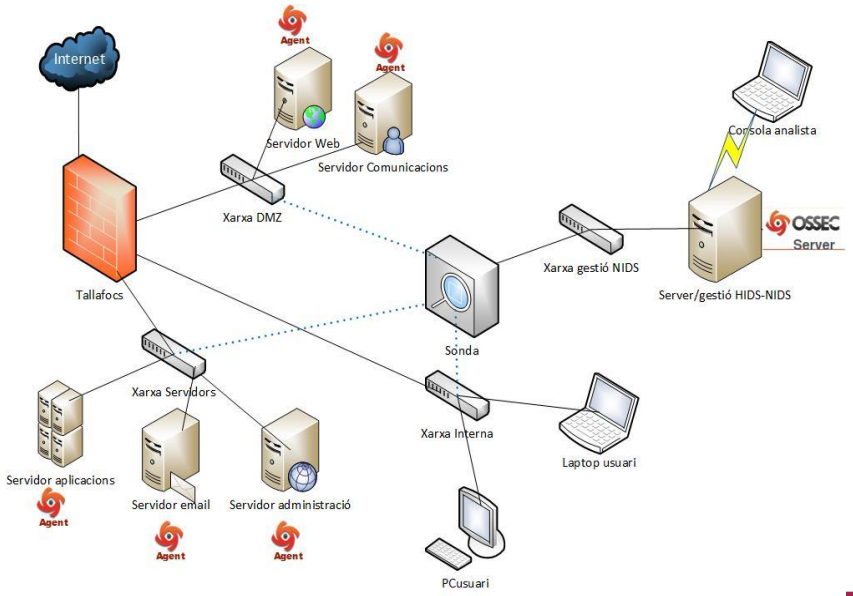
Esquema con los elementos de la plataforma

Arquitectura distribuida

- Sensores que capturan y procesan el tráfico de red
- Agentes que monitorizan la seguridad de los hosts
- Servidor que recibe las alertas generadas por los sensores y agentes
- Base de datos -> alertas, sesiones y logs normalizados
- Consola de analista

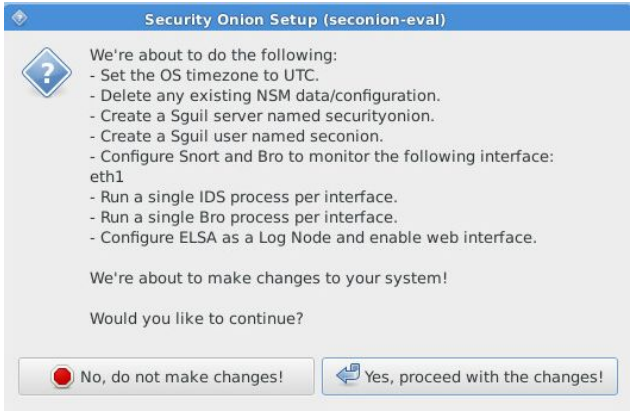
Diferentes configuraciones posibles según la distribución de la red y el tráfico

- sensor + servidor
- varios sensores + servidor
- sensor y servidor en el mismo equipo (standalone)



¿Cómo puedo probar Security Onion?

Es fácil hacer una instalación de Security Onion en modo evaluación



- Pasos:
  - Descargar la distribución de la web
  - En un equipo o VM, instalar distribución Security Onion (similar a instalar Ubuntu)
  - Ejecutar utilidad de setup para configurar interfaces de management y de captura
  - Reiniciar y ejecutar de nuevo la utilidad en modo quick-setup -> servidor y sensor estarán en modo standalone (integrados en una misma máquina), junto con las principales utilidades de HIDS, NIDS, análisis y visualización, todo integrado y preparado para funcionar.
- Ejecutar archivo pcap y ver las alertas que se han generado

Tareas post-instalación

- Tareas post-instalación: actualizar, definir redes internas, ajustar procesos, comprobar carga de las interfaces del sensor
- Configurar consola de analista -> para acceder a las alertas
- Pruebas post-instalación: generación de alertas
- Gran número de alertas en un primer momento a ordenar en categorías
- Ajustes post-instalación para reducir el número de falsos positivos
    - Deshabilitar, modificar, crear nuevas reglas con Snort
    - Autocategorías
    - Excluir ficheros de OSSEC

¿Qué problemáticas de seguridad puede resolver?

Problemáticas de seguridad:

- detección de ataques
- detección de servidores comprometidos -> tienen actividad sospechosa
- Vulnerabilidades en servidores, servicios o equipos
- Errores de configuración
- Detectar flujos de datos sospechosos o poco habituales
- Tener evidencias en el caso de accesos no autorizados o robos de datos
- En caso de ataque con éxito, tener herramientas de análisis para determinar lo ocurrido y el alcance del problema

Valoraciones y conclusiones

- Instalación del software es rápida y sencilla (y económica)
- Gestión de actualizaciones de firmas y software bien resuelta
- Ha permitido al CTTC
  - Fortalecer la seguridad de los equipos -> detectar vulnerabilidades y errores de config.
  - Mejora de las políticas de seguridad
  - Detectar ataques e investigar las causas
  - Aumentar la visibilidad de lo que ocurre en la red
- Exige un esfuerzo continuo de ajuste del sistema
- Trabajo continuo de clasificación de alertas e investigación de incidentes