Análisis de amenazas en artefactos forenses de Windows

Laboratorio

Análisis artefactos forenses de Windows

1.Laboratorio

En este laboratorio aprenderemos cómo analizar artefactos forenses de sistemas Windows utilizando herramientas como Chainsaw, una utilidad diseñada para buscar y analizar registros de eventos, y las reglas Sigma, un lenguaje abierto y estándar para la detección de eventos. Discutiremos los fundamentos de estas herramientas, su implementación práctica en un laboratorio, y cómo se pueden combinar para identificar patrones de actividad maliciosa. Además, se incluirán ejemplos prácticos para configurar un entorno de laboratorio y ejecutar análisis efectivos.

2. Sigma Rules

Las reglas Sigma son un estándar abierto para la detección de amenazas en sistemas de información. Están diseñadas para describir patrones o indicadores de actividad sospechosa en registros de eventos (logs) de forma comprensible y flexible, similar a cómo las reglas YARA se utilizan para identificar malware en archivos.

Características principales de las reglas Sigma:

Estandarización:

Sigma proporciona un formato común para definir detecciones, independientemente de la plataforma o solución de monitoreo (como SIEMs: Splunk, Elastic, etc.).

Simplicidad:

Las reglas están escritas en un formato **legible por humanos** (usualmente YAML), lo que facilita su comprensión y modificación por analistas.

Independencia de la plataforma:

No dependen de un proveedor o herramienta específica. Una regla Sigma puede traducirse a diferentes lenguajes de consulta mediante herramientas como el **Sigma Converter**.

Estructura básica de una regla Sigma: Las reglas se organizan en secciones clave como:

- **title**: Nombre descriptivo de la regla.
- **id**: Identificador único (UUID) para la regla.
- **description**: Explicación del objetivo de la regla.

- **logsource**: Fuente de los registros (por ejemplo, Windows Event Logs, Apache Logs).
- **detection**: Criterios específicos de detección.
- **level**: Nivel de severidad (informativo, bajo, medio, alto, crítico).

Ejemplo:

title: Suspicious Process Execution

id: a1b2c3d4-5678-90ab-cdef-1234567890ab

description: Detecta la ejecución de procesos sospechosos.

logsource:

category: process_creation

product: windows

detection:

selection:

CommandLine|contains: ['powershell.exe', '-enc']

condition: selection

level: high

Uso práctico:

Ciberseguridad: Detección de actividad maliciosa como movimientos laterales, escalación de privilegios, malware, etc.

Respuesta a incidentes: Proporciona alertas específicas basadas en comportamientos definidos.

Análisis de amenazas: Ayuda a identificar patrones específicos de actores de amenazas.

Conversión:

Las reglas Sigma pueden traducirse a consultas específicas de herramientas (como Splunk SPL o Elastic Query DSL) usando herramientas como **Sigmac**.

3. Chainsaw

Chainsaw es una herramienta open-source que analiza registros de eventos de Windows utilizando técnicas avanzadas como:

- **Búsqueda basada en Sigma rules**: Sigma es un estándar de reglas genéricas para detección de amenazas que se traduce a múltiples herramientas SIEM. Chainsaw soporta estas reglas para identificar actividad sospechosa en registros.
- **Análisis de patrones de ataque comunes**: Chainsaw incluye heurísticas específicas para detectar actividades relacionadas con técnicas conocidas del MITRE ATT&CK.
- **Desempeño optimizado:** Diseñado para manejar grandes cantidades de registros sin sacrificar velocidad o precisión.

https://github.com/WithSecureLabs/chainsaw

Casos de uso

- **Identificación de anomalías:** Buscar eventos inusuales como inicios de sesión fallidos repetitivos, cambios en las políticas de auditoría o ejecuciones de scripts PowerShell con parámetros maliciosos.
- **Detección de actividad lateral:** Rastrear movimientos laterales en la red, como conexiones remotas sospechosas o uso de herramientas como PsExec.
- **Búsqueda de IOCs:** Analizar los registros para encontrar Indicadores de Compromiso (IPs, hashes, o cadenas específicas).
- **Verificación post-intrusión:** Recolectar evidencia tras un incidente para entender el alcance del ataque.

Flujo típico de trabajo con Chainsaw

Recolección de logs:

- Exportar los registros de eventos relevantes desde los sistemas Windows comprometidos o sospechosos, por ejemplo:

wevtutil epl Security logs.evtx

Ejecución de Chainsaw:

- **Análisis básico**: Escanear los registros con reglas Sigma predefinidas:

./chainsaw.exe hunt evtx_attack_samples/ -s sigma/ --mapping mappings/sigma-event-logs-all.yml

- **Búsqueda de palabras clave**: Buscar patrones específicos:

Search for the case-insensitive word 'mimikatz':

./chainsaw search mimikatz -i evtx_attack_samples/

Search for Powershell Script Block Events (EventID 4014):

./chainsaw search -t 'Event.System.EventID: =4104' evtx_attack_samples/

- **Generación de resúmenes**: Identificar eventos de alto interés como cuentas creadas o cambios de privilegios:

chainsaw timeline logs.evtx

Análisis de resultados:

- Los resultados se presentan en formatos estructurados y filtrados, facilitando el análisis rápido de eventos relevantes.

Toma de acción:

- Aislar máquinas comprometidas, implementar bloqueos en firewalls o ajustes en políticas de seguridad basados en los hallazgos.

Ventajas de Chainsaw

- **Portabilidad**: Funciona en sistemas locales sin necesidad de infraestructura adicional.
- **Velocidad**: Procesa grandes volúmenes de registros rápidamente.
- **Integración con Sigma**: Aprovecha una librería de reglas comunitarias y personalizables.
- **Facilidad de uso**: Su sintaxis es simple y amigable para analistas.

4. Laboratorio practico

Descargar las herramientas y fuentes de datos de prueba (Visor de eventos de Windows EVTX):

1. Descargar Chainsaw:

https://github.com/WithSecureLabs/chainsaw/tree/master?tab=readme-ov-file#downloading-and-running

2. Descargar reglas SIGMA:

https://github.com/SigmaHQ/sigma

3. Descargar samples de logs de eventos de Windows:

https://github.com/sbousseaden/EVTX-ATTACK-SAMPLES

Para este laboratorio utilizaremos los eventos de "Credential Access".

Tareas a realizar:

1. **Analizar registros de acceso y volcado a NTDS:**

```
C:\chainsaw>chainsaw.exe search NTDS.dit -i "EVTX-ATTACK-SAMPLES-master\Credential Access"
```

A. Indicar hostname y dominio del equipo al que se ha accedido.

HOSTNAME: DC1

DOMINIO: insecurebank

B. Indicar username del usuario que ha accedido.

USERNAME: bob

```
---
Event_attributes:
  xmlns: http://schemas.microsoft.com/win/2004/08/events/event
Event:
  System:
    Provider_attributes:
      Name: ESENT
    EventID_attributes:
      Qualifiers: 0
    EventID: 325
    Level: 4
    Task: 1
    Keywords: '0x80000000000000'
    TimeCreated_attributes:
      SystemTime: 2019-11-26T23:55:00.000000Z
    EventRecordID: 1970
    Channel: Application
    Computer: DC1.insecurebank.local
    Security: null
  EventData:
    Data:
    - NTDS
    - '3392'
    - ''
    - '2'
    - C:\Users\bob\Desktop\test\Folder\ntds\Active Directory\ntds.dit
    - '0'
    - '[1] 0.000, [2] 0.000, [3] 0.000, [4] 0.047, [5] 0.000, [6] 0.000, [7] 0.000, [8] 0.000, [9] 0.000, [10] 0.000,
 [11] 0.000.'
    Binary: null
```


2. **Analizar si se ha ejecutado mimikatz sobre algún equipo.**

```
C:\chainsaw>chainsaw.exe search mimikatz -i "EVTX-ATTACK-SAMPLES-master\Credential Access"
```

A. Indicar hostname del equipo:

HOSTNAME: PC04

B. Indicar username del usuario que lo ejecutó.

USERNAME: IEUser

C. Indicar la ruta en donde se ejecutó mimikatz.

RUTA: c:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe

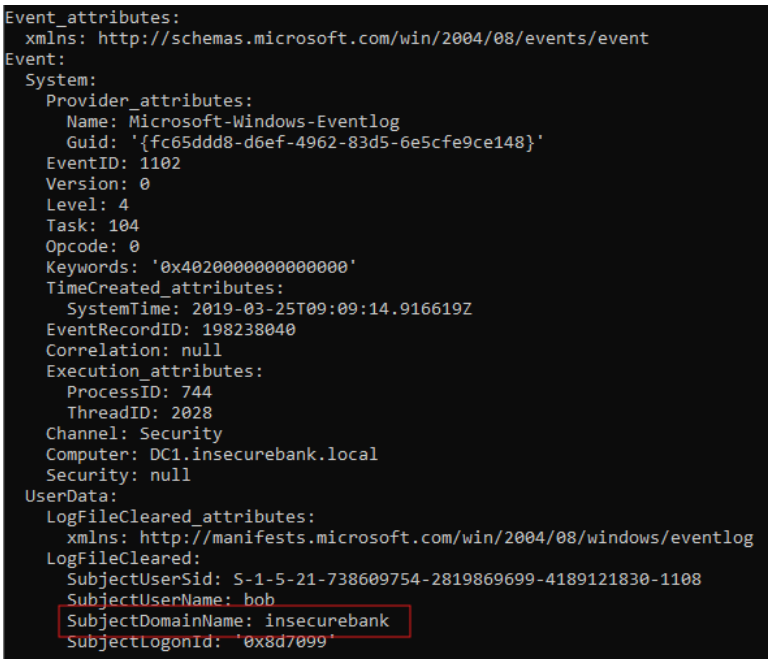

```
Event_attributes:
  xmlns: http://schemas.microsoft.com/win/2004/08/events/event
Event:
  System:
    Provider_attributes:
      Name: Microsoft-Windows-Sysmon
      Guid: 5770385F-C22A-43E0-BF4C-06F5698FFBD9
    EventID: 10
    Version: 3
    Level: 4
    Task: 10
    Opcode: 0
    Keywords: '0x8000000000000000'
    TimeCreated_attributes:
      SystemTime: 2019-03-17T19:37:11.661930Z
    EventRecordID: 4807
    Correlation: null
    Execution_attributes:
      ProcessID: 344
      ThreadID: 2032
    Channel: Microsoft-Windows-Sysmon/Operational
    Computer: PC04.example.corp
    Security_attributes:
      UserID: S-1-5-18
  EventData:
    RuleName: ''
    UtcTime: 2019-03-17 19:37:11.641
    SourceProcessGUID: 365ABB72-A1E3-5C8E-0000-0010CEF72200
    SourceProcessId: 3588
    SourceThreadId: 2272
    SourceImage: C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe
    TargetProcessGUID: 365ABB72-0886-5C8F-0000-001030560000
    TargetProcessId: 476
    TargetImage: C:\Windows\system32\lsass.exe
    GrantedAccess: '0x1010'
    CallTrace: C:\Windows\SYSTEM32\ntdll.dll+4595c|C:\Windows\system32\KERNELBASE.dll+8185|C:\Users\IEUser\Desktop\mi
mikatz_trunk\Win32\mimikatz.exe+5c5a9|C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c86c|C:\Users\IEUser
\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5cbd2|C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c4ff|C:\U
sers\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+3b3d3
```

3. **Indique los dominios que se detectan en los registros analizados**

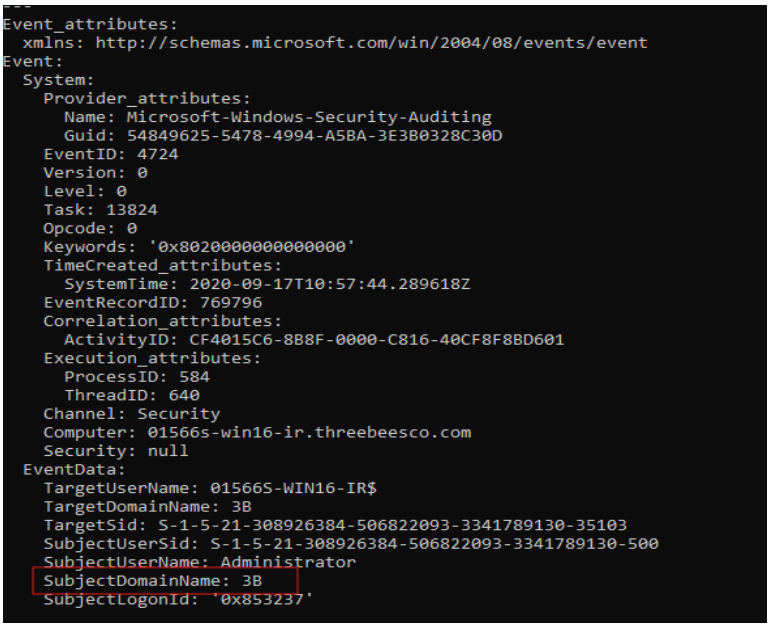
```
C:\chainsaw>chainsaw.exe search DomainName -i "EVTX-ATTACK-SAMPLES-master\Credential Access"
```

DOMINIOS:

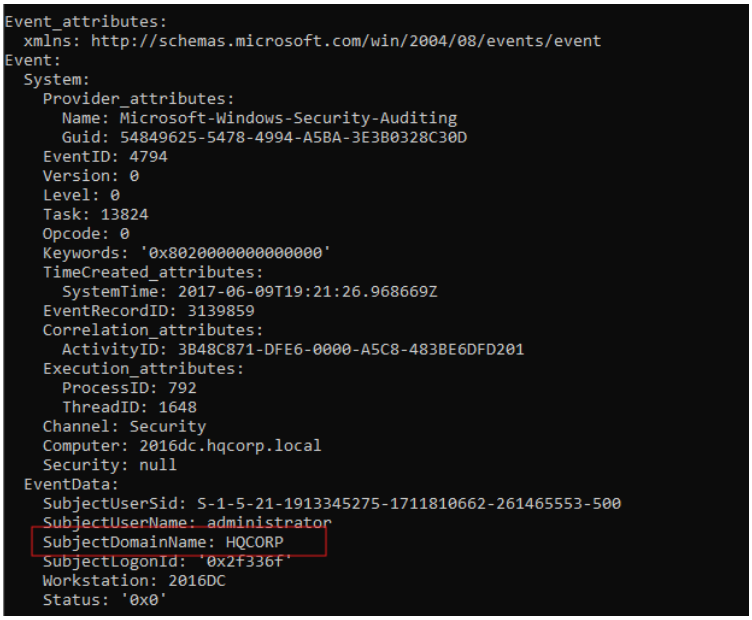
- Insecurebank:



-3B - THREEBEESCO.COM:



- hqcorp:



4. **Indicar si ha habido algún ataque de fuerza bruta a los servicios de bases de datos SQL:**

```
C:\chainsaw>chainsaw.exe search SQL -i "EVTX-ATTACK-SAMPLES-master\Credential Access"
```

A. Indicar IP de origen que realiza el ataque.

IP: 10.0.2.17

B. Indicar hostname del equipo.

HOSTNAME: MSEDGEWIN10

A. Indicar nombre del servicio de base de datos atacado.

SERVICIO: MSSQLSERVER

5. **Indicar si se ha realizado algún dump (volcado de información) a través de powershell.**

```
C:\chainsaw>chainsaw.exe hunt "EVTX-ATTACK-SAMPLES-master\Credential Access" -s sigma-master\rules\windows\powershell --mapping mappings\sigma-event-logs-all.yml --full
```

```
C:\chainsaw>chainsaw.exe search "lsass.dmp" "EVTX-ATTACK-SAMPLES-master\Credential Access"
```

A. Indicar Hostname del equipo donde se realizó el volcado de información.

HOSTNAME: MSEDGEWIN10

B. Indicar ruta y nombre del archivo powershell ejecutado.

RUTA: C:\Users\Public\lsass_wer_ps.ps1

C. Indicar ruta y nombre del archivo dump generado.

RUTA: C:\Users\IEUser\Desktop\lsass.dmp