PLAYBOOK BLUE TEAM #1 / PLAYBOOK BLUE TEAM #1

Investigación de actividad sospechosa en logs (login + frecuencia + IOCs)

/ Investigating suspicious activity in logs (login + frequency + IOCs)

1. PROPÓSITO / PURPOSE

ES:

Establecer un proceso claro y repetible para investigar actividad sospechosa en registros (logs) relacionada con:

- intentos de acceso (login failures)

- frecuencia de intentos

- IPs y dominios sospechosos (IOCs)

EN:

Establish a clear, repeatable process to investigate suspicious activity in logs related to:

- access attempts (login failures)

- attempt frequency

- suspicious IPs and domains (IOCs)

2. ALCANCE / SCOPE

ES:

Este playbook aplica a investigaciones iniciales (nivel 1) en:

- servidores Linux/macOS

- equipos de usuario (endpoints)

- aplicaciones que registran intentos de autenticación y conexiones salientes

No cubre:

- análisis forense profundo

- respuesta completa a incidentes (IR) a gran escala

EN:

This playbook applies to initial (tier 1) investigations on:

- Linux/macOS servers

- user endpoints

- applications that log authentication attempts and outbound connections

It does not cover:

- deep forensic analysis

- full-scale incident response (IR)

3. SEÑALES DE ALERTA (IOAs / IOCs) / ALERT SIGNALS (IOAs / IOCs)

ES:

Indicadores que deben disparar una investigación:

- Múltiples intentos fallidos de login en poco tiempo.

- Muchos errores desde la misma IP.

- Conexiones salientes repetidas a la misma IP externa poco conocida.

- Conexiones a dominios sospechosos (ej. "malware", "suspicious", "evil", "update" raro).

- Correlación entre intentos de fuerza bruta y tráfico saliente hacia la misma IP.

EN:

Indicators that should trigger an investigation:

- Multiple failed login attempts in a short time window.

- Many errors from the same IP address.

- Repeated outbound connections to the same unknown external IP.

- Connections to suspicious domains (e.g., containing "malware", "suspicious", "evil", odd "update").

- Correlation between brute-force attempts and outbound traffic to the same IP.

4. HERRAMIENTAS BÁSICAS (CLI) / BASIC CLI TOOLS

ES (explicado simple):

- grep: buscar líneas que contengan una palabra/frase.

- wc -l: contar líneas.

- | (pipe): pasar el resultado de un comando al siguiente.

- sort: ordenar líneas.

- uniq -c: agrupar y contar líneas iguales.

- cut: extraer columnas específicas de una línea.

EN (simple explanation):

- grep: search for lines containing a word or phrase.

- wc -l: count lines.

- | (pipe): pass the output of one command into the next.

- sort: sort lines.

- uniq -c: group and count identical lines.

- cut: extract specific columns from a line.

5. PROCEDIMIENTO PASO A PASO / STEP-BY-STEP PROCEDURE

5.1. Recolección de contexto / Context collection

ES:

1) Identificar el archivo de logs relevante (ej.: auth.log, system.log, app.log).

2) Confirmar periodo de tiempo a analizar (ej.: última hora, último día).

3) Trabajar siempre sobre una copia si es posible.

EN:

1) Identify the relevant log file (e.g., auth.log, system.log, app.log).

2) Confirm the time window to analyze (e.g., last hour, last day).

3) If possible, work on a copy of the log file.

5.2. Detectar intentos fallidos de login / Detect failed login attempts

ES:

Ejemplo de comando:

grep "ERROR" servidor.log

Para contar el total:

grep "ERROR" servidor.log | wc -l

EN:

Example command:

grep "ERROR" server.log

To count total:

grep "ERROR" server.log | wc -l

5.3. Analizar frecuencia por minuto / Analyze frequency per minute

ES:

Ejemplo:

grep "11:00" servidor.log | grep "ERROR" | wc -l

grep "11:01" servidor.log | grep "ERROR" | wc -l

Interpretación:

- Valores muy altos en pocos minutos pueden indicar ataque automatizado (fuerza bruta).

EN:

Example:

grep "11:00" server.log | grep "ERROR" | wc -l

grep "11:01" server.log | grep "ERROR" | wc -l

Interpretation:

- High numbers in a short period can indicate automated brute-force activity.

5.4. Identificar IPs más activas / Identify most active IPs

ES (versión simple conceptual):

1) Filtrar solo las líneas con errores:

grep "ERROR" servidor.log

2) (Opcional avanzado) Extraer la columna donde aparece la IP, ordenar y contar:

grep "ERROR" servidor.log | sort | uniq -c

EN (conceptual simple):

1) Filter only error lines:

grep "ERROR" server.log

2) (Optional, more advanced) Extract the IP column, sort and count:

grep "ERROR" server.log | sort | uniq -c

Nota:

En este curso, primero se entiende el concepto; luego se practica la extracción de columnas con cut/awk.

5.5. Buscar IOCs de dominios / Search for domain IOCs

ES:

Ejemplos:

grep "evil-domain" ioc.log

grep -E "malware|suspicious|evil" ioc.log

EN:

Examples:

grep "evil-domain" ioc.log

grep -E "malware|suspicious|evil" ioc.log

5.6. Clasificar tráfico normal vs sospechoso / Classify normal vs suspicious traffic

ES:

Marcar como normal:

- DNS conocidos (8.8.8.8, 1.1.1.1, etc.).

- Dominios legítimos (ej.: updates.microsoft.com).

- IPs internas (192.168.x.x, 10.x.x.x) en contexto esperado.

Marcar como sospechoso:

- IPs externas que aparecen también en ataques previos.

- Dominios con nombres claramente maliciosos o extraños.

- Conexiones repetidas a la misma IP poco común.

EN:

Mark as normal:

- Known DNS servers (8.8.8.8, 1.1.1.1, etc.).

- Legitimate domains (e.g., updates.microsoft.com).

- Internal IP ranges (192.168.x.x, 10.x.x.x) when expected.

Mark as suspicious:

- External IPs that also appear in previous attacks.

- Domains with clearly malicious or odd names.

- Repeated connections to the same unusual IP.

6. TABLA DE DECISIONES / DECISION TABLE

ES:

| Evidencia | Severidad | Acción sugerida |

|---|---|---|

| 1–2 intentos fallidos aislados | Baja | Monitorizar |

| 5+ fallos en 1–2 minutos | Media | Revisar host y usuario |

| 10+ fallos en pocos minutos | Alta | Bloquear IP temporalmente |

| IP coincide con IOC previo | Alta | Bloquear IP y revisar más logs |

| Dominio malicioso confirmado | Crítica | Aislar host y activar respuesta a incidente |

EN:

| Evidence | Severity | Suggested action |

|---|---|---|

| 1–2 isolated failed attempts | Low | Monitor |

| 5+ failures within 1–2 minutes | Medium | Review host and user |

| 10+ failures in a few minutes | High | Temporarily block IP |

| IP matches a previous known IOC | High | Block IP and review additional logs |

| Confirmed malicious domain | Critical | Isolate host and trigger incident response |

7. RECOMENDACIONES GENERALES / GENERAL RECOMMENDATIONS

ES:

- Documentar siempre comandos utilizados y hallazgos.

- Correlacionar múltiples fuentes de logs (login, red, aplicaciones).

- Actualizar este playbook cuando aparezcan nuevos IOCs o técnicas.

- Practicar con archivos de prueba como los utilizados en las Investigaciones SOC #1, #2 y #3.

EN:

- Always document commands used and key findings.

- Correlate multiple log sources (login, network, applications).

- Update this playbook when new IOCs or techniques appear.

- Practice with test files like those used in SOC Investigations #1, #2, and #3.

8. PLANTILLA DE INFORME RÁPIDO / QUICK REPORT TEMPLATE

ES:

Título:

SOC Incident Report – [tipo de incidente]

Resumen:

Breve descripción de lo detectado (qué, cuándo, dónde).

Hallazgos:

- [IP sospechosa]

- [dominios maliciosos]

- [frecuencia de intentos]

Conclusión:

Evaluación del riesgo y posible impacto.

Recomendaciones:

Acciones concretas a tomar.

EN:

Title:

SOC Incident Report – [incident type]

Summary:

Short description of what was detected (what, when, where).

Findings:

- [suspicious IP]
- [malicious domains]
- [attempt frequency]

Conclusion:

Risk evaluation and potential impact.

Recommendations:

Concrete actions to be taken.