Laboratorio 5.1 – Analisi di un incidente di sicurezza simulato

1. Panoramica del laboratorio

1.1 Descrizione del laboratorio

In questo laboratorio vestirai i panni di un **analista della sicurezza che risponde a un incidente**. Utilizzando uno scenario simulato, seguirai l'intero **ciclo di vita della risposta agli incidenti**:

- Indagare su avvisi e registri.
- Identifica gli indicatori di compromissione (IOC).
- Contenere, eliminare e riprendersi dalla minaccia.
- Documentare le azioni intraprese e le prove raccolte.
- Conduci una revisione post-incidente con le lezioni apprese.

Questo esercizio combina competenze tecniche (analisi dei log, azioni di risposta) con **pensiero critico e reporting strutturato**: esattamente ciò che fanno i team di sicurezza informatica nel mondo reale quando rispondono agli attacchi.

1.2 Obiettivi di apprendimento

Dopo aver completato questo laboratorio, sarai in grado di:

- Analizzare i log per identificare attività sospette e confermare gli incidenti.
- Riconoscere e documentare **gli indicatori di compromissione (IOC)**.
- Applicare il modello di risposta **Contenere → Sradicare → Recuperare**.
- Conservare le prove mantenendo **la catena di custodia**.
- Completare un **rapporto di risposta agli incidenti** (cronologia, sistemi, account, azioni).
- Condurre una **revisione post-incidente** e proporre miglioramenti in materia di rilevamento, politiche e formazione.

1.3 Prerequisiti

Prima di iniziare questo laboratorio, è necessario:

- Comprendere le nozioni di base sul **ciclo di vita della risposta agli incidenti** (NIST o simili).

- Essere in grado di esaminare i log di sistema e riconoscere modelli insoliti.
- Avere accesso a:
    - Un **set di dati di log** (fornito nei materiali del corso o dalle indicazioni del docente).
    - Un editor di testo o un foglio di calcolo per organizzare i risultati.
    - **Un modello di risposta agli incidenti** (cronologia, azioni, passaggi successivi).

Facoltativo ma consigliato: familiarità con i concetti SIEM e le pratiche forensi di base.

1.4 Tempo di completamento stimato

Attività	**Tempo stimato**
Introduzione allo scenario Revisione dell'allerta C	30
minuti Revisione dei log Identificazione degli IOC C	45 minuti
Fasi di risposta all'incidente	60 minuti
Documentazione C Gestione delle prove	45 minuti
Revisione post-incidente C lezioni apprese	30-45 minuti
Conclusioni C riflessione	15 minuti
Tempo totale stimato	**~4–4,5 ore**

Punto di controllo
Prima di proseguire, assicurati di:

- Comprendi lo scopo di questa simulazione (esercitarsi sul ciclo di vita completo di un incidente).
- Hai a disposizione i file di log, il modello e gli strumenti per prendere appunti.
- Di poter dedicare circa **4–4,5 ore** al completamento dell'esercitazione.

2. Configurazione dello scenario – L'avviso iniziale

2.1 Contesto

È notte fonda, sono **le 2:41 del mattino**, quando il sistema **SIEM (Security Information and Event Management)** della tua organizzazione genera un allarme. In qualità di analista di turno, devi determinare se si tratta di:

- Un'anomalia innocua, oppure
- **un incidente di sicurezza** legittimo **in corso**.

2.2 Dettagli dell'allarme

L'allarme SIEM include i seguenti indicatori sospetti:

- **Attività di accesso**: accesso riuscito dall'indirizzo IP 203.0.113.41.
- **Account utente**: il login ha utilizzato l'account **dbadmin**, che normalmente funziona solo durante l'orario di lavoro.
- **Ora di accesso**: **2:41 del mattino**, ben al di fuori dei normali modelli di utilizzo.
- **Attività di follow-up**: improvviso picco nel **traffico di rete in uscita** dal server del database delle risorse umane dell'azienda verso un server FTP esterno.

2.3 Il tuo ruolo

Il tuo ruolo è quello di **responsabile della risposta agli incidenti**. Le tue responsabilità sono:

1. **Esaminare** attentamente **l'allerta**.
2. **Raccogliere ulteriori prove** dai registri e dall'attività di rete.
3. **Decidere** se si tratta di un falso positivo o di un incidente confermato.
4. **Agire** se necessario.

Suggerimento: non saltare a conclusioni affrettate basandoti solo sull'avviso, ma consideralo come un punto di partenza per l'indagine.

2.4 Obiettivi dell'indagine

In questa fase, i tuoi obiettivi sono:

- Verificare se l'accesso era legittimo.
- Determinare se l'esfiltrazione dei dati era **autorizzata** o **dolosa**.
- Identificare eventuali **indicatori** precoci **di compromissione (IOC)** per approfondire l'indagine nelle fasi successive.

Punto di controllo
Prima di proseguire:

- Hai compreso i dettagli dell'avviso iniziale (ora, account, IP, trasferimento dati)?
- Hai un modo per prendere appunti mentre esamini i log e costruisci la tua cronologia?
- Sei pronto per iniziare **la revisione dei registri e l'identificazione degli IOC**?

3. Revisione dei log e identificazione degli IOC

3.1 Revisione dei registri di autenticazione

Il primo passo consiste nel controllare i **registri di autenticazione** per ottenere dettagli sul login sospetto.

I registri mostrano:

```
2025-09-21 02:41:06 LOGIN RIUSCITO utente=dbadmin ip=203.0.113.41
21/09/2025 09:15:42 LOGIN RIUSCITO utente=dbadmin ip=10.0.2.15
2025-09-20 14:05:33 LOGIN RIUSCITO utente=dbadmin ip=10.0.2.15
```

Osservazioni:

- **Il login** delle **2:41 AM** risulta insolito.
- I login precedenti provenivano da un **IP interno (10.0.2.15)** durante l'orario di lavoro.
- Il login sospetto proveniva da un **IP esterno straniero (203.0.113.41)**.

3.2 Registri di accesso ai file

Successivamente, controlla i registri di accesso ai file sul server del database delle risorse umane.

```
2025-09-21 02:43:11 ACCESSO AI FILE utente=dbadmin /HR/employee_records.xlsx
2025-09-21 02:44:27 ACCESSO AI FILE utente=dbadmin /HR/salary_data.csv
21/09/2025 02:45:03 ACCESSO AI FILE utente=dbadmin /HR/benefits.docx
```

Osservazioni:

- I file sensibili delle risorse umane sono stati consultati immediatamente dopo l'accesso sospetto.
- Questi file vengono consultati raramente al di fuori dei cicli mensili di elaborazione delle buste paga.

3.3 Registri delle attività di rete

Infine, esamini i registri del traffico di rete.

```
21/09/2025 02:46:10 TRASFERIMENTO IN USCITA utente=dbadmin server=203.0.113.50 protocollo=FTP
dimensione=1,2 GB 21/09/2025 02:49:55 TRASFERIMENTO IN USCITA utente=dbadmin server=203.0.113.50
protocollo=FTP dimensione=850 MB
```

Osservazioni:

- Grandi quantità di dati sono state esfiltrate su un **server FTP esterno.**
- Il traffico normale del database utilizza solitamente **SQL sulla porta 1433**, non FTP.

3.4 Identificazione degli indicatori di compromissione (IOC)

Dalla revisione dei log, si identificano i seguenti IOC:

- **Indirizzo IP sospetto**: 203.0.113.41 (origine del login).
- **Ora di accesso insolita**: 2:41 del mattino.
- **Account utilizzato**: dbadmin (probabilmente compromesso).
- **File sensibili consultati**: documenti relativi alle risorse umane e dati relativi alle buste paga.
- **Traffico in uscita**: trasferimenti FTP di grandi dimensioni verso 203.0.113.50.

3.5 Conferma dell'incidente

A questo punto, le prove indicano che si tratta di un **incidente confermato**:

- Accesso esterno da IP insolito → **Accesso non autorizzato**.
- Accesso ai dati delle risorse umane → **Informazioni sensibili a rischio**.
- Trasferimenti FTP in uscita di grandi dimensioni → **Esfiltrazione dei dati**

confermata. **Conclusione: non** si tratta di **un falso positivo**, è necessario avviare le

azioni di contenimento.

Punto di controllo
Prima di proseguire:

- Hai identificato almeno **tre IOC** dai log?
- Capisci perché si tratta di una violazione confermata?
- Sei pronto ad adottare **misure di risposta agli incidenti**?

4. Misure di risposta agli incidenti

4.1 Contenimento

La prima priorità è **impedire che l'attacco continui**. Azioni da intraprendere immediatamente:

1. **Disattiva l'account compromesso** (dbadmin).
2. **Isolare il server interessato** dalla rete per impedire un'ulteriore fuga di dati.
3. Informare **il responsabile del team di risposta agli incidenti (IR)** e segnalare l'accaduto secondo la procedura prevista. Obiettivo: contenere la minaccia prima che si diffonda ulteriormente.

4.2 Eradicazione

Una volta contenuta la minaccia, concentrarsi sulla **rimozione della presenza dell'autore dell'attacco**. I passaggi includono:

- Eseguire una scansione del sistema interessato alla ricerca di **malware, rootkit o backdoor**.
- Rimuovere eventuali file dannosi o attività pianificate non autorizzate.
- Verificare la presenza di **account secondari compromessi** creati dall'autore dell'attacco. Obiettivo: garantire che l'autore dell'attacco non abbia più accesso.

4.3 Ripristino

Dopo l'eliminazione, procedere al **ripristino delle normali operazioni**:

1. Ripristinare il sistema compromesso da un **backup pulito noto**.
2. Applicare **le patch di sicurezza** e aggiornare le configurazioni prima di riportarlo online.
3. Monitorare attentamente il sistema per individuare eventuali segni di attività dannose ricorrenti. Obiettivo: tornare alla normalità con difese migliorate.

4.4 Documentazione delle azioni di risposta

Durante le fasi di contenimento → eradicazione → ripristino:

- Registrare **i timestamp** di ogni azione.
- Annotare **chi ha eseguito l'azione**.
- Assicurarsi che le azioni siano registrate nel **rapporto** ufficiale **di risposta agli incidenti**. Questa documentazione è fondamentale per la conformità, la segnalazione e l'apprendimento.

Punto di controllo
Prima di proseguire:

- Hai acquisito tutte e tre le fasi (Contenimento → Eliminazione → Ripristino)?
- Hai iniziato a documentare ogni azione con l'ora e i dettagli?
- Capisci perché il recupero deve includere il monitoraggio?

5. Documentazione e gestione delle prove

5.1 Perché la documentazione è importante

Ogni azione intrapresa durante un incidente deve essere **registrata e contrassegnata con l'ora**.

- Crea una **cronologia chiara** di ciò che è accaduto e quando.
- Fornisce prove per **la revisione post-incidente** e le indagini legali.
- Garantisce la conformità alle **politiche** e ai quadri normativi **dell'organizzazione** (ad esempio ISO 27001, NIST, GDPR).

5.2 Conservazione dei registri

I log sono la vostra prova principale. Proteggeteli prima che vengano sostituiti o cancellati.

- Esporta i registri degli avvisi SIEM.
- Copiate i registri di autenticazione del sistema.
- Salvate i registri del traffico di rete.
- Assicurati che i backup siano archiviati in una **posizione di sola lettura**.

Suggerimento: conserva sempre la **copia originale intatta** e lavora sui duplicati.

5.3 Acquisizione di dati volatili

Alcune prove scompaiono rapidamente se non vengono acquisite immediatamente.

- Dump della memoria del server compromesso (contenuto della RAM).
- Elenchi dei processi attivi e connessioni di rete.
- Screenshot di sessioni sospette.

5.4 Catena di custodia

Per mantenere l'integrità, seguire una procedura **di catena di custodia**:

1. Registrare **chi ha raccolto le prove**, **quando** e **come**.

2. Conservare le prove in modo sicuro (ad esempio, su un'unità crittografata o in un armadietto forense).
3. Documentare ogni passaggio di consegne in caso di trasferimento delle prove.

Ciò garantisce che le prove siano **legalmente difendibili** e a prova di manomissione.

5.5 Compilazione del rapporto sull'incidente

Il modello di risposta agli incidenti dovrebbe includere:

- **Cronologia degli eventi** (allerta, rilevamento, risposta).
- **Sistemi interessati**.
- **Account coinvolti**.
- **Azioni intraprese**.
- **Prossimi passi da compiere**.

Punto di controllo
Prima di proseguire:

- Hai esportato e conservato tutti i registri rilevanti?
- Hai acquisito tutte le prove volatili prima che andassero perse?
- Hai registrato le azioni nel rapporto sull'incidente con indicazione dell'ora?
- Hai mantenuto la catena di custodia per tutte le prove critiche?

6. Revisione post-incidente e lezioni apprese

6.1 Perché le revisioni post-incidente sono importanti

La risoluzione di un incidente non è la fine, ma l'**inizio di un processo di miglioramento**. Una revisione strutturata garantisce che:

- Le cause alla radice siano comprese.
- Le regole di rilevamento siano aggiornate.
- I team imparano dagli errori e dai successi.
- L'organizzazione diventa più resiliente.

6.2 Esamina i risultati

Dopo il contenimento e il ripristino, riunire il team di risposta agli incidenti per esaminare:

- **Cronologia degli eventi** (allerta → indagine → contenimento → ripristino).
- **La rapidità con cui il team ha risposto**.
- **Cosa ha funzionato bene** (ad esempio, rilevamento rapido, escalation efficace).
- **Cosa non ha funzionato** (ad esempio, monitoraggio debole,

comunicazione ritardata). Documentare questi risultati nel rapporto

ufficiale.

6.3 Miglioramenti da implementare

Sulla base dei risultati ottenuti, intraprendere azioni volte a rafforzare le difese:

- **Regole di rilevamento** → Aggiornare SIEM per segnalare tempi di accesso insoliti o trasferimenti FTP.
- **Firewall** → Bloccare gli IP sospetti e limitare il traffico FTP in uscita.
- **Formazione degli utenti** → Organizza sessioni di sensibilizzazione sulla sicurezza degli account e sulla segnalazione di attività sospette.
- **Manuali di gestione degli incidenti** → Aggiungere questo scenario ai manuali operativi per una risposta più rapida in futuro.

6.4 Formazione del team

Anche la revisione post-incidente è **un'opportunità di apprendimento**:

- Condividere le lezioni apprese tra i reparti IT, sicurezza e leadership.
- Eseguire **un'esercitazione teorica** per provare lo stesso scenario.
- Aggiornare l'inserimento dei nuovi membri del team con gli insegnamenti tratti

da questo incidente. Ogni incidente è un'occasione per affinare le competenze del team.

6.5 Esempi di lezioni apprese (da questo scenario di laboratorio)

- Gli account amministrativi condivisi (dbadmin) rappresentano un rischio → Implementare il principio del privilegio minimo e il monitoraggio.
- Il traffico FTP in uscita deve essere **monitorato o limitato**.
- Gli accessi fuori orario dovrebbero attivare **avvisi per impostazione predefinita**.
- La documentazione degli incidenti deve essere standardizzata e rivista regolarmente.

Punto di controllo
Prima di proseguire:

- Hai riassunto cosa ha funzionato e cosa non ha funzionato in questo incidente?
- Hai proposto almeno **due miglioramenti** relativi a strumenti, politiche o formazione?
- Hai registrato le lezioni apprese per incidenti futuri e le hai condivise con il tuo team?

7. Conclusioni

7.1 Punti chiave

In questo laboratorio hai completato **un'esercitazione simulata di risposta agli incidenti** che ha riunito l'intero ciclo di vita della risposta alla sicurezza informatica. Hai:
Hai esaminato un avviso proveniente da un SIEM.
Identificato gli indicatori di compromissione (IOC) nei registri e nei dati di rete.
Applicato il framework di risposta **Contenere → Sradicare → Recuperare**.
Conservato le prove e mantenuto una catena di custodia adeguata.
Documentato la cronologia dell'incidente e le azioni intraprese in un rapporto formale. Condotto una revisione post-incidente e identificato le lezioni apprese.

7.2 Competenze acquisite

Al termine di questo laboratorio, sarai in grado di:

- Analizzare i registri per confermare o respingere attività sospette.
- Rispondere in modo sistematico agli incidenti utilizzando le migliori pratiche.
- Creare **rapporti** professionali **sugli incidenti** con cronologie, azioni e prove.
- Proporre **miglioramenti** attuabili in materia di rilevamento, risposta e formazione degli utenti.

7.3 Passo successivo: Quiz finale del Modulo 5

Hai completato il **laboratorio pratico finale del Modulo 5: Rilevamento delle minacce e risposta agli incidenti**.

Il passo successivo è sostenere il **quiz finale del Modulo 5**, che tratterà:

- Concetti relativi al rilevamento delle minacce (avvisi, IOC, nozioni di base sul SIEM).
- Ciclo di vita della risposta agli incidenti (contenimento, eliminazione, ripristino).
- Gestione delle prove e catena di custodia.
- Revisione post-incidente e miglioramento continuo.

Punto di controllo finale

Prima di passare al quiz:

- Hai completato e salvato il tuo rapporto di risposta agli incidenti?
- Siete in grado di spiegare chiaramente cosa ha reso questo incidente una **violazione confermata**?
- Siete in grado di riassumere **tre lezioni apprese** da questo

laboratorio? Se sì, siete pronti per il quiz!

8. Appendice

8.1 Modello di risposta agli incidenti

Utilizza questo modello per strutturare la documentazione relativa agli incidenti:

Campo	Dettagli
ID dell'incidente	[Identificatore univoco]
Data/ora di rilevamento	[ad es., 21/09/2025 alle 02:41]
Segnalato da	[SIEM / Analista / Utente]
Sistemi interessati	[Server database, file HR]
Account coinvolti	[dbadmin]
Indicatori di compromissione (IOC)	[IP sospetti, accessi anomali, trasferimenti FTP] Azioni
di contenimento	[Account disabilitato, server isolato]
Azioni di eradicazione	[Scansione malware, rimozione backdoor]
Azioni di ripristino	[Ripristino da backup pulito]
Prove raccolte	[Log, dump della memoria, modulo della catena
di custodia] Passi successivi	[Blocco degli IP, aggiornamento delle regole
SIEM, formazione degli utenti]	
Stato	[In corso / Chiuso]

8.2 Elenco di riferimento degli indicatori di compromissione (IOC)

Categorie IOC comuni da tenere sotto controllo:

- **Registri di autenticazione** → Orari di accesso insoliti, IP estranei, ripetuti tentativi falliti seguiti da tentativi riusciti.
- **Attività dei file** → Accessi insoliti a directory sensibili, trasferimenti di file di grandi dimensioni.
- **Traffico di rete** → Connessioni in uscita verso IP sconosciuti, protocolli anomali (ad esempio FTP invece di HTTPS).

- **Attività dei processi** → Servizi imprevisti, attività pianificate o esecuzione di comandi.

Suggerimento: verificare sempre gli IOC con **feed di intelligence sulle minacce noti** per conferma.

8.3 Errori comuni nella risposta agli incidenti

- **Passare direttamente al contenimento** senza confermare l'incidente.
- **Mancata documentazione delle azioni** mentre vengono eseguite.
- **Mancata conservazione delle prove volatili** (RAM, connessioni attive).
- **Ignorare la catena di custodia**, che può invalidare le prove in contesti legali.
- **Saltare la revisione post-incidente**, perdendo opportunità per migliorare le difese.

8.4 Ulteriori letture e risorse

- **Guida alla gestione degli incidenti di sicurezza informatica del NIST (SP 800-61r2)**
  https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
- **Manuale per la gestione degli incidenti SANS**
  https://www.sans.org/white-papers/33901/
- Migliori pratiche **FIRST (Forum of Incident Response and Security Teams)**
  https://www.first.org/
- **MITRE ATTsCK Framework** – Per mappare le tecniche e i comportamenti degli aggressori https://attack.mitre.org/

Lettura consigliata: *Incident Response & Computer Forensics* (Luttgens, Pepe, Mandia).