

Benchmark W24D4

Cosa è Splunk

Breve descrizione su cosa sia il software, che cosa fa, e il perchè è utile in ambito di cyber security

Analisi con query

Dopo aver importato i dati dal file di prova “tutorialdata.zip” posso elaborarli con delle query e trarre conclusioni sui log analizzati utilizzando l'Al.

Identificazione tentativi di accesso falliti

```
source="tutorialdata.zip:*" sourcetype="www1/secure" host="Daniele" "failed password"  
| rex "Failed password for (invalid user )?(?< user>\w+) from (?<src_ip>\d+.\d+.\d+.\d+)"  
| eval failure_reason=if(match(_raw, "invalid user"), "Invalid User", "Incorrect Password")  
| table _time src_ip user failure_reason
```

la query mostra il timestamp, il motivo del fallimento, il nome utente e l'indirizzo IP di origine:

splunk>enterprise App ▾

Ricerca Analytics Set di dati Report Allarmi Dashboard

Nuova ricerca Salva come ▾ Crea vista tabella Chiudi

```
source="tutorialdata.zip:*" sourcetype="www1/secure" host="Daniele" "failed password"
| rex "Failed password for (invalid user )?(?<user>\w+) from (?<src_ip>\d+\.\d+\.\d+\.\d+)"
| eval failure_reason=if(match(_raw, "invalid user"), "Invalid User", "Incorrect Password")
| table _time src_ip user failure_reason
```

✓ 33.253 eventi (prima di 03/11/24 22:23:25.000) Nessun campionamento degli eventi ▾

Processo ▾ || ▢ ↻ 🗑️ ⬇️ 🔍 Modalità intelligente ▾

Eventi Pattern **Statistiche (33.253)** Visualizzazione

20 per pagina ▾ ✓ Formato Anteprima ▾

_time ▾	src_ip ▾	user ▾	failure_reason ▾
2024-10-28 04:37:05	194.215.205.19	desktop	Invalid User
2024-10-28 04:37:05	194.215.205.19	rdb	Invalid User
2024-10-28 04:37:05	194.215.205.19	games	Incorrect Password
2024-10-28 04:37:05	194.215.205.19	library	Invalid User
2024-10-28 04:37:05	87.194.216.51	nagios	Incorrect Password
2024-10-28 04:37:05	87.194.216.51	helpdesk	Invalid User
2024-10-28 04:37:05	87.194.216.51	fpass	Invalid User
2024-10-28 04:37:05	87.194.216.51	vpuser	Invalid User
2024-10-28 04:37:05	87.194.216.51	uni	Invalid User
2024-10-28 04:37:05	87.194.216.51	sys	Invalid User
2024-10-28 04:37:05	87.194.216.51	mysql	Invalid User
2024-10-28 04:37:05	87.194.216.51	system	Invalid User
2024-10-28 04:37:05	87.194.216.51	vmware	Invalid User

Attiva Windows
Passa a Impostazioni per attivare Windows.

Identificazione sessioni SSH aperte con successo

source="tutorialdata.zip:*" sourcetype="www1/secure" host="Daniele" "Accepted password" "djohnson" | rex "sshd[(?<session_id>\d+)]: Accepted password for (?< user>\w+)" | where user="djohnson"| eval status="Success" | table _time user session_id status

Filtrando per l'utente "djohnson" ottengo le seguenti sessioni:

splunk enterprise App ▾

splunk > listen to your data

Ricerca Analytics Set di dati Report Allarmi Dashboard

Nuova ricerca Salva come ▾ Crea vista tabella Chiudi

source="tutorialdata.zip:*" sourcetype="www1/secure" host="Daniele" "Accepted password" "djohnson" | rex "sshd\[(<session_id>\d+)\]: Accepted password for (?<user>\w+)" | where user="djohnson" | eval status="Success" | table _time user session_id status

✓ 955 eventi (prima di 03/11/24 22:31:39,000) Nessun campionamento degli eventi ▾

Processo ▾ || ▢ → ↻ ⬇ ⚙ Modalità intelligente ▾

Eventi Pattern **Statistiche (955)** Visualizzazione

20 per pagina ▾ ✓ Formato Anteprima ▾

_time ↕	user ↕	session_id ↕	status ↕
2024-10-30 04:37:04	djohnson	57740	Success
2024-10-30 04:37:04	djohnson	27688	Success
2024-10-30 04:37:04	djohnson	95467	Success
2024-10-30 04:37:04	djohnson	98759	Success
2024-10-30 04:37:04	djohnson	99654	Success
2024-10-30 04:37:04	djohnson	45962	Success
2024-10-30 04:37:04	djohnson	94001	Success
2024-10-30 04:37:04	djohnson	52325	Success
2024-10-30 04:37:04	djohnson	83594	Success
2024-10-30 04:37:04	djohnson	41627	Success
2024-10-30 04:37:04	djohnson	50467	Success
2024-10-30 04:37:04	djohnson	89967	Success
2024-10-30 04:37:04	djohnson	48946	Success
2024-10-30 04:37:04	djohnson	84890	Success

Attiva Windows
Passa a Impostazioni per attivare Windows.

Ricerca tentativi di accesso falliti

```
source="tutorialdata.zip:*" sourcetype="www1/secure" host="Daniele" ("failed password" OR "Accepted password")
| rex "password for (invalid user )?(?< user>\w+) from (?< src_ip>86.212.199.60) port (?< port>\d+)"
| eval status=if(searchmatch("failed password"), "Failed", "Success")
| where src_ip="86.212.199.60"
| table _time src_ip user port status
```

Daniele Zoccheddu

Messaggi

Impostazioni

Attività

Guida

Trova

RicercaAnalyticsSet di datiReportAllarmiDashboard

Nuova ricercaSalva comeCrea vista tabellaChi

```
source="tutorialdata.zip:*" sourcetype="www1/secure" host="Daniele" ("failed password" OR "Accepted password")  
| rex "password for (invalid user )?(?<user>\w+) from (?<src_ip>86\.\d{1,3}\.\d{1,3}\.\d{1,3}) port (?<port>\d+)"  
| eval status=if(searchmatch("failed password"), "Failed", "Success")  
| where src_ip="86.212.199.60"  
| table _time src_ip user port status
```

✓ 158 eventi (prima di 03/11/24 22:38:08,000) Nessun campionamento degli eventiProcessoModalità intelligente

EventiPatternStatistiche (158)Visualizzazione

20 per paginaFormatoAnteprima

_time ↕	src_ip ↕	user ↕	port ↕	status ↕
2024-10-29 04:37:04	86.212.199.60	services	1393	Failed
2024-10-29 04:37:04	86.212.199.60	sync	1695	Failed
2024-10-29 04:37:04	86.212.199.60	admin	3673	Failed
2024-10-29 04:37:04	86.212.199.60	nginx	1582	Failed
2024-10-29 04:37:04	86.212.199.60	whois	1635	Failed
2024-10-29 04:37:04	86.212.199.60	mailman	4339	Failed
2024-10-29 04:37:04	86.212.199.60	mailman	1954	Failed
2024-10-29 04:37:04	86.212.199.60	rdb	2650	Failed
2024-10-28 04:37:04	86.212.199.60	ncsd	4022	Failed
2024-10-28 04:37:04	86.212.199.60	games	1763	Failed
2024-10-28 04:37:04	86.212.199.60	noone	1582	Failed
2024-10-28 04:37:04	86.212.199.60	fpass	3420	Failed

Solitamente quando ci sono multipli tentativi errati di accesso da parte di uno stesso indirizzo IP in un sistema (fallendo di inserire correttamente la password) questo è indice di un possibile tentativo di bruteforcing. Questa query da gli indirizzi IP e il numero di tentativi di quelli che provano senza successo ad accedere per più di 5 volte:

```
source="tutorialdata.zip:*" sourcetype="www1/secure" host="Daniele" "failed password"
| rex "Failed password for (invalid user )?(?< user>\w+) from (?<src_ip>\d+.\d+.\d+.\d+)"
| stats count by src_ip
| where count > 5
| table src_ip count
```

splunk>enterprise App ▾

Ricerca Analytics Set di dati Report Allarmi Dashboard

Nuova ricerca Salva come ▾ Crea vista tabella Chiudi

```
source="tutorialdata.zip:*" sourcetype="www1/secure" host="Daniele" "failed password"
| rex "Failed password for (invalid user )?(?<user>\w+) from (?<src_ip>\d+\.\d+\.\d+\.\d+)"
| stats count by src_ip
| where count > 5
| table src_ip count
```

✓ 33.253 eventi (prima di 03/11/24 22:42:27:000) Nessun campionamento degli eventi ▾ Processo ▾ || ▢ ↗ ⚙ ⬇ ⚡ Modalità intelligente ▾

Eventi Pattern **Statistiche (182)** Visualizzazione

20 per pagina ▾ ✓ Formato Anteprima ▾ < Prec 1 2 3 4 5 6 7 8 ... Avanti >

src_ip ↕	count ↕
107.3.146.207	281
108.65.113.83	248
109.169.32.135	514
110.138.30.229	163
110.159.208.78	125
111.161.27.20	85
112.111.162.4	118
117.21.246.164	194
118.142.68.222	91
12.130.60.4	227
12.130.60.5	155
121.254.179.199	182

Attiva Windows
Passa a Impostazioni per attivare Windows.

Ricerca Internal Server Error

Gli Internal Server Error sono errori generici che indicano che il server ha incontrato una condizione imprevista che gli ha impedito di soddisfare una richiesta.

```
source="tutorialdata.zip:*" sourcetype="access_combined_wcookie" host="Daniele"
("Internal Server Error" OR "500")
| eval status="Internal Server Error"
| table _time src_ip status_code error_message status
```

Splunk Enterprise interface showing a search query and results.

Nuova ricerca

source="tutorialdata.zip:*" sourcetype="access_combined_wcookie" host="Daniele"
("Internal Server Error" OR "500")
| eval status="Internal Server Error"|
| table _time src_ip status_code error_message status

781 eventi (prima di 03/11/24 22:47:39,000) Nessun campionamento degli eventi

Processo Visualizzazione

Eventi Pattern **Statistiche (781)** Visualizzazione

20 per pagina Formato Anteprima

_time	src_ip	status_code	error_message	status
2024-10-27 07:38:08				Internal Server Error
2024-10-27 06:39:31				Internal Server Error
2024-10-27 01:37:03				Internal Server Error
2024-10-27 01:34:17				Internal Server Error
2024-10-27 01:32:16				Internal Server Error
2024-10-27 01:02:45				Internal Server Error
2024-10-27 00:38:28				Internal Server Error
2024-10-27 00:13:33				Internal Server Error
2024-10-27 00:13:33				Internal Server Error
2024-10-26 22:36:02				Internal Server Error
2024-10-26 21:54:50				Internal Server Error
2024-10-26 19:26:28				Internal Server Error
2024-10-26 18:50:51				Internal Server Error

Conclusione tratte analizzando i log con la AI

Tentativi di Accesso Falliti:

Nei log relativi ai tentativi di accesso falliti ("Failed password"), è emerso che diversi indirizzi IP hanno ripetutamente tentato di accedere al sistema senza successo. Questi comportamenti potrebbero indicare:

- **Attività di forza bruta:** IP che eseguono numerosi tentativi falliti possono indicare tentativi di forza bruta, in cui un attaccante cerca di indovinare le credenziali.
- **Potenziale abuso di credenziali:** Alcuni utenti specifici possono essere presi di mira ripetutamente, suggerendo che l'attaccante abbia alcune informazioni preliminari sulle credenziali valide.

Accessi SSH di Successo per Utenti Specifici:

Le sessioni SSH aperte con successo dall'utente "djohnson" hanno mostrato accessi regolari e legittimi. Tuttavia, è importante considerare:

- **Monitoraggio degli utenti privilegiati:** L'account "djohnson" potrebbe essere amministrativo, quindi è essenziale monitorare questi accessi per individuare attività anomale, come connessioni fuori orario o da IP insoliti.

Tentativi di Accesso da un IP Specifico:

Analizzando i tentativi di accesso falliti provenienti dall'indirizzo IP **86.212.199.60**, è stato riscontrato un comportamento ripetitivo che suggerisce:

- **Attività sospette o dannose:** L'IP potrebbe far parte di un attacco mirato, con tentativi di accesso ripetuti verso utenti specifici e su porte definite.
- **Inserimento nella blacklist:** Si potrebbe considerare l'aggiunta di questo IP alla blacklist o l'implementazione di un sistema di rilevamento delle intrusioni (IDS) per prevenire futuri tentativi.

Indirizzi IP con Più di 5 Tentativi di Accesso Falliti:

Gli indirizzi IP con oltre 5 tentativi di accesso falliti rappresentano una potenziale minaccia. I modelli osservati indicano:

- **Potenziale attacco di forza bruta distribuita:** Se più IP eseguono tentativi ripetuti, potrebbe trattarsi di un attacco coordinato.
- **Segmentazione degli attacchi:** In alcuni casi, tali attacchi possono essere distanziati nel tempo per evitare il rilevamento; è fondamentale monitorare continuamente questi IP e implementare sistemi di difesa come firewall e strumenti di prevenzione delle intrusioni.

Errori di Server Interno (Internal Server Error):

Gli errori di tipo "Internal Server Error" (codice 500) possono indicare problemi nei servizi interni o nelle applicazioni web. Questi errori sono spesso associati a:

- **Problemi di configurazione o codice:** Gli errori 500 sono comunemente causati da configurazioni errate o problemi nel codice dell'applicazione; è cruciale che il team di sviluppo esamini i log per individuarne la causa.

- **Possibili vettori di attacco:** Gli errori 500, se correlati a input dell'utente, possono esporre vulnerabilità sfruttabili per attacchi di iniezione o altre tecniche di exploit.

Monitorare costantemente questi eventi e adottare misure preventive aiuta a mantenere la sicurezza del sistema e prevenire intrusioni o disservizi.