

Trovare Failed Password

Nuova ricerca Salva come ▾ Crea vista tabella Chiudi

source="tutorialdata.zip:*" host="LAPTOP-RQN1IRNJ" index="nadir" "failed password" Sempre ▾ 🔍

✓ **33.253 eventi** (prima di 02/11/24 20:05:54,000) Nessun campionamento degli eventi ▾

Processo ▾ || ■ ➔ 🖨️ ⬇️ ! Modalità intelligente ▾

Eventi (33.253) Pattern Statistiche Visualizzazione

Formato timeline ▾ — Zoom indietro + Zoom area selezionata × Deseleziona 1 ora per colonna

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

< Nascondi campi	☰ Tutti i campi	i	Ora	Evento
CAMPI SELEZIONATI		>	01/11/24 16:38:23,000	Thu Nov 01 2024 16:38:23 mailsv1 sshd[5276]: Failed password for invalid user appserver from 194.8.74.23 port 3351 ssh2 host = LAPTOP-RQN1IRNJ source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
a host 1		>	01/11/24 16:38:23,000	Thu Nov 01 2024 16:38:23 mailsv1 sshd[1039]: Failed password for root from 194.8.74.23 port 3768 ssh2 host = LAPTOP-RQN1IRNJ source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
a source 4		>	01/11/24 16:38:23,000	Thu Nov 01 2024 16:38:23 mailsv1 sshd[5258]: Failed password for invalid user testuser from 194.8.74.23 port 3626 ssh2 host = LAPTOP-RQN1IRNJ source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
a sourcetype 1		>	01/11/24 16:38:23,000	Thu Nov 01 2024 16:38:23 mailsv1 sshd[1165]: Failed password for apache from 194.8.74.23 port 4604 ssh2 host = LAPTOP-RQN1IRNJ source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
CAMPI INTERESSANTI		>	01/11/24 16:38:23,000	Thu Nov 01 2024 16:38:23 mailsv1 sshd[3760]: Failed password for invalid user mongodb from 194.8.74.23 port 2472 ssh2 host = LAPTOP-RQN1IRNJ source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
# date_hour 1		>	01/11/24 16:38:23,000	Thu Nov 01 2024 16:38:23 mailsv1 sshd[4998]: Failed password for mail from 194.8.74.23 port 1552 ssh2 host = LAPTOP-RQN1IRNJ source = tutorialdata.zip:\mailsv\secure.log sourcetype = www1/secure
# date_mday 8		>	01/11/24 16:38:23,000	Thu Nov 01 2024 16:38:23 mailsv1 sshd[1930]: Failed password for games from 194.8.74.23 port 3007 ssh2
# date_minute 1				
a date_month 2				
# date_second 4				
a date_wday 7				
# date_year 1				
a date_zone 1				
a index 1				
# linecount 1				
a punct 3				
a splunk_server 1				

Trovare richieste accettate con l'utente *djohnson*

splunk>enterpriseApp

AdministratorMessaggiImpostazioniAttivitàGuidaTrova

RicercaAnalyticsSet di datiReportAllarmiDashboard

Nuova ricercaSalva comeCrea vista tabellaChiudi

source="tutorialdata.zip:*" host="LAPTOP-RQN1IRNJ" index="nadir" "accepted password" "djohnson" "ssh2"

Sempre

✓ 955 eventi (prima di 02/11/24 20:12:38,000) Nessun campionamento degli eventi ▼ Processo || Modalità intelligente ▼

Eventi (955)PatternStatisticheVisualizzazione

Formato timeline ▼ Zoom indietroZoom area selezionataDeseleziona1 giorno per colonna

Elenco ✎ Formato20 per pagina < Prec12345678...Avanti >

< Nascondi campiTutti i campiCAMPI SELEZIONATIa host 1a source 4a sourcetype 1CAMPI INTERESSANTI# date_hour 1# date_mday 8# date_minute 1a date_month 2# date_second 4a date_wday 7# date_year 1a date_zone 1a index 1

i	Ora	Evento
>	01/11/24 16:38:23,000	Thu Nov 01 2024 16:38:23 mailsv1 sshd[54545]: Accepted password for djohnson from 10.3.10.46 port 5143 ssh2 host = LAPTOP-RQN1IRNJ source = tutorialdata.zip:.mailsv/secure.log sourcetype = www1/secure
>	01/11/24 16:38:23,000	Thu Nov 01 2024 16:38:23 mailsv1 sshd[90328]: Accepted password for djohnson from 10.3.10.46 port 3914 ssh2 host = LAPTOP-RQN1IRNJ source = tutorialdata.zip:.mailsv/secure.log sourcetype = www1/secure
>	01/11/24 16:38:23,000	Thu Nov 01 2024 16:38:23 mailsv1 sshd[52473]: Accepted password for djohnson from 10.3.10.46 port 5449 ssh2 host = LAPTOP-RQN1IRNJ source = tutorialdata.zip:.mailsv/secure.log sourcetype = www1/secure
>	01/11/24 16:38:23,000	Thu Nov 01 2024 16:38:23 mailsv1 sshd[96461]: Accepted password for djohnson from 10.3.10.46 port 3041 ssh2 host = LAPTOP-RQN1IRNJ source = tutorialdata.zip:.mailsv/secure.log sourcetype = www1/secure
>	01/11/24 16:38:23,000	Thu Nov 01 2024 16:38:23 mailsv1 sshd[1269]: Accepted password for djohnson from 10.3.10.46 port 2652 ssh2 host = LAPTOP-RQN1IRNJ source = tutorialdata.zip:.mailsv/secure.log sourcetype = www1/secure
>	01/11/24	Thu Nov 01 2024 16:38:23 mailsv1 sshd[94708]: Accepted password for djohnson from 10.3.10.46 port 2408 ssh2

splunk>enterprise App ▾ Administrator ▾ 1 Messaggi ▾ Impostazioni ▾ Attività ▾ Guida ▾ Trova 🔍

Ricerca Analytics Set di dati Report Allarmi Dashboard >

Nuova ricerca

Salva come ▾ Crea vista tabella Chiudi

source="tutorialdata.zip:*" host="LAPTOP-RQN1IRNJ" index="nadir" "fail*" "86.212.199.60""port"

Sempre 🔍

✓ 158 eventi (prima di 02/11/24 20:15:00,000) Nessun campionamento degli eventi ▾ Processo ▾ || ■ ↻ 🖨 ⬇️ ! Modalità intelligente ▾

Eventi (158) Pattern Statistiche Visualizzazione

Formato timeline ▾ — Zoom indietro + Zoom area selezionata × Deseleziona 1 giorno per colonna

Elenco ▾ ✂ Formato 20 per pagina ▾ < Prec 1 2 3 4 5 6 7 8 Avanti >

	i	Ora	Evento
CAMPI SELEZIONATI <i>a</i> host 1 <i>a</i> source 4 <i>a</i> sourcetype 1	>	01/11/24 16:38:23,000	Thu Nov 01 2024 16:38:23 mailsrv sshd[5728]: Failed password for invalid user agushto from 86.212.199.60 port 3692 ssh2 host = LAPTOP-RQN1IRNJ source = tutorialdata.zip:\mailsv\secure.log sourcetype = wwwI/secure
	>	01/11/24 16:38:23,000	Thu Nov 01 2024 16:38:23 mailsrv sshd[4843]: Failed password for invalid user tomcat from 86.212.199.60 port 1464 ssh2 host = LAPTOP-RQN1IRNJ source = tutorialdata.zip:\mailsv\secure.log sourcetype = wwwI/secure
	>	01/11/24 16:38:23,000	Thu Nov 01 2024 16:38:23 mailsrv sshd[5718]: Failed password for invalid user desktop from 86.212.199.60 port 3518 ssh2 host = LAPTOP-RQN1IRNJ source = tutorialdata.zip:\mailsv\secure.log sourcetype = wwwI/secure
	>	01/11/24 16:38:23,000	Thu Nov 01 2024 16:38:23 mailsrv sshd[1008]: Failed password for invalid user yp from 86.212.199.60 port 2856 ssh2 host = LAPTOP-RQN1IRNJ source = tutorialdata.zip:\mailsv\secure.log sourcetype = wwwI/secure
	>	01/11/24 16:38:23,000	Thu Nov 01 2024 16:38:23 mailsrv sshd[5878]: Failed password for mail from 86.212.199.60 port 1054 ssh2 host = LAPTOP-RQN1IRNJ source = tutorialdata.zip:\mailsv\secure.log sourcetype = wwwI/secure
	>	01/11/24	Thu Nov 01 2024 16:38:23 mailsrv sshd[2649]: Failed password for apache from 86.212.199.60 port 2630 ssh2

CAMPI INTERESSANTI
date_hour 1
date_mday 7
date_minute 1
a date_month 2
date_second 4
a date_wday 6
date_year 1
a date_zone 1
a index 1

Trovare IP che hanno tentato di accedere più di 5 volte

Ho elaborato una *query* che indicasse a Splunk di individuare tutte quelle stringhe che, per numero e ordine di caratteri, hanno la struttura di un indirizzo IP, dando ad esse il nome "ip". Solo allora ho potuto chiedere a Splunk di contare gli accessi da parte di quegli IP e mostrarmi quelli maggiori di 5 nel tag "Allarme dei 5 accessi"..

Nuova ricerca

source="tutorialdata.zip:*" host="LAPTOP-RQN1IRNJ" index="nadir" "failed password" | rex field=_raw "Failed password for .* from (?<ip>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})" | stats count by ip | where count > 5 | rename count as "Allarme dei 5 accessi"

✓ 33.253 eventi (prima di 02/11/24 20:23:49,000) Nessun campionamento degli eventi

Processo

Eventi Pattern **Statistiche (182)** Visualizzazione

20 per pagina Formato Anteprima

ip	Allarme dei 5 accessi
107.3.146.207	282
108.65.113.83	249
109.169.32.135	515
110.138.30.229	163
110.159.208.78	125
111.161.27.20	86
112.111.162.4	120
117.21.246.164	195
118.142.68.222	92
12.130.60.4	227
12.130.60.5	155
121.254.179.199	183
121.9.245.177	162

Ultim'ora
Tragedia nel par...

Cerca

20:25
02/11/2024

Internal Server Error

Gli internal server error, sono identificati dal codice di stato HTTP 500, quindi mi basta specificarlo nella query

RicercaAnalyticsSet di datiReportAllarmiDashboard

Nuova ricerca

Salva comeCrea vista tabellaChiudi

source="tutorialdata.zip:*" host="LAPTOP-RQN1IRNJ" index="nadir2" "500"

Sempre

781 eventi (prima di 04/11/24 18:03:27,000) Nessun campionamento degli eventi

Processo

Modalità intelligente

Formato timelineZoom indietroZoom area selezionataDeselezione1 ora per colonna

ElencoFormato20 per pagina

Nascondi campiTutti i campi

CAMPI SELEZIONATI

a host 1

a source 3

a sourcetype 1

CAMPI INTERESSANTI

a action 5

bytes 100+

a categoryId 8

a clientip 100+

date_hour 24

date_mday 8

date_minute 60

a date_month 2

date_second 60

a date_wday 7

date_year 1

a date_zone 1

a file 5

a ident 1

a index 1

a itemid 14

a JSESSIONID 100+

linecount 1

i	Ora	Evento
>	01/11/24 18:18:59,000	198.35.1.75 - - [01/Nov/2024:18:18:59] "GET /cart.do?action=addtocart&itemId=EST-13&JSESSIONID=SD10SL2FF4ADFF53099 HTTP 1.1" 500 2324 "http://www.buttercupgames.com/category.screen?categoryId=NULL" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 645 host = LAPTOP-RQN1IRNJ source = tutorialdata.zip:\www1\access.log sourcetype = access_combined_wcookie
>	01/11/24 18:18:55,000	198.35.1.75 - - [01/Nov/2024:18:18:55] "GET /product.screen?productId=SF-BVS-G01&JSESSIONID=SD10SL2FF4ADFF53099 HTTP 1.1" 500 2809 "http://www.buttercupgames.com/cart.do?action=view&itemId=EST-14" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 370 host = LAPTOP-RQN1IRNJ source = tutorialdata.zip:\www1\access.log sourcetype = access_combined_wcookie
>	01/11/24 17:42:03,000	125.89.78.6 - - [01/Nov/2024:17:42:03] "POST /cart.do?action=changequantity&itemId=EST-16&JSESSIONID=SD10SL8FF3ADFF52952 HTTP 1.1" 500 1165 "http://www.buttercupgames.com/product.screen?productId=SF-BVS-G01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 230 host = LAPTOP-RQN1IRNJ source = tutorialdata.zip:\www2\access.log sourcetype = access_combined_wcookie
>	01/11/24 17:17:00,000	194.146.236.22 - - [01/Nov/2024:17:17:00] "POST /product.screen?productId=SF-BVS-G01&JSESSIONID=SD4SL3FF2ADFF52813 HTTP 1.1" 500 299 "http://www.buttercupgames.com/cart.do?action=remove&itemId=EST-13" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 749 host = LAPTOP-RQN1IRNJ source = tutorialdata.zip:\www1\access.log sourcetype = access_combined_wcookie
>	01/11/24 17:15:13,000	121.254.179.199 - - [01/Nov/2024:17:15:13] "POST /product.screen?productId=SF-BVS-G01&JSESSIONID=SD0SL9FF10ADFF52799 HTTP 1.1" 500 2243 "http://www.buttercupgames.com/oldlink?itemId=EST-13" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 642 host = LAPTOP-RQN1IRNJ source = tutorialdata.zip:\www3\access.log sourcetype = access_combined_wcookie
>	01/11/24 17:00:43,000	212.27.63.151 - - [01/Nov/2024:17:00:43] "GET /product.screen?productId=MB-AG-G07&JSESSIONID=SD2SL8FF2ADFF52732 HTTP 1.1" 200 1505 "http://www.buttercupgames.com/oldlink?itemId=EST-27" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; InfoPath.1; .NET4.0C; .NET4.0E; MS-RTC LM 8)" 500 host = LAPTOP-RQN1IRNJ source = tutorialdata.zip:\www1\access.log sourcetype = access_combined_wcookie
>	01/11/24 16:54:07,000	76.89.103.115 - - [01/Nov/2024:16:54:07] "GET /cart.do?action=remove&itemId=EST-17&JSESSIONID=SD1SL9FF9ADFF52693 HTTP 1.1" 500 2606 "http://www.buttercupgames.com/category.screen?categoryId=NULL" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; MS-RTC LM 8; InfoPath.2)" 158

Trarre conclusioni utilizzando AI.

CON L'AIUTO DI CHAT-GPT HO PROVATO A FORMULARE DELLE IPOTESI SUI DATI RACCOLTI E FILTRATI

1. Tentativi di accesso falliti:

- Diversi log mostrano ripetuti tentativi di accesso falliti tramite SSH (come evidenziato dai messaggi "Failed password"). Questi potrebbero indicare tentativi di brute-force o attacchi di credential stuffing. L'elevato numero di tentativi di accesso falliti provenienti da diversi indirizzi IP potrebbe indicare un attacco distribuito, in cui più attori o botnet tentano simultaneamente di accedere al sistema per bypassare le misure di protezione basate sul rilevamento da singolo IP
- La presenza di indirizzi IP specifici che effettuano molti tentativi suggerisce attività sospette provenienti da possibili attori malevoli che tentano di accedere senza autorizzazione.

2. Tentativi di accesso riusciti:

- Alcuni log riportano accessi accettati (come evidenziato da "Accepted password"), indicando che ci sono connessioni SSH andate a buon fine, potenzialmente legittime, ma che devono essere analizzate per confermare l'autenticità degli utenti.

3. Indirizzi IP sospetti:

- Sono stati identificati indirizzi IP che hanno eseguito molti tentativi di accesso falliti. In uno screenshot specifico, si osserva che ci sono IP con un numero considerevole di tentativi non riusciti (es. 282, 249, 515 eventi). Questi IP potrebbero essere inclusi in una lista di blocco temporanea o permanente per proteggere il sistema.

4. Accessi ripetuti e frequenti:

- La visualizzazione dei log mostra una frequenza elevata di tentativi di connessione da parte di indirizzi IP specifici. La quantità di tentativi superiori a una soglia (come il filtro che identifica gli "allarmi dei 5 accessi") evidenzia un'attività anomala che dovrebbe essere monitorata attentamente.

5. Log di errore HTTP 500:

- Alcuni log indicano errori HTTP 500, che possono rappresentare malfunzionamenti nei servizi web o potenziali tentativi di attacco, come vulnerabilità di tipo DoS (Denial of Service) o attacchi mirati che provocano errori server-side.

Ipotesi di rischio per la sicurezza:

- **Attacchi Brute-force:** L'elevato numero di tentativi di accesso falliti da vari IP suggerisce un attacco brute-force in corso, volto a ottenere l'accesso non autorizzato ai sistemi.
- **Compromissione di Credenziali:** Se gli accessi accettati provengono da IP non riconosciuti o insoliti, potrebbe indicare che alcune credenziali sono state compromesse.
- **Test di Vulnerabilità:** Gli errori HTTP 500 potrebbero essere il risultato di attacchi per individuare vulnerabilità o tentativi di sfruttamento di difetti nel software del server.
- **Potenziale Escalation:** Se un attaccante è riuscito a ottenere l'accesso con credenziali valide (come indicato dai tentativi di accesso riusciti), potrebbe tentare di eseguire un'escalation dei privilegi per aumentare il controllo sul sistema.

Raccomandazioni:

- **Blocco IP:** Implementare un blocco IP temporaneo per gli indirizzi con attività sospette.
- **Monitoraggio attivo:** Incrementare il livello di monitoraggio e correlare questi eventi con altri dati di log per rilevare schemi di comportamento dannoso.
- **Analisi delle credenziali:** Verificare se gli accessi accettati sono stati eseguiti da utenti noti o se sono il risultato di credenziali compromesse.
- **Patch e aggiornamenti:** Assicurarsi che il sistema sia aggiornato per mitigare potenziali vulnerabilità sfruttabili.