

1. Crea una query Splunk per identificare tutti i tentativi di accesso falliti "Failed password". La query dovrebbe mostrare il timestamp, l'indirizzo IP di origine, il nome utente e il motivo del fallimento.

The screenshot shows a Splunk search interface with the following query: `index=main "Failed password" | rex "Failed password for (invalid user)?(?<username>S\S+) from (?<ip>\d+\.\d+\.\d+\.\d+)" | table_time, username, _raw`. The results table displays 15 rows of failed password attempts, each with a timestamp, username, and a detailed log message.

_time	username	_raw
2025-05-01 05:46:15		Tue May 01 2025 05:46:15 www2 sshd[4748]: Failed password for invalid user db from 202.179.8.245 port 3639 ssh2
2025-05-01 05:46:15		Tue May 01 2025 05:46:15 www2 sshd[2386]: Failed password for invalid user dbinst1 from 202.179.8.245 port 3465 ssh2
2025-05-01 05:46:15		Tue May 01 2025 05:46:15 www2 sshd[1317]: Failed password for invalid user guest from 202.179.8.245 port 2757 ssh2
2025-05-01 05:46:15		Tue May 01 2025 05:46:15 www2 sshd[4983]: Failed password for invalid user db from 202.179.8.245 port 1323 ssh2
2025-05-01 05:46:15		Tue May 01 2025 05:46:15 www2 sshd[5830]: Failed password for invalid user admin from 202.179.8.245 port 1706 ssh2
2025-05-01 05:46:15		Tue May 01 2025 05:46:15 www2 sshd[4147]: Failed password for root from 202.179.8.245 port 4201 ssh2
2025-05-01 05:46:15		Tue May 01 2025 05:46:15 www2 sshd[5659]: Failed password for cher from 202.179.8.245 port 2875 ssh2
2025-05-01 05:46:15		Tue May 01 2025 05:46:15 www2 sshd[5289]: Failed password for invalid user trac from 202.179.8.245 port 1027 ssh2
2025-05-01 05:46:15		Tue May 01 2025 05:46:15 www2 sshd[5084]: Failed password for invalid user rightscale from 202.179.8.245 port 4955 ssh2
2025-05-01 05:46:15		Tue May 01 2025 05:46:15 www2 sshd[3736]: Failed password for invalid user alex from 202.179.8.245 port 1276 ssh2
2025-05-01 05:46:15		Tue May 01 2025 05:46:15 www2 sshd[3785]: Failed password for invalid user mailman from 202.179.8.245 port 1443 ssh2
2025-05-01 05:46:15		Tue May 01 2025 05:46:15 www2 sshd[1394]: Failed password for jboss from 202.179.8.245 port 2070 ssh2
2025-05-01 05:46:15		Tue May 01 2025 05:46:15 www2 sshd[4634]: Failed password for invalid user whois from 202.179.8.245 port 1757 ssh2
2025-05-01 05:46:15		Tue May 01 2025 05:46:15 www2 sshd[4840]: Failed password for invalid user services from 202.179.8.245 port 3288 ssh2
2025-05-01 05:46:15		Tue May 01 2025 05:46:15 www2 sshd[5593]: Failed password for invalid user vpxuser from 202.179.8.245 port 4394 ssh2
2025-05-01 05:46:15		Tue May 01 2025 05:46:15 www2 sshd[1725]: Failed password for invalid user mysql from 194.215.205.19 port 1087 ssh2

2. Scrivi una query Splunk per trovare tutte le sessioni SSH aperte con successo. La query dovrebbe filtrare per l'utente "djohnson" e mostrare il timestamp e l'ID utente.

The screenshot shows a Splunk search interface with the following query: `index=main "Accepted password" "djohnson" | rex "Accepted password for (?<username>S\S+) from" | search username="djohnson" | table_time, username`. The results table displays 15 rows of successful SSH sessions for the user 'djohnson', each with a timestamp and username.

_time	username
2025-05-03 05:46:14	djohnson
2025-05-03 05:46:14	djohnson
2025-05-03 05:46:14	djohnson
2025-05-03 05:46:14	djohnson
2025-05-03 05:46:14	djohnson
2025-05-03 05:46:14	djohnson
2025-05-03 05:46:14	djohnson
2025-05-03 05:46:14	djohnson
2025-05-03 05:46:14	djohnson
2025-05-03 05:46:14	djohnson
2025-05-03 05:46:14	djohnson
2025-05-03 05:46:14	djohnson
2025-05-03 05:46:14	djohnson
2025-05-03 05:46:14	djohnson
2025-05-03 05:46:14	djohnson
2025-05-03 05:46:14	djohnson

Scrivi una query Splunk per trovare tutti i tentativi di accesso falliti provenienti dall'indirizzo IP "86.212.199.60". La query dovrebbe mostrare il timestamp, il nome utente e il numero di

porta.

Nuova ricerca Salva come Crea vista tabella Chiudi

index=main "Failed password" "86.212.199.68" | rex "Failed password for (invalid user)?(?<username>[a-z]+) from 86.212.199.68 port [?<port>[0-9]+]" | table _time, username, port

✓ 316 eventi (prima di 04/05/25 19:22:16.000) Nessun campionamento degli eventi

Processo

Eventi Pattern **Statistiche (316)** Visualizzazione

Mostra: 20 per pagina Formato Antepriima: on

_time	username	port
2025-05-01 05:46:15	whois	4566
2025-05-01 05:46:15	ftp	2043
2025-05-01 05:46:15	hsqldb	2198
2025-05-01 05:46:15	hammer	1323
2025-04-26 05:46:15	hsqldb	4379
2025-04-26 05:46:15	admin	2831
2025-04-26 05:46:15	system	4294
2025-04-26 05:46:15	alex	2121
2025-04-26 05:46:15	mantis	2735
2025-04-26 05:46:15	jira	1958
2025-04-26 05:46:15	vmware	4457
2025-04-26 05:46:15	nagios	2048
2025-04-26 05:46:15	mail	1775
2025-05-02 05:46:14	services	1393
2025-05-02 05:46:14	sync	1695
2025-05-02 05:46:14	admin	3673

3. Crea una query Splunk per identificare gli indirizzi IP che hanno tentato di accedere ("Failed password") al sistema più di 5 volte. La query dovrebbe mostrare l'indirizzo IP e il numero di tentativi.

splunk enterprise App

Ricerca Analytics Set di dati Report Allarmi Dashboard

Nuova ricerca Salva come Crea vista tabella Chiudi

index=main "Failed password" | rex "from (?<ip>[a-zA-Z0-9]+\.[a-zA-Z0-9]+\.[a-zA-Z0-9]+\.[a-zA-Z0-9]+)" | stats count by ip | where count > 5

✓ 66.506 eventi (prima di 04/05/25 19:24:07.000) Nessun campionamento degli eventi

Processo

Eventi Pattern **Statistiche (185)** Visualizzazione

Mostra: 20 per pagina Formato Antepriima: on

ip	count
10.1.10.172	32
10.2.10.163	54
10.3.10.46	242
107.3.146.207	564
108.65.113.83	498
109.169.32.135	1030
110.138.30.229	326
110.159.208.78	250
111.161.27.20	172
112.111.162.4	240
117.21.246.164	399
118.142.68.222	184
12.138.68.4	454
12.138.68.5	318
121.254.179.199	366
121.9.245.177	324

4. Crea una query Splunk per trovare tutti gli Internal Server Error.

RicercaAnalyticsSet di datiReportAllarmiDashboard

Search & Reporting

Nuova ricerca

Salva comeCrea vista tabellaChiudi

index=main ("Internal Server Error" OR "500") | table _time, host, source, _raw

Sempre

✓ 1.580 eventi (prima di 04/05/25 19:25:51.000) Nessun campionamento degli eventi

ProcessoModalità intelligente

EventiPattern

Statistiche (1.580)

Visualizzazione

Mostra: 20 per paginaFormatoAnteprima: on

< Prec12345678...Avanti >

_time	host	source	_raw
2025-04-30 07:38:08	Server	tutorialdata.zip:\www3/access.log	111.161.27.20 - - [30/Apr/2025:07:38:08] "POST /category.screen?categoryID=NULL&JSESSIONID=S05SL10FF1ADFF29958 HTTP 1.1" 500 2657 "http://www.buttercupgames.com/category.screen?categoryID=NULL" "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)" 181
2025-04-30 06:39:31	Server	tutorialdata.zip:\www3/access.log	222.169.224.226 - - [30/Apr/2025:06:39:31] "GET /oldlink?itemID=EST-26&JSESSIONID=S010SL6FF10ADFF29767 HTTP 1.1" 500 2549 "http://www.buttercupgames.com/cart.do?action=changequantity&itemID=EST-26" "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)" 238
2025-04-30 01:37:03	Server	tutorialdata.zip:\www3/access.log	81.18.148.190 - - [30/Apr/2025:01:37:03] "GET /cart.do?action=view&itemID=EST-17&JSESSIONID=S08SL2FF5ADFF28096 HTTP 1.1" 500 2173 "http://www.buttercupgames.com/category.screen?categoryID=NULL" "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" 353
2025-04-30 01:34:17	Server	tutorialdata.zip:\www3/access.log	86.51.1.2 - - [30/Apr/2025:01:34:17] "GET /cart.do?action=view&itemID=EST-17&JSESSIONID=S08SL1FF2ADFF28065 HTTP 1.1" 500 2720 "http://www.buttercupgames.com/cart.do?action=view&itemID=EST-17" "Mozilla/5.0 (iPad; U; CPU OS 4_3_5 like Mac OS X; en-us) AppleWebKit/533.17.9 (KHTML, like Gecko) Version/5.0.2 Mobile/8L1 Safari/6533.18.5" 488
2025-04-30 01:32:16	Server	tutorialdata.zip:\www3/access.log	125.89.78.6 - - [30/Apr/2025:01:32:16] "GET /product.screen?productID=SF-BVS-G01&JSESSIONID=S08SL6FF10ADFF28064 HTTP 1.1" 500 2311 "http://www.buttercupgames.com/cart.do?action=addtocart&itemID=EST-11" "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)" 617
2025-04-30 01:02:45	Server	tutorialdata.zip:\www3/access.log	91.205.189.15 - - [30/Apr/2025:01:02:45] "POST /product.screen?productID=SF-BVS-G01&JSESSIONID=S08SL9FF3ADFF27878 HTTP 1.1" 500 377 "http://www.buttercupgames.com/oldlink?itemID=EST-21" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)" 560
2025-04-30 00:38:28	Server	tutorialdata.zip:\www3/access.log	142.233.200.21 - - [30/Apr/2025:00:38:28] "GET /cart.do?action=addtocart&itemID=EST-36&JSESSIONID=S01SL7FF10ADFF27714 HTTP 1.1" 500 2638 "http://www.buttercupgames.com/category.screen?categoryID=NULL" "Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_3; en-US) AppleWebKit/533.4 (KHTML, like Gecko) Chrome/5.0.375.38 Safari/533.4" 664
2025-04-30 00:13:33	Server	tutorialdata.zip:\www3/access.log	91.205.189.27 - - [30/Apr/2025:00:13:33] "GET /oldlink?itemID=EST-21&JSESSIONID=S06SL4FF5ADFF27595 HTTP 1.1" 500 2144 "http://www.buttercupgames.com/product.screen?productID=SF-BVS-G01" "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)" 866
2025-04-30 00:13:33	Server	tutorialdata.zip:\www3/access.log	91.205.189.27 - - [30/Apr/2025:00:13:33] "GET /category.screen?categoryID=NULL&JSESSIONID=S06SL4FF5ADFF27595 HTTP 1.1" 500 1285 "http://www.buttercupgames.com/product.screen?productID=SF-BVS-G01" "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)" 452
2025-04-30 00:36:02	Server	tutorialdata.zip:\www3/access.log	69.80.0.18 - - [29/Apr/2025:22:36:02] "GET /cart.do?action=view&itemID=EST-27&JSESSIONID=S010SL6FF4ADFF27175 HTTP 1.1" 500 3290 "http://www.buttercupgames.com/category.screen?categoryID=NULL" "Mozilla/5.0 (compatible; MSIE 7.0; Windows NT 6.1; .NET CLR 3.0.30717; .NET CLR 3.0.4506.116; .NET CLR 3.5.30729; .NET4.0C; MS-SPK-1.0.0; InfoPath.3.0) 348