

REPORT ESERCIZIO W24D4

Report Analisi Log Splunk

In questo report vengono presentate le analisi di sicurezza eseguite tramite **Splunk** su un dataset di log estratti dal file **tutorialdata.zip**. Sono state realizzate **5 query** mirate per identificare comportamenti sospetti, tentativi di accesso falliti, sessioni SSH, errori HTTP e attività anomale da parte di IP specifici.

Conclusioni AI-based

Dall'analisi dei Log sono emerse diverse evidenze significative:

1. Tentativi di accesso falliti:

Numerosi eventi contengono messaggi di **'Failed password'**, soprattutto da utenti non validi. Questo suggerisce attività di brute-force o attacchi automatizzati su SSH.

The screenshot displays the Splunk search interface. At the top, the search bar contains the query `index=* "Failed password"`. Below the search bar, a summary bar indicates **33,253** events found. The main results pane shows a list of events, each with a timestamp and a description of a failed password attempt. The events are filtered by the search criteria and are displayed in a table format. The table has columns for **Ora** (Time) and **Evento** (Event). The events are sorted by time, showing a sequence of failed password attempts from May 3, 2025, at 17:45:56. The events include details such as the host, source, and the specific user or service that was targeted. The interface also includes a sidebar with filters for **Campi selezionati** (Selected fields) and **Campi interessanti** (Interesting fields). The bottom of the screen shows the Windows taskbar with the time 02:07 and date 05/05/2025.

Ora	Evento
03/05/25 17:45:56.000	Thu May 03 2025 17:45:56 mailsv1 ssh[3276]: Failed password for invalid user appserver from 194.8.74.23 port 3351 ssh2
03/05/25 17:45:56.000	Thu May 03 2025 17:45:56 mailsv1 ssh[1039]: Failed password for root from 194.8.74.23 port 3768 ssh2
03/05/25 17:45:56.000	Thu May 03 2025 17:45:56 mailsv1 ssh[5258]: Failed password for invalid user testuser from 194.8.74.23 port 3626 ssh2
03/05/25 17:45:56.000	Thu May 03 2025 17:45:56 mailsv1 ssh[1165]: Failed password for apache from 194.8.74.23 port 4084 ssh2
03/05/25 17:45:56.000	Thu May 03 2025 17:45:56 mailsv1 ssh[3768]: Failed password for invalid user mongod from 194.8.74.23 port 2472 ssh2
03/05/25 17:45:56.000	Thu May 03 2025 17:45:56 mailsv1 ssh[4998]: Failed password for mall from 194.8.74.23 port 1552 ssh2
03/05/25 17:45:56.000	Thu May 03 2025 17:45:56 mailsv1 ssh[1938]: Failed password for games from 194.8.74.23 port 3987 ssh2
03/05/25 17:45:56.000	Thu May 03 2025 17:45:56 mailsv1 ssh[3881]: Failed password for invalid user desktop from 194.8.74.23 port 2285 ssh2
03/05/25 17:45:56.000	Thu May 03 2025 17:45:56 mailsv1 ssh[3759]: Failed password for nagios from 194.8.74.23 port 3789 ssh2

2. Accessi SSH riusciti dell'utente djohnson:

Sono stati registrati molti login riusciti da parte di questo utente, tutti da un singolo IP, il che può indicare attività legittima o un account compromesso sfruttato da un solo host.

Nuova ricerca

Index** "Accepted password" "djohnson"

✓ 955 eventi (prima di 05/05/25 02:11:58.000) Nessun campionamento degli eventi

Processo

Formato timeline

Zoom indietro

Zoom area selezionata

Delezioni

1 giorno per colonna

Formato

Mostra: 20 per pagina

Visualizza: Elenco

1 2 3 4 5 6 7 8

Avanti

Nascondi campi

Tutti i campi

CAMPI SELEZIONATI

a host 1

a source 4

a sourcetype 1

CAMPI INTERESSANTI

date_hour 1

date_minute 1

date_month 2

date_second 4

date_week 7

date_year 1

date_zone 1

index 1

linecount 1

punct 1

splunk_server 1

timestamp 1

timestamppos 1

Escludi nuovi campi

i	Ora	Evento
>	03/05/25 17:45:56.000	Thu May 03 2025 17:45:56 mailsv ssh[54545]: Accepted password for djohnson from 10.3.10.46 port 5143 ssh2 host = DESKTOP-9KIO4BT source = tutorialdata.zip:mailsv/secure.log sourcetype = www/secure
>	03/05/25 17:45:56.000	Thu May 03 2025 17:45:56 mailsv ssh[50328]: Accepted password for djohnson from 10.3.10.46 port 3914 ssh2 host = DESKTOP-9KIO4BT source = tutorialdata.zip:mailsv/secure.log sourcetype = www/secure
>	03/05/25 17:45:56.000	Thu May 03 2025 17:45:56 mailsv ssh[52473]: Accepted password for djohnson from 10.3.10.46 port 5449 ssh2 host = DESKTOP-9KIO4BT source = tutorialdata.zip:mailsv/secure.log sourcetype = www/secure
>	03/05/25 17:45:56.000	Thu May 03 2025 17:45:56 mailsv ssh[59481]: Accepted password for djohnson from 10.3.10.46 port 3041 ssh2 host = DESKTOP-9KIO4BT source = tutorialdata.zip:mailsv/secure.log sourcetype = www/secure
>	03/05/25 17:45:56.000	Thu May 03 2025 17:45:56 mailsv ssh[1269]: Accepted password for djohnson from 10.3.10.46 port 2652 ssh2 host = DESKTOP-9KIO4BT source = tutorialdata.zip:mailsv/secure.log sourcetype = www/secure
>	03/05/25 17:45:56.000	Thu May 03 2025 17:45:56 mailsv ssh[94708]: Accepted password for djohnson from 10.3.10.46 port 2408 ssh2 host = DESKTOP-9KIO4BT source = tutorialdata.zip:mailsv/secure.log sourcetype = www/secure
>	03/05/25 17:45:56.000	Thu May 03 2025 17:45:56 mailsv ssh[58104]: Accepted password for djohnson from 10.3.10.46 port 4577 ssh2 host = DESKTOP-9KIO4BT source = tutorialdata.zip:mailsv/secure.log sourcetype = www/secure
>	03/05/25 17:45:56.000	Thu May 03 2025 17:45:56 mailsv ssh[50837]: Accepted password for djohnson from 10.3.10.46 port 8128 ssh2 host = DESKTOP-9KIO4BT source = tutorialdata.zip:mailsv/secure.log sourcetype = www/secure
>	03/05/25 17:45:56.000	Thu May 03 2025 17:45:56 mailsv ssh[6989]: Accepted password for djohnson from 10.3.10.46 port 8781 ssh2 host = DESKTOP-9KIO4BT source = tutorialdata.zip:mailsv/secure.log sourcetype = www/secure

3. Attacchi mirati da un IP specifico:

L'indirizzo IP 86.212.199.60 ha generato numerosi tentativi falliti, usando diversi username e porte. Questo comportamento è tipico di uno scanner automatico.

Nuova ricerca

Index** "Failed password" "86.212.199.60"

✓ 158 eventi (prima di 05/05/25 02:15:34.000) Nessun campionamento degli eventi

Processo

Formato timeline

Zoom indietro

Zoom area selezionata

Delezioni

1 giorno per colonna

Formato

Mostra: 20 per pagina

Visualizza: Elenco

1 2 3 4 5 6 7 8

Avanti

Nascondi campi

Tutti i campi

CAMPI SELEZIONATI

a host 1

a source 4

a sourcetype 1

CAMPI INTERESSANTI

date_hour 1

date_minute 1

date_month 2

date_second 4

date_week 5

date_year 1

date_zone 1

index 1

linecount 1

punct 2

splunk_server 1

timestamp 1

timestamppos 1

Escludi nuovi campi

i	Ora	Evento
>	03/05/25 17:45:56.000	Thu May 03 2025 17:45:56 mailsv ssh[5728]: Failed password for invalid user aquasht from 86.212.199.60 port 3692 ssh2 host = DESKTOP-9KIO4BT source = tutorialdata.zip:mailsv/secure.log sourcetype = www/secure
>	03/05/25 17:45:56.000	Thu May 03 2025 17:45:56 mailsv ssh[4843]: Failed password for invalid user tomcat from 86.212.199.60 port 1464 ssh2 host = DESKTOP-9KIO4BT source = tutorialdata.zip:mailsv/secure.log sourcetype = www/secure
>	03/05/25 17:45:56.000	Thu May 03 2025 17:45:56 mailsv ssh[5718]: Failed password for invalid user desktop from 86.212.199.60 port 3518 ssh2 host = DESKTOP-9KIO4BT source = tutorialdata.zip:mailsv/secure.log sourcetype = www/secure
>	03/05/25 17:45:56.000	Thu May 03 2025 17:45:56 mailsv ssh[1008]: Failed password for invalid user yp from 86.212.199.60 port 2856 ssh2 host = DESKTOP-9KIO4BT source = tutorialdata.zip:mailsv/secure.log sourcetype = www/secure
>	03/05/25 17:45:56.000	Thu May 03 2025 17:45:56 mailsv ssh[5878]: Failed password for mail from 86.212.199.60 port 1054 ssh2 host = DESKTOP-9KIO4BT source = tutorialdata.zip:mailsv/secure.log sourcetype = www/secure
>	03/05/25 17:45:56.000	Thu May 03 2025 17:45:56 mailsv ssh[2649]: Failed password for apache from 86.212.199.60 port 2630 ssh2 host = DESKTOP-9KIO4BT source = tutorialdata.zip:mailsv/secure.log sourcetype = www/secure
>	03/05/25 17:45:56.000	Thu May 03 2025 17:45:56 mailsv ssh[2873]: Failed password for invalid user services from 86.212.199.60 port 4740 ssh2 host = DESKTOP-9KIO4BT source = tutorialdata.zip:mailsv/secure.log sourcetype = www/secure
>	03/05/25 17:45:56.000	Thu May 03 2025 17:45:56 mailsv ssh[2285]: Failed password for invalid user irc from 86.212.199.60 port 1203 ssh2 host = DESKTOP-9KIO4BT source = tutorialdata.zip:mailsv/secure.log sourcetype = www/secure
>	03/05/25 17:45:56.000	Thu May 03 2025 17:45:56 mailsv ssh[3688]: Failed password for invalid user mysql from 86.212.199.60 port 4802 ssh2 host = DESKTOP-9KIO4BT source = tutorialdata.zip:mailsv/secure.log sourcetype = www/secure

4. Elenco di IP ostili:

Sono stati identificati più di 100 indirizzi IP che hanno tentato l'accesso fallendo oltre 5 volte. Questi IP potrebbero essere inseriti in una blacklist o sottoposti a sistemi di throttling.

Nuova ricerca

Salva come Crea vista tabella Chiudi

Index* "failed password" | rex "from (?<ip>\d+\.\d+\.\d+\.\d+)" | stats count by ip | where count > 5

✓ 33.253 eventi (prima di 05/05/25 02:26:50.000) Nessun campionamento degli eventi

Processo Modaltà intelligente

Eventi Pattern Statistiche (185) Visualizzazione

Mostra: 20 per pagina Formato Anteprioma: on

ip	count
10.1.10.172	16
10.2.10.163	47
10.3.10.46	121
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	182
123.118.73.155	150
123.196.113.11	179
123.30.108.208	167

Ricerca in Windows e nel Web

60:27 05/05/2025

5. Errori 500 - Internal Server Error:

Diversi endpoint dell'applicazione web (come /cart.do e /product.screen) generano errori 500, il che potrebbe indicare problemi lato server, vulnerabilità o carichi anomali da automatismi.

Nuova ricerca

Salva come Crea vista tabella Chiudi

Index* sourcetype="access_combined_wcookie" | rex "HTTP/\d\.\d\.\d\s{3}status\d{3}" | search status=500 | table _time, status, uri_path, _raw

✓ 733 eventi (prima di 05/05/25 02:46:42.000) Nessun campionamento degli eventi

Processo Modaltà intelligente

Eventi Pattern Statistiche (733) Visualizzazione

Mostra: 20 per pagina Formato Anteprioma: on

_time	status	uri_path	_raw
2025-05-02 14:54:56	500	/oldlink	200.240.243.170 - - [02/May/2025:14:54:56] "GET /oldlink?itemId=EST-13&SESSIONID=SD9SL7FF2ADFF45006 HTTP 1.1" 500 3235 "http://www.buttercupgames.com/cart.do?action=view&itemId=EST-13" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; .NET CLR 1.1.4322; InfoPath.1; HS-RTC LM 8)" 738
2025-05-02 14:54:56	500	/cart.do	200.240.243.170 - - [02/May/2025:14:54:56] "GET /cart.do?action=view&itemId=EST-13&SESSIONID=SD9SL7FF2ADFF45006 HTTP 1.1" 500 541 "http://www.buttercupgames.com/category.screen?categoryId=NULL" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; .NET CLR 1.1.4322; InfoPath.1; HS-RTC LM 8)" 912
2025-05-02 13:19:50	500	/cart.do	64.120.19.156 - - [02/May/2025:13:19:50] "GET /cart.do?action=remove&itemId=EST-21&SESSIONID=SD3SL9FF2ADFF44587 HTTP 1.1" 500 2524 "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" 958
2025-05-02 13:18:26	500	/product.screen	91.217.178.210 - - [02/May/2025:13:18:26] "GET /product.screen?productId=SF-BVS-G01&SESSIONID=SD3SL2FF1ADFF44586 HTTP 1.1" 500 3911 "http://www.buttercupgames.com/product.screen?productId=SF-BVS-G01" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322) 575
2025-05-02 12:06:22	500	/product.screen	85.62.218.82 - - [02/May/2025:12:06:22] "POST /product.screen?productId=SF-BVS-G01&SESSIONID=SD2SL1FF6ADFF44307 HTTP 1.1" 500 3774 "http://www.buttercupgames.com/product.screen?productId=SF-BVS-G01" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; .NET CLR 1.1.4322; InfoPath.1; HS-RTC LM 8)" 139
2025-05-02 12:06:18	500	/category.screen	85.62.218.82 - - [02/May/2025:12:06:18] "GET /category.screen?categoryId=NULL&SESSIONID=SD2SL1FF6ADFF44307 HTTP 1.1" 500 2369 "http://www.buttercupgames.com/category.screen?categoryId=NULL" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; .NET CLR 1.1.4322; InfoPath.1; HS-RTC LM 8)" 601
2025-05-02 10:36:24	500	/category.screen	202.91.242.117 - - [02/May/2025:10:36:24] "GET /category.screen?categoryId=NULL&SESSIONID=SD3SL4FF4ADFF44002 HTTP 1.1" 500 2285 "http://www.buttercupgames.com/cart.do?action=addtocart&itemId=EST-19" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)" 367
2025-05-02 10:02:10	500	/oldlink	173.44.37.226 - - [02/May/2025:10:02:10] "POST /oldlink?itemId=EST-26&SESSIONID=SD2SL9FF5ADFF43851 HTTP 1.1" 500 3282 "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" 436
2025-05-02 09:21:03	500	/category.screen	91.205.40.22 - - [02/May/2025:09:21:03] "POST /category.screen?categoryId=NULL&SESSIONID=SD7SL7FF1ADFF43679 HTTP 1.1" 500 443 "http://www.buttercupgames.com/category.screen?categoryId=NULL" "Mozilla/5.0 (compatible; Googlebot/2.1; http://www.google.com/bot.html)" 630
2025-05-02 08:18:28	500	/category.screen	203.45.206.135 - - [02/May/2025:08:18:28] "GET /category.screen?categoryId=NULL&SESSIONID=SD4SL4FF3ADFF43402 HTTP 1.1" 500 1074 "http://www.buttercupgames.com/oldlink?itemId=EST-6" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 195
2025-05-02 07:39:04	500	/cart.do	183.60.133.18 - - [02/May/2025:07:39:04] "GET /cart.do?action=addtocart&itemId=EST-27&SESSIONID=SD3SL6FF1ADFF43186 HTTP 1.1" 500 2173 "http://www.buttercupgames.com/product.screen?productId=SF-BVS-G01" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-us; rv:1.9.2.38) Gecko/20100800 Firefox/3.6.38 (.NET CLR 3.5.30729; NET4.RC)" 417

Ricerca in Windows e nel Web

60:47 05/05/2025

Conclusione finale:

I Log analizzati evidenziano pattern coerenti con un contesto di rete esposta, probabilmente soggetta a tentativi di scansione, brute-force e potenziali vulnerabilità web.

Si raccomanda di applicare controlli su IP sospetti, implementare sistemi IDS/IPS e monitorare costantemente endpoint critici con alert automatici.