

# Report Esercizio 10/02/2025

## Analisi Log Splunk Leonardo Catalano

“La traccia di oggi ci chiede di effettuare un’analisi con Splunk di un log “ssh.log.”

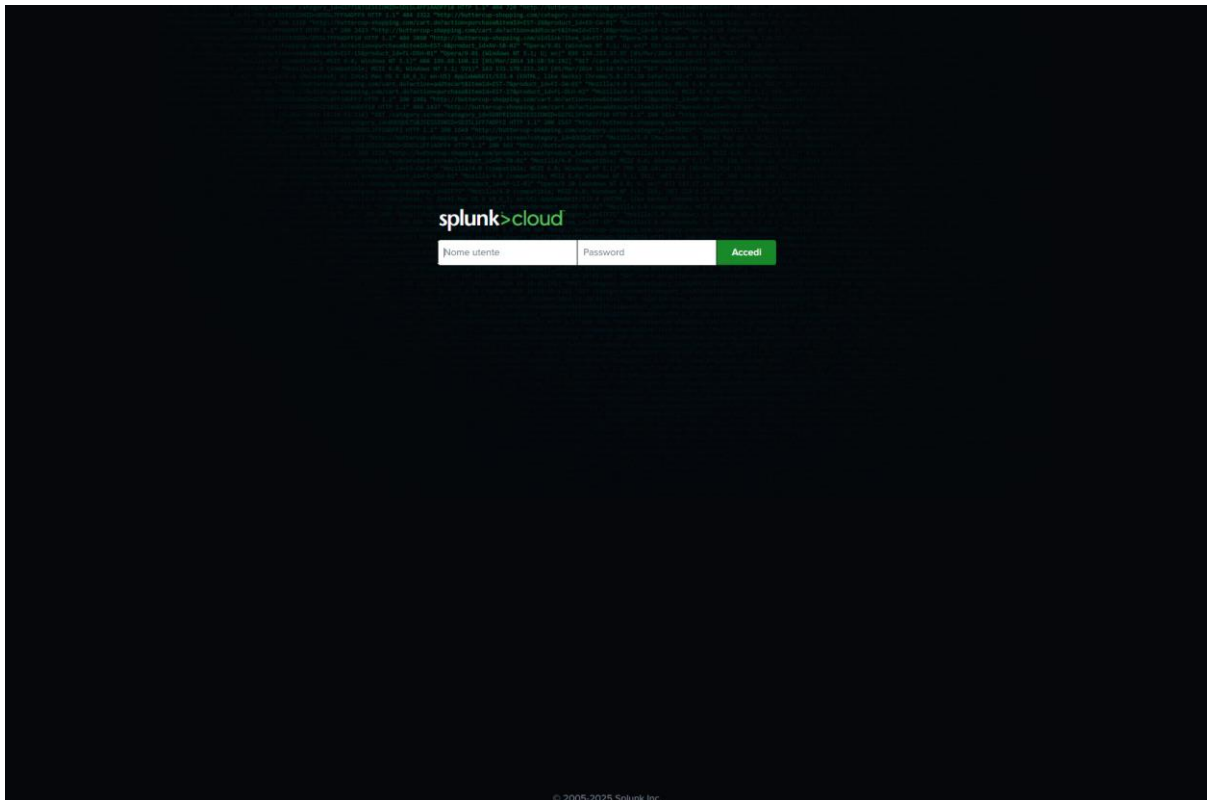
Le fasi da effettuare saranno le seguenti:

1. Identificare ed analizzare gli elementi rilevanti, (ovvero login falliti, tentativi di attacco, traffico anomalo).

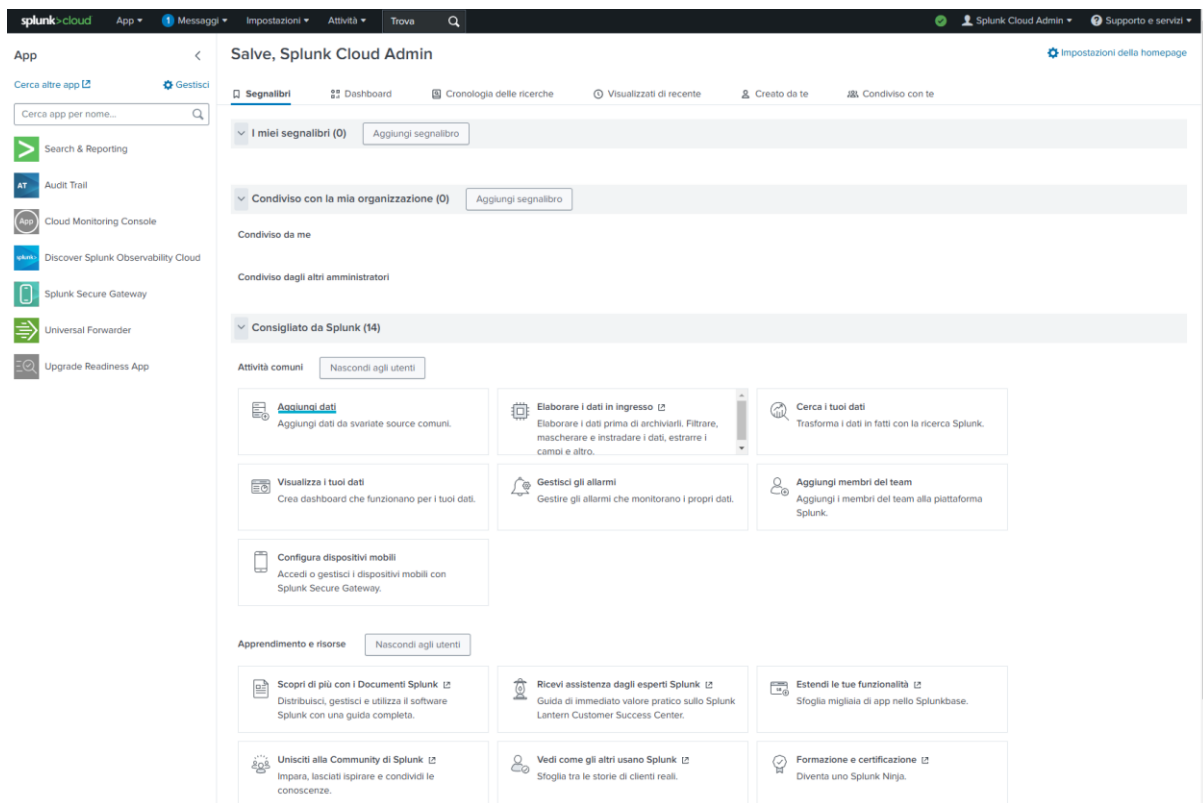
### -Splunk CloudMacchina Kali Linux:

Per poter effettuare l’analisi con Splunk, in questo caso utilizzo Splunk Cloud.

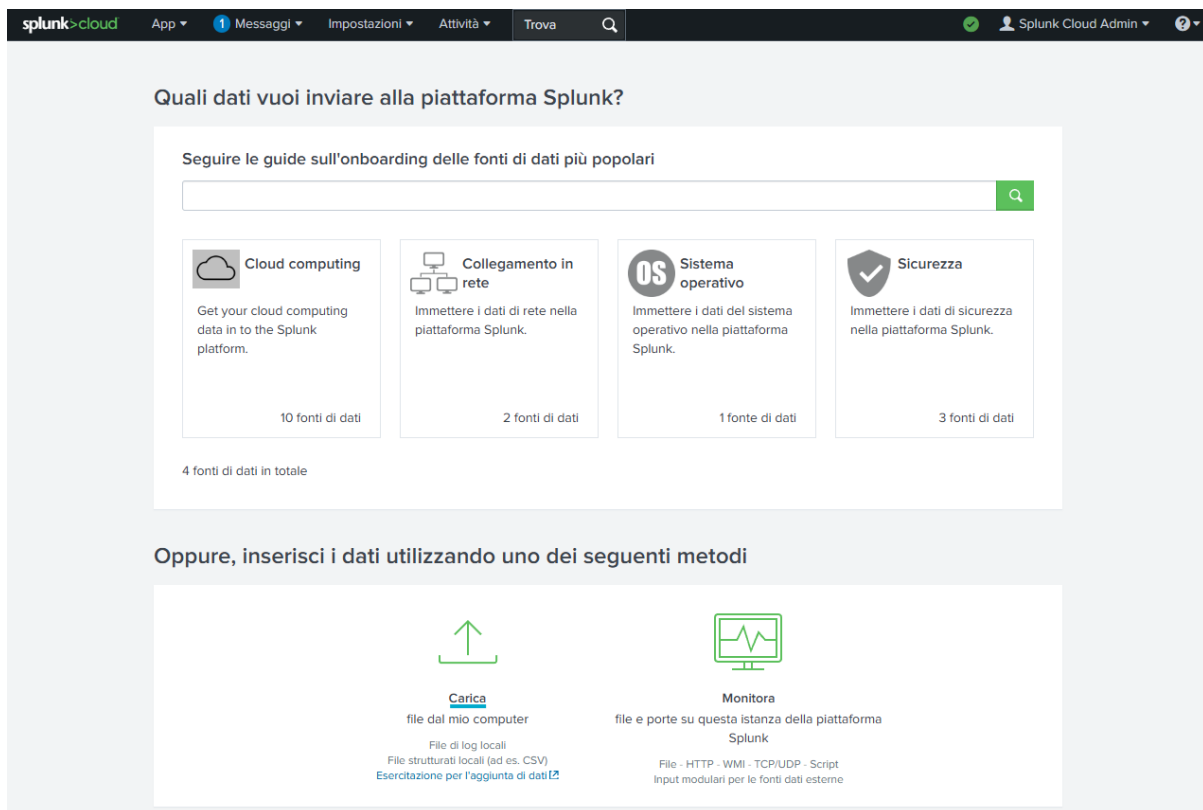
Per poter utilizzare Splunk Cloud dovremo registrarsi sul sito e utilizzare le credenziali ricevute per accedere alla nostra interfaccia privata di Splunk Cloud.



Una volta inserito i dati di login avremo la nostra interfaccia privata di Splunk Cloud.



Andando nella sezione Aggiungi dati possiamo uploadare il file "ssh.log".



splunkcloudApp1MessaggiImpostazioniAttivitàTrovaSplunk Cloud Admin

Aggiungi datiSeleziona sourceImposta source typeImpostazioni di inputVerificaFineIndietroAvanti

### Seleziona source

Scegliere un file da caricare nella piattaforma Splunk, cercando nel computer oppure trascinandolo nella casella di destinazione qui di seguito. [Ulteriori informazioni](#)

File selezionato: **ssh.log**

Seleziona file

Trascina i file di dati qui

La dimensione di caricamento massima per i file è di 500 MB

File caricato con successo.

#### Domande frequenti

- Quali tipi di file può indicizzare la piattaforma Splunk?
- Che cos'è una fonte dati (source)?
- Come faccio a inserire i dati remoti nella mia piattaforma Splunk?

Da selezione file scegliamo il file da uploudare "ssh.log" e andiamo avanti.

splunkcloudApp1MessaggiImpostazioniAttivitàTrovaSplunk Cloud AdminSupporto e servizi

Aggiungi datiSeleziona sourceImposta source typeImpostazioni di inputVerificaFineIndietroAvanti

### Imposta source type

Questa pagina consente di vedere come la piattaforma Splunk visualizza i dati prima dell'indicizzazione. Se gli eventi appaiono corretti e hanno i timestamp giusti, fare clic su "Avanti" per continuare. In caso contrario, utilizzare le opzioni di seguito per definire le suddivisioni in eventi e i timestamp corretti. Se non si è in grado di trovare un source type appropriato per i dati, crearne uno nuovo facendo clic su "Salva come".

Source: **ssh.log**

Source type: defaultSalva come

Suddivisioni in eventiTimestampAvanzate

	Ora	Evento
1	10/02/25 13:52:46,000	1331901011.840000 CTHC0o3BAR0OPDJYue nSSH_5_0 SSH-1.99-Cisco-1.25 - 192.168.202.68 53633 192.168.28.254 22 failure INBOUND SSH-2.0-Ope timestamp = none
2	10/02/25 13:52:46,000	1331901030.210000 CBHpSz2Z13rdKbAvvd nSSH_5_0 SSH-1.99-Cisco-1.25 - 192.168.202.68 35820 192.168.23.254 22 failure INBOUND SSH-2.0-Ope timestamp = none
3	10/02/25 13:52:46,000	1331901032.030000 C2h6wz2S5MWTIAk6Hb nSSH_5_0 SSH-1.99-Cisco-1.25 - 192.168.202.68 36254 192.168.26.254 22 failure INBOUND SSH-2.0-Ope timestamp = none
4	10/02/25 13:52:46,000	1331901034.340000 CeV76r1JXPbjJ58yKb nSSH_5_0 SSH-2.0-OpenSSH_5.8p1 Debian-tubuntu3 - 192.168.202.68 37764 192.168.27.102 22 failure INBOUND SSH-2.0-Ope timestamp = none
5	10/02/25 13:52:46,000	1331901041.920000 CPJHML3uGn4IV2MGWi nSSH_5_0 SSH-2.0-OpenSSH_5.8p1 Debian-7ubuntu1 - 192.168.202.68 40244 192.168.27.101 22 failure INBOUND SSH-2.0-Ope timestamp = none
6	10/02/25 13:52:46,000	1331901079.500000 CENo31KCFmQXZ00k nSSH_5_0 SSH-2.0-OpenSSH_5.8p1 Debian-tubuntu3 - 192.168.202.68 36127 192.168.27.202 22 failure INBOUND SSH-2.0-Ope timestamp = none
7	10/02/25 13:52:46,000	1331901097.470000 C6CHGN11FXTDZ00nk nSSH_5_0 SSH-2.0-OpenSSH_5.8p1 Debian-tubuntu3 - 192.168.202.68 36700 192.168.25.202 22 failure INBOUND SSH-2.0-Ope timestamp = none
8	10/02/25 13:52:46,000	1331901115.030000 CrIry24rv0Rpn3PCe2 nSSH_5_0 SSH-2.0-OpenSSH_5.8p1 Debian-7ubuntu1 - 192.168.202.68 41737 192.168.25.101 22 failure INBOUND SSH-2.0-Ope timestamp = none
9	10/02/25 13:52:46,000	1331901153.280000 Cv5b8P1NEoRNg0vGR9 nSSH_5_0 SSH-2.0-OpenSSH_5.8p1 Debian-tubuntu3 - 192.168.202.68 42331 192.168.25.102 22 failure INBOUND SSH-2.0-Ope timestamp = none
10	10/02/25 13:52:46,000	1331901866.390000 Cz0bMSKRfX0BicrK1 nSSH_5_0 SSH-2.0-OpenSSH_5.8p1 Debian-7ubuntu1 - 192.168.202.79 44642 192.168.229.101 22 undetermined INBOUND - timestamp = none
11	10/02/25 13:52:46,000	1331901866.390000 Cr0HEJ4pfTtKAd2wt6 nSSH_5_0 SSH-2.0-OpenSSH_4.3 - 192.168.202.79 33525 192.168.229.156 22 undetermined INBOUND - timestamp = none
12	10/02/25 13:52:46,000	1331901877.420000 C4v10V3Yw437mJu3Fe nSSH_5_0 SSH-1.99-Cisco-1.25 - 192.168.202.79 44850 192.168.229.254 22 undetermined INBOUND - timestamp = none

Ora dovremo impostare il source Type, per permettere a Splunk di visualizzare in

maniera corretta i dati, lasciando quello di default si può vedere che cmq va bene e ci sono i primi log di tentativi falliti di login "failure INBOUND SSH" da parte dell'indirizzo 192.168.202.68.

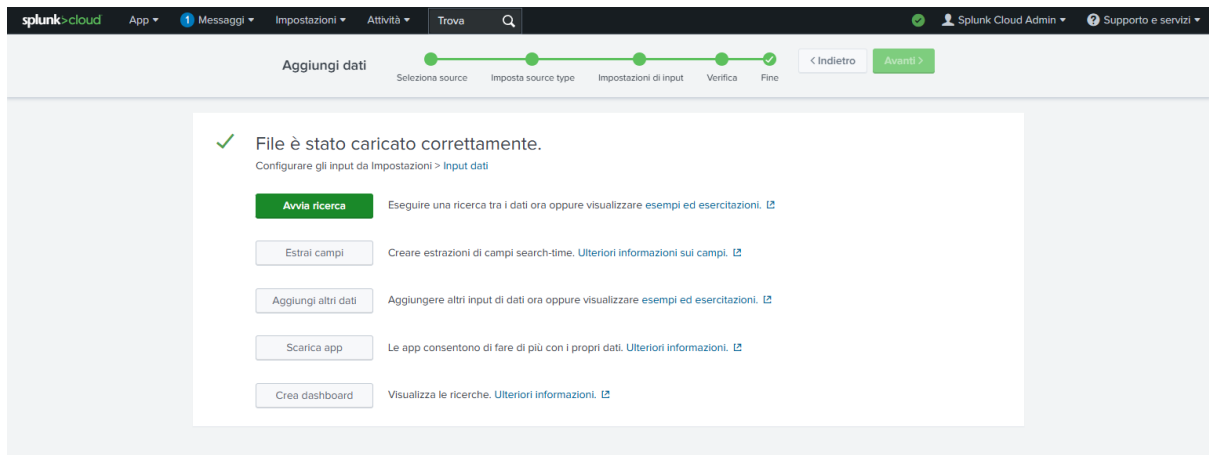
Andando avanti andremo ad impostare i parametri di input.

The screenshot shows the 'Impostazioni di input' (Input Settings) page in the Splunk Cloud interface. The page is part of the 'Aggiungi dati' (Add Data) workflow, with steps: Seleziona source, Imposta source type, Impostazioni di input, Verifica, and Fine. The 'Impostazioni di input' step is currently active. It contains instructions for setting the 'Host' and 'Indice' (Index). The 'Host' field is set to 'si-i-0c43a0a52f036df4f.prd-p-oaggqi.sj' and the 'Indice' is set to 'Default'. There are also links for 'Ulteriori informazioni' (More information) and a 'Domande frequenti' (Frequently asked questions) section.

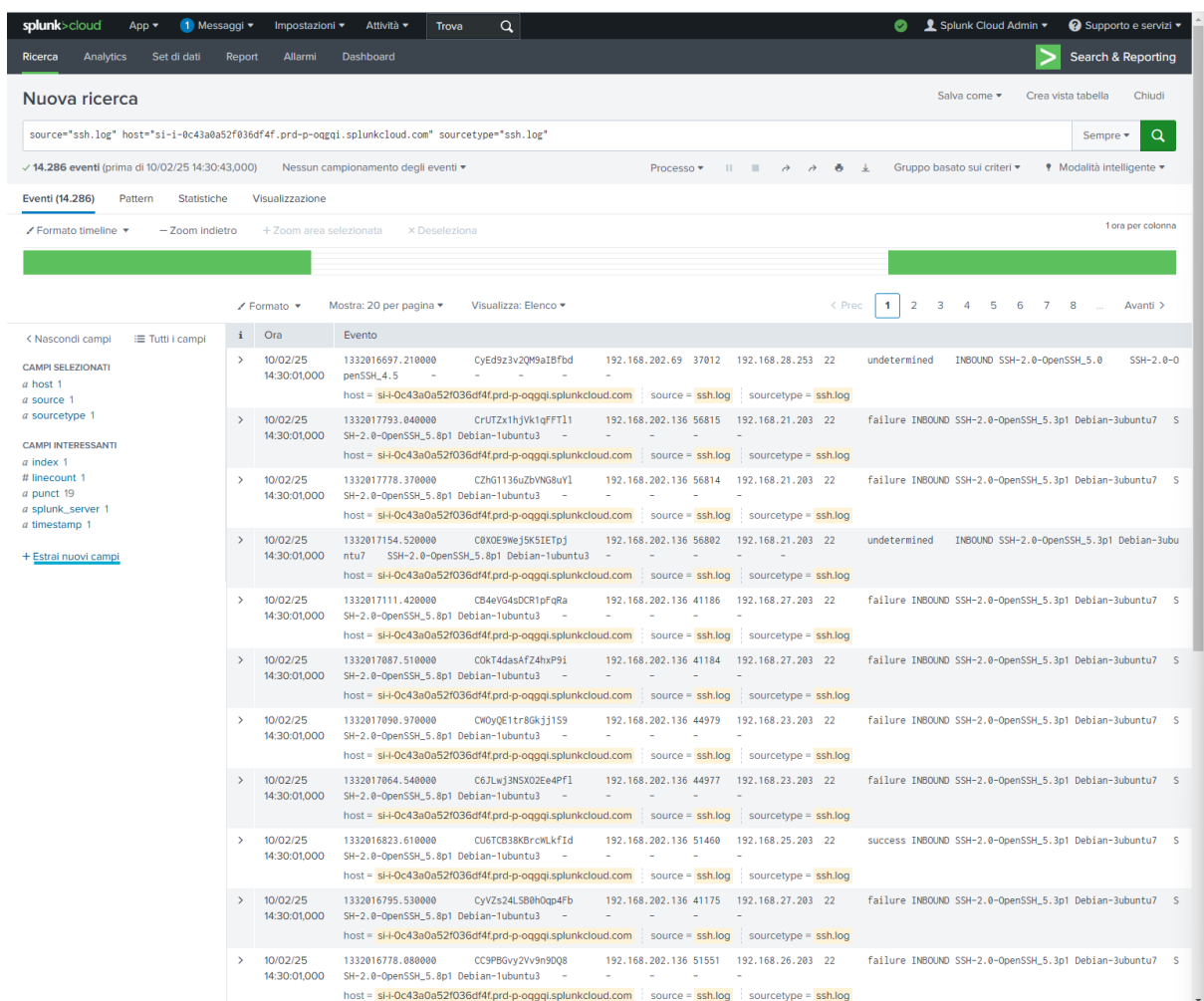
In questo caso lascio i parametri di Default e vado su "Verifica".

The screenshot shows the 'Verifica' (Verify) page in the Splunk Cloud interface. It displays a summary of the configuration: 'Tipo di input' (Input type) is 'File caricato' (Uploaded file), 'Nome file' (File name) is 'ssh.log', 'Source type' is 'ssh.log', 'Host' is 'si-i-0c43a0a52f036df4f.prd-p-oaggqi.splunkcloud.com', and 'Indice' (Index) is 'Default'. The 'Invia' (Send) button is highlighted in green.

Invio il file e le impostazioni:



Da cui possiamo avviare la ricerca, ed estrarre i campi interessati con le query:



Questa è l'interfaccia finale, da cui possiamo modificare la query e i filtri per andare a ricercare soltanto dei determinati log.

Se andiamo su Estrai nuovi campi, ci si aprirà un'interfaccia dove potremmo andare ad applicare dei filtri sui log .

Settando il tempo sugli ultimi 90 giorni, come numero eventi 10.000 e su "filtro" possiamo andare a scrivere il filtro che vogliamo, il 1° controllo che faccio è sui failure per vedere quanti sono.

✓ 1.960 eventi (prima di 10/02/25 14:50:25,000)
20 per pagina
< Prec.
1
2
3
4
5
6
7
8
...
Avanti >

_raw											
1332017793.040000	CrUTZx1hjVklqFFT11	192.168.202.136	56815	192.168.21.203	22	failure INBOUND SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7	SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3	-	-	-	-
1332017778.370000	CZhG1136uZbVNG8uYl	192.168.202.136	56814	192.168.21.203	22	failure INBOUND SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7	SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3	-	-	-	-
1332017111.420000	CB4eVG4sDCR1pFqRa	192.168.202.136	41186	192.168.27.203	22	failure INBOUND SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7	SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3	-	-	-	-
1332017087.510000	COKT4dasAfZ4hxP9l	192.168.202.136	41184	192.168.27.203	22	failure INBOUND SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7	SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3	-	-	-	-
1332017090.970000	CW0yQE1tr8GkjJ1S9	192.168.202.136	44979	192.168.23.203	22	failure INBOUND SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7	SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3	-	-	-	-
1332017064.540000	C6JLwj3NSXO2Ee4PF1	192.168.202.136	44977	192.168.23.203	22	failure INBOUND SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7	SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3	-	-	-	-
1332016795.530000	CyVzs24LS0hOqp4Fb	192.168.202.136	41175	192.168.27.203	22	failure INBOUND SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7	SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3	-	-	-	-
1332016778.080000	CC9PBGvy2Vv9n3Q08	192.168.202.136	51551	192.168.26.203	22	failure INBOUND SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7	SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3	-	-	-	-
1332016737.580000	CEe3kws3yn1nWlGh3	192.168.202.136	51549	192.168.26.203	22	failure INBOUND SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7	SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3	-	-	-	-
1332016700.380000	Cx0BosKL4U3BztR7	192.168.202.136	41171	192.168.27.203	22	failure INBOUND SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7	SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3	-	-	-	-
1332016697.140000	C1D6v73pWtLrLznhk	192.168.202.69	36782	192.168.26.203	22	failure INBOUND SSH-2.0-OpenSSH_5.0	SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3	-	-	-	-
1332016117.960000	Cs98WG30oUF4o3JCc	192.168.202.136	43815	192.168.25.253	22	failure INBOUND SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7	SSH-2.0-OpenSSH_4.5	-	-	-	-
1332016093.390000	CQ3yf24THfNo9TJIH4	192.168.202.136	49316	192.168.24.253	22	failure INBOUND SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7	SSH-2.0-OpenSSH_4.5	-	-	-	-
1332016069.920000	CDPaSrARYJJjKlN8	192.168.202.136	49314	192.168.24.253	22	failure INBOUND SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7	SSH-2.0-OpenSSH_4.5	-	-	-	-
1332015982.680000	ChRy9H38H0xtOmJ023	192.168.202.136	33059	192.168.23.253	22	failure INBOUND SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7	SSH-2.0-OpenSSH_4.5	-	-	-	-
1332015954.440000	CP5R321S3mJV7UEGv8	192.168.202.136	33057	192.168.23.253	22	failure INBOUND SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7	SSH-2.0-OpenSSH_4.5	-	-	-	-
1332015936.780000	Chq1SM20Cv09wJwAh	192.168.202.136	60265	192.168.21.102	22	failure INBOUND SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7	SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3	-	-	-	-
1332014961.000000	C9Xd7rlrqWvxdE7h	192.168.202.136	56568	192.168.21.203	22	failure INBOUND SSH-2.0-Nmap-SSH2-Hostkey	SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3	-	-	-	-
1332014961.040000	Ch5j9guzUhp0lkcA6	192.168.202.136	60076	192.168.21.102	22	failure INBOUND SSH-2.0-Nmap-SSH2-Hostkey	SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3	-	-	-	-
1332014960.620000	C4wXMJ3QXd18LqZZc	192.168.202.136	56543	192.168.21.203	22	failure INBOUND SSH-2.0-Nmap-SSH2-Hostkey	SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3	-	-	-	-

Analizzando i tentativi falliti di Inbound con L’SSH al Web Server Debian, noto che c’è un attaccante che fa parte della rete 192.168.21.0 che con vari indirizzi ip sta attaccando varie macchine con diversi indirizzi ip anche di reti diversi (come sottolineati) per cercare di accedere con l’ssh ai web server. Ciò mi fa pensare ad un attacco di brute force.

-Filtro Undetermined:

Oltre ai tipi failure ho trovato il tipo undetermined (indeterminati) e anche qui trovo tentativi di accesso “falliti” ma anche degli Nmap sugli host.

Eventi

✓ 32 eventi (prima di 10/02/25 14:59:46,000)

20 per pagina

< Prec

1

2

Avanti >

undetermined

Applica

Esempio: 10.000 eventi ▼

Tutti gli eventi ▼

\_raw

1332016697.210000	CyEd9z3v2QM9aIBfb	192.168.202.69	37012	192.168.28.253	22	undetermined	INBOUND	SSH-2.0-OpenSSH_5.0	SSH-2.0-OpenSSH_4.5	-	-	-	-	-
1332017154.520000	C0XOE9weJ5KSIETpJ	192.168.202.136	56802	192.168.21.203	22	undetermined	INBOUND	SSH-2.0-OpenSSH_5.3p1	Debian-3ubuntu7	SSH-2.0-OpenSSH_5.8p1	Debian-1ubuntu3	-	-	-
1332016648.650000	C9QMwZ2HnZJ0yQh011	192.168.202.136	33529	192.168.28.253	22	undetermined	INBOUND	SSH-2.0-OpenSSH_5.3p1	Debian-3ubuntu7	SSH-2.0-OpenSSH_4.5	-	-	-	-
1332016065.680000	CTWHDFFzXZnBNHBq7	192.168.202.136	48999	192.168.21.253	22	undetermined	INBOUND	SSH-2.0-OpenSSH_5.3p1	Debian-3ubuntu7	SSH-1.99-OpenSSH_4.5	-	-	-	-
1332015948.270000	CTRmqT1JbgTQECItIf	192.168.202.136	48992	192.168.21.253	22	undetermined	INBOUND	SSH-2.0-OpenSSH_5.3p1	Debian-3ubuntu7	SSH-1.99-OpenSSH_4.5	-	-	-	-
1332011665.090000	CapkM63Pls4ZQYFWmk	192.168.202.68	43693	192.168.28.253	22	undetermined	INBOUND	SSH-2.0-OpenSSH_5.0	SSH-2.0-OpenSSH_4.5	-	-	-	-	-
1332014962.420000	C9eUXI3GSamu4rvinc	192.168.202.136	48897	192.168.21.253	22	undetermined	INBOUND	SSH-2.0-Nmap-SSH2-Hostkey	SSH-1.99-OpenSSH_4.5	-	-	-	-	-
1332014962.120000	CvGvWX2pw7tRDE45p1	192.168.202.136	56642	192.168.21.203	22	undetermined	INBOUND	SSH-1.5-NmapNSE_1.0	SSH-2.0-OpenSSH_5.8p1	Debian-1ubuntu3	-	-	-	-
1332014962.160000	CqRmU2YHenc5nUXi	192.168.202.136	48883	192.168.21.253	22	undetermined	INBOUND	SSH-2.0-Nmap-SSH2-Hostkey	SSH-1.99-OpenSSH_4.5	-	-	-	-	-
1332014961.950000	KczM6a2xK1krWRGv4	192.168.202.136	48869	192.168.21.253	22	undetermined	INBOUND	SSH-1.5-Nmap-SSH1-Hostkey	SSH-1.99-OpenSSH_4.5	-	-	-	-	-
1332014961.840000	C0sIst4WvDtA5CAD02	192.168.202.136	48861	192.168.21.253	22	undetermined	INBOUND	SSH-1.5-NmapNSE_1.0	SSH-1.99-OpenSSH_4.5	-	-	-	-	-
1332014961.450000	C1dN9xRjGsluup936	192.168.202.136	60105	192.168.21.102	22	undetermined	INBOUND	SSH-1.5-NmapNSE_1.0	SSH-2.0-OpenSSH_5.8p1	Debian-1ubuntu3	-	-	-	-
1332014960.260000	CF5qT13pB1V35QL4P1	192.168.202.136	56523	192.168.21.203	22	undetermined	INBOUND	SSH-1.5-Nmap-SSH1-Hostkey	SSH-2.0-OpenSSH_5.8p1	Debian-1ubuntu3	-	-	-	-
1332014960.250000	CaeoRv2ZEj5ctI8421	192.168.202.136	60023	192.168.21.102	22	undetermined	INBOUND	SSH-1.5-Nmap-SSH1-Hostkey	SSH-2.0-OpenSSH_5.8p1	Debian-1ubuntu3	-	-	-	-
1332014883.950000	C8Bw6F2JD1ASZt0Z1h	192.168.202.102	4380	192.168.21.253	22	undetermined	INBOUND	SSH-1.5-ssh.py	SSH-1.99-OpenSSH_4.5	-	-	-	-	-
1332013747.050000	Cp7tq32KsWLYxpFKgd	192.168.202.141	8122	192.168.229.101	22	undetermined	INBOUND	-	SSH-2.0-OpenSSH_5.8p1	Debian-7ubuntu1	-	-	-	-
1332016697.210000	CyEd9z3v2QM9aIBfb	192.168.202.69	37012	192.168.28.253	22	undetermined	INBOUND	SSH-2.0-OpenSSH_5.0	SSH-2.0-OpenSSH_4.5	-	-	-	-	-
1332017154.520000	C0XOE9weJ5KSIETpJ	192.168.202.136	56802	192.168.21.203	22	undetermined	INBOUND	SSH-2.0-OpenSSH_5.3p1	Debian-3ubuntu7	SSH-2.0-OpenSSH_5.8p1	Debian-1ubuntu3	-	-	-
1332016648.650000	C9QMwZ2HnZJ0yQh011	192.168.202.136	33529	192.168.28.253	22	undetermined	INBOUND	SSH-2.0-OpenSSH_5.3p1	Debian-3ubuntu7	SSH-2.0-OpenSSH_4.5	-	-	-	-
1332016065.680000	CTWHDFFzXZnBNHBq7	192.168.202.136	48999	192.168.21.253	22	undetermined	INBOUND	SSH-2.0-OpenSSH_5.3p1	Debian-3ubuntu7	SSH-1.99-OpenSSH_4.5	-	-	-	-

Andando a filtrare soltanto gli nmap, negli ultimi 90 giorni non c'è alcun nmap che ha avuto successo, solo undetermined e failure.



## Eventi

✓ 24 eventi (prima di 10/02/25 15:02:05,000)

20 per pagina ▾ < Prec **1** 2 Avanti >

nmap Applica Esempio: 10.000 eventi ▼ Tutti gli eventi ▼

row	id	ip	port	os	arch	bits	lang	type	method	target	result	comment	date	time
1332014362.420000	-	C9eUXI3GSamu4rvinc	192.168.202.136	48897	192.168.21.253	22	undetermined	INBOUND	SSH-2.0-Nmap-SSH2-Hostkey	SSH-1.99-OpenSSH_4.5	-	-	-	-
1332014362.120000	-	CvGvWX2pw7RDE45p1	192.168.202.136	56642	192.168.21.203	22	undetermined	INBOUND	SSH-1.5-NmapNSE_1.0	SSH-2.0-OpenSSH_5.8p1	Debian-1ubuntu3	-	-	-
1332014362.160000	-	CqRmIu2YhGenc5nLXI	192.168.202.136	48883	192.168.21.253	22	undetermined	INBOUND	SSH-2.0-Nmap-SSH2-Hostkey	SSH-1.99-OpenSSH_4.5	-	-	-	-
1332014361.950000	-	CkzM6a2xKK1krWRGv4	192.168.202.136	48869	192.168.21.253	22	undetermined	INBOUND	SSH-1.5-Nmap-SSH1-Hostkey	SSH-1.99-OpenSSH_4.5	-	-	-	-
1332014361.840000	-	COs1st4wvDTA5CAD02	192.168.202.136	48861	192.168.21.253	22	undetermined	INBOUND	SSH-1.5-NmapNSE_1.0	SSH-1.99-OpenSSH_4.5	-	-	-	-
1332014361.450000	-	CIdN9xRJGslUup936	192.168.202.136	60105	192.168.21.102	22	undetermined	INBOUND	SSH-1.5-NmapNSE_1.0	SSH-2.0-OpenSSH_5.8p1	Debian-1ubuntu3	-	-	-
1332014361.000000	-	C9Xd7r1rqHvxxdE7h	192.168.202.136	56568	192.168.21.203	22	failure	INBOUND	SSH-2.0-Nmap-SSH2-Hostkey	SSH-2.0-OpenSSH_5.8p1	Debian-1ubuntu3	-	-	-
1332014361.040000	-	ChSJ9guzUHoPkca6	192.168.202.136	60076	192.168.21.102	22	failure	INBOUND	SSH-2.0-Nmap-SSH2-Hostkey	SSH-2.0-OpenSSH_5.8p1	Debian-1ubuntu3	-	-	-
1332014360.620000	-	C4wXMJ3QdXf8LqQZ2c	192.168.202.136	55543	192.168.21.203	22	failure	INBOUND	SSH-2.0-Nmap-SSH2-Hostkey	SSH-2.0-OpenSSH_5.8p1	Debian-1ubuntu3	-	-	-
1332014360.630000	-	CmS3YU3t21Hb2B7Bfc	192.168.202.136	60051	192.168.21.102	22	failure	INBOUND	SSH-2.0-Nmap-SSH2-Hostkey	SSH-2.0-OpenSSH_5.8p1	Debian-1ubuntu3	-	-	-
1332014360.260000	-	CfSqt13pB1V35QL4P1	192.168.202.136	56523	192.168.21.203	22	undetermined	INBOUND	SSH-1.5-Nmap-SSH1-Hostkey	SSH-2.0-OpenSSH_5.8p1	Debian-1ubuntu3	-	-	-
1332014360.250000	-	CaeORvZ2eJ5t1B421	192.168.202.136	60023	192.168.21.102	22	undetermined	INBOUND	SSH-1.5-Nmap-SSH1-Hostkey	SSH-2.0-OpenSSH_5.8p1	Debian-1ubuntu3	-	-	-
1332014362.420000	-	C9eUXI3GSamu4rvinc	192.168.202.136	48897	192.168.21.253	22	undetermined	INBOUND	SSH-2.0-Nmap-SSH2-Hostkey	SSH-1.99-OpenSSH_4.5	-	-	-	-
1332014362.120000	-	CvGvWX2pw7RDE45p1	192.168.202.136	56642	192.168.21.203	22	undetermined	INBOUND	SSH-1.5-NmapNSE_1.0	SSH-2.0-OpenSSH_5.8p1	Debian-1ubuntu3	-	-	-
1332014362.160000	-	CqRmIu2YhGenc5nLXI	192.168.202.136	48883	192.168.21.253	22	undetermined	INBOUND	SSH-2.0-Nmap-SSH2-Hostkey	SSH-1.99-OpenSSH_4.5	-	-	-	-
1332014361.950000	-	CkzM6a2xKK1krWRGv4	192.168.202.136	48869	192.168.21.253	22	undetermined	INBOUND	SSH-1.5-Nmap-SSH1-Hostkey	SSH-1.99-OpenSSH_4.5	-	-	-	-
1332014361.840000	-	COs1st4wvDTA5CAD02	192.168.202.136	48861	192.168.21.253	22	undetermined	INBOUND	SSH-1.5-NmapNSE_1.0	SSH-1.99-OpenSSH_4.5	-	-	-	-
1332014361.450000	-	CIdN9xRJGslUup936	192.168.202.136	60105	192.168.21.102	22	undetermined	INBOUND	SSH-1.5-NmapNSE_1.0	SSH-2.0-OpenSSH_5.8p1	Debian-1ubuntu3	-	-	-
1332014361.000000	-	C9Xd7r1rqHvxxdE7h	192.168.202.136	56568	192.168.21.203	22	failure	INBOUND	SSH-2.0-Nmap-SSH2-Hostkey	SSH-2.0-OpenSSH_5.8p1	Debian-1ubuntu3	-	-	-
1332014361.040000	-	ChSJ9guzUHoPkca6	192.168.202.136	60076	192.168.21.102	22	failure	INBOUND	SSH-2.0-Nmap-SSH2-Hostkey	SSH-2.0-OpenSSH_5.8p1	Debian-1ubuntu3	-	-	-