

Analisi del malware e Splunk - rsyslog

Cybersecurity & Ethical Hacking

Matteo Mattia

INDICE GENERALE

INTRODUZIONE

[OFFICIAL]

1. Installazione e configurazione di Splunk
2. Importazione dei dati
3. Query eseguite e risultati principali
4. Conclusioni sull'analisi dei log con Splunk (utilizzando AI)

[EXTRA] rsyslog

CONCLUSIONE

INTRODUZIONE

In questo progetto ho utilizzato Splunk Enterprise per analizzare log di sicurezza e accesso a un server, importando il dataset di esempio "tutorialdata.zip" fornito dalla documentazione ufficiale Splunk.

L'obiettivo è stato installare Splunk su un ambiente Kali Linux in VirtualBox, caricare i dati e creare query SPL (Search Processing Language) specifiche per identificare pattern critici: tentativi di accesso falliti via SSH, sessioni aperte con successo, attività sospette da un IP specifico, fonti di attacco più attive e errori applicativi sul server web.

Grazie a questa analisi ho potuto evidenziare vulnerabilità e comportamenti anomali nei log, simulando un contesto reale di monitoraggio della sicurezza.

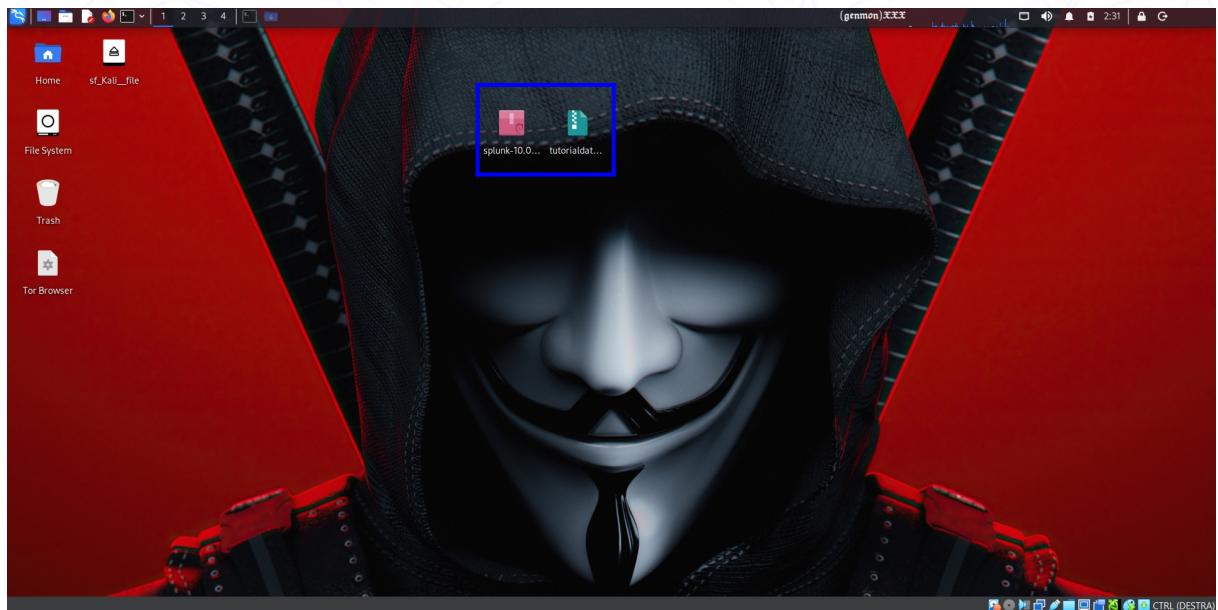
L'analisi si è estesa anche alla configurazione di un'infrastruttura di centralizzazione dei log tramite rsyslog, implementando un sistema per ricevere i log di un client Windows su un server Kali Linux.

[OFFICIAL]

1. Installazione e configurazione di Splunk

Ho scaricato e installato Splunk Enterprise versione 10.0.1 su Kali Linux tramite pacchetto .deb

<https://download.splunk.com/products/splunk/releases/10.0.1/linux/splunk-10.0.1-c486717c322b-linux-amd64.deb>



Ho avviato Splunk risolvendo conflitti di librerie (utilizzando LD_LIBRARY_PATH per compatibilità OpenSSL).

```
Certificate request self-signature ok
subject=CN = kali, O = SplunkUser
Done

Waiting for web server at http://127.0.0.1:8000 to be available..... Done

If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com

The Splunk web interface is at http://kali:8000

(M6D6R6㉿kali)-[~]
```

Ho effettuato l'accesso all'interfaccia web su <http://localhost:8000> con credenziali impostate via terminale.



The dashboard interface for Splunk Enterprise. At the top, it says "Hello, Administrator". Below this are sections for "Bookmarks", "Dashboard", "Search history", "Recently viewed", "Created by you", and "Shared with you". On the left, there is a sidebar titled "Apps" with a list of available apps: "Search & Reporting", "Audit Trail", "Data Management", "Discover Splunk Observability Cloud", "Splunk Secure Gateway", and "Upgrade Readiness App". A message at the bottom of the sidebar says "Find more apps" and "Manage".

2. Importazione dei dati

Ho caricato il file "tutorialdata.zip" tramite "Add Data > Upload" in Splunk.

The screenshot shows the 'Add Data' wizard in Splunk. The current step is 'Select Source'. A green dot indicates the task is complete. The progress bar has five steps: 'Select Source' (green), 'Set Source Type' (white), 'Input Settings' (white), 'Review' (white), and 'Done' (white). Below the progress bar, the text 'Selected File: tutorialdata.zip' is displayed, along with a 'Select File' button. A large input field below it also shows 'Selected File: tutorialdata.zip'. To the right of the input field is a placeholder 'Drop your data file here'. Below this, a message states 'The maximum file upload size is 500 Mb'. At the bottom right of the screen, a green checkmark icon and the text 'File Successfully Uploaded' are visible.

I dati sono stati indicizzati nell'index "main" con sourcetype principale "secure-2" per i log SSH e sourcetype compatibile per i log web.

L'indicizzazione è stata completata con successo, rendendo disponibili 439.456 eventi ricercabili, come dimostrato dalla query di verifica sulla source "tutorialdata.zip*"

The screenshot shows the Splunk search interface with a search bar containing 'source="tutorialdata.zip*"' and a result count of '439,456 events (before 12/20/25 2:59:58.000 AM)'. The 'Events' tab is selected, showing 439,456 events. The timeline format is set to 'Timeline format'. The search results table has columns for 'Time' and 'Event'. One event is highlighted in yellow: '12/18/25 6:46:11:000 PM host = kali | source = tutorialdata.zip./mailsv1.secure.log | sourcetype = secure-2'. The event details show 'Thu Dec 18 2025 18:46:11 mailsv1 sshd[5276]: Failed password for invalid user appserver from 194.8.74.23 port 3351 ssh2 host = kali | source = tutorialdata.zip./mailsv1.secure.log | sourcetype = secure-2'. The bottom of the table shows other events, including one for '12/18/25 7:06:11:000 PM'.

3. Query eseguite e risultati principali

Query 1 – Identificazione di tutti i tentativi di accesso falliti ("Failed password")

New Search

```
index=main sourcetype=secure-2 "Failed password"
| rex "Failed password for (invalid user )?(?<user>\S+) from (?<src_ip>\S+) port (?<port>\d+)"
| eval reason="Failed password"
| table _time src_ip user reason
```

✓ 33,253 events (before 12/20/25 1:49:22.000 AM) No Event Sampling ▾

Events Patterns Statistics (33,253) Visualization

Show: 20 Per Page ▾ Format ▾ Preview: On

Risultato: ho identificato 33.253 eventi, con timestamp, IP di origine, nome utente e motivo del fallimento.

_time	src_ip	user	reason
2025-12-16 18:46:09	133.30.188.208	henri	Failed password
2025-12-16 18:46:09	123.30.188.208	root	Failed password
2025-12-16 18:46:09	128.241.220.82	helpdesk	Failed password
2025-12-16 18:46:09	128.241.220.82	root	Failed password
2025-12-16 18:46:09	128.241.220.82	irc	Failed password
2025-12-16 18:46:09	128.241.220.82	services	Failed password
2025-12-16 18:46:09	128.241.220.82	prince	Failed password
2025-12-16 18:46:09	128.241.220.82	root	Failed password
2025-12-16 18:46:09	128.241.220.82	sys	Failed password
2025-12-16 18:46:09	128.241.220.82	sunny	Failed password
2025-12-16 18:46:09	128.241.220.82	icinga	Failed password
2025-12-16 18:46:09	128.241.220.82	email	Failed password
2025-12-16 18:46:09	128.241.220.82	harrison	Failed password
2025-12-16 18:46:09	128.241.220.82	desktop	Failed password
2025-12-16 18:46:09	128.241.220.82	operator	Failed password
2025-12-16 18:46:09	128.241.220.82	none	Failed password
2025-12-16 18:46:09	128.241.220.82	administrator	Failed password
2025-12-16 18:46:09	128.241.220.82	informix	Failed password
2025-12-16 18:46:09	187.231.45.62	vpxuser	Failed password
2025-12-16 18:46:09	187.231.45.62	ubuntu	Failed password

Query 2 – Sessioni SSH aperte con successo per l'utente “djohnson”

New Search

```
index=main sourcetype=secure-2 "session opened" "djohnson"
| rex "session opened for user djohnson by \(uid=(?<uid>\d+)\\""
| table _time uid
```

✓ 1,269 events (before 12/20/25 1:51:24.000 AM)

No Event Sampling ▾

Events

Patterns

Statistics (1,269)

Visualization

Risultato: ho trovato 1.269 eventi, tutti con uid=0 (privilegi root).

_time	uid
2025-12-18 18:46:08	0
2025-12-18 18:46:08	0
2025-12-18 18:46:08	0
2025-12-18 18:46:08	0
2025-12-18 18:46:08	0
2025-12-18 18:46:08	0
2025-12-18 18:46:08	0
2025-12-18 18:46:08	0
2025-12-18 18:46:08	0
2025-12-18 18:46:08	0
2025-12-18 18:46:08	0
2025-12-18 18:46:08	0
2025-12-18 18:46:08	0
2025-12-18 18:46:08	0
2025-12-18 18:46:08	0
2025-12-18 18:46:08	0
2025-12-18 18:46:08	0
2025-12-18 18:46:08	0
2025-12-18 18:46:08	0
2025-12-18 18:46:08	0
2025-12-18 18:46:08	0
2025-12-18 18:46:08	0
2025-12-18 18:46:08	0
2025-12-18 18:46:08	0
2025-12-18 18:46:08	0
2025-12-18 18:46:08	0
2025-12-18 18:46:08	0
2025-12-18 18:46:08	0
2025-12-18 18:46:08	0
2025-12-18 18:46:08	0
2025-12-18 18:46:08	0
2025-12-18 18:46:08	0
2025-12-18 18:46:08	0

Query 3 – Tentativi di accesso falliti dall'IP “86.212.199.60”

The screenshot shows a "New Search" interface. The search bar contains the following query:

```
index=main sourcetype=secure-2 "Failed password" "86.212.199.60"
| rex "Failed password for (invalid user )?(?<user>\$+) from 86.212.199.60 port (?<port>\d+)"
| table _time user port
```

Below the query, it says "✓ 158 events (before 12/20/25 1:52:56.000 AM)" and "No Event Sampling".

The interface includes tabs for "Events", "Patterns", "Statistics (158)", and "Visualization". The "Statistics" tab is selected. Below the tabs are buttons for "Show: 20 Per Page", "Format", and "Preview: On".

Risultato: ho rilevato 158 eventi, con timestamp, nome utente e numero di porta.

_time	user	port
2025-12-11 18:46:10	hsqlb	4379
2025-12-11 18:46:10	admin	2831
2025-12-11 18:46:10	system	4296
2025-12-11 18:46:10	alex	2121
2025-12-11 18:46:10	mantis	2735
2025-12-11 18:46:10	jira	1958
2025-12-11 18:46:10	vmore	4457
2025-12-11 18:46:10	nagios	2048
2025-12-11 18:46:10	mail	1775
2025-12-17 18:46:09	services	1393
2025-12-17 18:46:09	sync	1695
2025-12-17 18:46:09	admin	3673
2025-12-17 18:46:09	nginx	1582
2025-12-17 18:46:09	whois	1635
2025-12-17 18:46:09	mailman	4339
2025-12-17 18:46:09	mailman	1954
2025-12-17 18:46:09	rdb	2658
2025-12-16 18:46:09	ncsd	4822
2025-12-16 18:46:09	games	1763
2025-12-16 18:46:09	none	1581

Query 4 – Indirizzi IP con più di 5 tentativi falliti

New Search

```
index=main sourcetype=secure-2 "Failed password"
| rex "Failed password for (invalid user )?(?<user>\S+) from (?<src_ip>\S+)"
| stats count by src_ip
| where count > 5
| sort - count
| table src_ip count
```

✓ 33,253 events (before 12/20/25 1:54:00.000 AM) No Event Sampling ▾

Events Patterns Statistics (182) Visualization

Show: 20 Per Page ▾ Format ▾ Preview: On

Risultato: ho identificato 182 IP distinti, il più attivo è 87.194.216.51 con 19.482 tentativi, seguito da altri con migliaia di tentativi.

src_ip	count
87.194.216.51	19482
211.166.11.101	743
128.241.220.82	622
109.169.32.195	515
194.215.205.19	514
216.21.226.11	433
168.138.40.166	297
65.19.167.94	286
107.3.140.207	252
95.130.170.231	279
223.205.219.67	274
27.1.11.11	273
27.35.11.11	270
59.162.167.100	267
91.210.194.143	253
27.161.11.11	251
108.65.113.83	249
53.99.230.91	244
198.228.212.52	237
108.75.2.128	232

Query 5 – Tutti gli Internal Server Error

New Search

```
index=main status=500
| table _time clientip request status bytes
```

✓ **733 events** (before 12/20/25 1:55:27.000 AM) No Event Sampling ▾

Events Patterns **Statistics (733)** Visualization

Show: 20 Per Page ▾ Format ▾ Preview: On

Risultato: ho trovato 733 eventi di errore HTTP 500.

_time	clientip	request	status	bytes
2025-12-17 11:27:37	142.233.200.21		500	868
2025-12-17 16:16:41	201.28.169.162		500	3643
2025-12-17 09:34:27	76.89.103.115		500	297
2025-12-17 07:55:28	182.236.164.11		500	3317
2025-12-17 06:28:17	71.192.86.285		500	578
2025-12-17 06:26:31	211.166.11.191		500	622
2025-12-17 05:44:09	58.68.236.98		500	3891
2025-12-17 04:46:08	178.212.8.44		500	3482
2025-12-17 02:26:59	209.114.36.109		500	209
2025-12-17 01:52:31	196.28.38.71		500	2687
2025-12-17 01:29:59	86.212.199.68		500	629
2025-12-16 23:36:31	211.166.11.191		500	1787
2025-12-16 23:15:06	85.62.218.82		500	496
2025-12-16 22:33:15	128.241.220.82		500	1578
2025-12-16 22:21:41:19	27.175.11.11		500	1644
2025-12-16 22:14:18	27.175.11.11		500	1454
2025-12-16 18:10:01	201.42.223.29		500	3625
2025-12-16 15:02:46	221.264.246.72		500	3999
2025-12-16 14:27:37	27.182.11.11		500	2659
2025-12-16 13:00:35	2.229.4.58		500	2558

4. Conclusioni sull'analisi dei log con Splunk (utilizzando IA)

L'analisi dei log estratti da tutorialdata.zip che ho effettuato evidenzia un quadro di grave vulnerabilità del server, principalmente sul servizio SSH.

Ho rilevato **33.253 tentativi di accesso falliti** con messaggio "Failed password", generati da attacchi brute-force automatizzati su larga scala.

Tali tentativi coinvolgono **182 indirizzi IP distinti** che hanno superato i 5 eventi, con l'attaccante più attivo (**87.194.216.51**) responsabile di **19.482 tentativi**, seguito da altri IP con volumi elevati (es. 211.166.11.101 con 7.743 tentativi, 128.241.220.82 con 6.222).

I nomi utente bersaglio spaziano da account comuni (root, admin) a nomi applicativi (nagios, jira, oracle, mysql, test, guest), tipici di script con dizionari estesi.

L'indirizzo IP **86.212.199.60**, specificato nell'esame, ha prodotto **158 tentativi di accesso falliti** su diverse porte e utenti, confermando il suo ruolo come fonte attiva di attacco.

Nonostante il massiccio numero di fallimenti, ho registrato **1.269 sessioni SSH aperte con successo** per l'utente **djohnson**, tutte eseguite con privilegi di root (uid=0), indicative di intensa attività amministrativa legittima ma potenzialmente rischiosa in presenza di credenziali esposte.

Sul fronte web, ho rilevato **733 Internal Server Error (status 500)**, che possono derivare da malfunzionamenti applicativi, sovraccarico del server o tentativi di exploitation di vulnerabilità.

In sintesi, i log denunciano un sistema altamente esposto a minacce esterne, privo di adeguate contromisure, raccomando con urgenza:

- disabilitazione dell'autenticazione SSH via password in favore di chiavi pubbliche,
- implementazione di fail2ban o meccanismi simili per il blocco automatico di IP sospetti,
- configurazione di alert real-time in Splunk su tentativi falliti aggregati per IP e soglia,
- rafforzamento delle policy di accesso privilegiato e rotazione periodica delle credenziali,
- indagine approfondita sugli errori 500 per identificare eventuali vulnerabilità applicative.

L'utilizzo di Splunk mi ha permesso di estrarre, correlare e aggregare rapidamente grandi volumi di eventi, trasformando log grezzi in informazioni di intelligence di sicurezza actionable.

[EXTRA] rsyslog

Rsyslog è un potente e flessibile sistema di gestione dei log utilizzato in ambienti Linux e Unix per raccogliere, processare, filtrare, archiviare e trasmettere i messaggi di log generati da vari processi di sistema e applicazioni.

Per integrare i log di un client Windows in un server rsyslog su Kali Linux, si utilizza il **Rsyslog Windows Agent**, che forwarda gli Event Log di Windows verso un server syslog remoto.

Windows Agent: <https://www.rsyslog.com/windows-agent/windows-agent-download/>



Windows Agent Download - rs | +

rsyslog.com/windows-agent/windows-agent-download/

rsyslog.com uses cookies to ensure that we give you the best experience on our website. If you continue to use this site, you confirm and accept the use of Cookies on our site. You will find more information [Policy](#).

Ok Read more

Windows Agent Download

Latest Version

Rsyslog Windows Agent 8.1 Full / [Mirror]	Build 232, ALL OS, 87MB
Rsyslog Windows Agent 8.0 Mass Rollout	Build 230, ALL OS, Mass Rollout Files, 4MB

Current Version

daily stable build (Ubuntu)
daily stable build (CentOS)

8.2512.0 [\[doc\]](#) [\[download\]](#)

next: 8.2602.0, February 2026

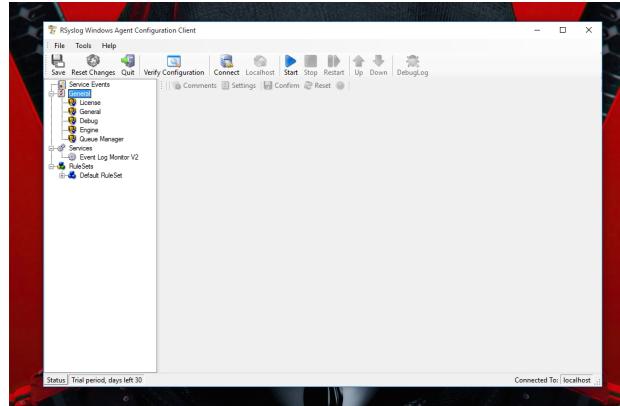
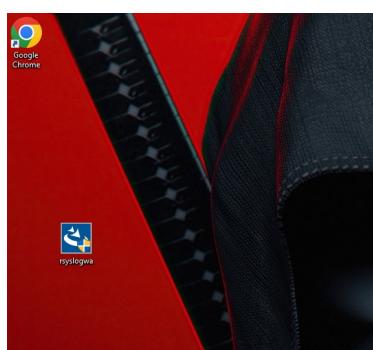
[rsyslog docker container](#)

[\[packages and older versions\]](#)

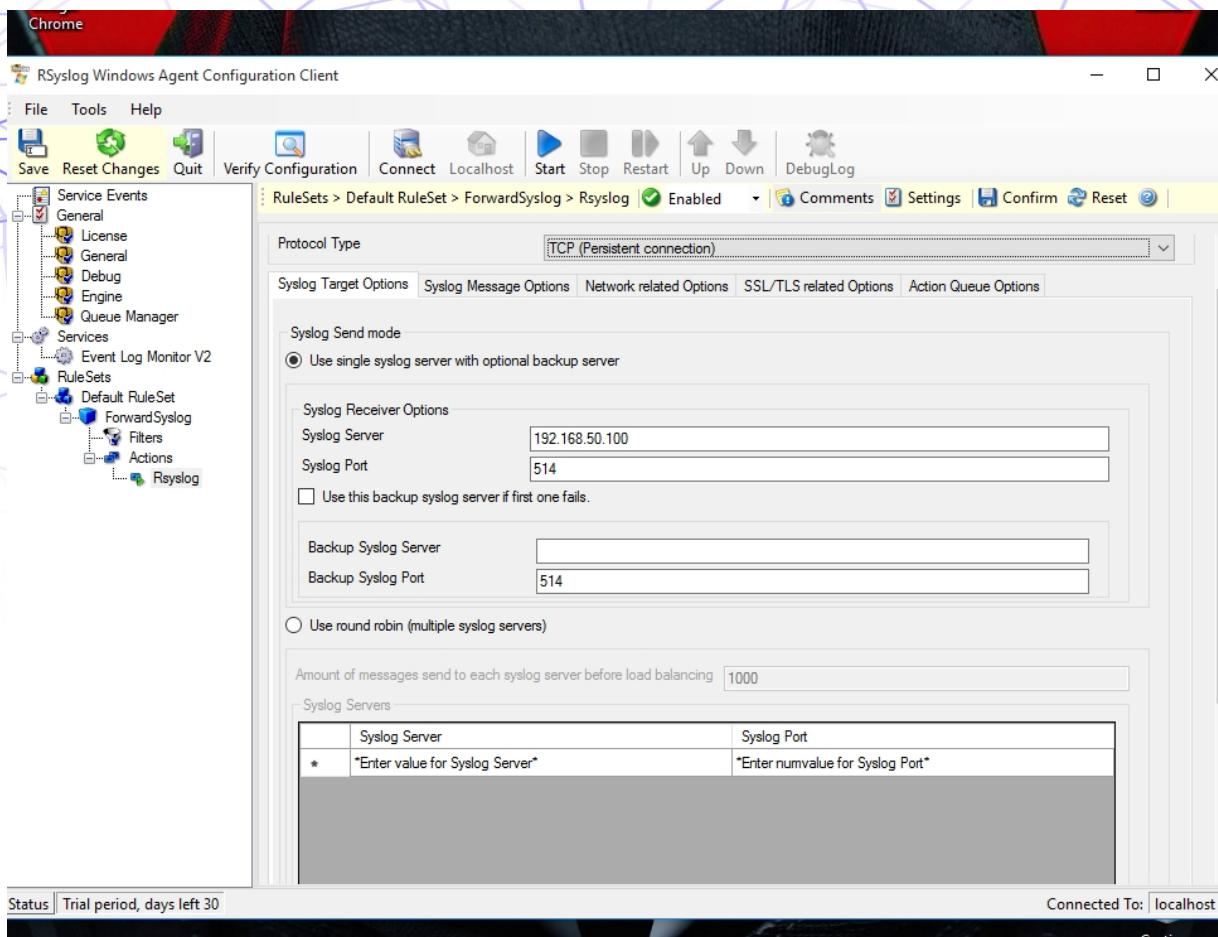
[Windows Agent: 8.1 \[download\]](#)

Old Versions

Rsyslog Windows Agent 7.5c	Build 228, ALL OS, 100MB
--	--------------------------



Installazione e configurazione del Rsyslog Windows Agent sul client Windows



Configurazione del server rsyslog su Kali Linux (ricezione log remoti)

Dalle schermate del file di configurazione `/etc/rsyslog.conf` e dello stato del servizio:

- Abilitare i moduli per ricezione UDP e TCP sulla porta 514
- Restrizione fonti consentite (dalla riga `$AllowedSender`)

Permette log TCP solo da localhost e dalla subnet 192.168.50.0/24; estendibile per UDP se necessario.

```
#####
#### MODULES #####
#####

module(load="imuxsock") # provides support for local system logging
module(load="imklog") # provides kernel logging support
#module(load="immark") # provides --MARK-- message capability

# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")

# provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="514")
$allowedSender TCP, 127.0.0.1, 192.168.50.0/24

#####
### GLOBAL DIRECTIVES #####
#####
```

- Il servizio rsyslog è attivo e in ascolto (versione 8.2510.0), come visibile da `systemctl status rsyslog`.

- Porta 514 TCP aperta per input syslog (dalla configurazione firewall/Splunk o simile: TCP port 514, Source type: syslog, Enabled).
- Verifica ascolto: `netstat -tulpn | grep 514` mostra rsyslog in LISTEN su TCP e UDP 514.

```

(M6D6R6㉿kali)-[~]
$ sudo systemctl status rsyslog
● rsyslog.service - System Logging Service
  Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; preset: enabled)
  Active: active (running) since Thu 2025-12-18 16:21:20 EST; 1min 0s ago
    Invocation: cb7e3763732b46a3b4e77e442b23be9b
TriggeredBy: ● syslog.socket
  Docs: man:rsyslog(8)
  Tor Browser: man:rsyslog.conf(5)
    https://www.rsyslog.com/doc/
  Main PID: 23825 (rsyslogd)
    Tasks: 4 (limit: 11141)
      Memory: 2.3M (peak: 2.7M)
        CPU: 85ms
      CGroup: /system.slice/rsyslog.service
          └─23825 /usr/sbin/rsyslogd -n -iNONE

Dec 18 16:21:20 kali systemd[1]: Starting rsyslog.service - System Logging Service...
Dec 18 16:21:20 kali rsyslogd[23825]: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) from systemd. [v8.2510.0]
Dec 18 16:21:20 kali systemd[1]: Started rsyslog.service - System Logging Service.
Dec 18 16:21:20 kali rsyslogd[23825]: [origin software="rsyslogd" swVersion="8.2510.0" x-pid="23825" x-info="https://www.rsyslog.com"] start

(M6D6R6㉿kali)-[~]
$ sudo netstat -tulpn | grep :514
tcp 0 0 0.0.0.0:514 > 12/18/2025 0.0.0.0:*
tcp6 0 ::1:514 > 9:12:00 AM 0.0.0.0:*
udp 0 0.0.0.0:514 > 12/18/2025 0.0.0.0:*
udp6 0 ::1:514 > 12/18/2025 0.0.0.0:*
```

Configurazione Splunk e Verifica

Configurazione TCP per ricevere i log di Windows

TCP port	Host Restriction	Source type	Status	Actions
514		syslog	Enabled Disable	Clone Delete

Verifica recezione log da Windows

Log ricevuti da host **192.168.50.102** (client Windows) su server 192.168.50.100

host="192.168.50.102" | No Event Sampling | Time range: Last 24 hours | Job | Smart Mode | 1 hour per column

Time	Event
2025-12-19T13:17:09.636575-05:00	host = 192.168.50.102 source = tcp:9997 sourcetype = syslog
2025-12-18T18:17:04:55.192.168.50.102	hell.Cndleitzation.MethodParam = 'DelayedAckTimeout'; ParameterType = 'System.UInt32'; Bindings = 'In'; Value = \$_.cmdleitzation_value; IsValuePresent = '\$true') else (\$_.cmdleitzation_methodParameter = [Microsoft.PowerShell.Cndleitzation.MethodParameter]@{Name = 'DelayedAckTimeout'; ParameterType = 'System.UInt32'; Binding s = 'In'; Value = \$_.cmdleitzation.defaultValue; IsValuePresent = '\$false' }) \$_.cmdleitzation_methodParameters.Add(\$_.cmdleitzation_methodParameter) Object\$_.cmdleitzation_MethodParamValue = \$null Object\$_.cmdleitzation_MethodParamName = '\$DelayedAckTimeout'; ParameterType = 'System.UInt32'; Bindings = 'Out'; Value = \$DelayedAckTimeout; IsValuePresent = '\$true') \$DelayedAckTimeout = [Microsoft.PowerShell.Cndleitzation.MethodParameter]@{Name = 'DelayedAckFrequency'; ParameterType = 'System.Byte'; Bindings = 'In'; Value = \$_.cmdleitzation_value; IsValuePresent = '\$true' } else (\$_.cmdleitzation_methodParameter = [Microsoft.PowerShell.Cndleitzation.MethodParameter]@{Name = 'DelayedAckFrequency'; ParameterType = 'System.Byte'; Bindings = 'In'; Value = \$_.cmdleitzation.defaultValue; IsValuePresent = '\$false' }) Object\$_.cmdleitzation_MethodParamValue = \$null Object\$_.cmdleitzation_MethodParamName = '\$DelayedAckFrequency'; ParameterType = 'System.Byte'; Bindings = 'Out'; Value = \$DelayedAckFrequency; IsValuePresent = '\$true')

Questa configurazione centralizza con successo i log Windows su rsyslog Kali, con ricezione TCP affidabile dalla subnet locale.

CONCLUSIONE

In questo progetto ho dimostrato l'efficacia di Splunk nel rilevamento rapido di pattern di attacco e anomalie operative, affiancato da un'infrastruttura di centralizzazione dei log tramite rsyslog che ha permesso l'integrazione dei log Windows in tempo reale.

L'esperienza mi ha consolidato competenze pratiche in installazione, indicizzazione dati e creazione di query SPL complesse.

In un contesto reale, questi insight mi permetterebbero di implementare contromisure immediate per rafforzare la sicurezza del sistema, oltre alla configurazione di un sistema distribuito di raccolta log che consente il monitoraggio centralizzato di ambienti eterogenei (Linux/Windows).

L'utilizzo di Splunk si è rivelato uno strumento potente per il monitoraggio e l'analisi forense dei log.