

Progetto W24D4


Analisi log eventi con Splunk

Scopo analisi e struttura dataset

Obiettivo: Utilizzo di Splunk per analizzare i log e identificare pattern di sicurezza, come tentativi di accesso falliti, sessioni SSH aperte e errori del server.

Dati: File tutorialdata.zip, contenente log di accesso e access log di un sistema.

Contenuti dell'archivio Tutorial Data:

- *access.log*: Contiene dati di accesso al server web Apache, utili per analizzare il traffico e le interazioni degli utenti con il sito. Questo file sarà utile, nel contesto di quest'analisi, per identificare gli errori del server.
 - *secure.log*: Contiene eventi di sicurezza, come tentativi di accesso e altre attività rilevanti per la sicurezza del sistema. Questo file sarà utile per l'identificazione di tentativi di accesso falliti "Failed password", per trovare tutte le sessioni SSH aperte con successo, per l'identificazione di tutti i tentativi di accesso falliti provenienti da un determinato indirizzo IP e per identificare gli indirizzi IP che hanno tentato di accedere al sistema più di 5 volte.
 - *vendor_sales.log*: Contiene informazioni sulle vendite dei prodotti, utilizzato per analisi commerciali e di transazioni. Non utile allo scopo di questa analisi.
- 

Evento: Failed password

Query 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.

*** source="tutorialdata.zip:\\secure.log" fail* AND password | table _time, src_ip, username, Event**

Obiettivo query: Identificare tutti i tentativi di accesso falliti al sistema

Spiegazione query:

source="tutorialdata.zip:\\secure.log": Specifica la sorgente dei dati, ovvero il file di log di sicurezza secure.log contenuto nell'archivio tutorialdata.zip. Questo indirizza Splunk a cercare i dati in questo file, che contiene informazioni di autenticazione come i tentativi di accesso.

fail* AND password: Filtra i log per includere solo gli eventi che contengono parole che iniziano con "fail" (ad esempio, "failed") e la parola "password".

table _time, src_ip, username, Event: Il comando *table* è utilizzato per selezionare e mostrare solo i campi specificati nella tabella finale. _time, src_ip, username, Event indicano i campi da mostrare nella tabella finale.

Campi:

_time: Mostra l'orario dell'evento;

src_ip: Mostra l'indirizzo IP da cui è partito il tentativo di accesso;

username: Mostra il nome utente utilizzato per effettuare il tentativo;

event: L'evento. In questo caso, il motivo del fallimento, indicato con "Failed password".



Evento: Failed password

New Search

Save As ▾







Create Table View

Close

* source="tutorialdata.zip:.\\www1/secure.log" fail* AND password | table _time, src_ip, username, Event

All time ▾ 

✓ 8,859 events (before 11/1/24 6:16:04.000 PM) No Event Sampling ▾

Job ▾       Verbose Mode ▾

Events (8,859)


Patterns

Statistics (8,859)

Visualization



< Hide Fields

 All Fields

SELECTED FIELDS

a host 1

a source 1

a sourcetype 1

INTERESTING FIELDS

date_hour 1

date_mday 8

date_minute 1

a date_month 1

date_second 1

a date_wday 7

date_year 1

a date_zone 1


i	Time	Event
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[1654]: Failed password for happy from 2.229.4.58 port 2111 ssh2 host = Progetto_W24D4 source = tutorialdata.zip:.\\www1/secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[5034]: Failed password for news from 2.229.4.58 port 4671 ssh2 host = Progetto_W24D4 source = tutorialdata.zip:.\\www1/secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[4225]: Failed password for apache from 2.229.4.58 port 4493 ssh2 host = Progetto_W24D4 source = tutorialdata.zip:.\\www1/secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[1089]: Failed password for invalid user local from 2.229.4.58 port 4910 ssh2 host = Progetto_W24D4 source = tutorialdata.zip:.\\www1/secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[5962]: Failed password for games from 2.229.4.58 port 2418 ssh2 host = Progetto_W24D4 source = tutorialdata.zip:.\\www1/secure.log sourcetype = www1/secure

Evento: Failed password

Analisi

Gli eventi nelle schermate successive mostrano tentativi SSH di accesso falliti “Failed password”. Gli eventi mostrano l’indirizzo ip di origine [2.229.4.58] e [198.35.2.120], il numero di porta e il tipo di servizio ssh2.

Gli eventi sono avvenuti tutti a intervalli di tempo ravvicinati, alle 16:36:59 del 30 ottobre 2024. Questo pattern suggerisce un attacco coordinato in un brevissimo periodo di tempo. L’indirizzo ip sorgente è sempre lo stesso per molteplici tentativi, indice di tentativi di autenticarsi utilizzano diversi nomi utente, come *happy*, *news*, *apache*, *local*, *games*, *sneezy*, *doc*, *vmware*, *root*, *operator*. Alcuni tentativi, tra i quali *operator* e *admin*, mostrano anche il campo “invalid user”, il che indica che si è tentato di effettuare l’accesso utilizzando un nome utente non registrato nel sistema, con una password sbagliata.



Evento: Failed password

List ▾

Format

50 Per Page ▾

< Prev

1

2

3

4

5

6

7

8

...

Next >

< Hide Fields

All Fields

SELECTED FIELDS

a host 1

a source 1

a sourcetype 1

INTERESTING FIELDS

date_hour 1

date_mday 8

date_minute 1

a date_month 1

date_second 1

a date_wday 7

date_year 1

a date_zone 1

a index 1

linecount 1

a punct 3

a splunk_server 1

timeendpos 1

timestartpos 1

+ Extract New Fields

i	Time	Event
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[1654]: Failed password for happy from 2.229.4.58 port 2111 ssh2 host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[5034]: Failed password for news from 2.229.4.58 port 4671 ssh2 host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[4225]: Failed password for apache from 2.229.4.58 port 4493 ssh2 host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[1089]: Failed password for invalid user local from 2.229.4.58 port 4910 ssh2 host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[5962]: Failed password for games from 2.229.4.58 port 2418 ssh2 host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[5222]: Failed password for sneezy from 2.229.4.58 port 4309 ssh2 host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[1412]: Failed password for invalid user email from 2.229.4.58 port 2831 ssh2 host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[1837]: Failed password for sneezy from 2.229.4.58 port 3039 ssh2 host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[5555]: Failed password for invalid user admin from 2.229.4.58 port 4286 ssh2 host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[4737]: Failed password for invalid user vmware from 2.229.4.58 port 3349 ssh2 host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[3298]: Failed password for doc from 2.229.4.58 port 2119 ssh2 host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[5757]: Failed password for invalid user operator from 2.229.4.58 port 4283 ssh2 host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[2764]: Failed password for root from 2.229.4.58 port 3829 ssh2 host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure

Evento: Failed password

< Hide Fields

All Fields

List

Format

50 Per Page

< Prev

1

2

3

4

5

6

7

8

...

Next >

i	Time	Event
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[3459]: Failed password for invalid user irc from 198.35.2.120 port 1495 ssh2 host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[3895]: Failed password for jboss from 198.35.2.120 port 3593 ssh2 host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[5243]: Failed password for invalid user vmware from 198.35.2.120 port 1342 ssh2 host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[1507]: Failed password for invalid user divine from 198.35.2.120 port 1858 ssh2 host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[5178]: Failed password for invalid user info from 198.35.2.120 port 3855 ssh2 host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[4232]: Failed password for invalid user lucy from 198.35.2.120 port 2068 ssh2 host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[4376]: Failed password for backup from 198.35.2.120 port 4914 ssh2 host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[4428]: Failed password for jira from 198.35.2.120 port 2593 ssh2 host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[2747]: Failed password for invalid user administrator from 198.35.2.120 port 4369 ssh2 host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[4704]: Failed password for invalid user sys from 198.35.2.120 port 2177 ssh2 host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[2961]: Failed password for invalid user brian from 203.45.206.135 port 3004 ssh2 host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[3888]: Failed password for invalid user operator from 81.18.148.190 port 1931 ssh2 host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[4583]: Failed password for invalid user demo from 81.18.148.190 port 2696 ssh2 host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure

Evento: Failed password

Analisi

Gli eventi indicano che un potenziale attaccante potrebbe star tentando di indovinare le credenziali di accesso al servizio SSH tramite un attacco di forza bruta basato su nomi utente. I tentativi includono username generici, il che indica che l'attaccante sta utilizzando una lista di nomi utente comuni per accedere al sistema.

Il fatto che il servizio a cui si stia tentando di effettuare l'accesso sia sempre SSH ma la porta sia diversa per i vari tentativi, potrebbe indicare che l'attacco si sta effettuando tramite uno script che cerca di evitare blocchi basati su porta e di identificare porte alternative su cui potrebbe essere attivo il servizio SSH. Inoltre, tutti i tentativi di accesso falliti si sono verificati in un periodo estremamente ravvicinato. Ciò è indicativo dell'utilizzo di uno script automatizzato piuttosto che di un attacco manuale.



Evento: Failed password

Remediation e azioni preventive

Blocco e segnalazione IP sospetti


Gli IP sospetti dovrebbero essere bloccati a livello di firewall per prevenire ulteriori tentativi di accesso. Inoltre, sarebbe indicato monitorare futuri tentativi di accesso da tali indirizzi IP per identificare eventuali varianti dell'attacco.

Autenticazione a due fattori

L'implementazione di un'autenticazione a due fattori (2FA) per gli accessi SSH renderebbe molto più difficile per un attaccante effettuare con successo l'accesso anche qualora dovesse trovare le credenziali corrette tramite attacco di forza bruta.

Limitazione accessi SSH

Si potrebbe inoltre configurare il server SSH per bloccare temporaneamente o definitivamente gli indirizzi IP che effettuano troppi tentativi falliti in un breve periodo di tempo.



Evento: Failed password

Monitoraggio e allerte proattive

L'impostazione di alert di sistema su Splunk può aiutare gli analisti di sicurezza a identificare eventuali numerosi tentativi di accesso falliti in rapida successione dallo stesso indirizzo IP.

La configurazione di dashboard per monitorare in tempo reale i tentativi di accesso falliti può essere utile per identificare tempestivamente eventuali attacchi di forza bruta e prendere le dovute contromisure per mitigare i rischi di compromissione del sistema.



Evento: sessioni ssh aperte / “djohnson”

Query 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.*

*** source="tutorialdata.zip:\\secure.log" “session opened for user djohnson” | table _time, user**

Obiettivo query: Trovare tutte le sessioni SSH aperte con successo per l'utente specifico "djohnson".

Spiegazione query:

source="tutorialdata.zip:\\secure.log": Specifica a Splunk di cercare risultati all'interno del file di log di sicurezza secure.log contenuto nell'archivio tutorialdata.zip.

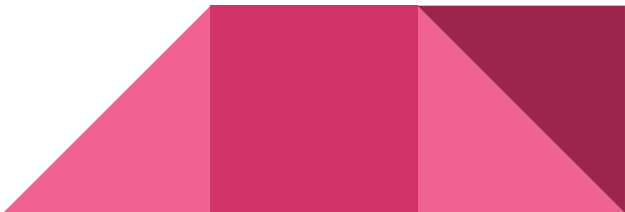
“session opened for user djohnson”: Filtra per cercare all'interno dei log solo gli eventi che contengono la stringa “session opened for user djohnson”, per identificare le sessioni SSH aperte con successo da quel nome utente.

table _time, user: Il comando *table* è utilizzato per selezionare e mostrare solo i campi specificati nella tabella finale. _time, user indicano i campi da mostrare nella tabella finale.

Campi:

_time: Mostra l'orario in cui la sessione è stata aperta;

user: Mostra ID dell'utente associato alla sessione SSH.



Evento: sessioni ssh aperte / “djohnson”

New Search

[Save As ▾](#)[Create Table View](#)[Close](#)

* source="tutorialdata.zip:\\www1\\secure.log" "session opened for user djohnson" | table _time, user

[All time ▾](#)

✓ 281 events (before 11/2/24 4:42:09:00 PM) No Event Sampling ▾

Job ▾ || Verbose Mode ▾

Events (281) Patterns Statistics (281) Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect

1 day per column

List ▾ Format 50 Per Page ▾

< Prev 1 2 3 4 5 6 Next >

< Hide Fields

All Fields

SELECTED FIELDS

a host 1

a source 1

a sourcetype 1

INTERESTING FIELDS

date_hour 1

date_mday 8

date_minute 1

a date_month 1

date_second 1

a date_wday 7

date_year 1

a date_zone 1

a index 1

linecount 1

a punct 1

a splunk_server 1

timeendpos 1

timestartpos 1

uid 1

+ Extract New Fields

i	Time	Event
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[51734]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = Progetto_W24D4 source = tutorialdata.zip:\\www1\\secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[86262]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = Progetto_W24D4 source = tutorialdata.zip:\\www1\\secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[82331]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = Progetto_W24D4 source = tutorialdata.zip:\\www1\\secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[87661]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = Progetto_W24D4 source = tutorialdata.zip:\\www1\\secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[28526]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = Progetto_W24D4 source = tutorialdata.zip:\\www1\\secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[41169]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = Progetto_W24D4 source = tutorialdata.zip:\\www1\\secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[37571]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = Progetto_W24D4 source = tutorialdata.zip:\\www1\\secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[63104]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = Progetto_W24D4 source = tutorialdata.zip:\\www1\\secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[46915]: pam_unix(sshd:session): session opened for user djohnson by (uid=0)

Evento: sessioni ssh aperte / “djohnson”


Analisi

Il messaggio logga l'evento con il testo: “session opened for user djohnson by (uid=0)”, che implica che l'utente djohnson ha aperto con successo una sessione. L'uid=0 indica che l'azione è eseguita dall'utente root o con privilegi di amministrazione. Questo potrebbe rappresentare un rischio di privilege escalation.

I session id diversi (ad esempio, sshd[51734], sshd[86262], ecc.), indicano che ogni sessione è gestita come un'istanza separata del processo sshd.

La riga "pam_unix(sshd)" indica che la sessione SSH (Secure Shell) è stata aperta su un sistema Unix/Linux.

Inoltre, tutti gli eventi mostrano lo stesso timestamp: Thu Oct 30 2024 16:36:59, suggerendo che le sessioni sono state aperte nello stesso secondo. Questo potrebbe indicare l'utilizzo di uno script automatico per aprire più sessioni contemporaneamente, indizio di un comportamento malevolo o un tentativo di abuso del sistema. Potrebbe anche trattarsi di uno script legittimo eseguito con autorizzazione e, in questo caso, bisognerebbe effettuare delle verifiche al livello interno.



Evento: sessioni ssh aperte / “djohnson”

Analisi

L'apertura simultanea di molte sessioni SSH potrebbe comportare un sovraccarico del server, con conseguenti rischi di rallentamento delle prestazioni.

Ogni connessione SSH consuma memoria e risorse CPU per essere mantenuta attiva, e l'eventuale sovraccarico potrebbe ridurre la capacità del server di gestire ulteriori richieste e compromettere le prestazioni di altri servizi critici in esecuzione sullo stesso host.

Questo comportamento con apertura di molteplici connessioni simultanee potrebbe essere indice di un attacco DoS interno mirato a sovraccaricare il server con connessioni SSH fino a saturarne le risorse e renderlo indisponibile ad utenti legittimi.



Evento: sessioni ssh aperte / “djohnson”

List ▾ / Format		50 Per Page ▾		< Prev 1 2 3 4 5 6 Next >	
< Hide Fields	⋮ All Fields	i	Time	Event	
SELECTED FIELDS a host 1 a source 1 a sourcetype 1		>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[51734]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1\secure	
		>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[86262]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1\secure	
INTERESTING FIELDS # date_hour 1 # date_mday 8 # date_minute 1 # date_month 1 # date_second 1 a date_wday 7 # date_year 1 a date_zone 1 a index 1 # linecount 1 a punct 1 a splunk_server 1 # timeendpos 1 # timestartpos 1 # uid 1		>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[82331]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1\secure	
		>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[87661]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1\secure	
		>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[28526]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1\secure	
		>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[41169]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1\secure	
		>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[37571]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1\secure	
		>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[63104]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1\secure	
		>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[46915]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1\secure	
		>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[64457]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1\secure	
		>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[7137]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1\secure	
		>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[55360]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1\secure	
+ Extract New Fields		>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[86409]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1\secure	
		>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[95284]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1\secure	
		>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[27639]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1\secure	
		>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[37012]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1\secure	
		>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[60850]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1\secure	
		>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[2315]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1\secure	

Evento: sessioni ssh aperte / “djohnson”

List ▾ / Format 50 Per Page ▾

< Prev 1 2 3 4 5 6 Next >

< Hide Fields	≡ All Fields	i	Time	Event
SELECTED FIELDS a host 1 a source 1 a sourcetype 1		>	10/29/24 4:36:59.000 PM	Wed Oct 29 2024 16:36:59 www1 sshd[34712]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
		>	10/29/24 4:36:59.000 PM	Wed Oct 29 2024 16:36:59 www1 sshd[16188]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
INTERESTING FIELDS # date_hour 1 # date_mday 8 # date_minute 1 # date_month 1 # date_second 1 # date_wday 7 # date_year 1 # date_zone 1 # index 1 # linecount 1 # punct 1 # splunk_server 1 # timeendpos 1 # timestamppos 1 # uid 1		>	10/29/24 4:36:59.000 PM	Wed Oct 29 2024 16:36:59 www1 sshd[36325]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
		>	10/29/24 4:36:59.000 PM	Wed Oct 29 2024 16:36:59 www1 sshd[75676]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
		>	10/29/24 4:36:59.000 PM	Wed Oct 29 2024 16:36:59 www1 sshd[11572]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
		>	10/29/24 4:36:59.000 PM	Wed Oct 29 2024 16:36:59 www1 sshd[93383]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
		>	10/29/24 4:36:59.000 PM	Wed Oct 29 2024 16:36:59 www1 sshd[15187]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
		>	10/29/24 4:36:59.000 PM	Wed Oct 29 2024 16:36:59 www1 sshd[11891]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
		>	10/29/24 4:36:59.000 PM	Wed Oct 29 2024 16:36:59 www1 sshd[46764]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
+ Extract New Fields		>	10/29/24 4:36:59.000 PM	Wed Oct 29 2024 16:36:59 www1 sshd[63632]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
		>	10/29/24 4:36:59.000 PM	Wed Oct 29 2024 16:36:59 www1 sshd[32435]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
		>	10/29/24 4:36:59.000 PM	Wed Oct 29 2024 16:36:59 www1 sshd[83934]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
		>	10/29/24 4:36:59.000 PM	Wed Oct 29 2024 16:36:59 www1 sshd[3313]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
		>	10/29/24 4:36:59.000 PM	Wed Oct 29 2024 16:36:59 www1 sshd[13435]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
		>	10/29/24 4:36:59.000 PM	Wed Oct 29 2024 16:36:59 www1 sshd[25611]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
		>	10/29/24 4:36:59.000 PM	Wed Oct 29 2024 16:36:59 www1 sshd[14249]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
		>	10/29/24 4:36:59.000 PM	Wed Oct 29 2024 16:36:59 www1 sshd[6980]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure

Evento: sessioni ssh aperte / “djohnson”

Remediation e azioni preventive

Monitoraggio accesso per utenti privilegiati

Data la sensibilità dell'accesso con uid=0, sarebbe prudente monitorare costantemente l'attività dell'utente djohnson e verificare la necessità di tutti questi accessi con privilegi di root. Il comportamento potrebbe essere dovuto ad esempio a un'operazione cron mal configurata e dovrebbe essere monitorato per garantire la sicurezza del sistema. In caso contrario, si tratterebbe di un utente malevolo che è riuscito ad effettuare con successo un'operazione di privilege escalation.

Verifica processo e Rate Limiting

È consigliabile verificare se l'utente djohnson ha uno script o un processo pianificato che apre queste sessioni. In caso affermativo, si dovrebbe valutare se è possibile ridurre il numero di sessioni aperte contemporaneamente. Se le sessioni simultanee per lo stesso utente non sono necessarie, sarebbe utile applicare una policy di rate limiting per l'accesso SSH.

Molti sistemi consentono infatti di impostare limiti sul numero di connessioni SSH simultanee per utente, riducendo così i rischi di comportamenti anomali o non autorizzati.



Evento: sessioni ssh aperte / “djohnson”

Revoca accesso e reset credenziali

In caso di accesso illegittimo, bisognerebbe revocare immediatamente l'accesso dell'utente djohnson e resettare la sua password poiché le sue credenziali sono state compromesse.

Monitoraggio e alert

Configurare degli alert in tempo reale per monitorare attività inusuali come accessi SSH multipli in un breve intervallo di tempo e notificare l'amministratore di sistema ogni volta che si verifica un evento simile, così da poter analizzare tempestivamente l'eventuale verificarsi di questo evento.



Evento: accessi falliti da source_ip "86.212.199.60"

Query 3: *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.*

*** source="tutorialdata.zip:\\secure.log" "failed password" "from 86.212.199.60" | table _time, username, port**

Obiettivo query: Identificare tutti i tentativi di accesso falliti provenienti dall'indirizzo IP "86.212.199.60".

Spiegazione query:

source="tutorialdata.zip:\\secure.log": Questa parte della query specifica la sorgente dei dati, che in questo caso è il file secure.log all'interno dell'archivio tutorialdata.zip. Il file di log secure.log contiene informazioni utili alla query in oggetto, quali i tentativi di accesso falliti.

"failed password": Questo filtra per gli eventi che contengono la stringa "failed password".

"from 86.212.199.60": Questa parte della query filtra ulteriormente per restringere i risultati ai tentativi di accesso falliti che provengono dall'indirizzo IP specifico 86.212.199.60.

table _time, username, port: Il comando *table* formatta i risultati. In questo caso, verranno mostrati solo i campi time, username e port.



Evento: accessi falliti da source_ip “86.212.199.60”

Query 3: *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.*

*** source="tutorialdata.zip:\\secure.log" “failed password” “from 86.212.199.60” | table _time, username, port**

Obiettivo query: Identificare tutti i tentativi di accesso falliti provenienti dall'indirizzo IP "86.212.199.60".

Campi:

_time: Mostra l'orario in cui è stato effettuato l'accesso, indicandone data e ora;

username: Mostra il nome dell'utente che ha tentato di effettuare l'accesso. Questo può aiutare gli analisti a capire se c'è stato un pattern di nomi utente particolari;

port: Mostra il numero della porta utilizzata per il tentativo di accesso.



Evento: accessi falliti da source_ip “86.212.199.60”

splunk>enterprise

Apps

Administrator

3 Messages

Settings

Activity

Help

Find

Search

Analytics

Datasets

Reports

Alerts

Dashboards

>

New Search

Save As

Create Table View

Close

* source="tutorialdata.zip:.\\www1\\secure.log" "Failed password" "from 86.212.199.60" | table _time, username, port

All time

Q

1 event (before 11/1/24 6:20:37.000 PM) No Event Sampling

Job

||

↶

🖨

⬇

🗨 Verbose Mode

Events (1)

Patterns

Statistics (1)

Visualization

Format Timeline

Zoom Out

Zoom to Selection

Deselect

1 millisecond per column

List

Format

20 Per Page

< Hide Fields

All Fields

SELECTED FIELDS

a host 1

a source 1

a sourcetype 1

INTERESTING FIELDS

date_hour 1

date_mday 1

date_minute 1

a date_month 1

date_second 1

a date_wday 1

date_year 1

a date_zone 1

a index 1

i	Time	Event
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[1385]: Failed password for invalid user db from 86.212.199.60 port 2690 ssh2 host = Progetto_W24D4 source = tutorialdata.zip:.\\www1\\secure.log sourcetype = www1/secure

Evento: accessi falliti da source_ip “86.212.199.60”

Analisi

L'unico evento risultante dalla query è un tentativo di accesso fallito per l'utente db con un indirizzo IP sorgente di 86.212.199.60 sulla porta 2690. Ciò suggerisce che l'utente db potrebbe non essere registrato o abilitato sul sistema. Questo è l'unico evento mostrato nei risultati, quindi potrebbe essere un caso isolato. Il tentativo di accesso è stato effettuato su una porta non standard per il servizio SSH, il che potrebbe indicare un tentativo di eludere i controlli di sicurezza.

Questo potrebbe anche indicare che l'attaccante conosce i metodi per aggirare i firewall o altre misure difensive e potrebbe rappresentare una minaccia avanzata. Inoltre, l'indirizzo IP da cui è stato effettuato il tentativo di accesso è un IP esterno e non locale. Potrebbe essere utile indagare l'origine geografica dell'indirizzo IP e verificare se è stato attore di altri eventi di sicurezza significativi.



Evento: accessi falliti da source_ip “86.212.199.60”

Remediation e azioni preventive

Blocco IP

Bloccare l'indirizzo IP 86.212.199.60 per prevenire ulteriori tentativi di accesso.


Implementazione regole firewall su porte specifiche

Valutare la configurazione delle regole del firewall per limitare gli accessi SSH a specifiche porte, preferibilmente utilizzando un indirizzo IP interno o VPN per accedere alla macchina in sicurezza.

Alert e audit periodici

Eseguire audit periodici sui log di accesso per identificare pattern sospetti. Una ricerca continuativa su tentativi falliti e porte non standard può essere utile per identificare minacce persistenti.

Configurare alert in Splunk per generare notifiche su tentativi falliti ripetuti dallo stesso IP o su accessi SSH tentati su porte non standard, in modo da identificare e rispondere tempestivamente a potenziali minacce.



Evento: indirizzi IP che hanno tentato di accedere al sistema più di 5 volte.

Query 4: *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.*

```
* source="tutorialdata.zip:\\secure.log" "Failed password" | rex "from (?<src_ip>\\S+)" | top src_ip limit=0 countfield = Failed_Attempts | where Failed_Attempts > 5 | table src_ip, Failed_Attempts
```


Obiettivo query: Identificare tutti i tentativi di accesso falliti provenienti dall'indirizzo IP "86.212.199.60".

Spiegazione query:

source="tutorialdata.zip:\\secure.log": Questa parte della query specifica la sorgente dei dati, ovvero il file secure.log all'interno dell'archivio tutorialdata.zip.

"Failed password": "Failed password" è utilizzato per filtrare i log e includere solo gli eventi che contengono la frase "Failed password", che indica un tentativo di accesso fallito.

rex "from (?<src_ip>\\S+)": Questo comando rex utilizza un'espressione regolare per estrarre l'indirizzo IP dell'origine del tentativo di accesso fallito. L'espressione *from (?<src_ip>\\S+)* cerca la parola "from", seguita dall'IP, che viene salvato in una "named capture group" chiamata src_ip. \\S+ qui indica una sequenza di caratteri non vuoti. Questa regex permette di estrarre l'indirizzo IP di origine da ogni evento in cui compare "Failed password".



Evento: indirizzi IP che hanno tentato di accedere al sistema più di 5 volte.

Query 4: 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.

```
* source="tutorialdata.zip:\\secure.log" "Failed password" | rex "from (?<src_ip>\\S+)" | top src_ip limit=0 countfield = Failed_Attempts | where Failed_Attempts > 5 | table src_ip, Failed_Attempts
```


Obiettivo query: Identificare tutti i tentativi di accesso falliti provenienti dall'indirizzo IP "86.212.199.60".

Spiegazione query:

top src_ip limit=0 countfield=Failed_Attempts: *top* è un comando Splunk che qui elenca e raggruppa i valori più frequenti di un campo specifico, in questo caso *src_ip*. *limit=0* indica che non ci sono limiti sul numero di risultati, quindi vengono inclusi tutti gli IP, anche quelli che compaiono poche volte. *countfield=Failed_Attempts* specifica che il conteggio dei tentativi falliti verrà visualizzato come campo chiamato *Failed_Attempts*.

where Failed_Attempts > 5: Il comando *where* filtra i risultati, includendo solo gli indirizzi IP che hanno effettuato più di 5 tentativi di accesso falliti.

table src_ip, Failed_Attempts: Il comando *table* è utilizzato per formattare i risultati finali e facilitarne la visualizzazione, mostrando solo i campi *src_ip* e *Failed_Attempts* in una tabella.



Evento: indirizzi IP che hanno tentato di accedere al sistema più di 5 volte.

Query 4: *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.*

*** source="tutorialdata.zip:.\secure.log" "Failed password" | rex "from (?<src_ip>\S+)" | top src_ip limit=0
countfield = Failed_Attempts | where Failed_Attempts > 5 | table src_ip, Failed_Attempts**

Campi:

src_ip: Mostra gli indirizzi IP da cui provengono i tentativi di accesso;

Failed_Attempts: Mostra il numero di tentativi di accesso falliti per ciascun IP.

La tab Statistics mostra il riassunto delle statistiche dei log, raggruppando i risultati per ogni indirizzo IP con il numero di log correlati ad esso.



Evento: > 5 accessi falliti al sistema

New Search

[Save As ▼](#)[Create Table View](#)[Close](#)

```
* source="tutorialdata.zip:.\\www1\\secure.log" "Failed password" | rex "from (?<src_ip>\\S+)"  
| top src_ip limit=0 countfield=Failed_Attempts  
| where Failed_Attempts > 5  
| table src_ip, Failed_Attempts
```

[All time ▼](#)

✓ **8,859 events** (before 11/1/24 6:40:56.000 PM)

No Event Sampling ▼

Job ▼



Verbose Mode ▼

Events (8,859)

Patterns

Statistics (178)

Visualization

20 Per Page ▼

Format

Preview ▼

< Prev

1

2

3

4

5

6

7

8

9

Next >

src_ip ↕



Failed_Attempts ↕

87.194.216.51

272

128.241.220.82

175

109.169.32.135

153

216.221.226.11

151

194.215.205.19

147

211.166.11.101

136

65.19.167.94

121

108.65.113.83

109

221.204.246.72

107

27.96.191.11

105

70.38.1.235

101

Evento: > 5 accessi falliti al sistema

Analisi

Gli eventi elencati mostrati nella schermata successiva mostrano tentativi di accesso SSH falliti, con l'errore "Failed password". Questo suggerisce che ci sono stati numerosi tentativi non autorizzati di accedere al server attraverso SSH. L'origine di questi tentativi proviene dall'indirizzo IP 2.229.4.58, che appare costantemente in ogni riga, suggerendo che tutti i tentativi di accesso provengano dallo stesso IP.

I tentativi di accesso sono stati effettuati con nomi utenti diversi, tutti piuttosto generici, il che può indicare un tentativo di attacco brute force, dove gli attaccanti provano diverse combinazioni di nomi utente comuni per aumentare le probabilità di successo.

Il fatto che ad ogni tentativo le porte siano diverse, denota che l'attaccante sta cercando di identificare una configurazione SSH in ascolto su porte non standard o potrebbe tentare di evitare il rilevamento.



Evento: > 5 accessi falliti al sistema

List ▾

Format ▾

50 Per Page ▾

< Prev

1

2

3

4

5

6

7

8

...

Next >

< Hide Fields

All Fields

SELECTED FIELDS

a host 1

a source 1

a sourcetype 1

INTERESTING FIELDS

date_hour 1

date_mday 8

date_minute 1

date_month 1

date_second 1

date_wday 7

date_year 1

date_zone 1

index 1

linecount 1

punct 3

splunk_server 1

src_ip 100+

timeendpos 1

timestartpos 1

+ Extract New Fields

i	Time	Event
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[1654]: Failed password for happy from 2.229.4.58 port 2111 ssh2 host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[5034]: Failed password for news from 2.229.4.58 port 4671 ssh2 host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[4225]: Failed password for apache from 2.229.4.58 port 4493 ssh2 host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[1089]: Failed password for invalid user local from 2.229.4.58 port 4910 ssh2 host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[5962]: Failed password for games from 2.229.4.58 port 2418 ssh2 host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[5222]: Failed password for sneezy from 2.229.4.58 port 4309 ssh2 host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[1412]: Failed password for invalid user email from 2.229.4.58 port 2831 ssh2 host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[1837]: Failed password for sneezy from 2.229.4.58 port 3039 ssh2 host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[5555]: Failed password for invalid user admin from 2.229.4.58 port 4286 ssh2 host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[4737]: Failed password for invalid user vmware from 2.229.4.58 port 3349 ssh2 host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[3298]: Failed password for doc from 2.229.4.58 port 2119 ssh2 host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[5757]: Failed password for invalid user operator from 2.229.4.58 port 4283 ssh2 host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[2764]: Failed password for root from 2.229.4.58 port 3829 ssh2 host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[1420]: Failed password for invalid user redmine from 2.229.4.58 port 2449 ssh2 host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure
>	10/30/24 4:36:59.000 PM	Thu Oct 30 2024 16:36:59 www1 sshd[3459]: Failed password for invalid user irc from 198.35.2.120 port 1495 ssh2 host = Progetto_W24D4 source = tutorialdata.zip:\www1\secure.log sourcetype = www1/secure

Evento: > 5 accessi falliti al sistema

src_ip	Failed_Attempts
201.122.42.235	84
223.205.219.67	83
233.77.49.94	82
27.1.11.11	78
87.240.128.18	77
212.27.63.151	76
94.229.0.20	74
12.130.60.4	73
74.53.23.135	71
198.35.3.23	71
24.185.15.226	69
71.192.86.205	68
69.72.161.186	68
223.205.219.198	68
195.69.160.22	68
59.99.230.91	67
208.240.243.170	67
202.179.8.245	67
27.175.11.11	65
209.160.24.63	64

Evento: > 5 accessi falliti al sistema

ultima pagina di log che mostra che solo gli eventi superiori al 5 vengono mostrati nelle statistiche

50 Per Page ▾ ↗ Format Preview ▾		< Prev 1 2 3 4 Next >	
src_ip ⇅		Failed_Attempts ⇅ ↗	
46.251.224.66		19	
74.82.57.172		17	
193.33.170.23		16	
190.113.128.150		16	
74.208.173.14		14	
61.164.73.20		14	
60.18.93.11		14	
198.35.1.10		14	
147.213.138.201		14	
220.225.12.171		13	
111.161.27.20		13	
10.2.10.163		13	
203.92.58.136		12	
69.175.97.11		11	
175.44.3.30		11	
91.205.40.22		9	
67.170.226.218		9	
49.212.64.138		9	
78.111.167.117		8	
199.15.234.66		6	

Evento: > 5 accessi falliti al sistema

Remediation e azioni preventive

Blocco indirizzo IP


Dato l'elevato numero di eventi, è consigliabile bloccare l'indirizzo IP 2.229.4.58 e altri indirizzi IP sospetti sul firewall per prevenire ulteriori tentativi di accesso.

Rate limiting per SSH

Configurare un limite sui tentativi di accesso SSH per ridurre la probabilità di attacchi brute force. Molti sistemi supportano fail2ban, un tool di sicurezza scritto in Python pensato per prevenire attacchi di forza bruta, che blocca temporaneamente IP che mostrano comportamenti sospetti.

Monitoraggio e alert

Configurare alert su Splunk per notificare gli amministratori di sistema quando si verifica un numero anomalo di tentativi di accesso falliti da un singolo o più indirizzi IP. Potrebbe trattarsi di un attacco distribuito (Distributed Brute Force Attack), in cui vari IP tentano di accedere simultaneamente per aggirare i blocchi.



Evento: > 5 accessi falliti al sistema

Revisione politiche di accesso


Rivedere le policy di autenticazione per l'accesso SSH, inclusa la necessità di password complesse e aggiornamenti regolari delle password. Considerare l'uso di chiavi SSH al posto delle password per gli utenti autorizzati, in modo da aumentare ulteriormente la sicurezza. Le chiavi SSH sono molto più difficili da forzare rispetto alle password.

Verifica indirizzo IP

È utile anche verificare se l'IP 2.229.4.58 e gli altri indirizzi IP collegati ai tentativi di accesso falliti siano noti per attività sospette. Esistono banche dati pubbliche di IP blacklist che possono aiutare a identificare se l'IP è stato segnalato per attacchi simili in passato.

Log correlati e pattern di attacco potenziali

È possibile che l'attaccante stia cercando pattern di credenziali o vulnerabilità su più servizi. Esaminare se ci sono tentativi simili su altri protocolli o servizi, come HTTP/HTTPS o database, potrebbe fornire informazioni aggiuntive sull'intento e sulla portata dell'attacco.



Evento: Internal Server Error (status code: 500)

Query 5: Crea una query Splunk per trovare tutti gli Internal Server Error.

```
* source="tutorialdata.zip:\\access.log" "500" | stats count by clientip | rename count as "Internal_Server_Errors" | table clientip, Internal_Server_Errors
```

Obiettivo query: Identificare tutti gli errori interni del server (HTTP 500).

Spiegazione query:


source="tutorialdata.zip:\\access.log": Specifica il file di origine, access.log, contenuto nell'archivio tutorialdata.zip. Questo indica a Splunk di cercare i dati in questo particolare file di log di accesso, dove sono registrate le richieste web, gli errori HTTP, ecc.

"500": Cerca nel log tutti gli eventi che contengono il codice di stato HTTP 500. Questa parte della query filtra tutti gli eventi che non contengono il codice 500, lasciando solo quelli relativi agli errori interni del server.

stats count by clientip: Il comando *stats* permette di visualizzare quanti eventi ci sono per ogni indirizzo IP client. *count* calcola il numero totale di eventi (in questo caso, eventi con codice 500) per ciascun valore di clientip. *by clientip* specifica che il conteggio deve essere raggruppato per l'indirizzo IP del client (clientip), ossia l'indirizzo IP da cui proviene la richiesta che ha causato l'errore.

rename count as "Internal_Server_Errors": Questo comando rinomina la colonna count in Internal_Server_Errors per rendere i risultati più chiari.

table clientip, Internal_Server_Errors: Il comando *table* viene usato per visualizzare solo le colonne clientip e Internal_Server_Errors nell'output finale.



Evento: Internal Server Error (status code: 500)

Query 5: *Crea una query Splunk per trovare tutti gli Internal Server Error.*

```
* source="tutorialdata.zip:\\access.log" "500" | stats count by clientip | rename count as "Internal_Server_Errors" | table clientip, Internal_Server_Errors
```

Obiettivo query: Identificare tutti gli errori interni del server (HTTP 500).

Campi:

clientip: Mostra gli indirizzi IP dei client che hanno causato errori di tipo 500;

Internal_Server_Errors: Mostra il numero totale di errori 500 generati da ciascun indirizzo IP.



Evento: Internal Server Error (status code: 500)

New Search

Save AsCreate Table ViewClose

* source="tutorialdata.zip:\\www1/access.log" "500" | stats count by clientip
| rename count as "Internal_Server_Errors"
| table clientip, Internal_Server_Errors

All time

✓ 438 events (before 11/1/24 6:45:54.000 PM)No Event Sampling

JobPauseRefreshDownloadVerbose Mode

Events (438)PatternsStatistics (127)Visualization

Format TimelineZoom OutZoom to SelectionDeselect1 day per column

ListFormat20 Per Page

Prev12345678...Next

< Hide FieldsAll Fields

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a action 5
bytes 100+
a categoryid 6
a clientip 100+
date_hour 24
date_mday 8
date_minute 56
a date_month 1
date_second 58
a date_wday 7

i	Time	Event
>	10/30/24 6:18:59.000 PM	198.35.1.75 - - [30/Oct/2024:18:18:59] "GET /cart.do?action=addtocart&itemId=EST-13&SESSIONID=SD10SL2FF4ADFF53099 HTTP 1.1" 500 2324 "http://www.butt ercupgames.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 = Progetto_W24D4 source = tutorialdata.zip:\\www1/access.log sourcetype = access_combined_wcookie
>	10/30/24 6:18:59.000 PM	198.35.1.75 - - [30/Oct/2024:18:18:59] "GET /cart.do?action=addtocart&itemId=EST-13&SESSIONID=SD10SL2FF4ADFF53099 HTTP 1.1" 500 2324 "http://www.butt ercupgames.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 = Progetto_W24D4 source = tutorialdata.zip:\\www1/access.log sourcetype = access_combined_wcookie
>	10/30/24 6:18:59.000 PM	198.35.1.75 - - [30/Oct/2024:18:18:59] "GET /cart.do?action=addtocart&itemId=EST-13&SESSIONID=SD10SL2FF4ADFF53099 HTTP 1.1" 500 2324 "http://www.butt ercupgames.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 = Progetto_W24D4 source = tutorialdata.zip:\\www1/access.log sourcetype = access_combined_wcookie
>	10/30/24 6:18:59.000 PM	198.35.1.75 - - [30/Oct/2024:18:18:59] "GET /cart.do?action=addtocart&itemId=EST-13&SESSIONID=SD10SL2FF4ADFF53099 HTTP 1.1" 500 2324 "http://www.butt ercupgames.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 = Progetto_W24D4 source = tutorialdata.zip:\\www1/access.log sourcetype = access_combined_wcookie

Evento: Internal Server Error (status code: 500)

Analisi

Ogni voce di log contiene un codice di stato 500, il che conferma che si tratta di errori interni del server. Questi errori possono essere causati da problemi di configurazione, errori di programmazione o condizioni di sistema che il server non può gestire.

Si osserva che gli URL richiesti si ripetono: [GET /cart.do?action=addtocart&itemId=EST-13]; [GET /category.screen?categoryId=NULL]; [GET /product.screen?productId=FS-SV3-0018]. Questo suggerisce che i tentativi di accesso agli stessi endpoint portano a errori ripetuti. È possibile che questi endpoint abbiano un problema comune di backend che impedisce la corretta elaborazione delle richieste.

Anche gli indirizzi IP dei clienti si ripetono. Nelle schermate mostrate successivamente è possibile osservare log relativi a richieste dagli indirizzi IP: [198.35.1.75]; [194.146.236.22].



Evento: Internal Server Error (status code: 500)

Analisi

Gli endpoint che generano errori includono percorsi specifici, come `/cart.do`, `/category.screen`, `/product.screen`. Questi errori indicano potenziali problemi nei moduli di gestione del carrello e della visualizzazione dei prodotti. Potrebbe trattarsi di problemi con il database, di errori logici nell'applicazione, o di dati mancanti (come nel caso di `categoryId=NULL`).

Gli user-agent indicano che i client utilizzano versioni di browser e sistemi operativi specifici, tra cui Chrome su Windows NT 6.1 e Mozilla su Windows NT 5.1. Sebbene il riconoscimento del browser non sia sempre accurato, questo potrebbe indicare che gli errori 500 non sono limitati a un singolo tipo di browser o sistema operativo, il che suggerisce che il problema è lato server e non dipende dal tipo di client.

Alcuni URL contengono il campo `JSESSIONID`, il cui valore è `SD10L52FF4ADDF53099`. Questo campo indica una sessione specifica per gli utenti e conferma che questi log provengono da un sistema che utilizza sessioni per la gestione delle interazioni utente. La presenza di `JSESSIONID` può aiutare a tracciare sessioni specifiche che riscontrano errori ripetuti, suggerendo un possibile problema con la gestione della sessione sul server.



Evento: Internal Server Error (status code: 500)

List Format 50 Per Page 		< Prev 1 2 3 4 5 6 7 8 9 Next >	
< Hide Fields All Fields	i	Time	Event
SELECTED FIELDS a host 1 a source 1 a sourcetype 1 a user 1	>	10/30/24 6:18:59.000 PM	198.35.1.75 - - [30/Oct/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 = Progetto_W24D4 source = tutorialdata.zip:./www1/access.log sourcetype = access_combined_wcookie user = -
	>	10/30/24 6:18:59.000 PM	198.35.1.75 - - [30/Oct/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 = Progetto_W24D4 source = tutorialdata.zip:./www1/access.log sourcetype = access_combined_wcookie user = -
INTERESTING FIELDS a action 5 # bytes 100+ a categoryid 6 a clientip 100+ # date_hour 24 # date_mday 8 # date_minute 56 a date_month 1 # date_second 58 a date_wday 7 a date_year 1 a date_zone 1 a file 4 a ident 1 a index 1 a itemid 14 a JSESSIONID 100+ # linecount 1 a method 2 # other 100+ a productid 12 a punct 27 a referer 65 a referer_domain 2 a req_time 100+ a splunk_server 1 # status 2 # timeendpos 6 # timestamppos 6 a uri 100+ a uri_path 4 a uri_query 100+ a useragent 25	>	10/30/24 6:18:59.000 PM	198.35.1.75 - - [30/Oct/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 = Progetto_W24D4 source = tutorialdata.zip:./www1/access.log sourcetype = access_combined_wcookie user = -
	>	10/30/24 6:18:59.000 PM	198.35.1.75 - - [30/Oct/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 = Progetto_W24D4 source = tutorialdata.zip:./www1/access.log sourcetype = access_combined_wcookie user = -
	>	10/30/24 6:18:55.000 PM	198.35.1.75 - - [30/Oct/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 = Progetto_W24D4 source = tutorialdata.zip:./www1/access.log sourcetype = access_combined_wcookie user = -
	>	10/30/24 6:18:55.000 PM	198.35.1.75 - - [30/Oct/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 = Progetto_W24D4 source = tutorialdata.zip:./www1/access.log sourcetype = access_combined_wcookie user = -
	>	10/30/24 6:18:55.000 PM	198.35.1.75 - - [30/Oct/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 = Progetto_W24D4 source = tutorialdata.zip:./www1/access.log sourcetype = access_combined_wcookie user = -
	>	10/30/24 6:18:55.000 PM	198.35.1.75 - - [30/Oct/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 = Progetto_W24D4 source = tutorialdata.zip:./www1/access.log sourcetype = access_combined_wcookie user = -
	>	10/30/24 5:17:00.000 PM	194.146.236.22 - - [30/Oct/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 = Progetto_W24D4 source = tutorialdata.zip:./www1/access.log sourcetype = access_combined_wcookie user = -
	>	10/30/24 5:17:00.000 PM	194.146.236.22 - - [30/Oct/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 = Progetto_W24D4 source = tutorialdata.zip:./www1/access.log sourcetype = access_combined_wcookie user = -
>	>	10/30/24 5:17:00.000 PM	194.146.236.22 - - [30/Oct/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

Evento: Internal Server Error (status code: 500)

New Search

Save As ▾Create Table ViewClose

* source="tutorialdata.zip:.\www1/access.log" "500" | stats count by clientip
| rename count as "Internal_Server_Errors"
| table clientip, Internal_Server_Errors

All time ▾

Q

✓ 438 events (before 11/1/24 6:45:54.000 PM)No Event Sampling ▾

Job ▾⏸⏹➡🖨⬇️🗨 Verbose Mode ▾

Events (438)PatternsStatistics (127)Visualization

50 Per Page ▾✍️FormatPreview ▾

< Prev123Next >

clientip ⚙️	Internal_Server_Errors ⚙️
107.3.146.207	3
108.65.113.83	5
109.169.32.135	3
110.138.30.229	2
111.161.27.20	2
112.111.162.4	1
117.21.246.164	2
118.142.68.222	1
12.130.60.5	4
121.254.179.199	1
121.9.245.177	1
123.196.113.11	2
124.160.192.241	1
125.17.14.100	1

Evento: Internal Server Error (status code: 500)

Remediation e azioni preventive

Controllo log backend


Esaminare i log di backend, come i log del database o di altre applicazioni interne, per individuare eventuali errori collegati a questi endpoint problematici.

Debugging Endpoint specifici

Analizzare e fare il debugging delle funzionalità addtocart, category.screen, e product.screen per assicurarsi che gestiscano correttamente tutti i casi, inclusi dati mancanti o non validi.

Monitoraggio sessioni

Controllare il sistema di gestione delle sessioni (JSESSIONID) per assicurarsi che gestisca correttamente le sessioni scadute o non valide.



Considerazioni generali sugli eventi analizzati


L'analisi dei log inclusi nell'archivio tutorialdata.zip permette di trarre alcune conclusioni generali sugli eventi visualizzati.

Presenza di vulnerabilità comuni: Gli incidenti di sicurezza evidenziati nei log indicano la presenza di vulnerabilità comuni come configurazioni SSH deboli o non sicure. Questo potrebbe indicare una mancanza di attenzione nelle pratiche di hardening dei sistemi e la configurazione di limitazioni specifiche per evitare compromissioni di sistema.

Lacune nei controlli di accesso: Molti incidenti sembrano derivare da problemi con i controlli di accesso, come l'uso di credenziali deboli o l'accesso non monitorato a risorse critiche. Tali tentativi non sono bloccati in tempo reale, suggerendo una mancanza di restrizioni sull'accesso o di rilevamento proattivo tramite strumenti di blocco automatico come fail2ban. Migliorare la gestione delle credenziali e implementare l'autenticazione multifattoriale potrebbe ridurre notevolmente questi rischi.

Errori del server e criticità lato backend: Gli errori interni del server (HTTP 500) ripetuti su endpoint specifici suggeriscono problemi strutturali, probabilmente dovuti a configurazioni errate o problemi applicativi persistenti che richiedono debug e testing approfonditi.

Necessità di formazione sulla sicurezza: Alcuni incidenti potrebbero essere stati causati da errori umani, come il clic su link di phishing o la condivisione accidentale di dati sensibili con conseguente compromissione delle credenziali di accesso. Una formazione continua per i dipendenti sulle migliori pratiche di sicurezza potrebbe ridurre l'incidenza di questi errori.



Conclusioni

Splunk è un potente e utile strumento per l'analisi delle cause principali (*root causes*) di eventi di sicurezza. La sua capacità di correlare errori e comportamenti anomali aiuta infatti a identificare rapidamente minacce ed eventuali vulnerabilità in un sistema.

Le query utilizzate in quest'analisi hanno offerto una visione chiara di eventi critici come tentativi di brute-force, sessioni SSH non autorizzate ed errori del server. Questi dati permettono un'analisi approfondita a posteriori volta a identificare attività sospette e migliorare la sicurezza, riducendo il rischio di attacchi e potenziali disservizi.

Gli eventi rilevanti per la sicurezza, al netto di falsi positivi, possono essere utilizzati per verifiche di conformità e audit. Splunk facilita la redazione di report per dimostrare l'efficacia delle misure di sicurezza, supportando un'analisi retrospettiva e formativa per evitare incidenti futuri.



Conclusioni

L'analisi degli accessi falliti e degli errori di sistema aiuta a individuare pattern di attacco ricorrenti, permettendo di progettare difese mirate e strategie di prevenzione personalizzate.

I report generati da Splunk forniscono informazioni “data-driven” fondamentali per decisioni strategiche e una distribuzione più efficace delle risorse verso le aree di maggiore criticità.

Splunk è altamente scalabile e si adatta a volumi elevati di log e a requisiti di monitoraggio complessi. La flessibilità delle query permette una personalizzazione completa, offrendo risposte mirate per le specifiche esigenze dell'organizzazione. Inoltre, le query di Splunk possono generare alert automatici, notificando in tempo reale gli amministratori per una risposta immediata. Ciò riduce i tempi di diagnostica e consente una reazione tempestiva agli incidenti di sicurezza.

Grazie alla sua capacità di monitoraggio continuo e alla rapidità di adattamento, Splunk è uno strumento essenziale per l'evoluzione delle strategie di sicurezza e la gestione avanzata dei log.

