

Nuova ricerca

source="tutorialdata.zip:\*" sourcetype="\*" "Failed password" "86.212.199.60"

Da 01/11/24 fino a 30/11/24

Q

26 eventi (01/11/24 00:00:00,000 - 01/12/24 00:00:00,000)

Nessun campionamento degli eventi

Processo

Modalità intelligente

Eventi (26)

Pattern

Statistiche

Visualizzazione

Formato timeline

Zoom indietro

Zoom area selezionata

Deseleziona

1 giorno per colonna

Elenco

Formato

50 per pagina

Nascondi campi

Tutti i campi

CAMPI SELEZIONATI

a host 1

a ip 1

a source 2

a sourcetype 1

CAMPI INTERESSANTI

# date\_hour 1

# date\_mday 1

# date\_minute 1

# date\_month 1

# date\_second 2

# date\_wday 1

# date\_year 1

a date\_zone 1

# index 1

# linecount 1

a punct 2

a splunk\_server 1

a status 1

a time\_stamp 2

i	Ora	Evento
>	01/11/24 04:36:40,000	Thu Nov 01 2024 04:36:40 mailsv1 sshd[5728]: Failed password for invalid user agushto from 86.212.199.60 port 3692 ssh2 host = dati_test   ip = 86.212.199.60   source = tutorialdata.zip:/mailsv/secure.log   sourcetype = secure-2
>	01/11/24 04:36:40,000	Thu Nov 01 2024 04:36:40 mailsv1 sshd[4843]: Failed password for invalid user tomcat from 86.212.199.60 port 1464 ssh2 host = dati_test   ip = 86.212.199.60   source = tutorialdata.zip:/mailsv/secure.log   sourcetype = secure-2
>	01/11/24 04:36:40,000	Thu Nov 01 2024 04:36:40 mailsv1 sshd[5718]: Failed password for invalid user desktop from 86.212.199.60 port 3518 ssh2 host = dati_test   ip = 86.212.199.60   source = tutorialdata.zip:/mailsv/secure.log   sourcetype = secure-2
>	01/11/24 04:36:40,000	Thu Nov 01 2024 04:36:40 mailsv1 sshd[1008]: Failed password for invalid user yp from 86.212.199.60 port 2856 ssh2 host = dati_test   ip = 86.212.199.60   source = tutorialdata.zip:/mailsv/secure.log   sourcetype = secure-2
>	01/11/24 04:36:40,000	Thu Nov 01 2024 04:36:40 mailsv1 sshd[5878]: Failed password for mail from 86.212.199.60 port 1054 ssh2 host = dati_test   source = tutorialdata.zip:/mailsv/secure.log   sourcetype = secure-2
>	01/11/24 04:36:40,000	Thu Nov 01 2024 04:36:40 mailsv1 sshd[2649]: Failed password for apache from 86.212.199.60 port 2630 ssh2 host = dati_test   source = tutorialdata.zip:/mailsv/secure.log   sourcetype = secure-2
>	01/11/24 04:36:40,000	Thu Nov 01 2024 04:36:40 mailsv1 sshd[2079]: Failed password for invalid user services from 86.212.199.60 port 4740 ssh2 host = dati_test   ip = 86.212.199.60   source = tutorialdata.zip:/mailsv/secure.log   sourcetype = secure-2
>	01/11/24 04:36:40,000	Thu Nov 01 2024 04:36:40 mailsv1 sshd[2205]: Failed password for invalid user irc from 86.212.199.60 port 1203 ssh2 host = dati_test   ip = 86.212.199.60   source = tutorialdata.zip:/mailsv/secure.log   sourcetype = secure-2

Conclusioni ChatGPT:

- **Possibile tentativo di attacco di brute-force:** Sono presenti 26 eventi di "Failed password" per nomi utente differenti, come agushto, tomcat, desktop, yp, mail, apache, irc, ecc. La varietà dei nomi utente suggerisce che l'IP 86.212.199.60 stia tentando un attacco di tipo brute-force per indovinare una combinazione valida di nome utente e password. Questo comportamento è comune negli attacchi automatizzati, in cui vengono tentati login su account predefiniti o comuni per ottenere accesso non autorizzato.
- **Origine del traffico sospetto:** Tutti i tentativi falliti provengono dall'IP 86.212.199.60, il che indica che questo indirizzo potrebbe essere compromesso o intenzionalmente utilizzato per lanciare attacchi verso server remoti. Se questo IP proviene da una regione non riconosciuta o non pertinente per l'organizzazione, potrebbe aumentare ulteriormente i sospetti su questa attività.
- **Nomi utente sospetti:** Gli account tentati includono agushto, tomcat, desktop, mail, apache, irc, ecc., che sono spesso nomi utente comuni o collegati a servizi di sistema. Questo tipo di tentativi potrebbe suggerire che l'attaccante stia cercando di accedere tramite utenti predefiniti o account di sistema, sperando che le password non siano state cambiate rispetto alle impostazioni di default.
- **Rischio per la sicurezza:** Se i tentativi continuano o se l'attaccante riesce a individuare una combinazione corretta di nome utente e password, potrebbe ottenere accesso non autorizzato al sistema, con potenziali implicazioni di sicurezza gravi, come furto di dati o compromissione dell'infrastruttura.

Azioni consigliate:

- **Bloccare l'IP sospetto:** Implementare una regola firewall o configurare un meccanismo di blocco automatico per prevenire ulteriori tentativi di login dall'IP 86.212.199.60.
- **Abilitare il fail2ban o meccanismi simili:** Strumenti come fail2ban possono bloccare automaticamente gli indirizzi IP che tentano ripetutamente di accedere al sistema con password errate, limitando il rischio di attacchi brute-force.
- **Verifica della sicurezza delle credenziali:** Assicurarsi che tutti gli account abbiano password forti e uniche. Potrebbe essere utile anche disabilitare l'accesso SSH per account non utilizzati o di sistema, riducendo il numero di potenziali punti di accesso.
- **Implementare l'autenticazione a due fattori (2FA):** L'autenticazione a due fattori per l'accesso SSH aggiungerebbe un ulteriore livello di sicurezza, rendendo più difficile per gli attaccanti accedere anche se riuscissero a indovinare una password.

- **Monitoraggio e segnalazione:** Continuare a monitorare i log per ulteriori tentativi di accesso da IP non autorizzati e configurare allarmi per notificare il personale di sicurezza in caso di attività sospetta.

In sintesi, questa schermata suggerisce che l'IP 86.212.199.60 stia effettuando un attacco di brute-force. Bloccare l'IP, rafforzare le misure di sicurezza e monitorare attentamente il sistema sono passi essenziali per mitigare il rischio.