Report di Sicurezza - Analisi Log Splunk

Report di Sicurezza - Analisi Log Splunk

1. Sommario

Nel corso dell'analisi sono stati esaminati diversi file di log provenienti da Splunk, relativi a tentativi di accesso falliti e ad errori di sistema. L'indagine ha messo in luce una serie di attività sospette, tipiche di attacchi automatizzati (brute-force) e tentativi di sfruttamento di vulnerabilità applicative.

2. Analisi per File

🗀 failedpass.csv

- Numerosi tentativi di login falliti su utenti generici e di sistema (`root`, `admin`, `oracle`, `nagios`, ecc.)

- Orario fisso e ripetitivo (`05:46:09`), suggerisce script automatizzato.

- Porte elevate e casuali, tipico di attacchi non convenzionali.

- Alcuni nomi utente sospetti: `testuser`, `noone`, `daemon`, `mantis`.

🗀 failedpassword.csv

- Log dettagliati di SSH con indirizzo IP sorgente e messaggi di errore (`Failed password for invalid user`)

- IP coinvolti: `194.215.205.19`, `87.194.216.51`

- Attacchi su nomi utente come `games`, `mysql`, `system`, `fpass`, `library`, ecc.

- Molti utenti non esistenti → uso di dizionari.

🗀 internalservererror.csv

- Numerosi HTTP 500 su `/cart.do`, `/product.screen`, `/oldlink`

- Parametri anomali (`categoryId=NULL`) indicano tentativi di fuzzing/scansione.

- User-Agent obsoleti → possibili bot o strumenti automatici.

- IP unici e distribuiti, scenario compatibile con attacchi applicativi.

🗀 morethen5.csv

- Elenco IP con >5 tentativi di accesso.

- IP `194.215.205.19` appare anche nei log SSH → conferma di attività ostile.

- Oltre 15 IP attivi in attività sospette → suggerisce botnet o scanner distribuiti.

🗀 ssh_djohnson.csv

- Tutti i tentativi sono sull'utente `djohnson`, nello stesso secondo.

- Attacco mirato e insistente.

- Potenziale rischio di compromissione specifica → da verificare accessi riusciti.

3. Indicatori di Compromissione (IOC)

- **Orario fisso** degli attacchi: `05:46:08/09`

- **Utenti sospetti**: `noone`, `daemon`, `testuser`, `system`, `fpass`, `djohnson`

- **IP coinvolti**:

  - `194.215.205.19`

  - `87.194.216.51`

  - Tutti quelli in `morethen5.csv`

4. Raccomandazioni

🔐 Protezione Account

- Verifica ed eventualmente disabilita gli utenti non utilizzati.

- Implementa l'autenticazione a due fattori dove possibile.

- Imposta login via SSH solo con chiavi.

🛡️ Difese perimetrali

- Applica `fail2ban` o simili per bloccare brute-force.

- Blocca gli IP segnalati.

- Limita l'accesso ai servizi a indirizzi IP autorizzati.

📈 Splunk - Suggerimenti di Alert

```
index=* "Failed password"
| stats count by src_ip, user
| where count > 5

index=* status=500
| stats count by uri_path, src_ip
| where count > 5

index=* "Failed password" user=djohnson
| stats count by _time, src_ip
```