Etap 4

Witamy po niebieskiej stronie :) Przeanalizujemy teraz jak wygląda przeprowadzony przez Was atak bruteforce oczami zespołu SOC. Warunkiem koniecznym do przejścia do tego etapu jest ukończenie etapów wcześniejszych (0-3), ponieważ zebrane podczas nich logi będą stanowiły fundament do dalszej pracy.

🔵 Blue Team Instrukcja

Ten przewodnik zawiera konkretne cele do osiągnięcia po każdym etapie ataku (1, 2, 3), wykorzystując efektywną analizę logów generowanych podczas prób uwierzytelniania (pliki auth_attempts_YYYYMMDD_HHMM.jsonl)

Krok 0

(jeśli korzystałeś kiedykolwiek z komendy jq w bashu możesz ten krok pominąć). Wprowadźmy/przypomnijmy kilka podstawowych komend, które przydadzą nam się również później:

- aby uniknąć ciągłego ręcznego wpisywania nazwy pliku, możesz użyć zmiennej BASH, która automatycznie znajdzie najnowszy log:
  LOGFILE=$(ls -t auth_attempts.jsonl | head -n 1*
  dalej możesz pisać już tylko $LOG_FILE
- wgląd we wszystkie dane z formatowaniem:
  cat $LOG_FILE | jq '.'
- wgląd w podsumowanie z liczbą zdarzeń:
  cat $LOG_FILE | wc -l
- wyodrębnianie kluczowych pól:
  cat $LOG_FILE | jq -r '[.datetime, .ip_address, .attempted_username, .result]'
  cat $LOG_FILE | jq -r '[.datetime, .ip_address, .attempted_username, .result] | @csv' (w formacie CSV)
- filtrowanie udanych logowań:
  cat $LOG_FILE | jq 'select(.result == "SUCCESS")'

Disclaimer:

jq jest jedynie propozycją do użycia w celu analizy otrzymanych logów w formacie JSON. Do dyspozycji macie całą gamę narzędzi i języków programowania które możecie wykorzystać do analizy wygenerowanego artefaktu: PowerShell, Bash, Python, Splunk Free, Elastic :)

Disclaimer 2:

Zdajemy sobie sprawę że realizacja wszystkich tych punktów to masa roboty, dlatego stawiamy Ci za cel analizę przynajmniej jednego z wyszczególnionych celów analizy przypadających na każdy etap. Jeśli jesteś niebieski, spróbuj popracować z resztą podpunktów we własnym zakresie :)

Krok 1

Jeśli pomyślnie zakończyłeś etap 1 Cel: Wykrycie skanowania nazw użytkowników i próby optymalizacji ataku. Poszczególne cele analizy (do uzyskania dowolnym narzędziem):

- lista unikalnych adresów IP
- liczba prób dla każdego IP
- IP skanujące loginy
- ilość nieudanych prób na znanym użytkowniku
- identyfikacja udanych ataków

Krok 2

Jeśli pomyślnie zakończyłeś etap 2 Cel: Wykrycie ataku pomimo braku wskazówek (ogólny błąd). Wskazówka: Analiza opiera się na wolumenie i czasie. Poszczególne cele analizy:

- izolowanie aktywności dla konkretnego hosta
- określenie liczby unikalnych prób logowania na konto 'user1'
- wykrycie nagłego wzrostu logowań (spike)
- weryfikacja braku rozróżniania błędów

Krok 3

Jeśli pomyślnie zakończyłeś etap 3 Cel: Wykrycie, czy mechanizm opóźnienia działa, i czy atakujący próbuje go ominąć (np. przełączając IP) Poszczególne cele analizy:

- potwierdzenie zastosowania opóźnienia
- średnie opóźnienie w logach
- wykrycie, że opóźnienie dotyczyło jednego IP
- wykrycie ataku typu IP Rotation

Tyle z niebieskiego :)