

Write-up: boot_time (level1)

<https://dreamhack.io/wargame/challenges/1326>

[1. Challenge Info](#)

[2. Problem Description](#)

[3. Provided Files](#)

[4. Tools Used](#)

[5. Analysis Steps](#)

[5.1 디스크 이미지 마운트](#)

[5.2 PC가 마지막으로 부팅된 시간 확인](#)

[5.6 최종 정보 정리](#)

[6. Flag](#)

1. Challenge Info

- **Challenge Name:** boot_time
- **Category:** Forensics
- **Difficulty Level:** Level 1
- **Platform:** DreamHack Wargame
- **Objective:**

고객의 해킹 사고를 분석해 해당 PC가 마지막으로 부팅된 시간을 구하여 플래그를 완성하라.

플래그 형식: DH{yyyy_MM_dd_hh_mm_ss}

- yy, MM, dd, hh, mm, ss는 시간을 표현하는 방식으로 각각 연, 월, 일, 시, 분, 초를 나타냄
- 시간은 UTC+9를 기준

2. Problem Description

“당신은 고객에게서 해킹 사고를 분석해달라는 의뢰를 받았습니다.

주어진 이미지의 이벤트 로그를 분석하여, 해당 PC가 마지막으로 부팅된 시간을 구해 주세요.”

- 제공된 디스크 이미지: `DiskImage02.E01`
- 이 파일은 `nikonikoni`, `chrome_artifacts` 문제와 동일

3. Provided Files

- `DiskImage02.E01` (Windows 시스템의 디스크 이미지 파일, E01 포맷)

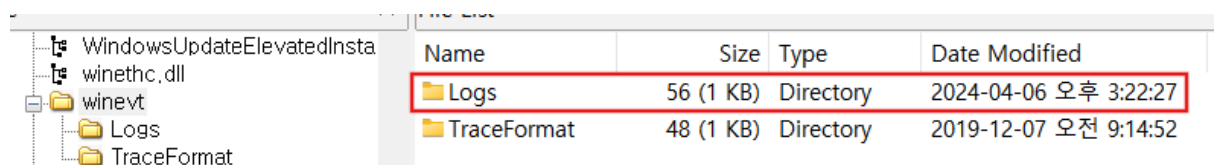
4. Tools Used

Tool	Version
FTK Imager	v4.7.8.31
이벤트 뷰어	v1.0

5. Analysis Steps

5.1 디스크 이미지 마운트

- 도구: FTK Imager
- 제공된 `DiskImage02.E01` 파일을 FTK Imager로 열기
- 로그파일 추출
 - 경로: `C:\Windows\system32\winevt\Logs`



Name	Size	Type	Date Modified
Logs	56 (1 KB)	Directory	2024-04-06 오후 3:22:27
TraceFormat	48 (1 KB)	Directory	2019-12-07 오전 9:14:52

5.2 PC가 마지막으로 부팅된 시간 확인

- 도구: 이벤트 뷰어
- 추출한 로그 파일을 이벤트 뷰어로 열기
- `system.evtx` 확인
 - Event ID 12: 시스템이 시작되었음을 알리는 이벤트
 - PC가 마지막으로 부팅된 시간: `2024-04-07 12:23:30`

System 이벤트 수: 1,458

필터링됨: 로그:

수준	날짜 및 시간	원본	이벤트 ID	작업 범주
정보	2024-01-17 오전 10:59:16	Kernel-General	12 (1)	
정보	2024-01-17 오전 11:01:11	Kernel-General	12 (1)	
정보	2024-01-17 오전 11:18:28	Kernel-General	12 (1)	
정보	2024-04-04 오후 8:58:55	Kernel-General	12 (1)	
정보	2024-04-04 오후 9:00:07	Kernel-General	12 (1)	
정보	2024-04-04 오후 9:02:02	Kernel-General	12 (1)	
정보	2024-04-04 오후 9:34:25	Kernel-General	12 (1)	
정보	2024-04-04 오후 9:39:46	Kernel-General	12 (1)	
정보	2024-04-07 오전 12:23:30	Kernel-General	12 (1)	

이벤트 12, Kernel-General

일반 자세히

운영 체제가 시스템 시간 2024 - 04 - 06T15:23:27.500000000Z에 시작되었습니다.

로그 이름(M): 시스템
 원본(S): Kernel-General
 이벤트 ID(E): 12
 수준(L): 정보
 사용자(U): SYSTEM
 Opcode(O): 정보

로그된 날짜(D): 2024-04-07 오전 12:23:30
 작업 범주(Y): (1)
 키워드(K): (128)
 컴퓨터(R): DESKTOP-JIC1U1P

→ 플래그 실패

- security.evtx 확인
 - Event ID 4608: Windows 보안 로그에서 시스템이 시작되었음을 알리는 이벤트
 - PC가 마지막으로 부팅된 시간: 2024-04-07 12:23:44

Security 이벤트 수: 5,485

필터링됨: 로그:

수준	날짜 및 시간	원본	이벤트 ID	작업 범주
정보	2024-01-17 오전 10:59:23	Microsoft Windo...	4608	Security State Change
정보	2024-01-17 오전 11:01:17	Microsoft Windo...	4608	Security State Change
정보	2024-01-17 오전 11:18:35	Microsoft Windo...	4608	Security State Change
정보	2024-04-04 오후 8:59:10	Microsoft Windo...	4608	Security State Change
정보	2024-04-04 오후 9:00:16	Microsoft Windo...	4608	Security State Change
정보	2024-04-04 오후 9:02:12	Microsoft Windo...	4608	Security State Change
정보	2024-04-04 오후 9:34:34	Microsoft Windo...	4608	Security State Change
정보	2024-04-04 오후 9:39:57	Microsoft Windo...	4608	Security State Change
정보	2024-04-07 오전 12:23:44	Microsoft Windo...	4608	Security State Change

이벤트 4608, Microsoft Windows security auditing.

일반 자세히

Windows를 시작하고 있습니다.

이 이벤트는 LSASS.EXE가 시작되고 감사 하위 시스템이 초기화될 때 기록됩니다.

로그 이름(M): 보안

원본(S): Microsoft Windows security **로그된 날짜(D): 2024-04-07 오전 12:23:44**

이벤트 ID(E): 4608 작업 범주(Y): Security State Change

수준(L): 정보 키워드(K): 감사 성공

사용자(U): 해당 없음 컴퓨터(R): DESKTOP-JIC1U1P

Opcode(O): 정보

5.6 최종 정보 정리

- PC가 마지막으로 부팅된 시간: 2024-04-07 12:23:44

6. Flag

DH{2024_04_07_00_23_44}

축하합니다!

1 LEVEL 1 boot_time
문제를 해결했습니다.

대단해요. 문제를 어떻게 해결하셨나요?
풀이를 작성하면 포인트까지 받을 수 있어요.

괜찮아요

 풀이 작성하기