

문제1. Baby's first forensics

난이도: 비기너

종목: 포렌식

Challenge

899 Solves

# Baby's First Forensics


## 100

beginner

They've been trying to breach our infrastructure all morning! They're trying to get more info on our covert kangaroos! We need your help, we've captured some traffic of them attacking us, can you tell us what tool they were using and its version?

NOTE: Wrap your answer in the `DUCTF{}`, e.g.  
`DUCTF{nmap_7.25}`

Author: Pix

 capture.pcap

Flag

Submit

문제설명: 공격에 사용된 툴과 그것의 버전을 밝혀라.

확장자가 pcap인 것을 보아 네트워크 포렌식 문제인가 보다.

솔직히 네트워크 포렌식 문제는 별로 풀고 싶진 않긴 한데, 비기너 난이도라니까 일단 해보자.

Challenge

529 Solves

# SAM I AM

## 100

beginner

The attacker managed to gain Domain Admin on our rebels Domain Controller! Looks like they managed to log on with an account using WMI and dumped some files.

Can you reproduce how they got the Administrator's Password with the artifacts provided?

Place the Administrator Account's Password in `DUCTF{ }`, e.g.

`DUCTF{password123!}`

Author: TurboPenguin

↓ samiam.zip

Flag

Submit

공격자가 우리 도메인 컨트롤러의 관리자 권한을 해킹했다. vmi를 이용해서 로그인 한 뒤 파일을 덤프한 것으로 보인다.

WMI) 네트워크에서 관리정보를 액세스하고 공유하는 표준을 만들기 위해 마이크로소프트가 구현한 프로그램.

WMIC) WMI용 커멘드 셸.



제공된 아티팩트(증거물)로 관리자 암호를 어떻게 얻었는지 재현하라;

즉 관리자 암호를 알아내면 끝.

문제 이름은 왜 sam I am 일까?

기묘하게 운율이 맞는 게 언어유희를 통한 힌트 같기도 하고.

📁 samiam

 sam	✔	2024-07-07 오후 4:03	BAK 파일	32KB
 system	✔	2024-07-07 오후 4:03	BAK 파일	12,036KB

안에는 두 개의 백업 파일이 있다.

용량과 이름을 보아서는 혹시 레지스트리 파일 백업인가?

```
A regf, , Æ ,
0 ;ÿî
0
0 p
0 \ S y s t e m R
0 o o t \ S y s t
0 e m 3 2 \ C o n
0 f i g \ S A M
D " <: # ± ä € ° ¨ ° ð ' µ -
D " <: # ± ä € ° ¨ ° ð ' µ -
A # <: # ± ä € ° ¨ °
1 ð ' µ - r m t m | % ü Ÿ Ä Ä Ü
0
0
0
0
n
```

맞다.

일단 파일 시그니처를 레지스트리 파일에 맞게 바꾼 뒤 레지스트리 분석 전용 도구를 이용해보자.

## 2) HKLM\SAM

- 해당 하이브는 사용자의 로컬 계정 정보(사용자 패스워드, 사용자 프로필 등)와 그룹 정보를 갖고 있음 (리눅스 /etc/passwd와 비슷)
- 만약 조사하고자 하는 시스템이 도메인 컨트롤러라면 AD(Active Directory)에 도메인 계정과 그룹 정보를 가짐
- 이 하이브는 일반 관리자 계정으로도 접근이 불가능하며, 시스템 계정으로만 접근 가능

시스템 계정 권한을 얻는 방법에는 여러 가지가 있으며 대체로 조사 과정에서는 통합 포렌식 도구들을 통해 얻는다.

대표적인 도구로는 psExec를 이용하여 일시적으로 얻는 방법이 있다.

그렇군....

파일 헤더에 전부 refg가 기입되어 있는 것으로 보아 따로 시그니처를 수정할 필요는 없어 보인다.

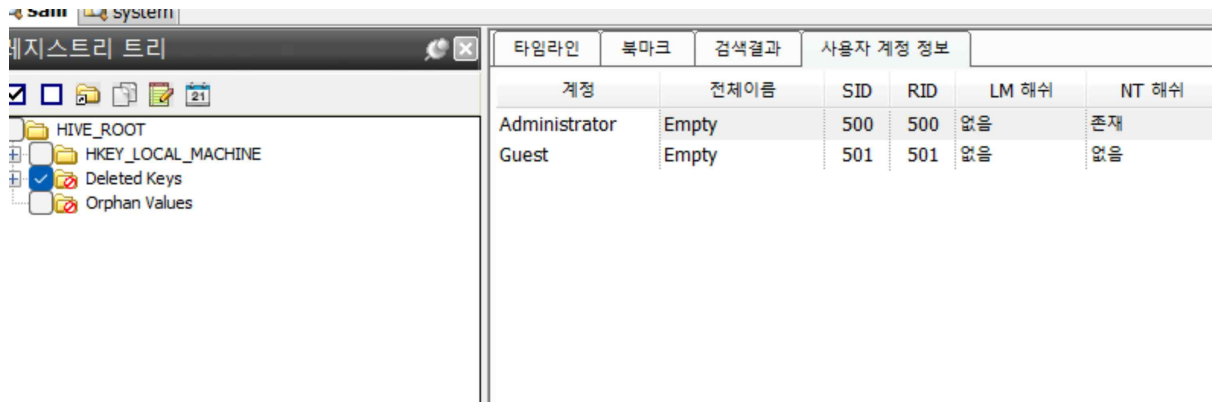
Name	S	C	O	Modified Time	Change Time
sam.bak				0000-00-00 00:00:00	0000-00-00 00:00:00
system.bak				0000-00-00 00:00:00	0000-00-00 00:00:00

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results
CsITool-CreateHive-{00000000-0000-0000-0000-000000000000}						
ControlSet001						
ControlSet002						
DriverDatabase						
HardwareConfig						
MountedDevices						
RNG						
ExternalEntropyCount						
Seed						
Select						
Current						
Default						
Failed						
LastKnownGood						
Setup						
WPA						

Metadata	
Name	Seed
Type	REG_BIN
Value	
0x0	52 75 6E 61
0x10	69 73 8D A1
0x20	17 84 08 D1
0x30	4E 24 B1 E1
0x40	1E 6D 3B C1



오웬토시와 레가 둘 모두로 분석이 가능한데, 이번 경우에는 레가 쪽이 가독성이 좋을 것 같다.

타입라인	북마크	검색결과	사용자 계정 정보				
계정	전체이름	SID	RID	LM 해쉬	NT 해쉬	상태	로그인횟수
Administrator	Empty	500	500	없음	존재	사용	0
Guest	Empty	501	501	없음	없음	미사용	0

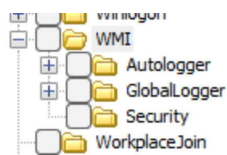
일단 관리자 계정으로 로그인한 기록은 없다. (횟수가 0으로 기록.) WMI로 우회하여 로그인했기 때문에 기록에 집계되지 않았을 수도 있다.

" LOGON 모든 로그인 세션의 목록을 확인합니다  
# wmic logon list full /format:list | more

이런 명령어로 우회하지 않았을까?

- HKEY\_USER: 시스템에 있는 모든 계정과 그룹에 대한 시스템 환경 정보가 정의

일단 여길 한번 확인해보자.



System 레지스트리의 controlset001 폴더 하위항목. WMI 데이터를 담당하는 폴더가 따로 존재한다.

# Windows 레지스트리의 WMI 클래스

이 섹션에서 설명하는 모든 WMI 클래스는 Windows 레지스트리에도 반영됩니다.

**주의:** 이 페이지에는 기계 번역된 콘텐츠가 포함되어 있습니다.

클래스는 다음 경로에서 찾을 수 있습니다.

64비트 시스템의 경우: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\F-Secure\Monitoring`

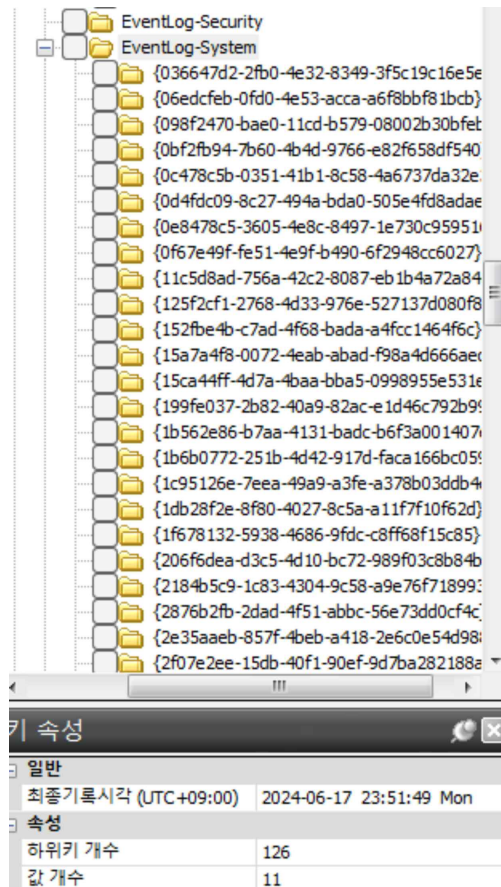
32비트 시스템의 경우: `HKEY_LOCAL_MACHINE\SOFTWARE\F-Secure\Monitoring`

?

아니....그냥도 있던데?

그리고 어차피 software 레지스트리가 없어서 확인이 불가능하다.

힌트를 좀 얻기 위해 WMI 공격사례를 검색해보았다.



하....개많은데?ㅋㅋㅋ

아래의 파일을 하나씩 체크해보면 공통적으로 다음과 같은 키를 가지고 있다.

키 탐색    타임라인 아이템		
값 이름	값 종류	값 데이터
Enabled	REG_DWORD	00000001
EnableLevel	REG_DWORD	00000000
LoggerName	REG_SZ	EventLog-System
MatchAnyKeyword	REG_QWORD	00 00 00 00 00 00 00 40
MatchAllKeyword	REG_QWORD	00 00 00 00 00 00 00 00
EnableProperty	REG_DWORD	00000001
Status	REG_DWORD	00000000

이게 각각 뭘 의미하는 걸까?

enable property; 조건부 서식(?) 활성화

> 아무튼 무언가가 수정 가능한 상태

matchanykeyword

>?

matchallkeyword

>?

사용자 정보	HKU	USER_SID	각 사용자의 설정 정보 (NTUSER.dat)
--------	-----	----------	---------------------------

아....그래. 저 dat 파일이 없어서 현재 sam 레지스트리를 통해 사용자 암호를 캐내는 건 불가능하다.

그럼 결국 WMI를 통한 해킹 경로를 좇아 암호를 알아낼 수밖에 없다는 건데, WMI 레지스트리에 대한 정보값이 없어도 너무 없다.



???

WMI 공격 사례 몇 개를 읽어봤는데 여전히 무슨 값을 체크해야 하는 건지 모르겠다.

참고자료

<https://yum-history.tistory.com/265>