Suninatas Game 30

해커가 김장군의 PC에 침투한 흔적을 발견하였다.
사고 직후 김장군의 PC에서 획득한 메모리 덤프를 제공받은 당신은 해커가 한 행동을 밝혀내야한다.

1. 김장군 PC의 IP 주소는?
2. 해커가 열람한 기밀문서의 파일명은?
3. 기밀문서의 주요 내용은? 내용속에 "Key"가 있다.

인증키 형식 : lowercase(MD5(1번답+2번답+3번키))

문제는 다음과 같다. 문제에서 제공하는 메모리 덤프를 다운받아준다.

먼저 ip주소를 알아내려면 네트워크 정보를 검색해야 한다. 네트워크 정보 검색은 ip주소를 포함한 다양한 네트워크 관련 데이터를 출력할 수 있다. 여기서 사용하는 플러그인은 windows.netscan이다.

```
PS C:\volatility3> python vol.py -f "MemoryDump(SuNiNaTaS)" windows.netscan
```

```
0x3e1c2a30      TCPv4   0.0.0.0 49153   0.0.0.0 0       LISTENING       73
0x3e1e2008      TCPv4   192.168.197.138 49252   61.111.58.11    80      ES
0x3e1f0340      TCPv4   0.0.0.0 49154   0.0.0.0 0       LISTENING       89
0x3ee4f9e8      TCPv4   192.168.197.138 49173   23.43.5.163     80      CL
0x3ee7d688      TCPv4   192.168.197.138 49163   211.233.62.122  80      ES
0x3ee7d910      TCPv4   192.168.197.138 49167   121.189.57.82   80      ES
0x3f26e5f0      UDPv4   192.168.197.138 138     *       0               4
0x3f270450      TCPv4   192.168.197.138 139     0.0.0.0 0       LISTENING
0x3f270768      UDPv4   192.168.197.138 137     *       0               4
0x3f430b70      TCPv4   192.168.197.138 49168   216.58.197.132  80      ES
0x3f7854b8      TCPv4   192.168.197.138 49164   211.233.62.122  80      ES
0x3f78bd68      TCPv4   192.168.197.138 49179   59.18.34.167    443     ES
0x3f7deb30      TCPv4   192.168.197.138 49184   114.108.157.50  80      ES
0x3fc5f998      TCPv4   192.168.197.138 49178   59.18.34.167    443     ES
0x3fc6d638      TCPv4   192.168.197.138 49172   172.217.25.67   443     ES
0x3fc77df8      TCPv4   192.168.197.138 49176   172.217.25.67   443     ES
0x3fc84348      TCPv4   192.168.197.138 49169   216.58.197.132  80      ES
0x3fc86008      TCPv4   192.168.197.138 49175   59.18.35.55     80      CL
```

결과를 보면 192.168.197.138이라는 ip 주소가 지속적으로 나타나고 있음을 볼 수 있다. 따라서 이것을 김장군 pc의 ip주소라 추측할 수 있다.

파일명을 알아내기 위해서는 windows.cmdline 플러그인을 사용한다. 플러그인을 실행하면 메모리 덤프에서 발견된 각 프로세스의 정보를 볼 수 있고, 실행된 명령어 확인 및 사용자 활동을 분석할 수 있으므로 기밀문서로 의심되는 파일명을 찾아볼 수 있다.

```
PS C:\volatility3-develop> python vol.py -f "MemoryDump(SuNiNaTaS)" windows.cmdline
Volatility 3 Framework 2.25.0
Progress:  100.00               PDB scanning finished
PID     Process Args

4       System  -
236     smss.exe        \SystemRoot\System32\smss.exe
320     csrss.exe       %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=
 SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 Serve
nitialization,2 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
```

```
1840    iexplore.exe    "C:\Program Files\Internet Explorer\iexplore.exe" SCODEF:3948 CRED
2432    iexplore.exe    "C:\Program Files\Internet Explorer\iexplore.exe" SCODEF:3948 CRED
1256    cmd.exe "C:\Windows\system32\cmd.exe"
2920    conhost.exe     \??\C:\Windows\system32\conhost.exe "-178222926316055376 52-1122368
6393-1755504625193855 0102
3728    notepad.exe     notepad  C:\Users\training\Desktop\SecreetDocumen7.txt
4048    SearchProtocol  "C:\Windows\system32\SearchProtocolHost.exe" Global\UsGthrFltPipeM
-2591454169-3626909997-10006_ Global\UsGthrCtrlFltPipeMssGthrPipe_S-1-5-21-1227645660-2591
7483646 "Software\Microsoft\Windows Search" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT
ogramData\Microsoft\Search\Data\Temp\usgthrsvc" "DownLevelDaemon"  "1"
2696    SearchFilterHo  "C:\Windows\system32\SearchFilterHost.exe" 0 524 528 536 65536 532
```

Notepad.exe에서 SecreetDocumen7.txt라는 수상한 제목의 텍스트 파일을 작성했음을 관찰할 수 있다.

이제 기밀문서의 주요 내용을 알아내야 한다. 일단 파일의 정보를 알아내기 위해 windows.filescan 플러그인을 사용한다. windows.filescan 플러그인은 메모리 덤프에서 파일 객체(File Object)를 검색하여 관련된 정보를 보여주는 역할을 한다.

```
PS C:\volatility3-develop> python vol.py -f "MemoryDump(SuNiNaTaS)" windows.filescan
Volatility 3 Framework 2.25.0
Progress:  100.00               PDB scanning finished
Offset  Name

0x31adc98
```

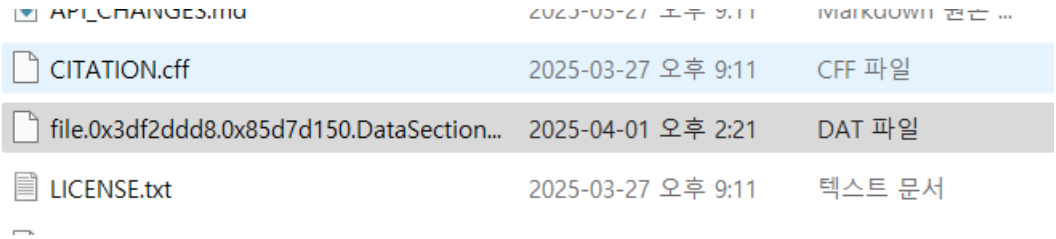
```
0x3df2b968      \Windows\System32\wdc.dll
0x3df2bad8      \Windows\System32\wercplsupport.dll
0x3df2bbb8      \Windows\System32\COLORCNV.DLL
0x3df2dc28      \Users\training\AppData\Local\Microsoft\Windows\Explore
0x3df2ddd8      \Users\training\Desktop\SecreetDocumen7.txt
0x3df2de98      \$Directory
0x3df2f308      \Users\training\AppData\Roaming\Microsoft\Windows\Start
0x3df2f428      \$Directory
0x3df30890      \Windows\System32\MFPlay.dll
0x3df33038      \Users\training\Desktop\desktop.ini
```

이렇게 SecreetDocumen7.txt 파일의 정보를 확인할 수 있다. 이때 물리적 메모리 주소까지 확인할 수 있으므로 이 정보를 이용하여 파일의 내용을 살펴볼 수 있다.

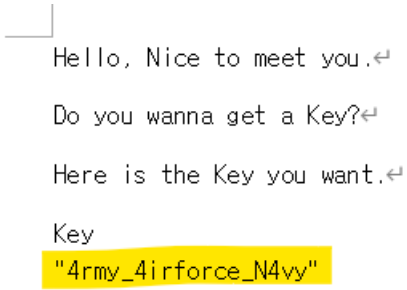
windows.dumpfiles 플러그인은 메모리 내의 특정 주소 또는 파일 객체와 관련된 데이터를 파일 시스템으로 추출 및 저장할 수 있다. 우리는 파일의 물리 메모리 주소를 알고 있으므로 옵션을 붙여 파일을 지정해 추출이 가능하다.

windows.dumpfiles --physaddr 0x3df2ddd8 명령어를 이용한다.

```
PS C:\volatility3-develop> python vol.py -f "MemoryDump(SuNiNaTaS)" windows.dumpfiles --physaddr 0x3df2ddd8
Volatility 3 Framework 2.25.0
Progress:  0.00          Scanning FileLayer using PageMapScanner
```

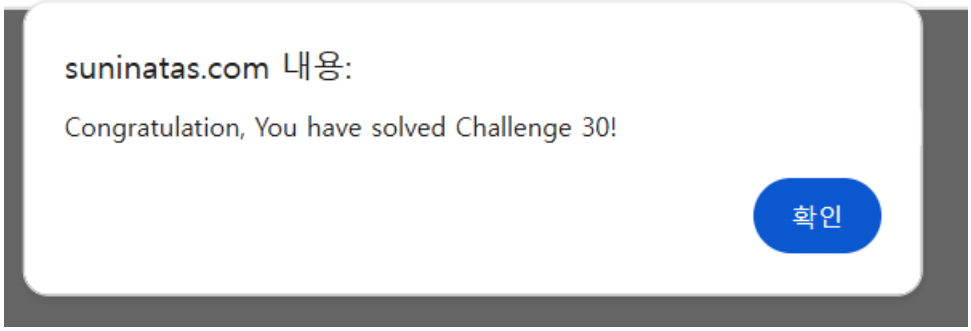


그러면 이렇게 dat 파일로 저장된다.



파일을 열어보면 이렇게 키를 확인할 수 있다.

앞에서 알아낸 세가지 답을 조합하면 192.168.197.138SecreetDocumen7.txt4rmy_4irforce_N4vy라 할 수 있다. 이를 md5값으로 암호화하고 입력하면 이렇게 문제를 해결할 수 있다.



문제를 풀면서 여기를 많이 참고했다. https://blog.onfvp.com/post/volatility-cheatsheet/