
ATTACK
DEFENSE
by PentesterAcademy

Name	Opensnoop: Trace Analysis
URL	https://attackdefense.com/challengedetails?cid=1116
Type	Linux Runtime Analysis : Profiling Tools

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Q1. A malicious process was searching for some files on the system. What is the name of that process?

Answer: 125316097e

Command: less logs

```
Tracing open()s. Ctrl-C to end.
COMM                PID      FD FILE
<...>               56784   0x3
<...>               56788   0x3 /etc/ld.so.cache
<...>               56788   0x3 /lib/x86_64-linux-gnu/libm.so.6
<...>               56788   0x3 /lib/x86_64-linux-gnu/libc.so.6
<...>               56789   0x3 /etc/ld.so.cache
<...>               56789   0x3 /lib/x86_64-linux-gnu/libc.so.6
<...>               56789   0x3 trace_pipe
<...>               56790   0x3 /etc/ld.so.cache
<...>               56790   0x3 /lib/x86_64-linux-gnu/libc.so.6
<...>               56791   0x3 /etc/ld.so.cache
<...>               56791   0x3 /lib/x86_64-linux-gnu/libc.so.6
<...>               56791   0x3 /lib/x86_64-linux-gnu/libdl.so.2
<...>               56791   0x0 /var/lib/xkb/server-0.xkm
Xorg                6054   0x25 /var/lib/xkb/server-0.xkm
125316097e          56793   0x3 /etc/ld.so.cache
125316097e          56793   0x3 /lib/x86_64-linux-gnu/libpthread.so.0
125316097e          56793   0x3 /lib/x86_64-linux-gnu/libc.so.6
125316097e          56793   0x3 /lib/x86_64-linux-gnu/libdl.so.2
```

```
125316097e          56793   0x3 /etc
125316097e          56793    -1 /etc/.simple-miner
125316097e          56793    -1 /etc/.dummy-snooper
125316097e          56793    -1 /etc/.escalator
125316097e          56793    -1 /etc/.logger
125316097e          56793    -1 /etc/.encryptor
125316097e          56793    -1 /etc/.silent-snooper
125316097e          56793    -1 /etc/.spy-adsadsdfrg
125316097e          56793    -1 /etc/.sync-sdfsd
125316097e          56793    -1 /etc/.session-logger
125316097e          56793   0x3 /etc/libpaper.d
125316097e          56793    -1 /etc/libpaper.d/.simple-miner
125316097e          56793    -1 /etc/libpaper.d/.dummy-snooper
125316097e          56793    -1 /etc/libpaper.d/.escalator
125316097e          56793    -1 /etc/libpaper.d/.logger
125316097e          56793    -1 /etc/libpaper.d/.encryptor
125316097e          56793    -1 /etc/libpaper.d/.silent-snooper
125316097e          56793    -1 /etc/libpaper.d/.spy-adsadsdfrg
125316097e          56793    -1 /etc/libpaper.d/.sync-sdfsd
125316097e          56793    -1 /etc/libpaper.d/.session-logger
```

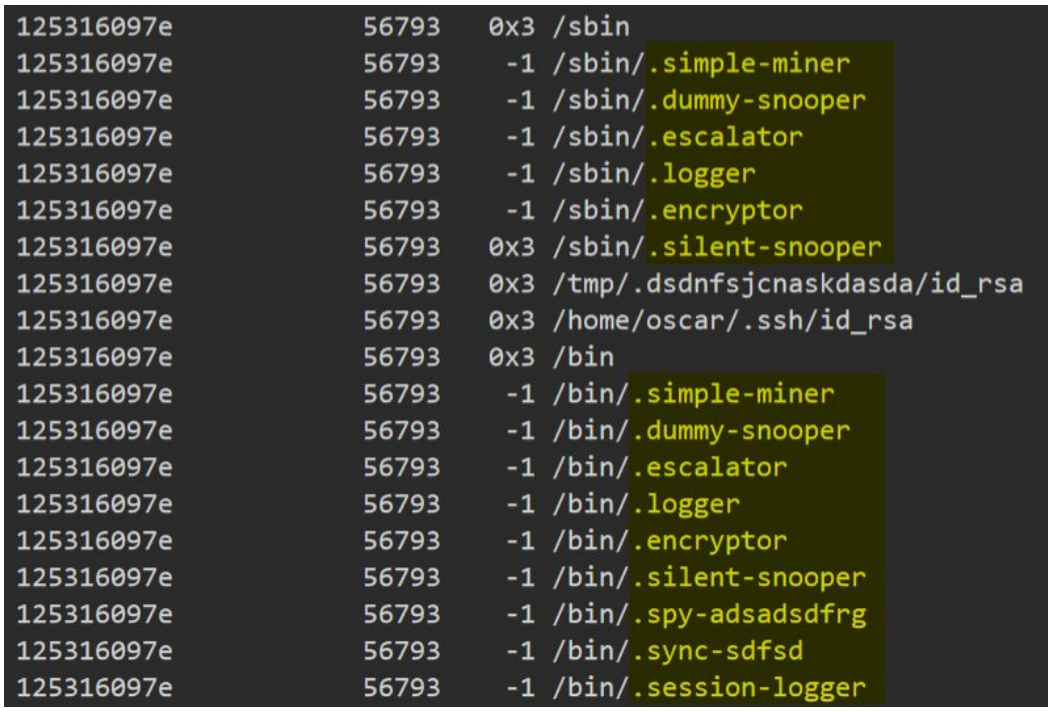
The process named '125316097e' is opening a lot of files and has a lot of unsuccessful attempts, indicated by -1.

Q2. The malicious process was successful in finding one of the files it was searching for. Provide the complete path of that file.

Answer: /sbin/.silent-snooper

```
125316097e            56793   0x3 /etc
125316097e            56793    -1 /etc/.simple-miner
125316097e            56793    -1 /etc/.dummy-snooper
125316097e            56793    -1 /etc/.escalator
125316097e            56793    -1 /etc/.logger
125316097e            56793    -1 /etc/.encryptor
125316097e            56793    -1 /etc/.silent-snooper
125316097e            56793    -1 /etc/.spy-adsadsdfrg
125316097e            56793    -1 /etc/.sync-sdfsd
125316097e            56793    -1 /etc/.session-logger
125316097e            56793   0x3 /etc/libpaper.d
125316097e            56793    -1 /etc/libpaper.d/.simple-miner
125316097e            56793    -1 /etc/libpaper.d/.dummy-snooper
125316097e            56793    -1 /etc/libpaper.d/.escalator
125316097e            56793    -1 /etc/libpaper.d/.logger
125316097e            56793    -1 /etc/libpaper.d/.encryptor
125316097e            56793    -1 /etc/libpaper.d/.silent-snooper
125316097e            56793    -1 /etc/libpaper.d/.spy-adsadsdfrg
125316097e            56793    -1 /etc/libpaper.d/.sync-sdfsd
125316097e            56793    -1 /etc/libpaper.d/.session-logger
```

```
125316097e            56793   0x3 /home/oscar
125316097e            56793    -1 /home/oscar/.simple-miner
125316097e            56793    -1 /home/oscar/.dummy-snooper
125316097e            56793    -1 /home/oscar/.escalator
125316097e            56793    -1 /home/oscar/.logger
125316097e            56793    -1 /home/oscar/.encryptor
125316097e            56793    -1 /home/oscar/.silent-snooper
125316097e            56793    -1 /home/oscar/.spy-adsadsdfrg
125316097e            56793    -1 /home/oscar/.sync-sdfsd
125316097e            56793    -1 /home/oscar/.session-logger
```



The above screenshots depict that the process was looking for some set for files in every directory.

The value '-1' before the file name indicates a failed attempt.

The logs reveal that the files that the malicious process looks for are:

'.simple-miner', '.dummy-snooper', '.escalator', '.logger', '.encryptor', '.silent-snooper', '.spy-adsadsdfrg', '.sync-sdfsd' and '.session-logger'.

Command: grep 125316097e logs | grep -v '\-1'

```
root@attackdefense:~# grep 125316097e logs | grep -v '\-1'
125316097e            56793   0x3 /etc/ld.so.cache
125316097e            56793   0x3 /lib/x86_64-linux-gnu/libpthread.so.0
125316097e            56793   0x3 /lib/x86_64-linux-gnu/libc.so.6
125316097e            56793   0x3 /lib/x86_64-linux-gnu/libdl.so.2
125316097e            56793   0x3 /lib/x86_64-linux-gnu/libutil.so.1
125316097e            56793   0x3 /lib/x86_64-linux-gnu/libz.so.1
125316097e            56793   0x3 /lib/x86_64-linux-gnu/libm.so.6
125316097e            56793   0x3 ./125316097e
```

```
125316097e            56793   0x3 /etc/john
125316097e            56793   0x3 /home/oscar
125316097e            56793   0x3 /sbin
125316097e            56793   0x3 /sbin/.silent-snooper
125316097e            56793   0x3 /tmp/.dsdnfsjcnaskdasda/id_rsa
125316097e            56793   0x3 /home/oscar/.ssh/id_rsa
125316097e            56793   0x3 /bin
125316097e            56793   0x3 /opt
125316097e            56793   0x3 /opt/containerd
125316097e            56793   0x3 /opt/containerd/bin
125316097e            56793   0x3 /opt/containerd/lib
root@attackdefense:~#
```

The above command shows all the files that were successfully opened by '125316097e' process.

Among the successfully opened files, the file name '.silent_snooper' was also opened and it was one of the files that the malicious process was searching for.

Q3. The malware had stored some secret in the file it had successfully found. Locate the file and retrieve the secret flag.

Answer: e98bc2aedf7b513f9e97dcfce3176d7b

Command: cat /sbin/.silent-snooper

```
root@attackdefense:~# cat /sbin/.silent-snooper
-== Silent-Snooper ==-
DATE: Tue Jun 18 15:36:56 UTC 2018
FLAG: e98bc2aedf7b513f9e97dcfce3176d7b
root@attackdefense:~#
```

Q4. The malware had generated a set of private ssh keys somewhere in the /tmp directory. Provide the complete path where the generated keys were stored?

Answer: /tmp/.dsdnfsjcnaskdasda/id_rsa

Command: grep 125316097e logs | grep -v '\-1'

```
root@attackdefense:~# grep 125316097e logs | grep -v '\-1'
125316097e            56793   0x3 /etc/ld.so.cache
125316097e            56793   0x3 /lib/x86_64-linux-gnu/libpthread.so.0
125316097e            56793   0x3 /lib/x86_64-linux-gnu/libc.so.6
125316097e            56793   0x3 /lib/x86_64-linux-gnu/libdl.so.2
125316097e            56793   0x3 /lib/x86_64-linux-gnu/libutil.so.1
125316097e            56793   0x3 /lib/x86_64-linux-gnu/libz.so.1
125316097e            56793   0x3 /lib/x86_64-linux-gnu/libm.so.6
125316097e            56793   0x3 ./125316097e
```

```
125316097e            56793   0x3 /etc/john
125316097e            56793   0x3 /home/oscar
125316097e            56793   0x3 /sbin
125316097e            56793   0x3 /sbin/.silent-snooper
125316097e            56793   0x3 /tmp/.dsdnfsjcnaskdasda/id_rsa
125316097e            56793   0x3 /home/oscar/.ssh/id_rsa
125316097e            56793   0x3 /bin
125316097e            56793   0x3 /opt
125316097e            56793   0x3 /opt/containerd
125316097e            56793   0x3 /opt/containerd/bin
125316097e            56793   0x3 /opt/containerd/lib
root@attackdefense:~#
```

OR

Command: grep id_rsa logs

```
root@attackdefense:~# grep id_rsa logs
125316097e            56793   0x3 /tmp/.dsdnfsjcnaskdasda/id_rsa
125316097e            56793   0x3 /home/oscar/.ssh/id_rsa
root@attackdefense:~#
```

Q5. The malware had replaced the private ssh keys of a user with the private keys it had generated. What is the name of that user?

Answer: oscar

```
root@attackdefense:~# grep id_rsa logs
125316097e            56793   0x3 /tmp/.dsdnfsjcnaskdasda/id_rsa
125316097e            56793   0x3 /home/oscar/.ssh/id_rsa
root@attackdefense:~#
```

References:

1. Opensnoop script (https://github.com/iovisor/bcc/blob/master/tools/opensnoop.py)
2. Opensnoop Examples (https://github.com/iovisor/bcc/blob/master/tools/opensnoop_example.txt)
3. BCC Tools (https://github.com/iovisor/bcc)