
ATTACK
DEFENSE
by PentesterAcademy

Name	Perf Basics I
URL	https://attackdefense.com/challengedetails?cid=1101
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. Provide the full path of the password cracking service.

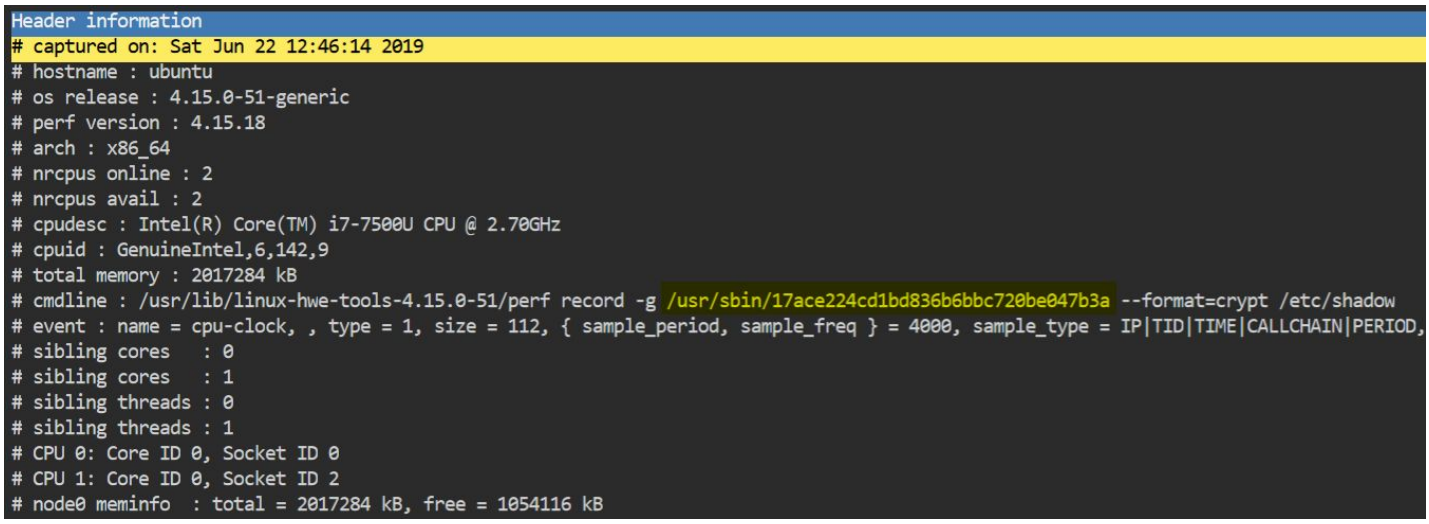
Answer: /usr/sbin/17ace224cd1bd836b6bbc720be047b3a

Solution:

Command: perf report

```
Samples: 89K of event 'cpu-clock', Event count (approx.): 22475000000
  Children      Self  Command          Shared Object                 Symbol
+    4.60%     0.00%  17ace224cd1bd83  [unknown]                     [.] 0xbb67ae8584caa73b
+    2.72%     2.72%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x0000000000006372
+    2.69%     2.69%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x0000000000006376
+    1.98%     1.97%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x0000000000006396
+    1.90%     1.90%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x00000000000063a3
+    1.78%     1.77%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x000000000000635b
+    1.76%     1.76%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x00000000000063d0
+    1.75%     1.74%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x0000000000006363
+    1.73%     1.72%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x000000000000638a
+    1.72%     1.72%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x000000000000634f
+    1.72%     1.72%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x000000000000637e
+    1.72%     1.71%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x00000000000063c3
+    1.69%     1.69%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x00000000000063bd
+    1.64%     1.64%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x00000000000063b0
+    1.61%     1.61%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x000000000000636a
+    1.53%     1.53%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x0000000000006343
```

Press 'i' to get the header information.



'cmdline' corresponds to the command executed when the trace was captured.

Q2. The service used a crypto library. What is the name of the shared object (.so file) of that library?

Answer: libcrypt-2.23.so

Command: perf report

```
Samples: 89K of event 'cpu-clock', Event count (approx.): 22475000000
  Children      Self  Command          Shared Object                 Symbol
+    4.60%     0.00%  17ace224cd1bd83  [unknown]                     [.] 0xbb67ae8584caa73b
+    2.72%     2.72%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x0000000000006372
+    2.69%     2.69%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x0000000000006376
+    1.98%     1.97%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x0000000000006396
+    1.90%     1.90%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x00000000000063a3
+    1.78%     1.77%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x000000000000635b
+    1.76%     1.76%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x00000000000063d0
+    1.75%     1.74%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x0000000000006363
+    1.73%     1.72%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x000000000000638a
+    1.72%     1.72%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x000000000000634f
+    1.72%     1.72%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x000000000000637e
+    1.72%     1.71%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x00000000000063c3
+    1.69%     1.69%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x00000000000063bd
+    1.64%     1.64%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x00000000000063b0
+    1.61%     1.61%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x000000000000636a
+    1.53%     1.53%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x0000000000006343
+    1.49%     1.49%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x0000000000006355
+    1.42%     1.42%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x00000000000063ca
+    1.33%     1.32%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x000000000000635f
+    1.30%     1.29%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x000000000000636d
+    1.29%     1.29%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x00000000000063b7
+    1.28%     1.28%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x00000000000062c1
+    1.23%     1.23%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x0000000000006349
+    1.22%     1.22%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x0000000000006367
+    1.20%     1.20%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x00000000000063c0
```

The events data reveals heavy usage of libcrypt-2.23.so.

Q3. The service was cracking the contents of a file. Provide the full path of that file.

Answer: /etc/shadow

Solution:

Command: perf report

```
Samples: 89K of event 'cpu-clock', Event count (approx.): 22475000000
  Children      Self  Command          Shared Object                 Symbol
+    4.60%     0.00%  17ace224cd1bd83  [unknown]                     [.] 0xbb67ae8584caa73b
+    2.72%     2.72%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x0000000000006372
+    2.69%     2.69%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x0000000000006376
+    1.98%     1.97%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x0000000000006396
+    1.90%     1.90%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x00000000000063a3
+    1.78%     1.77%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x000000000000635b
+    1.76%     1.76%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x00000000000063d0
+    1.75%     1.74%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x0000000000006363
+    1.73%     1.72%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x000000000000638a
+    1.72%     1.72%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x000000000000634f
+    1.72%     1.72%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x000000000000637e
+    1.72%     1.71%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x00000000000063c3
+    1.69%     1.69%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x00000000000063bd
+    1.64%     1.64%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x00000000000063b0
+    1.61%     1.61%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x000000000000636a
+    1.53%     1.53%  17ace224cd1bd83  libcrypt-2.23.so              [.] 0x0000000000006343
```

Press 'i' to get the header information.

```
Header information
# captured on: Sat Jun 22 12:46:14 2019
# hostname : ubuntu
# os release : 4.15.0-51-generic
# perf version : 4.15.18
# arch : x86_64
# nrcpus online : 2
# nrcpus avail : 2
# cpudesc : Intel(R) Core(TM) i7-7500U CPU @ 2.70GHz
# cpuid : GenuineIntel,6,142,9
# total memory : 2017284 kB
# cmdline : /usr/lib/linux-hwe-tools-4.15.0-51/perf record -g /usr/sbin/17ace224cd1bd836b6bbc720be047b3a --format=crypt /etc/shadow
# event : name = cpu-clock, , type = 1, size = 112, { sample_period, sample_freq } = 4000, sample_type = IP|TID|TIME|CALLCHAIN|PERIOD,
# sibling cores   : 0
# sibling cores   : 1
# sibling threads : 0
# sibling threads : 1
# CPU 0: Core ID 0, Socket ID 0
# CPU 1: Core ID 0, Socket ID 2
# node0 meminfo  : total = 2017284 kB, free = 1054116 kB
```

'cmdline' corresponds to the command executed when the trace was captured.

References:

1. Perf (https://perf.wiki.kernel.org/index.php/Main_Page)