ATTACK DEFENSE

by PentesterAcademy

Name	Perf Basics II
URL	https://attackdefense.com/challengedetails?cid=1102
Type	Linux Runtime Analysis: Profiling Tools

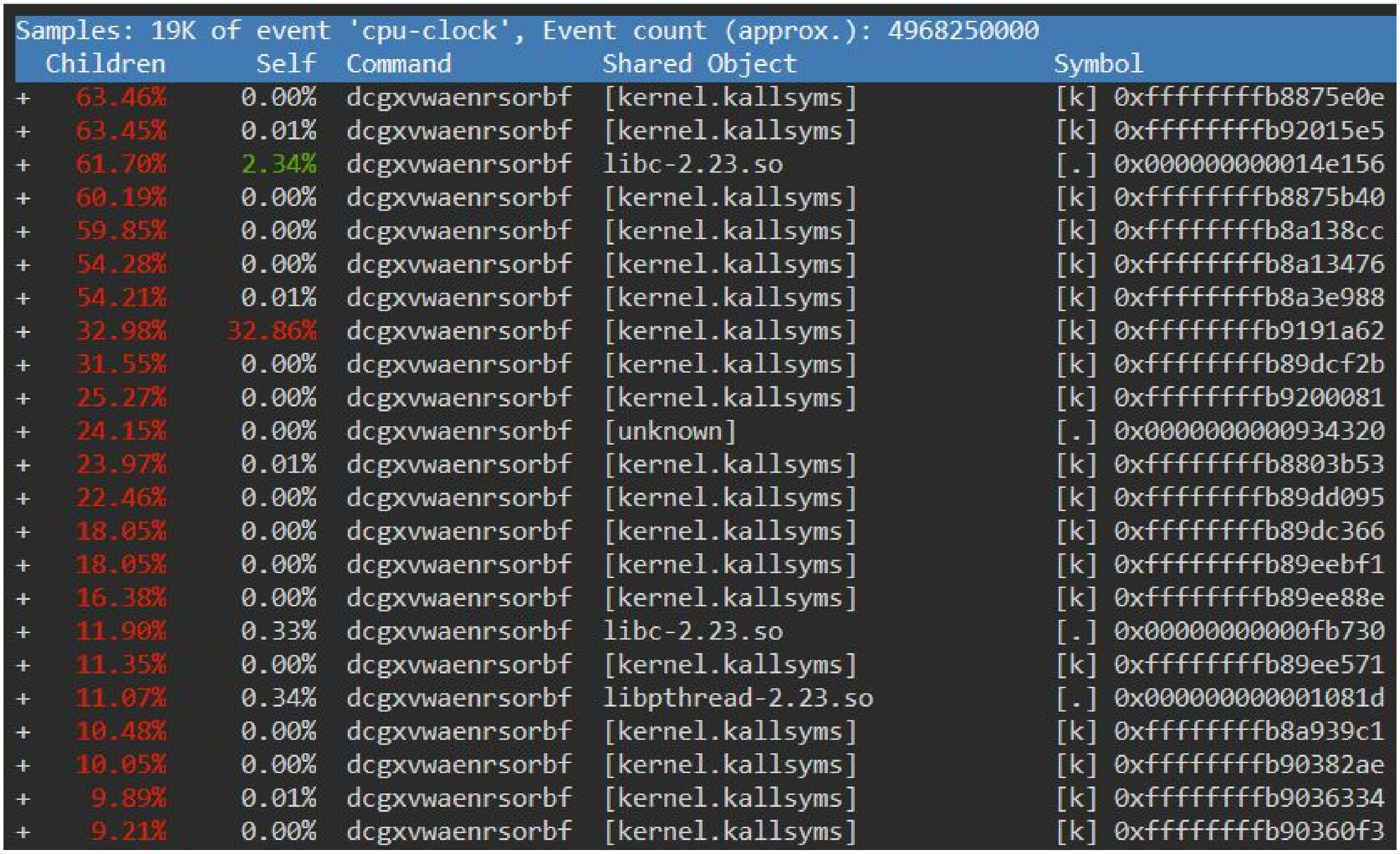
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this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

Q1. What is the name of the crypto miner service?

Answer: dcgxvwaenrsorbfsdfvzcasrvxc

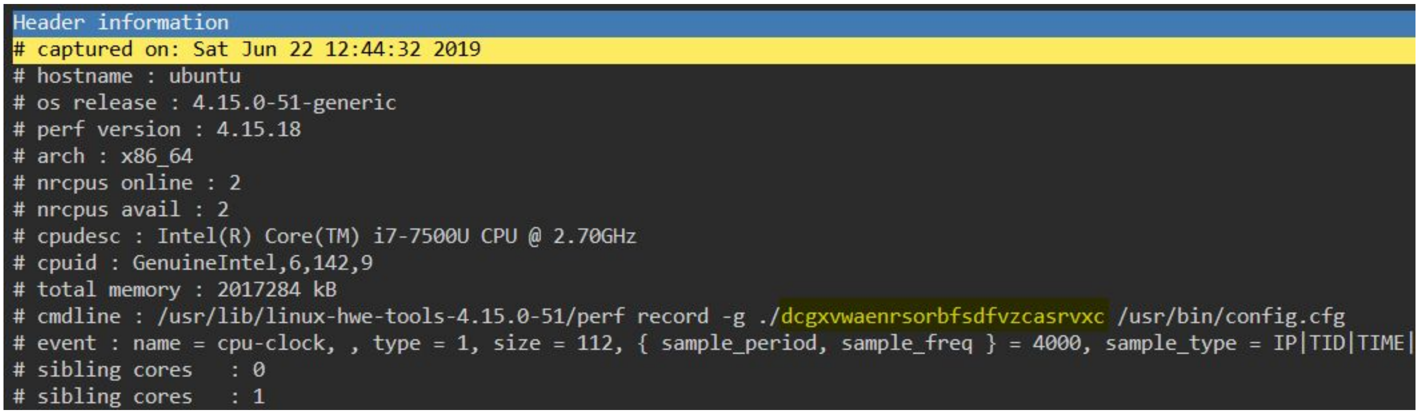
Solution:

Command: perf report



```
Samples: 19K of event 'cpu-clock', Event count (approx.): 4968250000
  Children      Self  Command          Shared Object              Symbol
+   63.46%     0.00%  dcgxvwaenrsorbf  [kernel.kallsyms]          [k] 0xffffffffb8875e0e
+   63.45%     0.01%  dcgxvwaenrsorbf  [kernel.kallsyms]          [k] 0xffffffffb92015e5
+   61.70%     2.34%  dcgxvwaenrsorbf  libc-2.23.so               [.] 0x000000000014e156
+   60.19%     0.00%  dcgxvwaenrsorbf  [kernel.kallsyms]          [k] 0xffffffffb8875b40
+   59.85%     0.00%  dcgxvwaenrsorbf  [kernel.kallsyms]          [k] 0xffffffffb8a138cc
+   54.28%     0.00%  dcgxvwaenrsorbf  [kernel.kallsyms]          [k] 0xffffffffb8a13476
+   54.21%     0.01%  dcgxvwaenrsorbf  [kernel.kallsyms]          [k] 0xffffffffb8a3e988
+   32.98%    32.86%  dcgxvwaenrsorbf  [kernel.kallsyms]          [k] 0xffffffffb9191a62
+   31.55%     0.00%  dcgxvwaenrsorbf  [kernel.kallsyms]          [k] 0xffffffffb89dcf2b
+   25.27%     0.00%  dcgxvwaenrsorbf  [kernel.kallsyms]          [k] 0xffffffffb9200081
+   24.15%     0.00%  dcgxvwaenrsorbf  [unknown]                  [.] 0x0000000000934320
+   23.97%     0.01%  dcgxvwaenrsorbf  [kernel.kallsyms]          [k] 0xffffffffb8803b53
+   22.46%     0.00%  dcgxvwaenrsorbf  [kernel.kallsyms]          [k] 0xffffffffb89dd095
+   18.05%     0.00%  dcgxvwaenrsorbf  [kernel.kallsyms]          [k] 0xffffffffb89dc366
+   18.05%     0.00%  dcgxvwaenrsorbf  [kernel.kallsyms]          [k] 0xffffffffb89eebf1
+   16.38%     0.00%  dcgxvwaenrsorbf  [kernel.kallsyms]          [k] 0xffffffffb89ee88e
+   11.90%     0.33%  dcgxvwaenrsorbf  libc-2.23.so               [.] 0x00000000000fb730
+   11.35%     0.00%  dcgxvwaenrsorbf  [kernel.kallsyms]          [k] 0xffffffffb89ee571
+   11.07%     0.34%  dcgxvwaenrsorbf  libpthread-2.23.so         [.] 0x000000000001081d
+   10.48%     0.00%  dcgxvwaenrsorbf  [kernel.kallsyms]          [k] 0xffffffffb8a939c1
+   10.05%     0.00%  dcgxvwaenrsorbf  [kernel.kallsyms]          [k] 0xffffffffb90382ae
+    9.89%     0.01%  dcgxvwaenrsorbf  [kernel.kallsyms]          [k] 0xffffffffb9036334
+    9.21%     0.00%  dcgxvwaenrsorbf  [kernel.kallsyms]          [k] 0xffffffffb90360f3
```

Press 'i' to get the header information.



```
Header information
# captured on: Sat Jun 22 12:44:32 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 ./dcgxvwaenrsorbfsdfvzcasrvxc /usr/bin/config.cfg
# event : name = cpu-clock, , type = 1, size = 112, { sample_period, sample_freq } = 4000, sample_type = IP|TID|TIME|
# sibling cores   : 0
# sibling cores   : 1
```

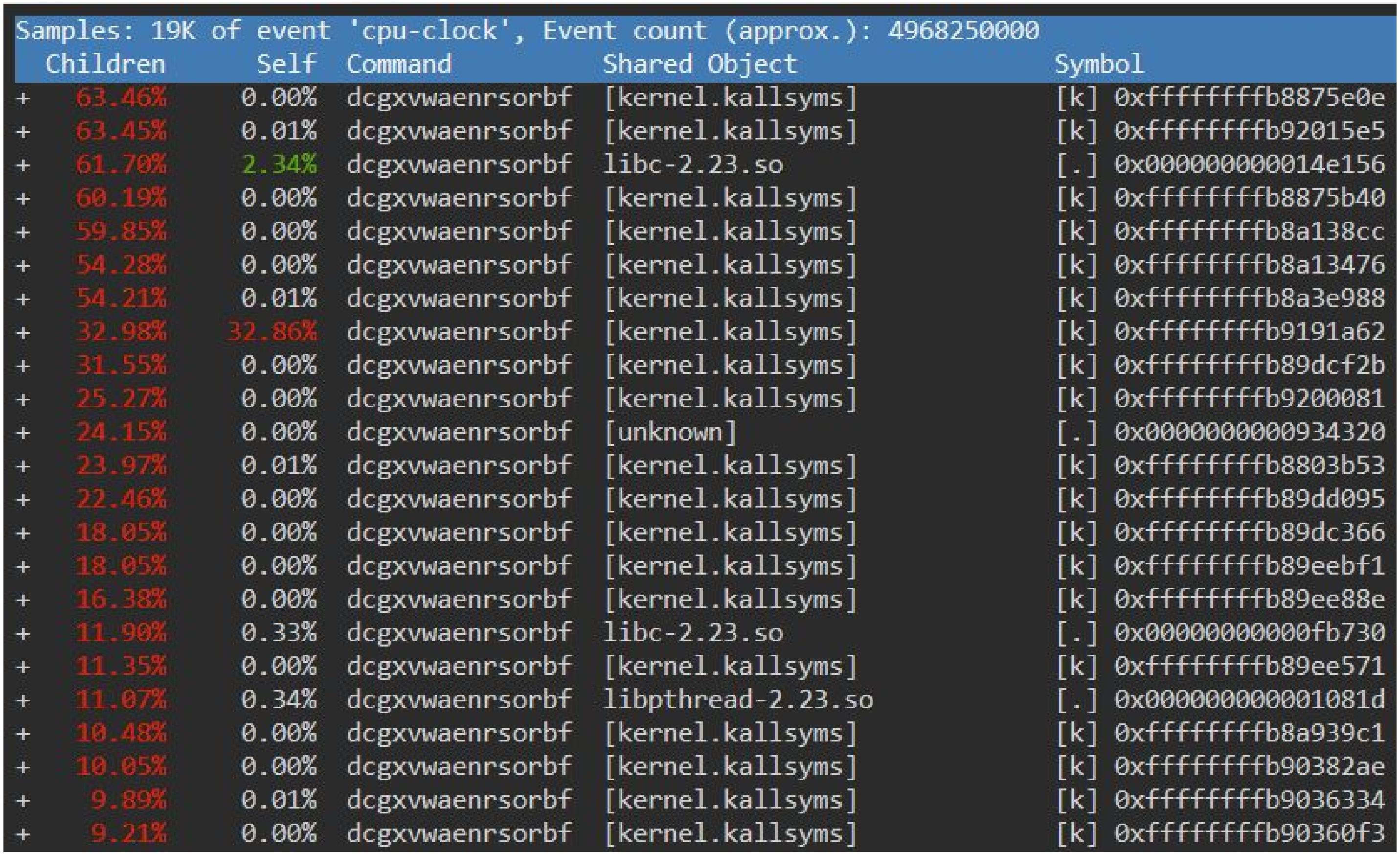
'cmdline' corresponds to the command executed when the trace was captured.

Q2. The mining service used a configuration file to connect to the pool server. Provide the complete path of the configuration file.

Answer: /usr/bin/config.cfg

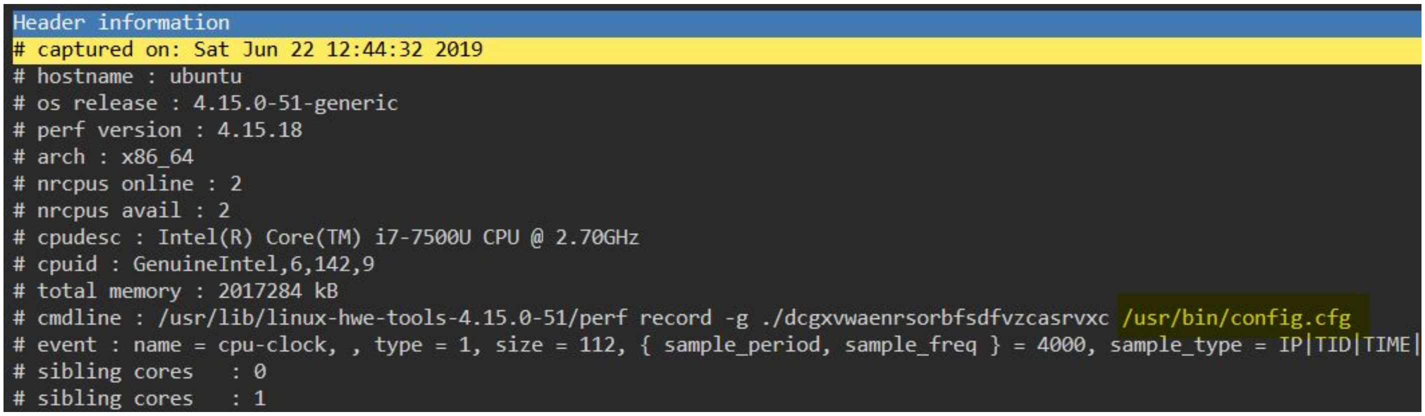
Solution:

Command: perf report



```
Samples: 19K of event 'cpu-clock', Event count (approx.): 4968250000
  Children      Self  Command          Shared Object                  Symbol
+   63.46%     0.00%  dcgxvwaenrsorbf  [kernel.kallsyms]              [k] 0xffffffffb8875e0e
+   63.45%     0.01%  dcgxvwaenrsorbf  [kernel.kallsyms]              [k] 0xffffffffb92015e5
+   61.70%     2.34%  dcgxvwaenrsorbf  libc-2.23.so                   [.] 0x000000000014e156
+   60.19%     0.00%  dcgxvwaenrsorbf  [kernel.kallsyms]              [k] 0xffffffffb8875b40
+   59.85%     0.00%  dcgxvwaenrsorbf  [kernel.kallsyms]              [k] 0xffffffffb8a138cc
+   54.28%     0.00%  dcgxvwaenrsorbf  [kernel.kallsyms]              [k] 0xffffffffb8a13476
+   54.21%     0.01%  dcgxvwaenrsorbf  [kernel.kallsyms]              [k] 0xffffffffb8a3e988
+   32.98%    32.86%  dcgxvwaenrsorbf  [kernel.kallsyms]              [k] 0xffffffffb9191a62
+   31.55%     0.00%  dcgxvwaenrsorbf  [kernel.kallsyms]              [k] 0xffffffffb89dcf2b
+   25.27%     0.00%  dcgxvwaenrsorbf  [kernel.kallsyms]              [k] 0xffffffffb9200081
+   24.15%     0.00%  dcgxvwaenrsorbf  [unknown]                      [.] 0x0000000000934320
+   23.97%     0.01%  dcgxvwaenrsorbf  [kernel.kallsyms]              [k] 0xffffffffb8803b53
+   22.46%     0.00%  dcgxvwaenrsorbf  [kernel.kallsyms]              [k] 0xffffffffb89dd095
+   18.05%     0.00%  dcgxvwaenrsorbf  [kernel.kallsyms]              [k] 0xffffffffb89dc366
+   18.05%     0.00%  dcgxvwaenrsorbf  [kernel.kallsyms]              [k] 0xffffffffb89eebf1
+   16.38%     0.00%  dcgxvwaenrsorbf  [kernel.kallsyms]              [k] 0xffffffffb89ee88e
+   11.90%     0.33%  dcgxvwaenrsorbf  libc-2.23.so                   [.] 0x00000000000fb730
+   11.35%     0.00%  dcgxvwaenrsorbf  [kernel.kallsyms]              [k] 0xffffffffb89ee571
+   11.07%     0.34%  dcgxvwaenrsorbf  libpthread-2.23.so             [.] 0x000000000001081d
+   10.48%     0.00%  dcgxvwaenrsorbf  [kernel.kallsyms]              [k] 0xffffffffb8a939c1
+   10.05%     0.00%  dcgxvwaenrsorbf  [kernel.kallsyms]              [k] 0xffffffffb90382ae
+    9.89%     0.01%  dcgxvwaenrsorbf  [kernel.kallsyms]              [k] 0xffffffffb9036334
+    9.21%     0.00%  dcgxvwaenrsorbf  [kernel.kallsyms]              [k] 0xffffffffb90360f3
```

Press 'i' to get the header information.



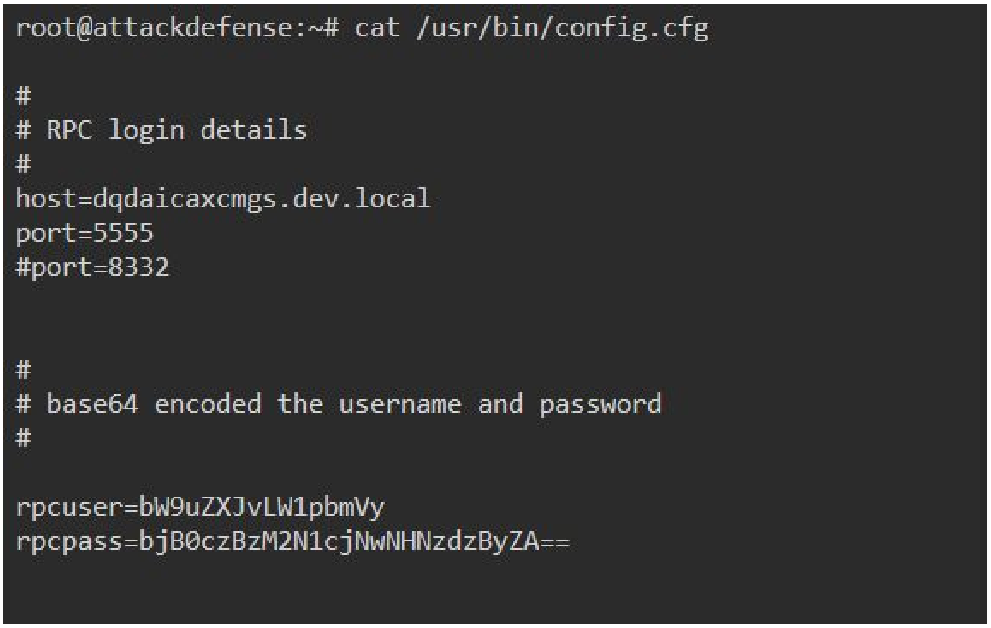
```
Header information
# captured on: Sat Jun 22 12:44:32 2019
# hostname : ubuntu
# os release : 4.15.0-51-generic
# perf version : 4.15.18
# arch : x86_64
# nrcpus online : 2
# nrcpus avail : 2
# cpudesc : Intel(R) Core(TM) i7-7500U CPU @ 2.70GHz
# cpuid : GenuineIntel,6,142,9
# total memory : 2017284 kB
# cmdline : /usr/lib/linux-hwe-tools-4.15.0-51/perf record -g ./dcgxvwaenrsorbfsdfvzcasrvxc /usr/bin/config.cfg
# event : name = cpu-clock, , type = 1, size = 112, { sample_period, sample_freq } = 4000, sample_type = IP|TID|TIME|
# sibling cores   : 0
# sibling cores   : 1
```

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

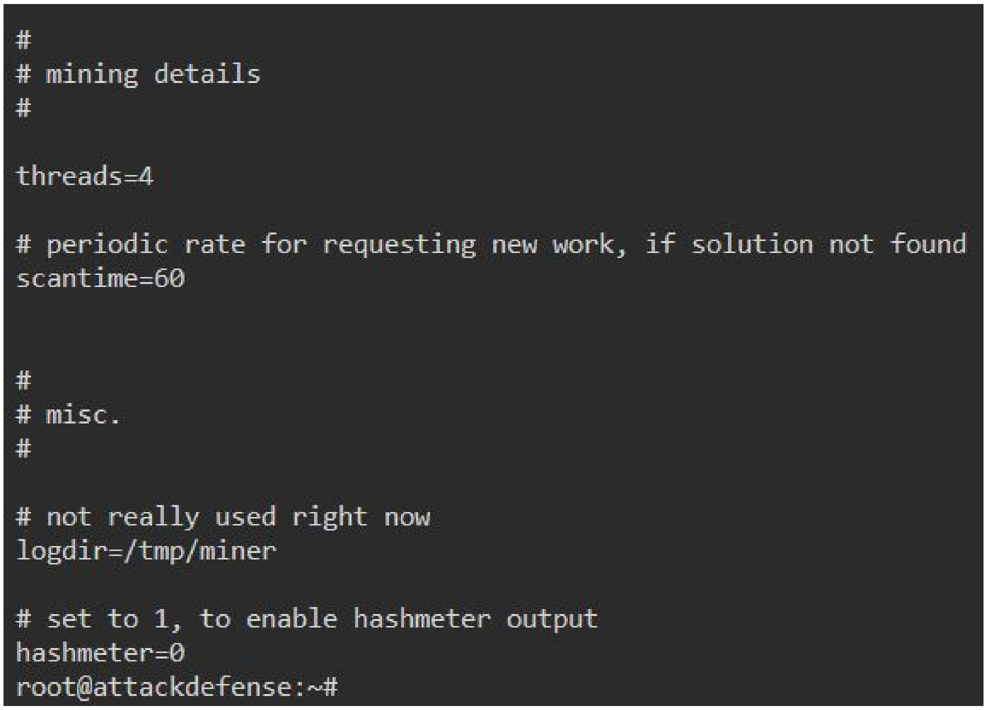
Q3. Retrieve the plain-text password used by the service to connect to the pool server.

Answer: n0ts0s3cur3p4ssw0rd

Command: cat /usr/bin/config.cfg



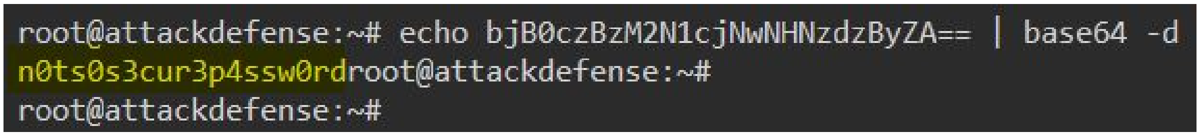
```
root@attackdefense:~# cat /usr/bin/config.cfg

#
# RPC login details
#
host=dqdaicaxcmgs.dev.local
port=5555
#port=8332


#
# base64 encoded the username and password
#

rpcuser=bW9uZXJvLW1pbmVy
rpcpass=bjB0czBzM2N1cjNwNHNzdzByZA==
```



```
#
# mining details
#

threads=4

# periodic rate for requesting new work, if solution not found
scantime=60


#
# misc.
#

# not really used right now
logdir=/tmp/miner

# set to 1, to enable hashmeter output
hashmeter=0
root@attackdefense:~#
```

The password is base64 encoded: bjB0czBzM2N1cjNwNHNzdzByZA==

Command: echo bjB0czBzM2N1cjNwNHNzdzByZA== | base64 -d



```
root@attackdefense:~# echo bjB0czBzM2N1cjNwNHNzdzByZA== | base64 -d
n0ts0s3cur3p4ssw0rdroot@attackdefense:~#
root@attackdefense:~#
```

References:

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