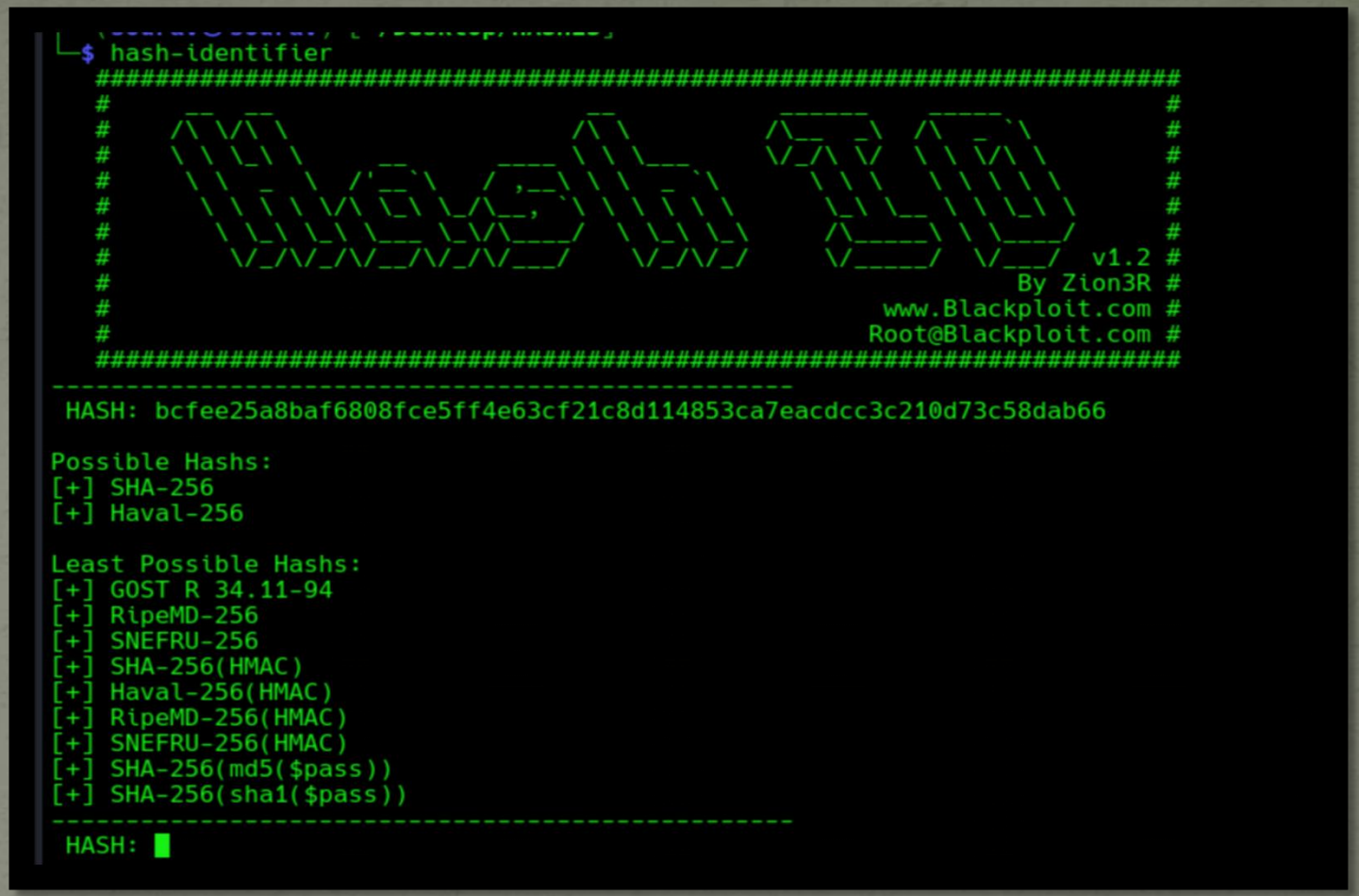
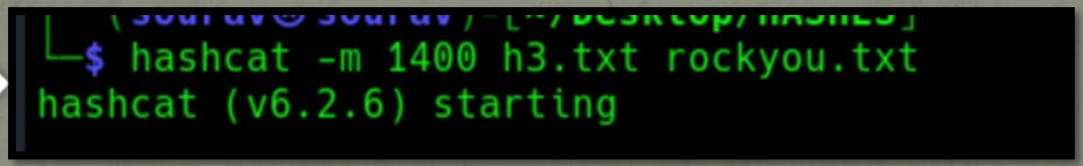
CRACKING HASHES USING HASHCAT

STEP 1

Using hash-identifier to check for possible hash-types. If the possible ones don't work , do checkout the least possible ones as well.



STEP 2



STEP 3

The hash has been cracked and the password is EARTH. We has cracked the hash using the SHA2-256 Algorithm and the rockyou.txt wordlist

```
ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache hit:
* Filename..: rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace..: 14344384

bcfee25a8baf6808fce5ff4e63cf21c8d114853ca7eacdcc3c210d73c58dab66:EARTH

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1400 (SHA2-256)
Hash.Target......: bcfee25a8baf6808fce5ff4e63cf21c8d114853ca7eacdcc3c2...8dab66
Time.Started.....: Sun Jul 21 19:34:03 2024 (4 secs)
Time.Estimated...: Sun Jul 21 19:34:07 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1676.0 kH/s (0.20ms) @ Accel:256 Loops:1 Thr:1 Vec:4
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 2144256/14344384 (14.95%)
Rejected.........: 0/2144256 (0.00%)
Restore.Point....: 2143744/14344384 (14.94%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: ELNENE16 -> E:A:E:W:
Hardware.Mon.#1..: Util: 18%

Started: Sun Jul 21 19:33:42 2024
Stopped: Sun Jul 21 19:34:08 2024
```