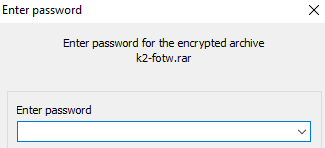
To demo some more of Rook's capabilities, I will show how to crack RAR passwords using [hashcat](https://hashcat.net/hashcat/).

**Crack RAR Passwords - Introduction**

If you didn't see my [last post](https://www.doyler.net/security-not-included/aws-password-cracking-rook), I have been using Rook for cloud password cracking.

While cleaning up my [new NAS](https://www.doyler.net/security-not-included/enable-shr-on-synology-ds3615xs), I came across a password protected RAR archive.

[](https://www.doyler.net/wp-content/uploads/crackRar/crackRar-2-protected.png)

This was likely only a video file related to my old [Day of Defeat](https://store.steampowered.com/app/30/Day_of_Defeat/) team, but I still wanted to check.

After a little bit of [research](https://hashcat.net/forum/thread-7716.html), I found a technique for obtaining and cracking these hashes using hashcat.

**Obtaining the Hash**

First, I used [rar2john](https://github.com/magnumripper/JohnTheRipper/blob/bleeding-jumbo/src/rar2john.c) to extract the password hash from the archive. Note that this is the un-redacted hash, so feel free to follow along at home!

root@kali:~/tools/johntheripper/run# ./rar2john ~/k2-fotw.rar

k2-fotw.rar:$RAR3$\*0\*e4d0bb299b3105fc\*fab80e0d0a16cbd86624af6e5333cabc:0::::/root/k2-fotw.rar

**Crack RAR Passwords - Rook Time**

With the hashes in hand, it was time to kick off [Rook](https://github.com/JumpsecLabs/Rook).

ubuntu@ip-1-2-3-4:~/tools/Rook$ python rook.py -t p3.16xlarge -f /home/ubuntu/hashes/k2.txt -m 12500 -i rook-crackingPrivate -s /home/ubuntu/.ssh/rook-crackingPrivate.pem --spot 9.07 --debug

██████╗ ██████╗ ██████╗ ██╗ ██╗

██╔══██╗██╔═══██╗██╔═══██╗██║ ██╔╝

██████╔╝██║ ██║██║ ██║█████╔╝

██╔══██╗██║ ██║██║ ██║██╔═██╗

██║ ██║╚██████╔╝╚██████╔╝██║ ██╗

╚═╝ ╚═╝ ╚═════╝ ╚═════╝ ╚═╝ ╚═╝

Terraform AWS instances for cracking hashes

[+] Bidding for spot instance at max price of 9.07.

[+] Creating Rook instance to crack passwords with an AWS p3.16xlarge instance. Please wait...

./terraform apply -var=identity=rook-crackingPrivate -var=hashmode=12500 -var=itype=p3.16xlarge -var=sshkeyfile=/home/ubuntu/.ssh/rook-crackingPrivate.pem -var=spotprice=9.07

data.http.myip: Refreshing state...

aws\_security\_group.rook\_security: Refreshing state... [id=sg-05c397e759c25050c]

aws\_spot\_instance\_request.rook-spot: Refreshing state... [id=sir-y9gg98dp]

null\_resource.local: Refreshing state... [id=4350831823518840210]

...

aws\_spot\_instance\_request.rook-spot (remote-exec): nohup: appending output to '/home/ubuntu/nohup.out'

aws\_spot\_instance\_request.rook-spot: Creation complete after 4m19s [id=sir-jfmi96fq]

Apply complete! Resources: 1 added, 0 changed, 0 destroyed.

After Rook created my interface, I connected to it to check the status.

ubuntu@ip-1-2-3-4:~/tools/Rook$ ssh -i ~/.ssh/rook-crackingPrivate.pem ubuntu@5.6.7.8

The authenticity of host '5.6.7.8 (5.6.7.8)' can't be established.

ECDSA key fingerprint is SHA256:LvvA+Fdfnoe4FokT7m6WTDjZlQNx0JwI+WwjRb+qdMQ.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '5.6.7.8' (ECDSA) to the list of known hosts.

Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-1057-aws x86\_64)

\* Documentation: https://help.ubuntu.com

\* Management: https://landscape.canonical.com

\* Support: https://ubuntu.com/advantage

System information as of Mon Apr 20 21:01:31 UTC 2020

System load: 0.24 Processes: 658

Usage of /: 26.5% of 7.69GB Users logged in: 0

Memory usage: 0% IP address for ens3: 172.31.25.122

Swap usage: 0%

0 packages can be updated.

0 updates are security updates.

\*\*\* System restart required \*\*\*

Last login: Mon Apr 20 20:52:44 2020 from 9.8.7.6

ubuntu@ip-1-2-3-4:~$ sudo su -

root@ip-1-2-3-4:~# screen -r

Hashcat was successfully running, and trying about 119,000 hashes a second. This wasn't terribly fast, so I was hoping that rockyou+best64 alone would crack the hash.

hashcat (v5.1.0) starting...

OpenCL Platform #1: NVIDIA Corporation

======================================

\* Device #1: Tesla V100-SXM2-16GB, 4032/16130 MB allocatable, 80MCU

\* Device #2: Tesla V100-SXM2-16GB, 4032/16130 MB allocatable, 80MCU

... <snip> ...

Session..........: hashcat

Status...........: Running

Hash.Type........: RAR3-hp

Hash.Target......: $RAR3$\*0\*e4d0bb299b3105fc\*fab80e0d0a16cbd86624af6e5333cabc

Time.Started.....: Thu Apr 23 21:14:03 2020 (34 mins, 33 secs)

Time.Estimated...: Thu Apr 23 23:46:50 2020 (1 hour, 58 mins)

Guess.Base.......: File (/words/rockyou.txt)

Guess.Mod........: Rules (/words/best64.rule)

Guess.Queue......: 1/3 (33.33%)

Speed.#1.........: 14658 H/s (15.50ms) @ Accel:1 Loops:16384 Thr:64 Vec:1

Speed.#2.........: 14870 H/s (15.36ms) @ Accel:1 Loops:16384 Thr:64 Vec:1

Speed.#3.........: 14910 H/s (23.99ms) @ Accel:1 Loops:16384 Thr:64 Vec:1

Speed.#4.........: 14984 H/s (9.73ms) @ Accel:1 Loops:16384 Thr:64 Vec:1

Speed.#5.........: 14913 H/s (19.62ms) @ Accel:1 Loops:16384 Thr:64 Vec:1

Speed.#6.........: 14870 H/s (24.80ms) @ Accel:1 Loops:16384 Thr:64 Vec:1

Speed.#7.........: 14740 H/s (21.83ms) @ Accel:1 Loops:16384 Thr:64 Vec:1

Speed.#8.........: 14997 H/s (24.95ms) @ Accel:1 Loops:16384 Thr:64 Vec:1

Speed.#\*.........: 118.9 kH/s

Recovered........: 0/1 (0.00%) Digests, 0/1 (0.00%) Salts

Progress.........: 260633600/1104517568 (23.60%)

Rejected.........: 0/260633600 (0.00%)

Restore.Point....: 3333120/14344384 (23.24%)

Restore.Sub.#1...: Salt:0 Amplifier:34-35 Iteration:114688-131072

Restore.Sub.#2...: Salt:0 Amplifier:43-44 Iteration:98304-114688

Restore.Sub.#3...: Salt:0 Amplifier:8-9 Iteration:245760-262144

Restore.Sub.#4...: Salt:0 Amplifier:0-1 Iteration:180224-196608

Restore.Sub.#5...: Salt:0 Amplifier:57-58 Iteration:245760-262144

Restore.Sub.#6...: Salt:0 Amplifier:34-35 Iteration:163840-180224

Restore.Sub.#7...: Salt:0 Amplifier:61-62 Iteration:180224-196608

Restore.Sub.#8...: Salt:0 Amplifier:10-11 Iteration:245760-262144

Candidates.#1....: japd -> fanj

Candidates.#2....: Taghiyev -> Tacnolu

Candidates.#3....: tak13974 -> taghiz14

Candidates.#4....: tacnoje -> ta0075

Candidates.#5....: tna -> tmf

Candidates.#6....: tamie -> talitie

Candidates.#7....: nanjazo -> kana

Candidates.#8....: talitoto6 -> tak13umis6

Hardware.Mon.#1..: Temp: 61c Util: 98% Core:1530MHz Mem: 877MHz Bus:16

Hardware.Mon.#2..: Temp: 56c Util: 96% Core:1530MHz Mem: 877MHz Bus:16

Hardware.Mon.#3..: Temp: 53c Util: 95% Core:1530MHz Mem: 877MHz Bus:16

Hardware.Mon.#4..: Temp: 61c Util: 78% Core:1530MHz Mem: 877MHz Bus:16

Hardware.Mon.#5..: Temp: 60c Util: 96% Core:1530MHz Mem: 877MHz Bus:16

Hardware.Mon.#6..: Temp: 53c Util: 96% Core:1530MHz Mem: 877MHz Bus:16

Hardware.Mon.#7..: Temp: 55c Util: 96% Core:1530MHz Mem: 877MHz Bus:16

Hardware.Mon.#8..: Temp: 59c Util: 97% Core:1530MHz Mem: 877MHz Bus:16

After just over an hour, hashcat said that it had cracked my hash!

Session..........: hashcat

Status...........: Cracked

Hash.Type........: RAR3-hp

Hash.Target......: $RAR3$\*0\*e4d0bb299b3105fc\*fab80e0d0a16cbd86624af6e5333cabc

Time.Started.....: Thu Apr 23 21:14:03 2020 (1 hour, 4 mins)

Time.Estimated...: Thu Apr 23 22:18:27 2020 (0 secs)

Guess.Base.......: File (/words/rockyou.txt)

Guess.Mod........: Rules (/words/best64.rule)

Guess.Queue......: 1/3 (33.33%)

Speed.#1.........: 14338 H/s (25.05ms) @ Accel:1 Loops:16384 Thr:64 Vec:1

Speed.#2.........: 14567 H/s (25.52ms) @ Accel:1 Loops:16384 Thr:64 Vec:1

Speed.#3.........: 14531 H/s (24.86ms) @ Accel:1 Loops:16384 Thr:64 Vec:1

Speed.#4.........: 14546 H/s (11.86ms) @ Accel:1 Loops:16384 Thr:64 Vec:1

Speed.#5.........: 14452 H/s (25.65ms) @ Accel:1 Loops:16384 Thr:64 Vec:1

Speed.#6.........: 14453 H/s (25.54ms) @ Accel:1 Loops:16384 Thr:64 Vec:1

Speed.#7.........: 14424 H/s (23.82ms) @ Accel:1 Loops:16384 Thr:64 Vec:1

Speed.#8.........: 14553 H/s (24.12ms) @ Accel:1 Loops:16384 Thr:64 Vec:1

Speed.#\*.........: 115.9 kH/s

Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts

Progress.........: 468254720/1104517568 (42.39%)

Rejected.........: 0/468254720 (0.00%)

Restore.Point....: 6036480/14344384 (42.08%)

Restore.Sub.#1...: Salt:0 Amplifier:11-12 Iteration:32768-49152

Restore.Sub.#2...: Salt:0 Amplifier:18-19 Iteration:81920-98304

Restore.Sub.#3...: Salt:0 Amplifier:8-9 Iteration:163840-180224

Restore.Sub.#4...: Salt:0 Amplifier:1-2 Iteration:245760-262144

Restore.Sub.#5...: Salt:0 Amplifier:34-35 Iteration:229376-245760

Restore.Sub.#6...: Salt:0 Amplifier:14-15 Iteration:180224-196608

Restore.Sub.#7...: Salt:0 Amplifier:40-41 Iteration:81920-98304

Restore.Sub.#8...: Salt:0 Amplifier:7-8 Iteration:196608-212992

Candidates.#1....: loosa017 -> longbone17

Candidates.#2....: lorryhat12 -> lore10012

Candidates.#3....: longbob14 -> loloart4

Candidates.#4....: 5248alol -> onairosesiol

Candidates.#5....: lostnureyie -> lorryjeie

Candidates.#6....: lore091000 -> loosa10100

Candidates.#7....: 1louise1717 -> 1lostnurice

Candidates.#8....: loloarseny63 -> lola84843

Hardware.Mon.#1..: Temp: 60c Util: 95% Core:1530MHz Mem: 877MHz Bus:16

Hardware.Mon.#2..: Temp: 56c Util: 96% Core:1530MHz Mem: 877MHz Bus:16

Hardware.Mon.#4..: Temp: 60c Util: 71% Core:1530MHz Mem: 877MHz Bus:16

Hardware.Mon.#5..: Temp: 60c Util: 96% Core:1530MHz Mem: 877MHz Bus:16

Hardware.Mon.#6..: Temp: 53c Util: 97% Core:1530MHz Mem: 877MHz Bus:16

Hardware.Mon.#7..: Temp: 55c Util: 51% Core:1530MHz Mem: 877MHz Bus:16

Hardware.Mon.#8..: Temp: 58c Util: 96% Core:1530MHz Mem: 877MHz Bus:16

Started: Thu Apr 23 21:12:55 2020

Stopped: Thu Apr 23 22:18:29 2020

**Verifying the Hash**

When hashcat finished running, I checked the output in the potfile.

root@ip-1-2-3-4:/opt/hashcat-5.1.0# cat hashcat.potfile

$RAR3$\*0\*e4d0bb299b3105fc\*fab80e0d0a16cbd86624af6e5333cabc:k2lol

This hash seemed reasonable based on the archive, my team, and past passwords.

With a potential password in hand, it was time to extract the archive!

root@kali:/root# 7z e k2-fotw.rar -pk2lol

7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21

p7zip Version 16.02 (locale=utf8,Utf16=on,HugeFiles=on,64 bits,16 CPUs x64)

Scanning the drive for archives:

1 file, 122179324 bytes (117 MiB)

Extracting archive: k2-fotw.rar

--

Path = k2-fotw.rar

Type = Rar

Physical Size = 122179324

Characteristics = BlockEncryption

Solid = -

Blocks = 666

Multivolume = -

Volumes = 1

Would you like to replace the existing file:

Path: ./Thumbs.db

Size: 8704 bytes (9 KiB)

Modified: 2007-04-14 06:50:50

with the file from archive:

Path: doyler/Thumbs.db

Size: 435712 bytes (426 KiB)

Modified: 2007-04-14 06:29:15

? (Y)es / (N)o / (A)lways / (S)kip all / A(u)to rename all / (Q)uit? y

Everything is Ok

Folders: 3

Files: 54

Size: 125000961

Compressed: 122179324

The extraction was successful, and I was able to access my files!

It turns out that this archive just had some scoreboards, a few files that I had backed up, and one fotw (Frags of the Week) video from DoD.

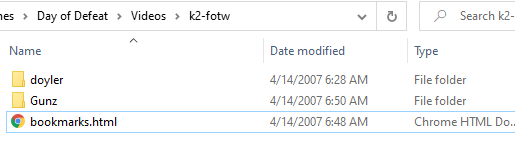
root@kali:/root/k2# ls

1.jpg 14.jpg 3.jpg 7.jpg Gunz/ k2-fotw.rar

10.jpg 15.jpg 4.jpg 8.jpg bookmarks.html k2.txt

12.jpg 16.jpg 5.jpg 9.jpg doyler/

13.jpg 2.jpg 6.jpg Emblem/ emblem.xml

[](https://www.doyler.net/wp-content/uploads/crackRar/crackRar-1-extracted.png)

**Crack RAR Passwords - Conclusion**

This was a simple example, but a great way for me to demo Rook's capabilities.

I still want to develop my own tool, but this is working great in the meantime.

Please let me know if you know of any other AWS cracking tools for me to try out. Additionally, any password cracking resources would be great, as I'm still learning!