14

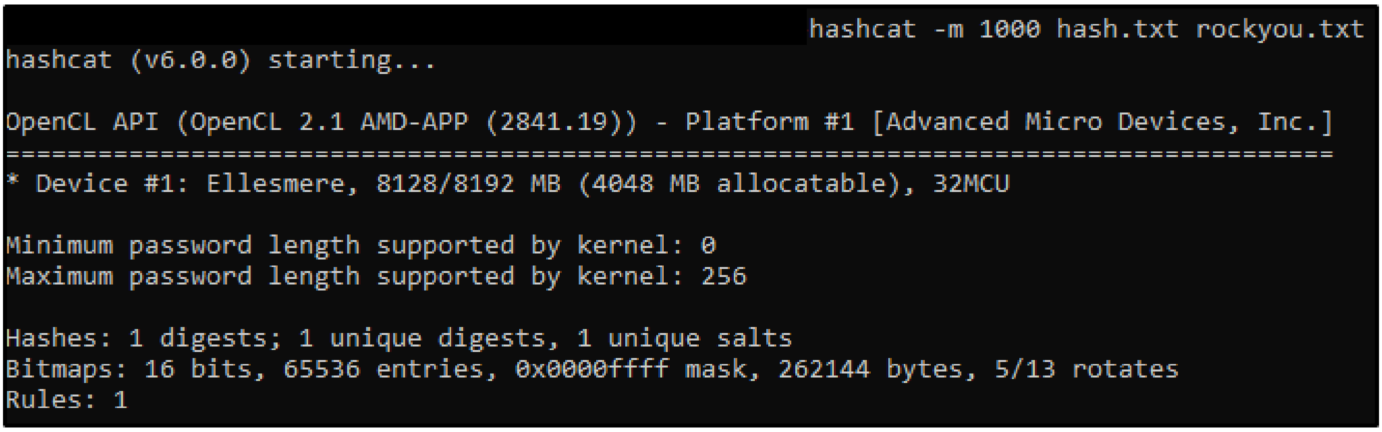
Overview of Password Cracking

Password cracking uses a password cracking tool such as Hashcat or John the Ripper along with a password wordlist such as rockyou.txt to crack a hash. Hashcat relies heavily on utilizing the GPU to crack hashes and is not recommended to be run inside of a VM. John the Ripper utilizes the CPU primarily and can be used inside of a VM.

Note: This section of the course along with other areas that use password cracking will require the use of Hashcat, if your device does not support Hashcat then you can utilize google colab to crack for you. Colabcat can be found here.

Password Hash Types
Inside of a Windows active directory environment there are 5 different types of hashes that you will commonly encounter. The first hash type is NetNTLM and NetNTLMv2 usually seen in LLMNR Poisoning attacks, the Hashcat mode for NetNTLMv2 is 5600. Another widely used hash is NTLM mainly used when dumping credentials, the Hashcat mode is 1000. When trying to identify a hash the Hashcat example hashes can help a lot, the page can be found here.

Cracking NTLM Hashes with Hashcat
1.) hashcat -m 1000 -a 0 hash.txt rockyou.txt



```
[redacted] hashcat -m 1000 hash.txt rockyou.txt
hashcat (v6.0.0) starting...

OpenCL API (OpenCL 2.1 AMD-APP (2841.19)) - Platform #1 [Advanced Micro Devices, Inc.]
=======================================================================================
* Device #1: Ellesmere, 8128/8192 MB (4048 MB allocatable), 32MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1
```

Hashcat NTLM hash command

Introduction to Rule Based Cracking

Sometimes your standard wordlist like rockyou is not enough to crack a hash. You can use a rule list to change the wordlist and add rules to it in order to crack a hash. A rule list works by having a set of rules that can append characters to a password, attach characters, and substitute words and characters.

Append Rule: appending to a word uses a $ operator before the character to append with.

Examples of Append Rule:

$1

$2

$a

Attach Rule: Attaching to a word uses a ^ operator before the character to attach with.

Examples of Attach Rule:

^1

^2

^a

Substitute Rule: Substituting a word or character uses an s, followed by the character you want to substitute, followed by the character to be substituted.

Examples of Substitute Rule:

sa@

sa4

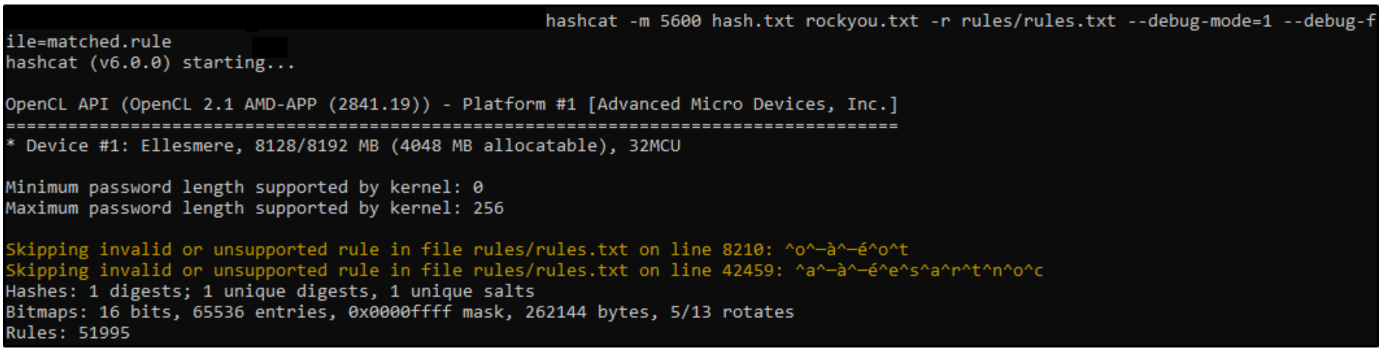
sl1

To make rule based attacks easier you can use a pre-compiled rule list. The one we will run the demo with is OneRuleToRuleThemAll, it is a large rule list that contains more 50,000 rules making it much more effective than creating your own list. The rules list can be found here

Using Rules to Conquer NetNTLMv2

Hashcat uses the -r switch to specify the use of a rules list; you can also add --debug-mode=1 and --debug-file=matched.rule to your command.

1.) hashcat -m 5600 hash.txt rockyou.txt -r rules/OneRuleToRuleThemAll.rule --debug-mode=1 --debug-file=matched.rule



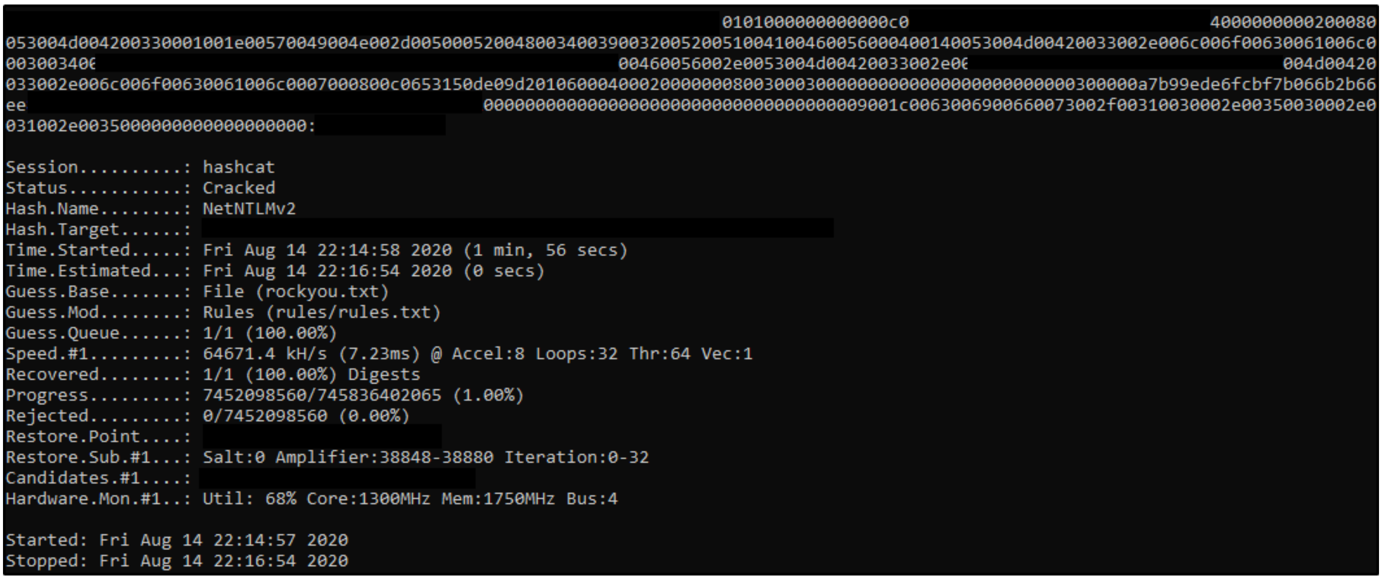
```
[redacted] hashcat -m 5600 hash.txt rockyou.txt -r rules/rules.txt --debug-mode=1 --debug-f
ile=matched.rule [redacted]
hashcat (v6.0.0) starting...

OpenCL API (OpenCL 2.1 AMD-APP (2841.19)) - Platform #1 [Advanced Micro Devices, Inc.]
======================================================================================
* Device #1: Ellesmere, 8128/8192 MB (4048 MB allocatable), 32MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Skipping invalid or unsupported rule in file rules/rules.txt on line 8210: ^o^—à^—é^o^t
Skipping invalid or unsupported rule in file rules/rules.txt on line 42459: ^a^—à^—é^e^s^a^r^t^n^o^c
Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 51995
```

Hashcat command with a rules list



```
[redacted] 0101000000000000c0 [redacted] 4000000000200080
053004d004200330001001e00570049004e002d0050005200480034003900320052005100410046005600040014005300 4d00420033002e006c006f00630061006c0
00300340[redacted] 00460056002e0053004d00420033002e0[redacted] 004d00420
033002e006c006f00630061006c0007000800c0653150de09d201060004000200000008003000300000000000000000000000000300000a7b99ede6fcbf7b066b2b66
ee [redacted] 000000000000000000000000000000000000009001c006300690066007300 2f00310030002e00350030002e0
031002e0035000000000000000000:[redacted]

Session..........: hashcat
Status...........: Cracked
Hash.Name........: NetNTLMv2
Hash.Target......: [redacted]
Time.Started.....: Fri Aug 14 22:14:58 2020 (1 min, 56 secs)
Time.Estimated...: Fri Aug 14 22:16:54 2020 (0 secs)
Guess.Base.......: File (rockyou.txt)
Guess.Mod........: Rules (rules/rules.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........: 64671.4 kH/s (7.23ms) @ Accel:8 Loops:32 Thr:64 Vec:1
Recovered........: 1/1 (100.00%) Digests
Progress.........: 7452098560/745836402065 (1.00%)
Rejected.........: 0/7452098560 (0.00%)
Restore.Point....: [redacted]
Restore.Sub.#1...: Salt:0 Amplifier:38848-38880 Iteration:0-32
Candidates.#1....: [redacted]
Hardware.Mon.#1..: Util: 68% Core:1300MHz Mem:1750MHz Bus:4

Started: Fri Aug 14 22:14:57 2020
Stopped: Fri Aug 14 22:16:54 2020
```

Hashcat cracked password with a rules list

Now that you know how to crack a password using a wordlist as well as a rule list, practice password cracking on the NTLM hash from Task 10 as well as the NetNTLMv2 hash from Task 13

Answer the questions below

What is the cracked password from the pfSense hash?

Correct Answer

What is the cracked password from LLMNR poisoning?

Correct Answer