Name-Gavade Vishal Ramnath

Roll.No-70

Batch-T3

Class-TY

1. Password Cracking Using John the Ripper

```
┌──(vishalgavade6621㉿kali)-[~]
└─$ sudo apt-get install john
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
john is already the newest version (1.9.0-Jumbo-1+git20211102-0kali5).
john set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.

┌──(vishalgavade6621㉿kali)-[~]
└─$ ls
Desktop    Downloads  Pictures  Templates
Documents  Music      Public    Videos

┌──(vishalgavade6621㉿kali)-[~]
└─$ cd Desktop

┌──(vishalgavade6621㉿kali)-[~/Desktop]
└─$ ls
'Linux Basic Commands.txt'   file1.txt   file1.txt.zip   file2.txt

┌──(vishalgavade6621㉿kali)-[~/Desktop]
└─$ zip2john file1.txt.zip >file2.txt
Created directory: /home/vishalgavade6621/.john
```

!? compressed length of AES entry too short.

┌──(vishalgavade6621㉿kali)-[~/Desktop]

└─$ john file2.txt

Using default input encoding: UTF-8

Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 128/128 SSE2 4x])

Cost 1 (HMAC size) is 0 for all loaded hashes

Will run 2 OpenMP threads

Proceeding with single, rules:Single

Press 'q' or Ctrl-C to abort, almost any other key for status

Almost done: Processing the remaining buffered candidate passwords, if any.

Proceeding with wordlist:/usr/share/john/password.lst

123456 (file1.txt.zip/file1.txt)

1g 0:00:00:01 DONE 2/3 (2024-04-22 04:19) 0.8333g/s 20816p/s 20816c/s 20816C/s 123456..222222

Use the "--show" option to display all of the cracked passwords reliably

Session completed.

---

2. Password Cracking Using MD5 and SHA Algorithm

┌──(vishalgavade6621㉿kali)-[~/Desktop]

└─$ john md5.txt --format=RAW-MD5

Using default input encoding: UTF-8

Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4x3])

Warning: no OpenMP support for this hash type, consider --fork=2

Proceeding with single, rules:Single

Press 'q' or Ctrl-C to abort, almost any other key for status

Almost done: Processing the remaining buffered candidate passwords, if any.

Proceeding with wordlist:/usr/share/john/password.lst

Proceeding with incremental:ASCII

vishal (?)

1g 0:00:00:35 DONE 3/3 (2024-04-22 04:29) 0.02828g/s 46077Kp/s 46077Kc/s 46077KC/s visst7..vishon

Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably

Session completed.

3. Password Cracking Using Shadow File

┌──(kali㉿kali)-[~]

└─$ sudo su

[sudo] password for kali:

┌──(root㉿kali)-[/home/kali]

└─# sudo useradd sai

┌──(root㉿kali)-[/home/kali]

└─# sudo passwd sai

New password:

Retype new password:

passwd: password updated successfully

┌──(root㉿kali)-[/home/kali]

└─# sudo cat/etc/shadow

sudo: cat/etc/shadow: command not found

┌──(root㉿kali)-[/home/kali]

└─# sudo cat /etc/shadow

root:*:19778:0:99999:7:::

daemon:*:19778:0:99999:7:::

bin:*:19778:0:99999:7:::

sys:*:19778:0:99999:7:::

sync:*:19778:0:99999:7:::

games:*:19778:0:99999:7:::

man:*:19778:0:99999:7:::

lp:*:19778:0:99999:7:::

mail:*:19778:0:99999:7:::

news:*:19778:0:99999:7:::

uucp:*:19778:0:99999:7:::

proxy:*:19778:0:99999:7:::

www-data:*:19778:0:99999:7:::

backup:*:19778:0:99999:7:::

list:*:19778:0:99999:7:::

irc:*:19778:0:99999:7:::

_apt:*:19778:0:99999:7:::

nobody:*:19778:0:99999:7:::

systemd-network:!*:19778::::::

systemd-timesync:!*:19778::::::

messagebus:!:19778::::::

tss:!:19778::::::

strongswan:!:19778::::::

tcpdump:!:19778::::::

usbmux:!:19778::::::

sshd:!:19778::::::

dnsmasq:!:19778::::::

avahi:!:19778::::::

speech-dispatcher:!:19778::::::

pulse:!:19778::::::

lightdm:!:19778::::::

saned:!:19778::::::

polkitd:!*:19778::::::

rtkit:!:19778::::::

colord:!:19778::::::

nm-openvpn:!:19778::::::

nm-openconnect:!:19778::::::

_galera:!:19778::::::

mysql:!:19778::::::

stunnel4:!*:19778::::::

_rpc:!:19778::::::

geoclue:!:19778::::::

Debian-snmp:!:19778::::::

sslh:!:19778::::::

ntpsec:!:19778::::::

redsocks:!:19778::::::

rwhod:!:19778::::::

_gophish:!:19778::::::

iodine:!:19778::::::

miredo:!:19778::::::

statd:!:19778::::::

redis:!:19778::::::

postgres:!:19778::::::

mosquitto:!:19778::::::

inetsim:!:19778::::::

_gvm:!:19778::::::

kali:yj9T$hW9K52EOJBFsViQ7HRz370$//6l5BWkvHl3PTkK6qgZhGFTLOFKR/zVCEwjlZIwAq0:19778:0:99999:7:::

_dvwa:!:19828::::::

sai:yj9T$dK7H25xb7Sg2bih97p.DM1$AwoMqLDxO0S7vgVI8uSIEbL9bTKr4LeHJ29Qn2sOHF5:19835:0:99999:7:::

┌──(root㉿kali)-[/home/kali]

└─# john --format=crypt /etc/shadow

Created directory: /root/.john

Using default input encoding: UTF-8

Loaded 2 password hashes with 2 different salts (crypt, generic crypt(3) [?/64])

Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 for all loaded hashes

Cost 2 (algorithm specific iterations) is 1 for all loaded hashes

Will run 4 OpenMP threads

Proceeding with single, rules:Single

Press 'q' or Ctrl-C to abort, almost any other key for status

kali (kali)

Almost done: Processing the remaining buffered candidate passwords, if any.

Proceeding with wordlist:/usr/share/john/password.lst

123456 (sai)

2g 0:00:00:22 DONE 2/3 (2024-04-22 04:46) 0.08928g/s 144.8p/s 144.9c/s 144.9C/s 123456..pepper

Use the "--show" option to display all of the cracked passwords reliably

Session completed.