



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Academic Year: 2025-26

Semester: V

Class / Branch/ Div: TEIT-C

Subject: Security Lab

Name of Student: Suyash Y Mane

Student ID: 24204008

Roll No. 10

Date of Submission: 14/08/2025

Experiment No: 11

Aim: To study password cracking using John the ripper.

Outputs:

```
apsit@apsit-HP-ProDesk-600-G4-PCI-MT:~/Downloads/Suyash$ sudo apt-get install john
[sudo] password for apsit:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  bridge-utils libllvm17t64 linux-headers-6.8.0-45 linux-headers-6.8.0-45-generic linux-image-6.8.0-45-generic linux-modules-6.8.0-45-generic
  linux-modules-extra-6.8.0-45-generic linux-tools-6.8.0-45 linux-tools-6.8.0-45-generic python3-netifaces ubuntu-fan
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  john-data
The following NEW packages will be installed:
  john john-data
0 upgraded, 2 newly installed, 0 to remove and 33 not upgraded.
Need to get 9,351 kB of archives.
After this operation, 20.6 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://archive.ubuntu.com/ubuntu noble/main amd64 john-data all 1.9.0-2build1 [9,141 kB]
Get:2 http://archive.ubuntu.com/ubuntu noble/main amd64 john amd64 1.9.0-2build1 [210 kB]
Fetched 9,351 kB in 8s (1,216 kB/s)
Selecting previously unselected package john-data.
(Reading database ... 334837 files and directories currently installed.)
Preparing to unpack .../john-data_1.9.0-2build1_all.deb ...
Unpacking john-data (1.9.0-2build1) ...
Selecting previously unselected package john.
Preparing to unpack .../john_1.9.0-2build1_amd64.deb ...
Unpacking john (1.9.0-2build1) ...
Setting up john-data (1.9.0-2build1) ...
Setting up john (1.9.0-2build1) ...
Processing triggers for man-db (2.12.0-4build2) ...
```

```
apsit@apsit-HP-ProDesk-600-G4-PCI-MT:~/Downloads/Suyash$ john -test
Created directory: /home/apsit/.john
Will run 12 OpenMP threads
Benchmarking: descript, traditional crypt(3) [DES 128/128 SSE2]... DONE
Many salts: 42598K c/s real, 3565K c/s virtual
Only one salt: 23917K c/s real, 2059K c/s virtual

Benchmarking: bsdicrypt, BSDI crypt(3) ("_J9..", 725 iterations) [DES 128/128 SSE2]... DONE
Many salts: 1114K c/s real, 95111 c/s virtual
Only one salt: 752364 c/s real, 66820 c/s virtual

Benchmarking: md5crypt [MD5 32/64 X2]... DONE
Raw: 109977 c/s real, 10016 c/s virtual

Benchmarking: bcrypt ("S2as05", 32 iterations) [Blowfish 32/64 X3]... DONE
Raw: 6337 c/s real, 597 c/s virtual

Benchmarking: LM [DES 128/128 SSE2]... DONE
Raw: 86999K c/s real, 7499K c/s virtual

Benchmarking: AFS, Kerberos AFS [DES 48/64 4K]... DONE
Short: 678400 c/s real, 670355 c/s virtual
Long: 3092K c/s real, 3092K c/s virtual

Benchmarking: tripcode [DES 128/128 SSE2]... DONE
Raw: 19149K c/s real, 1632K c/s virtual

Benchmarking: dummy [N/A]... DONE
Raw: 110419K c/s real, 107831K c/s virtual

Benchmarking: crypt, generic crypt(3) [7/64]... DONE
Many salts: 2171K c/s real, 182656 c/s virtual
Only one salt: 1991K c/s real, 166802 c/s virtual
```



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



```
apsit@apsit-HP-ProDesk-600-G4-PCI-MT:~/Downloads/Suyash$ sudo adduser suyash
info: Adding user `suyash' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `suyash' (1003) ...
info: Adding new user `suyash' (1003) with group `suyash (1003)' ...
info: Creating home directory `/home/suyash' ...
info: Copying files from `/etc/skel' ...
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
Changing the user information for suyash
Enter the new value, or press ENTER for the default
  Full Name []:
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:
Is the information correct? [Y/n] y
info: Adding new user `suyash' to supplemental / extra groups `users' ...
info: Adding user `suyash' to group `users' ...
```

sudo cat /etc/shadow

```
gnome-remote-desktop:!:19945:::::::
apsit:$6$FH6nMnPuNUYA0FL6$15wFmuSzgyTCLPzUDgDQNgT013eb7jw5WctdAcjn/k27kJDrftG3XioxQ7y/Br3VOTsWpybM9jHBVGtVU420a.:19945:0:99999:7:::
snapd-range-524288-root:!:19945:::::::
snap_daemon:!:19945:::::::
pct:$y$j9T$FjFqt1.toufDjxHuUUFwi/$X/OcNLMcD14wUn4RWZp4163uZFFDL0PoRkBwn8GFBK8:19945:0:99999:7:::
jenkins:!:19993:::::::
postgres:!:19993:::::::
sonarqube:!:19993:::::::
apsit1:$y$j9T$V/R55pU8Hp06.g.OYfGzi/$TU6Kd.dW.lvxNU8qX1qBx8SBBQybls3FD0CRpHkA04.:20132:0:99999:7:::
mysql:!:20272:::::::
suyash:$y$j9T$PlWtBK2ot.h8tzXiCL1Fa1$ZN.AKMmFHmqalYjIGHbFnArVGj9rE51YxH01RBIZyZA:20314:0:99999:7:::
```

```
apsit@apsit-HP-ProDesk-600-G4-PCI-MT:~/Downloads/Suyash$ cat suyash.txt
suyash:$y$j9T$PlWtBK2ot.h8tzXiCL1Fa1$ZN.AKMmFHmqalYjIGHbFnArVGj9rE51YxH01RBIZyZA:20314:0:99999:7:::
```

```
apsit@apsit-HP-ProDesk-600-G4-PCI-MT:~/Downloads/Suyash$ john suyash.txt
No password hashes loaded (see FAQ)
```

```
apsit@apsit-HP-ProDesk-600-G4-PCI-MT:~/Downloads/Suyash$ john --format=crypt suyash.txt
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
Will run 12 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
123456 (suyash)
1g 0:00:00.09 100% 2/3 0.1036g/s 320.8p/s 320.8c/s 320.8C/s 123456..pepper
Use the "--show" option to display all of the cracked passwords reliably
Session completed
apsit@apsit-HP-ProDesk-600-G4-PCI-MT:~/Downloads/Suyash$ john -show suyash.txt
suyash:123456:20314:0:99999:7:::

1 password hash cracked, 0 left
apsit@apsit-HP-ProDesk-600-G4-PCI-MT:~/Downloads/Suyash$ sudo userdel suyash
```

Conclusion:

In this experiment, we learnt and understood to study password cracking using John the ripper.