iGNITE Technologies

Defence Evasion

Hide Artifacts

(Mitre ID:T1564)

WWW.HACKINGARTICLES.IN

Contents

Introduction

An artifact can simply be defined as an important system file, which thus includes documentation, test plans, images, and even some executable modules.

Operating systems have a feature to hide these artifacts in order to avoid disrupting user work environments and prevent users from changing files or features on the system. However, an attacker can abuse these functionalities in order to carry out his evil intents by hiding these artifacts, which thus provides a clear path to evade detection. Let's try to understand the above statement by taking a simple example.

Suppose an **attacker penetrates your machine** and gets a **session enabled with that,** which thus allows him to **exploit your system**. The very first thing that the attacker would do is to **create a hidden file and hide his payload**, as by exploiting the operating system's features, i.e., **hiding artifacts**. Once the attacker has his payload hidden, he can now carry it out for his malicious intent by tricking the system administrator.

With that said, let's have a look at the various approaches that the attackers take to evade their presence.

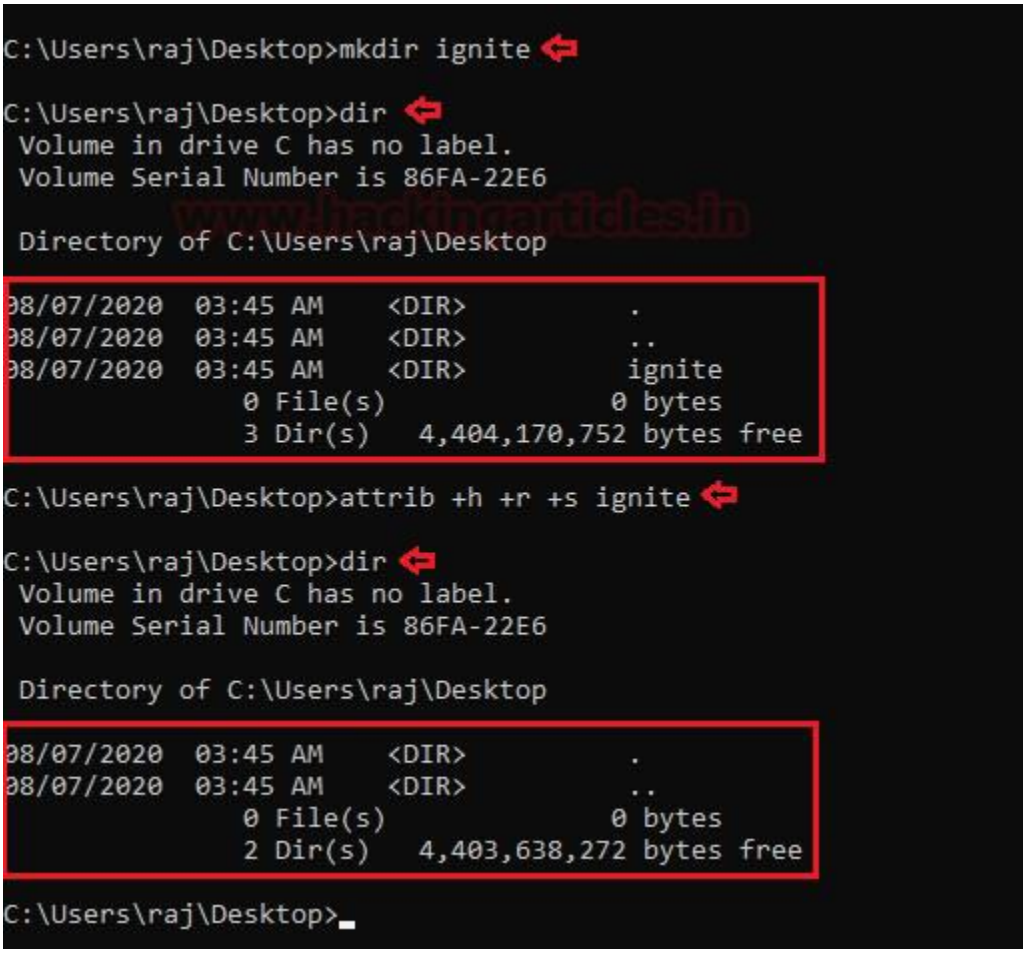
Hiding Files and Directories

Attackers may set files or directories to be hidden to evade detection mechanisms.

Let's boot into our command prompt by running it as an **administrator.** Furthermore, we'll create a folder over in our directory, as in our case, I've done it as **ignite** on the **Desktop.** The same can be confirmed by running the **dir** command.

In order to hide the file that we have just created, simply run the following command:

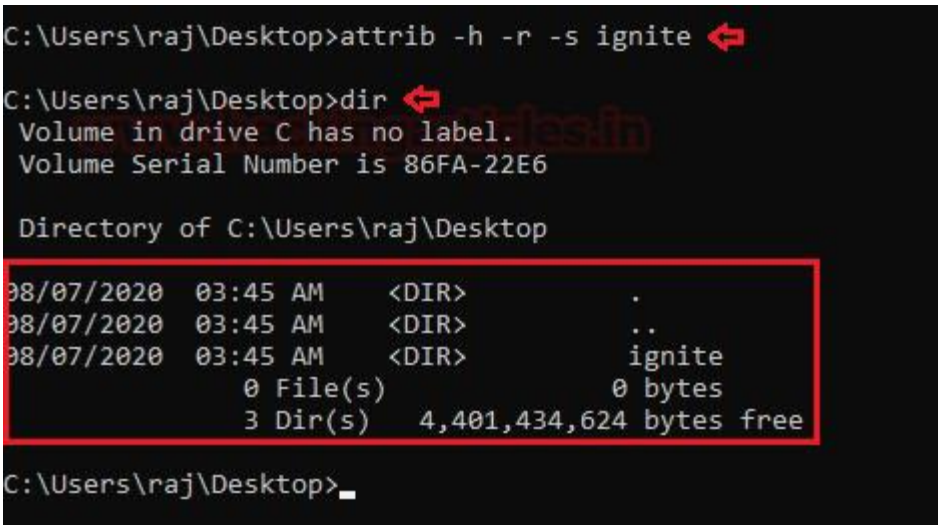
```
mkdir ignite
dir
attrib +h +r +s ignite
dir
```



Okay!! The file has been hidden now, but wait, let's see how to unhide it. Simply run the following command:

```
attrib -h -r -s ignite
dir
```

Great!! We can see from the screenshot below that when we used the **"dir"** command, we were able to get our file back onto the desktop.



Hiding Users

Adversaries may use hidden users to mask the presence of user accounts that they create. In this section, we will have a look at how users can be hidden.

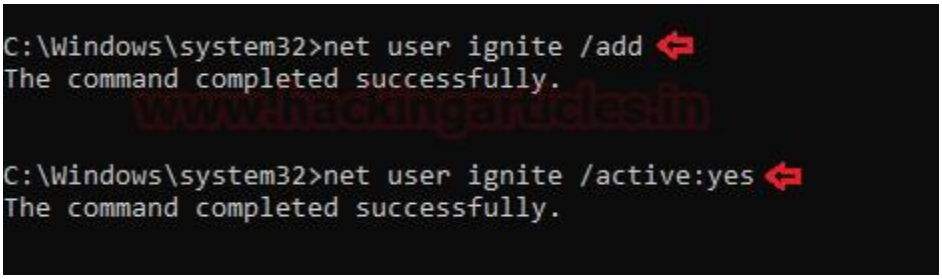
Using Command Prompt:

So, let's restart our command prompt and create a user, which we'll call **"ignite"** in this case. A user can be created by using the command:

net user ignite /add

Now that the user has been created, we need to activate it, which can be done by running the command:

net user ignite /active:yes



We will hide the user **"ignite"** by running the command:

net user ignite /active:no

To check the changes, we would simply restart our PC and notice that our user is no more visible on the sign-in page.

So, to unhide the user, simply re-run the command:

net user ignite /active:yes

We'll notice that our user **"ignite"** is again visible over at our sign-in page.

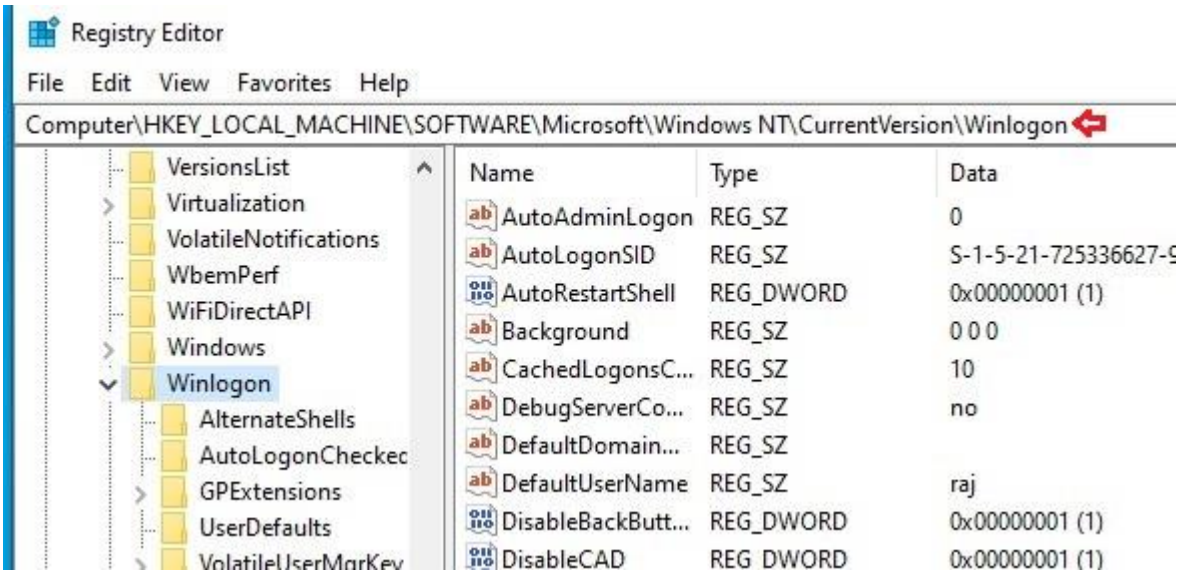
Using Registry Editor:

This method can be lengthier as compared to the above one, but it's always good to know. So, let's explore this path and hide our user.

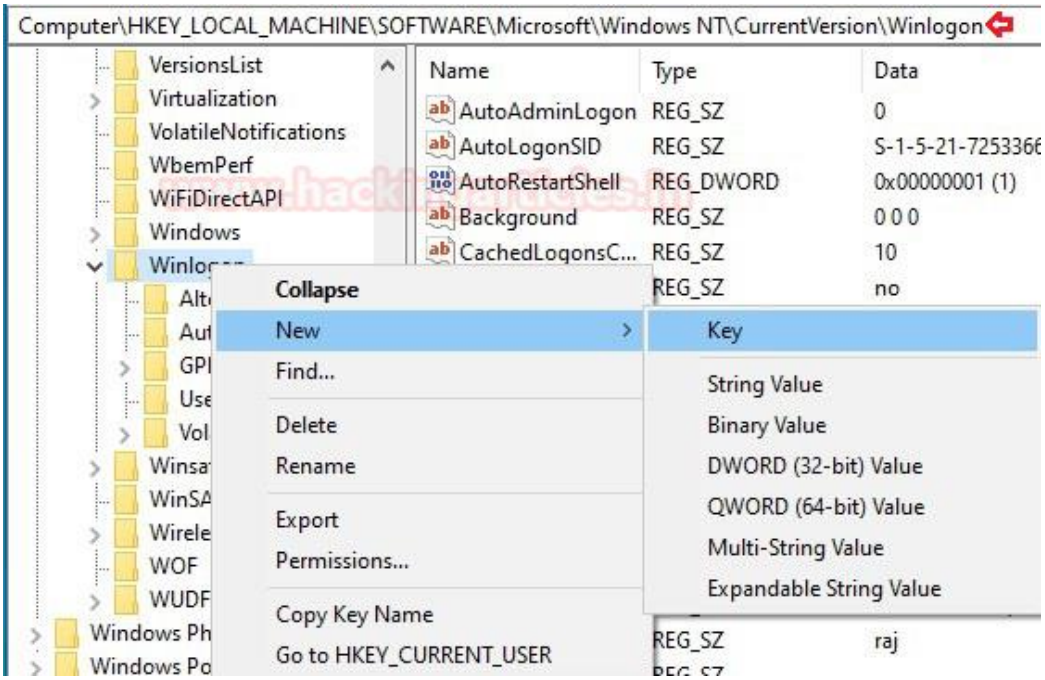
Over at the Run Window, type **"Regedit"** in the search prompt.

Once we enter the registry edit, just navigate to

HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon



Now, that we have navigated to the path mentioned above let's **Right-click on Winlogon -> Select New and choose Key**



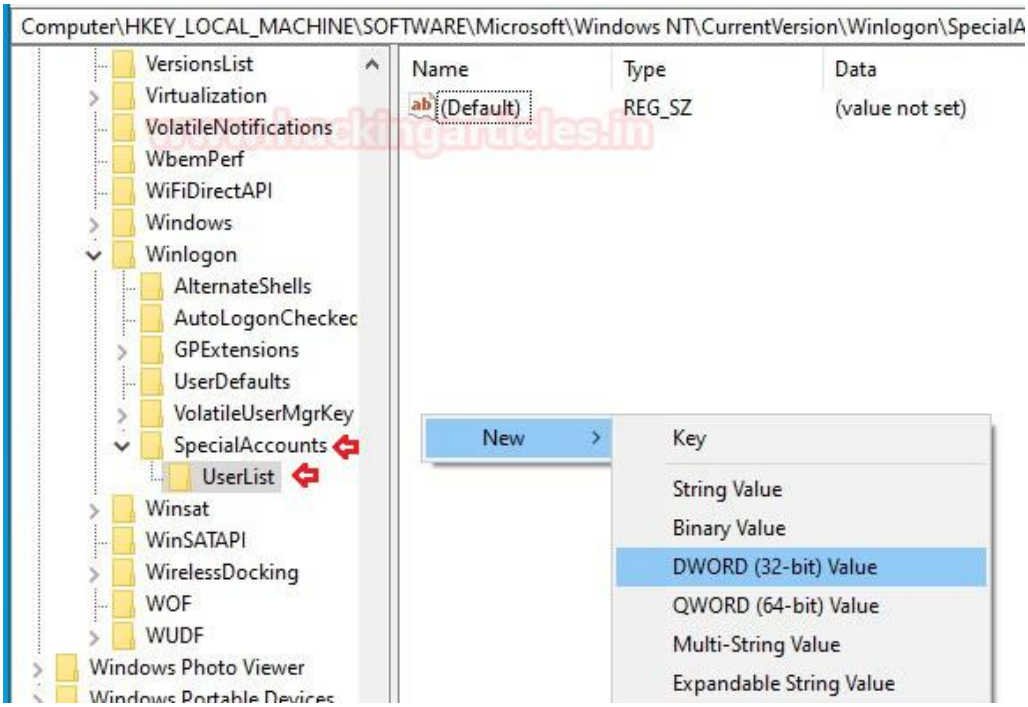
After completing the above process, we will rename the new key created as **"SpecialAccounts"**.

Then, right-click on SpecialAccounts-> Select New and choose Key. This key will be renamed **"UserList".**

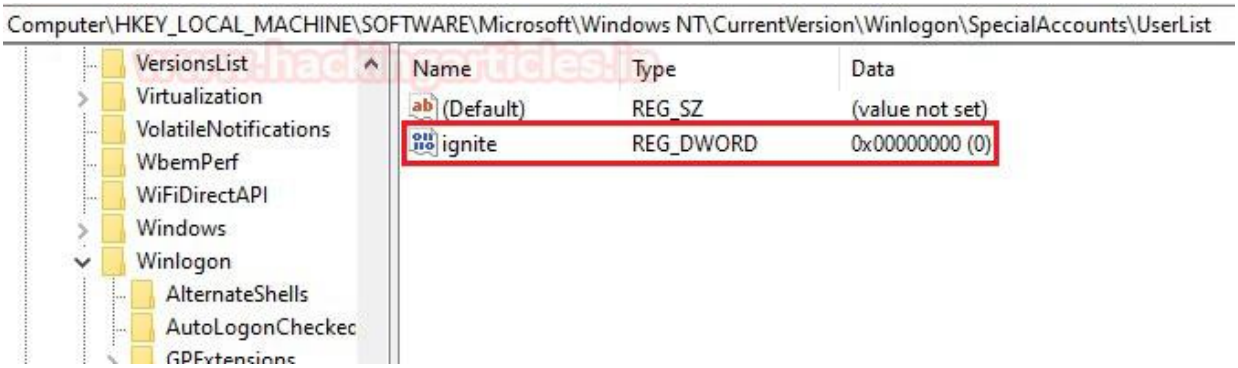
We can see that we have created two new keys. One is **"SpecialAccounts"** under **"Winlogon"**, and the second key is **"UserList"** under **"SpecialAccounts"**.

Over on the blank right-hand side, follow up as:

Right-click -> Choose New ->Select DWORD (32-bit) value as shown below



The new key created should be named after the user we are supposed to hide. In our case, we named the new key **"ignite"** because we are concealing this user.



Now, close your registry editor and restart your PC to see the changes. The user is now invisible.

In order to unhide the same user, we'll just go back to our registry editor and navigate to:

HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\SpecialAccounts\UserList

Then, we'll **double click** on the **ignite user** and **change** the **Value data from 0 to 1** and, hit enter

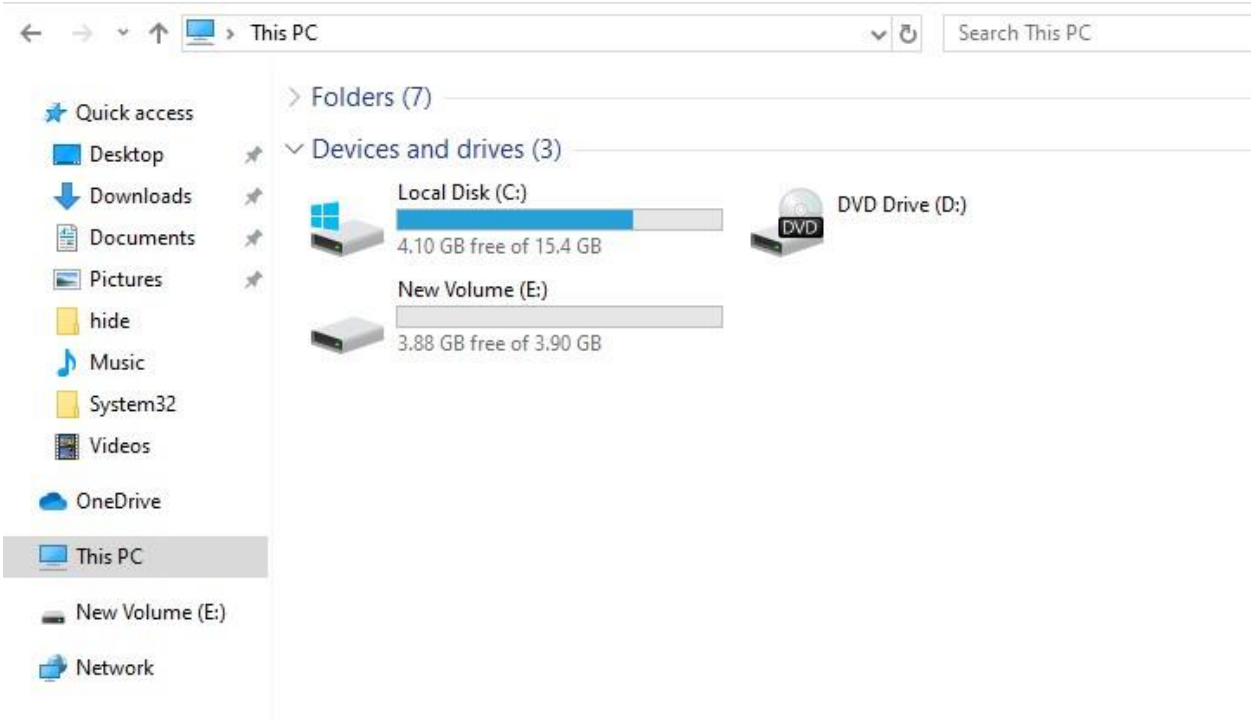
Again, restart your system to see the changes. Your user is back on the sign-in page.

Hiding File Systems

Adversaries may use a hidden file system to conceal malicious attacks from users and security tools. File systems provide a structure to store and access data from physical storage. So, let's deep dive and have a look at how the above is accomplished.

Method 1: Over Command Prompt

Let's say we have an E drive which we want to hide.



At your command prompt, type **"diskpart"** to open a disk partition.

Let's now list all the volumes available there by using **"list volume".**

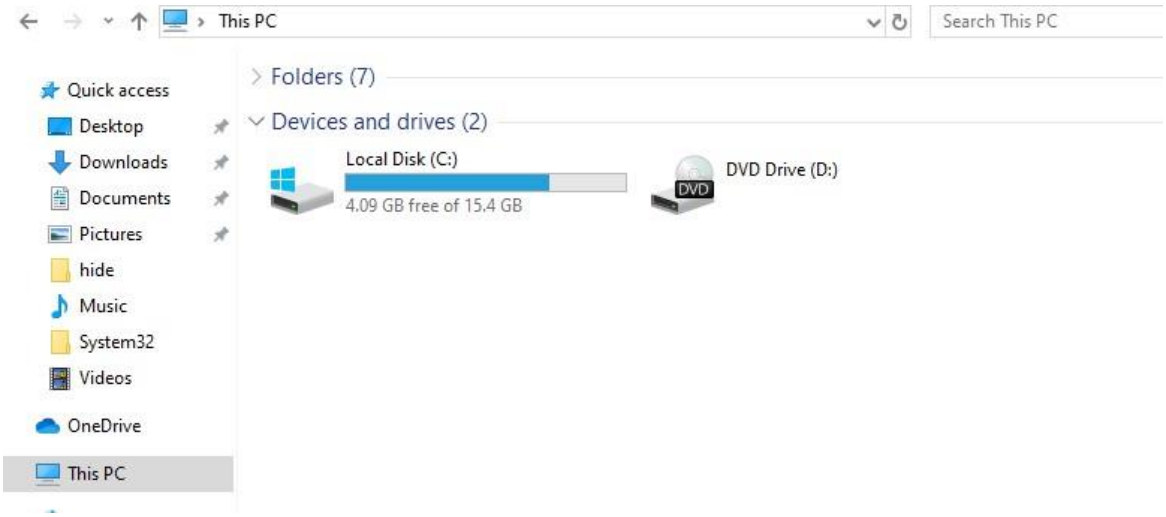
As the volumes are over on our screen, let's choose the volume that contains the drive that needs to be hidden. In our case, we selected volume 3 by running the command**: select volume 3**

Great!! We're almost there, now to hide the drive, simply run the command:

```
diskpart
list volume
select volume 3
remove letter e
```

```
C:\Windows\system32>diskpart

Microsoft DiskPart version 10.0.18362.1

Copyright (C) Microsoft Corporation.
On computer: DESKTOP-TT14AQK

DISKPART> list volume

  Volume ###  Ltr  Label        Fs     Type        Size     Status     Info
  ----------  ---  -----------  -----  ----------  -------  ---------  --------
  Volume 0     D                       DVD-ROM         0 B  No Media
  Volume 1         Recovery     NTFS   Partition    529 MB  Healthy
  Volume 2     C                NTFS   Partition     15 GB  Healthy    Boot
  Volume 3     E   New Volume   NTFS   Partition   3999 MB  Healthy
  Volume 4                      FAT32  Partition     99 MB  Healthy    System

DISKPART> select volume 3

Volume 3 is the selected volume.

DISKPART> remove letter e

DiskPart successfully removed the drive letter or mount point.

DISKPART>
```

From the below screenshot we can see that Drive E is successfully hidden.



Further, to unhide the drive simply run the command:

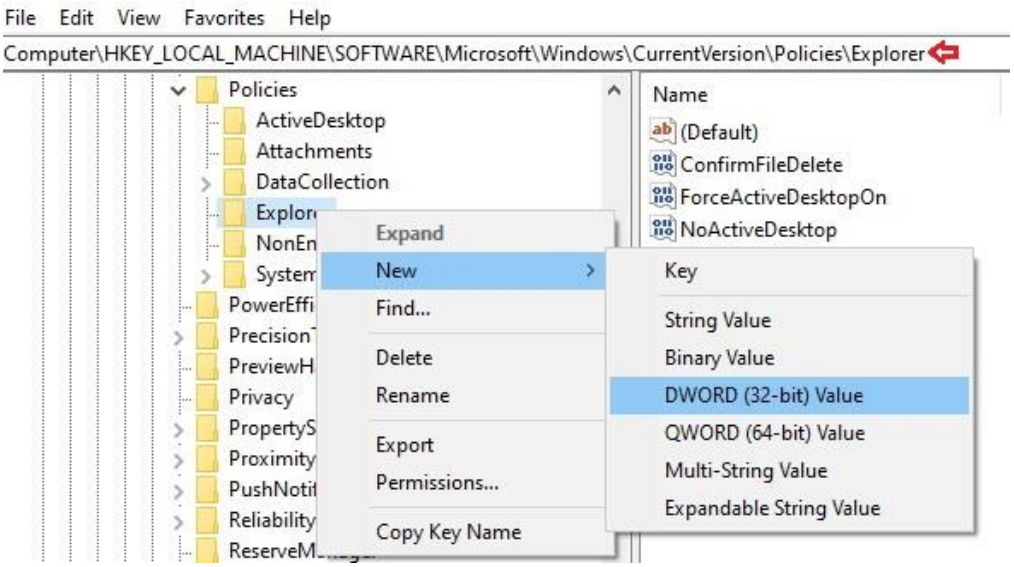
assign letter e

```
DISKPART> assign letter e

DiskPart successfully assigned the drive letter or mount point.

DISKPART>
```

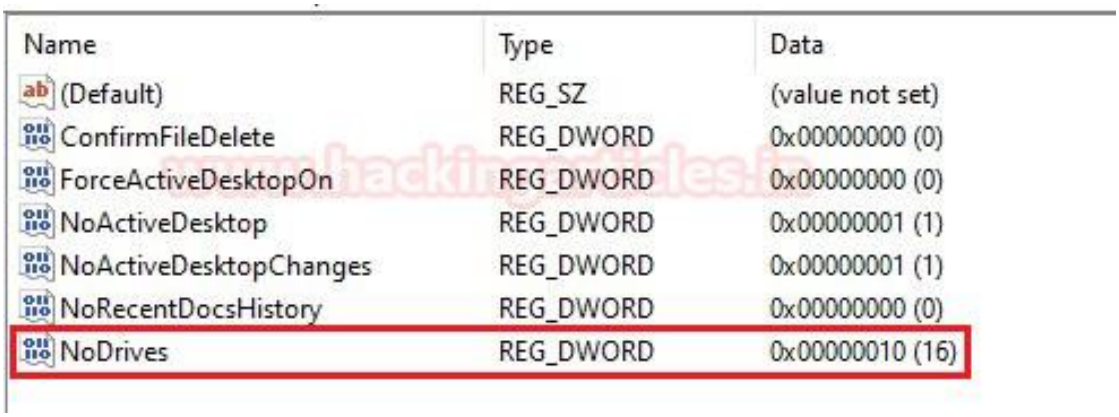
Method 2: Using Registry Editor

For this method, we'll go back into the registry editor as explained in the "Hidden User" section and navigate to **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer**

After navigating to the above-mentioned path, Right-click over on Explorer -> Select New -> DWORD (32-bit) Value as shown below.



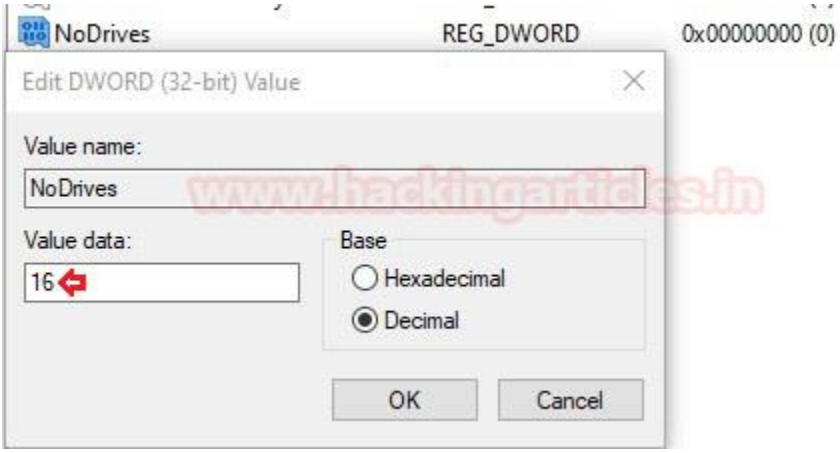
A new key will be generated, which must be renamed "NoDrives"



Name	Type	Data
(Default)	REG_SZ	(value not set)
ConfirmFileDelete	REG_DWORD	0x00000000 (0)
ForceActiveDesktopOn	REG_DWORD	0x00000000 (0)
NoActiveDesktop	REG_DWORD	0x00000001 (1)
NoActiveDesktopChanges	REG_DWORD	0x00000001 (1)
NoRecentDocsHistory	REG_DWORD	0x00000000 (0)
NoDrives	REG_DWORD	0x00000010 (16)

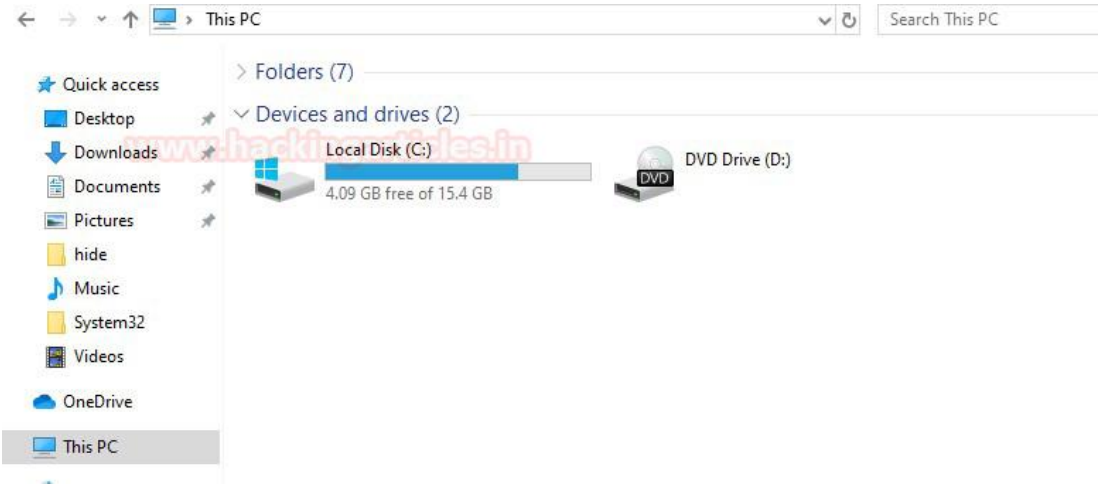
Now, that our new key has been renamed as "NoDrives", let's double click on it and change the base from Hexadecimal to Decimal and give input to the Value Data field according to the drive which we wish to hide.

In our case, as we're hiding the E drive, we will set the Value data to "16"as the decimal value of the alphabet E is 16. You can set it according to yours.



Reboot your system again, and check for the drives.

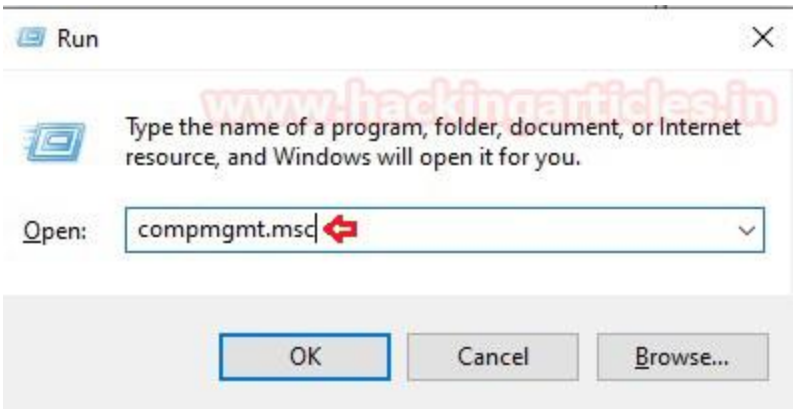
Great!! From the below screenshot you can see that our drive has been hidden now.



To unhide the drive, navigate back to "Regedit" as explained above and move to **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer**. Right-click on "NoDrives"and just Delete it. Again, restart your system and see that the drive is again visible.

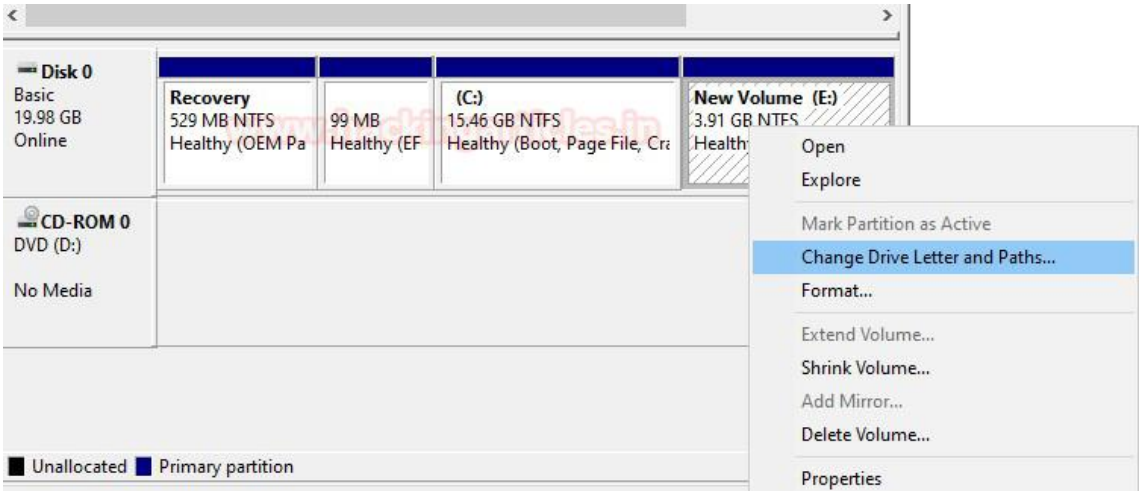
Method 3: Using Disk Management

Let's open Disk Management by running the command **"compmgmt.msc"** in the **Run Dialog Box** as shown below.

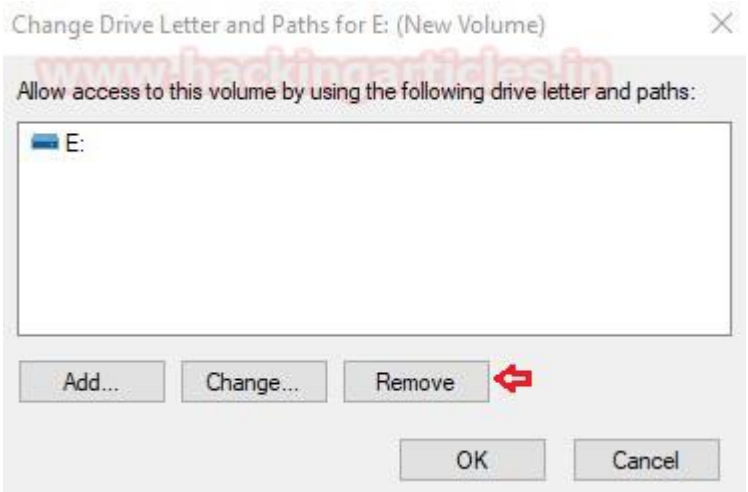


We'll select the drive which we want to hide and right-click on it.

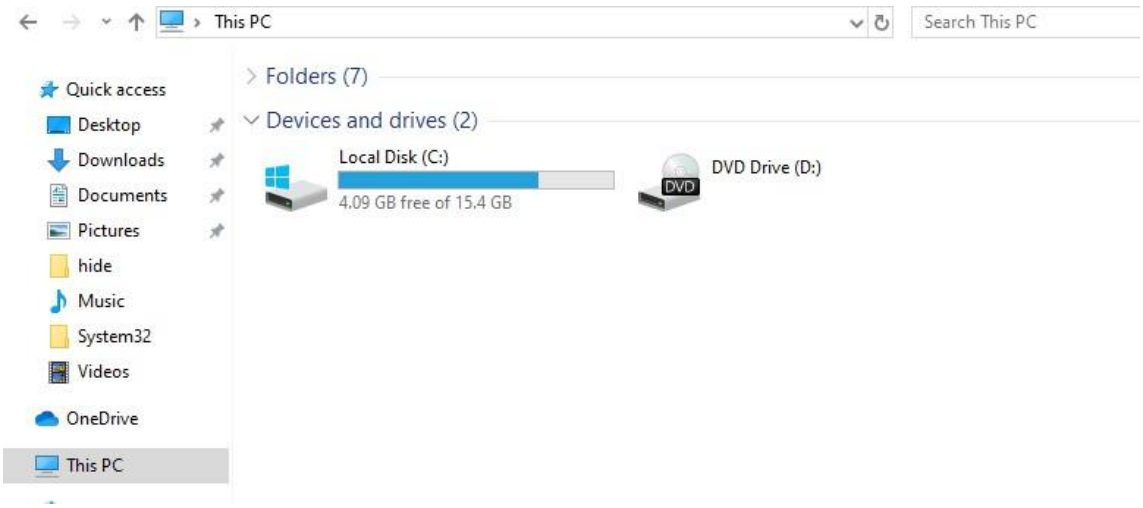
Then select **"Change Drive Letters and Paths"**.



After completing the above step, we'll select the drive and click on the **"Remove"** button.



Reboot your system and you'll notice that the drive is now hidden. In our case, drive E is not visible as we can see below.



Let's unhide the drive by going back to disk management. Double click on New Volume and, select **"Change Drive Letter and Paths".** Click the **Add** button, then select the **"Assign the following drive letter"** option and press OK to add the drive.

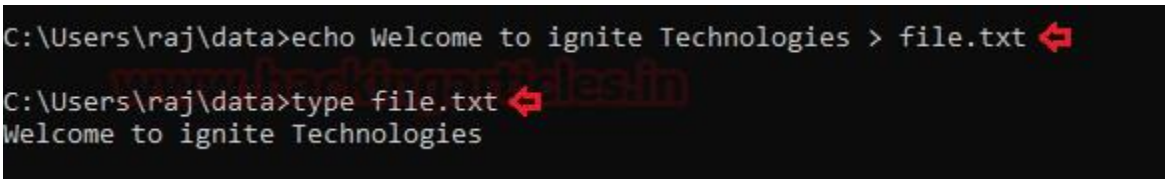
NTFS File Attributes

Adversaries may use NTFS file attributes to hide their malicious data to evade detection. Every New Technology File System **(NTFS)** formatted partition contains a Master File Table **(MFT)** that maintains records for every file and directory on the system. Let's explore how the above attack can be executed.

Boot up your Command Prompt again as an administrator in order to generate a file with some data in it:

echo Welcome to ignite Technologies > file.txt

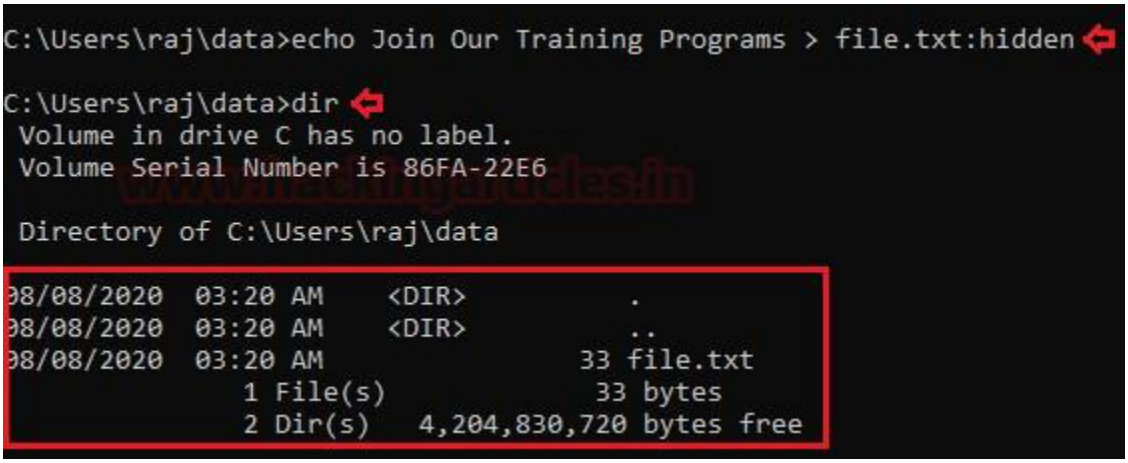
From the below image, we can see that our file has been created with the data we entered.



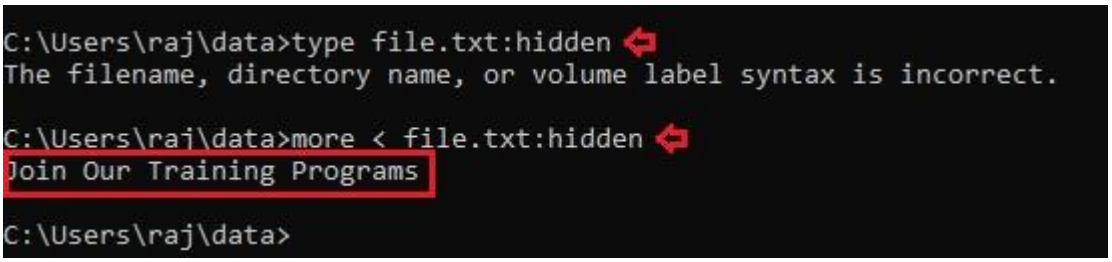
Now, let's create another file inside file.txt but this time we'll make it as hidden with

echo Join Our Training Programs > file.txt:hidden

From the below screenshot we can see that the file **"hidden"** is not visible at all.



Go ahead and type the command: type **file.txt:hidden** and hit Enter. You will notice that the file is still not visible to us.
But how to check the contents?
Simply run the command as **more < file.txt:hidden** and you will be there again.



Detection

The following methods can be used to detect such type of attacks:

- Monitoring processes, and command-line arguments for actions indicative of hidden artifacts.
- Monitoring event and authentication logs for records of hidden artifacts being used.
- Monitoring the file system and shell commands for hidden attribute usage.

Reference

https://attack.mitre.org/techniques/T1564/
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/attrib
https://www.pcmag.com/encyclopedia/term/artifact

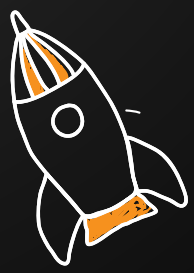
iGNITE Technologies

JOIN OUR TRAINING PROGRAMS

CLICK HERE

BEGINNER

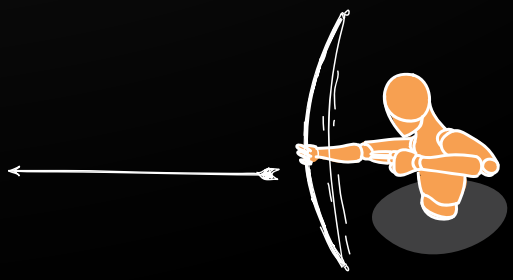
- Ethical Hacking
- Network Pentest
- Bug Bounty
- Wireless Pentest
- Network Security Essentials



ADVANCED

- Burp Suite Pro
- Android Pentest
- Web Services-API
- Advanced Metasploit
- Pro Infrastructure VAPT
- CTF
- Computer Forensics

EXPERT



- Red Team Operation
  - APT's - MITRE Attack Tactics
  - Active Directory Attack
  - MSSQL Security Assessment
- Privilege Escalation
  - Windows
  - Linux