PEAS Report

System Information

Basic System Information

Check if the Windows versions is vulnerable to some known exploit https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#kernel-exploits

```
OS Name: Microsoft Windows 11 Home Single Language
OS Version: 10.0.22621 N/A Build 22621
System Type: x64-based PC
Hostname: LAPTOP-9R1PMVC2
ProductName: Windows 10 Home Single Language
EditionID: CoreSingleLanguage
ReleaseId: 2009
BuildBranch: ni_release
CurrentMajorVersionNumber: 10
CurrentVersion: 6.3
Architecture: AMD64
ProcessorCount: 8
SystemLang: en-US
KeyboardLang: English (India)
TimeZone: (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
IsVirtualMachine: False
Current Time: 08-08-2023 14:53:53
HighIntegrity: False
PartOfDomain: False
Hotfixes: KB5027119, KB5028851, KB5012170, KB5028185, KB5025351, KB5028320,
[?] Windows vulns search powered by Watson(https://github.com/rasta-mouse/Watson)
```

Showing All Microsoft Updates

```
HotFix ID : KB2267602
Installed At (UTC) : 08-08-2023 00:26:20
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.393.2546.0)
Client Application ID : MoUpdateOrchestrator
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
================================================================================
==============
HotFix ID : KB2267602
Installed At (UTC) : 07-08-2023 11:24:00
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.393.2516.0)
Client Application ID : MoUpdateOrchestrator
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
================================================================================
==============
HotFix ID : KB2267602
Installed At (UTC) : 07-08-2023 07:53:37
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.393.2508.0)
Client Application ID : Windows Defender
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
================================================================================
==============
HotFix ID : KB2267602
Installed At (UTC) : 05-08-2023 01:38:37
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.393.2335.0)
Client Application ID : MoUpdateOrchestrator
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
================================================================================
==============
```

```
HotFix ID : KB2267602
Installed At (UTC) : 04-08-2023 23:26:47
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.393.2319.0)
Client Application ID : Windows Defender
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
================================================================================
==============
HotFix ID :
Installed At (UTC) : 04-08-2023 06:03:44
Title : 9WZDNCRD1HKW-Microsoft.XboxIdentityProvider
Client Application ID : Update;ScanForUpdates
Description : 9WZDNCRD1HKW-1152921505695555680
================================================================================
==============
HotFix ID :
Installed At (UTC) : 04-08-2023 06:02:44
Title : 9WZDNCRFJ3TT-26720RandomSaladGamesLLC.SimpleSolitaire
Client Application ID : Update;ScanForUpdates
Description : 9WZDNCRFJ3TT-1152921505695398549
================================================================================
==============
HotFix ID : KB2267602
Installed At (UTC) : 03-08-2023 22:59:27
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.393.2223.0)
Client Application ID : Windows Defender
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
================================================================================
==============
HotFix ID : KB5028185
Installed At (UTC) : 03-08-2023 21:19:43
Title : 2023-07 Cumulative Update for Windows 11 Version 22H2 for x64-based Systems
(KB5028185)
Client Application ID : MoUpdateOrchestrator
Description : Install this update to resolve issues in Windows. For a complete
listing of the issues that are included in this update, see the associated
Microsoft Knowledge Base article for more information. After you install this item,
you may have to restart your computer.
================================================================================
==============
HotFix ID : KB2267602
Installed At (UTC) : 03-08-2023 20:59:50
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.393.2243.0)
Client Application ID : Windows Defender
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
================================================================================
==============
HotFix ID : KB5028851
Installed At (UTC) : 03-08-2023 20:53:14
Title : 2023-07 Cumulative Update for .NET Framework 3.5 and 4.8.1 for Windows 11,
version 22H2 for x64 (KB5028851)
Client Application ID : MoUpdateOrchestrator
Description : Install this update to resolve issues in Windows. For a complete
listing of the issues that are included in this update, see the associated
Microsoft Knowledge Base article for more information. After you install this item,
you may have to restart your computer.
================================================================================
==============
HotFix ID : KB2267602
Installed At (UTC) : 03-08-2023 11:41:54
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.393.2180.0)
Client Application ID : MoUpdateOrchestrator
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
================================================================================
==============
HotFix ID :
Installed At (UTC) : 03-08-2023 03:15:56
```

```
Title : 9NCBCSZSJRSB-SpotifyAB.SpotifyMusic
Client Application ID : Update;ScanForUpdatesForUser
Description : 9NCBCSZSJRSB-1152921505696539330
================================================================================
==============
HotFix ID :
Installed At (UTC) : 03-08-2023 03:15:56
Title : 9NZQPT0MWTD0-A278AB0D.Asphalt9
Client Application ID : Update;ScanForUpdatesForUser
Description : 9NZQPT0MWTD0-1152921505696564657
================================================================================
==============
HotFix ID :
Installed At (UTC) : 03-08-2023 03:15:56
Title : 9NBLGGH33ZDV-A278AB0D.MARCHOFEMPIRES
Client Application ID : Update;ScanForUpdatesForUser
Description : 9NBLGGH33ZDV-1152921505696552883
================================================================================
==============
HotFix ID : KB2267602
Installed At (UTC) : 02-08-2023 17:27:39
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.393.2126.0)
Client Application ID : MoUpdateOrchestrator
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
================================================================================
==============
HotFix ID : KB2267602
Installed At (UTC) : 02-08-2023 00:49:03
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.393.2059.0)
Client Application ID : Windows Defender
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
================================================================================
==============
HotFix ID : KB2267602
Installed At (UTC) : 30-07-2023 07:37:15
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.393.1840.0)
Client Application ID : Windows Defender
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
================================================================================
==============
HotFix ID : KB2267602
Installed At (UTC) : 28-07-2023 03:58:21
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.393.1671.0)
Client Application ID : Windows Defender
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
================================================================================
==============
HotFix ID : KB890830
Installed At (UTC) : 28-07-2023 03:17:49
Title : Windows Malicious Software Removal Tool x64 - v5.115 (KB890830)
Client Application ID : MoUpdateOrchestrator
Description : After the download, this tool runs one time to check your computer
for infection by specific, prevalent malicious software (including Blaster, Sasser,
and Mydoom) and helps remove any infection that is found. If an infection is found,
the tool will display a status report the next time that you start your computer. A
new version of the tool will be offered every month. If you want to manually run
the tool on your computer, you can download a copy from the Microsoft Download
Center, or you can run an online version from microsoft.com. This tool is not a
replacement for an antivirus product. To help protect your computer, you should use
an antivirus product.
================================================================================
==============
HotFix ID : KB2267602
Installed At (UTC) : 25-07-2023 02:39:52
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.393.1373.0)
```

```
Client Application ID : Windows Defender
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
================================================================================
==============
HotFix ID : KB4052623
Installed At (UTC) : 25-07-2023 02:29:30
Title : Update for Microsoft Defender Antivirus antimalware platform - KB4052623
(Version 4.18.23050.9)
Client Application ID : Windows Defender
Description : This package will update Microsoft Defender Antivirus antimalware
platform's components on the user machine.
================================================================================
==============
HotFix ID :
Installed At (UTC) : 23-07-2023 10:11:49
Title : 9NBLGGH51CLL-Microsoft.Services.Store.Engagement
Client Application ID : <<PROCESS>>: svchost.exe
Description : 9NBLGGH51CLL-1152921505696449882
================================================================================
==============
HotFix ID :
Installed At (UTC) : 23-07-2023 10:11:49
Title : 9P105T65H4Z5-Microsoft.WindowsAppRuntime.1.3
Client Application ID : <<PROCESS>>: svchost.exe
Description : 9P105T65H4Z5-1152921505696411251
================================================================================
==============
HotFix ID : KB2267602
Installed At (UTC) : 23-07-2023 09:36:58
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.393.1190.0)
Client Application ID : Windows Defender
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
================================================================================
==============
HotFix ID : KB2267602
Installed At (UTC) : 21-07-2023 11:46:01
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.393.995.0)
Client Application ID : Windows Defender
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
================================================================================
==============
HotFix ID : KB2267602
Installed At (UTC) : 17-07-2023 23:21:28
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.393.694.0)
Client Application ID : Windows Defender
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
================================================================================
==============
HotFix ID : KB2267602
Installed At (UTC) : 17-07-2023 23:15:11
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.393.694.0)
Client Application ID : Windows Defender
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
================================================================================
==============
HotFix ID : KB2267602
Installed At (UTC) : 10-07-2023 23:11:25
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.4170.0)
Client Application ID : Windows Defender
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
================================================================================
```

```
===============
HotFix ID : KB5027231
Installed At (UTC) : 09-07-2023 03:56:43
Title : 2023-06 Cumulative Update for Windows 11 Version 22H2 for x64-based Systems
(KB5027231)
Client Application ID : MoUpdateOrchestrator
Description : Install this update to resolve issues in Windows. For a complete
listing of the issues that are included in this update, see the associated
Microsoft Knowledge Base article for more information. After you install this item,
you may have to restart your computer.
================================================================================
===============
HotFix ID : KB890830
Installed At (UTC) : 06-07-2023 09:04:44
Title : Windows Malicious Software Removal Tool x64 - v5.114 (KB890830)
Client Application ID : MoUpdateOrchestrator
Description : After the download, this tool runs one time to check your computer
for infection by specific, prevalent malicious software (including Blaster, Sasser,
and Mydoom) and helps remove any infection that is found. If an infection is found,
the tool will display a status report the next time that you start your computer. A
new version of the tool will be offered every month. If you want to manually run
the tool on your computer, you can download a copy from the Microsoft Download
Center, or you can run an online version from microsoft.com. This tool is not a
replacement for an antivirus product. To help protect your computer, you should use
an antivirus product.
================================================================================
===============
HotFix ID : KB5027119
Installed At (UTC) : 06-07-2023 08:58:53
Title : 2023-06 Cumulative Update for .NET Framework 3.5 and 4.8.1 for Windows 11,
version 22H2 for x64 (KB5027119)
Client Application ID : MoUpdateOrchestrator
Description : A security issue has been identified in a Microsoft software product
that could affect your system. You can help protect your system by installing this
update from Microsoft. For a complete listing of the issues that are included in
this update, see the associated Microsoft Knowledge Base article. After you install
this update, you may have to restart your system.
================================================================================
===============
HotFix ID :
Installed At (UTC) : 06-07-2023 03:38:53
Title : 9WZDNCRFJ26J-GAMELOFTSA.ASPHALT8AIRBORNE
Client Application ID : Update;ScanForUpdates
Description : 9WZDNCRFJ26J-1152921505696440776
================================================================================
===============
HotFix ID :
Installed At (UTC) : 06-07-2023 03:27:37
Title : 9WZDNCRFJ3MB-Evernote.Evernote
Client Application ID : Update;ScanForUpdates
Description : 9WZDNCRFJ3MB-1152921505696438672
================================================================================
===============
HotFix ID : KB2267602
Installed At (UTC) : 06-07-2023 03:23:29
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.3726.0)
Client Application ID : MoUpdateOrchestrator
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
================================================================================
===============
HotFix ID : KB5007651
Installed At (UTC) : 06-07-2023 03:23:15
Title : Update for Windows Security platform antimalware platform - KB5007651
(Version 1.0.2306.10002)
Client Application ID : MoUpdateOrchestrator
Description : This package will update Windows Security platform antimalware
platform's components on the user machine.
================================================================================
===============
HotFix ID :
Installed At (UTC) : 05-07-2023 09:40:19
Title : 9P6RC76MSMMJ-AmazonVideo.PrimeVideo
Client Application ID : Update;ScanForUpdates
Description : 9P6RC76MSMMJ-1152921505696457778
================================================================================
===============
```

```
HotFix ID :
Installed At (UTC) : 05-07-2023 09:40:17
Title : 9PDXGNCFSCZV-CanonicalGroupLimited.Ubuntu
Client Application ID : Update;ScanForUpdates
Description : 9PDXGNCFSCZV-1152921505696252822
================================================================================
==============
HotFix ID : KB2267602
Installed At (UTC) : 05-07-2023 08:47:34
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.3648.0)
Client Application ID : Windows Defender
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
================================================================================
==============
HotFix ID : KB2267602
Installed At (UTC) : 04-07-2023 07:18:30
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.3528.0)
Client Application ID : Windows Defender
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
================================================================================
==============
HotFix ID :
Installed At (UTC) : 03-07-2023 09:04:35
Title : 9P105T65H4Z5-Microsoft.WindowsAppRuntime.1.3
Client Application ID : <<PROCESS>>: svchost.exe
Description : 9P105T65H4Z5-1152921505696411251
================================================================================
==============
HotFix ID : KB2267602
Installed At (UTC) : 03-07-2023 03:13:19
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.3393.0)
Client Application ID : Windows Defender
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
================================================================================
==============
HotFix ID : KB2267602
Installed At (UTC) : 27-06-2023 23:10:02
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.2801.0)
Client Application ID : Windows Defender
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
================================================================================
==============
HotFix ID : KB4052623
Installed At (UTC) : 21-06-2023 12:11:58
Title : Update for Microsoft Defender Antivirus antimalware platform - KB4052623
(Version 4.18.23050.5)
Client Application ID : Windows Defender
Description : This package will update Microsoft Defender Antivirus antimalware
platform's components on the user machine.
================================================================================
==============
HotFix ID : KB2267602
Installed At (UTC) : 21-06-2023 12:02:57
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.2163.0)
Client Application ID : Windows Defender
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
================================================================================
==============
HotFix ID : KB2267602
Installed At (UTC) : 09-06-2023 03:44:10
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.919.0)
Client Application ID : Windows Defender
```

```
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
================================================================================
==============
HotFix ID :
Installed At (UTC) : 06-06-2023 07:22:09
Title : 9P8CP1L72JXS-Microsoft.ForzaHorizon4Demo
Client Application ID : Acquisition;Microsoft.WindowsStore_8wekyb3d8bbwe
Description : 9P8CP1L72JXS-1152921505688119605
================================================================================
==============
HotFix ID :
Installed At (UTC) : 06-06-2023 04:59:49
Title : 9P8CP1L72JXS-Microsoft.ForzaHorizon4Demo
Client Application ID : Acquisition;Microsoft.WindowsStore_8wekyb3d8bbwe
Description : 9P8CP1L72JXS-1152921505688119605
================================================================================
==============
HotFix ID :
Installed At (UTC) : 06-06-2023 04:54:52
Title : 9P8CP1L72JXS-Microsoft.ForzaHorizon4Demo
Client Application ID : Acquisition;Microsoft.WindowsStore_8wekyb3d8bbwe
Description : 9P8CP1L72JXS-1152921505688119605
================================================================================
==============
HotFix ID :
Installed At (UTC) : 06-06-2023 04:19:30
Title : 9P8CP1L72JXS-Microsoft.ForzaHorizon4Demo
Client Application ID : Acquisition;Microsoft.WindowsStore_8wekyb3d8bbwe
Description : 9P8CP1L72JXS-1152921505688119605
================================================================================
==============
HotFix ID :
Installed At (UTC) : 02-06-2023 03:00:24
Title : 9WZDNCRFJ26J-GAMELOFTSA.ASPHALT8AIRBORNE
Client Application ID : Acquisition;Microsoft.WindowsStore_8wekyb3d8bbwe
Description : 9WZDNCRFJ26J-1152921505696204562
================================================================================
==============
HotFix ID : KB2267602
Installed At (UTC) : 29-05-2023 23:46:34
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.2729.0)
Client Application ID : Windows Defender
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
================================================================================
==============
HotFix ID : KB2267602
Installed At (UTC) : 28-05-2023 23:06:21
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.2630.0)
Client Application ID : Windows Defender
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
================================================================================
==============
HotFix ID : KB2267602
Installed At (UTC) : 27-05-2023 11:31:10
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.2544.0)
Client Application ID : Windows Defender
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
================================================================================
==============
HotFix ID : KB2267602
Installed At (UTC) : 25-05-2023 00:00:29
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.2371.0)
Client Application ID : Windows Defender
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
```

```
================================================================================
==============
HotFix ID : KB2267602
Installed At (UTC) : 24-05-2023 23:25:34
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.2356.0)
Client Application ID : Windows Defender
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
================================================================================
==============
HotFix ID : KB2267602
Installed At (UTC) : 24-05-2023 02:09:29
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.2281.0)
Client Application ID : MoUpdateOrchestrator
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
================================================================================
==============
HotFix ID : KB2267602
Installed At (UTC) : 23-05-2023 22:17:31
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.2284.0)
Client Application ID : Windows Defender
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
================================================================================
==============
HotFix ID :
Installed At (UTC) : 23-05-2023 11:28:26
Title : 9NBLGGH33ZDV-A278AB0D.MARCHOFEMPIRES
Client Application ID : Update;ScanForUpdates
Description : 9NBLGGH33ZDV-1152921505696226447
================================================================================
==============
HotFix ID :
Installed At (UTC) : 23-05-2023 11:26:06
Title : 9NZQPT0MWTD0-A278AB0D.Asphalt9
Client Application ID : Update;ScanForUpdates
Description : 9NZQPT0MWTD0-1152921505696127151
================================================================================
==============
HotFix ID :
Installed At (UTC) : 23-05-2023 11:24:55
Title : 9WZDNCRD1HKW-Microsoft.XboxIdentityProvider
Client Application ID : Update;ScanForUpdates
Description : 9WZDNCRD1HKW-1152921505695555680
================================================================================
==============
HotFix ID :
Installed At (UTC) : 23-05-2023 11:24:55
Title : 9NBLGGH537C2-Microsoft.XboxGameOverlay
Client Application ID : Update;ScanForUpdates
Description : 9NBLGGH537C2-1152921505690350335
================================================================================
==============
HotFix ID :
Installed At (UTC) : 23-05-2023 11:23:45
Title : 9P086NHDNB9W-Microsoft.XboxSpeechtoTextOverlay
Client Application ID : Update;ScanForUpdates
Description : 9P086NHDNB9W-1152921504627240859
================================================================================
==============
HotFix ID : KB2267602
Installed At (UTC) : 22-05-2023 04:48:52
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.2067.0)
Client Application ID : MoUpdateOrchestrator
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
================================================================================
==============
HotFix ID : KB2267602
```

```
Installed At (UTC) : 22-05-2023 02:43:47
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.2067.0)
Client Application ID : Windows Defender
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
================================================================================
==============
HotFix ID : KB2267602
Installed At (UTC) : 22-05-2023 02:43:37
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.2067.0)
Client Application ID : MoUpdateOrchestrator
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
================================================================================
==============
HotFix ID : KB2267602
Installed At (UTC) : 19-05-2023 05:14:16
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.1824.0)
Client Application ID : MoUpdateOrchestrator
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
================================================================================
==============
HotFix ID : KB2267602
Installed At (UTC) : 19-05-2023 05:13:55
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.1824.0)
Client Application ID : MoUpdateOrchestrator
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
================================================================================
==============
HotFix ID : KB2267602
Installed At (UTC) : 19-05-2023 02:07:17
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.1807.0)
Client Application ID : Windows Defender
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
================================================================================
==============
HotFix ID :
Installed At (UTC) : 18-05-2023 07:53:55
Title : 9NBLGGH33ZDV-A278AB0D.MARCHOFEMPIRES
Client Application ID : Update;ScanForUpdatesForUser
Description : 9NBLGGH33ZDV-1152921505696226447
================================================================================
==============
HotFix ID :
Installed At (UTC) : 18-05-2023 07:52:55
Title : 9NZQPT0MWTD0-A278AB0D.Asphalt9
Client Application ID : Update;ScanForUpdatesForUser
Description : 9NZQPT0MWTD0-1152921505696127151
================================================================================
==============
HotFix ID : KB2267602
Installed At (UTC) : 17-05-2023 22:41:18
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.1512.0)
Client Application ID : MoUpdateOrchestrator
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
================================================================================
==============
HotFix ID : KB2267602
Installed At (UTC) : 16-05-2023 05:30:12
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.1472.0)
Client Application ID : MoUpdateOrchestrator
```

```
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
================================================================================
==============
HotFix ID : KB890830
Installed At (UTC) : 16-05-2023 05:30:03
Title : Windows Malicious Software Removal Tool x64 - v5.113 (KB890830)
Client Application ID : MoUpdateOrchestrator
Description : After the download, this tool runs one time to check your computer
for infection by specific, prevalent malicious software (including Blaster, Sasser,
and Mydoom) and helps remove any infection that is found. If an infection is found,
the tool will display a status report the next time that you start your computer. A
new version of the tool will be offered every month. If you want to manually run
the tool on your computer, you can download a copy from the Microsoft Download
Center, or you can run an online version from microsoft.com. This tool is not a
replacement for an antivirus product. To help protect your computer, you should use
an antivirus product.
================================================================================
==============
HotFix ID : KB5007651
Installed At (UTC) : 16-05-2023 05:27:15
Title : Update for Windows Security platform antimalware platform - KB5007651
(Version 1.0.2303.28002)
Client Application ID : MoUpdateOrchestrator
Description : This package will update Windows Security platform antimalware
platform's components on the user machine.
================================================================================
==============
HotFix ID : KB2267602
Installed At (UTC) : 16-05-2023 00:15:52
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.1441.0)
Client Application ID : Windows Defender
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
================================================================================
==============
HotFix ID : KB5025182
Installed At (UTC) : 14-05-2023 09:31:42
Title : 2023-04 Cumulative Update Preview for .NET Framework 3.5 and 4.8.1 for
Windows 11, version 22H2 for x64 (KB5025182)
Client Application ID : MoUpdateOrchestrator
Description : Install this update to resolve issues in Windows. For a complete
listing of the issues that are included in this update, see the associated
Microsoft Knowledge Base article for more information. After you install this item,
you may have to restart your computer.
================================================================================
==============
HotFix ID :
Installed At (UTC) : 14-05-2023 09:31:34
Title : Insyde Software - Firmware - 5.41.1.20
Client Application ID : MoUpdateOrchestrator
Description : Insyde Software Firmware driver update released in December 2021
================================================================================
==============
HotFix ID : KB5025182
Installed At (UTC) : 13-05-2023 13:05:40
Title : 2023-04 Cumulative Update Preview for .NET Framework 3.5 and 4.8.1 for
Windows 11, version 22H2 for x64 (KB5025182)
Client Application ID : MoUpdateOrchestrator
Description : Install this update to resolve issues in Windows. For a complete
listing of the issues that are included in this update, see the associated
Microsoft Knowledge Base article for more information. After you install this item,
you may have to restart your computer.
================================================================================
==============
HotFix ID :
Installed At (UTC) : 13-05-2023 13:05:40
Title : Insyde Software - Firmware - 5.41.1.20
Client Application ID : MoUpdateOrchestrator
Description : Insyde Software Firmware driver update released in December 2021
================================================================================
==============
HotFix ID : KB5026372
Installed At (UTC) : 13-05-2023 12:46:30
Title : 2023-05 Cumulative Update for Windows 11 Version 22H2 for x64-based Systems
```

```
(KB5026372)
Client Application ID : MoUpdateOrchestrator
Description : Install this update to resolve issues in Windows. For a complete
listing of the issues that are included in this update, see the associated
Microsoft Knowledge Base article for more information. After you install this item,
you may have to restart your computer.
================================================================================
==============
HotFix ID : KB5007651
Installed At (UTC) : 13-05-2023 12:30:30
Title : Update for Windows Security platform antimalware platform - KB5007651
(Version 1.0.2303.28002)
Client Application ID : MoUpdateOrchestrator
Description : This package will update Windows Security platform antimalware
platform's components on the user machine.
================================================================================
==============
HotFix ID : KB2267602
Installed At (UTC) : 13-05-2023 12:29:48
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.865.0)
Client Application ID : MoUpdateOrchestrator
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
================================================================================
==============
HotFix ID : KB4023057
Installed At (UTC) : 11-05-2023 04:56:04
Title : 2023-04 Update for Windows 11 Version 22H2 for x64-based Systems
(KB4023057)
Client Application ID : MoUpdateOrchestrator
Description : A security issue has been identified in a Microsoft software product
that could affect your system. You can help protect your system by installing this
update from Microsoft. For a complete listing of the issues that are included in
this update, see the associated Microsoft Knowledge Base article. After you install
this update, you may have to restart your system.
================================================================================
==============
HotFix ID :
Installed At (UTC) : 10-05-2023 02:45:34
Title : 9PKDZBMV1H3T-Microsoft.GetHelp
Client Application ID : Update;ScanForUpdates
Description : 9PKDZBMV1H3T-1152921505696240425
================================================================================
==============
HotFix ID :
Installed At (UTC) : 10-05-2023 02:16:55
Title : 9WZDNCRFJ3PT-MICROSOFT.ZUNEMUSIC
Client Application ID : Update;ScanForUpdates
Description : 9WZDNCRFJ3PT-1152921505696217949
================================================================================
==============
HotFix ID :
Installed At (UTC) : 10-05-2023 00:54:38
Title : 9PMMSR1CGPWG-Microsoft.HEIFImageExtension
Client Application ID : Update;ScanForUpdates
Description : 9PMMSR1CGPWG-1152921505696150909
================================================================================
==============
HotFix ID :
Installed At (UTC) : 10-05-2023 00:50:30
Title : 9NBLGGH4NNS1-Microsoft.DesktopAppInstaller
Client Application ID : Update;ScanForUpdates
Description : 9NBLGGH4NNS1-1152921505695813570
================================================================================
==============
HotFix ID :
Installed At (UTC) : 10-05-2023 00:49:01
Title : 9NG1H8B3ZC7M-Microsoft.MixedReality.Portal
Client Application ID : Update;ScanForUpdates
Description : 9NG1H8B3ZC7M-1152921505695703583
================================================================================
==============
HotFix ID :
Installed At (UTC) : 10-05-2023 00:48:57
Title : 9NZQPT0MWTD0-A278AB0D.Asphalt9
Client Application ID : Update;ScanForUpdates
Description : 9NZQPT0MWTD0-1152921505696127151
```

```
================================================================================
==============
HotFix ID :
Installed At (UTC) : 09-05-2023 23:50:30
Title : 9NSTH9KHZDLQ-Microsoft.UI.Xaml.2.8
Client Application ID : Update;ScanForUpdates
Description : 9NSTH9KHZDLQ-1152921505696266050
================================================================================
==============
HotFix ID : KB2267602
Installed At (UTC) : 09-05-2023 23:27:46
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.778.0)
Client Application ID : Windows Defender
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
================================================================================
==============
HotFix ID : KB4052623
Installed At (UTC) : 08-05-2023 22:29:32
Title : Update for Microsoft Defender Antivirus antimalware platform - KB4052623
(Version 4.18.2304.8)
Client Application ID : Windows Defender
Description : This package will update Microsoft Defender Antivirus antimalware
platform's components on the user machine.
================================================================================
==============
HotFix ID : KB2267602
Installed At (UTC) : 24-04-2023 23:39:58
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.387.2106.0)
Client Application ID : Windows Defender
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
================================================================================
==============
HotFix ID : KB2267602
Installed At (UTC) : 24-04-2023 00:03:14
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.387.2020.0)
Client Application ID : MoUpdateOrchestrator
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
================================================================================
==============
HotFix ID : KB2267602
Installed At (UTC) : 23-04-2023 21:58:40
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.387.2020.0)
Client Application ID : Windows Defender
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
================================================================================
==============
HotFix ID : KB2267602
Installed At (UTC) : 23-04-2023 21:58:29
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.387.2020.0)
Client Application ID : MoUpdateOrchestrator
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
================================================================================
==============
HotFix ID :
Installed At (UTC) : 22-04-2023 08:46:16
Title : 9WZDNCRFHVN5-MICROSOFT.WINDOWSCALCULATOR
Client Application ID : Update;ScanForUpdates
Description : 9WZDNCRFHVN5-1152921505695822217
================================================================================
==============
HotFix ID :
Installed At (UTC) : 22-04-2023 08:45:16
Title : 9N00JJ7S3L39-Microsoft.UI.Xaml.2.0
```

```
Client Application ID : Update;ScanForUpdates
Description : 9N00JJ7S3L39-115292150568837846
================================================================================
==============
HotFix ID :
Installed At (UTC) : 22-04-2023 08:45:15
Title : 9WZDNCRFJ3P2-MICROSOFT.ZUNEVIDEO
Client Application ID : Update;ScanForUpdates
Description : 9WZDNCRFJ3P2-115292150569582756 2
================================================================================
==============
HotFix ID :
Installed At (UTC) : 21-04-2023 05:05:27
Title : 9N00JJ7S3L39-Microsoft.UI.Xaml.2.0
Client Application ID : <<PROCESS>>: svchost.exe
Description : 9N00JJ7S3L39-115292150568837846
================================================================================
==============
HotFix ID : KB5025239
Installed At (UTC) : 21-04-2023 03:28:52
Title : 2023-04 Cumulative Update for Windows 11 Version 22H2 for x64-based Systems
(KB5025239)
Client Application ID : MoUpdateOrchestrator
Description : Install this update to resolve issues in Windows. For a complete
listing of the issues that are included in this update, see the associated
Microsoft Knowledge Base article for more information. After you install this item,
you may have to restart your computer.
================================================================================
==============
HotFix ID : KB890830
Installed At (UTC) : 21-04-2023 03:17:54
Title : Windows Malicious Software Removal Tool x64 - v5.112 (KB890830)
Client Application ID : MoUpdateOrchestrator
Description : After the download, this tool runs one time to check your computer
for infection by specific, prevalent malicious software (including Blaster, Sasser,
and Mydoom) and helps remove any infection that is found. If an infection is found,
the tool will display a status report the next time that you start your computer. A
new version of the tool will be offered every month. If you want to manually run
the tool on your computer, you can download a copy from the Microsoft Download
Center, or you can run an online version from microsoft.com. This tool is not a
replacement for an antivirus product. To help protect your computer, you should use
an antivirus product.
================================================================================
==============
HotFix ID : KB5012170
Installed At (UTC) : 21-04-2023 03:00:57
Title : 2022-08 Security Update for Windows 11 22H2 for x64-based Systems
(KB5012170)
Client Application ID : MoUpdateOrchestrator
Description : A security issue has been identified in a Microsoft software product
that could affect your system. You can help protect your system by installing this
update from Microsoft. For a complete listing of the issues that are included in
this update, see the associated Microsoft Knowledge Base article. After you install
this update, you may have to restart your system.
================================================================================
==============
HotFix ID : KB2267602
Installed At (UTC) : 21-04-2023 03:00:20
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.387.1619.0)
Client Application ID : MoUpdateOrchestrator
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
================================================================================
==============
HotFix ID : KB2267602
Installed At (UTC) : 20-04-2023 04:17:17
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.387.1643.0)
Client Application ID : Windows Defender
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
================================================================================
==============
HotFix ID : KB5007651
Installed At (UTC) : 20-04-2023 04:17:05
```

```
Title : Update for Microsoft Defender Antivirus antimalware platform - KB5007651
(Version 1.0.2303.27001)
Client Application ID : Windows Defender
Description : This package will update Microsoft Defender Antivirus antimalware
platform's components on the user machine.
================================================================================
==============
HotFix ID : KB4052623
Installed At (UTC) : 19-04-2023 02:47:26
Title : Update for Microsoft Defender Antivirus antimalware platform - KB4052623
(Version 4.18.2303.8)
Client Application ID : Windows Defender
Description : This package will update Microsoft Defender Antivirus antimalware
platform's components on the user machine.
================================================================================
==============
HotFix ID : KB4052623
Installed At (UTC) : 18-04-2023 23:06:47
Title : Update for Microsoft Defender Antivirus antimalware platform - KB4052623
(Version 4.18.2303.8)
Client Application ID : Windows Defender
Description : This package will update Microsoft Defender Antivirus antimalware
platform's components on the user machine.
================================================================================
==============
HotFix ID :
Installed At (UTC) : 18-04-2023 10:28:03
Title : Acer Incorporated - HIDClass - 1.0.0.10
Client Application ID : MoUpdateOrchestrator
Description : Acer Incorporated HIDClass driver update released in May 2022
================================================================================
==============
HotFix ID :
Installed At (UTC) : 18-04-2023 10:26:12
Title : Acer Incorporated - HIDClass - 1.0.0.10
Client Application ID : MoUpdateOrchestrator
Description : Acer Incorporated HIDClass driver update released in May 2022
================================================================================
==============
HotFix ID :
Installed At (UTC) : 18-04-2023 05:18:14
Title : Acer Incorporated - HIDClass - 1.0.0.10
Client Application ID : MoUpdateOrchestrator
Description : Acer Incorporated HIDClass driver update released in May 2022
================================================================================
==============
HotFix ID : KB5022497
Installed At (UTC) : 18-04-2023 03:54:44
Title : 2023-02 Cumulative Update for .NET Framework 3.5 and 4.8.1 for Windows 11,
version 22H2 for x64 (KB5022497)
Client Application ID : MoUpdateOrchestrator
Description : A security issue has been identified in a Microsoft software product
that could affect your system. You can help protect your system by installing this
update from Microsoft. For a complete listing of the issues that are included in
this update, see the associated Microsoft Knowledge Base article. After you install
this update, you may have to restart your system.
================================================================================
==============
HotFix ID : KB890830
Installed At (UTC) : 18-04-2023 03:53:43
Title : Windows Malicious Software Removal Tool x64 - v5.111 (KB890830)
Client Application ID : MoUpdateOrchestrator
Description : After the download, this tool runs one time to check your computer
for infection by specific, prevalent malicious software (including Blaster, Sasser,
and Mydoom) and helps remove any infection that is found. If an infection is found,
the tool will display a status report the next time that you start your computer. A
new version of the tool will be offered every month. If you want to manually run
the tool on your computer, you can download a copy from the Microsoft Download
Center, or you can run an online version from microsoft.com. This tool is not a
replacement for an antivirus product. To help protect your computer, you should use
an antivirus product.
================================================================================
==============
HotFix ID : KB5007651
Installed At (UTC) : 18-04-2023 03:38:24
Title : Update for Microsoft Defender Antivirus antimalware platform - KB5007651
(Version 1.0.2302.21002)
Client Application ID : MoUpdateOrchestrator
```

```
Description : This package will update Microsoft Defender Antivirus antimalware
platform's components on the user machine.
================================================================================
==============
HotFix ID :
Installed At (UTC) : 18-04-2023 03:37:26
Title : Acer Incorporated - HIDClass - 1.0.0.10
Client Application ID : MoUpdateOrchestrator
Description : Acer Incorporated HIDClass driver update released in May 2022
================================================================================
==============
HotFix ID : KB5007651
Installed At (UTC) : 18-04-2023 03:37:26
Title : Update for Microsoft Defender Antivirus antimalware platform - KB5007651
(Version 1.0.2302.21002)
Client Application ID : MoUpdateOrchestrator
Description : This package will update Microsoft Defender Antivirus antimalware
platform's components on the user machine.
================================================================================
==============
HotFix ID :
Installed At (UTC) : 18-04-2023 03:37:26
Title : Acer Incorporated - HIDClass - 1.0.0.10
Client Application ID : MoUpdateOrchestrator
Description : Acer Incorporated HIDClass driver update released in May 2022
================================================================================
==============
HotFix ID : KB5022497
Installed At (UTC) : 18-04-2023 03:37:26
Title : 2023-02 Cumulative Update for .NET Framework 3.5 and 4.8.1 for Windows 11,
version 22H2 for x64 (KB5022497)
Client Application ID : MoUpdateOrchestrator
Description : A security issue has been identified in a Microsoft software product
that could affect your system. You can help protect your system by installing this
update from Microsoft. For a complete listing of the issues that are included in
this update, see the associated Microsoft Knowledge Base article. After you install
this update, you may have to restart your system.
================================================================================
==============
HotFix ID : KB890830
Installed At (UTC) : 18-04-2023 03:37:26
Title : Windows Malicious Software Removal Tool x64 - v5.111 (KB890830)
Client Application ID : MoUpdateOrchestrator
Description : After the download, this tool runs one time to check your computer
for infection by specific, prevalent malicious software (including Blaster, Sasser,
and Mydoom) and helps remove any infection that is found. If an infection is found,
the tool will display a status report the next time that you start your computer. A
new version of the tool will be offered every month. If you want to manually run
the tool on your computer, you can download a copy from the Microsoft Download
Center, or you can run an online version from microsoft.com. This tool is not a
replacement for an antivirus product. To help protect your computer, you should use
an antivirus product.
================================================================================
==============
HotFix ID : KB5023706
Installed At (UTC) : 18-04-2023 03:37:25
Title : 2023-03 Cumulative Update for Windows 11 Version 22H2 for x64-based Systems
(KB5023706)
Client Application ID : MoUpdateOrchestrator
Description : Install this update to resolve issues in Windows. For a complete
listing of the issues that are included in this update, see the associated
Microsoft Knowledge Base article for more information. After you install this item,
you may have to restart your computer.
================================================================================
==============
HotFix ID : KB5007651
Installed At (UTC) : 18-04-2023 00:32:51
Title : Update for Microsoft Defender Antivirus antimalware platform - KB5007651
(Version 1.0.2302.21002)
Client Application ID : Windows Defender
Description : This package will update Microsoft Defender Antivirus antimalware
platform's components on the user machine.
================================================================================
==============
HotFix ID : KB5007651
Installed At (UTC) : 17-04-2023 22:28:42
Title : Update for Microsoft Defender Antivirus antimalware platform - KB5007651
(Version 1.0.2302.21002)
```

```
Client Application ID : Windows Defender
Description : This package will update Microsoft Defender Antivirus antimalware
platform's components on the user machine.
================================================================================
==============
HotFix ID : KB5007651
Installed At (UTC) : 17-04-2023 02:42:10
Title : Update for Microsoft Defender Antivirus antimalware platform - KB5007651
(Version 1.0.2302.21002)
Client Application ID : Windows Defender
Description : This package will update Microsoft Defender Antivirus antimalware
platform's components on the user machine.
================================================================================
==============
HotFix ID : KB5022497
Installed At (UTC) : 17-04-2023 02:28:18
Title : 2023-02 Cumulative Update for .NET Framework 3.5 and 4.8.1 for Windows 11,
version 22H2 for x64 (KB5022497)
Client Application ID : MoUpdateOrchestrator
Description : A security issue has been identified in a Microsoft software product
that could affect your system. You can help protect your system by installing this
update from Microsoft. For a complete listing of the issues that are included in
this update, see the associated Microsoft Knowledge Base article. After you install
this update, you may have to restart your system.
================================================================================
==============
HotFix ID : KB890830
Installed At (UTC) : 17-04-2023 02:28:17
Title : Windows Malicious Software Removal Tool x64 - v5.111 (KB890830)
Client Application ID : MoUpdateOrchestrator
Description : After the download, this tool runs one time to check your computer
for infection by specific, prevalent malicious software (including Blaster, Sasser,
and Mydoom) and helps remove any infection that is found. If an infection is found,
the tool will display a status report the next time that you start your computer. A
new version of the tool will be offered every month. If you want to manually run
the tool on your computer, you can download a copy from the Microsoft Download
Center, or you can run an online version from microsoft.com. This tool is not a
replacement for an antivirus product. To help protect your computer, you should use
an antivirus product.
================================================================================
==============
HotFix ID : KB5007651
Installed At (UTC) : 17-04-2023 02:28:14
Title : Update for Microsoft Defender Antivirus antimalware platform - KB5007651
(Version 1.0.2302.21002)
Client Application ID : MoUpdateOrchestrator
Description : This package will update Microsoft Defender Antivirus antimalware
platform's components on the user machine.
================================================================================
==============
HotFix ID :
Installed At (UTC) : 17-04-2023 02:28:11
Title : Acer Incorporated - HIDClass - 1.0.0.10
Client Application ID : MoUpdateOrchestrator
Description : Acer Incorporated HIDClass driver update released in May 2022
================================================================================
==============
HotFix ID :
Installed At (UTC) : 17-04-2023 02:25:28
Title : Acer Incorporated - HIDClass - 1.0.0.10
Client Application ID : MoUpdateOrchestrator
Description : Acer Incorporated HIDClass driver update released in May 2022
================================================================================
==============
HotFix ID : KB5007651
Installed At (UTC) : 17-04-2023 02:25:28
Title : Update for Microsoft Defender Antivirus antimalware platform - KB5007651
(Version 1.0.2302.21002)
Client Application ID : MoUpdateOrchestrator
Description : This package will update Microsoft Defender Antivirus antimalware
platform's components on the user machine.
================================================================================
==============
HotFix ID : KB5023706
Installed At (UTC) : 17-04-2023 02:25:27
Title : 2023-03 Cumulative Update for Windows 11 Version 22H2 for x64-based Systems
(KB5023706)
Client Application ID : MoUpdateOrchestrator
```

```
Description : Install this update to resolve issues in Windows. For a complete
listing of the issues that are included in this update, see the associated
Microsoft Knowledge Base article for more information. After you install this item,
you may have to restart your computer.
================================================================================
==============
HotFix ID : KB5022497
Installed At (UTC) : 17-04-2023 02:25:26
Title : 2023-02 Cumulative Update for .NET Framework 3.5 and 4.8.1 for Windows 11,
version 22H2 for x64 (KB5022497)
Client Application ID : MoUpdateOrchestrator
Description : A security issue has been identified in a Microsoft software product
that could affect your system. You can help protect your system by installing this
update from Microsoft. For a complete listing of the issues that are included in
this update, see the associated Microsoft Knowledge Base article. After you install
this update, you may have to restart your system.
================================================================================
==============
HotFix ID : KB890830
Installed At (UTC) : 17-04-2023 02:25:26
Title : Windows Malicious Software Removal Tool x64 - v5.111 (KB890830)
Client Application ID : MoUpdateOrchestrator
Description : After the download, this tool runs one time to check your computer
for infection by specific, prevalent malicious software (including Blaster, Sasser,
and Mydoom) and helps remove any infection that is found. If an infection is found,
the tool will display a status report the next time that you start your computer. A
new version of the tool will be offered every month. If you want to manually run
the tool on your computer, you can download a copy from the Microsoft Download
Center, or you can run an online version from microsoft.com. This tool is not a
replacement for an antivirus product. To help protect your computer, you should use
an antivirus product.
================================================================================
==============
HotFix ID : KB5022497
Installed At (UTC) : 17-04-2023 02:20:46
Title : 2023-02 Cumulative Update for .NET Framework 3.5 and 4.8.1 for Windows 11,
version 22H2 for x64 (KB5022497)
Client Application ID : MoUpdateOrchestrator
Description : A security issue has been identified in a Microsoft software product
that could affect your system. You can help protect your system by installing this
update from Microsoft. For a complete listing of the issues that are included in
this update, see the associated Microsoft Knowledge Base article. After you install
this update, you may have to restart your system.
================================================================================
==============
HotFix ID : KB5022497
Installed At (UTC) : 17-04-2023 02:20:46
Title : 2023-02 Cumulative Update for .NET Framework 3.5 and 4.8.1 for Windows 11,
version 22H2 for x64 (KB5022497)
Client Application ID : MoUpdateOrchestrator
Description : A security issue has been identified in a Microsoft software product
that could affect your system. You can help protect your system by installing this
update from Microsoft. For a complete listing of the issues that are included in
this update, see the associated Microsoft Knowledge Base article. After you install
this update, you may have to restart your system.
================================================================================
==============
HotFix ID : KB5007651
Installed At (UTC) : 16-04-2023 22:32:27
Title : Update for Microsoft Defender Antivirus antimalware platform - KB5007651
(Version 1.0.2302.21002)
Client Application ID : Windows Defender
Description : This package will update Microsoft Defender Antivirus antimalware
platform's components on the user machine.
================================================================================
==============
HotFix ID :
Installed At (UTC) : 30-03-2023 00:43:01
Title : 9NKSQGP7F2NH-5319275A.WhatsAppDesktop
Client Application ID : Update;
Description : 9NKSQGP7F2NH-1152921505696089938
================================================================================
==============
HotFix ID :
Installed At (UTC) : 30-03-2023 00:12:08
Title : 9N00JJ7S3L39-Microsoft.UI.Xaml.2.0
Client Application ID : <<PROCESS>>: svchost.exe
Description : 9N00JJ7S3L39-1152921505688378846
```

```
==================================================================================
===============
HotFix ID :
Installed At (UTC) : 30-03-2023 00:12:08
Title : 9N00JJ7S3L39-Microsoft.UI.Xaml.2.0
Client Application ID : <<PROCESS>>: svchost.exe
Description : 9N00JJ7S3L39-1152921505688378846
==================================================================================
===============
HotFix ID :
Installed At (UTC) : 30-03-2023 00:12:08
Title : 9N00JJ7S3L39-Microsoft.UI.Xaml.2.0
Client Application ID : <<PROCESS>>: svchost.exe
Description : 9N00JJ7S3L39-1152921505688378846
==================================================================================
===============
HotFix ID :
Installed At (UTC) : 30-03-2023 00:12:08
Title : 9N00JJ7S3L39-Microsoft.UI.Xaml.2.0
Client Application ID : <<PROCESS>>: svchost.exe
Description : 9N00JJ7S3L39-1152921505688378846
==================================================================================
===============
HotFix ID :
Installed At (UTC) : 29-03-2023 23:41:45
Title : 9NKSQGP7F2NH-5319275A.WhatsAppDesktop
Client Application ID : Update;
Description : 9NKSQGP7F2NH-1152921505696089938
==================================================================================
===============
HotFix ID : KB2267602
Installed At (UTC) : 27-03-2023 07:59:16
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.383.770.0)
Client Application ID : MoUpdateOrchestrator
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
==================================================================================
===============
HotFix ID : KB4023057
Installed At (UTC) : 04-03-2023 00:44:52
Title : 2023-01 Update for Windows 11 Version 22H2 for x64-based Systems
(KB4023057)
Client Application ID : MoUpdateOrchestrator
Description : A security issue has been identified in a Microsoft software product
that could affect your system. You can help protect your system by installing this
update from Microsoft. For a complete listing of the issues that are included in
this update, see the associated Microsoft Knowledge Base article. After you install
this update, you may have to restart your system.
==================================================================================
===============
HotFix ID : KB2267602
Installed At (UTC) : 26-02-2023 02:03:04
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.383.657.0)
Client Application ID : Windows Defender
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
==================================================================================
===============
HotFix ID : KB2267602
Installed At (UTC) : 19-02-2023 20:37:28
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.383.280.0)
Client Application ID : Windows Defender
Description : Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed
this item, it cannot be removed.
==================================================================================
===============
HotFix ID : KB4052623
Installed At (UTC) : 19-02-2023 20:27:09
Title : Update for Microsoft Defender Antivirus antimalware platform - KB4052623
(Version 4.18.2301.6)
Client Application ID : Windows Defender
Description : This package will update Microsoft Defender Antivirus antimalware
```

```
platform's components on the user machine.
================================================================================
===============
HotFix ID : KB5022303
Installed At (UTC) : 09-02-2023 14:26:04
Title : 2023-01 Cumulative Update for Windows 11 Version 22H2 for x64-based Systems
(KB5022303)
Client Application ID : TrustedInstaller FOD Enumerate
Description : Install this update to resolve issues in Windows. For a complete
listing of the issues that are included in this update, see the associated
Microsoft Knowledge Base article for more information. After you install this item,
you may have to restart your computer.
================================================================================
===============
HotFix ID :
Installed At (UTC) : 08-02-2023 05:01:03
Title :
Client Application ID : MoUpdateOrchestrator
Description :
================================================================================
===============
HotFix ID :
Installed At (UTC) : 07-02-2023 23:09:35
Title : 9PDXGNCFSCZV-CanonicalGroupLimited.Ubuntu
Client Application ID : Acquisition;Microsoft.WindowsStore_8wekyb3d8bbwe
Description : 9PDXGNCFSCZV-1152921505695746407
================================================================================
===============
HotFix ID :
Installed At (UTC) : 05-02-2023 12:06:35
Title : Windows 11, version 22H2
Client Application ID : MoUpdateOrchestrator
Description : Install the latest version of Windows: Windows 11, version 22H2.
================================================================================
===============
```

User Environment Variables

Check for some passwords or keys in the env variables

```
SystemDrive: C:
ProgramFiles(x86): C:\Program Files (x86)
ProgramW6432: C:\Program Files
PROCESSOR_IDENTIFIER: AMD64 Family 23 Model 24 Stepping 1, AuthenticAMD
TMP: C:\Users\MOHANA~1\AppData\Local\Temp
PROCESSOR_ARCHITECTURE: AMD64
VSCODE_GIT_ASKPASS_MAIN: c:\Users\MOHANAPRASAD\AppData\Local\Programs\Microsoft VS
Code\resources\app\extensions\git\dist\askpass-main.js
Path: C:\Program Files\Common Files\Oracle\Java\javapath;C:\WINDOWS\system32;C:\WI
NDOWS;C:\WINDOWS\System32\Wbem;C:\WINDOWS\System32\WindowsPowerShell\v1.0\;C:\WIND
OWS\System32\OpenSSH\;C:\Program Files\nodejs\;C:\Program Files\Git\cmd;C:\Program
Files\MySQL\MySQL Shell 8.0\bin\;C:\Users\MOHANAPRASAD\AppData\Local\Programs\Pyth
on\Python311\Scripts\;C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python31
1\;C:\Users\MOHANAPRASAD\anaconda3;C:\Users\MOHANAPRASAD\anaconda3\Library\mingw-w
64\bin;C:\Users\MOHANAPRASAD\anaconda3\Library\usr\bin;C:\Users\MOHANAPRASAD\anaco
nda3\Library\bin;C:\Users\MOHANAPRASAD\anaconda3\Scripts;C:\Users\MOHANAPRASAD\App
Data\Local\Microsoft\WindowsApps;C:\Users\MOHANAPRASAD\AppData\Local\GitHubDesktop
\bin;C:\Users\MOHANAPRASAD\AppData\Local\Programs\Microsoft VS
Code\bin;C:\Users\MOHANAPRASAD\AppData\Roaming\npm;C:\Program Files
(x86)\Nmap;C:\Program Files\OWASP\Zed Attack Proxy;
VSCODE_GIT_IPC_HANDLE: \\.\pipe\vscode-git-c042045146-sock
PROCESSOR_REVISION: 1801
TEMP: C:\Users\MOHANA~1\AppData\Local\Temp
USERPROFILE: C:\Users\MOHANAPRASAD
CommonProgramFiles(x86): C:\Program Files (x86)\Common Files
LOGONSERVER: \\LAPTOP-9R1PMVC2
USERNAME: MOHANAPRASAD
SystemRoot: C:\WINDOWS
CHROME_CRASHPAD_PIPE_NAME: \\.\pipe\LOCAL\crashpad_20056_KJRXDEABMRDHQXQF
OS: Windows_NT
OneDrive: C:\Users\MOHANAPRASAD\OneDrive
UIPATH_USER_SERVICE_PATH: C:\Program
Files\UiPath\Studio\UiPath.Service.UserHost.exe
CommonProgramFiles: C:\Program Files\Common Files
ProgramData: C:\ProgramData
```

```
LANG: en_US.UTF-8
GIT_ASKPASS: c:\Users\MOHANAPRASAD\AppData\Local\Programs\Microsoft VS
Code\resources\app\extensions\git\dist\askpass.sh
HOMEPATH: \Users\MOHANAPRASAD
OneDriveConsumer: C:\Users\MOHANAPRASAD\OneDrive
COMPUTERNAME: LAPTOP-9R1PMVC2
ALLUSERSPROFILE: C:\ProgramData
CommonProgramW6432: C:\Program Files\Common Files
VSCODE_NONCE: eab6a8e4-6a09-4f31-b80e-e06e27492099
SESSIONNAME: Console
DriverData: C:\Windows\System32\Drivers\DriverData
HOMEDRIVE: C:
windir: C:\WINDOWS
VSCODE_GIT_ASKPASS_NODE: C:\Users\MOHANAPRASAD\AppData\Local\Programs\Microsoft VS
Code\Code.exe
NUMBER_OF_PROCESSORS: 8
UIPATH_LANGUAGE: en
VBOX_HWVIRTEX_IGNORE_SVM_IN_USE: 1
ProgramFiles: C:\Program Files
ComSpec: C:\WINDOWS\system32\cmd.exe
ORIGINAL_XDG_CURRENT_DESKTOP: undefined
PATHEXT: .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC;.CPL
PSModulePath:
C:\Users\MOHANAPRASAD\OneDrive\Documents\WindowsPowerShell\Modules;C:\Program
Files\WindowsPowerShell\Modules;C:\WINDOWS\system32\WindowsPowerShell\v1.0\Modules
PROMPT: $P$G
VSCODE_INJECTION: 1
APPDATA: C:\Users\MOHANAPRASAD\AppData\Roaming
USERDOMAIN: LAPTOP-9R1PMVC2
PROCESSOR_LEVEL: 23
LOCALAPPDATA: C:\Users\MOHANAPRASAD\AppData\Local
TERM_PROGRAM_VERSION: 1.81.0
USERDOMAIN_ROAMINGPROFILE: LAPTOP-9R1PMVC2
COLORTERM: truecolor
EFC_7448: 1
PUBLIC: C:\Users\Public
TERM_PROGRAM: vscode
VSCODE_GIT_ASKPASS_EXTRA_ARGS: --ms-enable-electron-run-as-node
```

System Environment Variables

Check for some passwords or keys in the env variables

```
ComSpec: C:\WINDOWS\system32\cmd.exe
DriverData: C:\Windows\System32\Drivers\DriverData
OS: Windows_NT
Path: C:\Program Files\Common Files\Oracle\Java\javapath;C:\WINDOWS\system32;C:\WI
NDOWS;C:\WINDOWS\System32\Wbem;C:\WINDOWS\System32\WindowsPowerShell\v1.0\;C:\WIND
OWS\System32\OpenSSH\;C:\Program Files\nodejs\;C:\Program Files\Git\cmd
PATHEXT: .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
PROCESSOR_ARCHITECTURE: AMD64
PSModulePath: C:\Program
Files\WindowsPowerShell\Modules;C:\WINDOWS\system32\WindowsPowerShell\v1.0\Modules
TEMP: C:\WINDOWS\TEMP
TMP: C:\WINDOWS\TEMP
USERNAME: SYSTEM
windir: C:\WINDOWS
VBOX_HWVIRTEX_IGNORE_SVM_IN_USE: 1
UIPATH_LANGUAGE: en
UIPATH_USER_SERVICE_PATH: C:\Program
Files\UiPath\Studio\UiPath.Service.UserHost.exe
NUMBER_OF_PROCESSORS: 8
PROCESSOR_LEVEL: 23
PROCESSOR_IDENTIFIER: AMD64 Family 23 Model 24 Stepping 1, AuthenticAMD
PROCESSOR_REVISION: 1801
```

Credentials Guard

If enabled, a driver is needed to read LSASS memory https://book.hacktricks.xyz/windows-hardening/stealing-credentials/credentials-protections#credential-guard

```
CredentialGuard is not enabled
Virtualization Based Security Status: Not enabled
Configured: False
Running: False
```

AV Information

```
Some AV was detected, search for bypasses
Name: Norton Security Ultra
ProductEXE: C:\Program Files\Norton Security\Engine\22.21.5.44\WSCStub.exe
pathToSignedReportingExe: C:\Program Files\Norton
Security\Engine\22.21.5.44\nsWscSvc.exe
```

UAC Status

If you are in the Administrators group check how to bypass the UAC https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#basic-uac-bypass-full-file-system-access

```
ConsentPromptBehaviorAdmin: 5 - PromptForNonWindowsBinaries
EnableLUA: 1
LocalAccountTokenFilterPolicy:
FilterAdministratorToken:
[*] LocalAccountTokenFilterPolicy set to 0 and FilterAdministratorToken != 1.
[-] Only the RID-500 local admin account can be used for lateral movement.
```

PowerShell Settings

```
PowerShell v2 Version: 2.0
PowerShell v5 Version: 5.1.22621.1
PowerShell Core Version:
Transcription Settings:
Module Logging Settings:
Scriptblock Logging Settings:
PS history file: C:\Users\MOHANAPRASAD\AppData\Roaming\Microsoft\Windows\PowerShel
l\PSReadLine\ConsoleHost_history.txt
PS history size: 3538B
```

HKCU Internet Settings

```
CertificateRevocation: 1
DisableCachingOfSSLPages: 0
IE5_UA_Backup_Flag: 5.0
PrivacyAdvanced: 1
SecureProtocols: 10240
EnableNegotiate: 1
MigrateProxy: 1
ProxyEnable: 0
User Agent: Mozilla/4.0 (compatible; MSIE 8.0; Win32)
ZonesSecurityUpgrade: System.Byte[]
WarnonZoneCrossing: 0
LockDatabase: 133200923033334507
EnableHttp1_1: 1
```

HKLM Internet Settings

```
ActiveXCache: C:\Windows\Downloaded Program Files
CodeBaseSearchPath: CODEBASE
EnablePunycode: 1
MinorVersion: 0
WarnOnIntranet: 1
```

Drives Information

Remember that you should search more info inside the other drives

```
C:\ (Type: Fixed)(Volume label: Acer)(Filesystem: NTFS)(Available space: 32
GB)(Permissions: Authenticated Users [AppendData/CreateDirectories])
D:\ (Type: Fixed)(Volume label: New Volume)(Filesystem: NTFS)(Available space: 169
GB)(Permissions: Authenticated Users [WriteData/CreateFiles])
E:\ (Type: Fixed)(Volume label: New Volume)(Filesystem: NTFS)(Available space: 8
GB)(Permissions: Authenticated Users [WriteData/CreateFiles])
```

Enumerate LSA settings - auth packages included

```
auditbasedirectories : 0
auditbaseobjects : 0
Authentication Packages : msv1_0
Bounds : 00-30-00-00-00-20-00-00
crashonauditfail : 0
fullprivilegeauditing : 00
LimitBlankPasswordUse : 1
NoLmHash : 1
Notification Packages : scecli
Security Packages : ""
disabledomaincreds : 0
everyoneincludesanonymous : 0
forceguest : 0
LsaPid : 1220
ProductType : 3
restrictanonymous : 0
restrictanonymoussam : 1
SecureBoot : 1
```

Enumerating NTLM Settings

```
LanmanCompatibilityLevel : (Send NTLMv2 response only - Win7+ default)
NTLM Signing Settings
ClientRequireSigning : False
ClientNegotiateSigning : True
ServerRequireSigning : False
ServerNegotiateSigning : False
LdapSigning : Negotiate signing (Negotiate signing)
Session Security
NTLMMinClientSec : 536870912 (Require 128-bit encryption)
NTLMMinServerSec : 536870912 (Require 128-bit encryption)
NTLM Auditing and Restrictions
InboundRestrictions : (Not defined)
OutboundRestrictions : (Not defined)
InboundAuditing : (Not defined)
OutboundExceptions :
```

Enumerating Printers (WMI)

```
Name: OneNote for Windows 10
Status: Unknown
```

```
Sddl: O:SYD:(A;CIIO;RC;;;CO)(A;OIIO;RPWPSDRCWDWO;;;CO)(A;;SWRC;;;AC)(A;CIIO;RC;;;A
C)(A;OIIO;RPWPSDRCWDWO;;;AC)(A;;SWRC;;;S-1-15-3-1024-4044835139-2658482041-3127973
164-329287231-3865880861-1938685643-461067658-1087000422)(A;CIIO;RC;;;S-1-15-3-102
4-4044835139-2658482041-3127973164-329287231-3865880861-1938685643-461067658-10870
00422)(A;OIIO;RPWPSDRCWDWO;;;S-1-15-3-1024-4044835139-2658482041-3127973164-329287
231-3865880861-1938685643-461067658-1087000422)(A;OIIO;RPWPSDRCWDWO;;;S-1-5-21-259
9125077-3711717779-1984677719-1001)(A;;LCSWSDRCWDWO;;;S-1-5-21-2599125077-37117177
79-1984677719-1001)(A;OIIO;RPWPSDRCWDWO;;;LS)(A;;LCSWSDRCWDWO;;;LS)(A;OIIO;RPWPSDR
CWDWO;;;BA)(A;;LCSWSDRCWDWO;;;BA)
Is default: False
Is network printer: False
================================================================================
===============
Name: Microsoft XPS Document Writer
Status: Unknown
Sddl: O:SYD:(A;;LCSWSDRCWDWO;;;S-1-5-21-2599125077-3711717779-1984677719-1000)(A;O
IIO;RPWPSDRCWDWO;;;S-1-5-21-2599125077-3711717779-1984677719-1000)(A;OIIO;GA;;;CO)
(A;OIIO;GA;;;AC)(A;;SWRC;;;WD)(A;CIIO;GX;;;WD)(A;;SWRC;;;AC)(A;CIIO;GX;;;AC)(A;;LC
SWDTSDRCWDWO;;;BA)(A;OICIIO;GA;;;BA)(A;OIIO;GA;;;S-1-15-3-1024-4044835139-26584820
41-3127973164-329287231-3865880861-1938685643-461067658-1087000422)(A;;SWRC;;;S-1-
15-3-1024-4044835139-2658482041-3127973164-329287231-3865880861-1938685643-4610676
58-1087000422)(A;CIIO;GX;;;S-1-15-3-1024-4044835139-2658482041-3127973164-32928723
1-3865880861-1938685643-461067658-1087000422)
Is default: False
Is network printer: False
================================================================================
===============
Name: Microsoft Print to PDF
Status: Unknown
Sddl: O:SYD:(A;;LCSWSDRCWDWO;;;S-1-5-21-2599125077-3711717779-1984677719-1000)(A;O
IIO;RPWPSDRCWDWO;;;S-1-5-21-2599125077-3711717779-1984677719-1000)(A;OIIO;GA;;;CO)
(A;OIIO;GA;;;AC)(A;;SWRC;;;WD)(A;CIIO;GX;;;WD)(A;;SWRC;;;AC)(A;CIIO;GX;;;AC)(A;;LC
SWDTSDRCWDWO;;;BA)(A;OICIIO;GA;;;BA)(A;OIIO;GA;;;S-1-15-3-1024-4044835139-26584820
41-3127973164-329287231-3865880861-1938685643-461067658-1087000422)(A;;SWRC;;;S-1-
15-3-1024-4044835139-2658482041-3127973164-329287231-3865880861-1938685643-4610676
58-1087000422)(A;CIIO;GX;;;S-1-15-3-1024-4044835139-2658482041-3127973164-32928723
1-3865880861-1938685643-461067658-1087000422)
Is default: True
Is network printer: False
================================================================================
===============
Name: Hewlett-Packard HP LaserJet M1005
Status: Unknown
Sddl: O:SYD:(A;OIIO;GA;;;CO)(A;OIIO;GA;;;AC)(A;;SWRC;;;WD)(A;CIIO;GX;;;WD)(A;;SWRC
;;;AC)(A;CIIO;GX;;;AC)(A;;LCSWDTSDRCWDWO;;;BA)(A;OICIIO;GA;;;BA)(A;OIIO;GA;;;S-1-1
5-3-1024-4044835139-2658482041-3127973164-329287231-3865880861-1938685643-46106765
8-1087000422)(A;;SWRC;;;S-1-15-3-1024-4044835139-2658482041-3127973164-329287231-3
865880861-1938685643-461067658-1087000422)(A;CIIO;GX;;;S-1-15-3-1024-4044835139-26
58482041-3127973164-329287231-3865880861-1938685643-461067658-1087000422)
Is default: False
Is network printer: False
================================================================================
===============
Name: Fax
Status: Unknown
Sddl: O:SYD:(A;;LCSWSDRCWDWO;;;S-1-5-21-2599125077-3711717779-1984677719-1000)(A;O
IIO;RPWPSDRCWDWO;;;S-1-5-21-2599125077-3711717779-1984677719-1000)(A;OIIO;GA;;;CO)
(A;OIIO;GA;;;AC)(A;;SWRC;;;WD)(A;CIIO;GX;;;WD)(A;;SWRC;;;AC)(A;CIIO;GX;;;AC)(A;;LC
SWDTSDRCWDWO;;;BA)(A;OICIIO;GA;;;BA)(A;OIIO;GA;;;S-1-15-3-1024-4044835139-26584820
41-3127973164-329287231-3865880861-1938685643-461067658-1087000422)(A;;SWRC;;;S-1-
15-3-1024-4044835139-2658482041-3127973164-329287231-3865880861-1938685643-4610676
58-1087000422)(A;CIIO;GX;;;S-1-15-3-1024-4044835139-2658482041-3127973164-32928723
1-3865880861-1938685643-461067658-1087000422)
Is default: False
Is network printer: False
================================================================================
===============
```

Enumerating Named Pipes

```
Name CurrentUserPerms Sddl
BraveSoftwareCrashServices\S-1-5-18
O:SYG:SYD:(A;;FR;;;WD)(A;;FR;;;AN)(A;;FA;;;SY)(A;;FA;;;BA)
```

```
BraveSoftwareCrashServices\S-1-5-18-x64
O:SYG:SYD:(A;;FR;;;WD)(A;;FR;;;AN)(A;;FA;;;SY)(A;;FA;;;BA)
eventlog Everyone [WriteData/CreateFiles] O:LSG:LSD:P(A;;0x12019b;;;WD)(A;;CC;;;OW
)(A;;0x12008f;;;S-1-5-80-880578595-1860270145-482643319-2788375705-1540778122)
ExtEventPipe_Service Everyone [AllAccess] O:BAG:SY
GoogleCrashServices\S-1-5-18
O:SYG:SYD:(A;;FR;;;WD)(A;;FR;;;AN)(A;;FA;;;SY)(A;;FA;;;BA)
GoogleCrashServices\S-1-5-18-x64
O:SYG:SYD:(A;;FR;;;WD)(A;;FR;;;AN)(A;;FA;;;SY)(A;;FA;;;BA)
LOCAL\crashpad_20056_KJRXDEABMRDHQXQF MOHANAPRASAD [AllAccess] O:S-1-5-21-25991250
77-3711717779-1984677719-1001G:S-1-5-21-2599125077-3711717779-1984677719-513D:(A;;
FA;;;SY)(A;;FA;;;S-1-5-21-2599125077-3711717779-1984677719-1001)(A;;0x12019f;;;AC)
LOCAL\crashpad_22640_PQTOASDRQXOYXGAW MOHANAPRASAD [AllAccess] O:S-1-5-21-25991250
77-3711717779-1984677719-1001G:S-1-5-21-2599125077-3711717779-1984677719-513D:(A;;
FA;;;SY)(A;;FA;;;S-1-5-21-2599125077-3711717779-1984677719-1001)(A;;0x12019f;;;AC)
LOCAL\mojo.external_task_manager_21796 O:S-1-5-21-2599125077-3711717779-1984677719
-1001G:S-1-5-21-2599125077-3711717779-1984677719-513D:(A;;FA;;;OW)(A;;FA;;;SY)(A;;
FA;;;BA)
LOCAL\S-1-5-5-0-164728407-Teams-2.0-instance-pipe MOHANAPRASAD [AllAccess] O:S-1-5
-21-2599125077-3711717779-1984677719-1001G:S-1-5-21-2599125077-3711717779-19846777
19-513D:(A;;FR;;;WD)(A;;FR;;;AN)(A;;FA;;;SY)(A;;FA;;;BA)(A;;FA;;;S-1-5-21-25991250
77-3711717779-1984677719-1001)
ProtectedPrefix\LocalService\FTHPIPE Interactive [WriteData/CreateFiles]
O:LSG:LSD:P(A;;0x12019f;;;IU)(A;;FA;;;LS)
ROUTER Everyone [WriteData/CreateFiles]
O:SYG:SYD:P(A;;0x12019b;;;WD)(A;;0x12019b;;;AN)(A;;FA;;;SY)
```

Enumerating AMSI registered providers

```
Provider: {2781761E-28E0-4109-99FE-B9D127C57AFE}
Path: "C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.23050.9-0\MpOav.dll"
================================================================================
==============
Provider: {96237786-C89D-4504-837A-A3BA2C29524D}
Path: C:\Program Files\Norton Security\Engine\22.23.4.6\symamsi.dll
================================================================================
==============
```

Interesting Events information

Displaying Power off/on events for last 5 days

```
08-08-2023 14:05:51 : Awake
08-08-2023 13:29:00 : Sleep
08-08-2023 13:28:28 : Awake
08-08-2023 13:27:35 : Sleep
08-08-2023 12:33:24 : Awake
08-08-2023 12:33:05 : Sleep
08-08-2023 12:18:40 : Awake
08-08-2023 12:15:44 : Sleep
08-08-2023 11:37:48 : Awake
08-08-2023 11:32:56 : Sleep
08-08-2023 09:52:42 : Awake
08-08-2023 09:16:27 : Sleep
08-08-2023 09:12:41 : Awake
08-08-2023 00:10:30 : Sleep
07-08-2023 22:15:09 : Awake
07-08-2023 21:20:22 : Sleep
07-08-2023 21:00:58 : Awake
07-08-2023 20:50:04 : Sleep
07-08-2023 18:33:05 : Awake
07-08-2023 17:35:27 : Sleep
07-08-2023 17:34:55 : Awake
07-08-2023 17:34:26 : Sleep
```

```
07-08-2023 15:28:08 : Awake
07-08-2023 12:15:01 : Sleep
07-08-2023 12:09:10 : Awake
07-08-2023 09:25:29 : Sleep
07-08-2023 09:22:58 : Awake
07-08-2023 02:08:17 : Sleep
07-08-2023 00:47:52 : Awake
06-08-2023 23:43:47 : Sleep
06-08-2023 23:28:51 : Awake
06-08-2023 22:39:59 : Sleep
06-08-2023 22:16:03 : Awake
06-08-2023 22:12:35 : Sleep
06-08-2023 22:00:51 : Awake
06-08-2023 22:00:18 : Sleep
06-08-2023 21:44:09 : Awake
06-08-2023 21:41:25 : Sleep
06-08-2023 21:11:16 : Awake
05-08-2023 21:14:23 : Awake
05-08-2023 21:14:22 : Sleep
05-08-2023 18:14:21 : Sleep
05-08-2023 18:04:39 : Awake
05-08-2023 15:33:29 : Sleep
05-08-2023 14:36:04 : Awake
05-08-2023 14:35:45 : Sleep
05-08-2023 14:19:54 : Awake
05-08-2023 13:50:50 : Sleep
05-08-2023 12:37:43 : Awake
05-08-2023 12:21:34 : Sleep
05-08-2023 04:45:39 : Awake
04-08-2023 21:17:51 : Awake
04-08-2023 21:17:50 : Sleep
04-08-2023 18:17:49 : Sleep
04-08-2023 16:25:14 : Awake
04-08-2023 16:25:09 : Sleep
04-08-2023 15:23:16 : Awake
04-08-2023 10:55:24 : Sleep
04-08-2023 10:52:33 : Awake
04-08-2023 09:14:32 : Sleep
04-08-2023 08:57:01 : Awake
04-08-2023 08:52:07 : Sleep
04-08-2023 08:46:49 : Awake
04-08-2023 08:44:00 : Sleep
04-08-2023 08:29:55 : Awake
04-08-2023 08:29:08 : Sleep
04-08-2023 07:52:58 : Awake
04-08-2023 07:52:49 : Sleep
04-08-2023 07:48:37 : Startup
04-08-2023 10:03:58 : Shutdown
04-08-2023 09:48:20 : Unexpected Shutdown
04-08-2023 09:48:11 : Startup
04-08-2023 09:36:19 : Awake
03-08-2023 23:04:03 : Sleep
03-08-2023 22:38:39 : Awake
03-08-2023 20:44:31 : Awake
03-08-2023 20:44:30 : Sleep
03-08-2023 17:44:28 : Sleep
03-08-2023 17:02:32 : Awake
03-08-2023 16:10:08 : Sleep
03-08-2023 15:01:11 : Awake
```

Users Information

Users

Check if you have some admin equivalent privileges https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#users-and-groups

```
Current user: MOHANAPRASAD
Current groups: Domain Users, Everyone, Users, Interactive, Console Logon,
Authenticated Users, This Organization, Local account, Local, NTLM Authentication
================================================================================
===============
LAPTOP-9R1PMVC2\Administrator(Disabled): Built-in account for administering the
computer/domain
|->Groups: Administrators
|->Password: CanChange-NotExpi-Req
LAPTOP-9R1PMVC2\DefaultAccount(Disabled): A user account managed by the system.
|->Groups: System Managed Accounts Group
|->Password: CanChange-NotExpi-NotReq
LAPTOP-9R1PMVC2\Guest(Disabled): Built-in account for guest access to the
computer/domain
|->Groups: Guests
|->Password: NotChange-NotExpi-NotReq
LAPTOP-9R1PMVC2\MOHANAPRASAD
|->Groups: Administrators
|->Password: CanChange-NotExpi-NotReq
LAPTOP-9R1PMVC2\WDAGUtilityAccount(Disabled): A user account managed and used by
the system for Windows Defender Application Guard scenarios.
|->Password: CanChange-Expi-Req
```

Current User Idle Time

```
Current User : LAPTOP-9R1PMVC2\MOHANAPRASAD
Idle Time : 00h:00m:00s:156ms
```

Current Token privileges

Check if you can escalate privilege using some enabled token https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#token-manipulation

```
SeShutdownPrivilege: DISABLED
SeChangeNotifyPrivilege: SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED
SeUndockPrivilege: DISABLED
SeIncreaseWorkingSetPrivilege: DISABLED
SeTimeZonePrivilege: DISABLED
```

Display information about local users

```
Computer Name : LAPTOP-9R1PMVC2
User Name : Administrator
User Id : 500
Is Enabled : False
User Type : Administrator
Comment : Built-in account for administering the computer/domain
Last Logon : 27-11-2020 20:35:46
Logons Count : 22
Password Last Set : 01-01-1970 00:00:00
================================================================================
===============
Computer Name : LAPTOP-9R1PMVC2
User Name : DefaultAccount
User Id : 503
Is Enabled : False
User Type : Guest
Comment : A user account managed by the system.
Last Logon : 01-01-1970 00:00:00
Logons Count : 0
Password Last Set : 01-01-1970 00:00:00
================================================================================
===============
Computer Name : LAPTOP-9R1PMVC2
User Name : Guest
```

```
User Id : 501
Is Enabled : False
User Type : Guest
Comment : Built-in account for guest access to the computer/domain
Last Logon : 01-01-1970 00:00:00
Logons Count : 0
Password Last Set : 01-01-1970 00:00:00
================================================================================
===============
Computer Name : LAPTOP-9R1PMVC2
User Name : MOHANAPRASAD
User Id : 1001
Is Enabled : True
User Type : Administrator
Comment :
Last Logon : 08-08-2023 14:05:56
Logons Count : 1781
Password Last Set : 18-07-2022 15:06:58
================================================================================
===============
Computer Name : LAPTOP-9R1PMVC2
User Name : WDAGUtilityAccount
User Id : 504
Is Enabled : False
User Type : Guest
Comment : A user account managed and used by the system for Windows Defender
Application Guard scenarios.
Last Logon : 01-01-1970 00:00:00
Logons Count : 0
Password Last Set : 27-11-2020 19:22:33
================================================================================
===============
```

RDP Sessions

```
SessID pSessionName pUserName pDomainName State SourceIP
6 Console MOHANAPRASAD LAPTOP-9R1PMVC2 Active
```

Home folders found

```
C:\Users\All Users
C:\Users\Default
C:\Users\Default User
C:\Users\MOHANAPRASAD : MOHANAPRASAD [AllAccess]
C:\Users\Public : Interactive [WriteData/CreateFiles]
```

Password Policies

Check for a possible brute-force

```
Domain: Builtin
SID: S-1-5-32
MaxPasswordAge: 42.22:47:31.7437440
MinPasswordAge: 00:00:00
MinPasswordLength: 0
PasswordHistoryLength: 0
PasswordProperties: 0
================================================================================
===============
Domain: LAPTOP-9R1PMVC2
SID: S-1-5-21-2599125077-3711717779-1984677719
MaxPasswordAge: 42.00:00:00
MinPasswordAge: 00:00:00
MinPasswordLength: 0
PasswordHistoryLength: 0
```

```
PasswordProperties: 0
================================================================================
===============
```

Print Logon Sessions

```
Method: WMI
Logon Server:
Logon Server Dns Domain:
Logon Id: 164728615
Logon Time:
Logon Type: Interactive
Start Time: 08-08-2023 09:12:46
Domain: LAPTOP-9R1PMVC2
Authentication Package: NTLM
Start Time: 08-08-2023 09:12:46
User Name: MOHANAPRASAD
User Principal Name:
User SID:
================================================================================
===============
Method: WMI
Logon Server:
Logon Server Dns Domain:
Logon Id: 164728531
Logon Time:
Logon Type: Interactive
Start Time: 08-08-2023 09:12:46
Domain: LAPTOP-9R1PMVC2
Authentication Package: NTLM
Start Time: 08-08-2023 09:12:46
User Name: MOHANAPRASAD
User Principal Name:
User SID:
================================================================================
===============
Method: WMI
Logon Server:
Logon Server Dns Domain:
Logon Id: 112194466
Logon Time:
Logon Type: Interactive
Start Time: 07-08-2023 15:30:21
Domain: LAPTOP-9R1PMVC2
Authentication Package: NTLM
Start Time: 07-08-2023 15:30:21
User Name: MOHANAPRASAD
User Principal Name:
User SID:
================================================================================
===============
Method: WMI
Logon Server:
Logon Server Dns Domain:
Logon Id: 112194418
Logon Time:
Logon Type: Interactive
Start Time: 07-08-2023 15:30:21
Domain: LAPTOP-9R1PMVC2
Authentication Package: NTLM
Start Time: 07-08-2023 15:30:21
User Name: MOHANAPRASAD
User Principal Name:
User SID:
================================================================================
===============
Method: WMI
Logon Server:
Logon Server Dns Domain:
Logon Id: 108995613
Logon Time:
Logon Type: Interactive
Start Time: 07-08-2023 12:09:14
```

```
Domain: LAPTOP-9R1PMVC2
Authentication Package: NTLM
Start Time: 07-08-2023 12:09:14
User Name: MOHANAPRASAD
User Principal Name:
User SID:
================================================================================
===============
Method: WMI
Logon Server:
Logon Server Dns Domain:
Logon Id: 108995566
Logon Time:
Logon Type: Interactive
Start Time: 07-08-2023 12:09:14
Domain: LAPTOP-9R1PMVC2
Authentication Package: NTLM
Start Time: 07-08-2023 12:09:14
User Name: MOHANAPRASAD
User Principal Name:
User SID:
================================================================================
===============
Method: WMI
Logon Server:
Logon Server Dns Domain:
Logon Id: 105595074
Logon Time:
Logon Type: Interactive
Start Time: 07-08-2023 09:23:03
Domain: LAPTOP-9R1PMVC2
Authentication Package: NTLM
Start Time: 07-08-2023 09:23:03
User Name: MOHANAPRASAD
User Principal Name:
User SID:
================================================================================
===============
Method: WMI
Logon Server:
Logon Server Dns Domain:
Logon Id: 105595027
Logon Time:
Logon Type: Interactive
Start Time: 07-08-2023 09:23:03
Domain: LAPTOP-9R1PMVC2
Authentication Package: NTLM
Start Time: 07-08-2023 09:23:03
User Name: MOHANAPRASAD
User Principal Name:
User SID:
================================================================================
===============
Method: WMI
Logon Server:
Logon Server Dns Domain:
Logon Id: 82824465
Logon Time:
Logon Type: Interactive
Start Time: 06-08-2023 22:01:00
Domain: LAPTOP-9R1PMVC2
Authentication Package: NTLM
Start Time: 06-08-2023 22:01:00
User Name: MOHANAPRASAD
User Principal Name:
User SID:
================================================================================
===============
Method: WMI
Logon Server:
Logon Server Dns Domain:
Logon Id: 82824418
Logon Time:
Logon Type: Interactive
Start Time: 06-08-2023 22:01:00
Domain: LAPTOP-9R1PMVC2
Authentication Package: NTLM
Start Time: 06-08-2023 22:01:00
```

```
User Name: MOHANAPRASAD
User Principal Name:
User SID:
================================================================================
==============
Method: WMI
Logon Server:
Logon Server Dns Domain:
Logon Id: 495577
Logon Time:
Logon Type: Interactive
Start Time: 04-08-2023 07:49:04
Domain: LAPTOP-9R1PMVC2
Authentication Package: NTLM
Start Time: 04-08-2023 07:49:04
User Name: MOHANAPRASAD
User Principal Name:
User SID:
================================================================================
==============
Method: WMI
Logon Server:
Logon Server Dns Domain:
Logon Id: 495489
Logon Time:
Logon Type: Interactive
Start Time: 04-08-2023 07:49:04
Domain: LAPTOP-9R1PMVC2
Authentication Package: NTLM
Start Time: 04-08-2023 07:49:04
User Name: MOHANAPRASAD
User Principal Name:
User SID:
================================================================================
==============
```

Processes Information

Vulnerable Leaked Handlers

https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation/leaked-handle-exploitation

Getting Leaked Handlers, it might take some time...

```
[----------] 0% |■■■■■■■■■■■■■■■■■■■■■■###-------] 31%
/■■■■■■■■■■■■■■■■■■#------] 40% -■\■|■/■-■\■|■/■■■■■1% -■\■|■/■-■\■|■/■■■■■2%
-■\■|■/■-■\■|■■■■■3% /■-■\■|■■■■■4% /■-■\■|■/■-■\■|■/■-■\■|■/■■■■■5%
-■\■|■/■-■\■|■■■■■6% /■-■\■|■/■-■\■|■/■-■\■|■/■-■\■|■/■■■■■7%
-■\■|■/■-■\■|■/■-■\■■■■■8% |■/■-■\■|■/■-■\■■■■■9%
|■/■-■\■|■/■-■\■■■■■■■■■■■■■■■■#-----] 50% |■/■-■\■|■/■-■■■■■1%
\■|■/■-■■■■■2% \■|■/■-■\■|■/■-■\■■■■■3% |■/■-■■■■■4%
\■|■/■-■\■|■/■-■\■|■/■-■\■|■/■-■\■|■/■-■\■|■/■-■\■|■/■■■■■5%
-■\■|■/■-■\■■■■■6% |■/■-■\■|■/■-■■■■■7% \■|■/■■■■■8% -■\■|■/■-■\■|■■■■■9%
/■-■\■■■■■■■■■■■■■■■■#----] 61% |■/■-■\■|■/■-■■■■■2%
\■|■/■-■\■|■/■-■\■|■/■-■\■|■/■-■\■|■/■-■\■|■/■-■\■|■■■■■3% /■-■\■|■/■-■\■|■■■■■5%
/■-■\■|■/■-■\■■■■■6% |■/■-■\■|■/■-■\■|■/■-■\■|■/■-■\■■■■■7%
|■/■-■\■|■/■-■\■|■/■-■■■■■8% \■|■/■-■\■|■/■■■■■9% -■■■■■■■■■■■■■■#---] 70%
\■|■/■■■■■1% -■\■|■/■-■■■■■2% \■|■/■-■\■|■/■-■■■■■3% \■|■/■-■■■■■4%
\■|■/■■■■■5% -■\■|■/■-■\■|■/■-■\■|■/■-■\■|■/■-■\■|■/■-■\■|■■■■■6%
/■-■\■|■■■■■7% /■-■\■|■/■-■\■|■/■-■\■|■/■-■\■|■/■-■\■|■/■-■■■■■8%
\■|■/■-■\■|■/■-■\■|■■■■■9% /■-■\■|■/■-■\■|■■■■■■■■■■■■■#--] 80%
/■-■\■|■/■■■■■1%
-■\■|■/■-■\■|■/■-■\■|■/■-■\■|■/■-■\■|■/■-■\■|■/■-■\■|■/■-■\■|■/■■■■■2%
-■\■|■/■-■\■■■■■3%
|■/■-■\■|■/■-■\■|■/■-■\■|■/■-■\■|■/■-■\■|■/■-■\■|■/■-■\■|■/■-■\■|■■■■■4%
/■-■\■|■/■-■\■|■/■-■\■|■/■-■\■|■/■-■\■|■/■-■\■|■/■■■■■5%
-■\■|■/■-■\■|■/■-■\■|■/■-■\■|■/■-■\■|■/■-■\■■■■■6%
```

```
|■/■-■\■|■/■-■\■|■/■-■\■|■/■-■\■|■/■-■■■■7%
\■|■/■-■\■|■/■-■\■|■/■-■\■|■/■-■\■|■/■-■\■■■■8% |■/■-■\■|■/■-■■■■9%
\■|■/■-■\■|■■■■■■■■■■■#-] 90% /■-■■■■1% \■■■■2% |■/■■■■3% -■\■|■/■■■■4%
-■\■|■/■-■■■■5% \■|■/■-■\■■■■6%
|■/■-■\■|■/■-■\■|■/■-■\■|■/■-■\■|■/■-■\■|■/■-■\■|■/■-■\■|■/■■■■7%
-■\■|■/■-■\■|■■■■8% /■-■\■|■/■-■\■|■/■-■\■|■■■■■■■■■■■■■■■■■■■■■■■■
■■■■■■■■■■■■■■■■■■■■■■■■ Handle: 18772(key)
Handle Owner: Pid is 7448(explorer) with owner: MOHANAPRASAD
Reason: WriteKey
Registry: HKLM\■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
=================================================================================
===============
```

Services Information

Interesting Services -non Microsoft-

Check if you can overwrite some service binary or perform a DLL hijacking, also check for unquoted paths
https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#services

```
ACCSvc(Acer Incorporated - ACC Service)["C:\Program Files (x86)\Acer\Care
Center\ACCSvc.exe"] - Auto - Running
ACC Service
=================================================================================
===============
AdobeARMservice(Adobe Inc. - Adobe Acrobat Update Service)["C:\Program Files
(x86)\Common Files\Adobe\ARM\1.0\armsvc.exe"] - Auto - Running
Adobe Acrobat Updater keeps your Adobe software up to date.
=================================================================================
===============
AMD External Events Utility(AMD - AMD External Events Utility)[C:\WINDOWS\System32
\DriverStore\FileRepository\u0364341.inf_amd64_c22b73fb0c3a32d3\B364190\atiesrxx.e
xe] - Auto - Running
=================================================================================
===============
AMD Log Utility(Advanced Micro Devices, Inc. - AMD Log
Utility)[C:\WINDOWS\System32\amdlogsr.exe] - Auto - Running
=================================================================================
===============
AtherosSvc(Windows (R) Win 7 DDK provider -
AtherosSvc)[C:\WINDOWS\System32\drivers\AdminService.exe] - Auto - Running
=================================================================================
===============
brave(BraveSoftware Inc. - Brave Update Service (brave))["C:\Program Files
(x86)\BraveSoftware\Update\BraveUpdate.exe" /svc] - Auto - Stopped
Keeps your BraveSoftware software up to date. If this service is disabled or
stopped, your BraveSoftware software will not be kept up to date, meaning security
vulnerabilities that may arise cannot be fixed and features may not work. This
service uninstalls itself when there is no BraveSoftware software using it.
=================================================================================
===============
BraveElevationService(Brave Elevation Service (BraveElevationService))["C:\Program
Files\BraveSoftware\Brave-Browser\Application\115.1.56.20\elevation_service.exe"] -
Manual - Stopped
=================================================================================
===============
bravem(BraveSoftware Inc. - Brave Update Service (bravem))["C:\Program Files
(x86)\BraveSoftware\Update\BraveUpdate.exe" /medsvc] - Manual - Stopped
Keeps your BraveSoftware software up to date. If this service is disabled or
stopped, your BraveSoftware software will not be kept up to date, meaning security
vulnerabilities that may arise cannot be fixed and features may not work. This
service uninstalls itself when there is no BraveSoftware software using it.
=================================================================================
===============
BraveVpnService(Brave Software, Inc. - Brave Vpn Service
(BraveVpnService))["C:\Program
Files\BraveSoftware\Brave-Browser\Application\115.1.56.20\brave_vpn_helper.exe"] -
```

```
Manual - Stopped
=========================================================================================
==============
GoogleChromeElevationService(Google LLC - Google Chrome Elevation Service
(GoogleChromeElevationService))["C:\Program
Files\Google\Chrome\Application\115.0.5790.111\elevation_service.exe"] - Manual -
Stopped
=========================================================================================
==============
GoTrust ID Plugin(GOTrustID Inc. - GoTrust ID Plugin)["C:\Program Files\GoTrust ID
Plugin\GoTrust ID Plugin\GTFidoService.exe"] - Auto - Running - isDotNet
GoTrust ID Plugin
=========================================================================================
==============
GoTrustID Service(GOTrustID Inc. - GoTrustID Service)["C:\Program Files\GoTrust ID
Plugin\Bridge_Service.exe"] - Auto - Running - isDotNet
GoTrustID Service
=========================================================================================
==============
gupdate(Google LLC - Google Update Service (gupdate))["C:\Program Files
(x86)\Google\Update\GoogleUpdate.exe" /svc] - Auto - Stopped
Keeps your Google software up to date. If this service is disabled or stopped, your
Google software will not be kept up to date, meaning security vulnerabilities that
may arise cannot be fixed and features may not work. This service uninstalls itself
when there is no Google software using it.
=========================================================================================
==============
gupdatem(Google LLC - Google Update Service (gupdatem))["C:\Program Files
(x86)\Google\Update\GoogleUpdate.exe" /medsvc] - Manual - Stopped
Keeps your Google software up to date. If this service is disabled or stopped, your
Google software will not be kept up to date, meaning security vulnerabilities that
may arise cannot be fixed and features may not work. This service uninstalls itself
when there is no Google software using it.
=========================================================================================
==============
MozillaMaintenance(Mozilla Foundation - Mozilla Maintenance Service)["C:\Program
Files (x86)\Mozilla Maintenance Service\maintenanceservice.exe"] - Manual - Stopped
The Mozilla Maintenance Service ensures that you have the latest and most secure
version of Mozilla Firefox on your computer. Keeping Firefox up to date is very
important for your online security, and Mozilla strongly recommends that you keep
this service enabled.
=========================================================================================
==============
MySQL80(MySQL80)["C:\Program Files\MySQL\MySQL Server 8.0\bin\mysqld.exe"
--defaults-file="C:\ProgramData\MySQL\MySQL Server 8.0\my.ini" MySQL80] - Auto -
Running
=========================================================================================
==============
NortonSecurity(NortonLifelock Inc. - Norton Security)["C:\Program Files\Norton
Security\Engine\22.23.4.6\NortonSecurity.exe" /s "NortonSecurity" /m "C:\Program
Files\Norton Security\Engine\22.23.4.6\diMaster.dll" /prefetch:1] - Auto - Running
Norton Security
=========================================================================================
==============
nsWscSvc(NortonLifeLock Inc. - Norton WSC Service)["C:\Program Files\Norton
Security\Engine\22.23.4.6\nsWscSvc.exe"] - Auto - Running
Norton WSC Service
=========================================================================================
==============
QALSvc(Acer Incorporated - Quick Access Local Service)["C:\Program Files\Acer\Quick
Access Service\QALSvc.exe"] - Manual - Stopped
Quick Access Local Service
=========================================================================================
==============
QASvc(Acer Incorporated - Quick Access Service)["C:\Program Files\Acer\Quick Access
Service\QASvc.exe"] - Manual - Running
Quick Access Service
=========================================================================================
==============
QcomWlanSrv(Qualcomm Technologies Inc. - Qualcomm Atheros WLAN Driver
Service)[C:\WINDOWS\System32\drivers\QcomWlanSrvx64.exe] - Auto - Running
=========================================================================================
==============
RtkAudioUniversalService(Realtek Semiconductor - Realtek Audio Universal Service)[
"C:\WINDOWS\System32\DriverStore\FileRepository\realtekservice.inf_amd64_291337223
b900dd5\RtkAudUService64.exe"] - Auto - Running
Realtek Audio Universal Service
=========================================================================================
==============
```

```
ssh-agent(OpenSSH Authentication Agent)[C:\WINDOWS\System32\OpenSSH\ssh-agent.exe]
- Disabled - Stopped
Agent to hold private keys used for public key authentication.
=============================================================================
==============
Tenable Nessus(Tenable, Inc. - Tenable Nessus)["C:\Program
Files\Tenable\Nessus\nessus-service.exe"] - Auto - Running
Tenable Nessus Network Security Scanner
=============================================================================
==============
UEIPSvc(Acer Incorporated - User Experience Improvement Program)["C:\Program
Files\Acer\User Experience Improvement Program Service\Framework\UBTService.exe"] -
Manual - Running - isDotNet
=============================================================================
==============
UiPath RobotJS Service(UiPath - UiPath RobotJS Service)["C:\Program
Files\UiPath\Studio\UiPath.RobotJS.ServiceHost.exe"] - Auto - Running
UiPath Robot JS Add-on Service
=============================================================================
==============
UiPath.UpdateService(UiPath - UiPath Update Service)["C:\Program
Files\UiPath\Studio\UiPath.UpdateService.Worker.exe"] - Auto - Running
UiPath Update Service
=============================================================================
==============
```

Modifiable Services

Check if you can modify any service
https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#services

```
LOOKS LIKE YOU CAN MODIFY OR START/STOP SOME SERVICE/s:
RmSvc: GenericExecute (Start/Stop)
wcncsvc: GenericExecute (Start/Stop)
BcastDVRUserService_9d1b818: GenericExecute (Start/Stop)
ConsentUxUserSvc_9d1b818: GenericExecute (Start/Stop)
CredentialEnrollmentManagerUserSvc_9d1b818: GenericExecute (Start/Stop)
DeviceAssociationBrokerSvc_9d1b818: GenericExecute (Start/Stop)
DevicePickerUserSvc_9d1b818: GenericExecute (Start/Stop)
DevicesFlowUserSvc_9d1b818: GenericExecute (Start/Stop)
PimIndexMaintenanceSvc_9d1b818: GenericExecute (Start/Stop)
PrintWorkflowUserSvc_9d1b818: GenericExecute (Start/Stop)
UdkUserSvc_9d1b818: GenericExecute (Start/Stop)
UnistoreSvc_9d1b818: GenericExecute (Start/Stop)
UserDataSvc_9d1b818: GenericExecute (Start/Stop)
WpnUserService_9d1b818: GenericExecute (Start/Stop)
```

Checking write permissions in PATH folders (DLL Hijacking)

Check for DLL Hijacking in PATH folders https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#dll-hijacking

```
C:\Program Files\Common Files\Oracle\Java\javapath
C:\WINDOWS\system32
C:\WINDOWS
C:\WINDOWS\System32\Wbem
C:\WINDOWS\System32\WindowsPowerShell\v1.0\
C:\WINDOWS\System32\OpenSSH\
C:\Program Files\nodejs\
C:\Program Files\Git\cmd
```

Applications Information

Installed Applications --Via Program Files/Uninstall registry--

Check if you can modify installed software
https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#software

```
C:\Program Files (x86)\Acer\Care Center
C:\Program Files (x86)\Microsoft Office
C:\Program Files (x86)\Microsoft Visual Studio\Installer
C:\Program Files\Acer
C:\Program Files\Adobe
C:\Program Files\AMD
C:\Program Files\ATOMI
==> C:\Program Files\ATOMI\ActivePresenter\ActivePresenter.exe (Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\api-ms-win-core-console-l1-1-0.dll
(Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\api-ms-win-core-console-l1-2-0.dll
(Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\api-ms-win-core-datetime-l1-1-0.dll
(Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\api-ms-win-core-debug-l1-1-0.dll (Users
[AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\api-ms-win-core-errorhandling-l1-1-0.dll
(Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\api-ms-win-core-file-l1-1-0.dll (Users
[AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\api-ms-win-core-file-l1-2-0.dll (Users
[AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\api-ms-win-core-file-l2-1-0.dll (Users
[AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\api-ms-win-core-handle-l1-1-0.dll (Users
[AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\api-ms-win-core-heap-l1-1-0.dll (Users
[AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\api-ms-win-core-interlocked-l1-1-0.dll
(Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\api-ms-win-core-libraryloader-l1-1-0.dll
(Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\api-ms-win-core-localization-l1-2-0.dll
(Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\api-ms-win-core-memory-l1-1-0.dll (Users
[AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\api-ms-win-core-namedpipe-l1-1-0.dll
(Users [AllAccess])
==> C:\Program
Files\ATOMI\ActivePresenter\api-ms-win-core-processenvironment-l1-1-0.dll (Users
[AllAccess])
==> C:\Program
Files\ATOMI\ActivePresenter\api-ms-win-core-processthreads-l1-1-0.dll (Users
[AllAccess])
==> C:\Program
Files\ATOMI\ActivePresenter\api-ms-win-core-processthreads-l1-1-1.dll (Users
[AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\api-ms-win-core-profile-l1-1-0.dll
(Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\api-ms-win-core-rtlsupport-l1-1-0.dll
(Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\api-ms-win-core-string-l1-1-0.dll (Users
[AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\api-ms-win-core-synch-l1-1-0.dll (Users
[AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\api-ms-win-core-synch-l1-2-0.dll (Users
[AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\api-ms-win-core-sysinfo-l1-1-0.dll
(Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\api-ms-win-core-timezone-l1-1-0.dll
(Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\api-ms-win-core-util-l1-1-0.dll (Users
[AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\api-ms-win-crt-conio-l1-1-0.dll (Users
[AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\api-ms-win-crt-convert-l1-1-0.dll (Users
[AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\api-ms-win-crt-environment-l1-1-0.dll
(Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\api-ms-win-crt-filesystem-l1-1-0.dll
(Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\api-ms-win-crt-heap-l1-1-0.dll (Users
```

```
[AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\api-ms-win-crt-locale-l1-1-0.dll (Users
[AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\api-ms-win-crt-math-l1-1-0.dll (Users
[AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\api-ms-win-crt-multibyte-l1-1-0.dll
(Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\api-ms-win-crt-private-l1-1-0.dll (Users
[AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\api-ms-win-crt-process-l1-1-0.dll (Users
[AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\api-ms-win-crt-runtime-l1-1-0.dll (Users
[AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\api-ms-win-crt-stdio-l1-1-0.dll (Users
[AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\api-ms-win-crt-string-l1-1-0.dll (Users
[AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\api-ms-win-crt-time-l1-1-0.dll (Users
[AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\api-ms-win-crt-utility-l1-1-0.dll (Users
[AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\APOptimizer.dll (Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\assimp-vc142-mt.dll (Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\avcodec-59.dll (Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\avdevice-59.dll (Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\avfilter-8.dll (Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\avformat-59.dll (Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\avutil-57.dll (Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\BsSndRpt64.exe (Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\BugSplat64.dll (Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\BugSplatRc64.dll (Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\changes.txt (Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\concrt140.dll (Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\cpprest_2_10.dll (Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\credits.html (Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\freetype.dll (Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\harfbuzz.dll (Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\HDDInfo.dll (Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\InstallLog.txt (Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\libhunspell.dll (Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\msvcp140.dll (Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\msvcp140_1.dll (Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\msvcp140_2.dll (Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\msvcp140_atomic_wait.dll (Users
[AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\msvcp140_codecvt_ids.dll (Users
[AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\ooxml.dll (Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\portaudio.dll (Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\qtbridge.dll (Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\rlactivator.exe (Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\rlplugin.dll (Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\rltext2speech.dll (Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\rlupdater.exe (Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\sfnt2woff-zopfli.dll (Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\STIX2Math.otf (Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\svg.dll (Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\swresample-4.dll (Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\swscale-6.dll (Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\themes.config (Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\ucrtbase.dll (Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\unins000.dat (Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\unins000.exe (Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\unins000.msg (Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\UserManual9_en.pdf (Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\vccorlib140.dll (Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\vcruntime140.dll (Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\vcruntime140_1.dll (Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\WebView2Loader.dll (Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\wordbreak.dic (Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\wxmsw316u.dll (Users [AllAccess])
==> C:\Program Files\ATOMI\ActivePresenter\wxpdfdoc.dll (Users [AllAccess])
C:\Program Files\AVG
C:\Program Files\Blender Foundation
C:\Program Files\BlueStacks_nxt
C:\Program Files\BraveSoftware
C:\Program Files\Common Files
C:\Program Files\desktop.ini
C:\Program Files\DriverSetupUtility
```

```
C:\Program Files\Git
==> C:\Program Files\Git\etc\hosts (MOHANAPRASAD [AllAccess])
==> C:\Program Files\Git\etc\mtab (MOHANAPRASAD [AllAccess])
==> C:\Program Files\Git\etc\networks (MOHANAPRASAD [AllAccess])
==> C:\Program Files\Git\etc\protocols (MOHANAPRASAD [AllAccess])
==> C:\Program Files\Git\etc\services (MOHANAPRASAD [AllAccess])
C:\Program Files\Google
C:\Program Files\GoTrust ID Plugin
C:\Program Files\GTA install files
C:\Program Files\Internet Explorer
C:\Program Files\Java
C:\Program Files\JetBrains
C:\Program Files\Microsoft Office
C:\Program Files\Microsoft Update Health Tools
C:\Program Files\ModifiableWindowsApps
C:\Program Files\Mozilla Firefox
C:\Program Files\MSBuild
C:\Program Files\MySQL
C:\Program Files\nodejs
C:\Program Files\Norton Security
C:\Program Files\Npcap
C:\Program Files\OWASP
C:\Program Files\PCHealthCheck
C:\Program Files\Reference Assemblies
C:\Program Files\Sublime Text
C:\Program Files\Tenable
C:\Program Files\UiPath
C:\Program Files\Uninstall Information
C:\Program Files\VideoLAN
C:\Program Files\Windows Defender
C:\Program Files\Windows Mail
C:\Program Files\Windows Media Player
C:\Program Files\Windows NT
C:\Program Files\Windows Photo Viewer
C:\Program Files\Windows Sidebar
C:\Program Files\WindowsApps
C:\Program Files\WindowsPowerShell
C:\Program Files\WinRAR
```

Autorun Applications

Check if you can modify other users AutoRuns binaries (Note that is normal that you can modify HKCU registry and binaries indicated there) https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation/privilege-escalation-with-autorun-binaries

```
RegPath: HKLM\Software\Microsoft\Windows\CurrentVersion\Run
Key: SecurityHealth
Folder: C:\WINDOWS\system32
File: C:\WINDOWS\system32\SecurityHealthSystray.exe
================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows\CurrentVersion\Run
Key: RtkAudUService
Folder: C:\WINDOWS\System32\DriverStore\FileRepository\realtekservice.inf_amd64_29
1337223b900dd5
File: C:\WINDOWS\System32\DriverStore\FileRepository\realtekservice.inf_amd64_2913
37223b900dd5\RtkAudUService64.exe -background
================================================================================
===============
RegPath: HKCU\Software\Microsoft\Windows\CurrentVersion\Run
RegPerms: MOHANAPRASAD [FullControl]
Key: OneDrive
Folder: C:\Users\MOHANAPRASAD\AppData\Local\Microsoft\OneDrive
FolderPerms: MOHANAPRASAD [AllAccess]
File: C:\Users\MOHANAPRASAD\AppData\Local\Microsoft\OneDrive\OneDrive.exe
/background
FilePerms: MOHANAPRASAD [AllAccess]
================================================================================
===============
RegPath: HKCU\Software\Microsoft\Windows\CurrentVersion\Run
RegPerms: MOHANAPRASAD [FullControl]
Key: MicrosoftEdgeAutoLaunch_6DBFF247277BE856505924EE2239A856
Folder: C:\Program Files (x86)\Microsoft\Edge\Application
```

```
File: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
--no-startup-window --win-session-start /prefetch:5 (Unquoted and Space detected)
================================================================================
==============
RegPath: HKCU\Software\Microsoft\Windows\CurrentVersion\Run
RegPerms: MOHANAPRASAD [FullControl]
Key: GoogleChromeAutoLaunch_AD4FAD83FCF28F6CAE1B902DADA36706
Folder: C:\Program Files\BraveSoftware\Brave-Browser\Application
File: C:\Program Files\BraveSoftware\Brave-Browser\Application\brave.exe
--no-startup-window /prefetch:5 (Unquoted and Space detected)
================================================================================
==============
RegPath: HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
Key: Common Startup
Folder: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
FolderPerms: MOHANAPRASAD [Delete] (Unquoted and Space detected)
================================================================================
==============
RegPath: HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
Key: Common Startup
Folder: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
FolderPerms: MOHANAPRASAD [Delete] (Unquoted and Space detected)
================================================================================
==============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
Key: Userinit
Folder: C:\Windows\system32
File: C:\Windows\system32\userinit.exe,
================================================================================
==============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
Key: Shell
Folder: None (PATH Injection)
File: explorer.exe
================================================================================
==============
RegPath: HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot
Key: AlternateShell
Folder: None (PATH Injection)
File: cmd.exe
================================================================================
==============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Font Drivers
Key: Adobe Type Manager
Folder: None (PATH Injection)
File: atmfd.dll
================================================================================
==============
RegPath: HKLM\Software\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Font Drivers
Key: Adobe Type Manager
Folder: None (PATH Injection)
File: atmfd.dll
================================================================================
==============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: aux
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
==============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: midi
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
==============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: midimapper
Folder: None (PATH Injection)
File: midimap.dll
================================================================================
==============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: mixer
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
==============
```

```
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: msacm.imaadpcm
Folder: None (PATH Injection)
File: imaadp32.acm
================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: msacm.msadpcm
Folder: None (PATH Injection)
File: msadp32.acm
================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: msacm.msg711
Folder: None (PATH Injection)
File: msg711.acm
================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: msacm.msgsm610
Folder: None (PATH Injection)
File: msgsm32.acm
================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: vidc.i420
Folder: None (PATH Injection)
File: iyuv_32.dll
================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: vidc.iyuv
Folder: None (PATH Injection)
File: iyuv_32.dll
================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: vidc.mrle
Folder: None (PATH Injection)
File: msrle32.dll
================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: vidc.msvc
Folder: None (PATH Injection)
File: msvidc32.dll
================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: vidc.uyvy
Folder: None (PATH Injection)
File: msyuv.dll
================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: vidc.yuy2
Folder: None (PATH Injection)
File: msyuv.dll
================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: vidc.yvu9
Folder: None (PATH Injection)
File: tsbyuv.dll
================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: vidc.yvyu
Folder: None (PATH Injection)
File: msyuv.dll
================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: wave
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
```

```
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: wavemapper
Folder: None (PATH Injection)
File: msacm32.drv
================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: msacm.l3acm
Folder: C:\Windows\System32
File: C:\Windows\System32\l3codeca.acm
================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: aux1
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: aux2
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: midi1
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: midi2
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: mixer1
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: mixer2
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: wave1
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: wave2
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: MSVideo8
Folder: None (PATH Injection)
File: VfWWDM32.dll
================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: aux3
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: midi3
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
```

```
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: mixer3
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: wave3
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: aux
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: midi
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: midimapper
Folder: None (PATH Injection)
File: midimap.dll
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: mixer
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: msacm.imaadpcm
Folder: None (PATH Injection)
File: imaadp32.acm
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: msacm.msadpcm
Folder: None (PATH Injection)
File: msadp32.acm
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: msacm.msg711
Folder: None (PATH Injection)
File: msg711.acm
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: msacm.msgsm610
Folder: None (PATH Injection)
File: msgsm32.acm
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: vidc.cvid
Folder: None (PATH Injection)
File: iccvid.dll
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: vidc.i420
Folder: None (PATH Injection)
File: iyuv_32.dll
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: vidc.iyuv
Folder: None (PATH Injection)
File: iyuv_32.dll
================================================================================
===============
```

```
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: vidc.mrle
Folder: None (PATH Injection)
File: msrle32.dll
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: vidc.msvc
Folder: None (PATH Injection)
File: msvidc32.dll
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: vidc.uyvy
Folder: None (PATH Injection)
File: msyuv.dll
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: vidc.yuy2
Folder: None (PATH Injection)
File: msyuv.dll
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: vidc.yvu9
Folder: None (PATH Injection)
File: tsbyuv.dll
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: vidc.yvyu
Folder: None (PATH Injection)
File: msyuv.dll
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: wave
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: wavemapper
Folder: None (PATH Injection)
File: msacm32.drv
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: msacm.l3acm
Folder: C:\Windows\SysWOW64
File: C:\Windows\SysWOW64\l3codeca.acm
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: aux1
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: aux2
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: midi1
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: midi2
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
```

```
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: mixer1
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: mixer2
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: wave1
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: wave2
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: aux3
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: midi3
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: mixer3
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
Key: wave3
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
RegPath: HKLM\Software\Classes\htmlfile\shell\open\command
Folder: C:\Program Files\Internet Explorer
File: C:\Program Files\Internet Explorer\iexplore.exe %1 (Unquoted and Space
detected)
================================================================================
===============
RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
Key: *kernel32
Folder: None (PATH Injection)
File: kernel32.dll
================================================================================
===============
RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
Key: _wow64cpu
Folder: None (PATH Injection)
File: wow64cpu.dll
================================================================================
===============
RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
Key: _wowarmhw
Folder: None (PATH Injection)
File: wowarmhw.dll
================================================================================
===============
RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
Key: _xtajit
Folder: None (PATH Injection)
File: xtajit.dll
================================================================================
===============
```

```
RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
Key: advapi32
Folder: None (PATH Injection)
File: advapi32.dll
================================================================================
===============
RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
Key: clbcatq
Folder: None (PATH Injection)
File: clbcatq.dll
================================================================================
===============
RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
Key: combase
Folder: None (PATH Injection)
File: combase.dll
================================================================================
===============
RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
Key: COMDLG32
Folder: None (PATH Injection)
File: COMDLG32.dll
================================================================================
===============
RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
Key: coml2
Folder: None (PATH Injection)
File: coml2.dll
================================================================================
===============
RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
Key: DifxApi
Folder: None (PATH Injection)
File: difxapi.dll
================================================================================
===============
RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
Key: gdi32
Folder: None (PATH Injection)
File: gdi32.dll
================================================================================
===============
RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
Key: gdiplus
Folder: None (PATH Injection)
File: gdiplus.dll
================================================================================
===============
RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
Key: IMAGEHLP
Folder: None (PATH Injection)
File: IMAGEHLP.dll
================================================================================
===============
RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
Key: IMM32
Folder: None (PATH Injection)
File: IMM32.dll
================================================================================
===============
RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
Key: MSCTF
Folder: None (PATH Injection)
File: MSCTF.dll
================================================================================
===============
RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
Key: MSVCRT
Folder: None (PATH Injection)
File: MSVCRT.dll
================================================================================
===============
RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
Key: NORMALIZ
Folder: None (PATH Injection)
File: NORMALIZ.dll
================================================================================
===============
```

```
RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
Key: NSI
Folder: None (PATH Injection)
File: NSI.dll
================================================================================
===============
RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
Key: ole32
Folder: None (PATH Injection)
File: ole32.dll
================================================================================
===============
RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
Key: OLEAUT32
Folder: None (PATH Injection)
File: OLEAUT32.dll
================================================================================
===============
RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
Key: PSAPI
Folder: None (PATH Injection)
File: PSAPI.DLL
================================================================================
===============
RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
Key: rpcrt4
Folder: None (PATH Injection)
File: rpcrt4.dll
================================================================================
===============
RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
Key: sechost
Folder: None (PATH Injection)
File: sechost.dll
================================================================================
===============
RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
Key: Setupapi
Folder: None (PATH Injection)
File: Setupapi.dll
================================================================================
===============
RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
Key: SHCORE
Folder: None (PATH Injection)
File: SHCORE.dll
================================================================================
===============
RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
Key: SHELL32
Folder: None (PATH Injection)
File: SHELL32.dll
================================================================================
===============
RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
Key: SHLWAPI
Folder: None (PATH Injection)
File: SHLWAPI.dll
================================================================================
===============
RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
Key: user32
Folder: None (PATH Injection)
File: user32.dll
================================================================================
===============
RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
Key: WLDAP32
Folder: None (PATH Injection)
File: WLDAP32.dll
================================================================================
===============
RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
Key: wow64
Folder: None (PATH Injection)
File: wow64.dll
================================================================================
===============
```

```
RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
Key: wow64base
Folder: None (PATH Injection)
File: wow64base.dll
================================================================================
==============
RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
Key: wow64con
Folder: None (PATH Injection)
File: wow64con.dll
================================================================================
==============
RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
Key: wow64win
Folder: None (PATH Injection)
File: wow64win.dll
================================================================================
==============
RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
Key: WS2_32
Folder: None (PATH Injection)
File: WS2_32.dll
================================================================================
==============
RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
Key: xtajit64
Folder: None (PATH Injection)
File: xtajit64.dll
================================================================================
==============
RegPath: HKLM\Software\Microsoft\Active Setup\Installed
Components\{2C7339CF-2B09-4501-B3F3-F3508C9228ED}
Key: StubPath
Folder: \
FolderPerms: Authenticated Users [WriteData/CreateFiles]
File: /UserInstall
================================================================================
==============
RegPath: HKLM\Software\Microsoft\Active Setup\Installed
Components\{6BF52A52-394A-11d3-B153-00C04F79FAA6}
Key: StubPath
Folder: C:\WINDOWS\system32
File: C:\WINDOWS\system32\unregmp2.exe /FirstLogon
================================================================================
==============
RegPath: HKLM\Software\Microsoft\Active Setup\Installed
Components\{89820200-ECBD-11cf-8B85-00AA005B4340}
Key: StubPath
Folder: None (PATH Injection)
File: U
================================================================================
==============
RegPath: HKLM\Software\Microsoft\Active Setup\Installed
Components\{89820200-ECBD-11cf-8B85-00AA005B4383}
Key: StubPath
Folder: C:\Windows\System32
File: C:\Windows\System32\ie4uinit.exe -UserConfig
================================================================================
==============
RegPath: HKLM\Software\Microsoft\Active Setup\Installed
Components\{89B4C1CD-B018-4511-B0A1-5476DBF70820}
Key: StubPath
Folder: C:\Windows\System32
File: C:\Windows\System32\Rundll32.exe C:\Windows\System32\mscories.dll,Install
================================================================================
==============
RegPath: HKLM\Software\Microsoft\Active Setup\Installed
Components\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Key: StubPath
Folder: C:\Program Files\Google\Chrome\Application\115.0.5790.111\Installer
File: C:\Program
Files\Google\Chrome\Application\115.0.5790.111\Installer\chrmstp.exe
--configure-user-settings --verbose-logging --system-level --channel=stable
(Unquoted and Space detected)
================================================================================
==============
RegPath: HKLM\Software\Microsoft\Active Setup\Installed
Components\{9459C573-B17A-45AE-9F64-1857B5D58CEE}
```

```
Key: StubPath
Folder: C:\Program Files (x86)\Microsoft\Edge\Application\115.0.1901.200\Installer
File: C:\Program Files
(x86)\Microsoft\Edge\Application\115.0.1901.200\Installer\setup.exe
--configure-user-settings --verbose-logging --system-level --msedge
--channel=stable (Unquoted and Space detected)
================================================================================
==============
RegPath: HKLM\Software\Microsoft\Active Setup\Installed
Components\{AFE6A462-C574-4B8A-AF43-4CC60DF4563B}
Key: StubPath
Folder: C:\Program
Files\BraveSoftware\Brave-Browser\Application\115.1.56.20\Installer
File: C:\Program
Files\BraveSoftware\Brave-Browser\Application\115.1.56.20\Installer\chrmstp.exe
--configure-user-settings --verbose-logging --system-level (Unquoted and Space
detected)
================================================================================
==============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Active Setup\Installed
Components\{6BF52A52-394A-11d3-B153-00C04F79FAA6}
Key: StubPath
Folder: C:\WINDOWS\system32
File: C:\WINDOWS\system32\unregmp2.exe /FirstLogon
================================================================================
==============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Active Setup\Installed
Components\{89B4C1CD-B018-4511-B0A1-5476DBF70820}
Key: StubPath
Folder: C:\Windows\SysWOW64
File: C:\Windows\SysWOW64\Rundll32.exe C:\Windows\SysWOW64\mscories.dll,Install
================================================================================
==============
RegPath: HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper
Objects\{1FD49718-1D00-4B19-AF5F-070AF6D5D54C}
Folder: C:\Program Files (x86)\Microsoft\Edge\Application\115.0.1901.200\BHO
File: C:\Program Files
(x86)\Microsoft\Edge\Application\115.0.1901.200\BHO\ie_to_edge_bho_64.dll (Unquoted
and Space detected)
================================================================================
==============
RegPath:
HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper
Objects\{1FD49718-1D00-4B19-AF5F-070AF6D5D54C}
Folder: C:\Program Files (x86)\Microsoft\Edge\Application\115.0.1901.200\BHO
File: C:\Program Files
(x86)\Microsoft\Edge\Application\115.0.1901.200\BHO\ie_to_edge_bho_64.dll (Unquoted
and Space detected)
================================================================================
==============
Folder: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
FolderPerms: MOHANAPRASAD [Delete]
File: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini
(Unquoted and Space detected)
FilePerms: MOHANAPRASAD [Delete]
================================================================================
==============
Folder: C:\Users\MOHANAPRASAD\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup
FolderPerms: MOHANAPRASAD [AllAccess]
File: C:\Users\MOHANAPRASAD\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup\desktop.ini (Unquoted and Space detected)
FilePerms: MOHANAPRASAD [AllAccess]
================================================================================
==============
Folder: C:\windows\tasks
FolderPerms: Authenticated Users [WriteData/CreateFiles]
================================================================================
==============
Folder: C:\windows\system32\tasks
FolderPerms: Authenticated Users [WriteData/CreateFiles]
================================================================================
==============
Folder: C:\windows
File: C:\windows\system.ini
================================================================================
==============
Folder: C:\windows
```

```
File: C:\windows\win.ini
================================================================================
==============
Key: From WMIC
Folder: C:\Users\MOHANAPRASAD\AppData\Local\Microsoft\OneDrive
FolderPerms: MOHANAPRASAD [AllAccess]
File: C:\Users\MOHANAPRASAD\AppData\Local\Microsoft\OneDrive\OneDrive.exe
/background
FilePerms: MOHANAPRASAD [AllAccess]
================================================================================
==============
Key: From WMIC
Folder: C:\Program Files (x86)\Microsoft\Edge\Application
File: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
--no-startup-window --win-session-start /prefetch:5
================================================================================
==============
Key: From WMIC
Folder: C:\Program Files\BraveSoftware\Brave-Browser\Application
File: C:\Program Files\BraveSoftware\Brave-Browser\Application\brave.exe
--no-startup-window /prefetch:5
================================================================================
==============
Key: From WMIC
Folder: C:\WINDOWS\system32
File: C:\WINDOWS\system32\SecurityHealthSystray.exe
================================================================================
==============
Key: From WMIC
Folder: C:\WINDOWS\System32\DriverStore\FileRepository\realtekservice.inf_amd64_29
1337223b900dd5
File: C:\WINDOWS\System32\DriverStore\FileRepository\realtekservice.inf_amd64_2913
37223b900dd5\RtkAudUService64.exe -background
================================================================================
==============
```

Scheduled Applications --Non Microsoft--

Check if you can modify other users scheduled binaries https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation/privilege-escalation-with-autorun-binaries

```
(Adobe Systems Incorporated) Adobe Acrobat Update Task: C:\Program Files
(x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe
Trigger: At log on of any user-After triggered, repeat every 03:30:00
indefinitely.Trigger expires at 02-05-2027 08:00:00.
At 23:00 every day-Trigger expires at 02-05-2027 12:05:00.
================================================================================
==============
(App Explorer) App Explorer: C:\Users\MOHANAPRASAD\AppData\Local\Host App
Service\Engine\HostAppServiceUpdater.exe /LOGON
Permissions file: MOHANAPRASAD [AllAccess]
Permissions folder(DLL Hijacking): MOHANAPRASAD [AllAccess]
Trigger: At log on of any user
================================================================================
==============
(Acer Inc. SSD KCSE) StorPSCTL: "C:\Program Files\Acer\StorPSCTL\StorPSCTL.exe"
Trigger: At log on of any user
================================================================================
==============
(UiPath) UiPath RobotJS: C:\Program Files\UiPath\Studio\UiPath.RobotJS.UserHost.exe
Trigger: At log on of any user
================================================================================
==============
(UiPath) UiPath Upgrade Service Agent: C:\Program
Files\UiPath\Studio\UiPath.UpdateService.Agent.exe
Trigger: At log on of any user
================================================================================
==============
(LAPTOP-9R1PMVC2\MOHANAPRASAD)
User_Feed_Synchronization-{BFFDC885-F951-451E-B9FD-A48CACC58EE1}:
C:\Windows\system32\msfeedssync.exe sync
Trigger: At 16:57 every day-Trigger expires at 08-08-2033 16:57:24.
================================================================================
```

```
==============
(NortonLifeLock) Norton Security Ultra Autofix: C:\Program Files\Norton
Security\Engine\22.23.4.6\SymErr.exe /ui
==========================================================================
==============
(NortonLifeLock) Norton Security Ultra Error Analyzer: C:\Program Files\Norton
Security\Engine\22.23.4.6\SymErr.exe /analyze
==========================================================================
==============
(Acer) AcerJumpstartTask: "C:\Program Files (x86)\Acer\Acer Jumpstart\hermes.exe"
/default
Trigger: At log on of any user
On workstation unlock of any user.
==========================================================================
==============
(NortonLifeLock) AntimalwareMigrationTask: "C:\Program Files\Common Files\AV\Norton
Security Ultra\Upgrade.exe" /upgrade /user_logon
Trigger: At log on of any user-After triggered, repeat every 1.00:00:00
indefinitely.
==========================================================================
==============
```

Device Drivers --Non Microsoft--

Check 3rd party drivers for known vulnerabilities/rootkits. https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#vulnerable-drivers

```
Advanced Micro Devices, Inc. amdpsp sys - 5.17.0.0 [Advanced Micro Devices, Inc. ]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\amdpsp.sys
EFA - 7.4 [Broadcom]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\NGCx64\1617040.006\SYMEFASI64.SYS
Symantec Security Technologies - 17.2.15.16 [Broadcom]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\NGCx64\1617040.006\ccSetx64.sys
Iron - 9.2.0.58 [Broadcom]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\NGCx64\1617040.006\Ironx64.SYS
SYMEVENT - 14.0.8.101 [Broadcom]: C:\Windows\system32\Drivers\SYMEVENT64x86.SYS
Npcap - 1.75 [Insecure.Com LLC.]:
\\.\GLOBALROOT\SystemRoot\system32\DRIVERS\npcap.sys
Symantec Security Drivers - 17.2 [Broadcom]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\NGCx64\1617040.006\symnets.sys
AutoProtect - 15.7 [Broadcom]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\NGCx64\1617040.006\SRTSPX64.SYS
Symantec Intrusion Detection - 17.2 [Broadcom]: C:\Program Files\Norton
Security\NortonData\22.20.5.40\Definitions\IPSDefs\20210204.061\IDSvia64.sys
ERASER ENGINE - 119.1.2.22 [Broadcom]: C:\Program Files (x86)\Common Files\Symantec
Shared\EENGINE\eeCtrl64.sys
BASH - 12.1.0.271 [Broadcom]: C:\Program Files\Norton
Security\NortonData\22.20.5.40\Definitions\BASHDefs\20210202.001\BHDrvx64.sys
AMD SFH Controller Driver - 1.0.0.86 [Advanced Micro Devices]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\amdsfhkmdfi2c.sys
Driver for Qualcomm Atheros QCA61x4/QCA9377 Network Adapter - 12.0.0.953 [Qualcomm
Atheros, Inc.]: \\.\GLOBALROOT\SystemRoot\System32\drivers\Qcamain10x64.sys
ATI Radeon Family - 8.1.1.1634 [Advanced Micro Devices, Inc.]: \\.\GLOBALROOT\Syst
emRoot\System32\DriverStore\FileRepository\u0364341.inf_amd64_c22b73fb0c3a32d3\B36
4190\amdkmdag.sys
AMD Driver - 20.20.0.3 [Advanced Micro Devices, Inc.]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\amdlog.sys
AMD Audio CoProcessor - 2.89.0.62 [Advanced Micro Devices]: \\.\GLOBALROOT\SystemR
oot\System32\DriverStore\FileRepository\amdacpbus.inf_amd64_38546573cbb72307\amdac
pbus.sys
Acer Airplane Mode Controller - 1.0.0.8 [Acer Incorporated]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\AcerAirplaneModeController.sys
AMD GPIO Controller Driver - 2.2.0.130 [Advanced Micro Devices, Inc]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\amdgpio2.sys
AMD I2C Controller Driver - 1.2.0.118 [Advanced Micro Devices, Inc]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\amdi2c.sys
AMD HD Audio Driver - 10.0.1.16 [Advanced Micro Devices]:
\\.\GLOBALROOT\SystemRoot\system32\drivers\AtihdWT6.sys
Realtek(r) High Definition Audio Function Driver - 6.0.9198.1 [Realtek
Semiconductor Corp.]: \\.\GLOBALROOT\SystemRoot\system32\drivers\RTKVHD64.sys
ELAN I2C Driver - 12.40.0.10 [ELAN Microelectronic Corp.]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\ETDI2C.sys
BT Driver - 10.0.0.953 [Qualcomm]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\btfilter.sys
```

```
Bluestack Hypervisor - 2.1.24.117012 [Bluestack System Inc. ]: C:\Program
Files\BlueStacks_nxt\BstkDrv_nxt.sys
Symantec Eventing Platform - 1.5.1.29 [Symantec Corporation]: C:\Program
Files\Norton Security\NortonData\22.20.5.40\SymPlatform\SymEvnt.sys
```

Network Information

Network Shares

```
ADMIN$ (Path: C:\WINDOWS)
C$ (Path: C:\)
D$ (Path: D:\)
E$ (Path: E:\)
IPC$ (Path: )
Users (Path: C:\Users) -- Permissions: AllAccess
```

Network Ifaces and known hosts

The masks are only for the IPv4 addresses

```
Local Area Connection* 1[96:08:53:6F:EB:3B]: 169.254.151.229,
fe80::5f5f:5f81:5d79:3590%12 / 255.255.0.0
DNSs: fec0:0:0:ffff::1%1, fec0:0:0:ffff::2%1, fec0:0:0:ffff::3%1
Known hosts:
224.0.0.2 01-00-5E-00-00-02 Static
224.0.0.22 01-00-5E-00-00-16 Static
224.0.0.251 01-00-5E-00-00-FB Static
224.0.0.252 01-00-5E-00-00-FC Static
Local Area Connection* 2[A6:08:53:6F:EB:3B]: 169.254.239.201,
fe80::8d0:f939:69cd:48e3%21 / 255.255.0.0
DNSs: fec0:0:0:ffff::1%1, fec0:0:0:ffff::2%1, fec0:0:0:ffff::3%1
Known hosts:
224.0.0.2 01-00-5E-00-00-02 Static
224.0.0.22 01-00-5E-00-00-16 Static
224.0.0.251 01-00-5E-00-00-FB Static
224.0.0.252 01-00-5E-00-00-FC Static
Wi-Fi[94:08:53:6F:EB:3B]: 10.20.7.204, fe80::a404:f626:f3d2:a83c%10 / 255.255.248.0
Gateways: 10.20.0.1
DNSs: 8.8.8.8, 4.2.2.2
Known hosts:
10.2.0.1 00-00-00-00-00-00 Invalid
10.2.2.52 00-00-00-00-00-00 Invalid
10.2.3.110 00-00-00-00-00-00 Invalid
10.2.3.231 00-00-00-00-00-00 Invalid
10.2.3.245 00-00-00-00-00-00 Invalid
10.2.4.241 00-00-00-00-00-00 Invalid
10.20.0.1 00-02-B6-46-06-9D Dynamic
10.20.1.71 00-00-00-00-00-00 Invalid
10.20.1.72 48-9E-BD-A4-2E-2A Dynamic
10.20.7.83 AA-95-AD-8B-45-32 Dynamic
10.20.7.115 62-0D-2C-DB-81-08 Dynamic
10.20.7.128 28-CD-C4-D5-1F-AF Dynamic
10.20.7.144 00-00-00-00-00-00 Invalid
10.20.7.146 00-00-00-00-00-00 Invalid
10.20.7.162 00-00-00-00-00-00 Invalid
10.20.7.165 36-E7-DF-A7-CD-67 Dynamic
10.20.7.173 00-00-00-00-00-00 Invalid
10.20.7.185 70-66-55-DD-10-ED Dynamic
10.20.7.202 00-45-E2-D6-0A-9D Dynamic
10.20.7.221 00-00-00-00-00-00 Invalid
10.20.7.222 9C-2F-9D-69-E1-0D Dynamic
10.20.7.223 D4-1B-81-6D-37-1D Dynamic
10.20.7.224 B0-68-E6-29-93-D9 Dynamic
10.20.7.233 E4-A4-71-E4-4D-46 Dynamic
```

```
10.20.7.240 EA-D0-5D-C8-C0-F6 Dynamic
10.20.7.255 FF-FF-FF-FF-FF-FF Static
100.109.0.1 00-00-00-00-00-00 Invalid
192.168.43.1 00-00-00-00-00-00 Invalid
192.168.195.80 00-00-00-00-00-00 Invalid
192.168.199.249 00-00-00-00-00-00 Invalid
224.0.0.2 01-00-5E-00-00-02 Static
224.0.0.22 01-00-5E-00-00-16 Static
224.0.0.251 01-00-5E-00-00-FB Static
224.0.0.252 01-00-5E-00-00-FC Static
239.255.255.250 01-00-5E-7F-FF-FA Static
255.255.255.255 FF-FF-FF-FF-FF-FF Static
Loopback Pseudo-Interface 1[]: 127.0.0.1, ::1 / 255.0.0.0
DNSs: fec0:0:0:ffff::1%1, fec0:0:0:ffff::2%1, fec0:0:0:ffff::3%1
Known hosts:
224.0.0.2 00-00-00-00-00-00 Static
224.0.0.22 00-00-00-00-00-00 Static
224.0.0.251 00-00-00-00-00-00 Static
224.0.0.252 00-00-00-00-00-00 Static
239.255.255.250 00-00-00-00-00-00 Static
```

Current TCP Listening Ports

Check for services restricted from the outside

```
Enumerating IPv4 connections
Protocol Local Address Local Port Remote Address Remote Port State Process ID
Process Name
TCP 0.0.0.0 135 0.0.0.0 0 Listening 1532 svchost
TCP 0.0.0.0 445 0.0.0.0 0 Listening 4 System
TCP 0.0.0.0 2323 0.0.0.0 0 Listening 4 System
TCP 0.0.0.0 3306 0.0.0.0 0 Listening 4876 mysqld
TCP 0.0.0.0 5040 0.0.0.0 0 Listening 7468 svchost
TCP 0.0.0.0 8834 0.0.0.0 0 Listening 4244 nessusd
TCP 0.0.0.0 33060 0.0.0.0 0 Listening 4876 mysqld
TCP 0.0.0.0 42025 0.0.0.0 0 Listening 4 System
TCP 0.0.0.0 46937 0.0.0.0 0 Listening 16100 C:\Program Files\WindowsApps\SpotifyAB
.SpotifyMusic_1.217.834.0_x64__zpdnekdrzrea0\Spotify.exe
TCP 0.0.0.0 49664 0.0.0.0 0 Listening 1220 lsass
TCP 0.0.0.0 49665 0.0.0.0 0 Listening 1052 wininit
TCP 0.0.0.0 49666 0.0.0.0 0 Listening 1896 svchost
TCP 0.0.0.0 49667 0.0.0.0 0 Listening 2400 svchost
TCP 0.0.0.0 49668 0.0.0.0 0 Listening 3616 spoolsv
TCP 0.0.0.0 49669 0.0.0.0 0 Listening 1172 services
TCP 0.0.0.0 57621 0.0.0.0 0 Listening 16100 C:\Program Files\WindowsApps\SpotifyAB
.SpotifyMusic_1.217.834.0_x64__zpdnekdrzrea0\Spotify.exe
TCP 10.20.7.204 139 0.0.0.0 0 Listening 4 System
TCP 10.20.7.204 46902 157.240.192.52 443 Established 20356 C:\Program
Files\Google\Chrome\Application\chrome.exe
TCP 10.20.7.204 46944 35.186.224.47 443 Established 16100 C:\Program Files\Windows
Apps\SpotifyAB.SpotifyMusic_1.217.834.0_x64__zpdnekdrzrea0\Spotify.exe
TCP 10.20.7.204 46945 52.163.231.110 443 Established 1676 C:\Program Files\Windows
Apps\MicrosoftTeams_23195.1511.2279.823_x64__8wekyb3d8bbwe\msteams.exe
TCP 10.20.7.204 46946 104.199.240.237 443 Established 16100 C:\Program Files\Windo
wsApps\SpotifyAB.SpotifyMusic_1.217.834.0_x64__zpdnekdrzrea0\Spotify.exe
TCP 10.20.7.204 46959 20.198.119.143 443 Established 4268 svchost
TCP 10.20.7.204 46970 35.186.224.39 443 Established 21948 C:\Program Files\Windows
Apps\SpotifyAB.SpotifyMusic_1.217.834.0_x64__zpdnekdrzrea0\Spotify.exe
TCP 10.20.7.204 46996 74.125.24.188 443 Established 20356 C:\Program
Files\Google\Chrome\Application\chrome.exe
TCP 10.20.7.204 46998 20.198.119.84 443 Established 22768
C:\Users\MOHANAPRASAD\AppData\Local\Microsoft\OneDrive\OneDrive.exe
TCP 10.20.7.204 47581 13.68.168.63 443 Established 4080 NortonSecurity
TCP 10.20.7.204 47787 13.68.168.63 443 Established 4080 NortonSecurity
Enumerating IPv6 connections
Protocol Local Address Local Port Remote Address Remote Port State Process ID
Process Name
TCP [::] 135 [::] 0 Listening 1532 svchost
TCP [::] 445 [::] 0 Listening 4 System
TCP [::] 2323 [::] 0 Listening 4 System
TCP [::] 3306 [::] 0 Listening 4876 mysqld
TCP [::] 8834 [::] 0 Listening 4244 nessusd
TCP [::] 33060 [::] 0 Listening 4876 mysqld
TCP [::] 42025 [::] 0 Listening 4 System
```

```
TCP [::] 49664 [::] 0 Listening 1220 lsass
TCP [::] 49665 [::] 0 Listening 1052 wininit
TCP [::] 49666 [::] 0 Listening 1896 svchost
TCP [::] 49667 [::] 0 Listening 2400 svchost
TCP [::] 49668 [::] 0 Listening 3616 spoolsv
TCP [::] 49669 [::] 0 Listening 1172 services
```

Current UDP Listening Ports

Check for services restricted from the outside

```
Enumerating IPv4 connections
Protocol Local Address Local Port Remote Address:Remote Port Process ID Process
Name
UDP 0.0.0.0 123 *:* 4552 svchost
UDP 0.0.0.0 500 *:* 3948 svchost
UDP 0.0.0.0 1900 *:* 16100 C:\Program Files\WindowsApps\SpotifyAB.SpotifyMusic_1.2
17.834.0_x64__zpdnekdrzrea0\Spotify.exe
UDP 0.0.0.0 4500 *:* 3948 svchost
UDP 0.0.0.0 5050 *:* 7468 svchost
UDP 0.0.0.0 5353 *:* 16100 C:\Program Files\WindowsApps\SpotifyAB.SpotifyMusic_1.2
17.834.0_x64__zpdnekdrzrea0\Spotify.exe
UDP 0.0.0.0 5353 *:* 2596 svchost
UDP 0.0.0.0 5353 *:* 16100 C:\Program Files\WindowsApps\SpotifyAB.SpotifyMusic_1.2
17.834.0_x64__zpdnekdrzrea0\Spotify.exe
UDP 0.0.0.0 5353 *:* 21796 C:\Program Files
(x86)\Microsoft\Edge\Application\msedge.exe
UDP 0.0.0.0 5353 *:* 17384 C:\Program Files\Google\Chrome\Application\chrome.exe
UDP 0.0.0.0 5353 *:* 21796 C:\Program Files
(x86)\Microsoft\Edge\Application\msedge.exe
UDP 0.0.0.0 5353 *:* 16100 C:\Program Files\WindowsApps\SpotifyAB.SpotifyMusic_1.2
17.834.0_x64__zpdnekdrzrea0\Spotify.exe
UDP 0.0.0.0 5353 *:* 17384 C:\Program Files\Google\Chrome\Application\chrome.exe
UDP 0.0.0.0 5355 *:* 2596 svchost
UDP 0.0.0.0 54939 *:* 2596 svchost
UDP 0.0.0.0 57614 *:* 2596 svchost
UDP 0.0.0.0 57621 *:* 16100 C:\Program Files\WindowsApps\SpotifyAB.SpotifyMusic_1.
217.834.0_x64__zpdnekdrzrea0\Spotify.exe
UDP 0.0.0.0 57947 *:* 16100 C:\Program Files\WindowsApps\SpotifyAB.SpotifyMusic_1.
217.834.0_x64__zpdnekdrzrea0\Spotify.exe
UDP 0.0.0.0 60042 *:* 1676 C:\Program Files\WindowsApps\MicrosoftTeams_23195.1511.
2279.823_x64__8wekyb3d8bbwe\msteams.exe
UDP 10.20.7.204 137 *:* 4 System
UDP 10.20.7.204 138 *:* 4 System
UDP 10.20.7.204 1900 *:* 5528 svchost
UDP 10.20.7.204 2177 *:* 18544 svchost
UDP 10.20.7.204 50872 *:* 5528 svchost
UDP 127.0.0.1 1900 *:* 5528 svchost
UDP 127.0.0.1 49664 *:* 3976 svchost
UDP 127.0.0.1 50873 *:* 5528 svchost
Enumerating IPv6 connections
Protocol Local Address Local Port Remote Address:Remote Port Process ID Process
Name
UDP [::] 123 *:* 4552 svchost
UDP [::] 500 *:* 3948 svchost
UDP [::] 4500 *:* 3948 svchost
UDP [::] 5353 *:* 2596 svchost
UDP [::] 5353 *:* 16100 C:\Program Files\WindowsApps\SpotifyAB.SpotifyMusic_1.217.
834.0_x64__zpdnekdrzrea0\Spotify.exe
UDP [::] 5353 *:* 16100 C:\Program Files\WindowsApps\SpotifyAB.SpotifyMusic_1.217.
834.0_x64__zpdnekdrzrea0\Spotify.exe
UDP [::] 5353 *:* 21796 C:\Program Files
(x86)\Microsoft\Edge\Application\msedge.exe
UDP [::] 5353 *:* 17384 C:\Program Files\Google\Chrome\Application\chrome.exe
UDP [::] 5355 *:* 2596 svchost
UDP [::] 54939 *:* 2596 svchost
UDP [::] 57614 *:* 2596 svchost
UDP [::] 60042 *:* 1676 C:\Program Files\WindowsApps\MicrosoftTeams_23195.1511.227
9.823_x64__8wekyb3d8bbwe\msteams.exe
UDP [::1] 1900 *:* 5528 svchost
UDP [::1] 50871 *:* 5528 svchost
UDP [fe80::a404:f626:f3d2:a83c%10] 1900 *:* 5528 svchost
UDP [fe80::a404:f626:f3d2:a83c%10] 2177 *:* 18544 svchost
UDP [fe80::a404:f626:f3d2:a83c%10] 50870 *:* 5528 svchost
```

Firewall Rules

Showing only DENY rules (too many ALLOW rules always)

```
Current Profiles: PUBLIC
FirewallEnabled (Domain): True
FirewallEnabled (Private): True
FirewallEnabled (Public): True
DENY rules:
```

DNS cached --limit 70--

```
Entry Name Data
dns.google dns.google 8.8.4.4
dns.google dns.google 8.8.8.8
1.137.168.192.in-addr.arpa 1.137.168.192.in-addr.arpa. LAPTOP-9R1PMVC2.mshome.net
247.137.168.192.in-addr.arpa 247.137.168.192.in-addr.arpa. MITV.mshome.net
mitv.mshome.net MITV.mshome.net 192.168.137.247
mitv.mshome.net
laptop-9r1pmvc2.mshome.net LAPTOP-9R1PMVC2.mshome.net 192.168.137.1
laptop-9r1pmvc2.mshome.net
```

Enumerating Internet settings, zone and proxy configuration

```
General Settings
Hive Key Value
HKCU CertificateRevocation 1
HKCU DisableCachingOfSSLPages 0
HKCU IE5_UA_Backup_Flag 5.0
HKCU PrivacyAdvanced 1
HKCU SecureProtocols 10240
HKCU EnableNegotiate 1
HKCU MigrateProxy 1
HKCU ProxyEnable 0
HKCU User Agent Mozilla/4.0 (compatible; MSIE 8.0; Win32)
HKCU ZonesSecurityUpgrade System.Byte[]
HKCU WarnonZoneCrossing 0
HKCU LockDatabase 133200923033334507
HKCU EnableHttp1_1 1
HKLM ActiveXCache C:\Windows\Downloaded Program Files
HKLM CodeBaseSearchPath CODEBASE
HKLM EnablePunycode 1
HKLM MinorVersion 0
HKLM WarnOnIntranet 1
Zone Maps
No URLs configured
Zone Auth Settings
No Zone Auth Settings
```

Windows Credentials

Checking Windows Vault

https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#credentials-manager-windows-vault

```
GUID: 4bf4c442-9b8a-41a0-b380-dd4a704ddb28
Type: Web Credentials
Resource: 742ed62635302731e615ba988ae7511d
Identity: {793e6b3b-a0fb-4cbc-abf2-be16c2ced7b6}
PacakgeSid: S-1-15-2-337888173-3784501919-3848985668-446021496-2147755643-19607238
94-1217954087
Credential: 01rZwClWF2wuVK7SVrj7bSP12oaIh3g9x9sbYdS/4kgiZXc/YGzzc4P1q1Ccgxr9Td/rrr
yUWHAchVB3I+2pbMVBTJyQpb+XKsJS83POM2OtPpnRZUSkOah+y9oSkqIPGHuFDgQ7KGlEATzogXvv53k7
ApzulNZm7LRUjQYZED7ThUwYn7Tv1WtZjeqpndyfysO0eCXNEL5JwX27Q77XO4eBtF2dC4aBw/RifkJ7Uk
hFUEQ0IfRMW7CfGlmAGpTPw8K21/Ukho7uGXk40j9tfzd1VGPVFx1QGEiH/hyfq7tkiGySvsnRsOZwkouJ
4PXA4K7/gBoHqh3WaR5Iu8a17Rr/sL1vL0zuVoRdlz3MW+6MEtdSuPXFrXsbb20CC4UFrg3rR99S0JfZqT
F96oOtZ+oD9MshN1brLOSxARB+QVmsA8+oGjq21jbI3i/36M3L2Ra2zHKFqpLEEYk8dNyAIX0XgQY5XNRx
uRC9cCGNBc30FfYliIorELyBdM8KVizyynvHr0UtrXpDzdiJMr+A6a5okZSTIH9iAdPHY+ObmZOTpL7BU8
0pj5lzFEyNF4H485MmkK7X5eObCc1oe8XxsyM6WBOpAtKIy4xNpNeaHVXoesQ7Lr9/0VI4Sft9QsVo9z0h
nvW+RTCHxTB7GNgRntpZK59Z88LoDNLPOwrXg4G69aeGp2h2h9HjXL8hymhwv5Vbd6je6/HMoKKqwzZv/q
5gJzVcO5btu0L2sWFlyVUVneTZayBWw09GijdP14xuLzozuNqp0bGBWy+qsCdX/Z8GcdlU2m5Po3m6meJn
u2Xan7s4Ww6GOv+ocghEIafFLlDcKekejnwEYBo/af6oqhQpQzTx00m71raYjkRvF9vQOXYnKOBUEIX3s1
3n7pmGAZF75kTW8O88uFUxwg/kj3BMPjYh+9xtyg1J++G6gf0J5Ir+9VfwZILKCDQN0elxfYXA3p8VUCVN
hyKBDQfo+JPKWlf6N6iP3OwTAobesmdXzEAC37t9H31fvzzoiYYJVil1ud1SgZcxkehDWD0VCd0KiRC3KP
J0kqCu0tl+F74wOG9P0AlZmnoeWvOPtAnHWrIxNbUF3irzPY7w9H+yNv4iL2nN3X0RA2fC4a0bmGal34E4
HGRYilahNA8prhBGTqKposAD9bhre4d25X26hVGZe2wkYJTebjOZHdWk1QSi370Y3Jr+01cB2RpuLIB2c9
8J+4UcKx3e/7bWFu5X+qFXIbQmFS9Eba+vAbA3b4quR8SaA8ouR7bWQrTTn7fahyhnJpSJKBEAB5fcOQlj
Dz6Z/cdXo7HaA/Q+hNfZY5nycG548cpkT6n8FP/zDTCMV/AL5t5cGJh7E8ZqDts9WfP4DxbiNm+xy7mhPK
IH9//m4x0q1BSffwwcYcZH17JFbD3AA83+FPEFzrTikPrcfTdVaXnqoCmdgW31MmmX55S02dC7eR38YHtN
Zg6lueS91vreR8PdHbV+CWNTBVBNdY01gEIfMrZPWr4jpnYIzjSqPfW5bYEjK0qUcc0gPK1fI63i4qiAhb
tsB0+hl8aXvPqMyvfL0JF/ipVvUx1WL61VkNU/l75L/3hucP/rZsWoRxOK8SRrUpREyRAeCUXoAhtZPfrH
KM15ANHLM10nm6S7naawajkA4LXRvXdT7WDR4EM/xyCycOc3n449XFZ7G2tpQKwT0q4hLN7z3I6Fq0xgJl
JT7FxAxIB5frbavcOCL2YpxTjeTbeTPKnqYR6Y4grj92hULmpboIcWJUFWBFtufiJ1Vx7EZ+iQiEhThj8v
L+DpnAspNkOkCxxL63fIknI8Q9yEiU535Bo/XGSj8i6KSH+0C4yo6fj87x8+z1jPlKFBYP0//ReLMcUdy1
sbxCIhq86RMn7nlnW7C3MEyD3ZiXdWvjpwzkonEi2qJftb1R9DN4W5krLp6kzLEgWZjS6GWQa/wfV7DVwF
x7NLISRLmBpHsoEU4D44aDeq1hEoFu+vPZ1eXZTTg/dZXCveHkPmuFCqBH9Oyj6f4YxQ/Ab46QnMZ5V7a0
rXyoW5PFDQsfsUU9UeVZFNCjwsLAd6ZAksKV2itYZnqcMFd97cpYT+lmiA+KGOsUM/4RsKfA1j8z367krU
Q71NPXV+8m3W2RHPk7d3qCnQPbsMQ2mfKJzFmuPCzYv6YH6ip0RJsQD1awn+mT8WwXIFL2qx11o655SBYD
XTy1DcFq/xYTawQ2ejoZDpcK1D/Cp37UfZXCV+j+OzQZi7sr3aDnUPU6X1+mCGdRSS3CsX2S6kmMrX/H5S
OuIfL7q3igN32yaltClImIPg603kq/m3dkceIUBoG0LAgVqrPNFFLpbWAY/n+/1LbTWRZ13cfL+s4L1rRq
piWF8hgSWn1jQgpGUvEzUtoG1PFN3wqBOpSMgZ614hiuop6HLu17RnWemsh0BhTHdWze0l3sNaGgKx4Dmf
HTvjZCv22EIPv3IAiS4O8J9BqD9fTSHQr2NyeNTl80Mv8QGIQQHTADdfmPZ/i/JhphdKquoB9TkH4B6KjE
+vIQRNPY1k+Zkxr6zoWgSLpONvu5fDKPdox1GthqUeudTBwo7DBVwlC35E3Pvsgj0vMX0Wq8sHDGtbmf+k
sZd/RX0uotd4DToYHsMe1hscZQDeUdbHJf+llS+NfYcV69Tufer6Y/9JwvP+6hIk7MY/FqeRvKStBeehda
vaglo4cIdFCVjH7DE0cPuxTQwhbId1Y7aNoL/OdcZdLEJSmg97vost9Y3UKjMthKZUBeLmekKXLtMN3KVG
PIlAcmyMpxCEUaOrBniudQwH2IDhbcj4J4O/bb4rbDPwSSCx468h13p8OY2yC+Iq60tpC2uSdz1N6jUglh
DdIQ2MtjuPU4AeY0haby26sYwAJcvhC4YdUijeB2C/xif9bknoYohvEPN0yTD2t/86dTfNdV5W9mLvKmKW
wcZHfA5EDN4w+xG312hVPSijghsrMOHVlE4Mxz8y9+9qfsAY1t0CIEbe7VcdMWML6H2j7cUZh5PRUKvYxL
AQ7YbjdeR+oKLbGUamJGc8NZLcvddxzcJCspH9EvuOWyHGdbdZ1WycFgL0scVeGu3kKi3kvuth1Jw8kptO
yx2BYBNBqtfgXrzTzayFR7BQFlpDd2eqF2spkIkdqOgDaKCtcEFxbogdlcxvAE2XgLNebLiKP/ypPyLb+w
64jzlj8lmYcvNs7wK2Qrr+efpLwJAoHT5ckeykeDECywujS2DRYi7/JeZ08NFiLv8l5nT/OJ7u+DthcEHK
JoedukbjRev2UmE7clyb8Uat8/sWyqWr1Coo0FkuEsD/oh4Ygr5Tf2m0ZXdbq3hC78cLdfYFWy4NO2beVH
Fe6xW03gSR6oaW7MLSIFgSo39ptGV3W6tw5kXVgcxo72old3hkP4sdJIpTZlhFi46X9kk92zcQM1c8n4WL
mT7fKEH5mO+NAMabuyGYshWF7BcGzcS7DncZ6afjcs9n+GPnBs3Euw53GecR21G1LnhifCvYciEJLPF9xM
GuChaSFI0i+Sye8wr+P3DCNXG1pCnAIlAm7f5Nsr/l4mBzhQhtcqlzfPHjuwPq2Wt8cKS4cqEIbBQO7Sxf
Hg1TuwkGpDmnDZpixK7Rhgf1WsEW2YSpkMMghFkpR2+Uh2Ba8KR6tyJetao5FA2Lf4RbbfDbE7HfaSr5LU
LcBHe0qnX1q/pxfzQUcEyQIYnVl46zfMQEr7j9eEfil2h9MM9KF3V5TSLu2+oE7hJkGRLT645Ux5vyCe5J
FUHRr7lpJwIQsQ2gG9S6BmMfmSdDdB/mFMULbk3DoqfTczRMR7KAT56KIWMpqRr/VIZVRGk1xg271Fvxox
nWc8JNgEebKD0VDM4I3h/esrhWEqe9ovU4QSDO50CurxK0FWVa/Jc/hFtt8NsTsdWAxxohV9stcM9KF3V5
TSLlh1l2DoCeKBlAOwcNXb5x2JGadRE237yJVot+Dp1e66wMwHOPWhKdx/BwTCuCpjKQaIXS83XuJrbX7/
VHzuW/FMjWKvPBWRGzIu49M7QR9grMO4m9fMSiacskL52mz5xf2f2B9FoMaJaTdCmHhqEebL2GBReB2vtd
gTLSACzE/ibDj2+4D89mfcYDERq1bprC+VyGZ0IXaSQW5pLV2IiskzZxem6SqSMWYrgDckiC5EDx/WXAli
lpT6lfElgTsnZ1zu8W9ZmrMhvUc/GcA7rlP5V1VldXZ2iztnQqmyJRRueF1tnEGNo6tufqDJiK7MFEWiSm
ntiEmF2guIUP8cQUQIg1ATIc1b5eFqYPpvPvQFfGcF7x35MRv6euVnyBqvAoAvg2/tLcM1L4Ra/RCA6YSf
F7Ii6XGNIr5rf5OFRl/Sg9Wkkm3Yl6sdxTRO/yyBeP4Rv7+CQRTBMmE3rAJrqDsiMJJ6ni+MSDrsI8Qcq9
bagh//yzfSF2hLb927GokXwVtAIm84xY0Z3775mxPJ+DooyLO+CfEkqVthFa1keODrAWBJSLyZrRFUK065
KqsOmq/4uqjdEA4JraXuRX2teFe7Fs2eTfblntKishMC6bFTdZWnBBd4riUSW0XkCG+q0gYsLsfOMnUk8j
EoceJkLtu3pCyeBMkzG3Hm8j1Dsf1QA2PgHn7mV9JDoHI9qcUIDKBIg6UWiPbKSHuOEOyX1MSxpyhRgK/a
CAkdukcZoAJiYFVAYbezW+E/wyepw06wUPWEs5Q52q9cZ/wUArd8O8Cf6Hws5st7Vd4ECtL384TRQk4Pqu
oni8ohDRuFTO7fa3DtpeAkawCiksp/08DwF5cY5+XkxHCA37fIuuHCW/O1q3fjWmT62YwNq7BdrTHqze2D
dszVO0Qtbq3Ad/cdDYwHjuhpOWhMIzHBM+vMqc3afsFEw7ouZuVyrTcwwzhqSMUqi9HI7U6clOXmLgA3uZ
fqyU2KuzrH6uhX9am01gXLLDoRPc6g53ozWk074gOEGg+WLFYthPsbPcNDuVfasUypqxxC3BlxPTLeH8FL
NwBrfi7j1wFIpni3pCyeBMkzGzWYcgBCgzuY4vWSc8cCsX+vyN6MR+81qUh2Ba8KR6tyRyGIRSm4fGXez/
RbSAF2W65BYyuaOw67n/eJEnl2Zf280zANPoopG4s7TuBsmEw55MVrQmBPtqNsXiy5e0iyYM8xjHxsu9P7
Lufw2NgrhCgPkI4OKBgaKrJFRefepgjbL5XIZnQhdpLfDAwyhEklJskCXaNxOumXfoRlfWfOEUZPy1um/4
6vchw0wOObUlnBWiQed+oBOdtJM3z2SCC+FeTTIPFf7kCIYUMe5UQXC7WJ7KVrGG5HMn/a9m3NWOCH1wKn
0+fUoMKtY7nMooO/SGiVBCIsJN5GCuhxxjSU/5riJbudbcwk1MvUiyheahzQG1Yot12zi8o9uj4r6pkNLf
DSFJEL9IlBdZk9dt8TdWkidTE/BE5XHrXwprfqY17eXO7xb1masyG1wLulPJ1ZpjEdcz6S95HcBpkwc+df
r4WTRNYZ+oYcMZ2VZxrhMKcPbTNlEn6jIMV3sfieGvVYL0qewdUKdVYyLT645Ux5vyAheStVQ/Y8UEWiSm
ntiEmFhEUcezVqV4dIUbyxtbo9BrD771/4Lw9g4pAKfsMsICTEsTMSj28v/tKishMC6bFTdY6OcKMcUX9s
t4NAgphyOO2DdszVO0Qt2pdIByEa+E8Zhm4xrI1ig7bciMVg7nzL8NIUkQv0iUFo836+lzLNOep7UDobL3
iZxrwLxMoyiVbm1O0Z/uMzhuRR3SJWuV4I0lHW2JkjXDHUjg45didm2DtrhT95bMS/gWEKaHYdpjV4XW2c
QY2jqx3Cs9kU0gsdgnxpALpezwvqP1xCKlUzd5XsmNcpR0fdNT4yzFlv9m1olQQiLCTeRoAKk/bInN9Jhu
T4yvXph+Mcq7bzzRlhxxkvqEcxPoieBVwBLJ+OysWd4LgL10uA3qOdtNoj3InY46Ab7cxgibzqyU2KuzrH
```

```
6qZ2vJ6xGETGpcb36UP5vxedZzwk2AR5sgzB0CCRj+BRoBv5QTj+MVmFX7HTalazwl54zhIAYnxKoY7WNL
FQ3UYKcdKwdEoZ1Gjzfr6XMs05JdlbS3NiTPdjYqG8ilEqqll0/aa7vILQ91/TA1Mv51/+qk/52Ws2oGkM
FTVPkb4FiFTTIknFHNRs95VFlIGfY20juF455qc7
Last Modified: 20-06-2023 12:43:28
================================================================================
===============
GUID: 4bf4c442-9b8a-41a0-b380-dd4a704ddb28
Type: Web Credentials
Resource: f0cda63e6713d3c80b389b979b4589e4
Identity: {3e9fa1af-0ba7-4253-8b73-6971168d4482}
PacakgeSid: S-1-15-2-792116756-2163651165-1029707900-2144380252-3717869303-3061844
081-355238664
Credential: 018GetrxHFpu/NLwrkmHxJx/v7HoY823zvv33xUlIHciuvMYlJ8A2mfXswYS3l4wdeTj1d
U495bSMxhQ8fG13gDYn8jnzdzNlY5pqGF1qC57g/ZaYY9GrSh6rc6pTjOkdWBeJHv/HHDof0/EXul6dFBW
k2DhOe54KkhoHW9+Zt1q9+RavAqWh/pr1GGlA+rm7Gp960S1YyvGcJk4K2/I8kEHEU8OlVKSxnwkfIuREG
fe9Gh6P2HhM7q1NmT6DQx5+cQZOfWyxPgV5zv6Prn2QW+Cgkgw24KojgeiIk7OEAM2j9NuJWDRhQafEPT2
xKUFGchpvoltztyNMjf9VOnxIVg5Nhs/z0cITMgifa0V7cFt+souFo0RPFVz9kGHD9QDPLgzS56ubcf0Yi
3o6xVevgJer+ePf4gkTQ4eEyZ8itV1WJIBjxQUxLdXxQiXghIzuB0qvyw1TG5Nn5I+czwcNZyi68GHyKEo
ejBWjM+KNiy0OcLMHBdq3bouo8G237sz+4303Jzv9yUFur1+v/33eVfKLPw0YqCT/HklGA26C5QJcCFlWr
Z5tI2UMSTo8JSWd5m8VgDpLCkzfOs7kgH7Vg3D1uTdHygxjMXqi3KeRaejZWGhdD4W7A3xqINTP/DbNhXf
6yl4ptf71pwsCfT+txszxLvoDPg/UjN9Lq32ujc26OfRl18z79YjOj3lYPWW8LJ95YFTklqGuqCdpw4O19
mxA8apzYQqt0PM66WClA9KXGIurPF3vAz+F/7YYq3XOAWZQlO6oFowqRXV3lNB0EQ7m6akevQgQvMFg6m0
N7iOUG5b9aVdc+jgGloahsWYk0pNaw0E4ClIQNlIAyZUQYcYgF1+NWO5gPfnfB6o+QY0eIGbpNGSo9gucp
N2cnV2EarJOAM5SwhirXvz+fWRllJWQ59+T7jP2gARnFD/HmloOMV/10Cq0gpMxELL3pS8eI/o9QFvXrzF
1uRdLsz3nNiU+EqtJSOoUgD0CU2I+zvthC8+W6pIBlhUTurpACflR61tYc+TQt9W4ztfcWP99hQOndnH9y
hgTk9jBmeORkfCqYE5/yiFWNVngrJMrZ6qHFQ79v1jM8x81MVUwBCXWZYCcVwpRANZhFC3GfPUDpyyFKag
aw6rHiCGrswI6BI5mDqo1lyg4izNtM4W7p6MBq9D+OUOm066S1W4tOBGs6Ak6hjZJlJKO11P7wKzh0gFl6
rcCWnkbm6yUjKdZs7swRHGlgLI8cOAVGYmkG/pejiggTS1fzlCh2zT5xL3jYSLgg/+RzllriSxBzYSkTCO
nCz0E9gFNwIBNwyg3ZqIRXFpphERXGqO3AyuuGd65/8j5WocjeU82tpzEo9p1YX38blFW/ALKMRuWfsRuM
i3Eo3zKzjXF+89irlNgtB2JDVlKzjVez47KXMnrO5O4LDYLMSc8Qg95+Yh8MaQShPLV1FUqyI3QVLF3dWX
aA6llStBGWcZ52PSwcSIuN3RhB7Jq+kMa6YtNoVuBIxergw+mJopTvTisxG9TA1zGC93/h8zJnTlgv1jxC
Lg5BsPSm8G1G0ZIey31uHjIKZpYho8xqe29LfzVWXsd9/HWenOMnHdLP88W99ehqaNA5fT8BOLIdQYq/O8
StIF1apjpLVfmLZb7nvmRdt+XQmXZDcfUYet611I4OOXYnZthTAUlsotwLBbmRkJEJIjjIo9n7R/KiHA6d
VWp4NyRm/0APyvtWcN4Wapru0a+jRKgBS2BuCz8DGaw2azlRp0t75pHbcSNQo3hUK065KqsOmimPLc38H9
TU6eEQDOpdEFfZauZd+nKnNcVMq0SoE29vwMwHOPWhKdw5JtjNO7Ky+YXAnkK25oZDjVCnobAkjNNtxAo9
ysiJfDqG1qsV3WeCFOhlwN0MYKs+0i3rNd2beVl0/aa7vILQzuTuCw2CzElqOrYT9n2+PFyX5OB6jfl/O2
m7A8074cXXwmKtg+cRJRasWJFQyewdx+f1mhjzek8jvguY/whLyt8f5oQkQfCsFKZtw3aBmkRhZkWZGcE+
83aFU9KKOCGy1+wDIcPFirIaRJSf/n7ucpNNHEwNW8Qq3VBvJHVjwThO9+JN7tjNnwW0pLwOVzCH8GG2zQ
jZyYqtzTHBlTkDllaPhHmeLsCtSyIsU+bEbON+ARX8/CTL8h9cowR2XdF6K30UfbTosiqzRGAo+kRlDE8Z
9gAefaeS+lmiBT2WmEOQy7QruPtRVoOb53DonpZn84+cxP8wWvv3sl6JJ+u27WU8MP+lB7tMN5/cH2kBdy
COvR5bGe2hprDt5u0bobS3mym580RlzAhymR//I83YHZKK6DHdj66cH1yjBHZd0XpGYfPYOuE2BN/2rE82
gz5j7cPEsaeebMH2T/1lovC6W3v0C7SvN9kFAfK9bdEUKCatpCVEXAflPLmY7H/HJnNppFsFkqEG3ZMaJf
olYZpIr0PRYyfcJUf46jsbMdNszW7AypJx4cG6q8/qxOE3MAYUxBQaR2qqL6HwWurdlpt/xiKN4HYL/GJ/
a60VY607dMQ8/iOYkiBWOzdR4KRs2cRd63p49tqqJ4hoL/yY+Nb43t/Qlw8CD6u9wPX/9C8zACTaGJxRc/
+M8rWL/rNDngYlPePrzYGmP3yuLdEkvZDCQJaPSioEjvHzBCtCA7+WVQgkqY9gG+yTC+7uDFPz4M5Bdsoi
pLuJF8Os42jkk6igkG3xQFaRpFwILiUdatflcyPW6OGy/YW9Onllv/si/dStuC3hCnNHwknXkTbsVMWX5Z
KpUgfLtaeSp6HIh+HEmtJD0WMn3CVH+BgaG8vsSseXYdfz3xUjx6XJAx4ILKTuh0cQby2jUFDgUJNE77sX
hoJV3FZB93eaNgAh0qAi3XzqK5JJIxz540BvbTo5r1idm/31stDSJLC13MRH02/QdidRCyvyhYRP52yvuV
Jm9QSUaC/8mPjW+N4qhrSnaNVMjFgbFSdIxBynraQlRFwH5TziicitCbq/LbIyF8p+JajITvfiTe7YzZ9O
9+JN7tjNn6RbBZKhBt2TcVLDarGg2FC5gU1AcpU9KVSOaRK39fku4onIrQm6vy3dhA1LaVIXRsJq9MMEZs
60vEl8ej2eU/o7UTEwxt9XNSOkDXD/zCJyUrCA0dAV00AEwuxwJaeyQIKiqqRNNJzKE1LSPJThTQq8SXx6
PZ5T+tPS4VKvoLUb2LvFCL7nEodhVZfT3zzskYaTnWkqEvpw59L8PAH9m8417YT+JTGXlBfDLqjFhcA0MT
GhpWPEgsUj4+Whj5ZvaB0EfPaRGqPDji52TKizE3x0s7SevS86vPqO6knkHhDhchC/sJXGNU5EgG3uoF5D
p22q1xEE5j+Y5mMcjsB/AXNI8wRr8exxnOx3/m+IB++ZXwU97RlpK5vV7fMtoudol4CYgman5KoLKDKaOz
/BGNHzLWRQNjDn5bIyF8p+JajIKxydQjgog+ancSOxiZ6kg4myz8AaCEK5fkvV0Ee3GscvuxBkBgqtu3G2
xDH1jedVXo6HU1jNq2K/8nDeppc+qFXC7YqTJO362hicUXP/jPJ/EbEvVB3qe/8oWkF9eHznL5os49iECx
vHcnPh7IhLS0srTO/LrJMQD/LjQfMRdS5bjlBxjmx50VmISkLeQxzfHh3cDKUNZ+yjEBJQVPS/sSKN4HYL
/GJ/y47lB7UA/pE58qeBop8x955odcdupkDkrVc3b793WTD935OIjULUnnSzSqQ+sHGnAkd882/dGjcOts
RF6qe4FO13lJHK1zSBWM2a5zLAyl7jl9NOQnmwzKzjaOSTqKCQaOI2TDmB8uxlaz+KHQoTPcw6cmWbgoRC
jyvW3qsJ6Aie7WSRacb3rLnVRfMhmrReQd15//AJS94IWHmxtG7gPqzjaOSTqKCQGWMFnRPxuQZyEL+wlc
Y1TpU0AGSM1Lr5ShWAS9bX4Km6M4FqCBuKcLozgWoIG4pwCMjeYRvr1B4FtKS8Dlcwh2E4gsMrD6bzcxHA
8gbOCLtRycro/ym4KoKJDx7YR8oIzye2m0GZmeiIZ1J4GHvM4GHisFkr/mOeFqxYkVDJ7B3d4r2jAm0mRU
c39JJ18IlHiHfhwU0KsrLot2R/3XqO1E/ICbsw77lhxQF5abRlND3W5J6GKIbxD1RcfSqRLfxk6gotsZRq
YkYgdZJOLq7zzsvMQYxKPxsCWI80BsGLR8DYZQ5GGT+ZazqMYtrTOcpy3EUvSWz/pTYUpm3DdoGaRNjB1F
9KXfQbdfj0lG8fQ8LtqQtiequUz+OX005CebDMVFx9KpEt/GR9Oktw2GIaejwacNM79Miq/KKavwhfN7ES
IgGm5SJCJFvc6gglCOeFqHp3gk8DTgR79fy7StS5RQkG2QCyEG1hO1k7w5UpR6EbDxrl4dGtAfis59yaWu
itRRfb1io+B8I8GnDTO/TIqtv6euNro9cHtBnhHSNu7NsuJR1q1+VzI/hy6hQ0OPYvu3ryXRh6Qw9ZN0BT
e3jrHq4t0SS9kMJAwPX/9C8zACQ7WTvDlSlHoSmAgZKDCgUidc17nhstTFNE4A7QCspILME45P4aYQsMJp
N7X7wkW10bwqc86hcB/yl9Hafg6rvpHjRV509X1lTEQrwqQPV6eC79Kc0eoLcXNIgTSTBUpgqUQbo0Pqs9
fYfuCt3rPmMaR4MQLLC6NLYNFiLv8l5nTw0WIu/yXmdP84nu74O2FwQcomh526RuNF6/ZSYTtyXJvxRq3z
+xbKpavUKijQWS4SwP+iHhiCvlN/abRld1ureELvxwt19gVbLg07Zt5UcV7rFbTeBJHqhpbswtIgWBKjf2
m0ZXdbq3nUvtbbj9+8320j2ibY43aB7WzxSCcjkBZ6evks25vVT6p0DGRHQoa/a8C7vtNKdBrgn754P4qM
WLZcKe6O21eViSf/LNVPDOi2XCnujttXkAyTZg2akzmSqXN88eO7A+rZa3xwpLhyoQhsFA7tLF8eDVO7CQ
akOajApzWSWcRDlBsPSm8G1G0UmGOxKteqyLXEVezf1Aal0+7zrfZmocqrD771/4Lw9ghpvW6b7n/Ivu0+
1hh6gNWxqnCQXh8RliHnXWUiDuH5OuudtHvC4HJwkdukcZoAJivmt/k4VGX9L1hLOUOdqvXDTi28SMKCUV
K6cEHvWqx4QiL/hvM8PUgmcp/i3YL3NC9FCev9HA+xkXyE9anwMwqD6JuYPn/0XbKeEf2QsB5BDZtLmUCA
ZhD1NvT/81wLngG/x6d3Cw7PUMgjWLUgNRgSTz3H6CHDt0UTZU6fwisURnKf4t2C9zQqueQtSjLrF03w9B
KtKXnO2f94kSeXZl/WtkCVq8+vv0MuKXtS756xF0Gqfb5o8lIdfHlthW+eGUkf4+FW0osRgp4R/ZCwHkEP
2f2B9FoMaJ5vuHXQa8JgKtY7nMooO/SOurgt0d2x5QD2ygWz35GF8jgzx+YsMU70E4BGrp81ZRgFVBZeYH
```

```
gQEIRnc9tvpEEH+EQdSXpSB0VCtOuSqrDpq8irWtzvBxCbEgX8+camjGKhb8dugIBne+G9JwZm12QJWWUi
yKUHv9hEUcezVqV4f5mvCXZnJCKG8389J6sl+rXO7xb1masyFnNghQqRex/UPrWFoe1c2E1UAodW6P9Jg5
gDzbWA+Y66kti2083s38TSAtPbNim8yCiLxZY2ISSmVH/iqigDrJOy3EBUjOG+IF2c20yr9UPGeuljL3Uf
Xun/hZldjHnxNbYRWtZHjg63R+VscMSMzUzG2YEWPxN5mNRJh/jEVSGJKp9lfqPPfg1LtQxnR+IFqDLbFz
zQskwEGsk7IQBe3nadwROQYlv4wmquHpHmANwjP4xul/aSSo2hWtkrbpeW1qbPy4/9uCAIS9hek21G0Kfo
RlfWfOEUYBYElIvJmtEfM07INQplRDWHWXYOgJ4oHiva/r+gBAIPhFtt8NsTsdKccPTaUySFhDoHI9qcUI
DOxe9cKTgZCJ+zz1t+4hMJjHKRBF+VOZIinhH9kLAeQQmw+8Ncw10+JBOARq6fNWUZ/ofCzmy3tVS2/dux
qJF8E04tvEjCglFRk/URi8S4T5CEZ3Pbb6RBDrWwzMlInP/AtyhQEUerAxI4M8fmLDFO9pN0KYeGoR5o6V
+nB2cEYbeQOd3GDeH/TkUd0iVrleCDEUANDyJYrBbwVR0xSlR5tc0qtlFqhtShiY5l9Lj5EsYgMfTlunw5
zyMShx4mQu2+RR3SJWuV4I9pKvktQtwEfgcfPsTJSha/cpoI/uZLOxWHWXYOgJ4oFst4NAgphyOLEbw7Yw
x6nwn/hZldjHnxNIUbyxtbo9BjcfuMXSrimMyIo/xXY2zVuKkMc03yDESa70wtXlJcXi5b7MU8p48jVPy1
um/46vcvgVqS3vsSOhXNKrZRaobUqWyheFpRZSAxrTF8XBIARygxFVzSHJKxc1mHIAQoM7mPHiyfPlWbNe
B205zkZzsB2WvKB+ASJFfhtvStY/+UY+S2/duxqJF8FGSs5edWIl6q9pkL8Ha0AjIM/DmbQxuZLOkjqFfs
9yXSL2vMJi0pRx+pSPbFUmdcLHTJqj+diZQ6Z2vJ6xGETGDFhGoGsqVzzjaoctvgGsqzYdTfboKOv76Nzo
YTjFlQQgfPhEKu+mNmHRU9Lxi/lF7nS4gmRHRB790MSCCIGmdrOb5KGKbJ01lvVHgkailKDez/RbSAF2W8
scAk3JxyCcHDTA45tSWcGG5PjK9emH4wog7ZjjepOWdkNx9Rh63rVE6L9BS1scMsxoDgwpyj/TgC+Db+0t
wzUhpGQSv8tLfaoPc7mtFvAzF5raO4q2fktZeOs3zEBK+yF5K1VD9jxQn+tjqsw+FnOf+FmV2MefEw/fsi
4wGTUhMtw9o08qKPwbElGXfIVgbSaq4ekeYA3C5KEHHcPGgNcrRTX9OlAwvnuir4DNPI5UEltF5AhvqtJs
Xiy5e0iyYLW6CgEsFOOgK1V35VzZ7I/Uu1DGdH4gWmD6mbhuvhqcB205zkZzsB0Bs0XoJHWgy+Uq24jopQ
Cxe/mG2ss0PUC01gBHr4W/6ypymfKpPTxaw5AH47oLt4MwpQMv1CEpMnjoE5jcT4DIdbbY6gV7xG5cRV7N
/UBqXU0Ad/BVEriZ2L/PaozpbLFVX46cunfXCK70wtXlJcXijUSYf4xFUhiHP2GGSm2oj9/5hSOb/Mwe8+
rASiREAI9mn7qcczXNLNtVMvZWsrq7d0n21Kl5Pr35H14h8eUK+GmUn7K7WAo1PiTPKTqe4sABecO8awC/
yXxnBe8d+TEbQ+tYWh7VzYRC0AeZHvarByo8dPUDJvOAttyIxWDufMuY4q1xYnbmXAciqDFaXElkaAh2i8
UWqMFEL3/0A2ulEsJ9Ze1MUCsn6Km54zQqKu7jaoctvgGsqzc8q/9Aw+RsjEueCbUomSKtFhPwGqox5lPC
ls+WT0TYhP1D/Unc5vg1FjWxFgEOkWPPigs22SsEsSg7f4358zOHicIlsP5iS8iKP8V2Ns1bROi/QUtbHD
J21yTvwHaqpqn2BTNbKM7lka/1SGVURpM5bSnxPq+SKirBfxgCgFJY42qHLb4BrKvu0+1hh6gNW+sFh93l
fjKTbLxCqls6NddZdP2mu7yC0Pdf0wNTL+df/qpP+dlrNqBpDBU1T5G+BYhU0yJJxRzUbPeVRZSBn2OOYM
dfVYDsIZ1rIcdkSvfjFSQ2CWXsFXWE0/ttAckFBYQVPizKUD7EIpP4FFFhuX+N6JdSo5LmyC0pqwddbaO3
Last Modified: 01-03-2022 05:57:11
================================================================================
===============
GUID: 4bf4c442-9b8a-41a0-b380-dd4a704ddb28
Type: Web Credentials
Resource: d07c5c1d194d166f8953abec316eb1e3
Identity: {63812aa1-7c25-44fb-9a6e-0e88277d0908}
PacakgeSid: S-1-15-2-3847638010-438396508-3810139029-1908452196-1955773144-1529763
429-3426260615
Credential: 01O6UDMHAAYv1eQSbo6ELwI93f3aWdTNW5oAxfe5axq5hjItpdIpk/eKb4lD/ia9VZBnak
rOXUOFgISouWOFxphtgpKHDJSTR/VmlcL05amjv25Yswvm8upYY9KeQ/8WeQv06pHsKs/HDHKHGYfWxFr8
suLlGP4J9sYxM2HvYNVgVFDPV8cZIpKavI0DEk+HPDhj0p5D/xZ5C/Tqkewqz8cMcocZh9bEWvSu0la4+2
0j9dqGiId4PcfbG2HUv+JIImV3P2Bs83OD9atQnIMa/U3f6668lFhwHIC1eawgt03rVNAhjw0E6ZRF4auR
a5nUT4aaE1yRDm6tt3Ygxyw0IjdKsuBio6CVsHfR4WO/sTtYfxi2j4Xr6qUg6bc23pATFAKwhxT8BWmth0
9/xEUqJS41/47r3XpatgZH9sxBnQ4raeqPqIDnE1KuzDch/4kDyLjBFNjdosXpKoXjXEQ4jfVRgbtxjYzx
jotU0W2PsF8ualYFyiLvY78PiwsQaZfwEmaifGc6t1/S836iUuUSEFbIfZS8k/0Q9syqG7YTtUSvZGDTyP
wrsVhc9Ej0XDVkTX0JQvcLQVtDV4JwV/0ZuC+TgTT8a4jPI3g8NyrVIUC0H25AKKKv33IMSH11jacv0Ltb
lo1MYdem4hIzkTLyItP4TYioK9orqeJcJhwmP++rORg8iLR0VrOo5jdCj6PwXW+NNoHgwgoboRzcdKM8G/
l7/034BOpGN7HDirWF6XrU/72k28z8S9sqemF6VsoupW0T+nwDxQyRrSOSWmrigkD6mE02WPNi4vR1bKEf
0QvLxr7xewh7NSGFv2e3LscqkfcP0JB0eup2ViL9J8452B2SKZy9GRcXXi53IXWEtrYafQqlvh7rTdr2mX
c3Ew3ef3NcvyHKaHC/lVt3qN7r8cygoqrDNm/+rmAnNVw7lu27QvaxYWXJVRWSSXwPyWvKYxncpE6c3qUU
GHG7yQyNzIQXmmDgTG70b6KmKyearbPpXzXfDqvRQBwNfKZiG+mu0GbUuzovkVsxSWT4WwO4Ky3haJOHJo
XpUhmM/25CeipsP6wjjOQqf1Sp9wtliI+5swVc0TC8/H81sE9yc+DoyADTCCbdPO74WdVpvNKvm/hDZuH/
Lz1Iwhhh3WJd3+BWnIezrH1RBN/McBJdQ5jVoe6fv/mdzJ/T7oYE/nk+9C16FSPB5gVnK8RK6dPay7JaO2
kr2a8dK0pBOPquMpaEbE3qtx3DdPJBIAV2pFZ5EUhRkojAhhBJQ5bYmAvhbJkXDlomIArKhr235/uRIrEE
W8BDzjsI5QxIO2xxeNK+Z/VPd87w5BHayWs/F9cwshoQw06vLVB+JZVrj6QV6qgodHQ+ZgtzWh8pC2ZHsy
b6YesGq6ijWfG6IWFLGnSWvSiHgB75K/lzW8McFM4J/PPKXIA1rFlUEBK07fMsw/VeNEWmWSd4rOX3cZMk
Vi3YhcgX6j1kqmoGX6MAgTEIh2jn+pP6n2aJv47lFdGa2DBb3DEBZYwVRmqMUzDro04x85EqXY9EuYGN0L
xfKWeNy3AElCK4ai8WnHfcMsJ10iNixCtMoVXcQRUAvBNsB7wDmL9O08aVnh/HwDXIL7+meu0QxFWLexIQ
5V+ewQn7tCtL16IXGDtoTzkgZRriqB67gX3JHm1xMLNjTYfjkHCAEMMgwBQA/cXKnSIGUlRUVjR/ZCGFOk
irNlgQ7Ez8LwB/nQm4v9EEiN9rjVLGtJlAhSn0i7nHCzLTpEKxnpVDX0DXsXTuwPv7c+IbAs2bEXeweYla
CQ2ZAoE+YaCeuXCJAzn5F8WJdgHysXqB4nDxVfVS34b9DIBtWW22GKc/i4Rr8mvotvrZ0oTbdYAt8tG3kx
YIhD+2iQ3qciNGtsf47rwBznKuLy0H7hcwYIhJh6J3zFQqfpqPNxNrXfPHwDtYR/nc112KBp81OOhPYZE8
bMx4G8Tip1Z+tfdBv4xgofHwNtute33lgyo2XbTStIUvXTw3HP7LCHkYzMv2T6K7cztFKv/m3GcwLy2Umo
JaL042onpECH39bDy61O0BZ+XyJjoq/7eEw7c68yHkwbaSFHXtte2PcIVt2SYNI54cak/AkgmfOz3k/B6q
9iH2xFFSj5364C65XzEj3A+jnJc5urSn2iSuO2z/o33jsNQN3P5Ww2VfoSnXHXT0PQeB41pyTGLDz4O0fo
9Ys85dm6VeFS6MdRYu86eDbbXqVK5DDU5Vsaium9lbOGJXbv/Xd8dCJCGcGa8aE1fv4iH09NDCzvqIRPbf
6WB187PedWjAJDUkwDj7ua65Lk7d/h2MG5V5Y/GeR0I5cxUUG1uDsdl1rBH+LEmYCmAHOzo1WwnOHT3XdC
CY3SYlo8iC7ykp30tc0KmMXWaz+u+McTtPOON4HwqSjpzcMJx3v/OHD6L1oFLIM+BykG1a2ibL7h4+o3XL
9YezS1M5C/hI4vglqkiAV0mrtRx8dE1l04RAOeZHZ7ApRhpuULuTiqWU+vWvOE8yFfJcc/luN+0gsMO1uF
Ggk6qvzk+TzWlLhsz0QPi3O4bu7SWqqD94FzXVFCsRZq2A3M5zbpOeFBMbbWaTE95ijQS6DhkV3sxXM0iu
eSzilT6pJ2zQ/FLlRZf6BCpWcwpYV8fMoUZ9Fu7X25N8Uqm6qVicNT75oJNT+5TFv6dm96OxpwmoNrRWHW
gvRX2BtlwTEfPpkzOnyVf7acARbMZpe7Rr79p3xVNY46IiaL5x8gddVzYpPzBWVW1Bof1eqz+oEP/hR1fT
H9trHF1XOW8uUqW/772Y6pOuuwPVqx49l6S+X5nSkb5MeGlw3DNvDe98oWMCVCJbn0xB1FTTBjFfBtIPSV
pqVRndZRntwkxaQ5pT6nqj/S8e94dRkwn971IGTPeV3axjJRF/x9wZQajgJdyvz7SK/2FTUEzh6BNPfcrn
AVT/OvZDPG3s3MbaFOSO1hL2tXkR4gjbIeOVViLoZIL5abQ1ridhO89ZDSQQeTg5nBdHyPishoJzLarJkC
Ye8cSW1LnB24pG9XdkVkRi78tss2dHZq36jT0xXCmhSHcPP0pbLuJpN7X7wkW13g7wn0GoP19NIdCvY3J4
1OXzQy/xAYhBAdMAN1+Y9n+L8mGmF0qq6gH1OQfgHoqMT68hBE09jWT5mTGvrOhaBIuk42+7l8Mo92jHUa
2GpR651MHCjsMFXCULfkTc++yCPS8xfRarywcMa1uZ/6Sxl39FfS6i13gNOhgewx7WGxxvBbXKbSlAXIiE
4Q0kuaAIFm/1VBEqGFfjjQou0sjOR8uCc4KmPMCMd6F1q9qCWjhwh0UJWMfsMTRw+7FNDCFsh3Vjto2gv8
5428Z+7fF9KJpsmz8SvGvwQhuXVItotk6SYdMQHw4aihoMDJQlheNaLo4QBauZesSOWoHOpSxIOWAciIqC
```

```
EUIi5OSfJROx3PUZpbKewNrGMU3MRH02/Qdic17YT+JTGXlJ7tZJFpxvesatxCSHcd/K76jupJ5B4Q4SOk
DXD/zCJyI+PloY+Wb2j83WjDA9MJL59nmaN1t4tu35hPxEuEgs54mGKM152Emz8EkgseOvIdPs3PrpPmxv
YCAl0DfUWQldPOUmxjcVM6Ddl2nQaUgftvJIliaNw/orrCYORF4RBTIFzVexHtBsPT0uFSr6C1G6ebVhL9
Bbw3BClmpCox7wiuLdEkvZDCQGPIlAcmyMpxlvbmIf1uj7XlshxnW3WdVsnBYC9LHFXhrt5Cot5L7rYdSc
PJKbTssdgWATQarX4F+dPgLft+7mEBZaQ3dnqhdgq9RyPx2OkpigrXBBcW6IHZXMbwBNl4CzXmy4ij/8qT
8i2/sOuI85Y/JZmHLzbO8CtkK6/nn6S8CQKB0+XJHspHgxAssLo0tg0WIu/yXmdPDRYi7/JeZ0/zie7vg7
YXBByiaHnbpG40Xr9lJhO3Jcm/FGrfP7Fsqlq9QqKNBZLhLA/6IeGIK+U39ptGV3W6t4Qu/HC3X2BVsuDT
tm3lRxXusVtN4EkeqGluzC0iBYEqN/abRld1urcUjI7mQkPlhNgpKHDJSTR/0oAqt4YHN3uzeWuMJNXT/A
FlpDd2eqF2/aS8M1yGV0OLZcKe6O21eViSf/LNVPDOi2XCnujttXm9xEmOR3YVHh/FEwoioJHjpkItPtY6
89O6DGTIBz35GaIknZcgJG3F6dKs5OJXVaRqRKNHd2OqlEvnt7ATW9uRa/sXZ8OYa/vTsXPOT+oW3FW5z1
LTTGxH3xdKT4ELN31wldQeaHapo8RDwLQBi4rBBWp0zUSaWvWeMoM4Ip8YYuQb8IeaYh/YH6XtA/CUy3dM
q/LEWzAL7o+TZ9MNJCgP923Z8jG/HyaTtImNi83zEkrpz8gTIYtaSw94eBqmHqrQlehj11Hq7oMz6MvLra
7WDDgUEvSs4BDIkNxBj7hNDeFFGm6ffMYLuF0PHPzCSxX94UV2J1Dl0ALw2Vp00Y6vvhMKpW9GyXpPEcwV
UzcU04GuK2Ybp0XKy4VrtUA2QB3yquE7jjy9cnj4IT5LAi5Q8qrhO448vXJJnBxPAoPeqaPmx2T3lHEojX
g2KWI6OJgSjSvAvtZTKml0OQ4arRSmHuRNBavbyajiQYYzMaYDIhfR+/Y4YWDZYVpd8N3fmZHn7EfSmQCF
hMZYD/oJE/7YdXX+dY2lmLcomDiSu3H0RWhFv6Ukc62WpME2AMmV2sbrTwjleD/k0YbbISo9GRBF5w8wDN
7gXn5HQk/kDJcrgdjwjszPLi1XLLGP45SK3WQil1cwfs8iLztqEPw/wQZHwWtGL2F34Y2fxX43v23Bzgp+
btyAWdqLSn3kxcBb60aWLA8zoBzeHP/C8wGpa3xcdfIblPKBvZpcR4Z/zw4TMvgUR0QD0CXjlP4W/znnVd
GnKNADtdpNee5B6inugjM+SzPK0WwhjnwFJqoZzKW5UjqSmXmJsFu0gCPl65uPreyBritmG6dFyqpXalpK
dVTp8qrhO448vXJE1aeEiECZkG0o0G4pddakJSupmQ5Sj90aIAFvm1qaEnyCeX2/OS54+D+IAm+bpRmtuq
WbagE8BKc0NfqtbY6ZArZvyW3yLNq67I4UUqIX4hRRNWmXkdY2LyCdl9H6xmbvU+K3eLa/wWwPv0LBi13N
N+mmz8WhCYQ5rgXlxw2Js6N+Qc//vG93T1X+RsNLcYM2M5nfLQtsmAMMCQ20Xr0+87gmfFXPyy5tkb+3qV
6JX9W6r+t1zoK+PJYANIA7mOr9IZhepp3a7rPekvV6cVtJaD97rObpe8JJCUUL6XkS55uy6XXcPjVPfSE/
1et+EkS67I4UUqIX4lRHbRma4Gys1PpWliGBCX/ofXjuTJRxXeDSJJBRf2DvnrVcG1X1g+jAclNfe5N/hL
PiwnhZRNH6oqjOhEqRzY+kugjl0aMYTOBS0nn+gYtX1M4V+RfpmAwj4ZFJU0FXQfpd6yTAWNwWqLEMRC2o
m71dJMmOt8qk6UlmBJF+lRVVNZYU/tRfHfyeMoM4Ip8YYuJBhjMxpgMiEB6+q9W4OclHRA7odT3V2TUO95
M4jhlEkfslEh0ZUzgFJqoZzKW5UjFKU57Ltr2gixT/WpMQP0RVx+J4SHpSfktwtdb52eNtga4rZhunRcol
Dq2iTP33kXpuIthzqI9PxkWPW48279NBPybLBdETY6E7HaYflHsoXIikiIkx0q2j5sdk95RxKP/C8wGpa3
xczWE6yKM9cNgFanTNRJpa9U+NvKh/ObMj0XhQ7RYtzsS4elLHh5ejJqkQ/SX8iEJxEd7D8ctvKiQ6I0Gw
VSKJC7xvqjU5d5GmxM+RPGQMe9dTYjOydsJkSPjtC5N08QuDGmWevLwaBvB41B5xEFq1IOQBnM8+EpZErZ
EKGF2vSoSBritmG6dFynM8rDlBp9gHuunhF8623TO1Rh0llv1U0JPNzO1o0cM0E48RmC33m6hZiiqvHkRX
t7vcxqD5sJI75ouAxGTA1iQfAc3FZ4ceBTFKU57Ltr2gr1ZNIs9//qFu4wI/h+pAB4Jm/fV+3Mn7DwD87j
Rcz1SSwlAuLoxvDwur4q/xm759E5Tj1BCPVe/47QuTdPELgzundhiajgjcpKLUk9hyzoThKRXPqzYSdC+o
iOIVPg5Zz4OkLt27QXtXh1Auyao5798jmlntghmNTaSQmN5USnHyquE7jjy9cpweyAJvc6Sw5AGczz4Slk
QHJUQBKDZG1XPLmkuETNQqy4VrtUA2QB0ts8l7aAcetxjnSJgDCaJ7Lk91VZqV3dAyNtsS0YaX1nGJJv23
6QnjhtshKj0ZEEU2q9up/gdPHWH0SyqhtLJeNUKyVUxnDxZAiC7d87c9NMFrRi9hd+GNwVOLDRKtQSpBPy
bLBdETYxkPWy7NnjdVgiXgM3VE9iYTZgz/d+rSyvKq4TuOPL1ydfIblPKBvZpCNyiIcIsYpFpDCb3NmJ5z
ks6jWRYhaxYJm6ympRfGta2RDEqrxvige7QV9HBmFYjzuCZ8Vc/LLr18OArxvm2LAwwJDbRevT6hDfFZFA
yfeeq7UsoTC8DILMqi+fJcHIQ8lgA0gDuY6tsjwmStfMLn7j2skedDYLbaatRRJQOpy/FiesFLvm1yxzkV
xoLrwiaWtFPrfnHqKErqui7r2WHjH5QJ6wLe6H+p4j+lO9dSVH0WbHvPEEPDePghPksCLlC1hw3itd1j8L
VGVy2HTd2m2sADxNBZXqsL2HPKudHavWn/qUSzisfn/Qz0tND/jPYmL6P6vegZiSTlvYOlAeg5LCpuy6Tm
F0VkeYmFHXlTf/aVq79msc3Ixi+3zWddfvILM9zYC044+b2ieRTUE/a+7FQsi2uHAr4TuZsxbQ4XxJ3OJb
UcgPbuNJ55egsWuNFG0WFVTbWv+t2bfTDiM+pEsRqJYaYyT2UqaRozc0agr0mzQj5L8WXqLSmrB11to7c=
Last Modified: 06-06-2023 10:20:49
================================================================================
===============
```

Checking Credential manager

https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#credentials-manager-windows-vault

```
[!] Warning: if password contains non-printable characters, it will be printed as
unicode base64 encoded string
Username: SMOHANAPRASAD@outlook.com
Password:
Target: MicrosoftAccount:user=smohanaprasad@outlook.com
PersistenceType: LocalComputer
LastWriteTime: 08-08-2023 14:07:43
================================================================================
===============
Username: prasadredeem@outlook.com
Password:
Target: MicrosoftAccount:user=prasadredeem@outlook.com
PersistenceType: LocalComputer
LastWriteTime: 08-08-2023 10:02:52
================================================================================
===============
Username: bc8fe1538e0cea54
Password: (Unicode Base64 encoded) TS5SM19CQVkuLUNjZ010TFlqeSpxeUV3TWxuU21UZkFsRHN
peXZIS3Z4WTJmV0xzeXVrYVcqVHBSQ3dXS2dZITFKYmtoVFlJYmg5aTlwRWREYmM2NXlJaFhQdkRWOEYzU
G5VcG1sTzhjc2gxbUs3OXMwRGd4MUJwKngxQ3ZvdDM5Z05kSFd4TG5kOEdScnNVaWxkKmlvMHpBNWFNMG9
1UDVWcUNzZVNRUWhSaEg1OGM0cnQybmlOSmk5S0h4dG13RElXMllFd0c5SzNERiFrZldVOGZBdUpUaGRnY
2hXc2xuTjBMbnpCalRhNmV5OG4hTnhDRCF1SlZPZjN3RWl6VWsyT2EwITRDU1JvYTNPTE5ScDIqbTgxc3R
```

```
ReTZzV2pYaUJKYkxEWDQwQzhCand6MTBpRVNXS1EzSGZCbkl1U2hFKmFqNlh4ZWxmIXckJA==
Target: OneDrive Cached Credential
PersistenceType: LocalComputer
LastWriteTime: 25-01-2023 12:06:19
================================================================================
===============
Username: prasadsenapathy28
Password: (Unicode Base64 encoded)
Z2hvX1pZZTlmMTBtanViRlNHc1FlbmVrc2tGRWZUemEwYzRUUlN4cg==
Target: GitHub - https://api.github.com/prasadsenapathy28
PersistenceType: Enterprise
LastWriteTime: 07-12-2022 20:35:03
================================================================================
===============
Username: live:.cid.bc8fe1538e0cea54
Password: (Unicode Base64 encoded) eyJyYXdUb2tlbiI6ImV5SmhiR2NpT2lKU1V6STFOaUlzSW1
0cFpDSTZJakV3TmlJc0luZzFkQ0k2SW05UU1XRnhRbmxmUjNoWlUzcFNhWGh1UTI1emRFNVBVMnAyY3lJc
0luUjVjQ0k2SWtwWFZDSjkuZXlKcFlYUWlPakUyTnpJNU9UQTROelFzSW1WNGNDSTZNVFkzTXpBM056STN
NaXdpYzJ0NWNHVnBaQ0k2SW14cGRtVTZMbU5wWkM1aVl6aG1aVEUxTXpobE1HTmxZVFUwSWl3aWMyTndJa
m81TlRZc0ltTnphU0k2SWpFMk56STVPVEE0TnpJaUxDSmphV1FpT2lKaVl6aG1aVEUxTXpobE1HTmxZVFU
wSWl3aVlXRjBJam94TmpBM05URXdNamMzZlEubk1DbV9feUhKWVpkNmV3a1J5SEtlSlNSR19NWnpRbXFZL
S1tb0cwaXY0d2lKaDRhVHBnQzhFWVFPSUc0d1M1NXlfQTE3NzlzZG1CNXJDazRTT0FTQUdzN2lCYWJJNjh
NM05pNUwzV1NzN2pHMEtXdWpJOVlkaXlrMzlEUFBncWktMnJhMENhZzFIVjZDV1cwb1dESDFzdzhHTFFxN
jZnc0ZmVnVuNVVvY2JWWDQ3T2w1SEpESVFaekFXNjNwdGZPRmNrRzc4cUtwQ0pYSFc2SnhKLTNrbE50OFF
pNzlQLS1QSGZOM1hvaHZWSkt4YS01REpySVo0VVpaS3RpeFNkR09DSUhPT3ozNlhUbEIyMUh5dXptR1U2S
U1oN2N6eGhpYWdMdGxVVWYwUk9GYUFRTzRSSGRGRy1CYXBRX1U1cjdUeVI3TFFjLThhRzVYdVdJelN6LWZ
RIiwiZXhwaXJhdGlvbiI6MTY3MzA3NzI3MDY5NX0=
Target: MSIX-Skype for Desktop/live:.cid.bc8fe1538e0cea54
PersistenceType: Enterprise
LastWriteTime: 06-01-2023 13:11:13
================================================================================
===============
```

Remote Desktop Server/Client Settings

```
RDP Server Settings
Network Level Authentication :
Block Clipboard Redirection :
Block COM Port Redirection :
Block Drive Redirection :
Block LPT Port Redirection :
Block PnP Device Redirection :
Block Printer Redirection :
Allow Smart Card Redirection :
RDP Client Settings
Disable Password Saving : True
Restricted Remote Administration : False
```

Recently run commands

```
a: cmd\1
MRUList: adcb
b: temp\1
c: ncpa.cpl\1
d: %temp%\1
```

Checking for DPAPI Master Keys

https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#dpapi

```
MasterKey: C:\Users\MOHANAPRASAD\AppData\Roaming\Microsoft\Protect\S-1-5-21-259912
5077-3711717779-1984677719-1001\02e95601-d6c1-4208-99aa-ea889444697d
Accessed: 08-08-2023 14:06:38
Modified: 25-01-2023 11:04:00
================================================================================
===============
```

```
MasterKey: C:\Users\MOHANAPRASAD\AppData\Roaming\Microsoft\Protect\S-1-5-21-259912
5077-3711717779-1984677719-1001\098a535c-e9d3-419d-abe7-80f9e5f812e5
Accessed: 05-02-2023 23:06:27
Modified: 18-07-2022 15:06:59
================================================================================
===============
MasterKey: C:\Users\MOHANAPRASAD\AppData\Roaming\Microsoft\Protect\S-1-5-21-259912
5077-3711717779-1984677719-1001\1370821f-523a-4286-9066-e5af4d9add7c
Accessed: 08-08-2023 14:05:57
Modified: 25-07-2023 09:49:54
================================================================================
===============
MasterKey: C:\Users\MOHANAPRASAD\AppData\Roaming\Microsoft\Protect\S-1-5-21-259912
5077-3711717779-1984677719-1001\36d04b08-c14a-406d-a1ec-da2cc897b8ed
Accessed: 05-02-2023 23:06:27
Modified: 18-07-2022 15:06:59
================================================================================
===============
MasterKey: C:\Users\MOHANAPRASAD\AppData\Roaming\Microsoft\Protect\S-1-5-21-259912
5077-3711717779-1984677719-1001\3c33d0a7-9369-433c-a912-efa2fe6ac0af
Accessed: 08-08-2023 14:05:57
Modified: 26-04-2023 09:01:27
================================================================================
===============
MasterKey: C:\Users\MOHANAPRASAD\AppData\Roaming\Microsoft\Protect\S-1-5-21-259912
5077-3711717779-1984677719-1001\4369709a-fd5a-43a0-8314-abd5675e20d2
Accessed: 08-08-2023 09:56:29
Modified: 18-07-2022 15:06:59
================================================================================
===============
MasterKey: C:\Users\MOHANAPRASAD\AppData\Roaming\Microsoft\Protect\S-1-5-21-259912
5077-3711717779-1984677719-1001\50a322c8-eb8e-497e-8d9b-de8265c754c7
Accessed: 06-06-2023 23:53:53
Modified: 18-07-2022 15:06:59
================================================================================
===============
MasterKey: C:\Users\MOHANAPRASAD\AppData\Roaming\Microsoft\Protect\S-1-5-21-259912
5077-3711717779-1984677719-1001\6b241a57-a850-470c-9ea6-442eb4659723
Accessed: 08-08-2023 09:13:19
Modified: 18-07-2022 15:06:59
================================================================================
===============
MasterKey: C:\Users\MOHANAPRASAD\AppData\Roaming\Microsoft\Protect\S-1-5-21-259912
5077-3711717779-1984677719-1001\6f264f08-8121-4494-9dee-5c43652ecb8f
Accessed: 08-08-2023 09:56:29
Modified: 18-07-2022 15:06:59
================================================================================
===============
MasterKey: C:\Users\MOHANAPRASAD\AppData\Roaming\Microsoft\Protect\S-1-5-21-259912
5077-3711717779-1984677719-1001\e301c332-c436-4199-8c50-8d19af2a07ff
Accessed: 13-06-2023 22:43:00
Modified: 18-07-2022 15:06:59
================================================================================
===============
MasterKey: C:\Users\MOHANAPRASAD\AppData\Roaming\Microsoft\Protect\S-1-5-21-259912
5077-3711717779-1984677719-1001\f67d5977-e387-45e8-bfe3-a7fb9119be48
Accessed: 08-08-2023 09:54:06
Modified: 27-10-2022 10:27:21
================================================================================
===============
MasterKey: C:\Users\MOHANAPRASAD\AppData\Roaming\Microsoft\Protect\S-1-5-21-259912
5077-3711717779-1984677719-1001\f9bb1cfa-f0a1-473a-9f23-fa24865d2068
Accessed: 05-02-2023 23:06:27
Modified: 18-07-2022 15:06:59
================================================================================
===============
```

Checking for DPAPI Credential Files

https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#dpapi

Follow the provided link for further instructions in how to decrypt the creds file

```
CredFile: C:\Users\MOHANAPRASAD\AppData\Local\Microsoft\Credentials\378D493C2D85BB
CD8283D8BE243001D7
Description: Local Credential Data
■■
MasterKey: 1370821f-523a-4286-9066-e5af4d9add7c
Accessed: 08-08-2023 14:07:43
Modified: 08-08-2023 14:07:43
Size: 4400
================================================================================
===============
CredFile: C:\Users\MOHANAPRASAD\AppData\Local\Microsoft\Credentials\B5626D97E9DFBF
7A5FE21A0D802989DE
Description: Local Credential Data
■■
MasterKey: 1370821f-523a-4286-9066-e5af4d9add7c
Accessed: 08-08-2023 14:07:43
Modified: 08-08-2023 10:02:52
Size: 3920
================================================================================
===============
CredFile: C:\Users\MOHANAPRASAD\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19
A398EBF1B96859CE5D
Description: Local Credential Data
■■
MasterKey: 3c33d0a7-9369-433c-a912-efa2fe6ac0af
Accessed: 08-08-2023 14:07:43
Modified: 28-06-2023 14:58:14
Size: 11552
================================================================================
===============
CredFile: C:\Users\MOHANAPRASAD\AppData\Local\Microsoft\Credentials\E05DBE15D38053
457F3523A375594044
Description: Local Credential Data
■■
MasterKey: 02e95601-d6c1-4208-99aa-ea889444697d
Accessed: 08-08-2023 14:07:43
Modified: 25-01-2023 12:06:19
Size: 1232
================================================================================
===============
CredFile: C:\Users\MOHANAPRASAD\AppData\Roaming\Microsoft\Credentials\65C5E1FB51A7
D2C07A9CC4E8DC50C060
Description: Enterprise Credential Data
■■
MasterKey: f67d5977-e387-45e8-bfe3-a7fb9119be48
Accessed: 08-08-2023 12:44:22
Modified: 07-12-2022 20:35:03
Size: 586
================================================================================
===============
CredFile: C:\Users\MOHANAPRASAD\AppData\Roaming\Microsoft\Credentials\AF3AC1D7CA70
E29BDE520CFAC3AE1272
Description: Enterprise Credential Data
■■
MasterKey: f67d5977-e387-45e8-bfe3-a7fb9119be48
Accessed: 08-08-2023 12:44:22
Modified: 06-01-2023 13:11:13
Size: 1242
================================================================================
===============
```

Looking for saved Wifi credentials

```
SSID : 'CUTM KAVACH -2
' password : 'cutm@#kavach'
SSID : 'redmi 9A
' password : '26042004'
SSID : 'CUTM-LIBRARY
' password : 'cit@cutm'
SSID : 'vivo
' password : 'sundarnaveen'
SSID : 'SKCET_WiFi
' password : '$kcet@123'
SSID : 'SKCET_WIFI
```

```
' password : '$kcet@123'
SSID : 'OnePlus Nord CE 2 Lite 2
' password : 'spidey200522'
SSID : 'Xiaomi 11i
' password : 'utmaginesh'
SSID : 'Prithu
' password : 'qwerty555'
SSID : 'pricilla's Galaxy A71
' password : 'pricipaul94'
SSID : 'NW LAB
' password : '$kcet@123'
SSID : 'C3 BLOCK
' password : 'Wifi@123'
SSID : 'SKCET BOYS HOSTEL
' password : 'Hostel@123'
SSID : 'i2it-Wireless 3
' password : 'Hackathon@i2it3'
SSID : 'Maheshwari 5G
' password : '7401616777'
SSID : '??????????
' password : 'thismfdontmiss'
SSID : 'realme 8 Pro
' password : 'amsu2005'
SSID : 'OPPO A54
' password : '736f1ba3f138'
SSID : 'Redmi 2
' password : 'pranika123'
SSID : 'Sathish M51
' password : '7401616777'
SSID : 'vivo 1811 2
' password : 'Myaccount@123'
SSID : 'AgAAAOQmDR8APwF4Redmi 3S
' password : 'Myaccount@123'
SSID : 'PONS
' password : '9962875050'
SSID : 'sathish
' password : 'electrogreen'
SSID : 'Airtel-MyWiFi-AMF-311WW-37F7
' password : '1df29d2a'
SSID : 'CAAAAIv4exMAfwGZRedmi Note 4
' password : 'Myaccount@123'
SSID : 'HONOR Pad 5 2
' password : 'Myaccount@123'
SSID : 'senthil
' password : 's1234567890'
SSID : 'Redme save
' password : '55235523'
SSID : 'DotCom
' password : 'dot@98410'
```

Looking AppCmd.exe

https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#appcmd.exe

```
Not Found
You must be an administrator to run this check
```

Enumerating Security Packages Credentials

```
Version: NetNTLMv2
Hash: MOHANAPRASAD::LAPTOP-9R1PMVC2:1122334455667788:d05aa94eed8658b3a0df758848b87
e51:0101000000000000461d34ddac9d901a527b7cd08e3c1f60000000008003000300000000000000
0001000000000200000ff3349976c0c3e10615bca5b3e1b5599b8909352eb4d175165d1ee5bdbc0ab16
0a0010000000000000000000000000000000000000900000000000000000000
================================================================================
===============
```

Browsers Information

Firefox history -- limit 50

```
https://www.youtube.com
https://www.youtube.com
https://search.norton.com/safewebOnboarding?SSDCAT=321&lang=en&installSource=direc
t&source=direct&product=ngc&year=2015&guid=F7501B64-FB32-4FF1-89CB-AF13F88774AF&ve
r=22.23.4.6%3Fversion%3D22.23.4.6&layouttype=OEM&cipherid=0&partnerid=29500&puid=5
412&templatecat=SBU_W_29500_5412_21386627_NSBU_OEM_1&schemacat=SBU_W&schemaver=1.0
.0.0&olpchannel=LIMITED_OEM&osvers=10.0&oslocale=iso%3AIND&oslang=iso%3AENG&os=win
dows&cmpgn=may23&ShowUninstallSurvey=1&installStatus=updated&vendor=none&vendorsrc
=Firefox&machineLocation=IN&SW=0&3IN1=0&NPW=0&HP=0&DSP=0&browser=Firefox&cdest=dir
ectBrowsing
https://www.msn.com/en-in/?pc=ACTEMSN
https://search.norton.com/protect?&SSDCAT=321&installSource=direct&source=direct&p
roduct=ngc&year=2015&guid=F7501B64-FB32-4FF1-89CB-AF13F88774AF&ver=22.20.5.40&vers
ion=22.20.5.40&layouttype=OEM&cipherid=0&partnerid=29500&puid=5412&templatecat=SBU
_W_29500_5412_21386627_NSBU_OEM&schemacat=SBU_W&schemaver=1.0.0.0&olpchannel=LIMIT
ED_OEM&osvers=10.0&oslocale=iso%3aIND&oslang=iso%3aENG&os=windows&ShowUninstallSur
vey=1&installStatus=new&vendor=none&vendorsrc=Firefox&machineLocation=IN&browser=F
irefox&cdest=direct&geoLoc=IN&isROWStatus=true&cmpgn=nov20&vendorOffered=askBrowsi
ng
https://search.norton.com/client?&SSDCAT=321&installSource=direct&source=direct&pr
oduct=ngc&year=2015&guid=F7501B64-FB32-4FF1-89CB-AF13F88774AF&ver=22.20.5.40&versi
on=22.20.5.40&layouttype=OEM&cipherid=0&partnerid=29500&puid=5412&templatecat=SBU_
W_29500_5412_21386627_NSBU_OEM&schemacat=SBU_W&schemaver=1.0.0.0&olpchannel=LIMITE
D_OEM&osvers=10.0&oslocale=iso%3aIND&oslang=iso%3aENG&os=windows&ShowUninstallSurv
ey=1&installStatus=new&vendor=none&vendorsrc=Firefox&machineLocation=IN&browser=Fi
refox&cdest=directBrowsing
https://www.youtube.com/YouTubemoc.ebutuoy.www
https://www.mozilla.org/media/img/mozorg/mozilla-256.4720741d4108.jpg
```

Showing saved credentials for Brave Browser

```
Url: http://172.16.17.254:2280/submit/user_login.php
Username: 22CSE107
Password: Myaccount@123
================================================================================
==============
Url: http://172.16.58.100:2280/submit/user_login.php
Username: 22CSE107
Password: Myaccount@123
================================================================================
==============
Url: https://account.jetbrains.com/create-account
Username: prasadsenapathy28
Password: prasad123@#*senapathy
================================================================================
==============
Url: https://amcatglobal.aspiringminds.com/
Username: mohanaprasad45@gmail.com
Password: SgLPjSwQ
================================================================================
==============
Url: https://amcatglobal.aspiringminds.com/
Username: mohanaprasad45@gmail.com_gb46
Password: R8Eoo2ck
================================================================================
==============
Url: https://animoto.com/builder/templates
Username: mohanaprasad45@gmail.com
Password: Myaccount@123
================================================================================
==============
Url: https://devfolio.co/
```

```
Username: m8
Password: Myaccount@123
================================================================================
==============
Url: https://github.com/session
Username: prasadsenapathy28
Password: prasad123@#*
================================================================================
==============
Url: https://home.openweathermap.org/users
Username: mohanaprasad45@gmail.com
Password: Myaccount@123
================================================================================
==============
Url:
Username: mohanaprasad45@gmail.com
Password: Myaccount@123
================================================================================
==============
Url:
Username: 22cse107@skcet.ac.in
Password: Myaccount@123
================================================================================
==============
Url: https://skcet530.examly.io/
Username: 2
Password: Myaccount@123
================================================================================
==============
Url: https://skcet530.examly.io/
Username: 22CSE107@skcet.ac.in
Password: 22cse107
================================================================================
==============
Url: https://skcet530.examly.io/
Username: 22cse102@skcet.ac.in
Password: 22cse102
================================================================================
==============
Url: https://www.amazon.in/ap/signin
Username: electrogreen2017@gmail.com
Password: 7401616777
================================================================================
==============
Url: https://www.linkedin.com/signup/cold-join
Username: mohanaprasad45@gmail.com
Password: Myaccount@123
================================================================================
==============
Url: https://www.tneaonline.org/user/login
Username: mohanaprasad45@gmail.com
Password: Myaccount@123
================================================================================
==============
```

IE favorites

```
http://go.microsoft.com/fwlink/p/?LinkId=255142
http://www.acer.com
```

Interesting files and registry

Enumerating Office 365 endpoints synced by OneDrive.

```
SID: S-1-5-19
================================================================================
===============
SID: S-1-5-20
================================================================================
===============
SID: S-1-5-21-2599125077-3711717779-1984677719-1001
Name: Business1
UserEmail SMOHANAPRASAD@outlook.com
UserFolder C:\Users\MOHANAPRASAD\OneDrive
WebServiceUrl https://www.odwebp.svc.ms
Name: Personal
UserEmail SMOHANAPRASAD@outlook.com
UserFolder C:\Users\MOHANAPRASAD\OneDrive
WebServiceUrl https://www.odwebp.svc.ms
LibraryType personal
LastModifiedTime 2023-08-08T04:25:45 (Tue 08 Aug 2023 04:25:45)
MountPoint C:\Users\MOHANAPRASAD\OneDrive
UrlNamespace https://d.docs.live.net
================================================================================
===============
SID: S-1-5-18
================================================================================
===============
```

Looking for possible regs with creds

https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#inside-the-registry

```
Not Found
Not Found
Not Found
Not Found
```

Looking for possible password files in users homes

https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#credentials-inside-files

```
C:\Users\MOHANAPRASAD\AppData\Roaming\Code\User\workspaceStorage\54432434e07f9b0de
1ef43397010e20c\ms-vscode.js-debug\.profile\ZxcvbnData\1\passwords.txt
C:\Users\MOHANAPRASAD\AppData\Local\Google\Chrome\User
Data\ZxcvbnData\3\passwords.txt
C:\Users\MOHANAPRASAD\AppData\Local\Packages\Microsoft.GetHelp_8wekyb3d8bbwe\Local
State\EBWebView\ZxcvbnData\3.0.0.0\passwords.txt
C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Lib\site-packages\dj
ango\contrib\auth\templates\registration\password_reset_subject.txt
C:\Users\MOHANAPRASAD\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\
Extensions\admmjipmmciaobhojoghlmleefbicajg\8.0.4.39_0\password_changer_rules.json
C:\Users\MOHANAPRASAD\OneDrive\Documents\MY PASSWORDS.xlsx
```

Searching known files that can contain creds in home

https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#credentials-inside-files

```
C:\Users\MOHANAPRASAD\.vscode\extensions\ms-python.python-2023.14.0\.devcontainer\
Dockerfile
C:\Users\MOHANAPRASAD\AppData\Local\Packages\Microsoft.SkypeApp_kzf8qxf38zg5c\Loca
lState\dtlscert.der
C:\Users\MOHANAPRASAD\AppData\Local\Packages\Microsoft.SkypeApp_kzf8qxf38zg5c\Loca
lState\dtlskey.der
```

Looking for documents --limit 100--

```
C:\Users\MOHANAPRASAD\anaconda3\pkgs\xlrd-2.0.1-pyhd3eb1b0_0\info\test\test.xls
C:\Users\MOHANAPRASAD\anaconda3\pkgs\xlrd-2.0.1-pyhd3eb1b0_0\info\recipe\test.xls
C:\Users\MOHANAPRASAD\anaconda3\pkgs\matplotlib-base-3.5.2-py39hd77b12b_0\Lib\site
-packages\matplotlib\mpl-data\images\back.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\matplotlib-base-3.5.2-py39hd77b12b_0\Lib\site
-packages\matplotlib\mpl-data\images\filesave.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\matplotlib-base-3.5.2-py39hd77b12b_0\Lib\site
-packages\matplotlib\mpl-data\images\forward.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\matplotlib-base-3.5.2-py39hd77b12b_0\Lib\site
-packages\matplotlib\mpl-data\images\hand.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\matplotlib-base-3.5.2-py39hd77b12b_0\Lib\site
-packages\matplotlib\mpl-data\images\help.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\matplotlib-base-3.5.2-py39hd77b12b_0\Lib\site
-packages\matplotlib\mpl-data\images\home.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\matplotlib-base-3.5.2-py39hd77b12b_0\Lib\site
-packages\matplotlib\mpl-data\images\matplotlib.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\matplotlib-base-3.5.2-py39hd77b12b_0\Lib\site
-packages\matplotlib\mpl-data\images\move.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\matplotlib-base-3.5.2-py39hd77b12b_0\Lib\site
-packages\matplotlib\mpl-data\images\qt4_editor_options.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\matplotlib-base-3.5.2-py39hd77b12b_0\Lib\site
-packages\matplotlib\mpl-data\images\subplots.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\matplotlib-base-3.5.2-py39hd77b12b_0\Lib\site
-packages\matplotlib\mpl-data\images\zoom_to_rect.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\binaryornot-0.4.4-pyhd3eb1b0_1\info\test\test
s\isBinaryFile\pdf.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\sphinx-5.0.2-py39haa95532_0\Lib\site-packages
\sphinx\ext\__pycache__\inheritance_diagram.cpython-39.pyc
C:\Users\MOHANAPRASAD\anaconda3\pkgs\sphinx-5.0.2-py39haa95532_0\Lib\site-packages
\sphinx\ext\inheritance_diagram.py
C:\Users\MOHANAPRASAD\anaconda3\pkgs\libarchive-3.6.1-hebabd0d_0\Library\share\man
\pdf\tar.5.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\libarchive-3.6.1-hebabd0d_0\Library\share\man
\pdf\mtree.5.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\libarchive-3.6.1-hebabd0d_0\Library\share\man
\pdf\libarchive_internals.3.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\libarchive-3.6.1-hebabd0d_0\Library\share\man
\pdf\libarchive_changes.3.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\libarchive-3.6.1-hebabd0d_0\Library\share\man
\pdf\libarchive.3.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\libarchive-3.6.1-hebabd0d_0\Library\share\man
\pdf\libarchive-formats.5.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\libarchive-3.6.1-hebabd0d_0\Library\share\man
\pdf\cpio.5.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\libarchive-3.6.1-hebabd0d_0\Library\share\man
\pdf\bsdtar.1.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\libarchive-3.6.1-hebabd0d_0\Library\share\man
\pdf\bsdcpio.1.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\libarchive-3.6.1-hebabd0d_0\Library\share\man
\pdf\archive_write_set_passphrase.3.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\libarchive-3.6.1-hebabd0d_0\Library\share\man
\pdf\archive_write_set_options.3.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\libarchive-3.6.1-hebabd0d_0\Library\share\man
\pdf\archive_write_open.3.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\libarchive-3.6.1-hebabd0d_0\Library\share\man
\pdf\archive_write_new.3.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\libarchive-3.6.1-hebabd0d_0\Library\share\man
\pdf\archive_write_header.3.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\libarchive-3.6.1-hebabd0d_0\Library\share\man
\pdf\archive_write_free.3.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\libarchive-3.6.1-hebabd0d_0\Library\share\man
\pdf\archive_write_format.3.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\libarchive-3.6.1-hebabd0d_0\Library\share\man
\pdf\archive_write_finish_entry.3.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\libarchive-3.6.1-hebabd0d_0\Library\share\man
\pdf\archive_write_filter.3.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\libarchive-3.6.1-hebabd0d_0\Library\share\man
\pdf\archive_write_disk.3.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\libarchive-3.6.1-hebabd0d_0\Library\share\man
\pdf\archive_write_data.3.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\libarchive-3.6.1-hebabd0d_0\Library\share\man
\pdf\archive_write_blocksize.3.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\libarchive-3.6.1-hebabd0d_0\Library\share\man
\pdf\archive_write.3.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\libarchive-3.6.1-hebabd0d_0\Library\share\man
```

```
\pdf\archive_util.3.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\libarchive-3.6.1-hebabd0d_0\Library\share\man
\pdf\archive_read_set_options.3.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\libarchive-3.6.1-hebabd0d_0\Library\share\man
\pdf\archive_read_open.3.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\libarchive-3.6.1-hebabd0d_0\Library\share\man
\pdf\archive_read_new.3.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\libarchive-3.6.1-hebabd0d_0\Library\share\man
\pdf\archive_read_header.3.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\libarchive-3.6.1-hebabd0d_0\Library\share\man
\pdf\archive_read_free.3.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\libarchive-3.6.1-hebabd0d_0\Library\share\man
\pdf\archive_read_format.3.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\libarchive-3.6.1-hebabd0d_0\Library\share\man
\pdf\archive_read_filter.3.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\libarchive-3.6.1-hebabd0d_0\Library\share\man
\pdf\archive_read_extract.3.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\libarchive-3.6.1-hebabd0d_0\Library\share\man
\pdf\archive_read_disk.3.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\libarchive-3.6.1-hebabd0d_0\Library\share\man
\pdf\archive_read_data.3.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\libarchive-3.6.1-hebabd0d_0\Library\share\man
\pdf\archive_read_add_passphrase.3.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\libarchive-3.6.1-hebabd0d_0\Library\share\man
\pdf\archive_read.3.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\libarchive-3.6.1-hebabd0d_0\Library\share\man
\pdf\archive_entry_time.3.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\libarchive-3.6.1-hebabd0d_0\Library\share\man
\pdf\archive_entry_stat.3.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\libarchive-3.6.1-hebabd0d_0\Library\share\man
\pdf\archive_entry_perms.3.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\libarchive-3.6.1-hebabd0d_0\Library\share\man
\pdf\archive_entry_paths.3.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\libarchive-3.6.1-hebabd0d_0\Library\share\man
\pdf\archive_entry_misc.3.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\libarchive-3.6.1-hebabd0d_0\Library\share\man
\pdf\archive_entry_linkify.3.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\libarchive-3.6.1-hebabd0d_0\Library\share\man
\pdf\archive_entry_acl.3.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\libarchive-3.6.1-hebabd0d_0\Library\share\man
\pdf\archive_entry.3.pdf
C:\Users\MOHANAPRASAD\anaconda3\pkgs\pylint-2.14.5-py39haa95532_0\Lib\site-package
s\pylint\pyreverse\__pycache__\diagrams.cpython-39.pyc
C:\Users\MOHANAPRASAD\anaconda3\pkgs\pylint-2.14.5-py39haa95532_0\Lib\site-package
s\pylint\pyreverse\diagrams.py
C:\Users\MOHANAPRASAD\anaconda3\pkgs\sympy-1.10.1-py39haa95532_0\Lib\site-packages
\sympy\categories\__pycache__\diagram_drawing.cpython-39.pyc
C:\Users\MOHANAPRASAD\anaconda3\pkgs\sympy-1.10.1-py39haa95532_0\Lib\site-packages
\sympy\categories\diagram_drawing.py
C:\Users\MOHANAPRASAD\anaconda3\pkgs\sympy-1.10.1-py39haa95532_0\Lib\site-packages
\sympy\liealgebras\tests\test_dynkin_diagram.py
C:\Users\MOHANAPRASAD\anaconda3\pkgs\sympy-1.10.1-py39haa95532_0\Lib\site-packages
\sympy\liealgebras\tests\__pycache__\test_dynkin_diagram.cpython-39.pyc
C:\Users\MOHANAPRASAD\anaconda3\pkgs\sympy-1.10.1-py39haa95532_0\Lib\site-packages
\sympy\liealgebras\__pycache__\dynkin_diagram.cpython-39.pyc
C:\Users\MOHANAPRASAD\anaconda3\pkgs\sympy-1.10.1-py39haa95532_0\Lib\site-packages
\sympy\liealgebras\dynkin_diagram.py
C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\pylint\pyreverse\__pycache__\dia
grams.cpython-39.pyc
C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\pylint\pyreverse\diagrams.py
C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\sphinx\ext\__pycache__\inheritan
ce_diagram.cpython-39.pyc
C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\sphinx\ext\inheritance_diagram.p
y
C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\matplotlib\mpl-data\images\back.
pdf
C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\matplotlib\mpl-data\images\files
ave.pdf
C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\matplotlib\mpl-data\images\forwa
rd.pdf
C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\matplotlib\mpl-data\images\hand.
pdf
C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\matplotlib\mpl-data\images\help.
pdf
C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\matplotlib\mpl-data\images\home.
pdf
C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\matplotlib\mpl-data\images\matpl
otlib.pdf
C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\matplotlib\mpl-data\images\move.
```

```
pdf
C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\matplotlib\mpl-data\images\qt4_e
ditor_options.pdf
C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\matplotlib\mpl-data\images\subpl
ots.pdf
C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\matplotlib\mpl-data\images\zoom_
to_rect.pdf
C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\sympy\liealgebras\tests\test_dyn
kin_diagram.py
C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\sympy\liealgebras\tests\__pycach
e__\test_dynkin_diagram.cpython-39.pyc
C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\sympy\liealgebras\__pycache__\dy
nkin_diagram.cpython-39.pyc
C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\sympy\liealgebras\dynkin_diagram
.py
C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\sympy\categories\__pycache__\dia
gram_drawing.cpython-39.pyc
C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\sympy\categories\diagram_drawing
.py
C:\Users\MOHANAPRASAD\anaconda3\Library\share\man\pdf\tar.5.pdf
C:\Users\MOHANAPRASAD\anaconda3\Library\share\man\pdf\mtree.5.pdf
C:\Users\MOHANAPRASAD\anaconda3\Library\share\man\pdf\libarchive_internals.3.pdf
C:\Users\MOHANAPRASAD\anaconda3\Library\share\man\pdf\libarchive_changes.3.pdf
C:\Users\MOHANAPRASAD\anaconda3\Library\share\man\pdf\libarchive.3.pdf
C:\Users\MOHANAPRASAD\anaconda3\Library\share\man\pdf\libarchive-formats.5.pdf
C:\Users\MOHANAPRASAD\anaconda3\Library\share\man\pdf\cpio.5.pdf
C:\Users\MOHANAPRASAD\anaconda3\Library\share\man\pdf\bsdtar.1.pdf
C:\Users\MOHANAPRASAD\anaconda3\Library\share\man\pdf\bsdcpio.1.pdf
C:\Users\MOHANAPRASAD\anaconda3\Library\share\man\pdf\archive_write_set_passphrase
.3.pdf
C:\Users\MOHANAPRASAD\anaconda3\Library\share\man\pdf\archive_write_set_options.3.
pdf
C:\Users\MOHANAPRASAD\anaconda3\Library\share\man\pdf\archive_write_open.3.pdf
```

Office Most Recent Files -- limit 50

```
Last Access Date User Application Document
2023-08-03 06:14 LAPTOP-9R1PMVC2\MOHANAPRASAD Office
C:\Users\MOHANAPRASAD\Downloads\cyberuser_accessKeys.csv
2023-06-13 17:11 LAPTOP-9R1PMVC2\MOHANAPRASAD Office
C:\Users\MOHANAPRASAD\Downloads\Activity2.pdf
2023-05-09 10:26 LAPTOP-9R1PMVC2\MOHANAPRASAD Office
C:\Users\MOHANAPRASAD\OneDrive\Desktop\ideathon\ideathon.pptx
2023-03-22 10:29 LAPTOP-9R1PMVC2\MOHANAPRASAD Office C:\Users\MOHANAPRASAD\AppData
\Local\Temp\Temp1_Python-Tutorial-Supplementary-Materials.zip\Python Tutorial
Supplementary Materials\transactions.xlsx
2023-03-20 13:51 LAPTOP-9R1PMVC2\MOHANAPRASAD Office
C:\Users\MOHANAPRASAD\Downloads\SPHH-Presentation-Addressing Specific Healthcare -
Challenges - Pain Killers.pptx
2023-02-20 01:44 LAPTOP-9R1PMVC2\MOHANAPRASAD Office
C:\Users\MOHANAPRASAD\Downloads\TCS Lab Manual (2).docx
2023-02-13 08:54 LAPTOP-9R1PMVC2\MOHANAPRASAD Office
C:\Users\MOHANAPRASAD\Downloads\SPHH-Presentation-Addressing Specific Healthcare -
Challenges - Pain Killers (1).pptx
2023-02-08 04:55 LAPTOP-9R1PMVC2\MOHANAPRASAD Office
C:\Users\MOHANAPRASAD\Downloads\CONSENT FORM(edited).docx
2023-02-08 04:41 LAPTOP-9R1PMVC2\MOHANAPRASAD Office
C:\Users\MOHANAPRASAD\Downloads\CONSENT FORM.docx
2023-01-24 04:39 LAPTOP-9R1PMVC2\MOHANAPRASAD Office
C:\Users\MOHANAPRASAD\Downloads\Solution.docx
2023-01-23 16:12 LAPTOP-9R1PMVC2\MOHANAPRASAD Office
C:\Users\MOHANAPRASAD\Downloads\Lab_final_updated (1).docx
2023-01-23 16:09 LAPTOP-9R1PMVC2\MOHANAPRASAD Office
C:\Users\MOHANAPRASAD\Downloads\Lab_final_updated.docx
2023-01-22 07:19 LAPTOP-9R1PMVC2\MOHANAPRASAD Office
C:\Users\MOHANAPRASAD\Downloads\Book1.xlsx
2023-01-21 16:27 LAPTOP-9R1PMVC2\MOHANAPRASAD Office D:\skillathon bot\Bot2.xlsx
2023-01-21 07:56 LAPTOP-9R1PMVC2\MOHANAPRASAD Office
C:\Users\MOHANAPRASAD\Downloads\Lab_final (2).docx
2023-01-21 03:47 LAPTOP-9R1PMVC2\MOHANAPRASAD Office
C:\Users\MOHANAPRASAD\Downloads\Lab_final (1).docx
2022-11-14 05:16 LAPTOP-9R1PMVC2\MOHANAPRASAD Office D:\ideathon\ideathon.pptx
2022-11-14 05:15 LAPTOP-9R1PMVC2\MOHANAPRASAD Office D:\MATLAB full project with
questions\EX_3_ MATLAB - (1) PROJECT.docx
```

```
2022-11-14 05:14 LAPTOP-9R1PMVC2\MOHANAPRASAD Office D:\MATLAB full project with
questions\EX_4_MATLAB.docx
2022-11-13 10:03 LAPTOP-9R1PMVC2\MOHANAPRASAD Office
C:\Users\MOHANAPRASAD\Downloads\EX_4_MATLAB.docx
2022-11-13 10:02 LAPTOP-9R1PMVC2\MOHANAPRASAD Office
C:\Users\MOHANAPRASAD\Downloads\EX_3_ MATLAB - (1) PROJECT.docx
2022-11-13 10:02 LAPTOP-9R1PMVC2\MOHANAPRASAD Office
C:\Users\MOHANAPRASAD\Downloads\EX_3_ MATLAB - (1).docx
2022-11-13 07:12 LAPTOP-9R1PMVC2\MOHANAPRASAD Office
C:\Users\MOHANAPRASAD\OneDrive\Desktop\Frontiers Book chapters- EDITED FINAL COPY -
9.11.2022.doc
2022-11-13 07:11 LAPTOP-9R1PMVC2\MOHANAPRASAD Office
C:\Users\MOHANAPRASAD\Downloads\Frontiers Book chapters- EDITED FINAL COPY -
9.11.2022.doc
2022-11-11 06:44 LAPTOP-9R1PMVC2\MOHANAPRASAD Office
C:\Users\MOHANAPRASAD\Downloads\ideathon (1).pptx
2022-11-09 16:03 LAPTOP-9R1PMVC2\MOHANAPRASAD Office
C:\Users\MOHANAPRASAD\Downloads\EX_3_ MATLAB -.docx
2022-07-18 08:56 LAPTOP-9R1PMVC2\MOHANAPRASAD Office
C:\Users\MOHANAPRASAD\OneDrive\Documents\MY PASSWORDS.xlsx
2022-02-25 03:44 LAPTOP-9R1PMVC2\MOHANAPRASAD Office
C:\Users\MOHANAPRASAD\Downloads\Paint shop tree Cleaning used Acid (1).xlsx
2022-02-25 03:43 LAPTOP-9R1PMVC2\MOHANAPRASAD Office
C:\Users\MOHANAPRASAD\Downloads\Paint shop tree Cleaning used Acid.xlsx
2022-02-23 16:44 LAPTOP-9R1PMVC2\MOHANAPRASAD Office
C:\Users\MOHANAPRASAD\Downloads\Plant Visit.pptx
2021-06-18 14:56 LAPTOP-9R1PMVC2\MOHANAPRASAD Office
C:\Users\MOHANAPRASAD\Downloads\MY PASSWORDS.xlsx
2020-12-31 10:01 LAPTOP-9R1PMVC2\MOHANAPRASAD Office
C:\Users\MOHANAPRASAD\OneDrive\Document.docx
2020-12-31 09:25 LAPTOP-9R1PMVC2\MOHANAPRASAD Office
C:\Users\MOHANAPRASAD\Documents\MY PASSWORDS.xlsx
```

Recent files --limit 70--

```
D:\Videos\@Srilinks4k_Thunivu_2023_Tamil_1080p_Proper_TRUE_HD_AVC_UNTOUCHED.mkv(08
-08-2023 12:44:58)
C:\Users\MOHANAPRASAD\Downloads\CyberCore - KVH 018(kavach).pdf(08-08-2023
12:44:58)
C:\Users\MOHANAPRASAD\Downloads\cyberuser_accessKeys.csv(08-08-2023 12:44:58)
D:\Videos\Doctor Strange(2022) HD Multi Audio.mkv(08-08-2023 12:44:58)
C:\Users\MOHANAPRASAD\Downloads(08-08-2023 12:44:58)
C:\Users\MOHANAPRASAD\Downloads\ex (3).json(08-08-2023 12:44:58)
D:\kavach\linpeas\ex.json(08-08-2023 12:44:58)
D:\kavach\linpeas\htmlout.html(08-08-2023 13:24:30)
C:\Users\MOHANAPRASAD\OneDrive\Pictures\Paithiyam\IMG-20210801-WA0023.jpg(08-08-20
23 12:44:58)
D:\kavach(08-08-2023 14:32:33)
D:\kavach\linpeas(08-08-2023 13:25:04)
D:\kavach\linpeas(08-08-2023 12:44:58)
D:\kavach\project\linux(08-08-2023 12:44:58)
D:\kavach\project\mac(08-08-2023 12:44:58)
D:\kavach\linpeas\machtml.html(08-08-2023 13:25:04)
D:\kavach\linpeas\macpdf.pdf(08-08-2023 12:44:58)
D:\kavach\linpeas\MacPEASjson.json(08-08-2023 12:44:58)
D:\kavach\linpeas\mout.pdf(08-08-2023 12:44:58)
D:\kavach\project\windows\network(08-08-2023 12:44:58)
D:\kavach\project\New folder(08-08-2023 12:44:58)
C:\Users\MOHANAPRASAD\OneDrive\Pictures\Paithiyam(08-08-2023 12:44:58)
D:\kavach\linpeas\peas.json(08-08-2023 12:44:58)
D:\kavach\linpeas\pout.pdf(08-08-2023 12:44:58)
D:\kavach\project\windows\process(08-08-2023 12:44:58)
D:\kavach\project(08-08-2023 12:44:58)
D:\kavach\scan(08-08-2023 14:33:17)
D:\kavach\project\windows\service(08-08-2023 12:44:58)
C:\Users\MOHANAPRASAD\OneDrive\Pictures\Paithiyam\Snapchat-995196646.jpg(08-08-202
3 12:44:58)
D:\kavach\project\windows\system(08-08-2023 12:44:58)
D:\Videos(08-08-2023 12:44:58)
D:\kavach\project\windows(08-08-2023 12:44:58)
D:\kavach\linpeas\wout.pdf(08-08-2023 13:15:20)
```

Searching hidden files or folders in C:\Users home (can be slow)

```
C:\Users\All Users\CyberLink\EvoParser\PhotoDirector\8.0\Boomerang
C:\Users\All Users\CyberLink\EvoParser\PhotoDirector\8.0
C:\Users\All Users\CyberLink\EvoParser\PowerDirector\14.0\Boomerang
C:\Users\All Users\CyberLink\EvoParser\PowerDirector\14.0
C:\Users\All
Users\CyberLink\CBE\D8D760AC-ACA2-493e-9623-61E9D47DE89C\PhotoDirector8.exe_v2
C:\Users\All Users\CyberLink\CBE\D8D760AC-ACA2-493e-9623-61E9D47DE89C\PDR.exe
C:\Users\All
Users\CyberLink\CBE\D8D760AC-ACA2-493e-9623-61E9D47DE89C\OLRSubmission.exe
C:\Users\All Users\CyberLink\CAE\987e6487
C:\Users\All Users\CyberLink\CAE\987e6487\cae.lcf
C:\Users\All Users\CyberLink\CAE\cae.lcf
C:\Users\All Users\CyberLink\PowerDirector\14.0\AnalyzeCacheFiles
C:\Users\All Users\CyberLink\GDPRDlg\Shared
C:\Users\All Users\CyberLink\CLUpdater\PowerDirector\14.0
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\hlinks
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\se
f\databases\SmartListing\ha_submission_events\hlinks
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\se
f\databases\scheduler\jobsdb\hlinks
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\se
f\databases\ProcessClassifier\pc_process_events\hlinks
C:\Users\All
Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\sef\hlinks
C:\Users\All
Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\SDSLuReg\hlinks
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Re
mediation\stage\hlinks
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Qu
ickStart\hlinks
C:\Users\All
Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Product\hlinks
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Pr
oduct\Jobs\hlinks
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Pr
oduct\SymWidgets\hlinks
C:\Users\All
Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\NUM\hlinks
C:\Users\All
Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\NPC\hlinks
C:\Users\All
Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\NCW\hlinks
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\NC
P\ncpclient\data\hlinks
C:\Users\All
Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\NCO\hlinks
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Lu
e\Downloads\hlinks
C:\Users\All
Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Lue\hlinks
C:\Users\All
Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Lue\Logs\hlinks
C:\Users\All
Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Logs\hlinks
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\it
bLURegBranding\hlinks
C:\Users\All
Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\IRON\hlinks
C:\Users\All
Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\IPUA\hlinks
C:\Users\All
Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\IPS\hlinks
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Ga
meBooster\hlinks
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Fr
amework\hlinks
C:\Users\All
Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\ErrMgmt\hlinks
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Er
rMgmt\SCD\hlinks
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Do
mainCategoryProvider\hlinks
C:\Users\All
```

```
Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\diStRptr\hlinks
C:\Users\All
Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\diMaster\hlinks
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Co
nnections\hlinks
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Cm
nClnt\ccGEvt\Global\hlinks
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Cm
nClnt\ccGLog\hlinks
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Cm
nClnt\ccJobMgr\hlinks
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Cm
nClnt\ccSetMgr\hlinks
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Cm
nClnt\ccSubSDK\hlinks
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Cm
nClnt\ErrorInstances\E6058C07\hlinks
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Cm
nClnt\ErrorInstances\C0D9300A\hlinks
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Cm
nClnt\ErrorInstances\BD3547E3\hlinks
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Cm
nClnt\ErrorInstances\709A67DF\hlinks
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Cm
nClnt\ErrorInstances\4598BC13\hlinks
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Cm
nClnt\ErrorInstances\33E3AFBB\hlinks
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Cm
nClnt\ErrorInstances\1A2B2EB3\hlinks
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Cm
nClnt\ErrorInstances\162BF8BA\hlinks
C:\Users\All
Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\CmnClnt\hlinks
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Cm
nClnt\STIC\hlinks
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Cm
nClnt\_lck\_{4E9CB39A-5F78-4887-A3D6-2790DE9DDE11}6
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Cm
nClnt\_lck\_{4E9CB39A-5F78-4887-A3D6-2790DE9DDE11}22
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Cm
nClnt\_lck\_UI.Host.{1AFE47BB-FCF1-4096-9039-1FEBC9A0CCCF}6
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Cm
nClnt\_lck\_UI.Host.{1AFE47BB-FCF1-4096-9039-1FEBC9A0CCCF}22
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Cm
nClnt\_lck\_SvcMgr-A2B50D70-5EA1-45a0-A983-0DB9E7101676G
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Cm
nClnt\_lck\_SNDPluginG
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Cm
nClnt\_lck\_RDRPluginG
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Cm
nClnt\_lck\_ICFMGR_{F34173A0-C9EA-45ab-B832-29D35E6D04EC}G
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Cm
nClnt\_lck\_CSDK_Session6
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Cm
nClnt\_lck\_CSDK_Session22
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Cm
nClnt\_lck\_CSDK_ServiceG
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Cm
nClnt\_lck\_AVPAPP_{BB639333-810A-4bf8-85F5-C537857F55FC}6
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Cm
nClnt\_lck\_AVPAPP_{BB639333-810A-4bf8-85F5-C537857F55FC}22
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Cm
nClnt\_lck\hlinks\_{4E9CB39A-5F78-4887-A3D6-2790DE9DDE11}22.data
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Cm
nClnt\_lck\hlinks\_{4E9CB39A-5F78-4887-A3D6-2790DE9DDE11}1.data
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Cm
nClnt\_lck\hlinks\_UI.Host.{1AFE47BB-FCF1-4096-9039-1FEBC9A0CCCF}5.data
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Cm
nClnt\_lck\hlinks\_UI.Host.{1AFE47BB-FCF1-4096-9039-1FEBC9A0CCCF}22.data
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Cm
nClnt\_lck\hlinks\_UI.Host.{1AFE47BB-FCF1-4096-9039-1FEBC9A0CCCF}1.data
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Cm
nClnt\_lck\hlinks\_SvcMgr-A2B50D70-5EA1-45a0-A983-0DB9E7101676G.data
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Cm
nClnt\_lck\hlinks\_SNDPluginG.data
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Cm
nClnt\_lck\hlinks\_RDRPluginG.data
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Cm
nClnt\_lck\hlinks\_ICFMGR_{F34173A0-C9EA-45ab-B832-29D35E6D04EC}G.data
```

```
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Cm
nClnt\_lck\hlinks\_CSDK_Session22.data
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Cm
nClnt\_lck\hlinks\_CSDK_Session1.data
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Cm
nClnt\_lck\hlinks\_CSDK_ServiceG.data
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Cm
nClnt\_lck\hlinks\_AVPAPP_{BB639333-810A-4bf8-85F5-C537857F55FC}22.data
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Cm
nClnt\_lck\hlinks
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Cm
nClnt\_lck\hlinks\_AVPAPP_{BB639333-810A-4bf8-85F5-C537857F55FC}1.data
C:\Users\All
Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\CLT\hlinks
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\CL
T\PIF2\Content\fe0001.norton.com\pif20\production\messages\100639\0\hlinks
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\CL
T\PIF2\Content\fe0001.norton.com\pif20\production\messages\100959\0\hlinks
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Cl
ientSDK\hlinks
C:\Users\All
Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\BASH\hlinks
C:\Users\All
Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\AntiSpam\hlinks
C:\Users\All
Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Webcam\hlinks
C:\Users\All
Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\USBScan\hlinks
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\to
ds\data\hlinks
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\Sy
mWidgets\safeweb\hlinks
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\sy
mnetdrv\hlinks
C:\Users\All
Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\SymELAM\hlinks
C:\Users\All
Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\SRTSP\hlinks
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\SP
Manifests\hlinks
C:\Users\All Users\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}\NGC_22.20.5.40\So
ftwareUpdater\hlinks
C:\Users\Default User
C:\Users\Default
C:\Users\All Users
C:\Users\Public\CyberLink\OLReg\HKEY_CLASS_ROOT\CLSID\Shared
C:\Users\Public\CyberLink\OLReg\HKEY_CLASS_ROOT\CLSID\{0E664C43-955A-44a4-9262-599
F535207E1}\Version\14.0
C:\Users\Public\CyberLink\OLReg\HKEY_CLASS_ROOT\CLSID\{A2540FA5-4E6F-4a42-A327-D94
7EC8F2323}\Version\8.0
C:\Users\Default
C:\Users\MOHANAPRASAD\AppData\Local\Packages\SpotifyAB.SpotifyMusic_zpdnekdrzrea0\
AC\INetHistory\History.IE5
C:\Users\MOHANAPRASAD\AppData\Local\Packages\SpotifyAB.SpotifyMusic_zpdnekdrzrea0\
AC\INetCookies\ESE
C:\Users\MOHANAPRASAD\AppData\Local\Packages\SpotifyAB.SpotifyMusic_zpdnekdrzrea0\
AC\INetCache
C:\Users\MOHANAPRASAD\AppData\Local\Packages\GAMELOFTSA.Asphalt8Airborne_0pp20fcew
vvtj\AC\INetCookies\ESE
C:\Users\MOHANAPRASAD\AppData\Local\Packages\GAMELOFTSA.Asphalt8Airborne_0pp20fcew
vvtj\AC\INetCache
C:\Users\MOHANAPRASAD\AppData\Local\Packages\CyberLinkCorp.ac.PowerDirectorforacer
Desktop_ypz87dpxkv292\AC\INetHistory\History.IE5
C:\Users\MOHANAPRASAD\AppData\Local\Packages\CyberLinkCorp.ac.PowerDirectorforacer
Desktop_ypz87dpxkv292\AC\INetHistory\History.IE5\MSHist012020121720201218
C:\Users\MOHANAPRASAD\AppData\Local\Packages\CyberLinkCorp.ac.PowerDirectorforacer
Desktop_ypz87dpxkv292\AC\INetHistory
C:\Users\MOHANAPRASAD\AppData\Local\Packages\CyberLinkCorp.ac.PowerDirectorforacer
Desktop_ypz87dpxkv292\AC\INetCookies\ESE
C:\Users\MOHANAPRASAD\AppData\Local\Packages\CyberLinkCorp.ac.PowerDirectorforacer
Desktop_ypz87dpxkv292\AC\INetCache
C:\Users\MOHANAPRASAD\AppData\Local\Packages\CyberLinkCorp.ac.PhotoDirectorforacer
Desktop_ypz87dpxkv292\AC\INetHistory\History.IE5
C:\Users\MOHANAPRASAD\AppData\Local\Packages\CyberLinkCorp.ac.PhotoDirectorforacer
Desktop_ypz87dpxkv292\AC\INetCookies\ESE
C:\Users\MOHANAPRASAD\AppData\Local\Packages\CyberLinkCorp.ac.PhotoDirectorforacer
Desktop_ypz87dpxkv292\AC\INetCache
C:\Users\MOHANAPRASAD\AppData\Local\Packages\C27EB4BA.DropboxOEM_xbfy0k16fey96\AC\
```

```
INetHistory\BackgroundTransferApi
C:\Users\MOHANAPRASAD\AppData\Local\Packages\C27EB4BA.DropboxOEM_xbfy0k16fey96\AC\
INetHistory\BackgroundTransferApiGroup
C:\Users\MOHANAPRASAD\AppData\Local\Packages\C27EB4BA.DropboxOEM_xbfy0k16fey96\AC\
INetCookies\ESE
C:\Users\MOHANAPRASAD\AppData\Local\Packages\C27EB4BA.DropboxOEM_xbfy0k16fey96\AC\
INetCache
C:\Users\MOHANAPRASAD\AppData\Local\Packages\AmazonVideo.PrimeVideo_pwbj9vvecjh7j\
AC\INetHistory\BackgroundTransferApi
C:\Users\MOHANAPRASAD\AppData\Local\Packages\AmazonVideo.PrimeVideo_pwbj9vvecjh7j\
AC\INetHistory\BackgroundTransferApiGroup
C:\Users\MOHANAPRASAD\AppData\Local\Packages\AmazonVideo.PrimeVideo_pwbj9vvecjh7j\
AC\INetHistory
C:\Users\MOHANAPRASAD\AppData\Local\Packages\AmazonVideo.PrimeVideo_pwbj9vvecjh7j\
AC\INetCookies\ESE
C:\Users\MOHANAPRASAD\AppData\Local\Packages\AmazonVideo.PrimeVideo_pwbj9vvecjh7j\
AC\INetCache
C:\Users\MOHANAPRASAD\AppData\Local\Packages\AmazonVideo.PrimeVideo_pwbj9vvecjh7j\
AC\AppCache\8QAE8PGZ
C:\Users\MOHANAPRASAD\AppData\Local\Packages\AmazonVideo.PrimeVideo_pwbj9vvecjh7j\
AC\AppCache
C:\Users\MOHANAPRASAD\AppData\Local\Packages\AmazonVideo.PrimeVideo_pwbj9vvecjh7j\
LocalCache\PlayReady\Cache
C:\Users\MOHANAPRASAD\AppData\Local\Packages\AmazonVideo.PrimeVideo_pwbj9vvecjh7j\
LocalCache\PlayReady\uoVWs_59FeQr47HpHY_tZrTn4ZSHGCWvusWfPlxmzio=\Cache
C:\Users\MOHANAPRASAD\AppData\Local\Packages\AdvancedMicroDevicesInc-2.AMDRadeonSo
ftware_0a9344xs7nr4m\AC\INetCookies\ESE
C:\Users\MOHANAPRASAD\AppData\Local\Packages\AdvancedMicroDevicesInc-2.AMDRadeonSo
ftware_0a9344xs7nr4m\AC\INetCache
C:\Users\MOHANAPRASAD\AppData\Local\Packages\AcerIncorporated.AcerRegistration_48f
rkmn4z8aw4\AC\INetCookies\ESE
C:\Users\MOHANAPRASAD\AppData\Local\Packages\AcerIncorporated.AcerRegistration_48f
rkmn4z8aw4\AC\INetCache
C:\Users\MOHANAPRASAD\AppData\Local\Packages\A278AB0D.MarchofEmpires_h6adky7gbf63m
\AC\INetCookies\ESE
C:\Users\MOHANAPRASAD\AppData\Local\Packages\A278AB0D.MarchofEmpires_h6adky7gbf63m
\AC\INetCache
C:\Users\MOHANAPRASAD\AppData\Local\Packages\A278AB0D.Asphalt9_h6adky7gbf63m\AC\IN
etCookies\ESE
C:\Users\MOHANAPRASAD\AppData\Local\Packages\A278AB0D.Asphalt9_h6adky7gbf63m\AC\IN
etCache
C:\Users\MOHANAPRASAD\AppData\Local\Packages\6F71D7A7.HotspotShieldFreeVPN_nsbqstb
b9qxb6\AC\INetCookies\ESE
C:\Users\MOHANAPRASAD\AppData\Local\Packages\6F71D7A7.HotspotShieldFreeVPN_nsbqstb
b9qxb6\AC\INetCache
C:\Users\MOHANAPRASAD\AppData\Local\Packages\59430GoodgameStudios.BigFarmMobileHar
vest_xnnsrk41c4qr8\AC\INetCookies\ESE
C:\Users\MOHANAPRASAD\AppData\Local\Packages\59430GoodgameStudios.BigFarmMobileHar
vest_xnnsrk41c4qr8\AC\INetCache
C:\Users\MOHANAPRASAD\AppData\Local\Packages\5319275A.51895FA4EA97F_cv1g1gvanyjgm\
AC\INetCookies\ESE
C:\Users\MOHANAPRASAD\AppData\Local\Packages\5319275A.51895FA4EA97F_cv1g1gvanyjgm\
AC\INetCache\AZIJUJKH
C:\Users\MOHANAPRASAD\AppData\Local\Packages\5319275A.51895FA4EA97F_cv1g1gvanyjgm\
AC\INetCache\B1L4C1FN
C:\Users\MOHANAPRASAD\AppData\Local\Packages\5319275A.51895FA4EA97F_cv1g1gvanyjgm\
AC\INetCache
C:\Users\MOHANAPRASAD\AppData\Local\Packages\26720RandomSaladGamesLLC.SimpleSpider
Solitaire_kx24dqmazqk8j\AC\INetCache
C:\Users\MOHANAPRASAD\AppData\Local\Packages\26720RandomSaladGamesLLC.SimpleSolita
ire_kx24dqmazqk8j\AC\INetCookies\ESE
C:\Users\MOHANAPRASAD\AppData\Local\Packages\26720RandomSaladGamesLLC.SimpleSolita
ire_kx24dqmazqk8j\AC\INetCache
C:\Users\MOHANAPRASAD\AppData\Local\Packages\26720RandomSaladGamesLLC.SimpleSolita
ire_kx24dqmazqk8j\AC\AppCache\0DWS8DMH
C:\Users\MOHANAPRASAD\AppData\Local\Packages\26720RandomSaladGamesLLC.SimpleSolita
ire_kx24dqmazqk8j\AC\AppCache
C:\Users\MOHANAPRASAD\AppData\Local\Packages\26720RandomSaladGamesLLC.SimpleMahjon
g_kx24dqmazqk8j\AC\INetCookies\ESE
C:\Users\MOHANAPRASAD\AppData\Local\Packages\26720RandomSaladGamesLLC.SimpleMahjon
g_kx24dqmazqk8j\AC\INetCache
C:\Users\MOHANAPRASAD\AppData\Local\Packages\26720RandomSaladGamesLLC.SimpleMahjon
g_kx24dqmazqk8j\AC\AppCache\U1CMN5BB
C:\Users\MOHANAPRASAD\AppData\Local\Packages\26720RandomSaladGamesLLC.SimpleMahjon
g_kx24dqmazqk8j\AC\AppCache
C:\Users\MOHANAPRASAD\AppData\Local\Packages\TiltingPoint.FoodTruckChefCookingGame
_85kh3h6wfjavg\AC\INetCookies\ESE
C:\Users\MOHANAPRASAD\AppData\Local\Packages\TiltingPoint.FoodTruckChefCookingGame
_85kh3h6wfjavg\AC\INetCache
```

```
C:\Users\MOHANAPRASAD\AppData\Local\Temp\BITF71C.tmp
C:\Users\MOHANAPRASAD\AppData\Local\Temp\edge_BITS_3000_1628098045\BITDE89.tmp
C:\Users\MOHANAPRASAD\AppData\Local\Temp\chrome_BITS_17640_900999123\BITC0FA.tmp
C:\Users\MOHANAPRASAD\AppData\Local\BraveSoftware\Brave-Browser\User
Data\Default\Network\Network Persistent State~RF466190d3.TMP
C:\Users\MOHANAPRASAD\AppData\Local\BraveSoftware\Brave-Browser\User
Data\Default\Network\Network Persistent State~RF5d67a7aa.TMP
C:\Users\MOHANAPRASAD\OneDrive\.849C9593-D756-4E56-8D6E-42412F2A707B
C:\Users\MOHANAPRASAD\OneDrive\Documents\ActivePresenter\.ActivePresenterCachedPro
jects
C:\Users\MOHANAPRASAD\OneDrive\Documents\GitHub\Complete-Python-3-Bootcamp\.git
C:\Users\MOHANAPRASAD\OneDrive\Documents\UiPath\Astrology Sun Sign
Calculator\.local
C:\Users\MOHANAPRASAD\OneDrive\Documents\UiPath\.tutorial\Unicorn Quick
Tutorial\.local
C:\Users\MOHANAPRASAD\Downloads\~$b_final (1).docx
C:\Users\MOHANAPRASAD\.git
```

Searching executable files in non-default folders with write (equivalent) permissions (can be slow)

```
File Permissions "C:\OEM\FRWP\Install_WP.cmd": Authenticated Users
[WriteData/CreateFiles]
File Permissions "C:\OEM\FRWP\For_NonGC\For_NonGC.cmd": Authenticated Users
[WriteData/CreateFiles]
File Permissions "C:\OEM\FRWP\For_NonGC\PBR_Restore_Planet9_PIC.cmd": Authenticated
Users [WriteData/CreateFiles]
File Permissions "C:\OEM\FRWP\For_GC\For_GC.cmd": Authenticated Users
[WriteData/CreateFiles]
File Permissions "C:\OEM\NAPP\UserAlaunch2nd_Initialize.cmd": Authenticated Users
[WriteData/CreateFiles]
File Permissions "C:\OEM\NAPP\UserAlaunch2nd_Finalize.cmd": Authenticated Users
[WriteData/CreateFiles]
File Permissions "C:\OEM\NAPP\UserAlaunch1st_Initialize.cmd": Authenticated Users
[WriteData/CreateFiles]
File Permissions "C:\OEM\NAPP\UserAlaunch1st_Finalize.cmd": Authenticated Users
[WriteData/CreateFiles]
File Permissions "C:\OEM\NAPP\NAPP4P_Initialize.cmd": Authenticated Users
[WriteData/CreateFiles]
File Permissions "C:\OEM\NAPP\NAPP4P_Finalize_Cleanup.cmd": Authenticated Users
[WriteData/CreateFiles]
File Permissions "C:\OEM\NAPP\NAPP4P_Finalize.cmd": Authenticated Users
[WriteData/CreateFiles]
File Permissions "C:\OEM\NAPP\NAPP3P_Initialize.cmd": Authenticated Users
[WriteData/CreateFiles]
File Permissions "C:\OEM\NAPP\NAPP3P_Finalize.cmd": Authenticated Users
[WriteData/CreateFiles]
File Permissions "C:\OEM\NAPP\NAPP3PStateDetection.ps1": Authenticated Users
[WriteData/CreateFiles]
File Permissions "C:\OEM\NAPP\NAPP2P_Initialize.cmd": Authenticated Users
[WriteData/CreateFiles]
File Permissions "C:\OEM\NAPP\NAPP2P_Finalize_TPMNoAutoProvision.cmd":
Authenticated Users [WriteData/CreateFiles]
File Permissions "C:\OEM\NAPP\NAPP2P_Finalize_ManufacturingMode.cmd": Authenticated
Users [WriteData/CreateFiles]
File Permissions "C:\OEM\NAPP\NAPP2P_Finalize_Checkflow.cmd": Authenticated Users
[WriteData/CreateFiles]
File Permissions "C:\OEM\NAPP\NAPP2P_Finalize.cmd": Authenticated Users
[WriteData/CreateFiles]
File Permissions "C:\OEM\NAPP\NAPP2P_ApplyImageToOSdrive.cmd": Authenticated Users
[WriteData/CreateFiles]
File Permissions "C:\OEM\NAPP\NAPP1P_Finalize.cmd": Authenticated Users
[WriteData/CreateFiles]
File Permissions "C:\OEM\NAPP\MountPartition_ARM64.exe": Authenticated Users
[WriteData/CreateFiles]
File Permissions "C:\OEM\NAPP\MountPartition.exe": Authenticated Users
[WriteData/CreateFiles]
File Permissions "C:\OEM\NAPP\GoToNAPP.cmd": Authenticated Users
[WriteData/CreateFiles]
File Permissions "C:\OEM\NAPP\FindValidDriveLetter.cmd": Authenticated Users
[WriteData/CreateFiles]
File Permissions "C:\OEM\NAPP\CheckFreeSpaceTag.cmd": Authenticated Users
```

```
[WriteData/CreateFiles]
File Permissions "C:\OEM\NAPP\OBRSetTool\CopyEFI_byOEM.cmd": Authenticated Users
[WriteData/CreateFiles]
File Permissions "C:\OEM\NAPP\OBRSetTool\modifybcdtoPBR.cmd": Authenticated Users
[WriteData/CreateFiles]
File Permissions "C:\OEM\NAPP\OBRSetTool\modifybcdtoWinRE.cmd": Authenticated Users
[WriteData/CreateFiles]
File Permissions "C:\OEM\NAPP\OBRSetTool\OBRSetTool_amd64.exe": Authenticated Users
[WriteData/CreateFiles]
File Permissions "C:\OEM\NAPP\OBRSetTool\OBRSetTool_x86.exe": Authenticated Users
[WriteData/CreateFiles]
File Permissions "C:\OEM\NAPP\NAPP4P_Patch\ClearDefaultPassword.cmd": Authenticated
Users [WriteData/CreateFiles]
File Permissions "C:\OEM\NAPP\NAPP2PInitCMD\32GFilter\RS5\__GetPhysicalMemory.ps1":
Authenticated Users [WriteData/CreateFiles]
File Permissions
"C:\OEM\NAPP\NAPP2PInitCMD\32GFilter\RS5\RS5_32GFilter_NAPP2P.cmd": Authenticated
Users [WriteData/CreateFiles]
File Permissions "C:\OEM\NAPP\NAPP2PInitCMD\32GFilter\RS4\__GetPhysicalMemory.ps1":
Authenticated Users [WriteData/CreateFiles]
File Permissions
"C:\OEM\NAPP\NAPP2PInitCMD\32GFilter\RS4\RS4_32GFilter_NAPP2P.cmd": Authenticated
Users [WriteData/CreateFiles]
File Permissions "C:\OEM\NAPP\NAPP2PInitCMD\32GFilter\RS3\__GetPhysicalMemory.ps1":
Authenticated Users [WriteData/CreateFiles]
File Permissions
"C:\OEM\NAPP\NAPP2PInitCMD\32GFilter\RS3\RS3_32GFilter_NAPP2P.cmd": Authenticated
Users [WriteData/CreateFiles]
File Permissions "C:\OEM\NAPP\NAPP2PInitCMD\32GFilter\RS2\__GetPhysicalMemory.ps1":
Authenticated Users [WriteData/CreateFiles]
File Permissions
"C:\OEM\NAPP\NAPP2PInitCMD\32GFilter\RS2\RS2_32GFilter_NAPP2P.cmd": Authenticated
Users [WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\utility\GCM\gcmt.cmd": Authenticated Users
[WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\utility\GCM\gcmt.exe": Authenticated Users
[WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\utility\GCM\MRDCreaterX_amd64.exe": Authenticated
Users [WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\utility\GCM\MRDCreaterX_ARM64.exe": Authenticated
Users [WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\utility\GCM\MRDCreaterX_x86.exe": Authenticated
Users [WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\utility\ReaderX\ReaderX_Console.exe":
Authenticated Users [WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\utility\devcon_amd64.exe": Authenticated Users
[WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\utility\devcon_ARM64.exe": Authenticated Users
[WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\utility\devcon_x86.exe": Authenticated Users
[WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\utility\FindValidDriveLetter.cmd": Authenticated
Users [WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\utility\MessageBoxX.exe": Authenticated Users
[WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\utility\PreloadSystemInfo.exe": Authenticated
Users [WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\utility\RunCmd.exe": Authenticated Users
[WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\utility\RunCmd_ARM64.exe": Authenticated Users
[WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\utility\RunCmd_X64.exe": Authenticated Users
[WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\DPOP\COPYOFPOPFORGREATERTHANRV36\MakPoPCopy.CMD":
Authenticated Users [WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\DPOP\GCMREADINESS\GCM_Setup.cmd": Authenticated
Users [WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\DPOP\GCMREADINESS\GenerateRegionTag.cmd":
Authenticated Users [WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\DPOP\OEMCustomize\Acer_Install.cmd": Authenticated
Users [WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\DPOP\OEMCustomize\BeforeOOBE.cmd": Authenticated
Users [WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\DPOP\OEMCustomize\FirstBoot.cmd": Authenticated
Users [WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\DPOP\OEMCustomize\UserAlaunch.cmd": Authenticated
Users [WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\DPOP\OEMRESOURCE\Wallpaper\Copy.cmd":
Authenticated Users [WriteData/CreateFiles]
```

```
File Permissions
"C:\OEM\Preload\DPOP\SETCAMERAFREQUENCY\PBR_RestoreCameraFrequency.cmd":
Authenticated Users [WriteData/CreateFiles]
File Permissions
"C:\OEM\Preload\DPOP\SETCAMERAFREQUENCY\RestoreCameraFrequency.cmd": Authenticated
Users [WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\DPOP\SETCAMERAFREQUENCY\SET_Frequency.cmd":
Authenticated Users [WriteData/CreateFiles]
File Permissions
"C:\OEM\Preload\DPOP\SETDSHOWBRIDGESFORUVC\PBR_RestoreCameraDshowBridges.cmd":
Authenticated Users [WriteData/CreateFiles]
File Permissions
"C:\OEM\Preload\DPOP\SETDSHOWBRIDGESFORUVC\RestoreCameraDshowBridges.cmd":
Authenticated Users [WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\DPOP\SETDSHOWBRIDGESFORUVC\SET_DShowBridges.cmd":
Authenticated Users [WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\DPOP\SYSPREP\_RemoveXMLUnwantNS.ps1":
Authenticated Users [WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\DPOP\SYSPREP\_ChangeWPAsConceptD.ps1":
Authenticated Users [WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\DPOP\SYSPREP\RUN.cmd": Authenticated Users
[WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\DPOP\SYSPREP\Offline_Unattend.cmd": Authenticated
Users [WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\DPOP\SYSPREP\DetectFirmwareInterface_X86.exe":
Authenticated Users [WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\DPOP\SYSPREP\DetectFirmwareInterface_AMD64.exe":
Authenticated Users [WriteData/CreateFiles]
File Permissions
"C:\OEM\Preload\DPOP\SYSPREP\Acer_sysprep_SetNotificationICON.cmd": Authenticated
Users [WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\DPOP\SYSPREP\Acer_sysprep_SetEdgeFavoriteBar.cmd":
Authenticated Users [WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\DPOP\SYSPREP\Acer_sysprep_Numlock.cmd":
Authenticated Users [WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\DPOP\SYSPREP\Acer_sysprep_ChangeWallpaper.cmd":
Authenticated Users [WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\DPOP\SYSPREP\Acer_sysprep.cmd": Authenticated
Users [WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\DPOP\SYSPREP\factory\AcerReboot.exe":
Authenticated Users [WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\DPOP\SYSPREP\factory\AddTaskbarLayoutPath.cmd":
Authenticated Users [WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\DPOP\SYSPREP\factory\AddTaskbarLayoutPath2.cmd":
Authenticated Users [WriteData/CreateFiles]
File Permissions
"C:\OEM\Preload\DPOP\SYSPREP\factory\FactorySysprep_FirstRunTask.cmd":
Authenticated Users [WriteData/CreateFiles]
File Permissions
"C:\OEM\Preload\DPOP\SYSPREP\factory\FactorySysprep_LayoutModification.cmd":
Authenticated Users [WriteData/CreateFiles]
File Permissions
"C:\OEM\Preload\DPOP\SYSPREP\factory\FactorySysprep_TBLayoutModification.cmd":
Authenticated Users [WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\DPOP\SYSPREP\factory\Factory_sysprep.cmd":
Authenticated Users [WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\DPOP\SYSPREP\factory\Factory_sysprep_Vars.cmd":
Authenticated Users [WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\DPOP\SYSPREP\factory\GenerateFirstRunTask.ps1":
Authenticated Users [WriteData/CreateFiles]
File Permissions
"C:\OEM\Preload\DPOP\SYSPREP\factory\GenerateLayoutModification.ps1": Authenticated
Users [WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\DPOP\SYSPREP\factory\RestoreAppAssoc.cmd":
Authenticated Users [WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\DPOP\SYSPREP\factory\RestoreUnattend.ps1":
Authenticated Users [WriteData/CreateFiles]
File Permissions
"C:\OEM\Preload\DPOP\SYSPREP\factory\SUB_AddTaskbarLayoutPath.cmd": Authenticated
Users [WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\Command\AlaunchX\Set2.cmd": Authenticated Users
[WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\Command\AlaunchX\PrepareAlaunchX.cmd":
Authenticated Users [WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\Command\AlaunchX\LockKeyboardMouse.exe":
Authenticated Users [WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\Command\AlaunchX\LaunchALaunchX.exe":
Authenticated Users [WriteData/CreateFiles]
```

```
File Permissions "C:\OEM\Preload\Command\AlaunchX\DisableS3.exe": Authenticated
Users [WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\Command\AlaunchX\DesktopCover_delete.bat":
Authenticated Users [WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\Command\AlaunchX\AppInRun.exe": Authenticated
Users [WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\Command\AlaunchX\ALaunchX.exe": Authenticated
Users [WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\Autorun\AutorunX\AutorunX.exe": Authenticated
Users [WriteData/CreateFiles]
File Permissions "C:\OEM\Preload\Autorun\CheckFiles.exe": Authenticated Users
[WriteData/CreateFiles]
File Permissions "C:\OEM\factory\windelay.exe": Authenticated Users
[WriteData/CreateFiles]
File Permissions "C:\OEM\FIVT\Tools\CheckACM\CheckACM.cmd": Authenticated Users
[WriteData/CreateFiles]
File Permissions "C:\OEM\FIVT\Tools\CHID\Run.cmd": Authenticated Users
[WriteData/CreateFiles]
File Permissions "C:\OEM\FIVT\Run.cmd": Authenticated Users [WriteData/CreateFiles]
File Permissions "C:\OEM\FIVT\CopyBOM.cmd": Authenticated Users
[WriteData/CreateFiles]
File Permissions "C:\OEM\FIVT\ModularizationItems\CheckRecoveryParLocationAndFreeS
pace\CheckRecoveryPar.cmd": Authenticated Users [WriteData/CreateFiles]
File Permissions "C:\OEM\FIVT\ModularizationItems\CheckRecoveryParLocationAndFreeS
pace\Tools\[Before 19H1]WinREFreeSpaceDetection.ps1": Authenticated Users
[WriteData/CreateFiles]
File Permissions "C:\OEM\FIVT\ModularizationItems\CheckRecoveryParLocationAndFreeS
pace\Tools\[19H1]WinREFreeSpaceDetection.ps1": Authenticated Users
[WriteData/CreateFiles]
File Permissions "C:\OEM\FIVT\ModularizationItems\CheckRecoveryParLocationAndFreeS
pace\Tools\FindValidDriveLetter.cmd": Authenticated Users [WriteData/CreateFiles]
File Permissions
"C:\OEM\FIVT\ModularizationItems\CheckSecureBoot\CheckSecureBoot.cmd":
Authenticated Users [WriteData/CreateFiles]
File Permissions "C:\OEM\FIVT\ModularizationItems\CheckSLIC\CheckSLIC.cmd":
Authenticated Users [WriteData/CreateFiles]
File Permissions "C:\OEM\FIVT\ModularizationItems\CheckSLIC\Tools\OACHECK.cmd":
Authenticated Users [WriteData/CreateFiles]
File Permissions
"C:\OEM\FIVT\ModularizationItems\CheckUnknownDevice\CheckUnknownDevice.cmd":
Authenticated Users [WriteData/CreateFiles]
File Permissions
"C:\OEM\FIVT\ModularizationItems\CheckVGADriverIsInboxorNot\CheckVGADriver.cmd":
Authenticated Users [WriteData/CreateFiles]
File Permissions
"C:\OEM\FIVT\ModularizationItems\CheckBIOSSkuID\CheckBIOSSkuID.cmd": Authenticated
Users [WriteData/CreateFiles]
File Permissions
"C:\OEM\FIVT\ModularizationItems\CheckBIOSSkuID\Tools\FindValidDriveLetter.cmd":
Authenticated Users [WriteData/CreateFiles]
File Permissions
"C:\OEM\FIVT\ModularizationItems\CheckCSUPExistence\CheckCSUP.cmd": Authenticated
Users [WriteData/CreateFiles]
File Permissions "C:\OEM\FIVT\ModularizationItems\CheckDesktopShortcutForJumpstart
\CheckDesktopShortcut.cmd": Authenticated Users [WriteData/CreateFiles]
File Permissions "C:\OEM\FIVT\ModularizationItems\CheckDesktopShortcutForJumpstart
\PublicDesktopPINCheck.ps1": Authenticated Users [WriteData/CreateFiles]
File Permissions
"C:\OEM\FIVT\ModularizationItems\CheckDumpFileExistence\CheckDumpFile.cmd":
Authenticated Users [WriteData/CreateFiles]
File Permissions "C:\OEM\FIVT\ModularizationItems\CheckGCMtags\CheckFileEmpty.ps1":
Authenticated Users [WriteData/CreateFiles]
File Permissions "C:\OEM\FIVT\ModularizationItems\CheckGCMtags\CheckGCMtags.cmd":
Authenticated Users [WriteData/CreateFiles]
File Permissions "C:\OEM\FIVT\ModularizationItems\CheckLogo8p1\CheckLogo8p1.cmd":
Authenticated Users [WriteData/CreateFiles]
File Permissions "C:\OEM\FIVT\ModularizationItems\CheckLogo8p1\CheckFileEmpty.ps1":
Authenticated Users [WriteData/CreateFiles]
File Permissions "C:\OEM\FIVT\ModularizationItems\CheckLogo8p1\x86\Run.cmd":
Authenticated Users [WriteData/CreateFiles]
File Permissions "C:\OEM\FIVT\ModularizationItems\CheckLogo8p1\amd64\Run.cmd":
Authenticated Users [WriteData/CreateFiles]
File Permissions
"C:\OEM\FIVT\ModularizationItems\CheckOEMInfList\CheckOEMInfList.cmd":
Authenticated Users [WriteData/CreateFiles]
File Permissions
"C:\OEM\FIVT\ModularizationItems\CheckProductKey\CheckProductKey.cmd":
Authenticated Users [WriteData/CreateFiles]
```

```
File Permissions "C:\OEM\FIVT\ModularizationItems\CheckProductKey\Tools\W1020H1\Ch
eckProductKey_W1020H1.cmd": Authenticated Users [WriteData/CreateFiles]
File Permissions
"C:\OEM\FIVT\ModularizationItems\CheckProductKey\Tools\W7\CheckProductKey_W7.cmd":
Authenticated Users [WriteData/CreateFiles]
File Permissions "C:\OEM\FIVT\ModularizationItems\CheckProductKey\Tools\W1019H1\Ch
eckProductKey_W1019H1.cmd": Authenticated Users [WriteData/CreateFiles]
File Permissions "C:\OEM\FIVT\ModularizationItems\CheckProductKey\Tools\W1019H2\Ch
eckProductKey_W1019H2.cmd": Authenticated Users [WriteData/CreateFiles]
File Permissions "C:\OEM\FIVT\ModularizationItems\CheckProductKey\Tools\W10RS4\Che
ckProductKey_W10RS4.cmd": Authenticated Users [WriteData/CreateFiles]
File Permissions "C:\OEM\FIVT\ModularizationItems\CheckProductKey\Tools\W10RS5\Che
ckProductKey_W10RS5.cmd": Authenticated Users [WriteData/CreateFiles]
File Permissions "C:\OEM\CaringCenter\DRV\Atheros Wireless LAN_M
NFA435A\Install.cmd": Authenticated Users [WriteData/CreateFiles]
File Permissions "C:\OEM\CaringCenter\DRV\Atheros Wireless LAN_M
NFA435A\QcomWlanSrvx64.exe": Authenticated Users [WriteData/CreateFiles]
File Permissions "C:\OEM\CaringCenter\DRV\Atheros Wireless LAN_M
NFA435A\Setup_Driver.cmd": Authenticated Users [WriteData/CreateFiles]
File Permissions "C:\OEM\CaringCenter\DRV\Realtek LAN_M
RTL8111H\Silent_Uninstall_CD.bat": Authenticated Users [WriteData/CreateFiles]
File Permissions "C:\OEM\CaringCenter\DRV\Realtek LAN_M
RTL8111H\Silent_Uninstall.bat": Authenticated Users [WriteData/CreateFiles]
File Permissions "C:\OEM\CaringCenter\DRV\Realtek LAN_M
RTL8111H\Silent_Install_CD.bat": Authenticated Users [WriteData/CreateFiles]
File Permissions "C:\OEM\CaringCenter\DRV\Realtek LAN_M
RTL8111H\Silent_Install.bat": Authenticated Users [WriteData/CreateFiles]
File Permissions "C:\OEM\CaringCenter\DRV\Realtek LAN_M RTL8111H\Setup_Driver.cmd":
Authenticated Users [WriteData/CreateFiles]
File Permissions "C:\OEM\CaringCenter\DRV\Realtek LAN_M RTL8111H\setup.exe":
Authenticated Users [WriteData/CreateFiles]
File Permissions "C:\OEM\CaringCenter\DRV\Realtek LAN_M RTL8111H\Install.cmd":
Authenticated Users [WriteData/CreateFiles]
File Permissions "C:\OEM\CaringCenter\DRV\Realtek LAN_M RTL8111H\AutoInst.exe":
Authenticated Users [WriteData/CreateFiles]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject\venv\Lib\sit
e-packages\pip\_vendor\distlib\t32.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject\venv\Lib\sit
e-packages\pip\_vendor\distlib\t64-arm.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject\venv\Lib\sit
e-packages\pip\_vendor\distlib\t64.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject\venv\Lib\sit
e-packages\pip\_vendor\distlib\w32.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject\venv\Lib\sit
e-packages\pip\_vendor\distlib\w64-arm.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject\venv\Lib\sit
e-packages\pip\_vendor\distlib\w64.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject\venv\Lib\sit
e-packages\setuptools\gui.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject\venv\Lib\sit
e-packages\setuptools\gui-arm64.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject\venv\Lib\sit
e-packages\setuptools\gui-64.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject\venv\Lib\sit
e-packages\setuptools\gui-32.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject\venv\Lib\sit
e-packages\setuptools\cli.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject\venv\Lib\sit
e-packages\setuptools\cli-arm64.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject\venv\Lib\sit
e-packages\setuptools\cli-64.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject\venv\Lib\sit
e-packages\setuptools\cli-32.exe": MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject\venv\Scripts\activate.bat":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject\venv\Scripts\activate.ps1":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject\venv\Scripts\deactivate.bat":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject\venv\Scripts\pip.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject\venv\Scripts\pip3.exe":
MOHANAPRASAD [AllAccess]
```

```
File Permissions
"C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject\venv\Scripts\pydoc.bat":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject\venv\Scripts\python.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject\venv\Scripts\pythonw.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject\venv\Scripts\wheel.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject\venv\Scripts\wheel3.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject1\venv\Lib\si
te-packages\pip\_vendor\distlib\t32.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject1\venv\Lib\si
te-packages\pip\_vendor\distlib\t64-arm.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject1\venv\Lib\si
te-packages\pip\_vendor\distlib\t64.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject1\venv\Lib\si
te-packages\pip\_vendor\distlib\w32.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject1\venv\Lib\si
te-packages\pip\_vendor\distlib\w64-arm.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject1\venv\Lib\si
te-packages\pip\_vendor\distlib\w64.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject1\venv\Lib\si
te-packages\setuptools\gui.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject1\venv\Lib\si
te-packages\setuptools\gui-arm64.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject1\venv\Lib\si
te-packages\setuptools\gui-64.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject1\venv\Lib\si
te-packages\setuptools\gui-32.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject1\venv\Lib\si
te-packages\setuptools\cli.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject1\venv\Lib\si
te-packages\setuptools\cli-arm64.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject1\venv\Lib\si
te-packages\setuptools\cli-64.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject1\venv\Lib\si
te-packages\setuptools\cli-32.exe": MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject1\venv\Scripts\activate.bat":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject1\venv\Scripts\activate.ps1":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject1\venv\Script
s\deactivate.bat": MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject1\venv\Scripts\pip.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject1\venv\Scripts\pip3.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject1\venv\Scripts\pydoc.bat":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject1\venv\Scripts\python.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject1\venv\Scripts\pythonw.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject1\venv\Scripts\wheel.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject1\venv\Scripts\wheel3.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject2.pyshop\venv
\Lib\site-packages\pip\_vendor\distlib\t32.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject2.pyshop\venv
\Lib\site-packages\pip\_vendor\distlib\t64-arm.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject2.pyshop\venv
\Lib\site-packages\pip\_vendor\distlib\t64.exe": MOHANAPRASAD [AllAccess]
```

```
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject2.pyshop\venv
\Lib\site-packages\pip\_vendor\distlib\w32.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject2.pyshop\venv
\Lib\site-packages\pip\_vendor\distlib\w64-arm.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject2.pyshop\venv
\Lib\site-packages\pip\_vendor\distlib\w64.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject2.pyshop\venv
\Lib\site-packages\setuptools\gui.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject2.pyshop\venv
\Lib\site-packages\setuptools\gui-arm64.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject2.pyshop\venv
\Lib\site-packages\setuptools\gui-64.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject2.pyshop\venv
\Lib\site-packages\setuptools\gui-32.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject2.pyshop\venv
\Lib\site-packages\setuptools\cli.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject2.pyshop\venv
\Lib\site-packages\setuptools\cli-arm64.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject2.pyshop\venv
\Lib\site-packages\setuptools\cli-64.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject2.pyshop\venv
\Lib\site-packages\setuptools\cli-32.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject2.pyshop\venv
\Scripts\activate.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject2.pyshop\venv
\Scripts\activate.ps1": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject2.pyshop\venv
\Scripts\deactivate.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject2.pyshop\venv
\Scripts\pip-3.11.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject2.pyshop\venv
\Scripts\pip.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject2.pyshop\venv
\Scripts\pip3.11.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject2.pyshop\venv
\Scripts\pip3.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject2.pyshop\venv
\Scripts\pydoc.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject2.pyshop\venv
\Scripts\python.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject2.pyshop\venv
\Scripts\pythonw.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject2.pyshop\venv
\Scripts\wheel-3.11.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject2.pyshop\venv
\Scripts\wheel.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject2.pyshop\venv
\Scripts\wheel3.11.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\PycharmProjects\pythonProject2.pyshop\venv
\Scripts\wheel3.exe": MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\.nuget\packages\nuget.commandline\4.6.2\tools\NuGet.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\.nuget\packages\microsoft.codeanalysis.ana
lyzers\3.0.0\tools\uninstall.ps1": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\.nuget\packages\microsoft.codeanalysis.ana
lyzers\3.0.0\tools\install.ps1": MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\.nuget\packages\newtonsoft.json\9.0.1\tools\install.ps1":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\.nuget\packages\uipath.ocr.activities\3.3.
2\build\net461\UiPath.OCR.Host.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\.nuget\packages\uipath.ocr.activities\3.3.
2\build\net461\UiPath.OCR.Host64.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\.nuget\packages\uipath.mail.activities\1.1
2.3\tools\net461\MainSessionServer\UiPath.Mail.MainSessionServer.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\.nuget\packages\uipath\21.10.40.21933\buil
d\UiPath\UiPathRemote.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\.nuget\packages\uipath\21.10.40.21933\buil
d\UiPath\slinject.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\.nuget\packages\uipath\21.10.40.21933\buil
d\UiPath\FuncServer_x86.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\.nuget\packages\uipath\21.10.40.21933\buil
d\UiPath\FuncServer_x64.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\.nuget\packages\uipath\21.10.40.21933\buil
d\UiPath\EvtServer_x64.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\.nuget\packages\uipath\21.10.40.21933\buil
```

```
d\UiPath\EvtServer.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\.nuget\packages\uipath.vision\3.1.4\build\
net461\UiPath.Vision.Host.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\.nuget\packages\uipath.uiautomation.activi
ties\21.10.6\build\UiExplorer.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\.nuget\packages\uipath.uiautomation.activi
ties\21.10.6\build\UiExplorer_x64.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\.nuget\packages\uipath.system.activities\2
1.10.5\build\net461\WorkerProcess.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\shell\condabin\conda-hook.ps1":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\yapf.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\xlwings.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\wheel.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\wcslint.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\watchmedo.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\volint.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\unidecode.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\twistd.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\twist.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\ttx.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\trial.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\tqdm.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\tldextract.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\tkconch.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\tifffile.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\tiffcomment.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\tiff2fsspec.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\tabulate.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\symilar.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\spyder.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\sphinx-quickstart.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\sphinx-build.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\sphinx-autogen.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\sphinx-apidoc.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\slugify.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\skivi.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\showtable.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\scrapy.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\samp_hub.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\qtpy.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\qta-browser.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\pytest.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\pyreverse.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\pylsp.exe": MOHANAPRASAD
[AllAccess]
```

```
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\pylint.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\pylint-config.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\pyjson5.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\pyhtmlizer.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\pygmentize.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\pyftsubset.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\pyftmerge.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\pyflakes.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\pydocstyle.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\pydoc.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\pyct.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\pycodestyle.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\pycc.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\pybabel.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\pttree.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\ptrepack.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\ptdump.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\pt2to3.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\pkginfo.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\pip3.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\pip.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\pep8.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\pasteurize.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\panel.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\numba.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\nosetests.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\normalizer.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\nltk.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\navigator-updater.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\menuinst.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\matplotlib.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\markdown_py.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\mailmail.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\lsm2bin.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\keyring.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\jupyter.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\jupyter-trust.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\Scripts\jupyter-troubleshoot.exe": MOHANAPRASAD
[AllAccess]
File Permissions
```

```
"C:\Users\MOHANAPRASAD\anaconda3\Scripts\jupyter-serverextension.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\jupyter-server.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\jupyter-run.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\jupyter-qtconsole.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\jupyter-notebook.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\jupyter-nbextension.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\jupyter-nbconvert.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\jupyter-nbclassic.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\jupyter-migrate.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\jupyter-labhub.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\Scripts\jupyter-labextension.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\jupyter-lab.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\jupyter-kernelspec.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\jupyter-kernel.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\jupyter-execute.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\jupyter-dejavu.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\jupyter-console.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\Scripts\jupyter-bundlerextension.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\jsonschema.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\jlpm.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\isympy.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\isort.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\ipython3.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\ipython.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\iptest3.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\iptest.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\intake.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\intake-server.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\imageio_remove_bin.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\Scripts\imageio_download_bin.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\imagecodecs.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\idle.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\holoviews.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\futurize.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\fonttools.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\flask.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\flake8.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\fitsinfo.exe":
MOHANAPRASAD [AllAccess]
```

```
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\fitsheader.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\fitsdiff.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\fitscheck.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\fits2bitmap.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\f2py.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\f2py.bat": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\epylint.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\datashader.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\dask-worker.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\dask-ssh.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\dask-scheduler.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\cythonize.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\cython.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\cygdb.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\cph.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\cookiecutter.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\conda.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\conda-verify.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\conda-token.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\conda-skeleton.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\conda-server.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\conda-repo.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\conda-render.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\conda-pack.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\conda-metapackage.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\conda-inspect.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\conda-index.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\conda-env.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\conda-develop.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\conda-debug.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\conda-convert.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\conda-content-trust.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\conda-build.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\conch.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\colorcet.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\ckeygen.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\chardetect.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\cftp.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\bokeh.exe": MOHANAPRASAD
[AllAccess]
```

```
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\blackd.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\black.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\binstar.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\autopep8.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\automat-visualize.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\anaconda.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\anaconda-project.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\anaconda-navigator.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\activate.bat":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Scripts\2to3.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\pre_uninstall.bat":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\post_install.bat":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\packaging-21.3-pyhd3eb1b0_0
\info\test\run_test.bat": MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\pkgs\lzo-2.10-he774522_2\info\test\run_test.bat":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\pkgs\lzo-2.10-he774522_2\info\recipe\bld.bat":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\lzo-2.10-he774522_2\Library
\libexec\lzo\examples\testmini.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\lzo-2.10-he774522_2\Library
\libexec\lzo\examples\simple.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\lzo-2.10-he774522_2\Library
\libexec\lzo\examples\lzotest.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\lzo-2.10-he774522_2\Library
\libexec\lzo\examples\lzopack.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\libiconv-1.16-h2bbff1b_2\in
fo\recipe\bld.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\libdeflate-1.8-h2bbff1b_5\i
nfo\test\run_test.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\libdeflate-1.8-h2bbff1b_5\i
nfo\recipe\bld.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\libdeflate-1.8-h2bbff1b_5\L
ibrary\bin\libdeflate-gzip.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\libdeflate-1.8-h2bbff1b_5\L
ibrary\bin\libdeflate-gunzip.exe": MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\pkgs\lerc-3.0-hd77b12b_0\info\test\run_test.bat":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\pkgs\lerc-3.0-hd77b12b_0\info\recipe\bld.bat":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\lcms2-2.12-h83e58a3_0\info\
test\run_test.bat": MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\pkgs\lcms2-2.12-h83e58a3_0\info\recipe\bld.bat":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\lcms2-2.12-h83e58a3_0\Libra
ry\bin\transicc.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\lcms2-2.12-h83e58a3_0\Libra
ry\bin\tificc.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\lcms2-2.12-h83e58a3_0\Libra
ry\bin\psicc.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\lcms2-2.12-h83e58a3_0\Libra
ry\bin\linkicc.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\lcms2-2.12-h83e58a3_0\Libra
ry\bin\jpgicc.exe": MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\pkgs\jq-1.6-haa95532_1\info\test\run_test.bat":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\jq-1.6-haa95532_1\Library\m
ingw-w64\bin\jq.exe": MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\pkgs\jpeg-9e-h2bbff1b_0\info\test\run_test.bat":
```

```
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\pkgs\jpeg-9e-h2bbff1b_0\info\recipe\bld.bat":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\jpeg-9e-h2bbff1b_0\Library\
bin\wrjpgcom.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\jpeg-9e-h2bbff1b_0\Library\
bin\rdjpgcom.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\jpeg-9e-h2bbff1b_0\Library\
bin\jpegtran.exe": MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\pkgs\jpeg-9e-h2bbff1b_0\Library\bin\djpeg.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\pkgs\jpeg-9e-h2bbff1b_0\Library\bin\cjpeg.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\idna-3.3-pyhd3eb1b0_0\info\
test\run_test.bat": MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\pkgs\icu-58.2-ha925a31_3\info\test\run_test.bat":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\pkgs\icu-58.2-ha925a31_3\info\recipe\bld.bat":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\pkgs\icu-58.2-ha925a31_3\Library\bin\uconv.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\icu-58.2-ha925a31_3\Library
\bin\pkgdata.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\icu-58.2-ha925a31_3\Library
\bin\makeconv.exe": MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\pkgs\icu-58.2-ha925a31_3\Library\bin\icupkg.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\icu-58.2-ha925a31_3\Library
\bin\icuinfo.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\icu-58.2-ha925a31_3\Library
\bin\gensprep.exe": MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\pkgs\icu-58.2-ha925a31_3\Library\bin\genrb.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\icu-58.2-ha925a31_3\Library
\bin\gennorm2.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\icu-58.2-ha925a31_3\Library
\bin\gendict.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\icu-58.2-ha925a31_3\Library
\bin\gencnval.exe": MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\pkgs\icu-58.2-ha925a31_3\Library\bin\gencmn.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\pkgs\icu-58.2-ha925a31_3\Library\bin\gencfu.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\icu-58.2-ha925a31_3\Library
\bin\genccode.exe": MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\pkgs\icu-58.2-ha925a31_3\Library\bin\genbrk.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\pkgs\icu-58.2-ha925a31_3\Library\bin\derb.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\entrypoints-0.4-py39haa9553
2_0\info\test\run_test.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\cfitsio-3.470-h2bbff1b_7\in
fo\test\run_test.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\cfitsio-3.470-h2bbff1b_7\in
fo\recipe\bld.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\bkcharts-0.2-py39haa95532_1
\info\test\run_test.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\backports-1.1-pyhd3eb1b0_0\
info\test\run_test.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\backports-1.1-pyhd3eb1b0_0\
info\recipe\bld.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\astropy-5.1-py39h080aedc_0\
info\test\run_test.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\astropy-5.1-py39h080aedc_0\
Scripts\fits2bitmap.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\astropy-5.1-py39h080aedc_0\
Scripts\fitscheck.exe": MOHANAPRASAD [AllAccess]
```

```
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\astropy-5.1-py39h080aedc_0\
Scripts\fitsdiff.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\astropy-5.1-py39h080aedc_0\
Scripts\fitsheader.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\astropy-5.1-py39h080aedc_0\
Scripts\fitsinfo.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\astropy-5.1-py39h080aedc_0\
Scripts\samp_hub.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\astropy-5.1-py39h080aedc_0\
Scripts\showtable.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\astropy-5.1-py39h080aedc_0\
Scripts\volint.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\astropy-5.1-py39h080aedc_0\
Scripts\wcslint.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\pywin32-302-py39h2bbff1b_2\
info\recipe\bld.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\pywin32-302-py39h2bbff1b_2\
Lib\site-packages\pythonwin\Pythonwin.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\pywin32-302-py39h2bbff1b_2\
Lib\site-packages\win32\pythonservice.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\pytz-2022.1-py39haa95532_0\
info\test\run_test.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\python-libarchive-c-2.9-pyh
d3eb1b0_1\info\test\run_test.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\nltk-3.7-pyhd3eb1b0_0\info\
test\run_test.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\pyyaml-6.0-py39h2bbff1b_1\i
nfo\test\run_test.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\pycparser-2.21-pyhd3eb1b0_0
\info\test\run_test.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\zope-1.0-py39haa95532_1\inf
o\recipe\bld.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\vc-14.2-h21ff451_1\info\rec
ipe\parent\activate.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\vc-14.2-h21ff451_1\info\rec
ipe\parent\install_activate.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\vc-14.2-h21ff451_1\info\rec
ipe\parent\install_runtime.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pkgs\tornado-6.1-py39h2bbff1b_0\
info\test\run_test.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\condabin\activate.bat":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\condabin\conda.bat": MOHANAPRASAD
[AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\condabin\conda_auto_activate.bat": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\condabin\conda_hook.bat":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\condabin\deactivate.bat":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\condabin\rename_tmp.bat":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\condabin\_conda_activate.bat":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\setuptools\gui.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\setuptools\gui-arm64.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\setuptools\gui-64.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\setuptools\gui-32.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\setuptools\cli.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\setuptools\cli-arm64.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\setuptools\cli-64.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\setuptools\cli-32.exe":
```

```
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\win32\pythonservice.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\greenlet\platf
orm\setup_switch_x64_masm.cmd": MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\pip\_vendor\distlib\w64.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\pip\_vendor\di
stlib\w64-arm.exe": MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\pip\_vendor\distlib\w32.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\pip\_vendor\distlib\t64.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\pip\_vendor\di
stlib\t64-arm.exe": MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\pip\_vendor\distlib\t32.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\conda\shell\co
ndabin\activate.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\conda\shell\co
ndabin\conda-hook.ps1": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\conda\shell\co
ndabin\conda.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\conda\shell\co
ndabin\conda_auto_activate.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\conda\shell\co
ndabin\conda_hook.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\conda\shell\co
ndabin\deactivate.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\conda\shell\co
ndabin\rename_tmp.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\conda\shell\co
ndabin\_conda_activate.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\conda\shell\Li
brary\bin\conda.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\conda\shell\Sc
ripts\activate.bat": MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\conda\shell\cli-32.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\conda\shell\cli-64.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\conda_build\cli-64.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\conda_build\cli-32.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\conda_pack\scr
ipts\windows\activate.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\conda_pack\scr
ipts\windows\deactivate.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\debugpy\_vendo
red\pydevd\pydevd_attach_to_process\linux_and_mac\compile_manylinux.cmd":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\debugpy\_vendo
red\pydevd\pydevd_attach_to_process\windows\compile_windows.bat": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\debugpy\_vendo
red\pydevd\pydevd_attach_to_process\inject_dll_amd64.exe": MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\pythonwin\Pythonwin.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\spyder\plugins
\ipythonconsole\scripts\conda-activate.bat": MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\testpath\cli-64.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\testpath\cli-32.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Lib\idlelib\idle.bat":
MOHANAPRASAD [AllAccess]
```

```
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\Lib\ctypes\macholib\fetch_macholib.bat":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\Lib\venv\scripts\nt\deactivate.bat": MOHANAPRASAD
[AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\Lib\venv\scripts\nt\activate.bat": MOHANAPRASAD
[AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\Lib\venv\scripts\common\Activate.ps1":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\Library\mkspecs\features\data\android\dx.bat":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\mingw-w64\bin\jq.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\Library\libexec\lzo\examples\testmini.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\Library\libexec\lzo\examples\simple.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\Library\libexec\lzo\examples\lzotest.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\Library\libexec\lzo\examples\lzopack.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\aec.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\assistant.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\brotli.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\bsdcat.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\bsdcpio.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\bsdtar.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\canbusutil.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\cjpeg.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\conda.bat":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\curl.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\cwebp.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\derb.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\designer.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\djpeg.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\dumpcpp.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\dumpdoc.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\dwebp.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\fax2ps.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\fax2tiff.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\genbrk.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\genccode.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\gencfu.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\gencmn.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\gencnval.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\gendict.exe":
```

```
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\gennorm2.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\genrb.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\gensprep.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\gif2h5-shared.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\gif2h5.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\gif2rgb.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\gifbuild.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\gifclrmp.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\giffix.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\giftext.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\giftool.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\h52gif-shared.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\h52gif.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\h5clear-shared.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\h5clear.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\h5copy-shared.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\h5copy.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\h5debug-shared.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\h5debug.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\h5diff-shared.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\h5diff.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\h5dump-shared.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\h5dump.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\Library\bin\h5format_convert-shared.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\Library\bin\h5format_convert.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\h5import-shared.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\h5import.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\h5jam-shared.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\h5jam.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\h5ls-shared.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\h5ls.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\h5mkgrp-shared.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\h5mkgrp.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\h5repack-shared.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\h5repack.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\h5repart-shared.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\h5repart.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\h5stat-shared.exe":
MOHANAPRASAD [AllAccess]
```

```
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\h5stat.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\h5unjam-shared.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\h5unjam.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\h5watch-shared.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\h5watch.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\icuinfo.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\icupkg.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\idc.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\jpegtran.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\jpgicc.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\lconvert.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\Library\bin\libdeflate-gunzip.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\libdeflate-gzip.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\linguist.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\linkicc.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\lrelease.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\lupdate.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\lz4.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\lzmainfo.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\makeconv.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\moc.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\openssl.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\opj_compress.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\opj_decompress.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\opj_dump.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\pal2rgb.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\pixeltool.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\pkgdata.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\png-fix-itxt.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\pngfix.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\ppm2tiff.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\psicc.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\pylupdate5.bat":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\pyrcc5.bat":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\pyuic5.bat":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\Library\bin\qcollectiongenerator.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\qdbus.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\qdbuscpp2xml.exe":
MOHANAPRASAD [AllAccess]
```

```
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\qdbusviewer.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\qdbusxml2cpp.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\qdoc.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\qgltf.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\qhelpconverter.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\qhelpgenerator.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\qlalr.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\qmake.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\qml.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\qmlcachegen.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\qmleasing.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\Library\bin\qmlimportscanner.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\qmllint.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\qmlmin.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\qmlplugindump.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\qmlprofiler.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\qmlscene.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\qmltestrunner.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\qscxmlc.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\Library\bin\qtattributionsscanner.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\qtdiag.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\qtpaths.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\qtplugininfo.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\Library\bin\QtWebEngineProcess.exe": MOHANAPRASAD
[AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\Library\bin\qwebengine_convert_dict.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\raw2tiff.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\rcc.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\rdjpgcom.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\repc.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\runxmlconf.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\sip.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\sqlite3.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\tclsh.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\tclsh86.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\tclsh86t.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\testcon.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\tiff2bw.exe":
MOHANAPRASAD [AllAccess]
```

```
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\tiff2pdf.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\tiff2ps.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\tiff2rgba.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\tiffcmp.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\tiffcp.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\tiffcrop.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\tiffdither.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\tiffdump.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\tiffinfo.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\tiffmedian.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\tiffset.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\tiffsplit.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\tificc.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\transicc.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\uconv.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\uic.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\unxz.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\windeployqt.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\winpty-agent.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\wish.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\wish86.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\wish86t.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\wrjpgcom.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\xmlcatalog.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\xmllint.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\xmlpatterns.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\Library\bin\xmlpatternsvalidator.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\xsltproc.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\xz.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\xz_static.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\zfp.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\zopfli.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\zopflipng.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\bin\zstd.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\usr\bin\cygcheck.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\usr\bin\cygpath.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\anaconda3\Library\usr\bin\cygwin-console-helper.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\usr\bin\dumper.exe":
MOHANAPRASAD [AllAccess]
```

```
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\usr\bin\getconf.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\usr\bin\getfacl.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\usr\bin\kill.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\usr\bin\ldd.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\usr\bin\ldh.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\usr\bin\locale.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\usr\bin\minidumper.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\usr\bin\mkgroup.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\usr\bin\mkpasswd.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\usr\bin\mount.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\usr\bin\passwd.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\usr\bin\patch.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\usr\bin\pldd.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\usr\bin\ps.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\usr\bin\regtool.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\usr\bin\setfacl.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\usr\bin\setmetamode.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\usr\bin\ssp.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\usr\bin\strace.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\usr\bin\tzset.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Library\usr\bin\umount.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\python.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\pythonw.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\Uninstall-Anaconda3.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\venvlauncher.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\venvwlauncher.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\anaconda3\_conda.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\OWASP
ZAP\webdriver\windows\32\chromedriver.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\OWASP
ZAP\webdriver\windows\32\geckodriver.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\OWASP
ZAP\webdriver\windows\64\geckodriver.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\Downloads\web
technology\node_modules\.bin\tsc.cmd": Everyone [AllAccess],MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\Downloads\web
technology\node_modules\.bin\tsc.ps1": Everyone [AllAccess],MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\Downloads\web
technology\node_modules\.bin\tsserver.cmd": Everyone [AllAccess],MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\Downloads\web
technology\node_modules\.bin\tsserver.ps1": Everyone [AllAccess],MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\Downloads\BraveBrowserSetup-BRV010.exe":
Everyone [AllAccess],MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\Downloads\GitHubDesktopSetup-x64.exe":
Everyone [AllAccess],MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\Downloads\JavaSetup8u371.exe": Everyone
[AllAccess],MOHANAPRASAD [AllAccess]
```

```
File Permissions
"C:\Users\MOHANAPRASAD\Downloads\sublime_text_build_4143_x64_setup.exe": Everyone
[AllAccess],MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\Downloads\VisualStudioSetup.exe": Everyone
[AllAccess],MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\Downloads\webex.exe": Everyone
[AllAccess],MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\Downloads\ZAP_2_12_0_windows.exe": Everyone
[AllAccess],MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\.vscode\extensions\ms-vscode.cpptools-1.16
.3-win32-x64\bin\cpptools.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\.vscode\extensions\ms-vscode.cpptools-1.16
.3-win32-x64\bin\cpptools-srv.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\.vscode\extensions\ms-vscode.cpptools-1.16
.3-win32-x64\debugAdapters\vsdbg\bin\VsDebugConsole.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\.vscode\extensions\ms-vscode.cpptools-1.16
.3-win32-x64\debugAdapters\vsdbg\bin\vsdbg.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\.vscode\extensions\ms-vscode.cpptools-1.16
.3-win32-x64\debugAdapters\vsdbg\bin\Remote Debugger\x86\msvsmon.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\.vscode\extensions\ms-vscode.cpptools-1.16
.3-win32-x64\debugAdapters\bin\WindowsDebugLauncher.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\.vscode\extensions\ms-vscode.cpptools-1.16
.3-win32-x64\debugAdapters\bin\OpenDebugAD7.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\.vscode\extensions\ms-vscode.cpptools-1.16
.3-win32-x64\debugAdapters\bin\createdump.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\.vscode\extensions\ms-vscode.cpptools-1.16
.3-win32-x64\LLVM\bin\clang-tidy.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\.vscode\extensions\ms-vscode.cpptools-1.16
.3-win32-x64\LLVM\bin\clang-format.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\.vscode\extensions\ms-python.python-2023.1
4.0\pythonFiles\lib\python\debugpy\_vendored\pydevd\pydevd_attach_to_process\injec
t_dll_x86.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\.vscode\extensions\ms-python.python-2023.1
4.0\pythonFiles\lib\python\debugpy\_vendored\pydevd\pydevd_attach_to_process\injec
t_dll_amd64.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\.vscode\extensions\ms-python.python-2023.1
4.0\pythonFiles\lib\python\debugpy\_vendored\pydevd\pydevd_attach_to_process\windo
ws\compile_windows.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\.vscode\extensions\ms-python.python-2023.1
4.0\pythonFiles\lib\python\debugpy\_vendored\pydevd\pydevd_attach_to_process\linux
_and_mac\compile_manylinux.cmd": MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\AppData\Local\balena-etcher-updater\installer.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Microsoft\OneDrive\OneDriveS
tandaloneUpdater.exe": MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\AppData\Local\Microsoft\OneDrive\OneDrive.exe": MOHANAPRASAD
[AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\AppData\Local\Microsoft\WindowsApps\winget.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Microsoft\WindowsApps\Window
sPackageManagerServer.exe": MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\AppData\Local\Microsoft\WindowsApps\ubuntu.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\AppData\Local\Microsoft\WindowsApps\Spotify.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\AppData\Local\Microsoft\WindowsApps\SnippingTool.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\AppData\Local\Microsoft\WindowsApps\Skype.exe": MOHANAPRASAD
[AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\AppData\Local\Microsoft\WindowsApps\python3.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\AppData\Local\Microsoft\WindowsApps\python.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\AppData\Local\Microsoft\WindowsApps\pbrush.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\AppData\Local\Microsoft\WindowsApps\notepad.exe":
```

```
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\AppData\Local\Microsoft\WindowsApps\msteamsupdate.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\AppData\Local\Microsoft\WindowsApps\msteams.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\AppData\Local\Microsoft\WindowsApps\mspaint.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\AppData\Local\Microsoft\WindowsApps\MicrosoftEdge.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\AppData\Local\Microsoft\WindowsApps\MessengerHelper.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\AppData\Local\Microsoft\WindowsApps\MediaPlayer.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Microsoft\WindowsApps\GameBa
rElevatedFT_Alias.exe": MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\AppData\Local\Microsoft\WindowsApps\clipchamp.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Microsoft\WindowsApps\Spotif
yAB.SpotifyMusic_zpdnekdrzrea0\Spotify.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Microsoft\WindowsApps\Micros
oftTeams_8wekyb3d8bbwe\msteamsupdate.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Microsoft\WindowsApps\Micros
oftTeams_8wekyb3d8bbwe\msteams.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Microsoft\WindowsApps\Micros
oft.ZuneMusic_8wekyb3d8bbwe\MediaPlayer.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Microsoft\WindowsApps\Micros
oft.XboxGamingOverlay_8wekyb3d8bbwe\GameBarElevatedFT_Alias.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Microsoft\WindowsApps\Micros
oft.WindowsNotepad_8wekyb3d8bbwe\notepad.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Microsoft\WindowsApps\Micros
oft.SkypeApp_kzf8qxf38zg5c\Skype.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Microsoft\WindowsApps\Micros
oft.ScreenSketch_8wekyb3d8bbwe\SnippingTool.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Microsoft\WindowsApps\Micros
oft.Paint_8wekyb3d8bbwe\pbrush.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Microsoft\WindowsApps\Micros
oft.Paint_8wekyb3d8bbwe\mspaint.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Microsoft\WindowsApps\Micros
oft.MicrosoftEdge_8wekyb3d8bbwe\MicrosoftEdge.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Microsoft\WindowsApps\Micros
oft.DesktopAppInstaller_8wekyb3d8bbwe\winget.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Microsoft\WindowsApps\Micros
oft.DesktopAppInstaller_8wekyb3d8bbwe\WindowsPackageManagerServer.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Microsoft\WindowsApps\Micros
oft.DesktopAppInstaller_8wekyb3d8bbwe\python3.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Microsoft\WindowsApps\Micros
oft.DesktopAppInstaller_8wekyb3d8bbwe\python.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Microsoft\WindowsApps\FACEBO
OK.317180B0BB486_8xx8rvfyw5nnt\MessengerHelper.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Microsoft\WindowsApps\Clipch
amp.Clipchamp_yxz26nhyzhsrt\clipchamp.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Microsoft\WindowsApps\Canoni
calGroupLimited.Ubuntu_79rhkp1fndgsc\ubuntu.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\JetBrains\PyCharm2022.3\tmp\
sendctrlc.x64.B02191CB70385B094C410A8C27775ABA.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Host App
Service\Engine\HostAppService.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Host App
Service\Engine\HostAppServiceInterface.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Host App
Service\Engine\HostAppServiceUpdateManager.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Host App
Service\Engine\HostAppServiceUpdater.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Host App
Service\Engine\HostAppServiceUpdaterMetrics.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Host App
Service\Engine\WebAppHelper.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Host App
Service\Uninstall.exe": MOHANAPRASAD [AllAccess]
File Permissions
```

```
"C:\Users\MOHANAPRASAD\AppData\Local\GitHubDesktop\bin\github.bat": MOHANAPRASAD
[AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\AppData\Local\GitHubDesktop\GitHubDesktop.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\GitHubDesktop\Update.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Discord\Update.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\tc
l\nmake\x86_64-w64-mingw32-nmakehlp.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Sc
ripts\wsdump.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Sc
ripts\watchmedo.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Sc
ripts\validate-patterns.exe": MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Scripts\ttx.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Scripts\tqdm.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Sc
ripts\streamlit.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Sc
ripts\streamlit.cmd": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Sc
ripts\send2trash.exe": MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Scripts\scapy.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Scripts\qtpy.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Sc
ripts\pygmentize.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Sc
ripts\pyftsubset.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Sc
ripts\pyftmerge.exe": MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Scripts\pip3.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Scripts\pip.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Sc
ripts\openai.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Sc
ripts\normalizer.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Sc
ripts\markdown-it.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Sc
ripts\jupyter.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Sc
ripts\jupyter-trust.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Sc
ripts\jupyter-troubleshoot.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Sc
ripts\jupyter-serverextension.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Sc
ripts\jupyter-server.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Sc
ripts\jupyter-run.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Sc
ripts\jupyter-qtconsole.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Sc
ripts\jupyter-notebook.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Sc
ripts\jupyter-nbextension.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Sc
ripts\jupyter-nbconvert.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Sc
ripts\jupyter-nbclassic.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Sc
ripts\jupyter-nbclassic-serverextension.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Sc
ripts\jupyter-nbclassic-extension.exe": MOHANAPRASAD [AllAccess]
```

```
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Sc
ripts\jupyter-nbclassic-bundlerextension.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Sc
ripts\jupyter-migrate.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Sc
ripts\jupyter-kernelspec.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Sc
ripts\jupyter-kernel.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Sc
ripts\jupyter-execute.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Sc
ripts\jupyter-events.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Sc
ripts\jupyter-dejavu.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Sc
ripts\jupyter-console.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Sc
ripts\jupyter-bundlerextension.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Sc
ripts\jsonschema.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Sc
ripts\ipython3.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Sc
ripts\ipython.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Sc
ripts\fonttools.exe": MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Scripts\flask.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Scripts\f2py.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Sc
ripts\django-admin.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Li
b\site-packages\win32\pythonservice.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Li
b\site-packages\winpty\winpty-agent.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Li
b\site-packages\setuptools\gui.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Li
b\site-packages\setuptools\gui-arm64.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Li
b\site-packages\setuptools\gui-64.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Li
b\site-packages\setuptools\gui-32.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Li
b\site-packages\setuptools\cli.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Li
b\site-packages\setuptools\cli-arm64.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Li
b\site-packages\setuptools\cli-64.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Li
b\site-packages\setuptools\cli-32.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Li
b\site-packages\pythonwin\Pythonwin.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Li
b\site-packages\pip\_vendor\distlib\w64.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Li
b\site-packages\pip\_vendor\distlib\w64-arm.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Li
b\site-packages\pip\_vendor\distlib\w32.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Li
b\site-packages\pip\_vendor\distlib\t64.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Li
b\site-packages\pip\_vendor\distlib\t64-arm.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Li
b\site-packages\pip\_vendor\distlib\t32.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Li
b\site-packages\debugpy\_vendored\pydevd\pydevd_attach_to_process\linux_and_mac\co
mpile_manylinux.cmd": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Li
b\site-packages\debugpy\_vendored\pydevd\pydevd_attach_to_process\windows\compile_
windows.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Li
b\site-packages\debugpy\_vendored\pydevd\pydevd_attach_to_process\inject_dll_amd64
.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Li
```

```
b\site-packages\debugpy\_vendored\pydevd\pydevd_attach_to_process\inject_dll_x86.e
xe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Li
b\ctypes\macholib\fetch_macholib.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Li
b\venv\scripts\nt\pythonw.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Li
b\venv\scripts\nt\python.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Li
b\venv\scripts\nt\deactivate.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Li
b\venv\scripts\nt\activate.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Li
b\venv\scripts\common\Activate.ps1": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Li
b\idlelib\idle.bat": MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\python.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\pythonw.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Microsoft VS
Code\unins000.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Microsoft VS
Code\Code.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Microsoft VS
Code\bin\code.cmd": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Microsoft VS
Code\bin\code-tunnel.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Microsoft VS
Code\tools\inno_updater.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Microsoft VS
Code\resources\app\node_modules.asar.unpacked\@vscode\ripgrep\bin\rg.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Microsoft VS Code\r
esources\app\node_modules.asar.unpacked\node-pty\build\Release\winpty-agent.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Microsoft VS
Code\resources\app\node_modules.asar.unpacked\node-vsce-sign\bin\vsce-sign.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Microsoft VS Code\r
esources\app\out\vs\workbench\contrib\terminal\browser\media\shellIntegration.ps1"
: MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Nicepage\Uninstall
Nicepage.exe": MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\AppData\Local\Programs\Nicepage\Nicepage.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Nicepage\resources\
app.asar.unpacked\node_modules\edge-launcher\dist\x86\MicrosoftEdgeLauncher.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Nicepage\resources\
app.asar.unpacked\node_modules\ssh2\util\pagent.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\Nicepage\resources\
app.asar.unpacked\node_modules\ssh2\util\build_pagent.bat": MOHANAPRASAD
[AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\AppData\Local\Programs\Nicepage\resources\elevate.exe":
MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\AppData\Local\Programs\balena-etcher\Uninstall
balenaEtcher.exe": MOHANAPRASAD [AllAccess]
File Permissions
"C:\Users\MOHANAPRASAD\AppData\Local\Programs\balena-etcher\balenaEtcher.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Programs\balena-etcher\resou
rces\elevate.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\pypa\virtualenv\wheel\3.11\i
mage\1\CopyPipInstall\pip-22.3.1-py3-none-any\pip\_vendor\distlib\w64.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\pypa\virtualenv\wheel\3.11\i
mage\1\CopyPipInstall\pip-22.3.1-py3-none-any\pip\_vendor\distlib\w64-arm.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\pypa\virtualenv\wheel\3.11\i
mage\1\CopyPipInstall\pip-22.3.1-py3-none-any\pip\_vendor\distlib\w32.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\pypa\virtualenv\wheel\3.11\i
mage\1\CopyPipInstall\pip-22.3.1-py3-none-any\pip\_vendor\distlib\t64.exe":
```

```
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\pypa\virtualenv\wheel\3.11\i
mage\1\CopyPipInstall\pip-22.3.1-py3-none-any\pip\_vendor\distlib\t64-arm.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\pypa\virtualenv\wheel\3.11\i
mage\1\CopyPipInstall\pip-22.3.1-py3-none-any\pip\_vendor\distlib\t32.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\pypa\virtualenv\wheel\3.11\i
mage\1\CopyPipInstall\setuptools-65.5.1-py3-none-any\setuptools\cli-32.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\pypa\virtualenv\wheel\3.11\i
mage\1\CopyPipInstall\setuptools-65.5.1-py3-none-any\setuptools\cli-64.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\pypa\virtualenv\wheel\3.11\i
mage\1\CopyPipInstall\setuptools-65.5.1-py3-none-any\setuptools\cli-arm64.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\pypa\virtualenv\wheel\3.11\i
mage\1\CopyPipInstall\setuptools-65.5.1-py3-none-any\setuptools\cli.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\pypa\virtualenv\wheel\3.11\i
mage\1\CopyPipInstall\setuptools-65.5.1-py3-none-any\setuptools\gui-32.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\pypa\virtualenv\wheel\3.11\i
mage\1\CopyPipInstall\setuptools-65.5.1-py3-none-any\setuptools\gui-64.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\pypa\virtualenv\wheel\3.11\i
mage\1\CopyPipInstall\setuptools-65.5.1-py3-none-any\setuptools\gui-arm64.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\pypa\virtualenv\wheel\3.11\i
mage\1\CopyPipInstall\setuptools-65.5.1-py3-none-any\setuptools\gui.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Temp\vscode-stable-user-x64\
CodeSetup-stable-6445d93c81ebe42c4cbd7a60712e0b17d9463e97.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Temp\vscode-update-user-x64\
CodeSetup-stable-695af097c7bd098fbf017ce3ac85e09bbc5dda06.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Local\Temp\i4jdel0.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Roaming\Code\User\workspaceStorage
\54432434e07f9b0de1ef43397010e20c\ms-vscode.js-debug\.profile\SwReporter\107.294.2
00\software_reporter_tool.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Roaming\.anaconda\navigator\.anaco
nda\navigator\scripts\notebook.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Roaming\.anaconda\navigator\.anaco
nda\navigator\scripts\anaconda-navigator-updater.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Roaming\Telegram
Desktop\tupdates\temp\Telegram.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Roaming\Telegram
Desktop\tupdates\temp\Updater.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Roaming\Telegram
Desktop\Telegram.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Roaming\Telegram
Desktop\unins000.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Roaming\Telegram
Desktop\Updater.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Roaming\npm\tsc.cmd": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Roaming\npm\tsc.ps1": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Roaming\npm\tsserver.cmd":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\MOHANAPRASAD\AppData\Roaming\npm\tsserver.ps1":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\All Users\UiPath\UiPath.Common\21.10.30.8095\BrowserExt
ension\ChromeNativeMessaging.exe": Users [WriteData/CreateFiles]
File Permissions "C:\Users\All Users\UiPath\UiPath.Common\21.10.30.8095\BrowserExt
ension\UiPath.BrowserBridge.Portable\UiPath.BrowserBridge.Portable.exe": Users
[WriteData/CreateFiles]
File Permissions "C:\Users\All Users\UiPath\UiPath.Common\21.10.30.8095\BrowserExt
ension\UiPath.BrowserBridge.Portable\createdump.exe": Users [WriteData/CreateFiles]
File Permissions "C:\Users\All
Users\UiPath\UiPath.Common\21.10.30.8095\JavaSupport\ScreenScrapeJavaSupport.exe":
Users [WriteData/CreateFiles]
File Permissions "C:\Users\All
Users\UiPath\UiPath.Common\21.10.30.8095\SetupExtensions.exe": Users
[WriteData/CreateFiles]
File Permissions "C:\Users\All
Users\UiPath\UiPath.Common\21.10.30.8095\slinject.exe": Users
```

```
[WriteData/CreateFiles]
File Permissions "C:\Users\All
Users\UiPath\UiPath.Common\21.10.30.8095\UiPath.MicrosoftOffice.Tools.exe": Users
[WriteData/CreateFiles]
File Permissions "C:\Users\All
Users\UiPath\UiPath.Common\21.10.30.8095\UiPathRemoteRuntime.exe": Users
[WriteData/CreateFiles]
File Permissions "C:\Users\All Users\OEM\UpgradeTool\Quick_Access_V_3_0\2020129181
551344FixpackB\BUnzip\ColorIntelligence\CACE.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\All Users\OEM\UpgradeTool\Quick_Access_V_3_0\2020129181
551344FixpackB\BUnzip\LumiFlex\SunlightReading.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\All Users\OEM\UpgradeTool\Quick_Access_V_3_0\2020129181
551344FixpackB\BUnzip\Setup.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\All Users\OEM\UpgradeTool\Quick_Access_V_3_0\2022221173
134176FixpackB\BUnzip\ColorIntelligence\CACE.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\All Users\OEM\UpgradeTool\Quick_Access_V_3_0\2022221173
134176FixpackB\BUnzip\LumiFlex\SunlightReading.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\All Users\OEM\UpgradeTool\Quick_Access_V_3_0\2022221173
134176FixpackB\BUnzip\Setup.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\All
Users\OEM\UpgradeTool\Quick_Access_V_3_0\UpgradeToolC.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\All Users\Adobe\ARM\S\11169\AdobeARMHelper.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\All
Users\Acer\updater2\Download\46680762\D\UNERYCHK.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\All
Users\Acer\updater2\Download\46680762\D\HTTP2GA.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\All
Users\Acer\updater2\Download\46680762\D\FpCheck.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\All
Users\Acer\updater2\Download\46833097\D\NeedToRunUpdateReBuildSSD.exe":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\All
Users\Acer\updater2\Download\46833097\D\HTTP2GA.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\All
Users\Acer\updater2\Download\46833097\D\FpCheck.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\All
Users\Acer\updater2\Download\47196322\D\RunCmdX.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\All
Users\Acer\updater2\Download\47196322\D\HTTP2GA.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\All
Users\Acer\updater2\Download\47196322\D\FpCheck.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\All
Users\Acer\updater2\Download\47196322\D\ALU_PreloadUtility_Detect.cmd":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\All
Users\Acer\updater2\Download\47309875\D\RunCmdX.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\All
Users\Acer\updater2\Download\47309875\D\HTTP2GA.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\All
Users\Acer\updater2\Download\47309875\D\FpCheck.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\All
Users\Acer\updater2\Download\47309875\D\ALU_PreloadProcess_Detect.cmd":
MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\All
Users\Acer\updater2\Download\47309875\B\RunCmdX.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\All
Users\Acer\updater2\Download\47309875\B\HTTP2GA.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\All
Users\Acer\updater2\Download\47309875\B\FpInstall.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\All
Users\Acer\updater2\Download\47309875\B\ALU_PreloadProcess_Patch.cmd": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\All
Users\Acer\updater2\Download\47427154\D\HTTP2GA.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\All
Users\Acer\updater2\Download\47427154\D\FpCheck.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\All
Users\Acer\updater2\Download\47427154\D\AcerDriveUpgradeDetect.exe": MOHANAPRASAD
[AllAccess]
File Permissions "C:\Users\All
Users\Acer\updater2\Download\51601557\D\RunCmdX.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\All
Users\Acer\updater2\Download\51601557\D\HTTP2GA.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\All
Users\Acer\updater2\Download\51601557\D\FpCheck.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\All
Users\Acer\updater2\Download\51601557\D\FixpackD_CheckNBTH2.cmd": MOHANAPRASAD
```

```
[AllAccess]
File Permissions "C:\Users\All
Users\Acer\updater2\Download\52684576\D\HTTP2GA.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\All
Users\Acer\updater2\Download\52684576\D\FpCheck.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\All
Users\Acer\updater2\Download\52684576\D\ALUSNCheck.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\All
Users\Acer\updater2\Download\52939959\D\HTTP2GA.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\All
Users\Acer\updater2\Download\52939959\D\FpCheck.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\All
Users\Acer\updater2\Download\52939959\D\ALUSNCheck.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\All
Users\Acer\updater2\Download\53927262\D\RunCmdX.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\All
Users\Acer\updater2\Download\53927262\D\HTTP2GA.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\All
Users\Acer\updater2\Download\53927262\D\FpCheck.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\All
Users\Acer\updater2\Download\53927262\D\CheckVersion.bat": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\All
Users\Acer\updater2\Download\61296880\D\RunCmdX.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\All
Users\Acer\updater2\Download\61296880\D\OemDetect.cmd": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\All
Users\Acer\updater2\Download\61296880\D\HTTP2GA.exe": MOHANAPRASAD [AllAccess]
File Permissions "C:\Users\All
Users\Acer\updater2\Download\61296880\D\FpCheck.bat": MOHANAPRASAD [AllAccess]
```

Looking for Linux shells/distributions - wsl.exe, bash.exe

```
C:\Windows\System32\wsl.exe
WSL - no installed Linux distributions found.
```

File Analysis

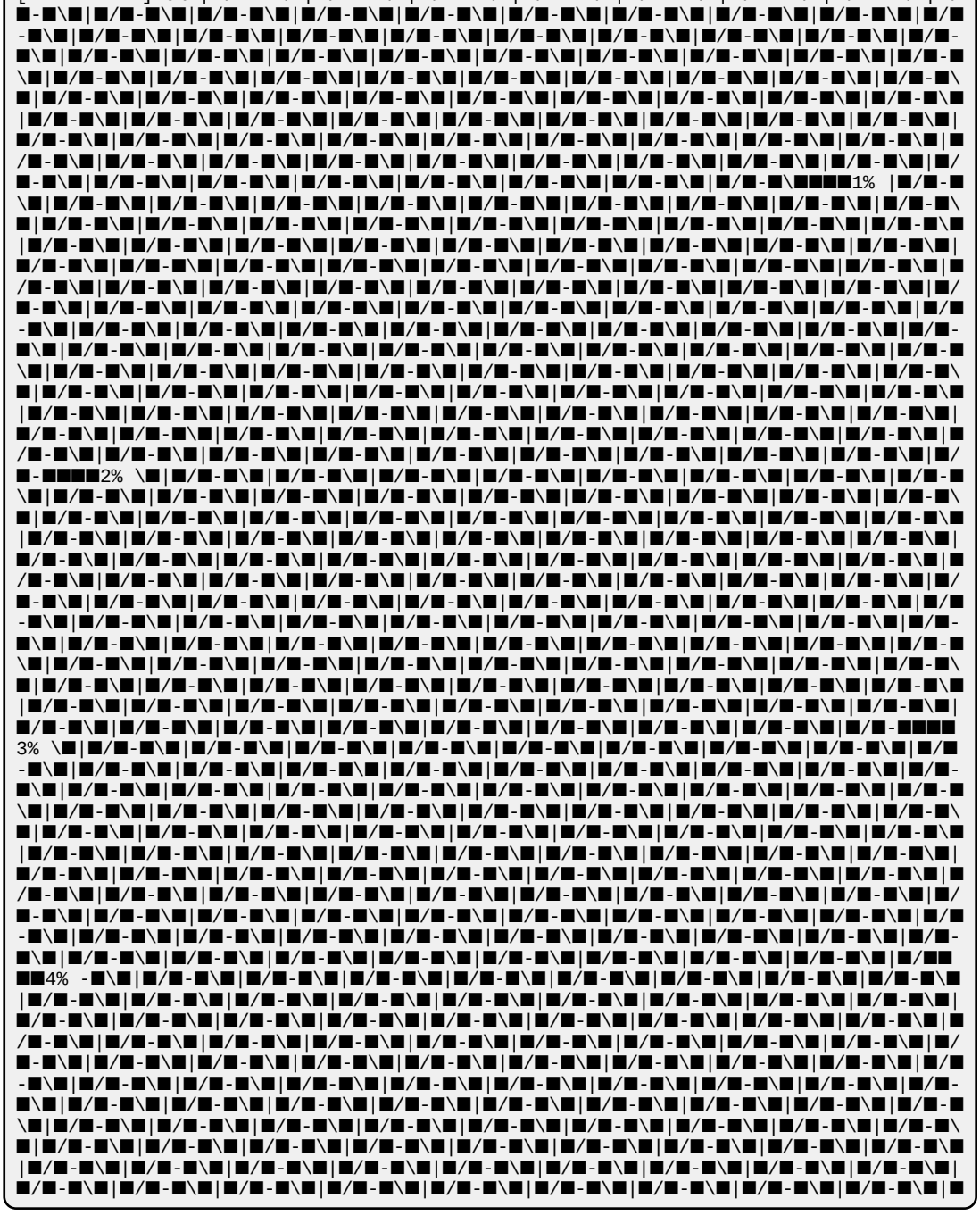
Found MySQL Files

```
Folder: C:\Users\MOHANAPRASAD\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\MySQL
Folder: C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Lib\site-pac
kages\django\db\backends\mysql
Folder: C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Lib\site-pac
kages\django\contrib\gis\db\backends\mysql
Folder: C:\Users\MOHANAPRASAD\AppData\Local\Programs\Python\Python311\Lib\site-pac
kages\jedi\third_party\django-stubs\django-stubs\db\backends\mysql
Folder: C:\Users\MOHANAPRASAD\AppData\Local\Temp\nvsIallR\dist\typeshed-fallback\s
tubs\SQLAlchemy\sqlalchemy\dialects\mysql
Folder: C:\Users\MOHANAPRASAD\AppData\Local\Temp\nvsIallR\dist\bundled\stubs\djang
o-stubs\contrib\gis\db\backends\mysql
Folder: C:\Users\MOHANAPRASAD\AppData\Local\Temp\nvsIallR\dist\bundled\stubs\djang
o-stubs\db\backends\mysql
Folder: C:\Users\MOHANAPRASAD\.vscode\extensions\ms-python.vscode-pylance-2023.8.1
0\dist\bundled\stubs\django-stubs\db\backends\mysql
Folder: C:\Users\MOHANAPRASAD\.vscode\extensions\ms-python.vscode-pylance-2023.8.1
0\dist\bundled\stubs\django-stubs\contrib\gis\db\backends\mysql
Folder: C:\Users\MOHANAPRASAD\.vscode\extensions\ms-python.python-2023.14.0\python
Files\lib\jedilsp\jedi\third_party\django-stubs\django-stubs\db\backends\mysql
Folder: C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\jedi\third_party\django-
stubs\django-stubs\db\backends\mysql
Folder: C:\Users\MOHANAPRASAD\anaconda3\Lib\site-packages\sqlalchemy\dialects\mysql
Folder: C:\Users\MOHANAPRASAD\anaconda3\pkgs\sqlalchemy-1.4.39-py39h2bbff1b_0\Lib\
site-packages\sqlalchemy\dialects\mysql
Folder: C:\Users\MOHANAPRASAD\anaconda3\pkgs\jedi-0.18.1-py39haa95532_1\Lib\site-p
```

```
ackages\jedi\third_party\django-stubs\django-stubs\db\backends\mysql
Folder: C:\Program Files\MySQL
Folder: C:\Program Files\MySQL\MySQL Shell
8.0\lib\Python3.10\Lib\site-packages\oci\mysql
Folder: C:\Program Files\MySQL\MySQL Server 8.0\include\mysql
Folder: C:\Program Files\JetBrains\PyCharm 2022.3.3\plugins\python\helpers\typeshe
d\stubs\SQLAlchemy\sqlalchemy\dialects\mysql
Folder: C:\Program Files (x86)\MySQL
```

Found CERTSB4 Files

```
File: C:\Users\All Users\Tenable\Nessus\nessus\tenable-plugins-b-20210201.pem
File: C:\Users\All Users\Tenable\Nessus\nessus\tenable-plugins-a-20210201.pem
File: C:\Users\All Users\Tenable\Nessus\nessus\tenable-plugins-20210201.pem
File: C:\Users\All Users\Tenable\Nessus\nessus\nessus_org.pem
File: C:\Users\All Users\Tenable\Nessus\nessus\CA\serverkey.pem
[----------] 0% |
```



```
/■-■\■|■/■-■\■|■/■-■\■|■/■-■\■|■/■-■\■|■/■-■\■|■/■-■\■|■/■-■\■|■/
■-■\■|■■■■■■■■■■■■■■■■■■■■ ■■■■■■■■■■■■■■■■■■■■Error looking for regexes
inside files: System.AggregateException: One or more errors occurred. --->
System.UnauthorizedAccessException: Access to the path 'C:\Users\All
Users\Tenable\Nessus\nessus\log.json' is denied.
at System.IO.__Error.WinIOError(Int32 errorCode, String maybeFullPath)
at System.IO.FileStream.Init(String path, FileMode mode, FileAccess access, Int32
rights, Boolean useRights, FileShare share, Int32 bufferSize, FileOptions options,
SECURITY_ATTRIBUTES secAttrs, String msgPath, Boolean bFromProxy, Boolean
useLongPath, Boolean checkHost)
at System.IO.FileStream..ctor(String path, FileMode mode, FileAccess access,
FileShare share, Int32 bufferSize, FileOptions options, String msgPath, Boolean
bFromProxy, Boolean useLongPath, Boolean checkHost)
at System.IO.StreamReader..ctor(String path, Encoding encoding, Boolean
detectEncodingFromByteOrderMarks, Int32 bufferSize, Boolean checkHost)
at System.IO.StreamReader..ctor(String path)
at winPEAS.Checks.FileAnalysis.<>c__DisplayClass6_2.<PrintYAMLRegexesSearchFiles>b
__4(CustomFileInfo f)
at System.Threading.Tasks.Parallel.<>c__DisplayClass17_0`1.<ForWorker>b__1()
at System.Threading.Tasks.Task.InnerInvokeWithArg(Task childTask)
at System.Threading.Tasks.Task.<>c__DisplayClass176_0.<ExecuteSelfReplicating>b__0
(Object <p0>)
--- End of inner exception stack trace ---
at System.Threading.Tasks.Task.ThrowIfExceptional(Boolean
includeTaskCanceledExceptions)
at System.Threading.Tasks.Task.Wait(Int32 millisecondsTimeout, CancellationToken
cancellationToken)
at System.Threading.Tasks.Parallel.ForWorker[TLocal](Int32 fromInclusive, Int32
toExclusive, ParallelOptions parallelOptions, Action`1 body, Action`2
bodyWithState, Func`4 bodyWithLocal, Func`1 localInit, Action`1 localFinally)
at System.Threading.Tasks.Parallel.ForEachWorker[TSource,TLocal](IEnumerable`1
source, ParallelOptions parallelOptions, Action`1 body, Action`2 bodyWithState,
Action`3 bodyWithStateAndIndex, Func`4 bodyWithStateAndLocal, Func`5
bodyWithEverything, Func`1 localInit, Action`1 localFinally)
at System.Threading.Tasks.Parallel.ForEach[TSource](IEnumerable`1 source,
ParallelOptions parallelOptions, Action`1 body)
at winPEAS.Checks.FileAnalysis.<>c__DisplayClass6_2.<PrintYAMLRegexesSearchFiles>b
__3()
at winPEAS.Helpers.CheckRunner.Run(Action action, Boolean isDebug, String
description)
at winPEAS.Checks.FileAnalysis.PrintYAMLRegexesSearchFiles()
---> (Inner Exception #0) System.UnauthorizedAccessException: Access to the path
'C:\Users\All Users\Tenable\Nessus\nessus\log.json' is denied.
at System.IO.__Error.WinIOError(Int32 errorCode, String maybeFullPath)
at System.IO.FileStream.Init(String path, FileMode mode, FileAccess access, Int32
rights, Boolean useRights, FileShare share, Int32 bufferSize, FileOptions options,
SECURITY_ATTRIBUTES secAttrs, String msgPath, Boolean bFromProxy, Boolean
useLongPath, Boolean checkHost)
at System.IO.FileStream..ctor(String path, FileMode mode, FileAccess access,
FileShare share, Int32 bufferSize, FileOptions options, String msgPath, Boolean
bFromProxy, Boolean useLongPath, Boolean checkHost)
at System.IO.StreamReader..ctor(String path, Encoding encoding, Boolean
detectEncodingFromByteOrderMarks, Int32 bufferSize, Boolean checkHost)
at System.IO.StreamReader..ctor(String path)
at winPEAS.Checks.FileAnalysis.<>c__DisplayClass6_2.<PrintYAMLRegexesSearchFiles>b
__4(CustomFileInfo f)
at System.Threading.Tasks.Parallel.<>c__DisplayClass17_0`1.<ForWorker>b__1()
at System.Threading.Tasks.Task.InnerInvokeWithArg(Task childTask)
at System.Threading.Tasks.Task.<>c__DisplayClass176_0.<ExecuteSelfReplicating>b__0
(Object <p0>)<---
/---------------------------------------------------------------------------
\
| Do you like PEASS? |
|---------------------------------------------------------------------------
|
| Get the latest version : https://github.com/sponsors/carlospolop |
| Follow on Twitter : @hacktricks_live |
| Respect on HTB : SirBroccoli |
|---------------------------------------------------------------------------
|
| Thank you! |
\---------------------------------------------------------------------------
/
```