# 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: Intel64 Family 6 Model 140 Stepping 2 GenuineIntel ~2496 Mhz
System Type: x64-based PC
Hostname: DESKTOP-SNEHA
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: 23-07-2023 10:27:43
HighIntegrity: True
PartOfDomain: False
Hotfixes: KB5028851, KB5012170, KB5028185, KB5028320,
[?] Windows vulns search powered by Watson(https://github.com/rasta-mouse/Watson)
```

## Showing All Microsoft Updates

```
HotFix ID : KB2267602
Installed At (UTC) : 22-07-2023 21:48:17
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.393.1141.0)
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) : 22-07-2023 05:11:25
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.393.1067.0)
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 22:35:36
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.393.1040.0)
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) : 21-07-2023 01:12:33
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.393.953.0)
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) : 20-07-2023 10:09:15
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.393.887.0)
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) : 19-07-2023 22:05:11
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.393.845.0)
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) : 19-07-2023 00:39:14
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.393.757.0)
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 22:39:43
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.393.671.0)
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) : 17-07-2023 11:11:08
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.393.629.0)
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 10:33:17
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.393.629.0)
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) : 17-07-2023 00:46:45
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.393.578.0)
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) : 16-07-2023 22:04:36
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.393.578.0)
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) : 16-07-2023 22:03:08
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.393.473.0)
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) : 15-07-2023 12:29:16
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.393.437.0)
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) : 15-07-2023 00:33:16
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.393.382.0)
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) : 13-07-2023 11:17:10
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 :
Installed At (UTC) : 13-07-2023 10:42:32
Title : Realtek Semiconductor Corp. - MEDIA - 6.0.9511.1
Client Application ID : MoUpdateOrchestrator
Description : Realtek Semiconductor Corp. MEDIA driver update released in May 2023
================================================================================
==============
HotFix ID :
Installed At (UTC) : 13-07-2023 10:42:26
Title : Intel Corporation - Bluetooth - 22.200.0.2
Client Application ID : MoUpdateOrchestrator
Description : Intel Corporation Bluetooth driver update released in December 2022
================================================================================
==============
HotFix ID : KB2267602
Installed At (UTC) : 13-07-2023 10:42:17
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.393.218.0)
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) : 13-07-2023 01:00:40
Title : 9WZDNCRFJBMP-MICROSOFT.WINDOWSSTORE
Client Application ID : Update;ScanForUpdatesForUser
Description : 9WZDNCRFJBMP-1152921505696522951
================================================================================
==============
HotFix ID :
Installed At (UTC) : 12-07-2023 23:38:55
Title : 9NBLGGH51CLL-Microsoft.Services.Store.Engagement
Client Application ID : <<PROCESS>>: svchost.exe
```

```
Description : 9NBLGGH51CLL-1152921505696486075
================================================================================
===============
HotFix ID : KB5028851
Installed At (UTC) : 12-07-2023 23:23:10
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 : KB890830
Installed At (UTC) : 12-07-2023 23:22:38
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) : 12-07-2023 00:26:49
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.393.120.0)
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) : 11-07-2023 11:46:55
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.393.60.0)
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) : 10-07-2023 22:40:02
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.4170.0)
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) : 10-07-2023 09:56:51
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.4116.0)
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) : 09-07-2023 09:18:47
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.4022.0)
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) : 08-07-2023 05:14:45
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.3914.0)
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) : 07-07-2023 22:37:04
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.3887.0)
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) : 07-07-2023 09:03:22
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.3834.0)
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) : 07-07-2023 09:03:07
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 : KB2267602
Installed At (UTC) : 03-07-2023 23:36:48
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.3493.0)
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) : 01-07-2023 23:22:10
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.3271.0)
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) : 30-06-2023 08:18:09
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.3099.0)
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) : 29-06-2023 20:14:50
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.3055.0)
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) : 29-06-2023 06:32:59
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.2994.0)
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) : 28-06-2023 01:19:10
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.2874.0)
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 10:41:30
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.2789.0)
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) : 27-06-2023 05:10:11
Title : Waves - Extension - 6.0.15.0
Client Application ID : MoUpdateOrchestrator
Description : Waves Extension driver update released in March 2023
================================================================================
===============
HotFix ID : KB2267602
Installed At (UTC) : 26-06-2023 05:25:48
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.2688.0)
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) : 26-06-2023 03:16:12
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.2667.0)
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) : 24-06-2023 22:33:05
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.2539.0)
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) : 24-06-2023 10:21:09
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.2475.0)
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) : 23-06-2023 20:40:57
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.2419.0)
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) : 23-06-2023 03:49:36
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.2276.0)
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) : 21-06-2023 23:37:29
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.2221.0)
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) : 21-06-2023 10:49:24
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.2163.0)
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) : 20-06-2023 22:41:54
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.2115.0)
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) : 20-06-2023 10:06:53
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.2070.0)
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) : 20-06-2023 05:26:30
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.2062.0)
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) : 19-06-2023 22:01:20
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.2013.0)
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) : 18-06-2023 05:27:22
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.1849.0)
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 : KB5027119
Installed At (UTC) : 18-06-2023 05:27:00
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 : KB2267602
Installed At (UTC) : 16-06-2023 23:45:29
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.1708.0)
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 : KB5027231
Installed At (UTC) : 14-06-2023 10:34:16
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 :
Installed At (UTC) : 14-06-2023 09:59:24
Title : 9P105T65H4Z5-Microsoft.WindowsAppRuntime.1.3
Client Application ID : <<PROCESS>>: svchost.exe
Description : 9P105T65H4Z5-1152921505696411251
================================================================================
===============
HotFix ID : KB890830
Installed At (UTC) : 14-06-2023 09:33:59
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 : KB2267602
Installed At (UTC) : 14-06-2023 09:27:03
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.1418.0)
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 : KB4052623
Installed At (UTC) : 13-06-2023 20:09:11
Title : Update for Microsoft Defender Antivirus antimalware platform - KB4052623
```

```
(Version 4.18.23050.5)
Client Application ID : MoUpdateOrchestrator
Description : This package will update Microsoft Defender Antivirus antimalware
platform's components on the user machine.
================================================================================
===============
HotFix ID : KB2267602
Installed At (UTC) : 13-06-2023 20:08:38
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.1348.0)
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) : 13-06-2023 01:27:46
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.1275.0)
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) : 12-06-2023 13:05:35
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.1206.0)
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) : 12-06-2023 13:05:15
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.1183.0)
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) : 11-06-2023 12:38:14
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.1131.0)
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) : 11-06-2023 02:07:37
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.1104.0)
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) : 10-06-2023 23:59:23
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.1083.0)
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) : 10-06-2023 11:41:37
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
```

```
(Version 1.391.1035.0)
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) : 09-06-2023 09:22:17
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.936.0)
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) : 08-06-2023 10:44:27
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.851.0)
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) : 07-06-2023 23:02:49
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.787.0)
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) : 07-06-2023 08:56:14
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.723.0)
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) : 06-06-2023 17:37:15
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.672.0)
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) : 06-06-2023 10:39:09
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.661.0)
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) : 05-06-2023 22:11:49
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.576.0)
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) : 04-06-2023 22:04:58
```

```
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.476.0)
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) : 04-06-2023 01:12:22
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.390.0)
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) : 03-06-2023 21:33:12
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.375.0)
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) : 03-06-2023 00:44:43
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.315.0)
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) : 02-06-2023 12:29:30
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.268.0)
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) : 01-06-2023 10:29:23
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.157.0)
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 : KB4052623
Installed At (UTC) : 31-05-2023 22:18:39
Title : Update for Microsoft Defender Antivirus antimalware platform - KB4052623
(Version 4.18.23050.3)
Client Application ID : MoUpdateOrchestrator
Description : This package will update Microsoft Defender Antivirus antimalware
platform's components on the user machine.
========================================================================================
===============
HotFix ID : KB2267602
Installed At (UTC) : 31-05-2023 22:18:05
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.109.0)
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) : 31-05-2023 10:14:09
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.391.64.0)
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) : 30-05-2023 10:46:59
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.2778.0)
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 : KB5026446
Installed At (UTC) : 30-05-2023 03:29:49
Title : 2023-05 Cumulative Update Preview for Windows 11 Version 22H2 for x64-based
Systems (KB5026446)
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 : KB5026446
Installed At (UTC) : 30-05-2023 02:21:53
Title : 2023-05 Cumulative Update Preview for Windows 11 Version 22H2 for x64-based
Systems (KB5026446)
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) : 30-05-2023 00:19:36
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.2739.0)
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) : 29-05-2023 22:39:04
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.2729.0)
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) : 29-05-2023 09:50:07
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.2656.0)
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) : 29-05-2023 09:45:33
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.2608.0)
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) : 28-05-2023 05:55:02
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.2573.0)
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) : 26-05-2023 21:36:13
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.2509.0)
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) : 26-05-2023 07:46:23
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.2456.0)
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 19:46:39
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.2412.0)
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) : 24-05-2023 23:22:28
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.2356.0)
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) : 24-05-2023 10:41:49
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.2349.0)
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 21:46:19
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 00:15:09
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.2171.0)
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) : 21-05-2023 23:31:49
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.2060.0)
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) : 21-05-2023 03:39:47
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.1993.0)
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 19:38:16
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.1855.0)
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 08:03:51
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) : 18-05-2023 11:32:34
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.1729.0)
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) : 18-05-2023 11:32:33
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.1729.0)
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) : 17-05-2023 23:09:00
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.1674.0)
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) : 17-05-2023 11:02:29
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.1621.0)
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 22:59:52
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 10:52:26
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.1489.0)
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 04:58:07
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.1422.0)
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) : 15-05-2023 10:26:38
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.1375.0)
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) : 15-05-2023 09:40:25
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.1362.0)
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) : 15-05-2023 04:46:46
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.1314.0)
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) : 14-05-2023 10:59:44
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.1261.0)
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) : 13-05-2023 22:51:15
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
```

```
(Version 1.389.1206.0)
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) : 13-05-2023 10:48:15
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.1163.0)
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) : 12-05-2023 20:04:19
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.1084.0)
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) : 12-05-2023 06:57:05
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.1036.0)
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) : 11-05-2023 21:34:50
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 : KB2267602
Installed At (UTC) : 11-05-2023 19:55:43
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.986.0)
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 19:55:07
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 : KB5026372
Installed At (UTC) : 11-05-2023 16:01:32
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 : KB2267602
Installed At (UTC) : 11-05-2023 08:02:06
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.915.0)
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) : 10-05-2023 07:52:33
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.817.0)
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) : 09-05-2023 19:34:26
Title : 9WZDNCRDTBVB-MICROSOFT.WINDOWSMAPS
Client Application ID : Update;ScanForUpdates
Description : 9WZDNCRDTBVB-1152921505696271927
================================================================================
===============
HotFix ID :
Installed At (UTC) : 09-05-2023 19:15:33
Title : 9WZDNCRFJ3Q2-Microsoft.BingWeather
Client Application ID : Update;ScanForUpdates
Description : 9WZDNCRFJ3Q2-1152921505696268329
================================================================================
===============
HotFix ID : KB2267602
Installed At (UTC) : 09-05-2023 06:44:35
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.691.0)
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) : 08-05-2023 21:00:06
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.659.0)
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) : 08-05-2023 13:05:10
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.612.0)
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) : 08-05-2023 13:04:48
Title : Update for Microsoft Defender Antivirus antimalware platform - KB5007651
(Version 1.0.2303.27001)
Client Application ID : MoUpdateOrchestrator
Description : This package will update Microsoft Defender Antivirus antimalware
platform's components on the user machine.
================================================================================
```

```
===============
HotFix ID : KB2267602
Installed At (UTC) : 07-05-2023 09:15:00
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.495.0)
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) : 07-05-2023 09:14:42
Title : Update for Microsoft Defender Antivirus antimalware platform - KB5007651
(Version 1.0.2303.27001)
Client Application ID : MoUpdateOrchestrator
Description : This package will update Microsoft Defender Antivirus antimalware
platform's components on the user machine.
================================================================================
===============
HotFix ID : KB2267602
Installed At (UTC) : 06-05-2023 21:07:24
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.448.0)
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) : 06-05-2023 21:07:14
Title : Update for Microsoft Defender Antivirus antimalware platform - KB5007651
(Version 1.0.2303.27001)
Client Application ID : MoUpdateOrchestrator
Description : This package will update Microsoft Defender Antivirus antimalware
platform's components on the user machine.
================================================================================
===============
HotFix ID : KB2267602
Installed At (UTC) : 06-05-2023 11:04:53
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.351.0)
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) : 06-05-2023 04:33:24
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.351.0)
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) : 06-05-2023 02:43:29
Title : Update for Microsoft Defender Antivirus antimalware platform - KB5007651
(Version 1.0.2303.27001)
Client Application ID : MoUpdateOrchestrator
Description : This package will update Microsoft Defender Antivirus antimalware
platform's components on the user machine.
================================================================================
===============
HotFix ID : KB2267602
Installed At (UTC) : 05-05-2023 08:33:24
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.272.0)
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) : 05-05-2023 03:58:01
Title : Update for Microsoft Defender Antivirus antimalware platform - KB5007651
(Version 1.0.2303.27001)
Client Application ID : MoUpdateOrchestrator
Description : This package will update Microsoft Defender Antivirus antimalware
platform's components on the user machine.
=====================================================================================
===============
HotFix ID : KB5007651
Installed At (UTC) : 04-05-2023 14:53:11
Title : Update for Microsoft Defender Antivirus antimalware platform - KB5007651
(Version 1.0.2303.27001)
Client Application ID : MoUpdateOrchestrator
Description : This package will update Microsoft Defender Antivirus antimalware
platform's components on the user machine.
=====================================================================================
===============
HotFix ID : KB2267602
Installed At (UTC) : 04-05-2023 14:52:51
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.215.0)
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) : 04-05-2023 03:00:19
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) : 04-05-2023 02:55:36
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.140.0)
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) : 03-05-2023 04:34:31
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.44.0)
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) : 03-05-2023 04:24:50
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.389.10.0)
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 : KB4052623
Installed At (UTC) : 03-05-2023 04:23:46
Title : Update for Microsoft Defender Antivirus antimalware platform - KB4052623
(Version 4.18.2304.8)
Client Application ID : MoUpdateOrchestrator
Description : This package will update Microsoft Defender Antivirus antimalware
platform's components on the user machine.
=====================================================================================
===============
HotFix ID : KB2267602
Installed At (UTC) : 02-05-2023 09:42:15
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
```

```
(Version 1.387.2964.0)
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) : 02-05-2023 04:50:10
Title : Realtek Semiconductor Corp. - MEDIA - 6.0.9481.1
Client Application ID : MoUpdateOrchestrator
Description : Realtek Semiconductor Corp. MEDIA driver update released in February
2023
================================================================================
===============
HotFix ID : KB2267602
Installed At (UTC) : 02-05-2023 04:49:56
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.387.2917.0)
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) : 02-05-2023 04:47:10
Title : 9WZDNCRDTBJJ-MICROSOFT.GETSTARTED
Client Application ID : Update;ScanForUpdatesForUser
Description : 9WZDNCRDTBJJ-1152921505696203113
================================================================================
===============
HotFix ID :
Installed At (UTC) : 30-04-2023 23:57:19
Title : Intel(R) Corporation - System - 10.29.0.8276
Client Application ID : MoUpdateOrchestrator
Description : Intel(R) Corporation System driver update released in November 2022
================================================================================
===============
HotFix ID :
Installed At (UTC) : 30-04-2023 23:56:27
Title : Intel(R) Corporation - MEDIA - 10.29.0.8276
Client Application ID : MoUpdateOrchestrator
Description : Intel(R) Corporation MEDIA driver update released in November 2022
================================================================================
===============
HotFix ID :
Installed At (UTC) : 30-04-2023 23:56:14
Title : Intel(R) Corporation - MEDIA - 10.29.0.8276
Client Application ID : MoUpdateOrchestrator
Description : Intel(R) Corporation MEDIA driver update released in November 2022
================================================================================
===============
HotFix ID :
Installed At (UTC) : 30-04-2023 23:56:02
Title : Intel(R) Corporation - System - 10.29.0.8276
Client Application ID : MoUpdateOrchestrator
Description : Intel(R) Corporation System driver update released in November 2022
================================================================================
===============
HotFix ID :
Installed At (UTC) : 30-04-2023 23:42:14
Title : Realtek - SoftwareComponent - 11.0.6000.1096
Client Application ID : MoUpdateOrchestrator
Description : Realtek SoftwareComponent driver update released in February 2023
================================================================================
===============
HotFix ID :
Installed At (UTC) : 30-04-2023 23:42:10
Title : Realtek - SoftwareComponent - 1.0.596.0
Client Application ID : MoUpdateOrchestrator
Description : Realtek SoftwareComponent driver update released in February 2023
================================================================================
===============
HotFix ID : KB2267602
Installed At (UTC) : 30-04-2023 23:35:29
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.387.2820.0)
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) : 29-04-2023 18:25:10
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.387.2676.0)
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) : 29-04-2023 04:10:20
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.387.2630.0)
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) : 28-04-2023 13:15:37
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.387.2553.0)
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) : 27-04-2023 22:42:38
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.387.2491.0)
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) : 27-04-2023 10:31:11
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.387.2422.0)
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) : 26-04-2023 22:08:15
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.387.2357.0)
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) : 26-04-2023 00:22:46
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.387.2251.0)
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) : 25-04-2023 11:47:01
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
```

```
(Version 1.387.2184.0)
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) : 24-04-2023 23:34:48
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.387.2106.0)
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) : 24-04-2023 10:50:55
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.387.2078.0)
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) : 24-04-2023 00:37:02
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 10:22:09
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.387.1965.0)
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) : 22-04-2023 22:13:46
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.387.1929.0)
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) : 22-04-2023 06:01:54
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.387.1870.0)
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) : 19-04-2023 11:53:24
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.387.1490.0)
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) : 19-04-2023 10:55:35
```

```
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.387.1554.0)
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) : 19-04-2023 01:15:23
Title : Update for Microsoft Defender Antivirus antimalware platform - KB5007651
(Version 1.0.2303.27001)
Client Application ID : MoUpdateOrchestrator
Description : This package will update Microsoft Defender Antivirus antimalware
platform's components on the user machine.
================================================================================
===============
HotFix ID : KB5007651
Installed At (UTC) : 18-04-2023 22:20:29
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 :
Installed At (UTC) : 18-04-2023 11:04:58
Title : Realtek Semiconductor Corp. - Extension - 6.0.9481.1
Client Application ID : MoUpdateOrchestrator
Description : Realtek Semiconductor Corp. Extension driver update released in
February 2023
================================================================================
===============
HotFix ID : KB2267602
Installed At (UTC) : 17-04-2023 19:31:23
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.387.1376.0)
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) : 17-04-2023 03:24:58
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.387.1281.0)
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) : 15-04-2023 22:47:24
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.387.1166.0)
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) : 15-04-2023 08:43:27
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.387.1123.0)
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) : 15-04-2023 06:58:57
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.387.1114.0)
```

```
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) : 13-04-2023 23:06:41
Title : Intel Corporation - SoftwareComponent - 18.7.6.1010
Client Application ID : MoUpdateOrchestrator
Description : Intel Corporation SoftwareComponent driver update released in
September 2022
================================================================================
===============
HotFix ID : KB2267602
Installed At (UTC) : 13-04-2023 21:53:52
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.387.968.0)
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) : 13-04-2023 21:52:43
Title : Realtek Semiconductor Corp. - MEDIA - 6.0.9418.1
Client Application ID : MoUpdateOrchestrator
Description : Realtek Semiconductor Corp. MEDIA driver update released in September
2022
================================================================================
===============
HotFix ID :
Installed At (UTC) : 13-04-2023 21:52:18
Title : Intel Corporation - SoftwareComponent - 18.7.6.1010
Client Application ID : MoUpdateOrchestrator
Description : Intel Corporation SoftwareComponent driver update released in
September 2022
================================================================================
===============
HotFix ID : KB5025239
Installed At (UTC) : 12-04-2023 23:35:18
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 : KB2267602
Installed At (UTC) : 12-04-2023 23:29:15
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602
(Version 1.387.862.0)
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) : 12-04-2023 23:19:05
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 : KB5007651
Installed At (UTC) : 12-04-2023 23:18:47
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) : 12-04-2023 23:02:46
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 : KB890830
Installed At (UTC) : 12-04-2023 09:38:11
Title : Windows Malicious Software Removal Tool x64 - v5.112 (KB890830)
Client Application ID : <<PROCESS>>: McVulCtr.exe
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 : KB5025239
Installed At (UTC) : 12-04-2023 09:21:29
Title : 2023-04 Cumulative Update for Windows 11 Version 22H2 for x64-based Systems
(KB5025239)
Client Application ID : <<PROCESS>>: McVulCtr.exe
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 : KB5025239
Installed At (UTC) : 12-04-2023 05:33:48
Title : 2023-04 Cumulative Update for Windows 11 Version 22H2 for x64-based Systems
(KB5025239)
Client Application ID : <<PROCESS>>: McVulCtr.exe
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) : 02-04-2023 23:13:55
Title : Intel Corporation - SCSIAdapter - 18.7.6.1010
Client Application ID : MoUpdateOrchestrator
Description : Intel Corporation SCSIAdapter driver update released in September
2022
================================================================================
================
HotFix ID :
Installed At (UTC) : 28-03-2023 11:23:48
Title : Dell, Inc. - Firmware - 0.2.17.0
Client Application ID : MoUpdateOrchestrator
Description : Dell, Inc. Firmware driver update released in February 2023
================================================================================
================
HotFix ID :
Installed At (UTC) : 23-03-2023 21:45:23
Title : Intel Corporation - Extension - 18.7.6.1010
Client Application ID : MoUpdateOrchestrator
Description : Intel Corporation Extension driver update released in September 2022
================================================================================
================
HotFix ID : KB890830
Installed At (UTC) : 17-03-2023 23:06:34
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 : KB890830
Installed At (UTC) : 16-03-2023 10:49:22
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) : 15-03-2023 04:09:12
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 :
Installed At (UTC) : 11-03-2023 11:10:07
Title : Intel - System - 3.1.0.4477
Client Application ID : MoUpdateOrchestrator
Description : Intel System driver update released in July 2021
================================================================================
===============
HotFix ID :
Installed At (UTC) : 11-03-2023 11:10:02
Title : Intel - HIDClass - 3.1.0.4477
Client Application ID : MoUpdateOrchestrator
Description : Intel HIDClass driver update released in July 2021
================================================================================
===============
HotFix ID :
Installed At (UTC) : 11-03-2023 11:09:56
Title : Intel - System - 3.1.0.4477
Client Application ID : MoUpdateOrchestrator
Description : Intel System driver update released in July 2021
================================================================================
===============
HotFix ID :
Installed At (UTC) : 10-03-2023 01:40:40
Title : Intel(R) Corporation - System - 10.29.0.7799
Client Application ID : MoUpdateOrchestrator
Description : Intel(R) Corporation System driver update released in June 2022
================================================================================
===============
HotFix ID :
Installed At (UTC) : 09-03-2023 08:46:13
Title : Intel(R) Corporation - System - 1.0.2256.0
Client Application ID : MoUpdateOrchestrator
Description : Intel(R) Corporation System driver update released in April 2022
================================================================================
===============
HotFix ID :
Installed At (UTC) : 09-03-2023 08:45:52
Title : Intel(R) Corporation - System - 10.29.0.7799
Client Application ID : MoUpdateOrchestrator
Description : Intel(R) Corporation System driver update released in June 2022
================================================================================
===============
HotFix ID :
Installed At (UTC) : 09-03-2023 08:45:17
Title : Intel(R) Corporation - MEDIA - 10.29.0.7799
Client Application ID : MoUpdateOrchestrator
Description : Intel(R) Corporation MEDIA driver update released in June 2022
================================================================================
```

```
===============
HotFix ID :
Installed At (UTC) : 07-03-2023 04:53:10
Title : 9NBLGGH5R558-Microsoft.Todos
Client Application ID : Update;ScanForUpdatesForUser
Description : 9NBLGGH5R558-1152921505696019655
================================================================================
===============
HotFix ID :
Installed At (UTC) : 07-03-2023 04:52:10
Title : 9WZDNCRFJBMP-MICROSOFT.WINDOWSSTORE
Client Application ID : Update;ScanForUpdatesForUser
Description : 9WZDNCRFJBMP-1152921505696013436
================================================================================
===============
HotFix ID :
Installed At (UTC) : 06-03-2023 19:21:21
Title : Realtek - SoftwareComponent - 11.0.6000.1062
Client Application ID : MoUpdateOrchestrator
Description : Realtek SoftwareComponent driver update released in July 2022
================================================================================
===============
HotFix ID :
Installed At (UTC) : 06-03-2023 19:21:19
Title : Realtek - SoftwareComponent - 1.0.0.9
Client Application ID : MoUpdateOrchestrator
Description : Realtek SoftwareComponent driver update released in September 2022
================================================================================
===============
HotFix ID :
Installed At (UTC) : 06-03-2023 19:21:17
Title : Realtek - SoftwareComponent - 1.0.565.0
Client Application ID : MoUpdateOrchestrator
Description : Realtek SoftwareComponent driver update released in September 2022
================================================================================
===============
HotFix ID :
Installed At (UTC) : 28-02-2023 02:45:32
Title : 9N5TDP8VCMHS-Microsoft.WebMediaExtensions
Client Application ID : Update;ScanForUpdatesForUser
Description : 9N5TDP8VCMHS-1152921505693791332
================================================================================
===============
HotFix ID :
Installed At (UTC) : 28-02-2023 02:43:58
Title : 9NBLGGH10PG8-MICROSOFT.PEOPLE
Client Application ID : Update;ScanForUpdatesForUser
Description : 9NBLGGH10PG8-1152921505693623180
================================================================================
===============
HotFix ID :
Installed At (UTC) : 28-02-2023 02:42:25
Title : 9NBLGGH537C2-Microsoft.XboxGameOverlay
Client Application ID : Update;ScanForUpdatesForUser
Description : 9NBLGGH537C2-1152921505690350335
================================================================================
===============
HotFix ID :
Installed At (UTC) : 27-02-2023 03:06:48
Title : 9N5TDP8VCMHS-Microsoft.WebMediaExtensions
Client Application ID : Update;ScanForUpdates
Description : 9N5TDP8VCMHS-1152921505693791332
================================================================================
===============
HotFix ID :
Installed At (UTC) : 27-02-2023 03:05:48
Title : 9NBLGGH537C2-Microsoft.XboxGameOverlay
Client Application ID : Update;ScanForUpdates
Description : 9NBLGGH537C2-1152921505690350335
================================================================================
===============
HotFix ID :
Installed At (UTC) : 27-02-2023 03:04:48
Title : 9NBLGGH10PG8-MICROSOFT.PEOPLE
Client Application ID : Update;ScanForUpdates
Description : 9NBLGGH10PG8-1152921505693623180
================================================================================
===============
HotFix ID :
```

```
Installed At (UTC) : 23-02-2023 20:33:13
Title : Dell, Inc. - Firmware - 0.2.16.0
Client Application ID : MoUpdateOrchestrator
Description : Dell, Inc. Firmware driver update released in December 2022
================================================================================
===============
HotFix ID :
Installed At (UTC) : 23-02-2023 20:31:12
Title : Realtek Semiconductor Corp. - Extension - 10.0.212.29
Client Application ID : MoUpdateOrchestrator
Description : Realtek Semiconductor Corp. Extension driver update released in
August 2022
================================================================================
===============
HotFix ID :
Installed At (UTC) : 23-02-2023 20:30:56
Title : Realtek Semiconductor Corp. - Extension - 6.0.9418.1
Client Application ID : MoUpdateOrchestrator
Description : Realtek Semiconductor Corp. Extension driver update released in
September 2022
================================================================================
===============
HotFix ID :
Installed At (UTC) : 23-02-2023 03:12:02
Title : 9NBLGGH537C2-Microsoft.XboxGameOverlay
Client Application ID : Update;ScanForUpdates
Description : 9NBLGGH537C2-1152921505690350335
================================================================================
===============
HotFix ID :
Installed At (UTC) : 23-02-2023 03:11:01
Title : 9N5TDP8VCMHS-Microsoft.WebMediaExtensions
Client Application ID : Update;ScanForUpdates
Description : 9N5TDP8VCMHS-1152921505693791332
================================================================================
===============
HotFix ID :
Installed At (UTC) : 23-02-2023 03:10:01
Title : 9NBLGGH10PG8-MICROSOFT.PEOPLE
Client Application ID : Update;ScanForUpdates
Description : 9NBLGGH10PG8-1152921505693623180
================================================================================
===============
HotFix ID :
Installed At (UTC) : 23-02-2023 03:08:27
Title : 9P7VS8XHG9G5-Microsoft.WindowsAppRuntime.1.2
Client Application ID : <<PROCESS>>: svchost.exe
Description : 9P7VS8XHG9G5-1152921505695970804
================================================================================
===============
HotFix ID :
Installed At (UTC) : 22-02-2023 11:27:29
Title : SAMSUNG Electronics Co., Ltd. - AndroidUsbDeviceClass - 2.19.1.0
Client Application ID : MoUpdateOrchestrator
Description : SAMSUNG Electronics Co., Ltd. AndroidUsbDeviceClass driver update
released in September 2022
================================================================================
===============
HotFix ID :
Installed At (UTC) : 21-02-2023 19:41:37
Title : SAMSUNG Electronics Co., Ltd. - AndroidUsbDeviceClass - 2.19.1.0
Client Application ID : MoUpdateOrchestrator
Description : SAMSUNG Electronics Co., Ltd. AndroidUsbDeviceClass driver update
released in September 2022
================================================================================
===============
HotFix ID : KB4023057
Installed At (UTC) : 20-02-2023 09:19:31
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 : KB5022845
Installed At (UTC) : 20-02-2023 09:19:28
Title : 2023-02 Cumulative Update for Windows 11 Version 22H2 for x64-based Systems
(KB5022845)
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) : 20-02-2023 09:09:55
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 :
Installed At (UTC) : 18-02-2023 11:15:58
Title : SAMSUNG Electronics Co., Ltd. - Modem - 2.19.1.0
Client Application ID : Device Driver Retrieval Client
Description : SAMSUNG Electronics Co., Ltd. Modem driver update released in
September 2022
================================================================================
==============
HotFix ID :
Installed At (UTC) : 18-02-2023 11:15:41
Title : SAMSUNG Electronics Co., Ltd. - USB - 2.19.1.0
Client Application ID : Device Driver Retrieval Client
Description : SAMSUNG Electronics Co., Ltd. USB driver update released in September
2022
================================================================================
==============
HotFix ID : KB5012170
Installed At (UTC) : 18-02-2023 07:52:13
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 :
Installed At (UTC) : 17-02-2023 23:05:03
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*

```
COMPUTERNAME: DESKTOP-SNEHA
PSExecutionPolicyPreference: Bypass
HOMEPATH: \Users\snehj
LOCALAPPDATA: C:\Users\snehj\AppData\Local
PSModulePath:
C:\Users\snehj\OneDrive\Documents\WindowsPowerShell\Modules;C:\Program
Files\WindowsPowerShell\Modules;C:\WINDOWS\system32\WindowsPowerShell\v1.0\Modules
PROCESSOR_ARCHITECTURE: AMD64
CommonProgramW6432: C:\Program Files\Common Files
CommonProgramFiles(x86): C:\Program Files (x86)\Common Files
ProgramFiles(x86): C:\Program Files (x86)
```

```
PROCESSOR_LEVEL: 6
LOGONSERVER: \\DESKTOP-SNEHA
PATHEXT: .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC;.CPL
HOMEDRIVE: C:
SystemRoot: C:\WINDOWS
MAVEN_HOME: C:\Program Files\Maven\apache-maven-3.9.0
ALLUSERSPROFILE: C:\ProgramData
DriverData: C:\Windows\System32\Drivers\DriverData
APPDATA: C:\Users\snehj\AppData\Roaming
Path: C:\Program Files\Microsoft\jdk-11.0.12.7-hotspot\bin;C:\ProgramData\Oracle\J
ava\javapath;C:\Program Files\Common Files\Oracle\Java\javapath;C:\Program Files
(x86)\Common Files\Oracle\Java\javapath;C:\Windows\system32;C:\Windows;C:\Windows\
System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Windows\System32\Open
SSH\;C:\Program Files\dotnet\;C:\Program Files\Microsoft SQL
Server\150\Tools\Binn\;C:\Program Files\nodejs\;C:\Program Files\Git\cmd;C:\WINDOW
S\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem;C:\WINDOWS\System32\WindowsPowerShe
ll\v1.0\;C:\WINDOWS\System32\OpenSSH\;C:\Program Files\Amazon\AWSCLIV2\;C:\Program
Files\Amazon\AWSCLI\bin;C:\Users\snehj\AppData\Local\Programs\Python\Python310\Sc
ripts\;C:\Users\snehj\AppData\Local\Programs\Python\Python310\;C:\Program
Files\MySQL\MySQL Shell 8.0\bin\;C:\Users\snehj\AppData\Local\Microsoft\WindowsApp
s;C:\Users\snehj\OneDrive\Documents\FlutterDev\flutter\bin;C:\Users\snehj\AppData\
Local\Programs\Microsoft VS Code\bin;C:\Users\snehj\AppData\Roaming\npm;C:\Program
Files\Maven\apache-maven-3.9.0\bin;C:\Apache24\bin;C:\MinGW\bin;C:\Windows\SysWOW6
4\;C:\Users\snehj\.dotnet\tools;C:\Users\snehj\AppData\Local\Programs\Python\Pytho
n310\Scripts\cmake.exe;C:\Users\snehj\ngrok-v3-stable-windows-amd64
(1)\ngrok.exe;C:\Program Files
(x86)\Nmap;C:\Users\snehj\AppData\Local\GitHubDesktop\bin
USERNAME: snehj
OneDrive: C:\Users\snehj\OneDrive
USERPROFILE: C:\Users\snehj
CommonProgramFiles: C:\Program Files\Common Files
OS: Windows_NT
USERDOMAIN_ROAMINGPROFILE: DESKTOP-SNEHA
PROCESSOR_IDENTIFIER: Intel64 Family 6 Model 140 Stepping 2, GenuineIntel
OneDriveConsumer: C:\Users\snehj\OneDrive
USERDOMAIN: DESKTOP-SNEHA
SystemDrive: C:
TEMP: C:\Users\snehj\AppData\Local\Temp
ProgramFiles: C:\Program Files
NUMBER_OF_PROCESSORS: 8
ComSpec: C:\WINDOWS\system32\cmd.exe
TMP: C:\Users\snehj\AppData\Local\Temp
ProgramData: C:\ProgramData
ProgramW6432: C:\Program Files
windir: C:\WINDOWS
PROCESSOR_REVISION: 8c02
PUBLIC: C:\Users\Public
ZES_ENABLE_SYSMAN: 1
```

# 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
MAVEN_HOME: C:\Program Files\Maven\apache-maven-3.9.0
NUMBER_OF_PROCESSORS: 8
OS: Windows_NT
Path: C:\Program Files\Microsoft\jdk-11.0.12.7-hotspot\bin;C:\ProgramData\Oracle\J
ava\javapath;C:\Program Files\Common Files\Oracle\Java\javapath;C:\Program Files
(x86)\Common Files\Oracle\Java\javapath;C:\Windows\system32;C:\Windows;C:\Windows\
System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Windows\System32\Open
SSH\;C:\Program Files\dotnet\;C:\Program Files\Microsoft SQL
Server\150\Tools\Binn\;C:\Program Files\nodejs\;C:\Program Files\Git\cmd;C:\WINDOW
S\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem;C:\WINDOWS\System32\WindowsPowerShe
ll\v1.0\;C:\WINDOWS\System32\OpenSSH\;C:\Program Files\Amazon\AWSCLIV2\;C:\Program
Files\Amazon\AWSCLI\bin\
PATHEXT: .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
PROCESSOR_ARCHITECTURE: AMD64
PROCESSOR_IDENTIFIER: Intel64 Family 6 Model 140 Stepping 2, GenuineIntel
PROCESSOR_LEVEL: 6
PROCESSOR_REVISION: 8c02
PSModulePath: C:\Program
Files\WindowsPowerShell\Modules;C:\WINDOWS\system32\WindowsPowerShell\v1.0\Modules
```

33

```
TEMP: C:\WINDOWS\TEMP
TMP: C:\WINDOWS\TEMP
USERNAME: SYSTEM
windir: C:\WINDOWS
ZES_ENABLE_SYSMAN: 1
```

## 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: McAfee VirusScan
ProductEXE: C:\Program Files\McAfee.com\Agent\mcupdate.exe
pathToSignedReportingExe: C:\Program Files\Common
Files\McAfee\ModuleCore\ProtectedModuleHost.exe
whitelistpaths: c:\program files\mcafee'c:\program files\common
files\mcafee'c:\program files (x86)\mcafee'c:\program files (x86)\common
files\mcafee'C:\DELL\FD09N'c:\programdata\mcafee
```

## Windows Defender configuration

```
Local Settings
Path Exclusions:
c:\program files\mcafee'c:\program files\common files\mcafee'c:\program files
(x86)\mcafee'c:\program files (x86)\common
files\mcafee'C:\DELL\FD09N'c:\programdata\mcafee
PolicyManagerPathExclusions:
c:\program files\mcafee'c:\program files\common files\mcafee'c:\program files
(x86)\mcafee'c:\program files (x86)\common
files\mcafee'C:\DELL\FD09N'c:\programdata\mcafee
Group Policy Settings
```

## 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-syste m-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\snehj\AppData\Roaming\Microsoft\Windows\PowerShell\PSRea
dLine\ConsoleHost_history.txt
PS history size: 260083B
```

## Enumerating PowerShell Session Settings using the registry

```
Name Microsoft.PowerShell
BUILTIN\Administrators AccessAllowed
NT AUTHORITY\INTERACTIVE AccessAllowed
BUILTIN\Remote Management Users AccessAllowed
================================================================================
===============
Name Microsoft.PowerShell.Workflow
BUILTIN\Administrators AccessAllowed
BUILTIN\Remote Management Users AccessAllowed
================================================================================
===============
Name Microsoft.PowerShell32
BUILTIN\Administrators AccessAllowed
NT AUTHORITY\INTERACTIVE AccessAllowed
BUILTIN\Remote Management Users AccessAllowed
================================================================================
===============
```

## HKCU Internet Settings

```
CertificateRevocation: 1
DisableCachingOfSSLPages: 0
IE5_UA_Backup_Flag: 5.0
PrivacyAdvanced: 1
SecureProtocols: 10880
User Agent: Mozilla/4.0 (compatible; MSIE 8.0; Win32)
ZonesSecurityUpgrade: System.Byte[]
WarnonZoneCrossing: 0
LockDatabase: 133211719049734484
EnableNegotiate: 1
ProxyEnable: 0
MigrateProxy: 1
```

## HKLM Internet Settings

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

## 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 : 1088
ProductType : 3
restrictanonymous : 0
restrictanonymoussam : 1
SamConnectedAccountsExist : 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 (Desktop)
Status: Unknown
Sddl: O:SYD:(A;;LCSWSDRCWDWO;;;S-1-5-21-3918106844-1363930152-1516286804-1001)(A;O
IIO;RPWPSDRCWDWO;;;S-1-5-21-3918106844-1363930152-1516286804-1001)(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 XPS Document Writer
Status: Unknown
Sddl: O:SYD:(A;;LCSWSDRCWDWO;;;S-1-5-21-3918106844-1363930152-1516286804-1000)(A;O
IIO;RPWPSDRCWDWO;;;S-1-5-21-3918106844-1363930152-1516286804-1000)(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-1-5-21-3918106844-1363930152-1516286804-1000)(A;O
IIO;RPWPSDRCWDWO;;;S-1-5-21-3918106844-1363930152-1516286804-1000)(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: Fax
Status: Unknown
Sddl: O:SYD:(A;;LCSWSDRCWDWO;;;S-1-5-21-3918106844-1363930152-1516286804-1000)(A;O
IIO;RPWPSDRCWDWO;;;S-1-5-21-3918106844-1363930152-1516286804-1000)(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
01a3cdfe-8914-45a1-9da7-afb32896dee7_UA_0 Administrators [TakeOwnership] O:BAG:SYD
:P(D;;0x1f019f;;;NU)(D;;0x1f019f;;;AN)(A;;0x1f019f;;;SY)(A;;0x1f019f;;;BA)
23771888-7c70-436c-a9db-a78daa1f914a Administrators [TakeOwnership] O:BAG:SYD:P(D;
;0x1f019f;;;NU)(D;;0x1f019f;;;AN)(A;;0x1f019f;;;SY)(A;;0x1f019f;;;BA)
2921b83a-2161-43f1-8fb1-3af405ffa5de Authenticated Users [TakeOwnership],
Administrators [TakeOwnership], Users [TakeOwnership] O:BAG:SYD:P(D;;0x1f019f;;;NU
)(D;;0x1f019f;;;AN)(A;;0x1f019f;;;AU)(A;;0x1f019f;;;SY)(A;;0x1f019f;;;BA)(A;;0x1f0
19f;;;BU)
3b16ca98-a71d-401d-907e-a48d7a5bd319_UA_0 Administrators [TakeOwnership] O:BAG:SYD
:P(D;;0x1f019f;;;NU)(D;;0x1f019f;;;AN)(A;;0x1f019f;;;SY)(A;;0x1f019f;;;BA)
3dc055d1-fb0e-4f35-8543-2afd8db9d160_UA_0 Administrators [TakeOwnership] O:BAG:SYD
:P(D;;0x1f019f;;;NU)(D;;0x1f019f;;;AN)(A;;0x1f019f;;;SY)(A;;0x1f019f;;;BA)
60389b31-53db-420d-b5dd-976da5a31d12_UA_0 Administrators [TakeOwnership] O:BAG:SYD
:P(D;;0x1f019f;;;NU)(D;;0x1f019f;;;AN)(A;;0x1f019f;;;SY)(A;;0x1f019f;;;BA)
d89d86a7-4c38-4256-aa40-42c7d8aaffeb_UA_0 Administrators [TakeOwnership] O:BAG:SYD
:P(D;;0x1f019f;;;NU)(D;;0x1f019f;;;AN)(A;;0x1f019f;;;SY)(A;;0x1f019f;;;BA)
e5d10cc6-a31e-40b7-a107-8e085dca3d19_UA_0 Administrators [TakeOwnership] O:BAG:SYD
:P(D;;0x1f019f;;;NU)(D;;0x1f019f;;;AN)(A;;0x1f019f;;;SY)(A;;0x1f019f;;;BA)
e5d10cc6-a31e-40b7-a107-8e085dca3d19_UE_UA_0 Authenticated Users [TakeOwnership],
Administrators [TakeOwnership], Users [TakeOwnership] O:BAG:SYD:P(D;;0x1f019f;;;NU
)(D;;0x1f019f;;;AN)(A;;0x1f019f;;;AU)(A;;0x1f019f;;;SY)(A;;0x1f019f;;;BA)(A;;0x1f0
19f;;;BU)
e651db2f-1d81-49fd-bdd1-de9a3e198cd1_UA_0 Administrators [TakeOwnership] O:BAG:SYD
:P(D;;0x1f019f;;;NU)(D;;0x1f019f;;;AN)(A;;0x1f019f;;;SY)(A;;0x1f019f;;;BA)
e651db2f-1d81-49fd-bdd1-de9a3e198cd1_UE_UA_0 Authenticated Users [TakeOwnership],
Administrators [TakeOwnership], Users [TakeOwnership] O:BAG:SYD:P(D;;0x1f019f;;;NU
)(D;;0x1f019f;;;AN)(A;;0x1f019f;;;AU)(A;;0x1f019f;;;SY)(A;;0x1f019f;;;BA)(A;;0x1f0
19f;;;BU)
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)
GoogleCrashServices\S-1-5-18 Administrators [AllAccess]
O:SYG:SYD:(A;;FR;;;WD)(A;;FR;;;AN)(A;;FA;;;SY)(A;;FA;;;BA)
GoogleCrashServices\S-1-5-18-x64 Administrators [AllAccess]
O:SYG:SYD:(A;;FR;;;WD)(A;;FR;;;AN)(A;;FA;;;SY)(A;;FA;;;BA)
intelSecurity_m12n_ipc_serverC7B89C6ACAEED1B150DD967AE82CD40F3952A0F8ABFC14C518227
B0E66181AB54DD9FB76E0101621285F7FB5205E0BB11F564B92AFAABA72434031354690E9A1
Everyone [AllAccess] O:BAG:SY
LOCAL\crashpad_2032_CXBINTHQYYEWTOOW snehj [AllAccess] O:S-1-5-21-3918106844-13639
30152-1516286804-1001G:S-1-5-21-3918106844-1363930152-1516286804-1001D:(A;;FA;;;SY
)(A;;FA;;;S-1-5-21-3918106844-1363930152-1516286804-1001)(A;;0x12019f;;;AC)
LOCAL\mojo.external_task_manager_33420 Administrators [AllAccess] O:S-1-5-21-39181
06844-1363930152-1516286804-1001G:S-1-5-21-3918106844-1363930152-1516286804-1001D:
(A;;FA;;;OW)(A;;FA;;;SY)(A;;FA;;;BA)
LOCAL\S-1-5-5-0-1985173-Teams-2.0-instance-pipe Administrators [AllAccess], snehj
[AllAccess] O:S-1-5-21-3918106844-1363930152-1516286804-1001G:S-1-5-21-3918106844-
1363930152-1516286804-1001D:(A;;FR;;;WD)(A;;FR;;;AN)(A;;FA;;;SY)(A;;FA;;;BA)(A;;FA
;;;S-1-5-21-3918106844-1363930152-1516286804-1001)
ROUTER Everyone [WriteData/CreateFiles]
O:SYG:SYD:P(A;;0x12019b;;;WD)(A;;0x12019b;;;AN)(A;;FA;;;SY)
```

```
Winsock2\CatalogChangeListener-314-0 Administrators [WriteData/CreateFiles]
O:BAG:SYD:(D;;FW;;;NU)(A;;0x120196;;;SY)(A;;0x120196;;;BA)
Winsock2\CatalogChangeListener-428-0 Administrators [WriteData/CreateFiles]
O:BAG:SYD:(D;;FW;;;NU)(A;;0x120196;;;SY)(A;;0x120196;;;BA)
Winsock2\CatalogChangeListener-440-0 Administrators [WriteData/CreateFiles]
O:BAG:SYD:(D;;FW;;;NU)(A;;0x120196;;;SY)(A;;0x120196;;;BA)
Winsock2\CatalogChangeListener-5b0-0 Administrators [WriteData/CreateFiles]
O:NSG:NSD:(D;;FW;;;NU)(A;;0x120196;;;SY)(A;;0x120196;;;BA)
Winsock2\CatalogChangeListener-5ec-0 Administrators [WriteData/CreateFiles]
O:SYG:SYD:(D;;FW;;;NU)(A;;0x120196;;;SY)(A;;0x120196;;;BA)
Winsock2\CatalogChangeListener-a10-0 Administrators [WriteData/CreateFiles]
O:LSG:LSD:(D;;FW;;;NU)(A;;0x120196;;;SY)(A;;0x120196;;;BA)
Winsock2\CatalogChangeListener-b94-0 Administrators [WriteData/CreateFiles]
O:SYG:SYD:(D;;FW;;;NU)(A;;0x120196;;;SY)(A;;0x120196;;;BA)
Winsock2\CatalogChangeListener-da4-0 Administrators [WriteData/CreateFiles]
O:SYG:SYD:(D;;FW;;;NU)(A;;0x120196;;;SY)(A;;0x120196;;;BA)
```

## Enumerating AMSI registered providers

```
Provider: {E6CF50BC-485D-41DE-A703-14D3E95C0146}
Path: "C:\Program Files\McAfee\MfeAV\AMSIExt.dll"
================================================================================
===============
```

## Enumerating Sysmon configuration

```
Installed: False
Hashing Algorithm: Not Defined
Options: Not Defined
Rules:
================================================================================
===============
```

## Installed .NET versions

```
CLR Versions
4.0.30319
.NET Versions
4.8.09032
.NET & AMSI (Anti-Malware Scan Interface) support
.NET version supports AMSI : True
OS supports AMSI : True
[!] The highest .NET version is enrolled in AMSI!
```

# Interesting Events information

## Printing Explicit Credential Events (4648) for last 30 days - A process logged on using plaintext credentials

```
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 23-07-2023 03:19:14
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
```

```
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 23-07-2023 03:19:14
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 22-07-2023 10:54:48
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 22-07-2023 10:54:48
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 22-07-2023 08:21:01
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 22-07-2023 08:21:01
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 22-07-2023 07:04:52
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 22-07-2023 07:04:52
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 22-07-2023 07:00:39
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 22-07-2023 07:00:39
```

```
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 22-07-2023 06:17:32
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 22-07-2023 06:17:32
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 22-07-2023 05:36:13
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 22-07-2023 05:36:13
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 22-07-2023 05:24:21
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 22-07-2023 05:24:21
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 22-07-2023 05:20:22
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 22-07-2023 05:20:22
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
```

```
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 22-07-2023 05:15:14
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 22-07-2023 05:15:14
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 22-07-2023 05:05:57
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 22-07-2023 05:05:57
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 22-07-2023 05:01:40
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 22-07-2023 05:01:40
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 22-07-2023 04:56:39
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 22-07-2023 04:56:39
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 22-07-2023 04:51:32
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
```

```
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 22-07-2023 04:51:32
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 22-07-2023 04:40:32
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 22-07-2023 04:40:32
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 22-07-2023 04:30:24
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 22-07-2023 04:30:24
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 22-07-2023 04:05:09
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 22-07-2023 04:05:09
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 22-07-2023 03:39:28
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 22-07-2023 03:39:28
```

```
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
=======================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 21-07-2023 15:15:26
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
=======================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 21-07-2023 15:15:26
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
=======================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 21-07-2023 15:03:47
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
=======================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 21-07-2023 15:03:47
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
=======================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 21-07-2023 09:30:50
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
=======================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 21-07-2023 09:30:50
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
=======================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 21-07-2023 08:57:14
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
=======================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 21-07-2023 08:57:14
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
=======================================================================================
===============
```

```
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 21-07-2023 08:47:45
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 21-07-2023 08:47:45
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 21-07-2023 08:25:13
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 21-07-2023 08:25:13
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 21-07-2023 08:05:33
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 21-07-2023 08:05:32
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 21-07-2023 06:39:28
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 21-07-2023 06:39:28
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 20-07-2023 16:10:31
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
```

```
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 20-07-2023 16:10:31
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 20-07-2023 15:04:45
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 20-07-2023 15:04:45
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 20-07-2023 13:06:18
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 20-07-2023 13:06:18
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 20-07-2023 09:28:44
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 20-07-2023 09:28:44
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 20-07-2023 09:02:40
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 20-07-2023 09:02:40
```

```
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 20-07-2023 08:31:13
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 20-07-2023 08:31:13
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 20-07-2023 08:04:03
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 20-07-2023 08:04:03
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 20-07-2023 07:23:50
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 20-07-2023 07:23:49
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 20-07-2023 06:53:19
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 20-07-2023 06:53:19
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
```

```
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 20-07-2023 06:19:22
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 20-07-2023 06:19:22
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 20-07-2023 03:42:31
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 20-07-2023 03:42:30
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 20-07-2023 03:32:36
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 20-07-2023 03:32:36
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 19-07-2023 16:57:42
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 19-07-2023 16:57:42
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 19-07-2023 15:03:07
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
```

```
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 19-07-2023 15:03:07
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 19-07-2023 05:58:11
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 19-07-2023 05:58:11
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 18-07-2023 15:11:04
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 18-07-2023 15:11:04
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 18-07-2023 10:17:30
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 18-07-2023 10:17:30
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 18-07-2023 10:10:43
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 18-07-2023 10:10:43
```

```
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 18-07-2023 08:12:58
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 18-07-2023 08:12:58
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 18-07-2023 06:44:34
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 18-07-2023 06:44:34
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 18-07-2023 04:49:58
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 18-07-2023 04:49:58
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 18-07-2023 04:11:47
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 18-07-2023 04:11:47
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
```

```
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 18-07-2023 04:06:14
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 18-07-2023 04:06:14
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 18-07-2023 03:52:54
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 18-07-2023 03:52:54
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 18-07-2023 03:43:36
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 18-07-2023 03:43:36
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 17-07-2023 16:51:36
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 17-07-2023 16:51:35
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 17-07-2023 16:32:03
IP Address : -
Process : C:\Windows\System32\lsass.exe
Target User : snehjanarthanan@outlook.com
```

```
Target Domain : MicrosoftAccount
================================================================================
===============
Subject User : DESKTOP-SNEHA$
Subject Domain : WORKGROUP
Created (UTC) : 17-07-2023 16:32:03
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : snehjanarthanan@outlook.com
Target Domain : MicrosoftAccount
================================================================================
===============
```

## Printing Account Logon Events (4624) for the last 10 days.

```
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 23-07-2023 03:19:14
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 23-07-2023 03:19:14
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 23-07-2023 03:19:14
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 23-07-2023 03:19:14
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 10:54:48
IP Address : -
Authentication Package : Negotiate
Lm Package :
```

```
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 10:54:48
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 10:54:48
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 10:54:48
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 08:21:01
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 08:21:01
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 08:21:01
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
```

```
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 08:21:01
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 07:04:52
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 07:04:52
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 07:04:52
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 07:04:52
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 07:00:39
IP Address : -
Authentication Package : Negotiate
Lm Package :
```

```
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 07:00:39
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 07:00:39
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 07:00:39
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 06:17:32
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 06:17:32
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 06:17:32
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
```

```
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 06:17:32
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 05:36:13
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 05:36:13
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 05:36:13
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 05:36:13
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 05:24:21
IP Address : -
Authentication Package : Negotiate
Lm Package :
```

```
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 05:24:21
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 05:24:21
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 05:24:21
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 05:20:22
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 05:20:22
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 05:20:22
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
```

```
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
====================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 05:20:22
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
====================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 05:15:14
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
====================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 05:15:14
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
====================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 05:15:14
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
====================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 05:15:14
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
====================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 05:05:57
IP Address : -
Authentication Package : Negotiate
Lm Package :
```

```
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 05:05:57
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 05:05:57
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 05:05:57
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 05:01:40
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 05:01:40
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 05:01:40
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
```

```
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 05:01:40
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 04:56:39
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 04:56:39
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 04:56:39
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 04:56:39
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 04:51:32
IP Address : -
Authentication Package : Negotiate
Lm Package :
```

```
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 04:51:32
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 04:51:32
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 04:51:32
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 04:40:32
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 04:40:32
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 04:40:32
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
```

```
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
=================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 04:40:32
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
=================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 04:30:24
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
=================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 04:30:24
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
=================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 04:30:24
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
=================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 04:30:24
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
=================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 04:05:09
IP Address : -
Authentication Package : Negotiate
Lm Package :
```

```
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 04:05:09
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 04:05:09
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 04:05:09
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 03:39:28
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 03:39:28
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 03:39:28
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
```

```
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 22-07-2023 03:39:28
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 21-07-2023 15:15:26
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 21-07-2023 15:15:26
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 21-07-2023 15:15:26
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 21-07-2023 15:15:26
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 21-07-2023 15:03:47
IP Address : -
Authentication Package : Negotiate
Lm Package :
```

```
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 21-07-2023 15:03:47
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 21-07-2023 15:03:47
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 21-07-2023 15:03:47
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 21-07-2023 09:30:50
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 21-07-2023 09:30:50
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 21-07-2023 09:30:50
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
```

```
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 21-07-2023 09:30:50
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 21-07-2023 08:57:14
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 21-07-2023 08:57:14
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 21-07-2023 08:57:14
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 21-07-2023 08:57:14
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 21-07-2023 08:47:45
IP Address : -
Authentication Package : Negotiate
Lm Package :
```

```
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 21-07-2023 08:47:45
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 21-07-2023 08:47:45
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 21-07-2023 08:47:45
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 21-07-2023 08:25:13
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 21-07-2023 08:25:13
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 21-07-2023 08:25:13
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
```

```
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 21-07-2023 08:25:13
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 21-07-2023 08:05:33
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 21-07-2023 08:05:33
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 21-07-2023 08:05:32
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 21-07-2023 08:05:32
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 21-07-2023 06:39:28
IP Address : -
Authentication Package : Negotiate
Lm Package :
```

```
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 21-07-2023 06:39:28
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 21-07-2023 06:39:28
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 21-07-2023 06:39:28
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 20-07-2023 16:10:31
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 20-07-2023 16:10:31
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 20-07-2023 16:10:31
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
```

```
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 20-07-2023 16:10:31
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 20-07-2023 15:04:45
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 20-07-2023 15:04:45
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 20-07-2023 15:04:45
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 20-07-2023 15:04:45
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 20-07-2023 13:06:18
IP Address : -
Authentication Package : Negotiate
Lm Package :
```

```
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 20-07-2023 13:06:18
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 20-07-2023 13:06:18
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 20-07-2023 13:06:18
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 20-07-2023 09:28:44
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 20-07-2023 09:28:44
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 20-07-2023 09:28:44
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
```

```
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 20-07-2023 09:28:44
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 20-07-2023 09:02:40
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 20-07-2023 09:02:40
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 20-07-2023 09:02:40
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 20-07-2023 09:02:40
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 20-07-2023 08:31:13
IP Address : -
Authentication Package : Negotiate
Lm Package :
```

```
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 20-07-2023 08:31:13
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 20-07-2023 08:31:13
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 20-07-2023 08:31:13
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 20-07-2023 08:04:03
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 20-07-2023 08:04:03
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 20-07-2023 08:04:03
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
```

```
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 20-07-2023 08:04:03
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 20-07-2023 07:23:50
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 20-07-2023 07:23:50
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 20-07-2023 07:23:49
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 20-07-2023 07:23:49
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 20-07-2023 06:53:19
IP Address : -
Authentication Package : Negotiate
Lm Package :
```

```
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 20-07-2023 06:53:19
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 20-07-2023 06:53:19
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 20-07-2023 06:53:19
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 20-07-2023 06:19:22
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 20-07-2023 06:19:22
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 20-07-2023 06:19:22
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
```

```
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
===============================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 20-07-2023 06:19:22
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
===============================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 20-07-2023 03:42:31
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
===============================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 20-07-2023 03:42:31
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
===============================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 20-07-2023 03:42:30
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
===============================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 20-07-2023 03:42:30
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
===============================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 20-07-2023 03:32:36
IP Address : -
Authentication Package : Negotiate
Lm Package :
```

```
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 20-07-2023 03:32:36
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 20-07-2023 03:32:36
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 20-07-2023 03:32:36
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 19-07-2023 16:57:42
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 19-07-2023 16:57:42
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 19-07-2023 16:57:42
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
```

```
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 19-07-2023 16:57:42
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 19-07-2023 15:03:07
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 19-07-2023 15:03:07
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 19-07-2023 15:03:07
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 19-07-2023 15:03:07
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 19-07-2023 05:58:11
IP Address : -
Authentication Package : Negotiate
Lm Package :
```

```
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 19-07-2023 05:58:11
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 19-07-2023 05:58:11
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 19-07-2023 05:58:11
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 18-07-2023 15:11:04
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 18-07-2023 15:11:04
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 18-07-2023 15:11:04
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
```

```
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 18-07-2023 15:11:04
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 18-07-2023 10:17:30
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 18-07-2023 10:17:30
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 18-07-2023 10:17:30
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 18-07-2023 10:17:30
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 18-07-2023 10:10:43
IP Address : -
Authentication Package : Negotiate
Lm Package :
```

```
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 18-07-2023 10:10:43
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 18-07-2023 10:10:43
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 18-07-2023 10:10:43
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 18-07-2023 08:12:58
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 18-07-2023 08:12:58
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 18-07-2023 08:12:58
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
```

```
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 18-07-2023 08:12:58
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 18-07-2023 06:44:34
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 18-07-2023 06:44:34
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 18-07-2023 06:44:34
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 18-07-2023 06:44:34
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 18-07-2023 04:49:58
IP Address : -
Authentication Package : Negotiate
Lm Package :
```

```
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 18-07-2023 04:49:58
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 18-07-2023 04:49:58
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 18-07-2023 04:49:58
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 18-07-2023 04:11:47
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 18-07-2023 04:11:47
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 18-07-2023 04:11:47
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
```

```
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
==============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 18-07-2023 04:11:47
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
==============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 18-07-2023 04:06:14
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
==============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 18-07-2023 04:06:14
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
==============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 18-07-2023 04:06:14
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
==============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 18-07-2023 04:06:14
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
==============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 18-07-2023 03:52:54
IP Address : -
Authentication Package : Negotiate
Lm Package :
```

```
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 18-07-2023 03:52:54
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 18-07-2023 03:52:54
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 18-07-2023 03:52:54
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 18-07-2023 03:43:36
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 18-07-2023 03:43:36
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 18-07-2023 03:43:36
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
```

```
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
=================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 18-07-2023 03:43:36
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
=================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 17-07-2023 16:51:36
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
=================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 17-07-2023 16:51:36
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
=================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 17-07-2023 16:51:35
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
=================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 17-07-2023 16:51:35
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
=================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 17-07-2023 16:32:03
IP Address : -
Authentication Package : Negotiate
Lm Package :
```

```
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 17-07-2023 16:32:03
IP Address : -
Authentication Package : Negotiate
Lm Package :
Logon Type : Unlock
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 17-07-2023 16:32:03
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
Subject User Name : DESKTOP-SNEHA$
Subject Domain Name : WORKGROUP
Created (Utc) : 17-07-2023 16:32:03
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :
Logon Type : CachedInteractive
Target User Name : snehjanarthanan@outlook.com
Target Domain Name : MicrosoftAccount
Target Outbound User Name : -
Target Outbound Domain Name : -
================================================================================
===============
```

## Displaying Power off/on events for last 5 days

```
23-07-2023 08:47:09 : Awake
23-07-2023 00:22:50 : Sleep
22-07-2023 09:09:26 : Awake
22-07-2023 05:30:04 : Sleep
21-07-2023 12:08:19 : Awake
21-07-2023 06:49:35 : Sleep
20-07-2023 09:02:33 : Awake
20-07-2023 06:00:22 : Sleep
19-07-2023 20:21:04 : Awake
19-07-2023 19:46:58 : Sleep
19-07-2023 11:27:55 : Awake
19-07-2023 04:25:23 : Sleep
```

# 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: snehj
Current groups: Everyone, Local account and member of Administrators group,
Administrators, Users, Interactive, Console Logon, Authenticated Users, This
Organization, snehjanarthanan@outlook.com, Local account, Local, Cloud Account
Authentication
================================================================================
===============
DESKTOP-SNEHA\Administrator(Disabled): Built-in account for administering the
computer/domain
|->Groups: Administrators
|->Password: CanChange-NotExpi-Req
DESKTOP-SNEHA\DefaultAccount(Disabled): A user account managed by the system.
|->Groups: System Managed Accounts Group
|->Password: CanChange-NotExpi-NotReq
DESKTOP-SNEHA\Guest(Disabled): Built-in account for guest access to the
computer/domain
|->Groups: Guests
|->Password: NotChange-NotExpi-NotReq
DESKTOP-SNEHA\snehj
|->Groups: Administrators,Users
|->Password: CanChange-NotExpi-Req
DESKTOP-SNEHA\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 : DESKTOP-SNEHA\snehj
Idle Time : 00h:00m:00s:000ms
```

## 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*

```
SeIncreaseQuotaPrivilege: DISABLED
SeSecurityPrivilege: DISABLED
SeTakeOwnershipPrivilege: DISABLED
SeLoadDriverPrivilege: DISABLED
SeSystemProfilePrivilege: DISABLED
SeSystemtimePrivilege: DISABLED
SeProfileSingleProcessPrivilege: DISABLED
SeIncreaseBasePriorityPrivilege: DISABLED
SeCreatePagefilePrivilege: DISABLED
SeBackupPrivilege: DISABLED
SeRestorePrivilege: DISABLED
SeShutdownPrivilege: DISABLED
SeDebugPrivilege: SE_PRIVILEGE_ENABLED
SeSystemEnvironmentPrivilege: DISABLED
SeChangeNotifyPrivilege: SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED
SeRemoteShutdownPrivilege: DISABLED
SeUndockPrivilege: DISABLED
SeManageVolumePrivilege: DISABLED
SeImpersonatePrivilege: SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED
SeCreateGlobalPrivilege: SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED
SeIncreaseWorkingSetPrivilege: DISABLED
SeTimeZonePrivilege: DISABLED
SeCreateSymbolicLinkPrivilege: DISABLED
SeDelegateSessionUserImpersonatePrivilege: DISABLED
```

## Display information about local users

```
Computer Name : DESKTOP-SNEHA
User Name : Administrator
User Id : 500
Is Enabled : False
User Type : Administrator
Comment : Built-in account for administering the computer/domain
Last Logon : 07-11-2021 16:52:42
Logons Count : 13
Password Last Set : 01-01-1970 00:00:00
===================================================================================
===============
Computer Name : DESKTOP-SNEHA
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 : DESKTOP-SNEHA
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 : DESKTOP-SNEHA
User Name : snehj
User Id : 1001
Is Enabled : True
User Type : Administrator
Comment :
Last Logon : 01-01-1970 00:00:00
Logons Count : 0
Password Last Set : 29-01-2022 19:32:35
===================================================================================
===============
Computer Name : DESKTOP-SNEHA
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 : 05-10-2021 09:16:02
===================================================================================
===============
```

## RDP Sessions

```
SessID pSessionName pUserName pDomainName State SourceIP
1 Console snehj DESKTOP-SNEHA Active
```

## Home folders found

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

## Looking for AutoLogon credentials

```
Some AutoLogon credentials were found
DefaultDomainName : .
DefaultUserName : snehj
```

## 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: DESKTOP-SNEHA
SID: S-1-5-21-3918106844-1363930152-1516286804
MaxPasswordAge: 42.00:00:00
MinPasswordAge: 00:00:00
MinPasswordLength: 0
PasswordHistoryLength: 0
PasswordProperties: 0
===============================================================================
===============
```

## Print Logon Sessions

```
Method: LSA
Logon Server:
Logon Server Dns Domain:
Logon Id: 1989927
Logon Time: 17-07-2023 16:32:03
Logon Type: Interactive
Start Time:
Domain: DESKTOP-SNEHA
Authentication Package: CloudAP
Start Time:
User Name: snehj
User Principal Name:
User SID: S-1-5-21-3918106844-1363930152-1516286804-1001
===============================================================================
===============
Method: LSA
Logon Server:
Logon Server Dns Domain:
Logon Id: 1989853
Logon Time: 17-07-2023 16:32:03
Logon Type: Interactive
Start Time:
Domain: DESKTOP-SNEHA
Authentication Package: CloudAP
Start Time:
User Name: snehj
User Principal Name:
User SID: S-1-5-21-3918106844-1363930152-1516286804-1001
===============================================================================
===============
Method: LSA
Logon Server:
Logon Server Dns Domain:
Logon Id: 131765
```

```
Logon Time: 17-07-2023 16:30:22
Logon Type: Interactive
Start Time:
Domain: Window Manager
Authentication Package: Negotiate
Start Time:
User Name: DWM-1
User Principal Name:
User SID: S-1-5-90-0-1
================================================================================
===============
Method: LSA
Logon Server:
Logon Server Dns Domain:
Logon Id: 131710
Logon Time: 17-07-2023 16:30:22
Logon Type: Interactive
Start Time:
Domain: Window Manager
Authentication Package: Negotiate
Start Time:
User Name: DWM-1
User Principal Name:
User SID: S-1-5-90-0-1
================================================================================
===============
Method: LSA
Logon Server:
Logon Server Dns Domain:
Logon Id: 996
Logon Time: 17-07-2023 16:30:22
Logon Type: Service
Start Time:
Domain: WORKGROUP
Authentication Package: Negotiate
Start Time:
User Name: DESKTOP-SNEHA$
User Principal Name:
User SID: S-1-5-20
================================================================================
===============
Method: LSA
Logon Server:
Logon Server Dns Domain:
Logon Id: 997
Logon Time: 17-07-2023 16:30:22
Logon Type: Service
Start Time:
Domain: NT AUTHORITY
Authentication Package: Negotiate
Start Time:
User Name: LOCAL SERVICE
User Principal Name:
User SID: S-1-5-19
================================================================================
===============
Method: LSA
Logon Server:
Logon Server Dns Domain:
Logon Id: 93483
Logon Time: 17-07-2023 16:30:22
Logon Type: Interactive
Start Time:
Domain: Font Driver Host
Authentication Package: Negotiate
Start Time:
User Name: UMFD-0
User Principal Name:
User SID: S-1-5-96-0-0
================================================================================
===============
Method: LSA
Logon Server:
Logon Server Dns Domain:
Logon Id: 93455
Logon Time: 17-07-2023 16:30:22
Logon Type: Interactive
Start Time:
```

```
Domain: Font Driver Host
Authentication Package: Negotiate
Start Time:
User Name: UMFD-1
User Principal Name:
User SID: S-1-5-96-0-1
================================================================================
==============
Method: LSA
Logon Server:
Logon Server Dns Domain:
Logon Id: 999
Logon Time: 17-07-2023 16:30:21
Logon Type: 0
Start Time:
Domain: WORKGROUP
Authentication Package: NTLM
Start Time:
User Name: DESKTOP-SNEHA$
User Principal Name:
User SID: S-1-5-18
================================================================================
==============
```

# Processes Information

## Vulnerable Leaked Handlers

```
Handle: 2016(key)
Handle Owner: Pid is 7408(RuntimeBroker) with owner: snehj
Reason: TakeOwnership
Registry: HKLM\software\classes\launcher.allappsdesktopapplication
================================================================================
==============
Handle: 7320(file)
Handle Owner: Pid is 30640(chrome) with owner: snehj
Reason: AppendData/CreateDirectories
File Path: \Users\snehj\AppData\Local\Google\Chrome\User Data\Profile 8\Sync
Data\LevelDB\MANIFEST-000178
File Owner: BUILTIN\Administrators
================================================================================
==============
Handle: 220(file)
Handle Owner: Pid is 26304(powershell) with owner: snehj
Reason: WriteData/CreateFiles
File Path: \Users\snehj\Downloads\peasout.txt
File Owner: BUILTIN\Administrators
================================================================================
==============
Handle: 2224(key)
Handle Owner: Pid is 8664(winPEASx64) with owner: snehj
Reason: AllAccess
Registry: HKLM\software\microsoft\windowsruntime\server
================================================================================
==============
Handle: 2392(key)
Handle Owner: Pid is 8664(winPEASx64) with owner: snehj
Reason: TakeOwnership
Registry:
HKLM\software\classes\clsid\{dffacdc5-679f-4156-8947-c5c76bc0b67f}\instance
================================================================================
==============
Handle: 2016(key)
Handle Owner: Pid is 7408(RuntimeBroker) with owner: snehj
Reason: TakeOwnership
Registry: HKLM\software\classes\launcher.allappsdesktopapplication
================================================================================
```

```
===============
Handle: 7320(file)
Handle Owner: Pid is 30640(chrome) with owner: snehj
Reason: AppendData/CreateDirectories
File Path: \Users\snehj\AppData\Local\Google\Chrome\User Data\Profile 8\Sync
Data\LevelDB\MANIFEST-000178
File Owner: BUILTIN\Administrators
================================================================================
===============
Handle: 220(file)
Handle Owner: Pid is 26304(powershell) with owner: snehj
Reason: WriteData/CreateFiles
File Path: \Users\snehj\Downloads\peasout.txt
File Owner: BUILTIN\Administrators
================================================================================
===============
Handle: 2224(key)
Handle Owner: Pid is 8664(winPEASx64) with owner: snehj
Reason: AllAccess
Registry: HKLM\software\microsoft\windowsruntime\server
================================================================================
===============
Handle: 2392(key)
Handle Owner: Pid is 8664(winPEASx64) with owner: snehj
Reason: TakeOwnership
Registry:
HKLM\software\classes\clsid\{dffacdc5-679f-4156-8947-c5c76bc0b67f}\instance
================================================================================
===============
Handle: 2016(key)
Handle Owner: Pid is 7408(RuntimeBroker) with owner: snehj
Reason: TakeOwnership
Registry: HKLM\software\classes\launcher.allappsdesktopapplication
================================================================================
===============
Handle: 7320(file)
Handle Owner: Pid is 30640(chrome) with owner: snehj
Reason: AppendData/CreateDirectories
File Path: \Users\snehj\AppData\Local\Google\Chrome\User Data\Profile 8\Sync
Data\LevelDB\MANIFEST-000178
File Owner: BUILTIN\Administrators
================================================================================
===============
Handle: 220(file)
Handle Owner: Pid is 26304(powershell) with owner: snehj
Reason: WriteData/CreateFiles
File Path: \Users\snehj\Downloads\peasout.txt
File Owner: BUILTIN\Administrators
================================================================================
===============
Handle: 2224(key)
Handle Owner: Pid is 8664(winPEASx64) with owner: snehj
Reason: AllAccess
Registry: HKLM\software\microsoft\windowsruntime\server
================================================================================
===============
Handle: 2392(key)
Handle Owner: Pid is 8664(winPEASx64) with owner: snehj
Reason: TakeOwnership
Registry:
HKLM\software\classes\clsid\{dffacdc5-679f-4156-8947-c5c76bc0b67f}\instance
================================================================================
===============
Handle: 2016(key)
Handle Owner: Pid is 7408(RuntimeBroker) with owner: snehj
Reason: TakeOwnership
Registry: HKLM\software\classes\launcher.allappsdesktopapplication
================================================================================
===============
Handle: 7320(file)
Handle Owner: Pid is 30640(chrome) with owner: snehj
Reason: AppendData/CreateDirectories
File Path: \Users\snehj\AppData\Local\Google\Chrome\User Data\Profile 8\Sync
Data\LevelDB\MANIFEST-000178
File Owner: BUILTIN\Administrators
================================================================================
===============
Handle: 220(file)
Handle Owner: Pid is 26304(powershell) with owner: snehj
```

```
Reason: WriteData/CreateFiles
File Path: \Users\snehj\Downloads\peasout.txt
File Owner: BUILTIN\Administrators
=================================================================================
==============
Handle: 2224(key)
Handle Owner: Pid is 8664(winPEASx64) with owner: snehj
Reason: AllAccess
Registry: HKLM\software\microsoft\windowsruntime\server
=================================================================================
==============
Handle: 2392(key)
Handle Owner: Pid is 8664(winPEASx64) with owner: snehj
Reason: TakeOwnership
Registry:
HKLM\software\classes\clsid\{dffacdc5-679f-4156-8947-c5c76bc0b67f}\instance
=================================================================================
==============
Handle: 2016(key)
Handle Owner: Pid is 7408(RuntimeBroker) with owner: snehj
Reason: TakeOwnership
Registry: HKLM\software\classes\launcher.allappsdesktopapplication
=================================================================================
==============
Handle: 7320(file)
Handle Owner: Pid is 30640(chrome) with owner: snehj
Reason: AppendData/CreateDirectories
File Path: \Users\snehj\AppData\Local\Google\Chrome\User Data\Profile 8\Sync
Data\LevelDB\MANIFEST-000178
File Owner: BUILTIN\Administrators
=================================================================================
==============
Handle: 220(file)
Handle Owner: Pid is 26304(powershell) with owner: snehj
Reason: WriteData/CreateFiles
File Path: \Users\snehj\Downloads\peasout.txt
File Owner: BUILTIN\Administrators
=================================================================================
==============
Handle: 2224(key)
Handle Owner: Pid is 8664(winPEASx64) with owner: snehj
Reason: AllAccess
Registry: HKLM\software\microsoft\windowsruntime\server
=================================================================================
==============
Handle: 2392(key)
Handle Owner: Pid is 8664(winPEASx64) with owner: snehj
Reason: TakeOwnership
Registry:
HKLM\software\classes\clsid\{dffacdc5-679f-4156-8947-c5c76bc0b67f}\instance
=================================================================================
==============
```

# 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*

```
Apache2.4(Apache2.4)["C:\Apache\Apache24\bin\httpd.exe" -k runservice] - Auto -
Stopped
YOU CAN MODIFY THIS SERVICE: AllAccess
Apache/2.4.55 (Win64)
=================================================================================
==============
cplspcon(Intel Corporation - Intel(R) Content Protection HDCP Service)[C:\WINDOWS\
System32\DriverStore\FileRepository\iigd_dch.inf_amd64_8a4323c80a901a5c\IntelCpHDC
```

```
PSvc.exe] - Auto - Running
YOU CAN MODIFY THIS SERVICE: AllAccess
Intel(R) Content Protection HDCP Service - enables communication with Content
Protection HDCP HW
================================================================================
===============
dcpm-notify(Dell Inc. - Dell Command | Power Manager Notify)["C:\Program
Files\Dell\CommandPowerManager\NotifyService.exe"] - Manual - Stopped - isDotNet
YOU CAN MODIFY THIS SERVICE: AllAccess
File Permissions: Administrators [AllAccess]
Possible DLL Hijacking in binary folder: C:\Program Files\Dell\CommandPowerManager
(Administrators [AllAccess])
================================================================================
===============
DDVCollectorSvcApi(Dell Technologies Inc. - Dell Data Vault Service
API)["C:\Program Files\Dell\DellDataVault\DDVCollectorSvcApi.exe"] - Auto - Running
YOU CAN MODIFY THIS SERVICE: AllAccess
File Permissions: Administrators [AllAccess]
Possible DLL Hijacking in binary folder: C:\Program Files\Dell\DellDataVault
(Administrators [AllAccess])
Dell Data Vault Service API exposes a COM API for working with the DDV services
================================================================================
===============
DDVDataCollector(Dell Technologies Inc. - Dell Data Vault Collector)["C:\Program
Files\Dell\DellDataVault\DDVDataCollector.exe"] - Auto - Running
YOU CAN MODIFY THIS SERVICE: AllAccess
File Permissions: Administrators [AllAccess]
Possible DLL Hijacking in binary folder: C:\Program Files\Dell\DellDataVault
(Administrators [AllAccess])
DDV Collector service gathers system information and stores it for later use
================================================================================
===============
DDVRulesProcessor(Dell Technologies Inc. - Dell Data Vault Processor)["C:\Program
Files\Dell\DellDataVault\DDVRulesProcessor.exe"] - Auto - Running
YOU CAN MODIFY THIS SERVICE: AllAccess
File Permissions: Administrators [AllAccess]
Possible DLL Hijacking in binary folder: C:\Program Files\Dell\DellDataVault
(Administrators [AllAccess])
DDV Rules Processor generates alerts based on data collected by DDV Collector
service
================================================================================
===============
Dell Digital Delivery Services(Dell Digital Delivery Services)["C:\Program Files
(x86)\Dell Digital Delivery Services\Dell.D3.WinSvc.exe"] - Auto - Running -
isDotNet
YOU CAN MODIFY THIS SERVICE: AllAccess
Possible DLL Hijacking in binary folder: C:\Program Files (x86)\Dell Digital
Delivery Services (Administrators [AllAccess])
Downloads and installs the applications that you purchased with your computer
================================================================================
===============
Dell SupportAssist Remediation(Dell INC. - Dell SupportAssist
Remediation)["C:\Program
Files\Dell\SARemediation\agent\DellSupportAssistRemedationService.exe"] - Auto -
Running - isDotNet
YOU CAN MODIFY THIS SERVICE: AllAccess
File Permissions: Administrators [AllAccess]
Possible DLL Hijacking in binary folder: C:\Program Files\Dell\SARemediation\agent
(Administrators [AllAccess])
Dell SupportAssist Remediation Service
================================================================================
===============
DellClientManagementService(Dell Client Management Service)["C:\Program Files
(x86)\Dell\UpdateService\ServiceShell.exe"] - Auto - Running - isDotNet
YOU CAN MODIFY THIS SERVICE: AllAccess
File Permissions: Administrators [AllAccess]
Possible DLL Hijacking in binary folder: C:\Program Files (x86)\Dell\UpdateService
(Administrators [AllAccess])
Enables Dell applications to manage Dell specific features of the system. If this
service is stopped, any services that explicitly depend on it will cause this
service to be restarted. If this service is disabled, any services that explicitly
depend on it will fail to function.
================================================================================
===============
DellTechHub(Dell - Dell TechHub)["C:\Program Files\Dell\TechHub\Dell.TechHub.exe"]
- Auto - Running
YOU CAN MODIFY THIS SERVICE: AllAccess
Possible DLL Hijacking in binary folder: C:\Program Files\Dell\TechHub
(Administrators [AllAccess])
```

Foundational service managing Dell applications through Dell TechHub
=============================================================================
==============
esifsvc(Intel Corporation - Intel(R) Dynamic Tuning service)["C:\WINDOWS\System32\
DriverStore\FileRepository\dptf_cpu.inf_amd64_1da48d5885266bb7\esif_uf.exe"] - Auto
- Running
YOU CAN MODIFY THIS SERVICE: AllAccess
Intel(R) Dynamic Tuning service
=============================================================================
==============
GoogleChromeElevationService(Google LLC - Google Chrome Elevation Service
(GoogleChromeElevationService))["C:\Program
Files\Google\Chrome\Application\114.0.5735.248\elevation_service.exe"] - Manual -
Stopped
YOU CAN MODIFY THIS SERVICE: AllAccess
Possible DLL Hijacking in binary folder: C:\Program
Files\Google\Chrome\Application\114.0.5735.248 (Administrators [AllAccess])
=============================================================================
==============
gupdate(Google LLC - Google Update Service (gupdate))["C:\Program Files
(x86)\Google\Update\GoogleUpdate.exe" /svc] - Auto - Stopped
YOU CAN MODIFY THIS SERVICE: AllAccess
File Permissions: Administrators [AllAccess]
Possible DLL Hijacking in binary folder: C:\Program Files (x86)\Google\Update
(Administrators [AllAccess])
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
YOU CAN MODIFY THIS SERVICE: AllAccess
File Permissions: Administrators [AllAccess]
Possible DLL Hijacking in binary folder: C:\Program Files (x86)\Google\Update
(Administrators [AllAccess])
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.
=============================================================================
==============
iaStorAfsService(Intel Corporation - Intel(R) Optane(TM) Memory
Service)[C:\WINDOWS\System32\iaStorAfsService.exe] - Manual - Stopped
YOU CAN MODIFY THIS SERVICE: AllAccess
Possible DLL Hijacking in binary folder: C:\WINDOWS\System32 (Administrators
[WriteData/CreateFiles])
Enables amazing system performance and responsiveness by accelerating frequently
used files
=============================================================================
==============
igccservice(Intel Corporation - Intel(R) Graphics Command Center Service)[C:\WINDO
WS\System32\DriverStore\FileRepository\igcc_dch.inf_amd64_524cec1494781ee1\OneApp.
IGCC.WinService.exe] - Auto - Running - isDotNet
YOU CAN MODIFY THIS SERVICE: AllAccess
Service for Intel(R) Graphics Command Center
=============================================================================
==============
igfxCUIService2.0.0.0(Intel Corporation - Intel(R) HD Graphics Control Panel Servi
ce)[C:\WINDOWS\System32\DriverStore\FileRepository\cui_dch.inf_amd64_1e611bd77bc26
0c3\igfxCUIServiceN.exe] - Auto - Running
YOU CAN MODIFY THIS SERVICE: AllAccess
Service for Intel(R) HD Graphics Control Panel
=============================================================================
==============
Intel(R) Capability Licensing Service TCP IP Interface(Intel(R) Corporation -
Intel(R) Capability Licensing Service TCP IP Interface)[C:\WINDOWS\System32\Driver
Store\FileRepository\iclsclient.inf_amd64_76523213b78d9046\lib\SocketHeciServer.ex
e] - Manual - Stopped
YOU CAN MODIFY THIS SERVICE: Start, AllAccess
Version: 1.63.1155.1
=============================================================================
==============
Intel(R) TPM Provisioning Service(Intel(R) Corporation - Intel(R) TPM Provisioning
Service)[C:\WINDOWS\System32\DriverStore\FileRepository\iclsclient.inf_amd64_76523
213b78d9046\lib\TPMProvisioningService.exe] - Auto - Stopped
YOU CAN MODIFY THIS SERVICE: Start, AllAccess

```
Version: 1.63.1155.1
================================================================================
===============
IntelAudioService(Intel - Intel(R) Audio Service)[C:\WINDOWS\System32\DriverStore\
FileRepository\intcoed.inf_amd64_c34ea2dc251566b0\\AS\\IAS\\IntelAudioService.exe]
- Auto - Running - isDotNet
YOU CAN MODIFY THIS SERVICE: AllAccess
================================================================================
===============
jhi_service(Intel Corporation - Intel(R) Dynamic Application Loader Host Interface
Service)[C:\WINDOWS\System32\DriverStore\FileRepository\dal.inf_amd64_b5484efd38ad
be8d\jhi_service.exe] - Auto - Running
YOU CAN MODIFY THIS SERVICE: Start, AllAccess
Intel(R) Dynamic Application Loader Host Interface Service - Allows applications to
access the local Intel (R) DAL
================================================================================
===============
McAfee WebAdvisor(McAfee, LLC - McAfee WebAdvisor)["C:\Program
Files\McAfee\WebAdvisor\ServiceHost.exe"] - Auto - Running
YOU CAN MODIFY THIS SERVICE: AllAccess
File Permissions: Administrators [AllAccess]
Possible DLL Hijacking in binary folder: C:\Program Files\McAfee\WebAdvisor
(Administrators [AllAccess])
McAfee WebAdvisor Service
================================================================================
===============
McAPExe(McAfee, LLC - McAfee AP Service)["C:\Program Files\Common
Files\McAfee\VSCore_22_12\McApExe.exe"] - Auto - Running
File Permissions: Administrators [AllAccess]
Possible DLL Hijacking in binary folder: C:\Program Files\Common
Files\McAfee\VSCore_22_12 (Administrators [AllAccess])
McAfee AP Service
================================================================================
===============
McAWFwk(McAfee, LLC - McAfee Activation Service)["C:\Program Files\Common
Files\McAfee\ActWiz\McAWFwk.exe"] - Manual - Stopped
YOU CAN MODIFY THIS SERVICE: AllAccess
File Permissions: Administrators [AllAccess]
Possible DLL Hijacking in binary folder: C:\Program Files\Common
Files\McAfee\ActWiz (Administrators [AllAccess])
McAfee Activation Service
================================================================================
===============
mccspsvc(McAfee, LLC - McAfee CSP Service)["C:\Program Files\Common
Files\McAfee\CSP\5.5.107.0\\McCSPServiceHost.exe"] - Auto - Running
YOU CAN MODIFY THIS SERVICE: AllAccess
Possible DLL Hijacking in binary folder: C:\Program Files\Common
Files\McAfee\CSP\5.5.107.0 (Administrators [AllAccess])
McAfee Cloud Platform Service
================================================================================
===============
mfefire(McAfee, LLC - McAfee Firewall Core Service)["C:\Program Files\Common
Files\McAfee\SystemCore\mfemms.exe"] - Manual - Stopped
File Permissions: Administrators [AllAccess]
Possible DLL Hijacking in binary folder: C:\Program Files\Common
Files\McAfee\SystemCore (Administrators [AllAccess])
Provides firewall services to McAfee products
================================================================================
===============
mfemms(McAfee, LLC - McAfee Service Controller)["C:\Program Files\Common
Files\McAfee\SystemCore\mfemms.exe"] - Auto - Running
File Permissions: Administrators [AllAccess]
Possible DLL Hijacking in binary folder: C:\Program Files\Common
Files\McAfee\SystemCore (Administrators [AllAccess])
Manages McAfee Services
================================================================================
===============
mfevtp(McAfee, LLC - McAfee Validation Trust Protection Service)["C:\Program
Files\Common Files\McAfee\SystemCore\mfemms.exe"] - Manual - Running
File Permissions: Administrators [AllAccess]
Possible DLL Hijacking in binary folder: C:\Program Files\Common
Files\McAfee\SystemCore (Administrators [AllAccess])
Provides validation trust protection services
================================================================================
===============
ModuleCoreService(McAfee, LLC - McAfee Module Core Service)["C:\Program
Files\Common Files\McAfee\ModuleCore\ModuleCoreService.exe"] - Auto - Running
YOU CAN MODIFY THIS SERVICE: AllAccess
```

```
File Permissions: Administrators [AllAccess]
Possible DLL Hijacking in binary folder: C:\Program Files\Common
Files\McAfee\ModuleCore (Administrators [AllAccess])
McAfee Module Core Service
================================================================================
===============
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
YOU CAN MODIFY THIS SERVICE: AllAccess
File Permissions: Administrators [AllAccess]
Possible DLL Hijacking in binary folder: C:\Program Files\MySQL\MySQL Server
8.0\bin (Administrators [AllAccess])
================================================================================
===============
PEFService(McAfee, LLC - McAfee PEF Service)["C:\Program Files\Common
Files\McAfee\PEF\CORE\PEFService.exe"] - Auto - Running
YOU CAN MODIFY THIS SERVICE: AllAccess
File Permissions: Everyone [WriteData/CreateFiles], Administrators [AllAccess]
Possible DLL Hijacking in binary folder: C:\Program Files\Common
Files\McAfee\PEF\CORE (Administrators [AllAccess])
McAfee PEF Service
================================================================================
===============
RAPSService(Rivet Networks, LLC. - Rivet AP Selector Service)["C:\Program
Files\Rivet Networks\SmartByte\RAPSService.exe"] - Auto - Running - isDotNet
YOU CAN MODIFY THIS SERVICE: AllAccess
File Permissions: Administrators [AllAccess]
Possible DLL Hijacking in binary folder: C:\Program Files\Rivet Networks\SmartByte
(Administrators [AllAccess])
This service provides provides a service which automatically connects of the best
known Wifi AP.
================================================================================
===============
RNDBWM(Rivet Networks, LLC. - Rivet Dynamic Bandwidth Management)["C:\Program
Files\Rivet Networks\SmartByte\RNDBWMService.exe"] - Manual - Stopped - isDotNet
YOU CAN MODIFY THIS SERVICE: AllAccess
File Permissions: Administrators [AllAccess]
Possible DLL Hijacking in binary folder: C:\Program Files\Rivet Networks\SmartByte
(Administrators [AllAccess])
This service dynamically manages bandwidth settings based on detection of internet
traffic congestion.
================================================================================
===============
RstMwService(Intel Corporation - Intel(R) Storage Middleware Service)[C:\WINDOWS\S
ystem32\DriverStore\FileRepository\iastorvd.inf_amd64_15c9ea6001a5206d\RstMwServic
e.exe] - Auto - Running
YOU CAN MODIFY THIS SERVICE: AllAccess
RPC endpoint service which allows communication between driver and Windows Store
Application
================================================================================
===============
RtkAudioUniversalService(Realtek Semiconductor - Realtek Audio Universal Service)[
"C:\WINDOWS\System32\DriverStore\FileRepository\realtekservice.inf_amd64_444148fa7
298b49f\RtkAudUService64.exe"] - Auto - Running
YOU CAN MODIFY THIS SERVICE: AllAccess
Realtek Audio Universal Service
================================================================================
===============
SessionSvc(Goodix - Session
Detection)[C:\WINDOWS\System32\drivers\GoodixSessionService.exe] - Auto - Running
YOU CAN MODIFY THIS SERVICE: AllAccess
File Permissions: Administrators [AllAccess]
Possible DLL Hijacking in binary folder: C:\WINDOWS\System32\drivers
(Administrators [WriteData/CreateFiles])
================================================================================
===============
SmartByte Analytics Service(Rivet Networks - SmartByte Analytics
Service)["C:\Program Files\Rivet Networks\SmartByte\SmartByteAnalyticsService.exe"]
- Auto - Running
YOU CAN MODIFY THIS SERVICE: AllAccess
File Permissions: Administrators [AllAccess]
Possible DLL Hijacking in binary folder: C:\Program Files\Rivet Networks\SmartByte
(Administrators [AllAccess])
SmartByte Analytics Service
================================================================================
===============
SmartByte Network Service x64(Rivet Networks - SmartByte Network
```

```
Service)["C:\Program Files\Rivet Networks\SmartByte\SmartByteNetworkService.exe"] -
Auto - Running
YOU CAN MODIFY THIS SERVICE: AllAccess
File Permissions: Administrators [AllAccess]
Possible DLL Hijacking in binary folder: C:\Program Files\Rivet Networks\SmartByte
(Administrators [AllAccess])
===============================================================================
===============
ssh-agent(OpenSSH Authentication Agent)[C:\WINDOWS\System32\OpenSSH\ssh-agent.exe]
- Disabled - Stopped
YOU CAN MODIFY THIS SERVICE: Start, AllAccess
Possible DLL Hijacking in binary folder: C:\WINDOWS\System32\OpenSSH
(Administrators [WriteData/CreateFiles])
Agent to hold private keys used for public key authentication.
===============================================================================
===============
SupportAssistAgent(Dell Inc. - Dell SupportAssist)["C:\Program
Files\Dell\SupportAssistAgent\bin\SupportAssistAgent.exe"] - Auto - Running
YOU CAN MODIFY THIS SERVICE: AllAccess
File Permissions: Administrators [AllAccess]
Possible DLL Hijacking in binary folder: C:\Program
Files\Dell\SupportAssistAgent\bin (Administrators [AllAccess])
Dell SupportAssist keeps your PC up to date and running at its best with
recommended software and driver updates. It also helps resolve issues quickly by
detecting common problems and sending issue details to Dell Technical Support
agents on your behalf.
===============================================================================
===============
TbtP2pShortcutService(Intel Corporation - Thunderbolt(TM) Peer to Peer
Shortcut)[C:\WINDOWS\TbtP2pShortcutService.exe] - Auto - Running
YOU CAN MODIFY THIS SERVICE: AllAccess
File Permissions: Administrators [AllAccess]
Possible DLL Hijacking in binary folder: C:\WINDOWS (Administrators
[WriteData/CreateFiles])
Thunderbolt(TM) Peer to Peer Shortcut
===============================================================================
===============
WavesAudioService(Waves Audio Ltd - Waves Audio Universal Services)[C:\WINDOWS\Sys
tem32\DriverStore\FileRepository\wavesapo10de.inf_amd64_f7373b847419c8d1\WavesAudi
oService.exe] - Auto - Running - isDotNet
YOU CAN MODIFY THIS SERVICE: AllAccess
Waves Audio universal global services
===============================================================================
===============
WavesSysSvc(Waves Audio Ltd. - Waves Audio Services)[C:\WINDOWS\System32\DriverSto
re\FileRepository\wavesapo10de.inf_amd64_f7373b847419c8d1\WavesSysSvc64.exe] - Auto
- Running
YOU CAN MODIFY THIS SERVICE: AllAccess
Waves Audio global services
===============================================================================
===============
WMIRegistrationService(Intel Corporation - Intel(R) Management Engine WMI Provider
Registration)[C:\WINDOWS\System32\DriverStore\FileRepository\mewmiprov.inf_amd64_d
4564390a9b1e980\WMIRegistrationService.exe] - Auto - Running
YOU CAN MODIFY THIS SERVICE: AllAccess
Intel(R) Management Engine WMI Provider Registration 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:
AJRouter: AllAccess
ALG: AllAccess
Apache2.4: AllAccess
AppIDSvc: AllAccess
Appinfo: Start, AllAccess
AppReadiness: AllAccess
AppXSvc: Start, GenericExecute (Start/Stop)
AudioEndpointBuilder: AllAccess
Audiosrv: AllAccess
```

```
autotimesvc: AllAccess
AxInstSV: AllAccess
BDESVC: Start, ChangeConfig
BFE: WriteDac
BITS: AllAccess
BrokerInfrastructure: WriteDac, Start
Browser: AllAccess
BTAGService: AllAccess
BthAvctpSvc: AllAccess
bthserv: AllAccess
camsvc: AllAccess
CDPSvc: AllAccess
CertPropSvc: ChangeConfig
ClickToRunSvc: Start, AllAccess
ClipSVC: Start, WriteDac
COMSysApp: AllAccess
CoreMessagingRegistrar: Start, GenericExecute (Start/Stop)
cplspcon: AllAccess
CryptSvc: AllAccess
DcomLaunch: WriteDac
dcpm-notify: AllAccess
dcsvc: AllAccess
DDVCollectorSvcApi: AllAccess
DDVDataCollector: AllAccess
DDVRulesProcessor: AllAccess
defragsvc: AllAccess
Dell Digital Delivery Services: AllAccess
Dell SupportAssist Remediation: AllAccess
Dell.CommandPowerManager.Service: AllAccess
DellClientManagementService: AllAccess
DellTechHub: AllAccess
DeviceAssociationService: AllAccess
DeviceInstall: AllAccess
DevQueryBroker: AllAccess
Dhcp: Start, AllAccess
diagnosticshub.standardcollector.service: AllAccess
diagsvc: AllAccess
DiagTrack: AllAccess
DispBrokerDesktopSvc: AllAccess
DisplayEnhancementService: Start, AllAccess
DmEnrollmentSvc: AllAccess
dmwappushservice: Start, AllAccess
DoSvc: Start, AllAccess
dot3svc: AllAccess
DPS: ChangeConfig
DsmSvc: AllAccess, Start
DsSvc: Start, AllAccess
DusmSvc: AllAccess
EapHost: AllAccess
edgeupdate: AllAccess
edgeupdatem: AllAccess
EFS: Start, ChangeConfig
embeddedmode: Start, GenericExecute (Start/Stop)
EntAppSvc: Start, GenericExecute (Start/Stop)
esifsvc: AllAccess
EventLog: AllAccess
EventSystem: AllAccess
Fax: Start, AllAccess
fdPHost: AllAccess
FDResPub: AllAccess
fhsvc: Start, AllAccess
FileSyncHelper: AllAccess
FontCache: Start, AllAccess
FrameServer: AllAccess
FrameServerMonitor: AllAccess
GoogleChromeElevationService: AllAccess
GraphicsPerfSvc: AllAccess
gupdate: AllAccess
gupdatem: AllAccess
hidserv: AllAccess
HvHost: AllAccess
iaStorAfsService: AllAccess
icssvc: Start, AllAccess
igccservice: AllAccess
igfxCUIService2.0.0.0: AllAccess
IKEEXT: AllAccess
InstallService: AllAccess
Intel(R) Capability Licensing Service TCP IP Interface: Start, AllAccess
```

```
Intel(R) TPM Provisioning Service: Start, AllAccess
IntelAudioService: AllAccess
InventorySvc: AllAccess, Start
iphlpsvc: AllAccess
IpxlatCfgSvc: AllAccess
jhi_service: Start, AllAccess
KeyIso: Start, AllAccess
KtmRm: Start, AllAccess
LanmanServer: AllAccess
LanmanWorkstation: AllAccess
lfsvc: Start, AllAccess
LicenseManager: AllAccess
lltdsvc: AllAccess
lmhosts: AllAccess
LxpSvc: AllAccess
MapsBroker: Start, AllAccess
McAfee WebAdvisor: AllAccess
McAWFwk: AllAccess
mccspsvc: AllAccess
McpManagementService: AllAccess
MicrosoftEdgeElevationService: AllAccess
MixedRealityOpenXRSvc: AllAccess
ModuleCoreService: AllAccess
mpssvc: WriteDac
MSDTC: Start, ChangeConfig
MSiSCSI: AllAccess
msiserver: Start, GenericExecute (Start/Stop)
MySQL80: AllAccess
NaturalAuthentication: Start, AllAccess
NcaSvc: AllAccess
NcbService: AllAccess
NcdAutoSetup: AllAccess
Netlogon: AllAccess
Netman: AllAccess
netprofm: AllAccess
NetSetupSvc: AllAccess, Start
NetTcpPortSharing: Start, AllAccess
NgcCtnrSvc: WriteDac
NgcSvc: WriteDac
NlaSvc: AllAccess
nsi: AllAccess
OneDrive Updater Service: AllAccess
p2pimsvc: Start, AllAccess
p2psvc: Start, AllAccess
PcaSvc: Start, AllAccess
PEFService: AllAccess
perceptionsimulation: AllAccess
PerfHost: AllAccess
PhoneSvc: Start, AllAccess
pla: Start, AllAccess
PlugPlay: AllAccess
PNRPAutoReg: Start, AllAccess
PNRPsvc: Start, AllAccess
PolicyAgent: AllAccess
Power: AllAccess
PrintNotify: AllAccess
ProfSvc: AllAccess
PushToInstall: AllAccess
QWAVE: Start, AllAccess
RAPSService: AllAccess
RasAuto: AllAccess
RasMan: Start, AllAccess
RemoteAccess: AllAccess
RemoteRegistry: AllAccess
RetailDemo: AllAccess
RmSvc: ChangeConfig, GenericExecute (Start/Stop)
RNDBWM: AllAccess
RpcEptMapper: WriteDac, Start
RpcLocator: AllAccess
RpcSs: WriteDac
RstMwService: AllAccess
RtkAudioUniversalService: AllAccess
SamSs: AllAccess
SCardSvr: ChangeConfig
ScDeviceEnum: ChangeConfig
Schedule: WriteDac
SCPolicySvc: ChangeConfig
SDRSVC: AllAccess
```

```
seclogon: Start, AllAccess
SEMgrSvc: Start, AllAccess
SENS: AllAccess
SensorDataService: AllAccess
SensorService: Start, AllAccess
SensrSvc: Start, AllAccess
SessionEnv: AllAccess
SessionSvc: AllAccess
SgrmBroker: AllAccess
SharedAccess: AllAccess
SharedRealitySvc: AllAccess
ShellHWDetection: AllAccess
shpamsvc: AllAccess
SmartByte Analytics Service: AllAccess
SmartByte Network Service x64: AllAccess
smphost: Start, AllAccess
SmsRouter: ChangeConfig, Start
SNMPTrap: AllAccess
spectrum: AllAccess
Spooler: AllAccess
sppsvc: Start, WriteDac
SQLWriter: AllAccess
SSDPSRV: Start, AllAccess
ssh-agent: Start, AllAccess
SstpSvc: Start, AllAccess
StateRepository: Start, GenericExecute (Start/Stop)
StiSvc: AllAccess
StorSvc: AllAccess
SupportAssistAgent: AllAccess
svsvc: AllAccess
swprv: AllAccess
SysMain: AllAccess
SystemEventsBroker: WriteDac, Start
TapiSrv: Start, AllAccess
TbtP2pShortcutService: AllAccess
TermService: AllAccess
Themes: AllAccess
TieringEngineService: AllAccess
TimeBrokerSvc: WriteDac, Start
TokenBroker: AllAccess
TrkWks: AllAccess
TroubleshootingSvc: AllAccess
TrustedInstaller: ChangeConfig
tzautoupdate: AllAccess
uhssvc: AllAccess
UmRdpService: AllAccess
upnphost: Start, AllAccess
UserManager: AllAccess
UsoSvc: Start, AllAccess
VacSvc: AllAccess
VaultSvc: Start, AllAccess
vds: AllAccess
vmicguestinterface: AllAccess
vmicheartbeat: AllAccess
vmickvpexchange: AllAccess
vmicrdv: AllAccess
vmicshutdown: AllAccess
vmictimesync: AllAccess
vmicvmsession: AllAccess
vmicvss: AllAccess
VSS: AllAccess
VSStandardCollectorService150: AllAccess
W32Time: AllAccess
WaaSMedicSvc: Start, AllAccess
WalletService: AllAccess
WarpJITSvc: AllAccess
WavesAudioService: AllAccess
WavesSysSvc: AllAccess
wbengine: AllAccess
WbioSrvc: Start, AllAccess
Wcmsvc: AllAccess
wcncsvc: GenericExecute (Start/Stop), AllAccess
WdiServiceHost: ChangeConfig
WdiSystemHost: ChangeConfig
WebClient: AllAccess
webthreatdefsvc: AllAccess
Wecsvc: AllAccess
WEPHOSTSVC: AllAccess
```

```
wercplsupport: AllAccess
WerSvc: AllAccess
WFDSConMgrSvc: AllAccess
WiaRpc: AllAccess
Winmgmt: AllAccess
WinRM: AllAccess
wisvc: AllAccess
WlanSvc: AllAccess
wlidsvc: Start, AllAccess
wlpasvc: AllAccess
WManSvc: AllAccess
wmiApSrv: AllAccess
WMIRegistrationService: AllAccess
WMPNetworkSvc: Start, AllAccess
workfolderssvc: AllAccess
WpcMonSvc: AllAccess
WPDBusEnum: AllAccess
WpnService: AllAccess
WSearch: AllAccess
wuauserv: Start, AllAccess
WwanSvc: AllAccess
XblAuthManager: AllAccess
XblGameSave: AllAccess
XboxGipSvc: AllAccess
XboxNetApiSvc: AllAccess
AarSvc_1eab96: AllAccess
BcastDVRUserService_1eab96: GenericExecute (Start/Stop), AllAccess
BluetoothUserService_1eab96: AllAccess
CaptureService_1eab96: AllAccess
cbdhsvc_1eab96: AllAccess
CDPUserSvc_1eab96: AllAccess
ConsentUxUserSvc_1eab96: GenericExecute (Start/Stop), AllAccess
CredentialEnrollmentManagerUserSvc_1eab96: GenericExecute (Start/Stop)
DeviceAssociationBrokerSvc_1eab96: GenericExecute (Start/Stop)
DevicePickerUserSvc_1eab96: GenericExecute (Start/Stop), AllAccess
DevicesFlowUserSvc_1eab96: GenericExecute (Start/Stop), AllAccess
MessagingService_1eab96: AllAccess
NPSMSvc_1eab96: AllAccess
OneSyncSvc_1eab96: Start, AllAccess
P9RdrService_1eab96: AllAccess
PenService_1eab96: AllAccess
PimIndexMaintenanceSvc_1eab96: GenericExecute (Start/Stop), AllAccess
PrintWorkflowUserSvc_1eab96: GenericExecute (Start/Stop)
UdkUserSvc_1eab96: GenericExecute (Start/Stop), AllAccess
UnistoreSvc_1eab96: GenericExecute (Start/Stop), AllAccess
UserDataSvc_1eab96: GenericExecute (Start/Stop), AllAccess
webthreatdefusersvc_1eab96: AllAccess
WpnUserService_1eab96: GenericExecute (Start/Stop), AllAccess
```

## Looking if you can modify any service registry

*Check if you can modify the registry of a service https://book.hacktricks.xyz/windows-harde
ning/windows-local-privilege-escalation#services-registry-permissions*

```
HKLM\system\currentcontrolset\services\.NET CLR Data (Administrators [FullControl])
HKLM\system\currentcontrolset\services\.NET CLR Networking (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\.NET CLR Networking 4.0.0.0 (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\.NET Data Provider for Oracle
(Administrators [FullControl])
HKLM\system\currentcontrolset\services\.NET Data Provider for SqlServer
(Administrators [FullControl])
HKLM\system\currentcontrolset\services\.NET Memory Cache 4.0 (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\.NETFramework (Administrators [FullControl])
HKLM\system\currentcontrolset\services\1394ohci (Administrators [FullControl])
HKLM\system\currentcontrolset\services\3ware (Administrators [FullControl])
HKLM\system\currentcontrolset\services\AarSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\AarSvc_1eab96 (Administrators [FullControl])
HKLM\system\currentcontrolset\services\ACPI (Administrators [FullControl])
HKLM\system\currentcontrolset\services\AcpiDev (Administrators [FullControl])
HKLM\system\currentcontrolset\services\acpiex (Administrators [FullControl])
```

```
HKLM\system\currentcontrolset\services\acpipagr (Administrators [FullControl])
HKLM\system\currentcontrolset\services\AcpiPmi (Administrators [FullControl])
HKLM\system\currentcontrolset\services\acpitime (Administrators [FullControl])
HKLM\system\currentcontrolset\services\Acx01000 (Administrators [FullControl])
HKLM\system\currentcontrolset\services\AcxHdAudio (Administrators [FullControl])
HKLM\system\currentcontrolset\services\ADOVMPPackage (Administrators [FullControl])
HKLM\system\currentcontrolset\services\ADP80XX (Administrators [FullControl])
HKLM\system\currentcontrolset\services\adsi (Administrators [FullControl])
HKLM\system\currentcontrolset\services\AFD (Administrators [FullControl])
HKLM\system\currentcontrolset\services\afunix (Administrators [FullControl])
HKLM\system\currentcontrolset\services\ahcache (Administrators [FullControl])
HKLM\system\currentcontrolset\services\AJRouter (Administrators [FullControl])
HKLM\system\currentcontrolset\services\ALG (Administrators [FullControl])
HKLM\system\currentcontrolset\services\amdgpio2 (Administrators [FullControl])
HKLM\system\currentcontrolset\services\amdi2c (Administrators [FullControl])
HKLM\system\currentcontrolset\services\AmdK8 (Administrators [FullControl])
HKLM\system\currentcontrolset\services\AmdPPM (Administrators [FullControl])
HKLM\system\currentcontrolset\services\amdsata (Administrators [FullControl])
HKLM\system\currentcontrolset\services\amdsbs (Administrators [FullControl])
HKLM\system\currentcontrolset\services\amdxata (Administrators [FullControl])
HKLM\system\currentcontrolset\services\Apache2.4 (Administrators [FullControl])
HKLM\system\currentcontrolset\services\AppID (Administrators [FullControl])
HKLM\system\currentcontrolset\services\AppIDSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\Appinfo (Administrators [FullControl])
HKLM\system\currentcontrolset\services\AppleLowerFilter (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\AppleSSD (Administrators [FullControl])
HKLM\system\currentcontrolset\services\applockerfltr (Administrators [FullControl])
HKLM\system\currentcontrolset\services\AppReadiness (Administrators [FullControl])
HKLM\system\currentcontrolset\services\AppXSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\arcsas (Administrators [FullControl])
HKLM\system\currentcontrolset\services\AsyncMac (Administrators [FullControl])
HKLM\system\currentcontrolset\services\atapi (Administrators [FullControl])
HKLM\system\currentcontrolset\services\AudioEndpointBuilder (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\Audiosrv (Administrators [FullControl])
HKLM\system\currentcontrolset\services\autotimesvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\AxInstSV (Administrators [FullControl])
HKLM\system\currentcontrolset\services\b06bdrv (Administrators [FullControl])
HKLM\system\currentcontrolset\services\bam (Administrators [FullControl])
HKLM\system\currentcontrolset\services\BasicDisplay (Administrators [FullControl])
HKLM\system\currentcontrolset\services\BasicRender (Administrators [FullControl])
HKLM\system\currentcontrolset\services\BattC (Administrators [FullControl])
HKLM\system\currentcontrolset\services\BcastDVRUserService (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\BcastDVRUserService_1eab96 (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\bcmfn2 (Administrators [FullControl])
HKLM\system\currentcontrolset\services\BDESVC (Administrators [FullControl])
HKLM\system\currentcontrolset\services\Beep (Administrators [FullControl])
HKLM\system\currentcontrolset\services\BFE (Administrators [FullControl])
HKLM\system\currentcontrolset\services\bfs (Administrators [FullControl])
HKLM\system\currentcontrolset\services\bindflt (Administrators [FullControl])
HKLM\system\currentcontrolset\services\BITS (Administrators [FullControl])
HKLM\system\currentcontrolset\services\BluetoothUserService (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\BluetoothUserService_1eab96 (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\bowser (Administrators [FullControl])
HKLM\system\currentcontrolset\services\BrokerInfrastructure (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\Browser (Administrators [FullControl])
HKLM\system\currentcontrolset\services\BTAGService (Administrators [FullControl])
HKLM\system\currentcontrolset\services\BthA2dp (Administrators [FullControl])
HKLM\system\currentcontrolset\services\BthAvctpSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\BthEnum (Administrators [FullControl])
HKLM\system\currentcontrolset\services\BthHFAud (Administrators [FullControl])
HKLM\system\currentcontrolset\services\BthHFEnum (Administrators [FullControl])
HKLM\system\currentcontrolset\services\BthLEEnum (Administrators [FullControl])
HKLM\system\currentcontrolset\services\BthMini (Administrators [FullControl])
HKLM\system\currentcontrolset\services\BTHMODEM (Administrators [FullControl])
HKLM\system\currentcontrolset\services\BthPan (Administrators [FullControl])
HKLM\system\currentcontrolset\services\BTHPORT (Administrators [FullControl])
HKLM\system\currentcontrolset\services\bthserv (Administrators [FullControl])
HKLM\system\currentcontrolset\services\BTHUSB (Administrators [FullControl])
HKLM\system\currentcontrolset\services\bttflt (Administrators [FullControl])
HKLM\system\currentcontrolset\services\buttonconverter (Administrators
[FullControl])
```

```
HKLM\system\currentcontrolset\services\CAD (Administrators [FullControl])
HKLM\system\currentcontrolset\services\camsvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\CaptureService (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\CaptureService_1eab96 (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\cbdhsvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\cbdhsvc_1eab96 (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\cdfs (Administrators [FullControl])
HKLM\system\currentcontrolset\services\CDPSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\CDPUserSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\CDPUserSvc_1eab96 (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\cdrom (Administrators [FullControl])
HKLM\system\currentcontrolset\services\CertPropSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\cfwids (Administrators [FullControl])
HKLM\system\currentcontrolset\services\cht4iscsi (Administrators [FullControl])
HKLM\system\currentcontrolset\services\cht4vbd (Administrators [FullControl])
HKLM\system\currentcontrolset\services\CimFS (Administrators [FullControl])
HKLM\system\currentcontrolset\services\circlass (Administrators [FullControl])
HKLM\system\currentcontrolset\services\CldFlt (Administrators [FullControl])
HKLM\system\currentcontrolset\services\CLFS (Administrators [FullControl])
HKLM\system\currentcontrolset\services\ClickToRunSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\ClipSVC (Administrators [FullControl])
HKLM\system\currentcontrolset\services\clr_optimization_v4.0.30319_32
(Administrators [FullControl])
HKLM\system\currentcontrolset\services\clr_optimization_v4.0.30319_64
(Administrators [FullControl])
HKLM\system\currentcontrolset\services\CmBatt (Administrators [FullControl])
HKLM\system\currentcontrolset\services\CNG (Administrators [FullControl])
HKLM\system\currentcontrolset\services\cnghwassist (Administrators [FullControl])
HKLM\system\currentcontrolset\services\CompositeBus (Administrators [FullControl])
HKLM\system\currentcontrolset\services\COMSysApp (Administrators [FullControl])
HKLM\system\currentcontrolset\services\condrv (Administrators [FullControl])
HKLM\system\currentcontrolset\services\ConsentUxUserSvc (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\ConsentUxUserSvc_1eab96 (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\CoreMessagingRegistrar (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\CoreUI (Administrators [FullControl])
HKLM\system\currentcontrolset\services\CPK1HWU (Administrators [FullControl])
HKLM\system\currentcontrolset\services\CPK2HWU (Administrators [FullControl])
HKLM\system\currentcontrolset\services\cplspcon (Administrators [FullControl])
HKLM\system\currentcontrolset\services\CredentialEnrollmentManagerUserSvc
(Administrators [FullControl])
HKLM\system\currentcontrolset\services\CredentialEnrollmentManagerUserSvc_1eab96
(Administrators [FullControl])
HKLM\system\currentcontrolset\services\crypt32 (Administrators [FullControl])
HKLM\system\currentcontrolset\services\CryptSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\dam (Administrators [FullControl])
HKLM\system\currentcontrolset\services\DCLocator (Administrators [FullControl])
HKLM\system\currentcontrolset\services\dcpm-notify (Administrators [FullControl])
HKLM\system\currentcontrolset\services\dcsvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\DDVCollectorSvcApi (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\DDVDataCollector (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\DDVRulesProcessor (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\defragsvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\Dell Digital Delivery Services
(Administrators [FullControl])
HKLM\system\currentcontrolset\services\Dell SupportAssist Remediation
(Administrators [FullControl])
HKLM\system\currentcontrolset\services\Dell.CommandPowerManager.Service
(Administrators [FullControl])
HKLM\system\currentcontrolset\services\DellClientManagementService (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\DellInstrumentation (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\DellTechHub (Administrators [FullControl])
HKLM\system\currentcontrolset\services\DeviceAssociationBrokerSvc (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\DeviceAssociationBrokerSvc_1eab96
(Administrators [FullControl])
HKLM\system\currentcontrolset\services\DeviceAssociationService (Administrators
```

```
[FullControl])
HKLM\system\currentcontrolset\services\DeviceInstall (Administrators [FullControl])
HKLM\system\currentcontrolset\services\DevicePickerUserSvc (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\DevicePickerUserSvc_1eab96 (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\DevicesFlowUserSvc (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\DevicesFlowUserSvc_1eab96 (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\DevQueryBroker (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\Dfsc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\dg_ssudbus (Administrators [FullControl])
HKLM\system\currentcontrolset\services\Dhcp (Administrators [FullControl
GenericAll])
HKLM\system\currentcontrolset\services\diagnosticshub.standardcollector.service
(Administrators [FullControl])
HKLM\system\currentcontrolset\services\diagsvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\DiagTrack (Administrators [FullControl])
HKLM\system\currentcontrolset\services\disk (Administrators [FullControl])
HKLM\system\currentcontrolset\services\DispBrokerDesktopSvc (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\DisplayEnhancementService (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\DmEnrollmentSvc (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\dmvsc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\dmwappushservice (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\Dnscache (Administrators [FullControl])
HKLM\system\currentcontrolset\services\DoSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\dot3svc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\dptf_acpi (Administrators [FullControl])
HKLM\system\currentcontrolset\services\dptf_cpu (Administrators [FullControl])
HKLM\system\currentcontrolset\services\drmkaud (Administrators [FullControl])
HKLM\system\currentcontrolset\services\DsmSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\DsSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\DusmSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\DXGKrnl (Administrators [FullControl])
HKLM\system\currentcontrolset\services\EapHost (Administrators [WriteKey
FullControl])
HKLM\system\currentcontrolset\services\ebdrv (Administrators [FullControl])
HKLM\system\currentcontrolset\services\ebdrv0 (Administrators [FullControl])
HKLM\system\currentcontrolset\services\edgeupdate (Administrators [FullControl])
HKLM\system\currentcontrolset\services\edgeupdatem (Administrators [FullControl])
HKLM\system\currentcontrolset\services\EFS (Administrators [FullControl])
HKLM\system\currentcontrolset\services\EhStorClass (Administrators [FullControl])
HKLM\system\currentcontrolset\services\EhStorTcgDrv (Administrators [FullControl])
HKLM\system\currentcontrolset\services\embeddedmode (Administrators [FullControl])
HKLM\system\currentcontrolset\services\EntAppSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\ErrDev (Administrators [FullControl])
HKLM\system\currentcontrolset\services\ESENT (Administrators [FullControl])
HKLM\system\currentcontrolset\services\esifsvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\esif_lf (Administrators [FullControl])
HKLM\system\currentcontrolset\services\EventLog (Administrators [FullControl
GenericAll])
HKLM\system\currentcontrolset\services\EventSystem (Administrators [FullControl])
HKLM\system\currentcontrolset\services\ExecutionContext (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\exfat (Administrators [FullControl])
HKLM\system\currentcontrolset\services\fastfat (Administrators [FullControl])
HKLM\system\currentcontrolset\services\Fax (Administrators [FullControl])
HKLM\system\currentcontrolset\services\fdc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\fdPHost (Administrators [FullControl])
HKLM\system\currentcontrolset\services\FDResPub (Administrators [FullControl])
HKLM\system\currentcontrolset\services\fhsvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\FileCrypt (Administrators [FullControl])
HKLM\system\currentcontrolset\services\FileInfo (Administrators [FullControl])
HKLM\system\currentcontrolset\services\FileSyncHelper (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\Filetrace (Administrators [FullControl])
HKLM\system\currentcontrolset\services\flpydisk (Administrators [FullControl])
HKLM\system\currentcontrolset\services\FltMgr (Administrators [FullControl])
HKLM\system\currentcontrolset\services\FontCache (Administrators [FullControl])
HKLM\system\currentcontrolset\services\FrameServer (Administrators [FullControl])
HKLM\system\currentcontrolset\services\FrameServerMonitor (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\FsDepends (Administrators [FullControl])
```

```
HKLM\system\currentcontrolset\services\Fs_Rec (Administrators [FullControl])
HKLM\system\currentcontrolset\services\fvevol (Administrators [FullControl])
HKLM\system\currentcontrolset\services\gencounter (Administrators [FullControl])
HKLM\system\currentcontrolset\services\genericusbfn (Administrators [FullControl])
HKLM\system\currentcontrolset\services\GeneStor (Administrators [FullControl])
HKLM\system\currentcontrolset\services\GenPass (Administrators [FullControl])
HKLM\system\currentcontrolset\services\GoogleChromeElevationService (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\GPIOClx0101 (Administrators [FullControl])
HKLM\system\currentcontrolset\services\GraphicsPerfSvc (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\gupdate (Administrators [FullControl])
HKLM\system\currentcontrolset\services\gupdatem (Administrators [FullControl])
HKLM\system\currentcontrolset\services\HdAudAddService (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\HDAudBus (Administrators [FullControl])
HKLM\system\currentcontrolset\services\HidBatt (Administrators [FullControl])
HKLM\system\currentcontrolset\services\HidBth (Administrators [FullControl])
HKLM\system\currentcontrolset\services\HidEventFilter (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\hidi2c (Administrators [FullControl])
HKLM\system\currentcontrolset\services\hidinterrupt (Administrators [FullControl])
HKLM\system\currentcontrolset\services\HidIr (Administrators [FullControl])
HKLM\system\currentcontrolset\services\hidserv (Administrators [FullControl])
HKLM\system\currentcontrolset\services\hidspi (Administrators [FullControl])
HKLM\system\currentcontrolset\services\HidSpiCx (Administrators [FullControl])
HKLM\system\currentcontrolset\services\HidUsb (Administrators [FullControl])
HKLM\system\currentcontrolset\services\HID_PCI (Administrators [FullControl])
HKLM\system\currentcontrolset\services\HpSAMD (Administrators [FullControl])
HKLM\system\currentcontrolset\services\Hsp (Administrators [FullControl])
HKLM\system\currentcontrolset\services\HTTP (Administrators [FullControl])
HKLM\system\currentcontrolset\services\hvcrash (Administrators [FullControl])
HKLM\system\currentcontrolset\services\HvHost (Administrators [FullControl])
HKLM\system\currentcontrolset\services\hvservice (Administrators [FullControl])
HKLM\system\currentcontrolset\services\HwNClx0101 (Administrators [FullControl])
HKLM\system\currentcontrolset\services\hwpolicy (Administrators [FullControl])
HKLM\system\currentcontrolset\services\hyperkbd (Administrators [FullControl])
HKLM\system\currentcontrolset\services\HyperVideo (Administrators [FullControl])
HKLM\system\currentcontrolset\services\i8042prt (Administrators [FullControl])
HKLM\system\currentcontrolset\services\iagpio (Administrators [FullControl])
HKLM\system\currentcontrolset\services\iai2c (Administrators [FullControl])
HKLM\system\currentcontrolset\services\iaLPSS2i_GPIO2 (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\iaLPSS2i_GPIO2_BXT_P (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\iaLPSS2i_GPIO2_CNL (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\iaLPSS2i_GPIO2_GLK (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\iaLPSS2i_I2C (Administrators [FullControl])
HKLM\system\currentcontrolset\services\iaLPSS2i_I2C_BXT_P (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\iaLPSS2i_I2C_CNL (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\iaLPSS2i_I2C_GLK (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\iaLPSS2_GPIO2_TGL (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\iaLPSS2_I2C_TGL (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\iaLPSSi_GPIO (Administrators [FullControl])
HKLM\system\currentcontrolset\services\iaLPSSi_I2C (Administrators [FullControl])
HKLM\system\currentcontrolset\services\iaStorAfs (Administrators [FullControl])
HKLM\system\currentcontrolset\services\iaStorAfsService (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\iaStorAV (Administrators [FullControl])
HKLM\system\currentcontrolset\services\iaStorAVC (Administrators [FullControl])
HKLM\system\currentcontrolset\services\iaStorV (Administrators [FullControl])
HKLM\system\currentcontrolset\services\iaStorVD (Administrators [FullControl])
HKLM\system\currentcontrolset\services\ibbus (Administrators [FullControl])
HKLM\system\currentcontrolset\services\ibtusb (Administrators [FullControl])
HKLM\system\currentcontrolset\services\icssvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\igccservice (Administrators [FullControl])
HKLM\system\currentcontrolset\services\igfxCUIService2.0.0.0 (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\igfxn (Administrators [FullControl])
HKLM\system\currentcontrolset\services\IKEEXT (Administrators [FullControl])
HKLM\system\currentcontrolset\services\IndirectKmd (Administrators [FullControl])
```

```
HKLM\system\currentcontrolset\services\inetaccs (Administrators [FullControl])
HKLM\system\currentcontrolset\services\InstallService (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\IntcAudioBus (Administrators [FullControl])
HKLM\system\currentcontrolset\services\IntcAzAudAddService (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\IntcDMic (Administrators [FullControl])
HKLM\system\currentcontrolset\services\IntcOED (Administrators [FullControl])
HKLM\system\currentcontrolset\services\IntcUSB (Administrators [FullControl])
HKLM\system\currentcontrolset\services\Intel(R) Capability Licensing Service TCP IP
Interface (Administrators [FullControl])
HKLM\system\currentcontrolset\services\Intel(R) TPM Provisioning Service
(Administrators [FullControl])
HKLM\system\currentcontrolset\services\IntelAudioService (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\IntelHaxm (Administrators [FullControl])
HKLM\system\currentcontrolset\services\intelide (Administrators [FullControl])
HKLM\system\currentcontrolset\services\intelpep (Administrators [FullControl])
HKLM\system\currentcontrolset\services\intelpmax (Administrators [FullControl])
HKLM\system\currentcontrolset\services\IntelPMT (Administrators [FullControl])
HKLM\system\currentcontrolset\services\intelppm (Administrators [FullControl])
HKLM\system\currentcontrolset\services\InventorySvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\iorate (Administrators [FullControl])
HKLM\system\currentcontrolset\services\IpFilterDriver (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\iphlpsvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\IPMIDRV (Administrators [FullControl])
HKLM\system\currentcontrolset\services\IPNAT (Administrators [FullControl])
HKLM\system\currentcontrolset\services\IPT (Administrators [FullControl])
HKLM\system\currentcontrolset\services\IpxlatCfgSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\isapnp (Administrators [FullControl])
HKLM\system\currentcontrolset\services\iScsiPrt (Administrators [FullControl])
HKLM\system\currentcontrolset\services\ISH (Administrators [FullControl])
HKLM\system\currentcontrolset\services\ISH_BusDriver (Administrators [FullControl])
HKLM\system\currentcontrolset\services\ItSas35i (Administrators [FullControl])
HKLM\system\currentcontrolset\services\jhi_service (Administrators [FullControl])
HKLM\system\currentcontrolset\services\kbdclass (Administrators [FullControl])
HKLM\system\currentcontrolset\services\kbdhid (Administrators [FullControl])
HKLM\system\currentcontrolset\services\kdnic (Administrators [FullControl])
HKLM\system\currentcontrolset\services\KeyIso (Administrators [FullControl])
HKLM\system\currentcontrolset\services\Killer Analytics Service (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\KSecDD (Administrators [FullControl])
HKLM\system\currentcontrolset\services\KSecPkg (Administrators [FullControl])
HKLM\system\currentcontrolset\services\ksthunk (Administrators [FullControl])
HKLM\system\currentcontrolset\services\KtmRm (Administrators [FullControl])
HKLM\system\currentcontrolset\services\LanmanServer (Administrators [FullControl])
HKLM\system\currentcontrolset\services\LanmanWorkstation (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\ldap (Administrators [FullControl])
HKLM\system\currentcontrolset\services\lfsvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\LicenseManager (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\lltdio (Administrators [FullControl])
HKLM\system\currentcontrolset\services\lltdsvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\lmhosts (Administrators [FullControl])
HKLM\system\currentcontrolset\services\LSI_SAS (Administrators [FullControl])
HKLM\system\currentcontrolset\services\LSI_SAS2i (Administrators [FullControl])
HKLM\system\currentcontrolset\services\LSI_SAS3i (Administrators [FullControl])
HKLM\system\currentcontrolset\services\LSM (Administrators [FullControl])
HKLM\system\currentcontrolset\services\luafv (Administrators [FullControl])
HKLM\system\currentcontrolset\services\LxpSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\MapsBroker (Administrators [FullControl])
HKLM\system\currentcontrolset\services\mausbhost (Administrators [FullControl])
HKLM\system\currentcontrolset\services\mausbip (Administrators [FullControl])
HKLM\system\currentcontrolset\services\MbbCx (Administrators [FullControl])
HKLM\system\currentcontrolset\services\McAfee WebAdvisor (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\McAPExe (Administrators [FullControl])
HKLM\system\currentcontrolset\services\McAWFwk (Administrators [FullControl])
HKLM\system\currentcontrolset\services\mccspsvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\McpManagementService (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\megasas2i (Administrators [FullControl])
HKLM\system\currentcontrolset\services\megasas35i (Administrators [FullControl])
HKLM\system\currentcontrolset\services\megasr (Administrators [FullControl])
HKLM\system\currentcontrolset\services\MEIx64 (Administrators [FullControl])
HKLM\system\currentcontrolset\services\MessagingService (Administrators
```

```
[FullControl])
HKLM\system\currentcontrolset\services\MessagingService_1eab96 (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\mfeaack (Administrators [FullControl])
HKLM\system\currentcontrolset\services\mfeavfk (Administrators [FullControl])
HKLM\system\currentcontrolset\services\mfeelamk (Administrators [FullControl])
HKLM\system\currentcontrolset\services\mfefire (Administrators [FullControl])
HKLM\system\currentcontrolset\services\mfefirek (Administrators [FullControl])
HKLM\system\currentcontrolset\services\mfehidk (Administrators [FullControl])
HKLM\system\currentcontrolset\services\mfemms (Administrators [FullControl])
HKLM\system\currentcontrolset\services\mfencbdc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\mfencrk (Administrators [FullControl])
HKLM\system\currentcontrolset\services\mfeplk (Administrators [FullControl])
HKLM\system\currentcontrolset\services\mfevtp (Administrators [FullControl])
HKLM\system\currentcontrolset\services\mfewfpk (Administrators [FullControl])
HKLM\system\currentcontrolset\services\MicrosoftEdgeElevationService
(Administrators [FullControl])
HKLM\system\currentcontrolset\services\Microsoft_Bluetooth_AvrcpTransport
(Administrators [FullControl])
HKLM\system\currentcontrolset\services\MixedRealityOpenXRSvc (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\mlx4_bus (Administrators [FullControl])
HKLM\system\currentcontrolset\services\MMCSS (Administrators [FullControl])
HKLM\system\currentcontrolset\services\Modem (Administrators [FullControl])
HKLM\system\currentcontrolset\services\ModuleCoreService (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\monitor (Administrators [FullControl])
HKLM\system\currentcontrolset\services\mouclass (Administrators [FullControl])
HKLM\system\currentcontrolset\services\mouhid (Administrators [FullControl])
HKLM\system\currentcontrolset\services\mountmgr (Administrators [FullControl])
HKLM\system\currentcontrolset\services\mpi3drvi (Administrators [FullControl])
HKLM\system\currentcontrolset\services\mpsdrv (Administrators [FullControl])
HKLM\system\currentcontrolset\services\mpssvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\MRxDAV (Administrators [FullControl])
HKLM\system\currentcontrolset\services\mrxsmb (Administrators [FullControl])
HKLM\system\currentcontrolset\services\mrxsmb20 (Administrators [FullControl])
HKLM\system\currentcontrolset\services\MsBridge (Administrators [FullControl])
HKLM\system\currentcontrolset\services\MSDTC (Administrators [FullControl])
HKLM\system\currentcontrolset\services\MSDTC Bridge 4.0.0.0 (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\Msfs (Administrators [FullControl])
HKLM\system\currentcontrolset\services\msgpiowin32 (Administrators [FullControl])
HKLM\system\currentcontrolset\services\mshidkmdf (Administrators [FullControl])
HKLM\system\currentcontrolset\services\mshidumdf (Administrators [FullControl])
HKLM\system\currentcontrolset\services\msisadrv (Administrators [FullControl])
HKLM\system\currentcontrolset\services\MSiSCSI (Administrators [FullControl])
HKLM\system\currentcontrolset\services\msiserver (Administrators [FullControl])
HKLM\system\currentcontrolset\services\MSKSSRV (Administrators [FullControl])
HKLM\system\currentcontrolset\services\MsLldp (Administrators [FullControl])
HKLM\system\currentcontrolset\services\MSPCLOCK (Administrators [FullControl])
HKLM\system\currentcontrolset\services\MSPQM (Administrators [FullControl])
HKLM\system\currentcontrolset\services\MsQuic (Administrators [FullControl])
HKLM\system\currentcontrolset\services\MsRPC (Administrators [FullControl])
HKLM\system\currentcontrolset\services\mssmbios (Administrators [FullControl])
HKLM\system\currentcontrolset\services\MSTEE (Administrators [FullControl])
HKLM\system\currentcontrolset\services\MTConfig (Administrators [FullControl])
HKLM\system\currentcontrolset\services\Mup (Administrators [FullControl])
HKLM\system\currentcontrolset\services\mvumis (Administrators [FullControl])
HKLM\system\currentcontrolset\services\MySQL80 (Administrators [FullControl])
HKLM\system\currentcontrolset\services\napagent (Administrators [FullControl])
HKLM\system\currentcontrolset\services\NativeWifiP (Administrators [FullControl])
HKLM\system\currentcontrolset\services\NaturalAuthentication (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\NcaSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\NcbService (Administrators [FullControl])
HKLM\system\currentcontrolset\services\NcdAutoSetup (Administrators [FullControl])
HKLM\system\currentcontrolset\services\ndfltr (Administrators [FullControl])
HKLM\system\currentcontrolset\services\NDIS (Administrators [FullControl])
HKLM\system\currentcontrolset\services\NdisCap (Administrators [FullControl])
HKLM\system\currentcontrolset\services\NdisImPlatform (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\NdisTapi (Administrators [FullControl])
HKLM\system\currentcontrolset\services\Ndisuio (Administrators [FullControl])
HKLM\system\currentcontrolset\services\NdisVirtualBus (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\NdisWan (Administrators [FullControl])
HKLM\system\currentcontrolset\services\ndiswanlegacy (Administrators [FullControl])
HKLM\system\currentcontrolset\services\NDKPerf (Administrators [FullControl])
HKLM\system\currentcontrolset\services\NDKPing (Administrators [FullControl])
```

```
HKLM\system\currentcontrolset\services\ndproxy (Administrators [FullControl])
HKLM\system\currentcontrolset\services\Ndu (Administrators [FullControl])
HKLM\system\currentcontrolset\services\NetAdapterCx (Administrators [FullControl])
HKLM\system\currentcontrolset\services\NetBIOS (Administrators [FullControl])
HKLM\system\currentcontrolset\services\NetbiosSmb (Administrators [FullControl])
HKLM\system\currentcontrolset\services\NetBT (Administrators [FullControl
GenericAll])
HKLM\system\currentcontrolset\services\Netlogon (Administrators [FullControl])
HKLM\system\currentcontrolset\services\Netman (Administrators [FullControl])
HKLM\system\currentcontrolset\services\netprofm (Administrators [FullControl])
HKLM\system\currentcontrolset\services\NetSetupSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\NetTcpPortSharing (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\netvsc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\Netwtw10 (Administrators [FullControl])
HKLM\system\currentcontrolset\services\NgcCtnrSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\NgcSvc (Administrators [TakeOwnership
FullControl])
HKLM\system\currentcontrolset\services\nhi (Administrators [FullControl])
HKLM\system\currentcontrolset\services\NlaSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\npcap (Administrators [FullControl])
HKLM\system\currentcontrolset\services\npcap_wifi (Administrators [FullControl])
HKLM\system\currentcontrolset\services\Npfs (Administrators [FullControl])
HKLM\system\currentcontrolset\services\NPSMSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\NPSMSvc_1eab96 (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\npsvctrig (Administrators [FullControl])
HKLM\system\currentcontrolset\services\nsi (Administrators [FullControl])
HKLM\system\currentcontrolset\services\nsiproxy (Administrators [FullControl])
HKLM\system\currentcontrolset\services\NTDS (Administrators [FullControl])
HKLM\system\currentcontrolset\services\Ntfs (Administrators [FullControl])
HKLM\system\currentcontrolset\services\Null (Administrators [FullControl])
HKLM\system\currentcontrolset\services\nvdimm (Administrators [FullControl])
HKLM\system\currentcontrolset\services\nvmedisk (Administrators [FullControl])
HKLM\system\currentcontrolset\services\nvraid (Administrators [FullControl])
HKLM\system\currentcontrolset\services\nvstor (Administrators [FullControl])
HKLM\system\currentcontrolset\services\OneDrive Updater Service (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\OneSyncSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\OneSyncSvc_1eab96 (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\p2pimsvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\p2psvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\P9NP (Administrators [FullControl])
HKLM\system\currentcontrolset\services\P9Rdr (Administrators [FullControl])
HKLM\system\currentcontrolset\services\P9RdrService (Administrators [FullControl])
HKLM\system\currentcontrolset\services\P9RdrService_1eab96 (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\Parport (Administrators [FullControl])
HKLM\system\currentcontrolset\services\partmgr (Administrators [FullControl])
HKLM\system\currentcontrolset\services\PcaSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\pci (Administrators [FullControl])
HKLM\system\currentcontrolset\services\pciide (Administrators [FullControl])
HKLM\system\currentcontrolset\services\pcmcia (Administrators [FullControl])
HKLM\system\currentcontrolset\services\pcw (Administrators [FullControl])
HKLM\system\currentcontrolset\services\pdc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\PEAUTH (Administrators [FullControl])
HKLM\system\currentcontrolset\services\PEFService (Administrators [FullControl])
HKLM\system\currentcontrolset\services\PenService (Administrators [FullControl])
HKLM\system\currentcontrolset\services\PenService_1eab96 (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\perceptionsimulation (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\percsas2i (Administrators [FullControl])
HKLM\system\currentcontrolset\services\percsas3i (Administrators [FullControl])
HKLM\system\currentcontrolset\services\PerfDisk (Administrators [FullControl])
HKLM\system\currentcontrolset\services\PerfHost (Administrators [FullControl])
HKLM\system\currentcontrolset\services\PerfNet (Administrators [FullControl])
HKLM\system\currentcontrolset\services\PerfOS (Administrators [FullControl])
HKLM\system\currentcontrolset\services\PerfProc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\PhoneSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\PimIndexMaintenanceSvc (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\PimIndexMaintenanceSvc_1eab96
(Administrators [FullControl])
HKLM\system\currentcontrolset\services\PktMon (Administrators [FullControl])
HKLM\system\currentcontrolset\services\pla (Administrators [FullControl])
HKLM\system\currentcontrolset\services\PlugPlay (Administrators [FullControl])
```

```
HKLM\system\currentcontrolset\services\pmem (Administrators [FullControl])
HKLM\system\currentcontrolset\services\PNPMEM (Administrators [FullControl])
HKLM\system\currentcontrolset\services\PNRPAutoReg (Administrators [FullControl])
HKLM\system\currentcontrolset\services\PNRPsvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\PolicyAgent (Administrators [FullControl])
HKLM\system\currentcontrolset\services\portcfg (Administrators [FullControl])
HKLM\system\currentcontrolset\services\PortProxy (Administrators [FullControl])
HKLM\system\currentcontrolset\services\Power (Administrators [FullControl])
HKLM\system\currentcontrolset\services\PptpMiniport (Administrators [FullControl])
HKLM\system\currentcontrolset\services\PrintNotify (Administrators [FullControl])
HKLM\system\currentcontrolset\services\PrintWorkflowUserSvc (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\PrintWorkflowUserSvc_1eab96 (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\PRM (Administrators [FullControl])
HKLM\system\currentcontrolset\services\Processor (Administrators [FullControl])
HKLM\system\currentcontrolset\services\ProfSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\Psched (Administrators [FullControl])
HKLM\system\currentcontrolset\services\PushToInstall (Administrators [FullControl])
HKLM\system\currentcontrolset\services\pvscsi (Administrators [FullControl])
HKLM\system\currentcontrolset\services\QWAVE (Administrators [FullControl])
HKLM\system\currentcontrolset\services\QWAVEdrv (Administrators [FullControl])
HKLM\system\currentcontrolset\services\Ramdisk (Administrators [FullControl])
HKLM\system\currentcontrolset\services\RAPSService (Administrators [FullControl])
HKLM\system\currentcontrolset\services\RasAcd (Administrators [FullControl])
HKLM\system\currentcontrolset\services\RasAgileVpn (Administrators [FullControl])
HKLM\system\currentcontrolset\services\RasAuto (Administrators [GenericAll
FullControl])
HKLM\system\currentcontrolset\services\Rasl2tp (Administrators [FullControl])
HKLM\system\currentcontrolset\services\RasMan (Administrators [GenericAll
FullControl])
HKLM\system\currentcontrolset\services\RasPppoe (Administrators [FullControl])
HKLM\system\currentcontrolset\services\RasSstp (Administrators [FullControl])
HKLM\system\currentcontrolset\services\rdbss (Administrators [FullControl])
HKLM\system\currentcontrolset\services\RDMANDK (Administrators [FullControl])
HKLM\system\currentcontrolset\services\rdpbus (Administrators [FullControl])
HKLM\system\currentcontrolset\services\RDPDR (Administrators [FullControl])
HKLM\system\currentcontrolset\services\RDPNP (Administrators [FullControl])
HKLM\system\currentcontrolset\services\RDPUDD (Administrators [FullControl])
HKLM\system\currentcontrolset\services\RdpVideoMiniport (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\rdyboost (Administrators [FullControl])
HKLM\system\currentcontrolset\services\Realtek (Administrators [FullControl])
HKLM\system\currentcontrolset\services\ReFS (Administrators [FullControl])
HKLM\system\currentcontrolset\services\ReFSv1 (Administrators [FullControl])
HKLM\system\currentcontrolset\services\RemoteAccess (Administrators [GenericAll
FullControl])
HKLM\system\currentcontrolset\services\RemoteRegistry (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\RetailDemo (Administrators [FullControl])
HKLM\system\currentcontrolset\services\RFCOMM (Administrators [FullControl])
HKLM\system\currentcontrolset\services\rhproxy (Administrators [FullControl])
HKLM\system\currentcontrolset\services\RmSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\RNDBWM (Administrators [FullControl])
HKLM\system\currentcontrolset\services\RoutePolicy (Administrators [FullControl])
HKLM\system\currentcontrolset\services\RpcEptMapper (Administrators [TakeOwnership
FullControl])
HKLM\system\currentcontrolset\services\RpcLocator (Administrators [FullControl])
HKLM\system\currentcontrolset\services\rspndr (Administrators [FullControl])
HKLM\system\currentcontrolset\services\RstMwService (Administrators [FullControl])
HKLM\system\currentcontrolset\services\RtkAudioUniversalService (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\RTSUER (Administrators [FullControl])
HKLM\system\currentcontrolset\services\s3cap (Administrators [FullControl])
HKLM\system\currentcontrolset\services\sbp2port (Administrators [FullControl])
HKLM\system\currentcontrolset\services\SCardSvr (Administrators [FullControl])
HKLM\system\currentcontrolset\services\ScDeviceEnum (Administrators [FullControl])
HKLM\system\currentcontrolset\services\scfilter (Administrators [FullControl])
HKLM\system\currentcontrolset\services\Schedule (Administrators [FullControl])
HKLM\system\currentcontrolset\services\scmbus (Administrators [FullControl])
HKLM\system\currentcontrolset\services\SCPolicySvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\ScrHIDDriver3 (Administrators [FullControl])
HKLM\system\currentcontrolset\services\sdbus (Administrators [FullControl])
HKLM\system\currentcontrolset\services\SDFRd (Administrators [FullControl])
HKLM\system\currentcontrolset\services\SDRSVC (Administrators [FullControl])
HKLM\system\currentcontrolset\services\sdstor (Administrators [FullControl])
HKLM\system\currentcontrolset\services\seclogon (Administrators [FullControl])
HKLM\system\currentcontrolset\services\SEMgrSvc (Administrators [FullControl])
```

```
HKLM\system\currentcontrolset\services\SENS (Administrators [FullControl])
HKLM\system\currentcontrolset\services\SensorDataService (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\SensorService (Administrators [FullControl])
HKLM\system\currentcontrolset\services\SensorsHIDClassDriver (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\SensrSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\SerCx (Administrators [FullControl])
HKLM\system\currentcontrolset\services\SerCx2 (Administrators [FullControl])
HKLM\system\currentcontrolset\services\Serenum (Administrators [FullControl])
HKLM\system\currentcontrolset\services\Serial (Administrators [FullControl])
HKLM\system\currentcontrolset\services\sermouse (Administrators [FullControl])
HKLM\system\currentcontrolset\services\SessionEnv (Administrators [FullControl])
HKLM\system\currentcontrolset\services\SessionSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\sfloppy (Administrators [FullControl])
HKLM\system\currentcontrolset\services\SgrmAgent (Administrators [FullControl])
HKLM\system\currentcontrolset\services\SgrmBroker (Administrators [FullControl])
HKLM\system\currentcontrolset\services\SharedAccess (Administrators [FullControl])
HKLM\system\currentcontrolset\services\SharedRealitySvc (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\ShellHWDetection (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\shpamsvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\SiSRaid2 (Administrators [FullControl])
HKLM\system\currentcontrolset\services\SiSRaid4 (Administrators [FullControl])
HKLM\system\currentcontrolset\services\SmartByte Analytics Service (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\SmartByte Network Service x64
(Administrators [FullControl])
HKLM\system\currentcontrolset\services\SmartSAMD (Administrators [FullControl])
HKLM\system\currentcontrolset\services\SmbCoSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\smphost (Administrators [FullControl])
HKLM\system\currentcontrolset\services\SmsRouter (Administrators [FullControl])
HKLM\system\currentcontrolset\services\SMSvcHost 4.0.0.0 (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\SNMPTrap (Administrators [FullControl])
HKLM\system\currentcontrolset\services\spaceparser (Administrators [FullControl])
HKLM\system\currentcontrolset\services\spaceport (Administrators [FullControl])
HKLM\system\currentcontrolset\services\SpatialGraphFilter (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\SpbCx (Administrators [FullControl])
HKLM\system\currentcontrolset\services\spectrum (Administrators [FullControl])
HKLM\system\currentcontrolset\services\Spooler (Administrators [FullControl])
HKLM\system\currentcontrolset\services\sppsvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\SQLWriter (Administrators [FullControl])
HKLM\system\currentcontrolset\services\srv2 (Administrators [FullControl])
HKLM\system\currentcontrolset\services\srvnet (Administrators [FullControl])
HKLM\system\currentcontrolset\services\SSDPSRV (Administrators [FullControl])
HKLM\system\currentcontrolset\services\ssh-agent (Administrators [FullControl])
HKLM\system\currentcontrolset\services\SstpSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\ssudmdm (Administrators [FullControl])
HKLM\system\currentcontrolset\services\StateRepository (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\stexstor (Administrators [FullControl])
HKLM\system\currentcontrolset\services\StiSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\storahci (Administrators [FullControl])
HKLM\system\currentcontrolset\services\storflt (Administrators [FullControl])
HKLM\system\currentcontrolset\services\stornvme (Administrators [FullControl])
HKLM\system\currentcontrolset\services\storqosflt (Administrators [FullControl])
HKLM\system\currentcontrolset\services\StorSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\storufs (Administrators [FullControl])
HKLM\system\currentcontrolset\services\storvsc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\SupportAssistAgent (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\svsvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\swenum (Administrators [FullControl])
HKLM\system\currentcontrolset\services\swprv (Administrators [FullControl])
HKLM\system\currentcontrolset\services\SysMain (Administrators [FullControl])
HKLM\system\currentcontrolset\services\SystemEventsBroker (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\TapiSrv (Administrators [FullControl])
HKLM\system\currentcontrolset\services\TbtP2pShortcutService (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\Tcpip (Administrators [FullControl])
HKLM\system\currentcontrolset\services\Tcpip6 (Administrators [FullControl])
HKLM\system\currentcontrolset\services\TCPIP6TUNNEL (Administrators [FullControl])
HKLM\system\currentcontrolset\services\tcpipreg (Administrators [FullControl])
HKLM\system\currentcontrolset\services\TCPIPTUNNEL (Administrators [FullControl])
```

```
HKLM\system\currentcontrolset\services\tdx (Administrators [FullControl])
HKLM\system\currentcontrolset\services\terminpt (Administrators [FullControl])
HKLM\system\currentcontrolset\services\TermService (Administrators [FullControl])
HKLM\system\currentcontrolset\services\TextInputManagementService (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\Themes (Administrators [FullControl])
HKLM\system\currentcontrolset\services\TieringEngineService (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\TimeBrokerSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\TokenBroker (Administrators [FullControl])
HKLM\system\currentcontrolset\services\TPM (Administrators [FullControl])
HKLM\system\currentcontrolset\services\TroubleshootingSvc (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\TSDDD (Administrators [FullControl])
HKLM\system\currentcontrolset\services\TsUsbFlt (Administrators [FullControl])
HKLM\system\currentcontrolset\services\TsUsbGD (Administrators [FullControl])
HKLM\system\currentcontrolset\services\tunnel (Administrators [FullControl])
HKLM\system\currentcontrolset\services\tzautoupdate (Administrators [FullControl])
HKLM\system\currentcontrolset\services\UASPStor (Administrators [FullControl])
HKLM\system\currentcontrolset\services\UcmCx0101 (Administrators [FullControl])
HKLM\system\currentcontrolset\services\UcmTcpciCx0101 (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\UcmUcsiAcpiClient (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\UcmUcsiCx0101 (Administrators [FullControl])
HKLM\system\currentcontrolset\services\Ucx01000 (Administrators [FullControl])
HKLM\system\currentcontrolset\services\UdeCx (Administrators [FullControl])
HKLM\system\currentcontrolset\services\udfs (Administrators [FullControl])
HKLM\system\currentcontrolset\services\UdkUserSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\UdkUserSvc_1eab96 (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\UEFI (Administrators [FullControl])
HKLM\system\currentcontrolset\services\Ufx01000 (Administrators [FullControl])
HKLM\system\currentcontrolset\services\UfxChipidea (Administrators [FullControl])
HKLM\system\currentcontrolset\services\ufxsynopsys (Administrators [FullControl])
HKLM\system\currentcontrolset\services\UGatherer (Administrators [FullControl])
HKLM\system\currentcontrolset\services\UGTHRSVC (Administrators [FullControl])
HKLM\system\currentcontrolset\services\uhssvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\umbus (Administrators [FullControl])
HKLM\system\currentcontrolset\services\UmPass (Administrators [FullControl])
HKLM\system\currentcontrolset\services\UmRdpService (Administrators [FullControl])
HKLM\system\currentcontrolset\services\UnistoreSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\UnistoreSvc_1eab96 (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\upnphost (Administrators [FullControl])
HKLM\system\currentcontrolset\services\UrsChipidea (Administrators [FullControl])
HKLM\system\currentcontrolset\services\UrsCx01000 (Administrators [FullControl])
HKLM\system\currentcontrolset\services\UrsSynopsys (Administrators [FullControl])
HKLM\system\currentcontrolset\services\Usb4DeviceRouter (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\Usb4HostRouter (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\usbaudio (Administrators [FullControl])
HKLM\system\currentcontrolset\services\usbaudio2 (Administrators [FullControl])
HKLM\system\currentcontrolset\services\usbccgp (Administrators [FullControl])
HKLM\system\currentcontrolset\services\usbcir (Administrators [FullControl])
HKLM\system\currentcontrolset\services\usbehci (Administrators [FullControl])
HKLM\system\currentcontrolset\services\usbhub (Administrators [FullControl])
HKLM\system\currentcontrolset\services\USBHUB3 (Administrators [FullControl])
HKLM\system\currentcontrolset\services\usbohci (Administrators [FullControl])
HKLM\system\currentcontrolset\services\usbprint (Administrators [FullControl])
HKLM\system\currentcontrolset\services\usbser (Administrators [FullControl])
HKLM\system\currentcontrolset\services\USBSTOR (Administrators [FullControl])
HKLM\system\currentcontrolset\services\usbuhci (Administrators [FullControl])
HKLM\system\currentcontrolset\services\usbvideo (Administrators [FullControl])
HKLM\system\currentcontrolset\services\USBXHCI (Administrators [FullControl])
HKLM\system\currentcontrolset\services\UserDataSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\UserDataSvc_1eab96 (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\UserManager (Administrators [FullControl])
HKLM\system\currentcontrolset\services\UsoSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\VacSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\VaultSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\vdrvroot (Administrators [FullControl])
HKLM\system\currentcontrolset\services\vds (Administrators [FullControl])
HKLM\system\currentcontrolset\services\VerifierExt (Administrators [FullControl])
HKLM\system\currentcontrolset\services\vhdmp (Administrators [FullControl])
HKLM\system\currentcontrolset\services\vhf (Administrators [FullControl])
```

```
HKLM\system\currentcontrolset\services\Vid (Administrators [FullControl])
HKLM\system\currentcontrolset\services\VirtualRender (Administrators [FullControl])
HKLM\system\currentcontrolset\services\vmbus (Administrators [FullControl])
HKLM\system\currentcontrolset\services\VMBusHID (Administrators [FullControl])
HKLM\system\currentcontrolset\services\vmgid (Administrators [FullControl])
HKLM\system\currentcontrolset\services\vmicguestinterface (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\vmicheartbeat (Administrators [FullControl])
HKLM\system\currentcontrolset\services\vmickvpexchange (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\vmicrdv (Administrators [FullControl])
HKLM\system\currentcontrolset\services\vmicshutdown (Administrators [FullControl])
HKLM\system\currentcontrolset\services\vmictimesync (Administrators [FullControl])
HKLM\system\currentcontrolset\services\vmicvmsession (Administrators [FullControl])
HKLM\system\currentcontrolset\services\vmicvss (Administrators [FullControl])
HKLM\system\currentcontrolset\services\volmgr (Administrators [FullControl])
HKLM\system\currentcontrolset\services\volmgrx (Administrators [FullControl])
HKLM\system\currentcontrolset\services\volsnap (Administrators [FullControl])
HKLM\system\currentcontrolset\services\volume (Administrators [FullControl])
HKLM\system\currentcontrolset\services\vpci (Administrators [FullControl])
HKLM\system\currentcontrolset\services\vsmraid (Administrators [FullControl])
HKLM\system\currentcontrolset\services\VSS (Administrators [FullControl])
HKLM\system\currentcontrolset\services\VSStandardCollectorService150
(Administrators [FullControl])
HKLM\system\currentcontrolset\services\VSTXRAID (Administrators [FullControl])
HKLM\system\currentcontrolset\services\vwifibus (Administrators [FullControl])
HKLM\system\currentcontrolset\services\vwififlt (Administrators [FullControl])
HKLM\system\currentcontrolset\services\vwifimp (Administrators [FullControl])
HKLM\system\currentcontrolset\services\W32Time (Administrators [FullControl
GenericAll])
HKLM\system\currentcontrolset\services\WaaSMedicSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\WacomPen (Administrators [FullControl])
HKLM\system\currentcontrolset\services\WalletService (Administrators [FullControl])
HKLM\system\currentcontrolset\services\wanarp (Administrators [FullControl])
HKLM\system\currentcontrolset\services\wanarpv6 (Administrators [FullControl])
HKLM\system\currentcontrolset\services\WarpJITSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\WavesAudioService (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\WavesSysSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\wbengine (Administrators [FullControl])
HKLM\system\currentcontrolset\services\WbioSrvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\wcifs (Administrators [FullControl])
HKLM\system\currentcontrolset\services\Wcmsvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\wcncsvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\WdBoot (Administrators [FullControl])
HKLM\system\currentcontrolset\services\WdDevFlt (Administrators [FullControl])
HKLM\system\currentcontrolset\services\Wdf01000 (Administrators [FullControl])
HKLM\system\currentcontrolset\services\WdFilter (Administrators [FullControl])
HKLM\system\currentcontrolset\services\wdiwifi (Administrators [FullControl])
HKLM\system\currentcontrolset\services\WdmCompanionFilter (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\WdNisDrv (Administrators [FullControl])
HKLM\system\currentcontrolset\services\WdNisSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\WebClient (Administrators [FullControl])
HKLM\system\currentcontrolset\services\webthreatdefsvc (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\webthreatdefusersvc (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\webthreatdefusersvc_1eab96 (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\Wecsvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\WEPHOSTSVC (Administrators [FullControl])
HKLM\system\currentcontrolset\services\wercplsupport (Administrators [FullControl])
HKLM\system\currentcontrolset\services\WerSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\WFDSConMgrSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\WFPLWFS (Administrators [FullControl])
HKLM\system\currentcontrolset\services\WiaRpc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\WifiCx (Administrators [FullControl])
HKLM\system\currentcontrolset\services\WiManH (Administrators [FullControl])
HKLM\system\currentcontrolset\services\WIMMount (Administrators [FullControl])
HKLM\system\currentcontrolset\services\WinDefend (Administrators [FullControl])
HKLM\system\currentcontrolset\services\Windows Workflow Foundation 4.0.0.0
(Administrators [FullControl])
HKLM\system\currentcontrolset\services\WindowsTrustedRT (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\WindowsTrustedRTProxy (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\WinHttpAutoProxySvc (Administrators
```

```
[FullControl])
HKLM\system\currentcontrolset\services\WinMad (Administrators [FullControl])
HKLM\system\currentcontrolset\services\Winmgmt (Administrators [GenericAll
FullControl])
HKLM\system\currentcontrolset\services\WinNat (Administrators [FullControl])
HKLM\system\currentcontrolset\services\WinRM (Administrators [FullControl])
HKLM\system\currentcontrolset\services\WinSetupMon (Administrators [FullControl])
HKLM\system\currentcontrolset\services\Winsock (Administrators [FullControl])
HKLM\system\currentcontrolset\services\WinSock2 (Administrators [FullControl])
HKLM\system\currentcontrolset\services\WINUSB (Administrators [FullControl])
HKLM\system\currentcontrolset\services\WinVerbs (Administrators [FullControl])
HKLM\system\currentcontrolset\services\wisvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\WlanSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\wlidsvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\wlpasvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\WManSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\WmiAcpi (Administrators [FullControl])
HKLM\system\currentcontrolset\services\WmiApRpl (Administrators [GenericAll
FullControl])
HKLM\system\currentcontrolset\services\wmiApSrv (Administrators [GenericAll
FullControl])
HKLM\system\currentcontrolset\services\WMIRegistrationService (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\WMPNetworkSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\Wof (Administrators [FullControl])
HKLM\system\currentcontrolset\services\workerdd (Administrators [FullControl])
HKLM\system\currentcontrolset\services\workfolderssvc (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\WpcMonSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\WPDBusEnum (Administrators [FullControl])
HKLM\system\currentcontrolset\services\WpdUpFltr (Administrators [FullControl])
HKLM\system\currentcontrolset\services\WpnService (Administrators [FullControl])
HKLM\system\currentcontrolset\services\WpnUserService (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\WpnUserService_1eab96 (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\ws2ifsl (Administrators [FullControl])
HKLM\system\currentcontrolset\services\WSearch (Administrators [FullControl])
HKLM\system\currentcontrolset\services\WSearchIdxPi (Administrators [FullControl])
HKLM\system\currentcontrolset\services\wtd (Administrators [FullControl])
HKLM\system\currentcontrolset\services\wuauserv (Administrators [FullControl])
HKLM\system\currentcontrolset\services\WudfPf (Administrators [FullControl])
HKLM\system\currentcontrolset\services\WUDFRd (Administrators [FullControl])
HKLM\system\currentcontrolset\services\WUDFWpdFs (Administrators [FullControl])
HKLM\system\currentcontrolset\services\WUDFWpdMtp (Administrators [FullControl])
HKLM\system\currentcontrolset\services\WwanSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\XblAuthManager (Administrators
[FullControl])
HKLM\system\currentcontrolset\services\XblGameSave (Administrators [FullControl])
HKLM\system\currentcontrolset\services\xboxgip (Administrators [FullControl])
HKLM\system\currentcontrolset\services\XboxGipSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\XboxNetApiSvc (Administrators [FullControl])
HKLM\system\currentcontrolset\services\xinputhid (Administrators [FullControl])
HKLM\system\currentcontrolset\services\xmlprov (Administrators [FullControl])
```

# 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](https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#dll-hijacking)

```
(DLL Hijacking) C:\Program Files\Microsoft\jdk-11.0.12.7-hotspot\bin:
Administrators [AllAccess]
(DLL Hijacking) C:\ProgramData\Oracle\Java\javapath: Administrators [AllAccess]
(DLL Hijacking) C:\Program Files\Common Files\Oracle\Java\javapath: Administrators
[AllAccess]
(DLL Hijacking) C:\Program Files (x86)\Common Files\Oracle\Java\javapath:
Administrators [AllAccess]
(DLL Hijacking) C:\Windows\system32: Administrators [WriteData/CreateFiles]
(DLL Hijacking) C:\Windows: Administrators [WriteData/CreateFiles]
(DLL Hijacking) C:\Windows\System32\Wbem: Administrators [WriteData/CreateFiles]
(DLL Hijacking) C:\Windows\System32\WindowsPowerShell\v1.0\: Administrators
[WriteData/CreateFiles]
(DLL Hijacking) C:\Windows\System32\OpenSSH\: Administrators
[WriteData/CreateFiles]
```

```
(DLL Hijacking) C:\Program Files\dotnet\: Administrators [AllAccess]
(DLL Hijacking) C:\Program Files\Microsoft SQL Server\150\Tools\Binn\:
Administrators [AllAccess]
(DLL Hijacking) C:\Program Files\nodejs\: Administrators [AllAccess]
(DLL Hijacking) C:\Program Files\Git\cmd: Administrators [AllAccess]
(DLL Hijacking) C:\WINDOWS\system32: Administrators [WriteData/CreateFiles]
(DLL Hijacking) C:\WINDOWS: Administrators [WriteData/CreateFiles]
(DLL Hijacking) C:\WINDOWS\System32\Wbem: Administrators [WriteData/CreateFiles]
(DLL Hijacking) C:\WINDOWS\System32\WindowsPowerShell\v1.0\: Administrators
[WriteData/CreateFiles]
(DLL Hijacking) C:\WINDOWS\System32\OpenSSH\: Administrators
[WriteData/CreateFiles]
(DLL Hijacking) C:\Program Files\Amazon\AWSCLIV2\: Administrators [AllAccess]
(DLL Hijacking) C:\Program Files\Amazon\AWSCLI\bin\: Administrators [AllAccess]
```

# 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)\Intel\Intel(R) Management Engine Components(Administrators
[AllAccess])
C:\Program Files (x86)\Microsoft Visual Studio\Installer(Administrators
[AllAccess])
C:\Program Files\Amazon(Administrators [AllAccess])
C:\Program Files\Android(Administrators [AllAccess])
C:\Program Files\Application Verifier(Administrators [AllAccess])
C:\Program Files\Common Files(Administrators [WriteData/CreateFiles])
C:\Program Files\Dell(Administrators [AllAccess])
C:\Program Files\desktop.ini(Administrators [AllAccess])
C:\Program Files\dotnet(Administrators [AllAccess])
C:\Program Files\Git(Administrators [AllAccess])
C:\Program Files\Google(Administrators [AllAccess])
C:\Program Files\IIS Express(Administrators [AllAccess])
C:\Program Files\Intel(Administrators [AllAccess])
C:\Program Files\Internet Explorer(Administrators [WriteData/CreateFiles])
C:\Program Files\Java(Administrators [AllAccess])
C:\Program Files\Maven(Administrators [AllAccess])
C:\Program Files\McAfee(Administrators [AllAccess])
C:\Program Files\McAfee.com(Administrators [AllAccess])
C:\Program Files\Microsoft(Administrators [AllAccess])
C:\Program Files\Microsoft Office(Administrators [AllAccess])
C:\Program Files\Microsoft Office 15(Administrators [AllAccess])
C:\Program Files\Microsoft OneDrive(Administrators [AllAccess])
C:\Program Files\Microsoft SQL Server(Administrators [AllAccess])
C:\Program Files\Microsoft Update Health Tools(Administrators [AllAccess])
C:\Program Files\Microsoft Visual Studio(Administrators [AllAccess])
C:\Program Files\ModifiableWindowsApps
C:\Program Files\MySQL(Administrators [AllAccess])
C:\Program Files\nodejs(Administrators [AllAccess])
C:\Program Files\Npcap(Administrators [AllAccess])
C:\Program Files\Python310(Administrators [AllAccess])
C:\Program Files\Rivet Networks(Administrators [AllAccess])
C:\Program Files\Sublime Text 3(Administrators [AllAccess], snehj [AllAccess])
C:\Program Files\Uninstall Information(Administrators [AllAccess])
C:\Program Files\Waves(Administrators [AllAccess])
C:\Program Files\Windows Defender(Administrators [WriteData/CreateFiles])
C:\Program Files\Windows Mail(Administrators [WriteData/CreateFiles])
C:\Program Files\Windows Media Player(Administrators [WriteData/CreateFiles])
C:\Program Files\Windows NT(Administrators [WriteData/CreateFiles])
C:\Program Files\Windows Photo Viewer(Administrators [WriteData/CreateFiles])
C:\Program Files\Windows Sidebar(Administrators [WriteData/CreateFiles])
C:\Program Files\WindowsApps
C:\Program Files\WindowsPowerShell(Administrators [WriteData/CreateFiles])
```

## 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
RegPerms: Administrators [FullControl GenericAll]
Key: SecurityHealth
Folder: C:\WINDOWS\system32
FolderPerms: Administrators [WriteData/CreateFiles]
File: C:\WINDOWS\system32\SecurityHealthSystray.exe
================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows\CurrentVersion\Run
RegPerms: Administrators [FullControl GenericAll]
Key: RtkAudUService
Folder: C:\WINDOWS\System32\DriverStore\FileRepository\realtekservice.inf_amd64_44
4148fa7298b49f
File: C:\WINDOWS\System32\DriverStore\FileRepository\realtekservice.inf_amd64_4441
48fa7298b49f\RtkAudUService64.exe -background
================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows\CurrentVersion\Run
RegPerms: Administrators [FullControl GenericAll]
Key: WavesSvc
Folder: C:\WINDOWS\System32\DriverStore\FileRepository\wavesapo10de.inf_amd64_f737
3b847419c8d1
File: C:\WINDOWS\System32\DriverStore\FileRepository\wavesapo10de.inf_amd64_f7373b
847419c8d1\WavesSvc64.exe -Jack
================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
RegPerms: Administrators [FullControl GenericAll]
Key: Delete Cached Update Binary
Folder: C:\WINDOWS\system32\cmd.exe\q\c del
FolderPerms: Administrators [WriteData/CreateFiles]
File: C:\WINDOWS\system32\cmd.exe /q /c del /q C:\Program Files\Microsoft
OneDrive\Update\OneDriveSetup.exe (Unquoted and Space detected)
================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
RegPerms: Administrators [FullControl GenericAll]
Key: Delete Cached Standalone Update Binary
Folder: C:\WINDOWS\system32\cmd.exe\q\c del
FolderPerms: Administrators [WriteData/CreateFiles]
File: C:\WINDOWS\system32\cmd.exe /q /c del /q C:\Program Files\Microsoft
OneDrive\StandaloneUpdater\OneDriveSetup.exe (Unquoted and Space detected)
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run
RegPerms: Administrators [FullControl GenericAll]
Key: SunJavaUpdateSched
Folder: C:\Program Files (x86)\Common Files\Java\Java Update
FolderPerms: Administrators [AllAccess]
File: C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe (Unquoted
and Space detected)
FilePerms: Administrators [AllAccess]
================================================================================
===============
RegPath: HKCU\Software\Microsoft\Windows\CurrentVersion\Run
RegPerms: snehj [FullControl], Administrators [FullControl]
Key: OneDrive
Folder: C:\Program Files\Microsoft OneDrive
FolderPerms: Administrators [AllAccess]
File: C:\Program Files\Microsoft OneDrive\OneDrive.exe /background (Unquoted and
Space detected)
FilePerms: Administrators [AllAccess]
================================================================================
===============
RegPath: HKCU\Software\Microsoft\Windows\CurrentVersion\Run
RegPerms: snehj [FullControl], Administrators [FullControl]
Key: MicrosoftEdgeAutoLaunch_8E71C056100E63E5636653030AABB799
Folder: C:\Program Files (x86)\Microsoft\Edge\Application
FolderPerms: Administrators [AllAccess]
File: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
--no-startup-window --win-session-start /prefetch:5 (Unquoted and Space detected)
```

```
FilePerms: Administrators [AllAccess]
========================================================================
===============
RegPath: HKCU\Software\Microsoft\Windows\CurrentVersion\Run
RegPerms: snehj [FullControl], Administrators [FullControl]
Key: Grammarly
Folder: C:\Users\snehj\AppData\Local\Grammarly\DesktopIntegrations
FolderPerms: Administrators [AllAccess], snehj [AllAccess]
File:
C:\Users\snehj\AppData\Local\Grammarly\DesktopIntegrations\Grammarly.Desktop.exe
========================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
RegPerms: Administrators [FullControl GenericAll]
Key: Common Startup
Folder: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
FolderPerms: snehj [Delete], Administrators [AllAccess] (Unquoted and Space
detected)
========================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
RegPerms: Administrators [GenericAll FullControl]
Key: Common Startup
Folder: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
FolderPerms: snehj [Delete], Administrators [AllAccess] (Unquoted and Space
detected)
========================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
RegPerms: Administrators [FullControl GenericAll]
Key: Userinit
Folder: C:\Windows\system32
FolderPerms: Administrators [WriteData/CreateFiles]
File: C:\Windows\system32\userinit.exe,
========================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
RegPerms: Administrators [FullControl GenericAll]
Key: Shell
Folder: None (PATH Injection)
File: explorer.exe
========================================================================
===============
RegPath: HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot
RegPerms: Administrators [FullControl]
Key: AlternateShell
Folder: None (PATH Injection)
File: cmd.exe
========================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Font Drivers
RegPerms: Administrators [FullControl GenericAll]
Key: Adobe Type Manager
Folder: None (PATH Injection)
File: atmfd.dll
========================================================================
===============
RegPath: HKLM\Software\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Font Drivers
RegPerms: Administrators [FullControl GenericAll]
Key: Adobe Type Manager
Folder: None (PATH Injection)
File: atmfd.dll
========================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: aux
Folder: None (PATH Injection)
File: wdmaud.drv
========================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: midi
Folder: None (PATH Injection)
File: wdmaud.drv
========================================================================
===============
```

```
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: midimapper
Folder: None (PATH Injection)
File: midimap.dll
================================================================================
==============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: mixer
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
==============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: msacm.imaadpcm
Folder: None (PATH Injection)
File: imaadp32.acm
================================================================================
==============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: msacm.msadpcm
Folder: None (PATH Injection)
File: msadp32.acm
================================================================================
==============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: msacm.msg711
Folder: None (PATH Injection)
File: msg711.acm
================================================================================
==============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: msacm.msgsm610
Folder: None (PATH Injection)
File: msgsm32.acm
================================================================================
==============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: vidc.i420
Folder: None (PATH Injection)
File: iyuv_32.dll
================================================================================
==============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: vidc.iyuv
Folder: None (PATH Injection)
File: iyuv_32.dll
================================================================================
==============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: vidc.mrle
Folder: None (PATH Injection)
File: msrle32.dll
================================================================================
==============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: vidc.msvc
Folder: None (PATH Injection)
File: msvidc32.dll
================================================================================
==============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: vidc.uyvy
Folder: None (PATH Injection)
File: msyuv.dll
================================================================================
==============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
```

```
RegPerms: Administrators [FullControl GenericAll]
Key: vidc.yuy2
Folder: None (PATH Injection)
File: msyuv.dll
================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: vidc.yvu9
Folder: None (PATH Injection)
File: tsbyuv.dll
================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: vidc.yvyu
Folder: None (PATH Injection)
File: msyuv.dll
================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: wave
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: wavemapper
Folder: None (PATH Injection)
File: msacm32.drv
================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: msacm.l3acm
Folder: C:\Windows\System32
FolderPerms: Administrators [WriteData/CreateFiles]
File: C:\Windows\System32\l3codeca.acm
================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: MSVideo8
Folder: None (PATH Injection)
File: VfWWDM32.dll
================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: aux2
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: midi2
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: mixer2
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: wave2
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
```

```
RegPerms: Administrators [FullControl GenericAll]
Key: aux3
Folder: None (PATH Injection)
File: wdmaud.drv
=================================================================120========================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: midi3
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: mixer3
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: wave3
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: aux1
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: midi1
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: mixer1
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: wave1
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: aux4
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: midi4
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: mixer4
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
```

```
Key: wave4
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: aux
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: midi
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: midimapper
Folder: None (PATH Injection)
File: midimap.dll
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: mixer
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: msacm.imaadpcm
Folder: None (PATH Injection)
File: imaadp32.acm
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: msacm.msadpcm
Folder: None (PATH Injection)
File: msadp32.acm
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: msacm.msg711
Folder: None (PATH Injection)
File: msg711.acm
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: msacm.msgsm610
Folder: None (PATH Injection)
File: msgsm32.acm
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: vidc.cvid
Folder: None (PATH Injection)
File: iccvid.dll
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: vidc.i420
Folder: None (PATH Injection)
File: iyuv_32.dll
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: vidc.iyuv
```

```
Folder: None (PATH Injection)
File: iyuv_32.dll
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: vidc.mrle
Folder: None (PATH Injection)
File: msrle32.dll
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: vidc.msvc
Folder: None (PATH Injection)
File: msvidc32.dll
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: vidc.uyvy
Folder: None (PATH Injection)
File: msyuv.dll
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: vidc.yuy2
Folder: None (PATH Injection)
File: msyuv.dll
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: vidc.yvu9
Folder: None (PATH Injection)
File: tsbyuv.dll
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: vidc.yvyu
Folder: None (PATH Injection)
File: msyuv.dll
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: wave
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: wavemapper
Folder: None (PATH Injection)
File: msacm32.drv
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: msacm.l3acm
Folder: C:\Windows\SysWOW64
FolderPerms: Administrators [WriteData/CreateFiles]
File: C:\Windows\SysWOW64\l3codeca.acm
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: aux2
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: midi2
```

```
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: mixer2
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: wave2
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: aux3
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: midi3
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: mixer3
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: wave3
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: aux1
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: midi1
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: mixer1
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: wave1
Folder: None (PATH Injection)
File: wdmaud.drv
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: aux4
Folder: None (PATH Injection)
```

```
File: wdmaud.drv
=============================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: midi4
Folder: None (PATH Injection)
File: wdmaud.drv
=============================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: mixer4
Folder: None (PATH Injection)
File: wdmaud.drv
=============================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
RegPerms: Administrators [FullControl GenericAll]
Key: wave4
Folder: None (PATH Injection)
File: wdmaud.drv
=============================================================================
===============
RegPath: HKLM\Software\Classes\htmlfile\shell\open\command
RegPerms: Administrators [FullControl GenericAll]
Folder: C:\Program Files\Internet Explorer
FolderPerms: Administrators [WriteData/CreateFiles]
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}
RegPerms: Administrators [FullControl]
Key: StubPath
Folder: \
FolderPerms: Authenticated Users [AppendData/CreateDirectories], Administrators
[AllAccess]
File: /UserInstall
================================================================================
===============
RegPath: HKLM\Software\Microsoft\Active Setup\Installed
Components\{6BF52A52-394A-11d3-B153-00C04F79FAA6}
RegPerms: Administrators [FullControl]
Key: StubPath
Folder: C:\WINDOWS\system32
FolderPerms: Administrators [WriteData/CreateFiles]
File: C:\WINDOWS\system32\unregmp2.exe /FirstLogon
================================================================================
===============
RegPath: HKLM\Software\Microsoft\Active Setup\Installed
Components\{89820200-ECBD-11cf-8B85-00AA005B4340}
RegPerms: Administrators [FullControl]
Key: StubPath
Folder: None (PATH Injection)
File: U
================================================================================
===============
RegPath: HKLM\Software\Microsoft\Active Setup\Installed
Components\{89820200-ECBD-11cf-8B85-00AA005B4383}
RegPerms: Administrators [FullControl]
Key: StubPath
Folder: C:\Windows\System32
FolderPerms: Administrators [WriteData/CreateFiles]
File: C:\Windows\System32\ie4uinit.exe -UserConfig
================================================================================
===============
RegPath: HKLM\Software\Microsoft\Active Setup\Installed
Components\{89B4C1CD-B018-4511-B0A1-5476DBF70820}
RegPerms: Administrators [FullControl]
Key: StubPath
Folder: C:\Windows\System32
FolderPerms: Administrators [WriteData/CreateFiles]
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}
RegPerms: Administrators [FullControl]
Key: StubPath
Folder: C:\Program Files\Google\Chrome\Application\114.0.5735.248\Installer
FolderPerms: Administrators [AllAccess]
File: C:\Program
Files\Google\Chrome\Application\114.0.5735.248\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}
RegPerms: Administrators [FullControl]
Key: StubPath
Folder: C:\Program Files (x86)\Microsoft\Edge\Application\115.0.1901.183\Installer
FolderPerms: Administrators [AllAccess]
File: C:\Program Files
(x86)\Microsoft\Edge\Application\115.0.1901.183\Installer\setup.exe
--configure-user-settings --verbose-logging --system-level --msedge
--channel=stable (Unquoted and Space detected)
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Active Setup\Installed
```

```
Components\{6BF52A52-394A-11d3-B153-00C04F79FAA6}
RegPerms: Administrators [FullControl]
Key: StubPath
Folder: C:\WINDOWS\system32
FolderPerms: Administrators [WriteData/CreateFiles]
File: C:\WINDOWS\system32\unregmp2.exe /FirstLogon
================================================================================
===============
RegPath: HKLM\Software\Wow6432Node\Microsoft\Active Setup\Installed
Components\{89B4C1CD-B018-4511-B0A1-5476DBF70820}
RegPerms: Administrators [FullControl]
Key: StubPath
Folder: C:\Windows\SysWOW64
FolderPerms: Administrators [WriteData/CreateFiles]
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}
RegPerms: Administrators [FullControl GenericAll]
Folder: C:\Program Files (x86)\Microsoft\Edge\Application\115.0.1901.183\BHO
FolderPerms: Administrators [AllAccess]
File: C:\Program Files
(x86)\Microsoft\Edge\Application\115.0.1901.183\BHO\ie_to_edge_bho_64.dll (Unquoted
and Space detected)
================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper
Objects\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}
RegPerms: Administrators [FullControl GenericAll]
Folder: C:\Program Files\Java\jre1.8.0_361\bin
FolderPerms: Administrators [AllAccess]
File: C:\Program Files\Java\jre1.8.0_361\bin\ssv.dll (Unquoted and Space detected)
================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper
Objects\{B164E929-A1B6-4A06-B104-2CD0E90A88FF}
RegPerms: Administrators [FullControl GenericAll]
Folder: C:\Program Files\McAfee\WebAdvisor\x64
FolderPerms: Administrators [AllAccess]
File: C:\Program Files\McAfee\WebAdvisor\x64\IEPlugin.dll (Unquoted and Space
detected)
FilePerms: Administrators [AllAccess]
================================================================================
===============
RegPath: HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper
Objects\{DBC80044-A445-435b-BC74-9C25C1C588A9}
RegPerms: Administrators [FullControl GenericAll]
Folder: C:\Program Files\Java\jre1.8.0_361\bin
FolderPerms: Administrators [AllAccess]
File: C:\Program Files\Java\jre1.8.0_361\bin\jp2ssv.dll (Unquoted and Space
detected)
================================================================================
===============
RegPath:
HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper
Objects\{1FD49718-1D00-4B19-AF5F-070AF6D5D54C}
RegPerms: Administrators [FullControl GenericAll]
Folder: C:\Program Files (x86)\Microsoft\Edge\Application\115.0.1901.183\BHO
FolderPerms: Administrators [AllAccess]
File: C:\Program Files
(x86)\Microsoft\Edge\Application\115.0.1901.183\BHO\ie_to_edge_bho_64.dll (Unquoted
and Space detected)
================================================================================
===============
RegPath:
HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper
Objects\{B164E929-A1B6-4A06-B104-2CD0E90A88FF}
RegPerms: Administrators [FullControl GenericAll]
Folder: C:\Program Files\McAfee\WebAdvisor\x64
FolderPerms: Administrators [AllAccess]
File: C:\Program Files\McAfee\WebAdvisor\x64\IEPlugin.dll (Unquoted and Space
detected)
FilePerms: Administrators [AllAccess]
================================================================================
===============
Folder: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
FolderPerms: snehj [Delete], Administrators [AllAccess]
File: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini
```

```
(Unquoted and Space detected)
FilePerms: Administrators [AllAccess], snehj [Delete]
================================================================================
===============
Folder: C:\Users\snehj\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup
FolderPerms: Administrators [AllAccess], snehj [AllAccess]
File: C:\Users\snehj\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup\desktop.ini (Unquoted and Space detected)
FilePerms: Administrators [AllAccess], snehj [AllAccess]
================================================================================
===============
Folder: C:\windows\tasks
FolderPerms: Authenticated Users [WriteData/CreateFiles], Administrators
[AllAccess]
================================================================================
===============
Folder: C:\windows\system32\tasks
FolderPerms: Authenticated Users [WriteData/CreateFiles], Administrators
[AllAccess]
================================================================================
===============
Folder: C:\windows
FolderPerms: Administrators [WriteData/CreateFiles]
File: C:\windows\system.ini
FilePerms: Administrators [AllAccess]
================================================================================
===============
Folder: C:\windows
FolderPerms: Administrators [WriteData/CreateFiles]
File: C:\windows\win.ini
FilePerms: Administrators [AllAccess]
================================================================================
===============
Key: From WMIC
Folder: C:\Windows\System32
FolderPerms: Administrators [WriteData/CreateFiles]
File: C:\Windows\System32\OneDriveSetup.exe /thfirstsetup (Unquoted and Space
detected)
================================================================================
===============
Key: From WMIC
Folder: C:\Windows\System32
FolderPerms: Administrators [WriteData/CreateFiles]
File: C:\Windows\System32\OneDriveSetup.exe /thfirstsetup (Unquoted and Space
detected)
================================================================================
===============
Key: From WMIC
Folder: C:\Program Files\Microsoft OneDrive
FolderPerms: Administrators [AllAccess]
File: C:\Program Files\Microsoft OneDrive\OneDrive.exe /background
FilePerms: Administrators [AllAccess]
================================================================================
===============
Key: From WMIC
Folder: C:\Program Files (x86)\Microsoft\Edge\Application
FolderPerms: Administrators [AllAccess]
File: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
--no-startup-window --win-session-start /prefetch:5
FilePerms: Administrators [AllAccess]
================================================================================
===============
Key: From WMIC
Folder: C:\Users\snehj\AppData\Local\Grammarly\DesktopIntegrations
FolderPerms: Administrators [AllAccess], snehj [AllAccess]
File:
C:\Users\snehj\AppData\Local\Grammarly\DesktopIntegrations\Grammarly.Desktop.exe
================================================================================
===============
Key: From WMIC
Folder: C:\WINDOWS\system32
FolderPerms: Administrators [WriteData/CreateFiles]
File: C:\WINDOWS\system32\SecurityHealthSystray.exe
================================================================================
===============
Key: From WMIC
Folder: C:\WINDOWS\System32\DriverStore\FileRepository\realtekservice.inf_amd64_44
4148fa7298b49f
```

```
File: C:\WINDOWS\System32\DriverStore\FileRepository\realtekservice.inf_amd64_4441
48fa7298b49f\RtkAudUService64.exe -background
================================================================================
==============
Key: From WMIC
Folder: C:\WINDOWS\System32\DriverStore\FileRepository\wavesapo10de.inf_amd64_f737
3b847419c8d1
File: C:\WINDOWS\System32\DriverStore\FileRepository\wavesapo10de.inf_amd64_f7373b
847419c8d1\WavesSvc64.exe -Jack
================================================================================
==============
```

## Scheduled Applications --Non Microsoft--

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

```
(Dell, Inc.) Dell SupportAssistAgent AutoUpdate: C:\Program
Files\Dell\SupportAssistAgent\bin\FrameworkAgents\SupportAssistInstaller.exe
AutoUpdate
Permissions file: Administrators [AllAccess]
Permissions folder(DLL Hijacking): Administrators [AllAccess]
Trigger: At 12:03 every Wednesday of every week, starting 31-05-2023
================================================================================
==============
(McAfee) McAfee Remediation (Prepare): C:\Program Files\Common Files\AV\McAfee
VirusScan\upgrade.exe /prepare
Permissions file: Administrators [AllAccess]
Permissions folder(DLL Hijacking): Administrators [AllAccess]
Trigger: When the task is created or modified-After triggered, repeat every
1.00:00:00 indefinitely.
================================================================================
==============
(McAfee) McAfeeLogon: C:\Program Files\Common Files\McAfee\Platform\McUICnt.exe
/platui
Permissions file: Administrators [AllAccess]
Permissions folder(DLL Hijacking): Administrators [AllAccess]
Trigger: At log on of any user
================================================================================
==============
(Rivet Networks) SmartByte Telemetry: "C:\Program Files\Rivet
Networks\SmartByte\SmartByteTelemetry.exe"
Permissions file: Administrators [AllAccess]
Permissions folder(DLL Hijacking): Administrators [AllAccess]
Trigger: At log on of any user
================================================================================
==============
(McAfee) DAD.Execute.Updates: "C:\Program Files\Common
Files\McAfee\DynamicAppDownloader\DADUpdater.exe"
Permissions file: Administrators [AllAccess]
Permissions folder(DLL Hijacking): Administrators [AllAccess]
Trigger: At 10:22 every day
Custom event filter
================================================================================
==============
(McAfee) McAfee Auto Maintenance Task Agent: McAMTaskAgent Class
(abceca3b-ea5a-496b-a021-5c6bab365e5c)
================================================================================
==============
```

## Device Drivers --Non Microsoft--

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

```
Intel(R) Rapid Storage Technology driver - 18.7.6.1010 [Intel Corporation]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\iaStorVD.sys
SYSCORE - 22.12.0.279 [Trellix US LLC.]:
\\.\GLOBALROOT\SystemRoot\system32\drivers\mfehidk.sys
```

```
SYSCORE - 22.12.0.279 [Trellix US LLC.]:
\\.\GLOBALROOT\SystemRoot\system32\drivers\mfewfpk.sys
Npcap - 1.75 [Insecure.Com LLC.]:
\\.\GLOBALROOT\SystemRoot\system32\DRIVERS\npcap.sys
Intel HD Graphics Drivers for Windows(R) - 31.0.101.3616 [Intel Corporation]: \\.\
GLOBALROOT\SystemRoot\System32\DriverStore\FileRepository\iigd_dch.inf_amd64_8a432
3c80a901a5c\igdkmdn64.sys
Thunderbolt(TM) Bus Driver - 9d3f5f097e6b1d487e3467b2ad4816e85b81621e [Intel
Corporation]: \\.\GLOBALROOT\SystemRoot\System32\drivers\TbtBusDrv.sys
ISS - 3.1.0.4477 [Intel]: \\.\GLOBALROOT\SystemRoot\System32\DriverStore\FileRepos
itory\ish.inf_amd64_2aeb613a4759eb99\ISH.sys
Intel(R) Serial IO Driver - 30.100.2104.1 [Intel Corporation]: \\.\GLOBALROOT\Syst
emRoot\System32\DriverStore\FileRepository\ialpss2_i2c_tgl.inf_amd64_312c301472918
6bd\iaLPSS2_I2C_TGL.sys
Intel(R) Management Engine Interface - 2211.2.3.0 [Intel Corporation]: \\.\GLOBALR
OOT\SystemRoot\System32\DriverStore\FileRepository\heci.inf_amd64_b3a92646bfdb3e11
\x64\TeeDriverW10x64.sys
Intel(R) Dynamic Tuning - 8.7.10600.20700 [Intel Corporation]: \\.\GLOBALROOT\Syst
emRoot\System32\DriverStore\FileRepository\dptf_acpi.inf_amd64_d1c42ae92fd1696b\dp
tf_acpi.sys
Intel(R) Smart Sound Technology BUS - 10.29.00.8276 [Intel(R) Corporation]: \\.\GL
OBALROOT\SystemRoot\System32\DriverStore\FileRepository\intcaudiobus.inf_amd64_570
c508944c60bf9\IntcAudioBus.sys
Intel(R) Serial IO Driver - 30.100.2104.1 [Intel Corporation]: \\.\GLOBALROOT\Syst
emRoot\System32\DriverStore\FileRepository\ialpss2_gpio2_tgl.inf_amd64_c330c09d72f
3e083\iaLPSS2_GPIO2_TGL.sys
Intel(R) HID Event Filter - 2.2.1.384 [Intel Corporation]: \\.\GLOBALROOT\SystemRo
ot\System32\DriverStore\FileRepository\hideventfilter.inf_amd64_010863cba57434d0\H
idEventFilter.sys
Intelr Wireless Manageability - 99.0.61.2 [Intel Corporation]: \\.\GLOBALROOT\Syst
emRoot\System32\DriverStore\FileRepository\wiman.inf_amd64_f54d0a27ac206b8c\WiManH
\WiManH.sys
Intel(R) Smart Sound Technology OED - 10.29.00.8276 [Intel(R) Corporation]: \\.\GL
OBALROOT\SystemRoot\System32\DriverStore\FileRepository\intcoed.inf_amd64_c34ea2dc
251566b0\IntcOED.sys
Realtek(r) High Definition Audio Function Driver - 6.0.9511.1 [Realtek
Semiconductor Corp.]: \\.\GLOBALROOT\SystemRoot\system32\drivers\RTKVHD64.sys
Intel(R) Smart Sound Technology for USB Audio - 10.29.00.8276 [Intel(R)
Corporation]: \\.\GLOBALROOT\SystemRoot\System32\DriverStore\FileRepository\intcus
b.inf_amd64_3d2eead2a9269bdf\IntcUSB.sys
Intel(R) Smart Sound Technology for Digital Microphones - 10.29.00.8276 [Intel(R)
Corporation]: \\.\GLOBALROOT\SystemRoot\System32\DriverStore\FileRepository\intcdm
ic.inf_amd64_6aba8b7eccecb981\IntcDMic.sys
ISS - 3.1.0.4477 [Intel]: \\.\GLOBALROOT\SystemRoot\System32\DriverStore\FileRepos
itory\ish_busdriver.inf_amd64_7d0487ed174b295f\ISH_BusDriver.sys
Intel(R) Wireless Bluetooth(R) - PHBTW5134 [Intel Corporation]: \\.\GLOBALROOT\Sys
temRoot\System32\DriverStore\FileRepository\ibtusb.inf_amd64_58342f0d15e5ce8a\ibtu
sb.sys
ISS - 3.1.0.4477 [Intel]: \\.\GLOBALROOT\SystemRoot\System32\DriverStore\FileRepos
itory\hid_pci.inf_amd64_8a8b0a6c84123637\HID_PCI.sys
SYSCORE - 22.12.0.279 [Trellix US LLC.]:
\\.\GLOBALROOT\SystemRoot\system32\drivers\mfeaack.sys
SYSCORE - 22.12.0.279 [Trellix US LLC.]:
\\.\GLOBALROOT\SystemRoot\system32\drivers\mfeplk.sys
SYSCORE - 22.12.0.279 [Trellix US LLC.]:
\\.\GLOBALROOT\SystemRoot\system32\drivers\mfeavfk.sys
SYSCORE - 22.12.0.279 [Trellix US LLC.]:
\\.\GLOBALROOT\SystemRoot\system32\drivers\mfefirek.sys
Anti-Malware Core - 22.12.0 [Trellix US LLC.]:
\\.\GLOBALROOT\SystemRoot\system32\DRIVERS\mfencbdc.sys
Intel(R) Dynamic Tuning - 8.7.10600.20700 [Intel Corporation]: \\.\GLOBALROOT\Syst
emRoot\System32\DriverStore\FileRepository\dptf_cpu.inf_amd64_1da48d5885266bb7\dpt
f_cpu.sys
Intel(R) Dynamic Tuning - 8.7.10600.20700 [Intel Corporation]: \\.\GLOBALROOT\Syst
emRoot\System32\DriverStore\FileRepository\dptf_cpu.inf_amd64_1da48d5885266bb7\esi
f_lf.sys
HAXM - 7.6.5 [Intel Corporation]: C:\Windows\system32\drivers\IntelHaxm.sys
Permissions file: Administrators [AllAccess]
Permissions folder(DLL Hijacking): Administrators [WriteData/CreateFiles]
================================================================================
===============
SmartByte Traffic Control - 9.8.4.10 [Rivet Networks, LLC.]:
\\.\GLOBALROOT\SystemRoot\system32\DRIVERS\SmbCo10X64.sys
SYSCORE - 22.12.0.279 [Trellix US LLC.]:
\\.\GLOBALROOT\SystemRoot\system32\drivers\cfwids.sys
Intelr Wireless WiFi Link Adapter - 22.170.2.1 [Intel Corporation]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\Netwtw10.sys
```

# Network Information

## Network Shares

```
ADMIN$ (Path: C:\WINDOWS)
C$ (Path: C:\)
IPC$ (Path: )
```

## Network Ifaces and known hosts

*The masks are only for the IPv4 addresses*

```
Local Area Connection* 1[AC:74:B1:A4:0D:A9]: 169.254.66.183,
fe80::5ab0:5dbe:4eeb:8fac%17 / 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:
224.0.0.22 01-00-5E-00-00-16 Static
Local Area Connection* 2[AE:74:B1:A4:0D:A8]: 169.254.136.251,
fe80::cdcc:d5a4:f666:6f8c%3 / 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:
224.0.0.22 01-00-5E-00-00-16 Static
Wi-Fi[AC:74:B1:A4:0D:A8]: 192.168.0.101, fe80::8679:587d:73d5:246a%18 /
255.255.255.0
Gateways: 192.168.0.1
DNSs: 192.168.0.1, 0.0.0.0
Known hosts:
100.127.0.1 00-00-00-00-00-00 Invalid
172.16.3.1 00-00-00-00-00-00 Invalid
172.16.8.1 00-00-00-00-00-00 Invalid
172.16.8.100 00-00-00-00-00-00 Invalid
172.20.10.1 00-00-00-00-00-00 Invalid
192.168.0.1 C0-06-C3-1F-CC-3B Dynamic
192.168.0.102 AC-B6-87-F0-D2-D2 Dynamic
192.168.0.255 FF-FF-FF-FF-FF-FF Static
192.168.1.1 60-A4-B7-F8-8E-E1 Dynamic
192.168.17.97 00-00-00-00-00-00 Invalid
192.168.43.1 00-00-00-00-00-00 Invalid
192.168.52.90 00-00-00-00-00-00 Invalid
192.168.149.77 00-00-00-00-00-00 Invalid
192.168.168.67 00-00-00-00-00-00 Invalid
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
Bluetooth Network Connection[AC:74:B1:A4:0D:AC]: 169.254.2.201,
fe80::f623:da4e:fa32:790e%5 / 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:
224.0.0.22 01-00-5E-00-00-16 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
224.0.0.231 00-00-00-00-00-00 Static
224.0.1.60 00-00-00-00-00-00 Static
239.192.152.143 00-00-00-00-00-00 Static
239.255.102.18 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 1456 C:\WINDOWS\system32\svchost.exe
TCP 0.0.0.0 445 0.0.0.0 0 Listening 4 System
TCP 0.0.0.0 3306 0.0.0.0 0 Listening 4628 C:\Program Files\MySQL\MySQL Server
8.0\bin\mysqld.exe
TCP 0.0.0.0 5040 0.0.0.0 0 Listening 10988 C:\WINDOWS\system32\svchost.exe
TCP 0.0.0.0 6646 0.0.0.0 0 Listening 7700 C:\Program Files\Common
Files\McAfee\MMSSHost\MMSSHOST.EXE
TCP 0.0.0.0 33060 0.0.0.0 0 Listening 4628 C:\Program Files\MySQL\MySQL Server
8.0\bin\mysqld.exe
TCP 0.0.0.0 49664 0.0.0.0 0 Listening 1088 C:\WINDOWS\system32\lsass.exe
TCP 0.0.0.0 49665 0.0.0.0 0 Listening 788 wininit
TCP 0.0.0.0 49666 0.0.0.0 0 Listening 2576 C:\WINDOWS\System32\svchost.exe
TCP 0.0.0.0 49667 0.0.0.0 0 Listening 2964 C:\WINDOWS\system32\svchost.exe
TCP 0.0.0.0 49668 0.0.0.0 0 Listening 3492 C:\WINDOWS\System32\spoolsv.exe
TCP 0.0.0.0 49675 0.0.0.0 0 Listening 1064 services
TCP 127.0.0.1 1123 0.0.0.0 0 Listening 16544 c:\Users\snehj\AppData\Roaming\Code\U
ser\globalStorage\tabnine.tabnine-vscode\binaries\4.5.22\x86_64-pc-windows-gnu\Tab
Nine.exe
TCP 127.0.0.1 8884 0.0.0.0 0 Listening 4 System
TCP 127.0.0.1 11724 127.0.0.1 49152 Established 16544 c:\Users\snehj\AppData\Roami
ng\Code\User\globalStorage\tabnine.tabnine-vscode\binaries\4.5.22\x86_64-pc-window
s-gnu\TabNine.exe
TCP 127.0.0.1 33629 127.0.0.1 49152 Established 16544 c:\Users\snehj\AppData\Roami
ng\Code\User\globalStorage\tabnine.tabnine-vscode\binaries\4.5.22\x86_64-pc-window
s-gnu\TabNine.exe
TCP 127.0.0.1 49152 0.0.0.0 0 Listening 6616 c:\Users\snehj\AppData\Roaming\Code\U
ser\globalStorage\tabnine.tabnine-vscode\binaries\4.5.22\x86_64-pc-windows-gnu\Tab
Nine-deep-local.exe
TCP 127.0.0.1 49152 127.0.0.1 11724 Established 6616 c:\Users\snehj\AppData\Roamin
g\Code\User\globalStorage\tabnine.tabnine-vscode\binaries\4.5.22\x86_64-pc-windows
-gnu\TabNine-deep-local.exe
TCP 127.0.0.1 49152 127.0.0.1 33629 Established 6616 c:\Users\snehj\AppData\Roamin
g\Code\User\globalStorage\tabnine.tabnine-vscode\binaries\4.5.22\x86_64-pc-windows
-gnu\TabNine-deep-local.exe
TCP 127.0.0.1 49670 127.0.0.1 49671 Established 4628 C:\Program Files\MySQL\MySQL
Server 8.0\bin\mysqld.exe
TCP 127.0.0.1 49671 127.0.0.1 49670 Established 4628 C:\Program Files\MySQL\MySQL
Server 8.0\bin\mysqld.exe
TCP 127.0.0.1 49672 127.0.0.1 49673 Established 4628 C:\Program Files\MySQL\MySQL
Server 8.0\bin\mysqld.exe
TCP 127.0.0.1 49673 127.0.0.1 49672 Established 4628 C:\Program Files\MySQL\MySQL
Server 8.0\bin\mysqld.exe
TCP 127.0.0.1 63025 0.0.0.0 0 Listening 26948
C:\Users\snehj\AppData\Local\Programs\Microsoft VS Code\Code.exe
TCP 127.0.0.1 63047 0.0.0.0 0 Listening 26948
C:\Users\snehj\AppData\Local\Programs\Microsoft VS Code\Code.exe
TCP 127.0.0.1 63084 127.0.0.1 63085 Established 24220
c:\Users\snehj\AppData\Local\Programs\Python\Python310\python.exe
TCP 127.0.0.1 63085 127.0.0.1 63084 Established 24220
c:\Users\snehj\AppData\Local\Programs\Python\Python310\python.exe
TCP 127.0.0.1 63086 127.0.0.1 63087 Established 24220
c:\Users\snehj\AppData\Local\Programs\Python\Python310\python.exe
TCP 127.0.0.1 63087 127.0.0.1 63086 Established 24220
c:\Users\snehj\AppData\Local\Programs\Python\Python310\python.exe
TCP 192.168.0.101 139 0.0.0.0 0 Listening 4 System
TCP 192.168.0.101 31116 20.198.119.143 443 Established 5892 C:\Program
Files\Microsoft OneDrive\OneDrive.exe
TCP 192.168.0.101 31627 142.251.10.188 5228 Established 31392 C:\Program
Files\Google\Chrome\Application\chrome.exe
TCP 192.168.0.101 31912 13.73.252.141 8883 Established 17632 C:\Program
Files\Dell\SupportAssistAgent\bin\SupportAssistAgent.exe
TCP 192.168.0.101 31944 172.217.194.188 5228 Established 31392 C:\Program
Files\Google\Chrome\Application\chrome.exe
TCP 192.168.0.101 33430 140.82.113.25 443 Established 31392 C:\Program
Files\Google\Chrome\Application\chrome.exe
TCP 192.168.0.101 33500 40.99.34.194 443 Established 6040
C:\WINDOWS\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\SearchHost.exe
TCP 192.168.0.101 33596 65.2.109.57 443 Established 9068 C:\Program
Files\McAfee\MfeAV\MFEAvSvc.exe
TCP 192.168.0.101 33606 117.18.232.200 443 Close Wait 6040
```

```
C:\WINDOWS\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\SearchHost.exe
TCP 192.168.0.101 33608 117.18.232.200 443 Close Wait 6040
C:\WINDOWS\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\SearchHost.exe
TCP 192.168.0.101 33614 152.199.43.62 443 Close Wait 6040
C:\WINDOWS\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\SearchHost.exe
TCP 192.168.0.101 33623 44.196.236.244 443 Established 320
C:\Users\snehj\AppData\Local\Grammarly\DesktopIntegrations\Grammarly.Desktop.exe
TCP 192.168.0.101 33627 44.196.236.244 443 Established 320
C:\Users\snehj\AppData\Local\Grammarly\DesktopIntegrations\Grammarly.Desktop.exe
TCP 192.168.0.101 33628 18.205.84.237 443 Close Wait 320
C:\Users\snehj\AppData\Local\Grammarly\DesktopIntegrations\Grammarly.Desktop.exe
TCP 192.168.0.101 33630 34.170.65.59 443 Established 16544 c:\Users\snehj\AppData\
Roaming\Code\User\globalStorage\tabnine.tabnine-vscode\binaries\4.5.22\x86_64-pc-w
indows-gnu\TabNine.exe
TCP 192.168.0.101 33632 34.170.65.59 443 Established 33460 C:\Users\snehj\AppData\
Roaming\Code\User\globalStorage\tabnine.tabnine-vscode\binaries\4.5.22\x86_64-pc-w
indows-gnu\WD-TabNine.exe
Enumerating IPv6 connections
Protocol Local Address Local Port Remote Address Remote Port State Process ID
Process Name
TCP [::] 135 [::] 0 Listening 1456 C:\WINDOWS\system32\svchost.exe
TCP [::] 445 [::] 0 Listening 4 System
TCP [::] 3306 [::] 0 Listening 4628 C:\Program Files\MySQL\MySQL Server
8.0\bin\mysqld.exe
TCP [::] 33060 [::] 0 Listening 4628 C:\Program Files\MySQL\MySQL Server
8.0\bin\mysqld.exe
TCP [::] 49664 [::] 0 Listening 1088 C:\WINDOWS\system32\lsass.exe
TCP [::] 49665 [::] 0 Listening 788 wininit
TCP [::] 49666 [::] 0 Listening 2576 C:\WINDOWS\System32\svchost.exe
TCP [::] 49667 [::] 0 Listening 2964 C:\WINDOWS\system32\svchost.exe
TCP [::] 49668 [::] 0 Listening 3492 C:\WINDOWS\System32\spoolsv.exe
TCP [::] 49675 [::] 0 Listening 1064 services
TCP [::1] 49669 [::] 0 Listening 4568 C:\WINDOWS\System32\DriverStore\FileReposito
ry\dal.inf_amd64_b5484efd38adbe8d\jhi_service.exe
```

## 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 0.0.0.0 500 *:* 3904 C:\WINDOWS\system32\svchost.exe
UDP 0.0.0.0 4500 *:* 3904 C:\WINDOWS\system32\svchost.exe
UDP 0.0.0.0 5050 *:* 10988 C:\WINDOWS\system32\svchost.exe
UDP 0.0.0.0 5353 *:* 30640 C:\Program Files\Google\Chrome\Application\chrome.exe
UDP 0.0.0.0 5353 *:* 31392 C:\Program Files\Google\Chrome\Application\chrome.exe
UDP 0.0.0.0 5353 *:* 2340 C:\WINDOWS\system32\svchost.exe
UDP 0.0.0.0 5353 *:* 33420 C:\Program Files
(x86)\Microsoft\Edge\Application\msedge.exe
UDP 0.0.0.0 5353 *:* 31392 C:\Program Files\Google\Chrome\Application\chrome.exe
UDP 0.0.0.0 5353 *:* 33420 C:\Program Files
(x86)\Microsoft\Edge\Application\msedge.exe
UDP 0.0.0.0 5353 *:* 30640 C:\Program Files\Google\Chrome\Application\chrome.exe
UDP 0.0.0.0 5355 *:* 2340 C:\WINDOWS\system32\svchost.exe
UDP 0.0.0.0 6646 *:* 7700 C:\Program Files\Common
Files\McAfee\MMSSHost\MMSSHOST.EXE
UDP 0.0.0.0 49262 *:* 31392 C:\Program Files\Google\Chrome\Application\chrome.exe
UDP 0.0.0.0 54913 *:* 31392 C:\Program Files\Google\Chrome\Application\chrome.exe
UDP 0.0.0.0 56655 *:* 31392 C:\Program Files\Google\Chrome\Application\chrome.exe
UDP 0.0.0.0 59952 *:* 31392 C:\Program Files\Google\Chrome\Application\chrome.exe
UDP 0.0.0.0 61520 *:* 2340 C:\WINDOWS\system32\svchost.exe
UDP 127.0.0.1 1900 *:* 10836 C:\WINDOWS\system32\svchost.exe
UDP 127.0.0.1 49664 *:* 3868 C:\WINDOWS\System32\svchost.exe
UDP 127.0.0.1 54048 *:* 10836 C:\WINDOWS\system32\svchost.exe
UDP 192.168.0.101 137 *:* 4 System
UDP 192.168.0.101 138 *:* 4 System
UDP 192.168.0.101 1900 *:* 10836 C:\WINDOWS\system32\svchost.exe
UDP 192.168.0.101 2177 *:* 17700 C:\WINDOWS\system32\svchost.exe
UDP 192.168.0.101 54047 *:* 10836 C:\WINDOWS\system32\svchost.exe
UDP 192.168.0.101 56305 *:* 31392 C:\Program
Files\Google\Chrome\Application\chrome.exe
UDP 192.168.0.101 60504 *:* 31392 C:\Program
Files\Google\Chrome\Application\chrome.exe
Enumerating IPv6 connections
```

```
Protocol Local Address Local Port Remote Address:Remote Port Process ID Process
Name
UDP [::] 500 *:* 3904 C:\WINDOWS\system32\svchost.exe
UDP [::] 4500 *:* 3904 C:\WINDOWS\system32\svchost.exe
UDP [::] 5353 *:* 2340 C:\WINDOWS\system32\svchost.exe
UDP [::] 5353 *:* 31392 C:\Program Files\Google\Chrome\Application\chrome.exe
UDP [::] 5353 *:* 30640 C:\Program Files\Google\Chrome\Application\chrome.exe
UDP [::] 5353 *:* 33420 C:\Program Files
(x86)\Microsoft\Edge\Application\msedge.exe
UDP [::] 5355 *:* 2340 C:\WINDOWS\system32\svchost.exe
UDP [::] 61520 *:* 2340 C:\WINDOWS\system32\svchost.exe
UDP [::1] 1900 *:* 10836 C:\WINDOWS\system32\svchost.exe
UDP [::1] 54046 *:* 10836 C:\WINDOWS\system32\svchost.exe
UDP [fe80::8679:587d:73d5:246a%18] 1900 *:* 10836 C:\WINDOWS\system32\svchost.exe
UDP [fe80::8679:587d:73d5:246a%18] 2177 *:* 17700 C:\WINDOWS\system32\svchost.exe
UDP [fe80::8679:587d:73d5:246a%18] 54045 *:* 10836 C:\WINDOWS\system32\svchost.exe
```

## 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
match.adsrvr.org match.adsrvr.org 52.223.40.198
match.adsrvr.org match.adsrvr.org 35.71.131.137
match.adsrvr.org match.adsrvr.org 15.197.193.217
match.adsrvr.org match.adsrvr.org 3.33.220.150
meet.google.com meet.google.com 142.250.195.142
rum14.perf.linkedin.com rum14.perf.linkedin.com ...linkedin-com.l-0005.l-msedge.net
rum14.perf.linkedin.com ...linkedin-com.l-0005.l-msedge.net l-0005.l-msedge.net
rum14.perf.linkedin.com l-0005.l-msedge.net 13.107.42.14
...802.prod.do.dsp.mp.microsoft.com ...802.prod.do.dsp.mp.microsoft.com
52.137.102.105
fp-vs-nocache.azureedge.net fp-vs-nocache.azureedge.net
fp-vs-nocache.ec.azureedge.net
fp-vs-nocache.azureedge.net fp-vs-nocache.ec.azureedge.net cs9.wpc.v0cdn.net
fp-vs-nocache.azureedge.net cs9.wpc.v0cdn.net 117.18.232.200
user-images.githubusercontent.com user-images.githubusercontent.com 185.199.108.133
user-images.githubusercontent.com user-images.githubusercontent.com 185.199.109.133
user-images.githubusercontent.com user-images.githubusercontent.com 185.199.110.133
user-images.githubusercontent.com user-images.githubusercontent.com 185.199.111.133
avatars.githubusercontent.com avatars.githubusercontent.com 185.199.111.133
avatars.githubusercontent.com avatars.githubusercontent.com 185.199.110.133
avatars.githubusercontent.com avatars.githubusercontent.com 185.199.108.133
avatars.githubusercontent.com avatars.githubusercontent.com 185.199.109.133
beacons4.gvt2.com beacons4.gvt2.com 216.239.32.116
github.githubassets.com github.githubassets.com 185.199.108.154
github.githubassets.com github.githubassets.com 185.199.109.154
github.githubassets.com github.githubassets.com 185.199.110.154
github.githubassets.com github.githubassets.com 185.199.111.154
fp-vp.azureedge.net fp-vp.azureedge.net fp-vp.ec.azureedge.net
fp-vp.azureedge.net fp-vp.ec.azureedge.net cs9.wpc.v0cdn.net
fp-vp.azureedge.net cs9.wpc.v0cdn.net 117.18.232.200
www.google.com www.google.com 142.250.195.196
beacons3.gvt2.com beacons3.gvt2.com 216.58.200.131
raw.githubusercontent.com raw.githubusercontent.com 185.199.111.133
raw.githubusercontent.com raw.githubusercontent.com 185.199.108.133
raw.githubusercontent.com raw.githubusercontent.com 185.199.110.133
raw.githubusercontent.com raw.githubusercontent.com 185.199.109.133
notify.tabnine.com notify.tabnine.com ...bnine-remote-gateway.tabnine.com
notify.tabnine.com ...bnine-remote-gateway.tabnine.com 34.170.65.59
objects.githubusercontent.com objects.githubusercontent.com 185.199.108.133
```

```
objects.githubusercontent.com objects.githubusercontent.com 185.199.109.133
objects.githubusercontent.com objects.githubusercontent.com 185.199.110.133
objects.githubusercontent.com objects.githubusercontent.com 185.199.111.133
fp-vp-nocache.azureedge.net fp-vp-nocache.azureedge.net
fp-vp-nocache.ec.azureedge.net
fp-vp-nocache.azureedge.net fp-vp-nocache.ec.azureedge.net cs9.wpc.v0cdn.net
fp-vp-nocache.azureedge.net cs9.wpc.v0cdn.net 117.18.232.200
beacons2.gvt2.com beacons2.gvt2.com 172.217.166.67
cdn.mxpnl.com cdn.mxpnl.com 35.186.235.23
cdn.mxpnl.com cdn.mxpnl.com 130.211.5.208
static-ecst.licdn.com static-ecst.licdn.com cs1404.wpc.epsiloncdn.net
static-ecst.licdn.com cs1404.wpc.epsiloncdn.net 152.199.43.62
google.com google.com 142.250.205.238
a.nel.cloudflare.com a.nel.cloudflare.com 35.190.80.1
```

## 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 10880
HKCU User Agent Mozilla/4.0 (compatible; MSIE 8.0; Win32)
HKCU ZonesSecurityUpgrade System.Byte[]
HKCU WarnonZoneCrossing 0
HKCU LockDatabase 133211719049734484
HKCU EnableNegotiate 1
HKCU ProxyEnable 0
HKCU MigrateProxy 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: My Dell
Identity: Windows User
PacakgeSid: S-1-15-2-457177802-1096569744-1416967971-3398845977-2226797469-2659906
712-2620288000
Credential: E0520512ED7A60BF2EF9DC4FE8028D5FF43EE454BE151EA30B92487F68830BFC
Last Modified: 30-01-2022 07:36:16
================================================================================
===============
```

## Checking Credential manager

```
[!] Warning: if password contains non-printable characters, it will be printed as
unicode base64 encoded string
Username: 100153259
Password: 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
Target: git:https://github.com
PersistenceType: LocalComputer
LastWriteTime: 02-11-2022 11:25:38
================================================================================
===============
Username: 2101bd1dba5b10b0
Password: (Unicode Base64 encoded) TS5SM19CQVkuLUNUeFk3OGVTVGRPYXVZRHN2Z3E4a2Z1a2l
PZGV3OU5CMVBYYWtHcVQwZ3VPd1JxcDlyT1llY2tOUktIUlg2OTkzVFNiNllnWHJraiFHcFZVNyFDQjVuW
DkzWCFWT09ZRUM5ZUYySFFKVkp1dHdHbUV6ek5VSVNHZEZ1akNGVDdzTlJRNkliMDFCRGVCTkJXb0xpGl
sQ2RuSkVWNkgqQmRoTHBrUDgwTENQbXl5cDl3OGl0T2UxdGFxNTVtZEFmeDhMNzRRN2lhWVZyNiFTZlZmY
3NMRE9ydEhzQ0pppV2J0cjhGYTEhOVhjSWJQIXU5akU3MGVBYiFsTk4yNWRGRndyUHJIWUo0bGdhQ1l6MGl
FYmtuYXpWcGJNVThVQ0NPNTJZdVB5NHlWOXQydkFDY3ZhRVp3azVMN3hqNDZrIVJCOFRwUUtGcnnpjMTBGY
1BBYlFrNkR3dTlqaWEqbXRuVmhhbXkxcGN5Z2RRYyo=
Target: OneDrive Cached Credential
PersistenceType: LocalComputer
LastWriteTime: 06-02-2023 06:21:53
================================================================================
===============
Username: snehjanarthanan@outlook.com
Password:
Target: MicrosoftAccount:user=snehjanarthanan@outlook.com
PersistenceType: LocalComputer
LastWriteTime: 23-07-2023 10:21:33
================================================================================
===============
Username: SnehaJanarthanan
Password: (Unicode Base64 encoded)
Z2hvXzVxMmNaZ0JleDlvUzZaZjN3N3hldkxRUjZsZ09mSTFQYTBCNA==
Target: GitHub - https://api.github.com/SnehaJanarthanan
PersistenceType: Enterprise
LastWriteTime: 14-07-2023 15:30:58
================================================================================
===============
```

# Saved RDP connections

```
Host Username Hint User SID
ec2-35-154-84-31.ap-south-1.compute.amazonaws.comDESKTOP-SNEHA\Administrator
S-1-5-21-3918106844-1363930152-1516286804-1001
```

# 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
```

# Checking for DPAPI Master Keys

*Follow the provided link for further instructions in how to decrypt the masterkey.*

```
MasterKey: C:\Users\snehj\AppData\Roaming\Microsoft\Protect\S-1-5-21-3918106844-13
63930152-1516286804-1001\263c5d95-51cc-43c7-afc6-d7c7fef0e54f
Accessed: 17-07-2023 22:02:06
Modified: 17-07-2023 22:02:06
================================================================================
==============
MasterKey: C:\Users\snehj\AppData\Roaming\Microsoft\Protect\S-1-5-21-3918106844-13
63930152-1516286804-1001\64f42e08-00cd-408d-806e-c40b8c4e42a8
Accessed: 17-07-2023 22:02:54
Modified: 17-07-2023 22:02:54
================================================================================
==============
MasterKey: C:\Users\snehj\AppData\Roaming\Microsoft\Protect\S-1-5-21-3918106844-13
63930152-1516286804-1001\85b5bc2c-b2ce-46d7-9cf8-48d9cc312c24
Accessed: 17-07-2023 22:02:37
Modified: 17-07-2023 22:02:37
================================================================================
==============
MasterKey: C:\Users\snehj\AppData\Roaming\Microsoft\Protect\S-1-5-21-3918106844-13
63930152-1516286804-1001\9cc78875-6eea-4ff6-aac4-e25ba983836f
Accessed: 17-07-2023 22:15:40
Modified: 17-07-2023 22:15:40
================================================================================
==============
MasterKey: C:\Users\snehj\AppData\Roaming\Microsoft\Protect\S-1-5-21-3918106844-13
63930152-1516286804-1001\b4077d80-0513-4df2-9dc2-8f4fe2b694fb
Accessed: 17-07-2023 22:02:37
Modified: 17-07-2023 22:02:37
================================================================================
==============
MasterKey: C:\Users\snehj\AppData\Roaming\Microsoft\Protect\S-1-5-21-3918106844-13
63930152-1516286804-1001\e2810598-b3c4-49b2-869b-6cfa33a57ade
Accessed: 17-07-2023 22:02:03
Modified: 17-07-2023 22:02:03
================================================================================
==============
```

# 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\snehj\AppData\Local\Microsoft\Credentials\37119E49A725CC10C92BB
B1992B8EAEE
Description: Local Credential Data
██
MasterKey: 85b5bc2c-b2ce-46d7-9cf8-48d9cc312c24
Accessed: 23-07-2023 10:21:33
Modified: 02-11-2022 11:25:38
Size: 544
================================================================================
==============
CredFile: C:\Users\snehj\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF
1B96859CE5D
Description: Local Credential Data
██
MasterKey: 263c5d95-51cc-43c7-afc6-d7c7fef0e54f
Accessed: 23-07-2023 10:21:33
Modified: 03-07-2023 12:03:12
Size: 11552
================================================================================
==============
CredFile: C:\Users\snehj\AppData\Local\Microsoft\Credentials\E05DBE15D38053457F352
3A375594044
Description: Local Credential Data
██
MasterKey: b4077d80-0513-4df2-9dc2-8f4fe2b694fb
Accessed: 23-07-2023 10:21:33
Modified: 06-02-2023 06:21:53
Size: 1264
================================================================================
```

```
===============
CredFile: C:\Users\snehj\AppData\Local\Microsoft\Credentials\EAA1BF2475948B58890E9
3655FFE6B81
Description: Local Credential Data
██
MasterKey: 263c5d95-51cc-43c7-afc6-d7c7fef0e54f
Accessed: 23-07-2023 10:21:33
Modified: 23-07-2023 10:21:33
Size: 4592
================================================================================
===============
CredFile: C:\Users\snehj\AppData\Roaming\Microsoft\Credentials\AD11377A9225B024C55
D8049A42BE770
Description: Enterprise Credential Data
██
MasterKey: 263c5d95-51cc-43c7-afc6-d7c7fef0e54f
Accessed: 17-07-2023 22:02:37
Modified: 14-07-2023 15:30:59
Size: 570
================================================================================
===============
CredFile: C:\WINDOWS\System32\config\systemprofile\AppData\Local\Microsoft\Credent
ials\DFBE70A7E5CC19A398EBF1B96859CE5D
Description: Local Credential Data
██
MasterKey: b5b879db-7f23-4790-999b-045c4bd1be7d
Accessed: 17-07-2023 22:02:37
Modified: 11-05-2023 18:51:59
Size: 11536
================================================================================
===============
```

## Looking for saved Wifi credentials

```
SSID : 'iPhone XR
' password : '123india'
SSID : 'SKCET_WiFi
' password : '$kcet@123'
SSID : 'OnePlus Nord CE 2 Lite
' password : 'spidey200522'
SSID : 'Prithu
' password : 'qwerty555'
SSID : 'Xiaomi 11i
' password : 'networkslow'
SSID : 'redmi 9A
' password : '26042004'
SSID : 'SKCET WIFI
' password : '$kcet@123'
SSID : 'NW LAB
' password : '$kcet@123'
SSID : 'Yavi's iPhone
' password : 'heysurprise'
SSID : 'Laddoo's Iphone
' password : 'Laadoo22'
SSID : 'SKCET_WIFI
' password : '$kcet@123'
SSID : '***
' password : 'subi2003'
SSID : 'Cool
' password : 'india143'
SSID : 'DSP LAB
' password : '$kcet@123'
SSID : 'Havon
' password : 'Havon@123'
SSID : 'VITC-EVENT
' password : 'Eve%$2319'
SSID : 'Cool 2
' password : 'India143'
SSID : 'Galaxy A20s8498
' password : 'password'
SSID : 'Yashu's iPhone
' password : 'surprise'
SSID : 'F-CODD LAB
' password : '$kcet@123'
```

```
SSID : 'GIMGRAY LAB
' password : '$kcet@123'
SSID : 'Sam
' password : 'blueray1'
SSID : 'AK LAB
' password : '$kcet@123'
SSID : 'TECNO SPARK Go Plus
' password : 'P@$$word'
SSID : '??
' password : 'srinisrini2003'
SSID : 'SKI-WIFI
' password : 'skct7278'
SSID : 'Ls
' password : 'selvik003'
SSID : 'Galaxy M3272BC
' password : 'taetaebora'
SSID : 'Sid
' password : 'Ar1c3nt#123'
SSID : 'Mark
' password : 'kalyan@1'
SSID : 'C3 BLOCK
' password : 'Wifi@123'
SSID : 'C4 BLOCK
' password : '$kcet@123'
SSID : '??
' password : 'gopishobi'
SSID : 'KK
' password : '55874793'
SSID : 'tamilarasi
' password : 'kajendran'
SSID : 'classic_coders
' password : 'passwordpassword'
SSID : 'Youth
' password : 'iamuthi2003'
SSID : 'Yashu Venkat
' password : '9487030021yv'
SSID : 'YASHU VENKAT
' password : 'iloveyou'
SSID : 'Siddhesh
' password : 'Ar1c3nt#123'
SSID : 'Redmi Note 9 Pro Max
' password : 'akirat06'
SSID : 'Kogan 9 Pro
' password : 'zxcvbnm1'
SSID : 'Jarvis
' password : 'skarty0123'
SSID : 'HeLiO G95
' password : 'piyush27'
SSID : 'Harsh
' password : 'incorrect'
SSID : 'Genie
' password : 'Magic$2022'
SSID : 'Galaxy A21s0D52
' password : 'rvgc3348'
SSID : 'EDDY 2406
' password : 'bhavikkpatel'
SSID : 'Cool_EXT
' password : 'india143'
SSID : 'C4 LAB 3
' password : '$kcet@123'
SSID : 'C4 LAB 2
' password : '$kcet@123'
SSID : 'C4 LAB 1
' password : '$kcet@123'
SSID : 'Aswin's Mobile
' password : 'broo1234'
SSID : 'Achu??
' password : 'sollamatene'
SSID : '&
' password : 'selvik003'
```

# Browsers Information

## Showing saved credentials for Chrome

```
Url: https://www.heymath.com/jsp/IxFreezoneValidate.jsp
Username: sishyaomr481
Password: sishyaomr481
================================================================================
===============
Url: https://user.readylink.in/login/process
Username: ret5504
Password: 837134
================================================================================
===============
Url:
Username: preethajana@icloud.com
Password: $Pounds14
================================================================================
===============
Url: https://join.secondlife.com/create
Username: snehajana
Password: sneha2003
================================================================================
===============
Url: https://meetingsapac17.webex.com/mw3300/mywebex/login/login.do
Username: snehajanarthanan123456@gmail.com
Password: Jpsm2003
================================================================================
===============
Url: https://rabbitcrm.com/school/parent/login/submit
Username: PPS1736
Password: 04/01/2010
================================================================================
===============
Url: https://brainly.in/login
Username: snehajanarthanan123456@gmail.com
Password: sneha2003
================================================================================
===============
Url: https://api.twitter.com/sessions
Username: 8668139752
Password: SnehaMaanas20031
================================================================================
===============
Url:
Username: snehajanarthanan123456@gmail.com
Password:
================================================================================
===============
Url: https://m.facebook.com/reg/
Username: 8668139752
Password: SnehaMaanas200310
================================================================================
===============
Url: https://myid.canon/canonid/
Username: snehajanarthanan123456@gmail.com
Password: Sneha2003
================================================================================
===============
Url:
https://accounts.tcscodevita.com/auth/realms/Codevita/login-actions/authenticate
Username: 21cse047@skcet.ac.in
Password: M@@nas2010
================================================================================
===============
Url: https://adobeid-na1.services.adobe.com/renga-idprovider/pages/login.do
Username: snehajanarthanan123456@gmail.com
Password: Jpsmjpsmjpsmjpsm2003
================================================================================
===============
Url: https://singlelogin.org/rpc.php
Username: snehajanarthanan123456@gmail.com
Password: 9$^q^MH9/xbdNkS
================================================================================
===============
```

```
Url: https://www.opinionoutpost.ca/
Username: E-mail
Password: Password
=============================================================================
===============
Url: https://twitter.com/sessions
Username: imnotgonafollowu
Password: SnehaMaanas200310
=============================================================================
===============
Url: https://englishtest.duolingo.com/register
Username: snehajanarthanan123456@gmail.com
Password: nSwaa5V9FUM6aHM
=============================================================================
===============
Url: https://login.live.com/ppsecure/post.srf
Username: janarthanansneha@gmail.com
Password: SnehaMaanas200310
=============================================================================
===============
Url: https://twitter.com/sessions
Username: 8668139752
Password: Sneha2003
=============================================================================
===============
Url: https://www.netflix.com/in/login
Username: jlakshmipathy@gmail.com
Password: software1
=============================================================================
===============
Url: https://www.goodreads.com/user/create
Username: snehajanrthanan123456@gmail.com
Password: SnehaMaanas200310
=============================================================================
===============
Url:
Username: snehajanarthanan123456@gmail.com
Password: sneha2942003
=============================================================================
===============
Url: https://www.topperlearning.com/sign-in
Username: snehajanarthanan123456@gmail.com
Password: b9opeq
=============================================================================
===============
Url: https://www.tumblr.com/login
Username: snehajanarthanan123456@gmail.com
Password: 8668139752jpsmsneha2942003
=============================================================================
===============
Url: https://www.fundancer.net/signup
Username: snehajanarthanan123456@gmail.com
Password: sneha2003
=============================================================================
===============
Url: https://www.meritnation.com/users/registration
Username: giveneh880@homedepinst.com
Password: x6qKJ7G$wPCiQ*.
=============================================================================
===============
Url: https://mobile.twitter.com/sessions
Username: 8668139752
Password: Sneha2003
=============================================================================
===============
Url: https://www.fueladream.com/home/login
Username: snehajanarthanan@gmail.com
Password: fueladream
=============================================================================
===============
Url: https://www.pinterest.com/pin/325455510554511584/
Username: snehajanarthanan123456@gmail
Password: jpsmjpsmjpsmjpsm
=============================================================================
===============
Url:
Username: snehajanarthanan123456@gmail.com
Password:
```

```
================================================================================
===============
Url: https://singlelogin.me/rpc.php
Username: SNEHAJANARTHANAN123456@GMAIL.COM
Password: SnehaMaanas200310
================================================================================
===============
Url: javascript:void(0)
Username: snehajanarthanan123456@gmail.com
Password: SnehaMaanas200310
================================================================================
===============
Url: https://archiveofourown.org/users/login
Username: snehajanarthanan123456@gmail.com
Password: jpsmsneha2942003
================================================================================
===============
Url: https://www.facebook.com/login.php
Username: preethajana@gmail.com
Password: timetable
================================================================================
===============
Url: http://chettinadvidyashram.in/chettinad/chettinadvidyashram/stuindex.aspx
Username: 34223
Password: 29042003
================================================================================
===============
Url: https://www.amazon.in/ap/signin
Username: jlakshmi@amazon.com
Password: pathy1
================================================================================
===============
Url: http://www.magisto.com/account/signup
Username: snehajanarthanan123456@gmail.com
Password: jpsmjpsmjpsmjpsm
================================================================================
===============
Url: https://twitter.com/sessions
Username: notgonafollowu
Password: SnehaMaanas200310
================================================================================
===============
Url: https://api.twitter.com/oauth/authorize
Username: notgonafollowu
Password: SnehaMaanas200310
================================================================================
===============
Url: https://archiveofourown.org/users
Username: imnotgonnafollowyou
Password: 8668139752jpsmsneha2942003
================================================================================
===============
Url: https://musescore.com/user/login
Username: sneha janarthanan
Password: sneha2003
================================================================================
===============
Url: javascript:;
Username: administrator
Password: administrator
================================================================================
===============
Url: https://accounts.spotify.com/
Username: snehajanarthanan123456@gmail.com
Password: 8668139752jpsmsneha2942003
================================================================================
===============
Url: https://www.wattpad.com/login
Username: Sneha Janarthanan
Password: Sneha2003
================================================================================
===============
Url: https://www.postermywall.com/index.php/authenticate/asynclogin
Username: snehajanarthanan123456@gmail.com
Password: Sneha2003
================================================================================
===============
Url:
```

```
Username: sojqulzmbdw0fucm32rq95q93
Password: sneha2003
================================================================================
===============
Url: https://www.scribd.com/login/signup
Username: sneha janarthanan
Password: Sneha2003
================================================================================
===============
Url: https://github.com/signup
Username: SnehaJanarthanan
Password: SnehaMaanas200310
================================================================================
===============
Url: https://www.linkedin.com/checkpoint/lg/login-submit
Username: snehajanarthanan@gmail.com
Password: &+e3W_TK8vq)nMg
================================================================================
===============
Url: https://www.amazon.com/ap/signin
Username: jlakshmi@amazon.com
Password: pathy1
================================================================================
===============
Url: https://devfolio.co/
Username: snehajanarthan
Password: SnehaMaanas200310
================================================================================
===============
Url: https://accounts.autodesk.com/User/RegisterUser
Username: snehajanarthanan123456@gmail.com
Password: SnehaMaanas200310
================================================================================
===============
Url: https://portal.naanmudhalvan.tn.gov.in/login
Username: au727721EUCS146
Password: 551901
================================================================================
===============
Url: https://imsoidc.bentley.com/
Username: 727721eucs146@skcet.ac.in
Password: SnehaMaanas200310
================================================================================
===============
Url: https://id.condenast.com/interaction/CAHj-W4b0o_LWoB2ZfYdI/register
Username: SNEHAJANARTHANAN123456@GMAIL.COM
Password: SnehaMaanas200310
================================================================================
===============
Url: https://login.usatoday.com/USAT-GUP-ARKADIUM/authenticate/
Username: SNEHAJANARTHANAN123456@GMAIL.COM
Password: ENiS5LHTbreT_*T
================================================================================
===============
Url: http://172.16.16.254:2280/submit/user_login.php
Username: 727721eucs146
Password: 9962230004
================================================================================
===============
Url: https://archive.org/account/signup
Username: SNEHAJANARTHANAN123456@GMAIL.COM
Password: CUQrwJXBj?H2Qy*
================================================================================
===============
Url: https://login.nvgs.nvidia.com/
Username: 727721eucs146@skcet.ac.in
Password: UpD2hdc.DK6Hy-k
================================================================================
===============
```

## Looking for GET credentials in Chrome history

=== Chrome (All Users) ===
https://accounts.google.com/CheckCookie?continue=https%3A%2F%2Ftakeout.google.com%
2Ftakeout%2Fdownload%3Fj%3Deceb1af7-2f4f-4842-91bd-495d70f6eebf%26i%3D4%26user%3D1
00163304658953442343%26rapt%3DAEjHL4Pb-JTIX5RcJRpoJlr4dyxvRUge5X0CnYJUvwPtPcUIgf_1
YDM_kwn1KGXv-QhMhtifpQRHx3HXEcIrdomh86qdCvrvow&hl=en&checkedDomains=youtube&checkC
onnection=youtube%3A299%3A0&pstMsg=1&osid=1&rart=ANgoxceQxMbk59PHpS3iwE_VIWXvOz5cN
7MBxI0aYeCU_dawKrZb49-XjA1NhB2KD1Er5oIYviurOMLtpX20EUb_VplqrjaAEQ&flowName=GlifWeb
SignIn&ifkv=Af_xneHjXMJ8PKWRpiGOZf2jEFkQ-JVgFJTaAKNAomRdUUa-KQvMnhXM9FOSg-HjBYCBjO
oH34htag&chtml=LoginDoneHtml&gidl=EgIIAA
https://www.amazon.in/ap/signin?openid.pape.max_auth_age=3600&openid.return_to=htt
ps%3A%2F%2Fmusic.amazon.in%2F%3FrefMarker%3Dnull&openid.identity=http%3A%2F%2Fspec
s.openid.net%2Fauth%2F2.0%2Fidentifier_select&openid.assoc_handle=amzn_webamp_in&o
penid.mode=checkid_setup&language=en_IN&openid.claimed_id=http%3A%2F%2Fspecs.openi
d.net%2Fauth%2F2.0%2Fidentifier_select&pageId=login&openid.ns=http%3A%2F%2Fspecs.o
penid.net%2Fauth%2F2.0Amazon
https://export-download.canva.com/b3ZYU/DAFXWsb3ZYU/43/0-45580913304.pdf?X-Amz-Alg
orithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAJHKNGJLC2J7OGJ6Q%2F20230121%2Fus-east
-1%2Fs3%2Faws4_request&X-Amz-Date=20230121T055459Z&X-Amz-Expires=16852&X-Amz-Signa
ture=4cd6593461f25ec765b7cde138faf472f36adb4ccb67ad24feb6cda38c72b555&X-Amz-Signed
Headers=host&response-content-disposition=attachment%3B%20filename%2A%3DUTF-8%27%2
7V-Seva%2520Maiyam%2520Janarthanan%2520L%2520JLP%2520Farms%2520Vedapatty%2520-%252
0Perur%2520Main%2520Road%2520Vedapatty%252C%2520Coimbatore%2520641007%252098842300
04%2520BILL%2520TO%2520INVOICE%2520%23%2520101%2520CHINMAYA%2520INTERNATIONAL%2520
RESIDENTIAL%2520SCHOOL%252C%2520SWAMI%2520CHINMAYANANDA%2520LANE%252C%2520NALLUR%2
520VAYAL%2520POST%252C%2520.pdf&response-expires=Sat%2C%2021%20Jan%202023%2010%3A3
5%3A51%20GMT
https://export-download.canva.com/b3ZYU/DAFXWsb3ZYU/33/0-45580483369.pdf?X-Amz-Alg
orithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAJHKNGJLC2J7OGJ6Q%2F20230121%2Fus-east
-1%2Fs3%2Faws4_request&X-Amz-Date=20230121T033523Z&X-Amz-Expires=26562&X-Amz-Signa
ture=03ba73fc6f86dc3b1b46f14e9ae3becd045833bc8b9d0d86e02cd0ff586b1c25&X-Amz-Signed
Headers=host&response-content-disposition=attachment%3B%20filename%2A%3DUTF-8%27%2
7V-Seva%2520Maiyam%2520Janarthanan%2520L%2520JLP%2520Farms%2520Vedapatty%2520-%252
0Perur%2520Main%2520Road%2520Vedapatty%252C%2520Coimbatore%2520641007%252098842300
04%2520BILL%2520TO%2520INVOICE%2520%23%2520101%2520CHINMAYA%2520INTERNATIONAL%2520
RESIDENTIAL%2520SCHOOL%252C%2520SWAMI%2520CHINMAYANANDA%2520LANE%252C%2520NALLUR%2
520VAYAL%2520POST%252C%2520.pdf&response-expires=Sat%2C%2021%20Jan%202023%2010%3A5
8%3A05%20GMT
https://mail.google.com/mail/?tab=rm&authuser=0&ogbl
https://www.youtube.com/redirect?event=video_description&redir_token=QUFFLUhqa0FHZ
ko5ZGNXcnAwM1BaWUg5eVYwUklNbUo3UXxBQ3Jtc0ttaVp0QUF0bGR2aGNqS0pvLWJUMFV2VVUtVVVwN0E
5VGxvRWQ2MmpyLTRqbHE3ZmU1VkhLeEJJRGFxQXlzQWVkZmZiRjZuUHVlRml4ZWlfdFo4U3VodWJppd0dLR
kJScFpteGstQjB4dGU5aXdoWmJSTQ&q=https%3A%2F%2Fwww.instagram.com%2Fcharlie_fornow%2
F&v=4EAcPK53ovw
https://takeout.google.com/accounts/SetOSID?authuser=0&continue=https%3A%2F%2Facco
unts.youtube.com%2Faccounts%2FSetSID%3Fssdc%3D1%26sidt%3DALWU2cue8%252F1KG6kYTLlOz
wcweml7NNhthp3iEXL2teVVqFtV9kbt5CNH6droXD3d112DxR2AmaUkY7gPxkgelcDVEiw6XwCiDuWaldI
ItxMHcmuxTBh%252BNJKglPvknnkmreARbCLWlPhS5HrJvewHz%252BdqHkUZazH9AqvA9uUjB16aT40Jc
D%252BQJXjRjWVhYZOof2tM%252Bfh4EXRF9Hv9wVUFNfUe0w%252FNp5FktG0aTUbJMCJ91Q6q9Gsbcr0
K6amzAS%252BcSVs05ny17HhplCf8Z%252Bh5W9uFQ3lmhcydwANxr0SCPC8AtMYwQo6YjZqyYM
https://takeout.google.com/takeout/download?j=eceb1af7-2f4f-4842-91bd-495d70f6eebf
&i=4&user=100163304658953442343&rapt=AEjHL4NcPhSAKY3BgJ-L16W94ZOobyO0KUGob1J79pH9A
Uxxd25zdN6qKrObFKLDEXRiMD6wE5iUstf3gIRv3aiFs1p90pKB6w=
https://takeout.google.com/takeout/download?j=eceb1af7-2f4f-4842-91bd-495d70f6eebf
&i=0&user=100163304658953442343&rapt=AEjHL4M6ZpstK0D59UE_Rd4uT_n4LyIDZAMG-VH_l2J3d
L2nZTufU8E_ujWhJiLyYVvEAITK-lsowT2ejXm_l_by8dlX-AdJwQ=7
https://doc-2k-0g-photos-data-export.googleusercontent.com/download/8s11bg6at9flgd
e0sb95gnk4lsoqnavv/9cigp4da6uers8bdnonqkcqj8nkjd0lb/1664680500000/311eabc9-84d2-47
9f-a75d-4fe2a5bfe54c/100163304658953442343/ADt3v-P-M-LgTFSYp9xY-MFewQguVGVZbRyplJX
vGXnoWjeRu9bGe9CgigH1-yhIgOSvnpWQIchoPwwYomE-xDeON0hjyTIorhOTCblGtTBSriS-yrxJvJXBo
qSS_bQOpd_E-qZbOJimKz0OPaF2nuLbvXnb7sb0__YIHhIhmuChOyBOkR3oeYPVH4mQKIZaMC_eH0t9WWJ
LbonbJEOPBE2GxAqx1v2gkkoJT7roL04PAOIHvVLk3nyBggU7EBXchDVLDX5np8chO-cK-rYTzI4ODo-sA
h7tJXMQOliEhGgYvihUbQUCypU=?authuser=0&nonce=pfsoaisqv2e2m&user=100163304658953442
343&hash=r3qigeh7cug7rst8r837rk123vm42d0a
https://www.amazon.com/gp/slredirect/picassoRedirect.html/ref=sspa_dk_detail_0?ie=
UTF8&adId=A03653812H980791TJ90F&qualifier=1684130089&id=6457475426910084&widgetNam
e=sp_detail&url=%2Fdp%2FB0C3FHXLBZ%2Fref%3Dsspa_dk_detail_0%3Fpsc%3D1%26pd_rd_i%3D
B0C3FHXLBZ%26pd_rd_w%3DavBtx%26content-id%3Damzn1.sym.eb7c1ac5-7c51-4df5-ba34-ca81
0f1f119a%26pf_rd_p%3Deb7c1ac5-7c51-4df5-ba34-ca810f1f119a%26pf_rd_r%3DB53FBT15HED
Q6DWBHRM%26pd_rd_wg%3Drsh6r%26pd_rd_r%3D32eccdac-9d0d-4199-8c5d-2b32df8fc05e%26s%3
Dbooks%26sp_csd%3Dd2lkZ2V0TmFtZT1zcF9kZXRhaWwwBenny
https://www.amazon.com/gp/slredirect/picassoRedirect.html/ref=sspa_dk_detail_6?ie=
UTF8&adId=A0185892IQWOE0BI4OSD&qualifier=1684130064&id=3685673277054854&widgetName
=sp_detail2&url=%2Fdp%2FB09Q96CX89%2Fref%3Dsspa_dk_detail_6%3Fpsc%3D1%26pd_rd_i%3D
B09Q96CX89%26pd_rd_w%3Dvx56G%26content-id%3Damzn1.sym.0d1092dc-81bb-493f-8769-d5c8
02257e94%26pf_rd_p%3D0d1092dc-81bb-493f-8769-d5c802257e94%26pf_rd_r%3DYE25N8P5QB5A
6MWCPQRZ%26pd_rd_wg%3DOOFDU%26pd_rd_r%3Db19cb447-455d-4206-a93a-c0ada2d97646%26s%3
Dbooks%26sp_csd%3Dd2lkZ2V0TmFtZT1zcF9kZXRhaWwyAmazon.com
https://takeout.google.com/accounts/SetOSID?authuser=0&continue=https%3A%2F%2Facco

unts.youtube.com%2Faccounts%2FSetSID%3Fssdc%3D1%26sidt%3DALWU2ctk1TyJ0PzOOflkAbezu
qQ7CP0hlqck6MI0e7fQkm96FgzhMOTUSgpP0fxOkpnL4SCPw9g6bFN7jFqSN2Z3lrxXA7kx%252BOxcG6f
0DwYEfsjZBrnCiDmwWgjj1EtTubBU2qOGQA%252Bwat0nUBCIZoscRowZakAk0qZOxkLVabDgsmravhDYo
YgYLEv0Qh5eCmM7zxNfT0Asa8i%252Bm%252FlQTPpBUSjQLwrrZh7Fc7tQWknOS1BIa6wh5cOrmu38B9v
h2pAFQujA3RWvFgYz4%252BMaYbn729Pka%252BKHMYlub%252FGzCJCbXwJuMh%252BUYugMzIfNAHK6Z
jp%252FykCAH9eKTTC7zKnkUS2rtrEOpgozV2MNjDsu40u4slRobawxqClsxISB1VdGr8e5369V5RReSDB
hDBmZcRI3z6h%252Bmtv7nyfQ0H3MJodrCv5eAZydbKOURxAuDV7n8MEQ%252BtDDE8S9Z9vSYInHcxlp6
0qVKOMKRvrzTOHInMSY64uakBx%252BUDeXPM2d1TC4k4NM5sPY7JBnEJGzAQdp3dWzX2dGzWjID1PYUqe
Kd%252BaIDWadlM87zPk%253D%26continue%3Dhttps%253A%252F%252Ftakeout.google.com%252F
settings%252Ftakeout%252Fdownload%253Fj%253Deceb1af7-2f4f-4842-91bd-495d70f6eebf%2
526i%253D0%2526pli%253D1%2526rapt%253DAEjHL4M6ZpstK0D59UE_Rd4uT_n4LyIDZAMG-VH_l2J3
dL2nZTufU8E_ujWhJiLyYVvEAITK-lsowT2ejXm_l_by8dlX-AdJwQ%26tcc%3D1%26dbus%3DIN&osidt
=ALWU2ctoNqdPx5TwIWe095rML11yrd3r2CNy2NLK8x2vqLAqGD5eHdxYq4xHTgjdW33a5uHFWS42mhOUs
ozx7hIn9XGob5K4qaz1CNehu6E04qUbRjeSSiDdbtxIdfu3ssqZJ-8IzLJxKC_SSYQOo8GOOY0-t843d5P
1vAN7SoklonYUA5bCJ_AC5Yzf3SsIwzpYlf2289hO_xqnH_CATxq2PoPl8ID8b6iSidrHdlYKoFtk9pFLS
qM&tcc=1&ifkv=Af_xneG4N74OlPaoWg9zWtBlV219YRTVbmCnlxRPo1qaNtdrQF7OWy4otwaRsSbKDUAV
5KKu2JrbQwManage
https://amazon.in/https://www.amazon.in/ap/signin?openid.pape.max_auth_age=3600&op
enid.return_to=https%3A%2F%2Fmusic.amazon.in%2F%3FrefMarker%3Dnull&openid.identity
=http%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0%2Fidentifier_select&openid.assoc_handl
e=amzn_webamp_in&openid.mode=checkid_setup&language=en_IN&openid.claimed_id=http%3
A%2F%2Fspecs.openid.net%2Fauth%2F2.0%2Fidentifier_select&pageId=login&openid.ns=ht
tp%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0amazon.in/ap/signin?openid.pape.max_auth_a
ge=3600&openid.return_to=https%3A%2F%2Fmusic.amazon.in%2F%3FrefMarker%3Dnull&openi
d.identity=http%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0%2Fidentifier_select&openid.a
ssoc_handle=amzn_webamp_in&openid.mode=checkid_setup&language=en_IN&openid.claimed
_id=http%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0%2Fidentifier_select&pageId=login&op
enid.ns=http%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0
https://accounts.google.com/CheckCookie?continue=https%3A%2F%2Ftakeout.google.com%
2Ftakeout%2Fdownload%3Fj%3Deceb1af7-2f4f-4842-91bd-495d70f6eebf%26i%3D5%26user%3D1
0016330465895344243%26rapt%3DAEjHL4OtZ9uNX9is0CbrT7Rr7eWmMGy7FOkEO8Vm6QN6YO8kMNTw
Ayytfy57mOtUakBY7nI58I7XmwWyUxdmwAyYd50KGIT2zg&hl=en&checkedDomains=youtube&checkC
onnection=youtube%3A2803%3A0&pstMsg=1&osid=1&rart=ANgoxcfw-TtMt8r9v32j6nloaKE1Y2M8
bdYGUSeIztALo5knT-gNFXjit3CFT8olYVBuAt4YYtr7jo2h8wyqZBh0p08M2BD1Rg&flowName=GlifWe
bSignIn&ifkv=Af_xneEDptunVR0DmqiYOrqsZjr9U4QfKfkF0Zay4EQf053oBZ4EAcLpYGdsEgYzwtJvh
pGH9xsz-w&chtml=LoginDoneHtml&gidl=EgIIAA=?
https://takeout.google.com/accounts/SetOSID?authuser=0&continue=https://takeout.go
ogle.com/settings/takeout/download?j%3Deceb1af7-2f4f-4842-91bd-495d70f6eebf%26i%3D
0%26pli%3D1&osidt=ALWU2ctRuxa3eLIChOeX4i_RR1pVM5phzTZYcYPRiaYCRY9E0KG9m-r8pQ9-hA8T
ZmLHpm1J5yeHRDonW_RDf7yvcOamaNN-kXKTuQibMZu3Y5XMH7IJh_t6GgBJz9xjo-OxfqgMVGypUPklwX
cOBxaCQKzpks3dhyuHNgtjkkvEAplB757YgY1z4I2q0eTH69K3kw1mENzgUy5Q5-_uUMI9eKhRdnCRaTpl
FtFqrmISN8PUyeTRW68&ifkv=Af_xneHP-vl-APEx_e35xa9NOE_s0gEwM_gfRzbyfAVxwACq5Do_In2Qn
O-8zMNfMh-ywJMIkBMFMA=
https://accounts.google.com/ServiceLogin?continue=https%3A%2F%2Ftakeout.google.com
%2Fsettings%2Ftakeout%2Fdownload%3Fj%3Deceb1af7-2f4f-4842-91bd-495d70f6eebf%26i%3D
0&sacu=1&passive=1209600&authuser=0Sign
https://accounts.google.com/o/oauth2/auth?login_hint=&prompt=login&response_type=c
ode&redirect_uri=https%3A%2F%2Fauth0.openai.com%2Flogin%2Fcallback&scope=email%20p
rofile&state=xqJlDl1HKZID_bxoP_FhadVLzhDnGUN5&client_id=799222349882-ne3i0s9jdm5s0
p7ll2d7tlsi1vc1halt.apps.googleusercontent.com@
https://accounts.google.com/signin/v2/challenge/pwd?TL=AG7eRGA-SeNkoOIwvkKPMuj7f1W
UHgc0WbIxa6KOADEWuU_3SyKCNrJTjxGLQGil&cid=1&continue=https%3A%2F%2Ftakeout.google.
com%2Fsettings%2Ftakeout%2Fdownload%3Fj%3Deceb1af7-2f4f-4842-91bd-495d70f6eebf%26i
%3D0%26pli%3D1&flowName=GlifWebSignIn&followup=https%3A%2F%2Ftakeout.google.com%2F
settings%2Ftakeout%2Fdownload%3Fj%3Deceb1af7-2f4f-4842-91bd-495d70f6eebf%26i%3D0%2
6pli%3D1&ifkv=Af_xneEMUx4wD4rMJ-q_0PNG_xUZuKIMzt0fhVYQk6Timw669qhOaqkNS3v5hMrPrSvV
sbB66t_Vog&osid=1&rart=ANgoxcd609N4H_yTQst--q4_zqP_-p0YAawLC3R64DH-xGkTchgb-jfSuMH
J9bqkiiU4fCMwfFzrDn0VX3ChHszCIxYMqnFe4g=
https://accounts.google.com/signin/v2/challenge/pwd?TL=AG7eRGDvxK_TjYBV038dPuHZBpi
q1LbT9cZo4CJfgD6BB6lbRiUIrwrSjsix1C9U&cid=1&continue=https%3A%2F%2Ftakeout.google.
com%2Ftakeout%2Fdownload%3Fj%3Deceb1af7-2f4f-4842-91bd-495d70f6eebf%26i%3D4%26user
%3D10016330465895344243%26rapt%3DAEjHL4NcPhSAKY3BgJ-L16W94ZoobyO0KUGob1J79pH9AUxx
d25zdN6qKrObFKLDEXRiMD6wE5iUstf3gIRv3aiFs1p90pKB6w&flowName=GlifWebSignIn&followup
=https%3A%2F%2Ftakeout.google.com%2Ftakeout%2Fdownload%3Fj%3Deceb1af7-2f4f-4842-91
bd-495d70f6eebf%26i%3D4%26user%3D10016330465895344243%26rapt%3DAEjHL4NcPhSAKY3BgJ
-L16W94ZoobyO0KUGob1J79pH9AUxxd25zdN6qKrObFKLDEXRiMD6wE5iUstf3gIRv3aiFs1p90pKB6w&i
fkv=Af_xneF4qm9rLteKTsD1x5J_gipi_YAfRDRaRzAVBJP7JfED9FpQ3GLges79S5tI2nrYkeVWZQSUmw
&osid=1&rart=ANgoxceQxMbk59PHpS3iwE_VIWXvOz5cN7MBxI0aYeCU_dawKrZb49-XjA1NhB2KD1Er5
oIYviurOMLtpX20EUb_VplqrjaAEQ
https://takeout.google.com/settings/takeout/downloads?user=10016330465895344243&r
apt=AEjHL4NcPhSAKY3BgJ-L16W94ZoobyO0KUGob1J79pH9AUxxd25zdN6qKrObFKLDEXRiMD6wE5iUst
f3gIRv3aiFs1p90pKB6w
https://accounts.google.com/signin/v2/challenge/pwd?TL=AG7eRGA4kqnFBqQL_8tYhWEJpFi
r_B1RMLz3lklWrUZvEMMqpN54mGFtBIeNaFMf&cid=1&continue=https%3A%2F%2Ftakeout.google.
com%2Fsettings%2Ftakeout%2Fdownload%3Fj%3Deceb1af7-2f4f-4842-91bd-495d70f6eebf%26i
%3D0%26pli%3D1&flowName=GlifWebSignIn&followup=https%3A%2F%2Ftakeout.google.com%2F
settings%2Ftakeout%2Fdownload%3Fj%3Deceb1af7-2f4f-4842-91bd-495d70f6eebf%26i%3D0%2
6pli%3D1&ifkv=Af_xneEFaCko6DuF1qewomOHBQ64mBtjxbweqsVnEcsI6KiDJju_k8v8Aus7mha4GNll
g7WDnEfWqg&osid=1&rart=ANgoxccoWHolY4Dd5Z6nvahnfrIp9OUZA5gythIBwdJ7m6voa_JH8FvazxN

xrbuEbJnH1opsOPmDU8Cnu3sjRFM51ykwDe234w&flowEntry=ServiceLogin=/
https://accounts.google.com/signin/v2/challenge/pwd?TL=AG7eRGCWSSw4DScwQzSlRoFyRBN
e_4Kq5eJv0potfu9Zvt92gaCRFociB-toFx9n&cid=1&continue=https%3A%2F%2Ftakeout.google.
com%2Ftakeout%2Fdownload%3Fj%3Deceb1af7-2f4f-4842-91bd-495d70f6eebf%26i%3D5%26user
%3D100163304658953442343%26rapt%3DAEjHL4OtZ9uNX9Is0CbrT7Rr7eWmMGy7FOkEO8Vm6QN6YO8k
MNTwAyytfy57mOtUakBY7nI58I7XmwWyUxdmwAyYd50KGIT2zg&flowName=GlifWebSignIn&followup
=https%3A%2F%2Ftakeout.google.com%2Ftakeout%2Fdownload%3Fj%3Deceb1af7-2f4f-4842-91
bd-495d70f6eebf%26i%3D5%26user%3D100163304658953442343%26rapt%3DAEjHL4OtZ9uNX9Is0C
brT7Rr7eWmMGy7FOkEO8Vm6QN6YO8kMNTwAyytfy57mOtUakBY7nI58I7XmwWyUxdmwAyYd50KGIT2zg&i
fkv=Af_xneHcwfLs7GBNBhJzw3ln6x9taB8LwDcxfZyvTiB6q-6xqCccQw7B5JewpUIyZICQGhczf2H9&o
sid=1&rart=ANgoxceWFffHRlN6UuGAWyiMjLvjkUr8YlqQGLJALjUX1cnvkBtXWPomwQci1uTbtOXiM8B
vOO4wJHwta2Ii0TuuqpdH-7WlWg=?U
https://doc-64-3k-photos-data-export.googleusercontent.com/download/8s1lbg6at9flgd
e0sb95gnk4lsoqnavv/pb42v0bqk21207ke3tig81b59ie1c81i/1665891000000/2c8b16ad-3152-45
2c-876e-10914c6a283e/100163304658953442343/ADt3v-MAxTwslnvaD68NVYd3xa6s29h1dkdsCtT
dFVjaUeY0h4BZpuTCiyZ6mn6S2GbxV_lkAeynw9HKtiXA1XvuvnVYqcL4QKxRYmxiW3RgzyKKbZBjCGgME
N7DfVzFNNqTLHIOV8H9KQK67Y1ij3418_F-GLuTQSLWWYl_1-_fbDBtjI2946f3Xswy00WxKuylYSEgmqJ
xktS244-s0tZbvLYsrl5Gc_Lf5XSw4n3qJaY9yXEbvPdn9HbX5b6n4h3JYor9kQoz15dsXZ1wvUbfjlDCl
uuXasp2gdO9AsTztTKzCH_c_PQ=?authuser=0&nonce=0dlgu37vqrpq0&user=100163304658953442
343&hash=fio52r4mhe3qgc1cnthdiiosbomhn3j6
https://accounts.google.com/ServiceLogin?continue=https%3A%2F%2Ftakeout.google.com
%2Fsettings%2Ftakeout%2Fdownload%3Fj%3Deceb1af7-2f4f-4842-91bd-495d70f6eebf%26i%3D
7&sacu=1&passive=1209600&authuser=0=
https://accounts.google.com/ServiceLogin?passive=1209600&osid=1&continue=https://t
akeout.google.com/settings/takeout/download?j%3Deceb1af7-2f4f-4842-91bd-495d70f6ee
bf%26i%3D7%26pli%3D1&followup=https://takeout.google.com/settings/takeout/download
?j%3Deceb1af7-2f4f-4842-91bd-495d70f6eebf%26i%3D7%26pli%3D1&rart=ANgoxceSBHEUnlvxC
IZOQXH4qK_DeP_i2Ch0e75LFM3dvtMN4ZWnRAEvsXODFE3W28nfhFcs7qsJD8ao7WYU82Wk9ac_LeOkeg&
authuser=0=
https://accounts.google.com/ServiceLogin?passive=1209600&osid=1&continue=https://t
akeout.google.com/takeout/download?j%3Deceb1af7-2f4f-4842-91bd-495d70f6eebf%26i%3D
4%26user%3D100163304658953442343%26rapt%3DAEjHL4NcPhSAKY3BgJ-L16W94ZOobyO0KUGob1J7
9pH9AUxxd25zdN6qKrObFKLDEXRiMD6wE5iUstf3gIRv3aiFs1p90pKB6w&followup=https://takeou
t.google.com/takeout/download?j%3Deceb1af7-2f4f-4842-91bd-495d70f6eebf%26i%3D4%26u
ser%3D100163304658953442343%26rapt%3DAEjHL4NcPhSAKY3BgJ-L16W94ZOobyO0KUGob1J79pH9A
Uxxd25zdN6qKrObFKLDEXRiMD6wE5iUstf3gIRv3aiFs1p90pKB6w&rart=ANgoxceQxMbk59PHpS3iwE_
VIWXvOz5cN7MBxI0aYeCU_dawKrZb49-XjA1NhB2KD1Er5oIYviurOMLtpX20EUb_VplqrjaAEQ&authus
er=0Sign
https://accounts.google.com/ServiceLogin?passive=1209600&osid=1&continue=https://t
akeout.google.com/settings/takeout/download?j%3Deceb1af7-2f4f-4842-91bd-495d70f6ee
bf%26i%3D0%26pli%3D1&followup=https://takeout.google.com/settings/takeout/download
?j%3Deceb1af7-2f4f-4842-91bd-495d70f6eebf%26i%3D0%26pli%3D1&rart=ANgoxcd609N4H_yTQ
st--q4_zqP_-p0YAawLC3R64DH-xGkTchgb-jfSuMHJ9bqkiiU4fCMwfFzrDn0VX3ChHszCIxYMqnFe4g&
authuser=0Sign
https://takeout.google.com/settings/takeout/downloads?user=100163304658953442343&r
apt=AEjHL4O624A_WelKnPtNuFcczolfsal2YOvwQrabRHFjm3kuvPSMMkXfyJd-TAKJmUkD1-47TJqfYR
-HYTs8FfuVByb5M5C7rA#i=0&j=eceb1af7-2f4f-4842-91bd-495d70f6eebfManage
https://export-download.canva.com/gbC2Q/DAFChjgbC2Q/44/0/0001-27757146082.png?X-Am
z-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAJHKNGJLC2J7OGJ6Q%2F20220602%2Fus
-east-1%2Fs3%2Faws4_request&X-Amz-Date=20220602T181352Z&X-Amz-Expires=51837&X-Amz-
Signature=e7749e3ea3ad7e676bbd5a05eff5862e299545173fa2650a0ed33785a19d7199&X-Amz-S
ignedHeaders=host&response-content-disposition=attachment%3B%20filename%2A%3DUTF-8
%27%27Sri.png&response-expires=Fri%2C%2003%20Jun%202022%2008%3A37%3A49%20GMT
https://accounts.google.com/signin/v2/challenge/pwd?TL=AG7eRGCpXbhU8aze3En-a1CKX-F
TKNmopxvDU04v15rXdrQ_vfnab2RIretDvixF&cid=1&continue=https%3A%2F%2Ftakeout.google.
com%2Fsettings%2Ftakeout%2Fdownload%3Fj%3Deceb1af7-2f4f-4842-91bd-495d70f6eebf%26i
%3D0%26pli%3D1&flowName=GlifWebSignIn&followup=https%3A%2F%2Ftakeout.google.com%2F
settings%2Ftakeout%2Fdownload%3Fj%3Deceb1af7-2f4f-4842-91bd-495d70f6eebf%26i%3D0%2
6pli%3D1&ifkv=Af_xneH-sh9iT-dZfUImHpygpisnJIKBkQyuHKBCOzgPXFL5S2thfc6aZcgr7e4DRapw
_Vp7MtVYMw&osid=1&rart=ANgoxcdlLdjzFb2Laa3Ad3FQjdvzowlXMq3VOQb4PDFhuCBto8ZjROAfewp
az3CLE_4-asoonitRHWIGMevYMFJDyLMUNzCRfg=
https://takeout.google.com/settings/takeout/downloads?user=100163304658953442343&r
apt=AEjHL4O624A_WelKnPtNuFcczolfsal2YOvwQrabRHFjm3kuvPSMMkXfyJd-TAKJmUkD1-47TJqfYR
-HYTs8FfuVByb5M5C7rAhttps://takeout.google.com/settings/takeout/downloads?user=100
163304658953442343&rapt=AEjHL4O624A_WelKnPtNuFcczolfsal2YOvwQrabRHFjm3kuvPSMMkXfyJ
d-TAKJmUkD1-47TJqfYR-HYTs8FfuVByb5M5C7rAhttps://takeout.google.com/settings/takeou
t/downloads?pli=1&rapt=AEjHL4O624A_WelKnPtNuFcczolfsal2YOvwQrabRHFjm3kuvPSMMkXfyJd
-TAKJmUkD1-47TJqfYR-HYTs8FfuVByb5M5C7rACL7gvO79vP8CEAM=application/x-zip-compresse
dapplication/x-zip
https://takeout.google.com/settings/takeout/downloads?user=100163304658953442343&r
apt=AEjHL4M6ZpstK0D59UE_Rd4uT_n4LyIDZAMG-VH_l2J3dL2nZTufU8E_ujWhJiLyYVvEAITK-lsowT
2ejXm_l_by8dlX-AdJwQhttps://takeout.google.com/settings/takeout/downloads?user=100
163304658953442343&rapt=AEjHL4M6ZpstK0D59UE_Rd4uT_n4LyIDZAMG-VH_l2J3dL2nZTufU8E_uj
WhJiLyYVvEAITK-lsowT2ejXm_l_by8dlX-AdJwQhttps://takeout.google.com/settings/takeou
t/downloads?pli=1&rapt=AEjHL4M6ZpstK0D59UE_Rd4uT_n4LyIDZAMG-VH_l2J3dL2nZTufU8E_ujW
hJiLyYVvEAITK-lsowT2ejXm_l_by8dlX-AdJwQCL7gvO79vP8CEAM=application/x-zip-compresse
dapplication/x-zip
https://takeout.google.com/settings/takeout/downloads?user=100163304658953442343&r
apt=AEjHL4OOPV7t0p2Pd0M-tc8jKG62RR4kzb5eouHykzspeiczpdh_YyEhhjq-8nV2_FH-WMZFU2V0eO

KexfoEI189beyAPmEM9A#i=5&j=eceb1af7-2f4f-4842-91bd-495d70f6eebfManage
https://accounts.google.com/CheckCookie?continue=https%3A%2F%2Ftakeout.google.com%
2Fsettings%2Ftakeout%2Fdownload%3Fj%3Deceb1af7-2f4f-4842-91bd-495d70f6eebf%26i%3D0
%26pli%3D1%26rapt%3DAEjHL4Ntv2ojNAJF6dBo29GPogF8yKgPYTQxhPOmLafERngHorGp8e3bhyEpzJ
zdgSka2HUTUodkW1cgaXoXsSVWjedBTW9AeQ&hl=en&checkedDomains=youtube&checkConnection=
youtube%3A331%3A0&pstMsg=1&osid=1&rart=ANgoxcd609N4H_yTQst--q4_zqP_-p0YAawLC3R64DH
-xGkTchgb-jfSuMHJ9bqkiiU4fCMwfFzrDn0VX3ChHszCIxYMqnFe4g&flowName=GlifWebSignIn&ifk
v=Af_xneEMUx4wD4rMJ-q_0PNG_xUZuKIMzt0fhVYQk6Timw669qhOaqkNS3v5hMrPrSvVsbB66t_Vog&c
html=LoginDoneHtml&gidl=EgIIAAManage
https://doc-bg-7g-photos-data-export.googleusercontent.com/download/8s1lbg6at9flgd
e0sb95gnk4lsoqnavv/d4mv4t536djb5h0jkavuj5mftjp4si2p/1664626500000/e1713771-4dbf-46
73-b8c5-9f1d0e67da14/100163304658953442343/ADt3v-OdomNZIjJM-q7JDyg4Id8g9YLGEf7rv0O
jcRUQWLibFK45urZz6WEn5Whl1uUlke7avJS_aEM49go7xnGBVmw0vIutx19mfRK5E07lnj9uBzCH_pU5v
VqMB7CFVH2GBRdrhxxIyDO0ekD6OmxMSxt1qNicpJYGDcm_ifs7rppMlwRkY40ze85GPWj_22VoHWPE9tJ
_Hy5OmB6rb2Voip-uHeet6VR5Hv8_CDUR3w9gPqwIsyjOyTDRLphjpbqk45Mkqnz307ZoSa0xzYERuXUr6
8UDAs7qF-TkSTTMhT86-CmGTCI=?nonce=ukc0e1vattjoi&user=100163304658953442343&authuse
r=0&hash=32m5e9o19pmbt3r2fbgpa11knh5p7fju
https://accounts.google.com/InteractiveLogin?authuser=0&continue=https://takeout.g
oogle.com/settings/takeout/download?j%3Deceb1af7-2f4f-4842-91bd-495d70f6eebf%26i%3
D0%26pli%3D1&ffgf=1&followup=https://takeout.google.com/settings/takeout/download?
j%3Deceb1af7-2f4f-4842-91bd-495d70f6eebf%26i%3D0%26pli%3D1&osid=1&passive=1209600&
rart=ANgoxcdlLdjzFb2Laa3Ad3FQjdvzowlXMq3VOQb4PDFhuCBto8ZjROAfewpaz3CLE_4-asoonitRH
WIGMevYMFJDyLMUNzCRfg&ifkv=Af_xneE5E0oG3qiRr3qdy8Yva71QjT34O3_IvNqvvcRaBEKOrcIkmRU
RqUZTeGFJqNAWRsXSTvD7twSign
https://p303.zlibcdn.com/dtoken/58491fca9ee309989bcb0ca49988ef159V
https://login.microsoftonline.com/common/oauth2/v2.0/authorize?client_id=a81d90ac-
aa75-4cf8-b14c-58bf348528fe&redirect_uri=https%3A%2F%2Fanswers.microsoft.com&respo
nse_type=code%20id_token&scope=openid%20profile&state=OpenIdConnect.Authentication
Properties%3D2Yc9ATRFGJJ72p8YJlsWx2_nWjbJBbIklSonPZkVN7dOAoDvhQYDnwttkFlsKxMlrLZEd
pEe-Lj8nMSkKmS47ngXiu4CEwaWlwAMtmnlMLlvpJcPSSvqrPu5y05-BRGKwDlJ0nrIs1uShIlOlTRb3oo
WEI8OwU8-nkzvqdTFvs8lSu0AoXYLTEvWvOr7pCJWxaiS-ZZ_KO-vX31rSsxZN5jMBjml4FKLUvsyU1WL6
uuNVoyatwawW7xrQWS36dF5_UHB4PfCmMjoBOAVL7H1p0hHJ8aZnSrbUfgRyphEhQMGflqZt-oCRX7dKH2
fSPeXBmLxMlbNu2zNEqgUzF3Bz4RBy6w8QFBycZPD0iFjR1ZPg-9gpyDi-WdC13xySWJL&response_mod
e=form_post&nonce=638210265971214578.NjJiOTMzMGUtN2U4NC00NGMwLWEwMjEtZWIxOTI5OTVjZ
jA1MGQ2MmNiYWYtMWNjYy00MGY0LTkwYWYtZWE2MDBhODcwMzhi&nopa=2&prompt=none&x-client-SK
U=ID_NET472&x-client-ver=6.17.0.0&sso_reload=trueRedirecting
https://export-download.canva.com/b3ZYU/DAFXWsb3ZYU/68/0/0001-43831839971.png?X-Am
z-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAJHKNGJLC2J7OGJ6Q%2F20230323%2Fus
-east-1%2Fs3%2Faws4_request&X-Amz-Date=20230323T034002Z&X-Amz-Expires=12175&X-Amz-
Signature=6a6144bfdb891e3508ce12691cff43c036f66db83ce81251ac77734b687d4ab2&X-Amz-S
ignedHeaders=host&response-content-disposition=attachment%3B%20filename%2A%3DUTF-8
%27%27V-Seva%2520Maiyam%2520Janarthanan%2520L%2520JLP%2520Farms%2520Vedapatty%2520
-%2520Perur%2520Main%2520Road%2520Vedapatty%252C%2520Coimbatore%2520641007%2520988
4230004%2520BILL%2520TO%2520INVOICE%2520%23%2520101%2520CHINMAYA%2520INTERNATIONAL
%2520RESIDENTIAL%2520SCHOOL%252C%2520SWAMI%2520CHINMAYANANDA%2520LANE%252C%2520NAL
LUR%2520VAYAL%2520POST%252C%2520.png&response-expires=Thu%2C%2023%20Mar%202023%200
7%3A02%3A57%20GMT
https://in.pinterest.com/offsite/?token=941-409&url=https%3A%2F%2Fchickpeaexpress.
com%2Frecipes%2Fdiy-mac-cheese-powder%2F&pin=760615824549902147&client_tracking_pa
rams=CwABAAAAEDExMTA0NjczNzYyNjg2NDELAAcAAAAPdW5rbm93bi91bmtub3duAA5c
https://doc-2g-8s-photos-data-export.googleusercontent.com/download/8s1lbg6at9flgd
e0sb95gnk4lsoqnavv/1j2hq12opq1t9cbp00iue54m73f8e76b/1664604000000/0c18a0c0-a714-48
d0-9f1f-82446f353f80/100163304658953442343/ADt3v-PUCDkV6hRDSr4HkihWxIDOihN6RFaj6Mp
Ya0SaiDmc8ZtS6h_EC3KWBxe4peWEPn_nSHy6ME0mtDO08NOQcBOU0ycg08jCoVaT4XJAd-ZKde8zl81lu
qMQYowIMh6I8pabNyB_1EVqKDdZS5bi-1f0fHYZth4hx0gPkAN7nSGgcThdE7oMTRXqGQYvK01CawGv3mA
3nU66Hlwo9RNxy1M7gFp9PNztwgeI_fdx-Uaks2kCVeKXyhjNHtP4D2kqv1Jo3uP4lfm2YHMAhjtm_FmbI
s0yq_WJksQxD6QaBwqYfQQSglc=?authuser=0&nonce=r5i6bbrbu4som&user=100163304658953442
343&hash=4p4snu43h3g11ka8l3pa4m388sk0slu8
https://export-download.canva.com/b3ZYU/DAFXWsb3ZYU/56/0/0001-43453771184.png?X-Am
z-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAJHKNGJLC2J7OGJ6Q%2F20230316%2Fus
-east-1%2Fs3%2Faws4_request&X-Amz-Date=20230316T052818Z&X-Amz-Expires=90725&X-Amz-
Signature=dde97e85a000cbf35018eba2f500996fc07d88bae78a2ea2cc53af39a2c09144&X-Amz-S
ignedHeaders=host&response-content-disposition=attachment%3B%20filename%2A%3DUTF-8
%27%27V-Seva%2520Maiyam%2520Janarthanan%2520L%2520JLP%2520Farms%2520Vedapatty%2520
-%2520Perur%2520Main%2520Road%2520Vedapatty%252C%2520Coimbatore%2520641007%2520988
4230004%2520BILL%2520TO%2520INVOICE%2520%23%2520101%2520CHINMAYA%2520INTERNATIONAL
%2520RESIDENTIAL%2520SCHOOL%252C%2520SWAMI%2520CHINMAYANANDA%2520LANE%252C%2520NAL
LUR%2520VAYAL%2520POST%252C%2520.png&response-expires=Fri%2C%2017%20Mar%202023%200
6%3A40%3A23%20GMT
https://doc-28-c4-photos-data-export.googleusercontent.com/download/8s1lbg6at9flgd
e0sb95gnk4lsoqnavv/tde4dhhvdcfr9iggsui9qbejttmi1mv5/1664685000000/ab056a26-d963-4b
83-989c-4795114305ef/100163304658953442343/ADt3v-OGKFZ7maOnfXQbGOqk-vhOK_6z7BV3fCl
SMy6qwB45XbJm5PXg_mQ8GpfidubEBtZA3sYDHeiQ29_Mh-Mii16kiUWyICzDonJxSPmUoZdSDZUTXESnp
_HTIQNXhaYx_tbrn7X8bPtlIeHPPqGOM8wFtz3eh78tj324oO6E8NowD8bq4rGfzLdWHsQy5dwl5DlAcMA
K68rhzIRNcP-lNrgAlqYyqmBUuif8IWbFshO_GSTxL8Mpmw7cVJNA0aCXbxLRSmVmN433Pp1fMV3OKdZ1V
3W5cJ97k44Wlh5ORKRUf3F9mXE=?authuser=0&nonce=hnqqh5v6o9ovq&user=100163304658953442
343&hash=d4ir1ttc5bdi8qsh95c1alakvg9h00gs
https://accounts.google.com/CheckCookie?continue=https%3A%2F%2Ftakeout.google.com%
2Ftakeout%2Fdownload%3Fj%3Deceb1af7-2f4f-4842-91bd-495d70f6eebf%26i%3D5%26user%3D1

00163304658953442343%26rapt%3DAEjHL4OOPV7t0p2Pd0M-tc8jKG62RR4kzb5eouHykzspeiczpdh_
YyEhhjq-8nV2_FH-WMZFU2V0eOKexfoEI189beyAPmEM9A&hl=en&checkedDomains=youtube&checkC
onnection=youtube%3A343%3A0&pstMsg=1&osid=1&rart=ANgoxceWFffHRlN6UuGAWyiMjLvjkUr8Y
lqQGLJALjUX1cnvkBtXWPomwQci1uTbtOXiM8BvOO4wJHwta2Ii0TuuqpdH-7WlWg&flowName=GlifWeb
SignIn&ifkv=Af_xneHcwfLs7GBNBhJzw3ln6x9taB8LwDcxfZyvTiB6q-6xqCccQw7B5JewpUIyZICQGh
czf2H9&chtml=LoginDoneHtml&gidl=EgIIAAManage
https://takeout.google.com/takeout/download?j=eceb1af7-2f4f-4842-91bd-495d70f6eebf
&i=4&user=100163304658953442343&rapt=AEjHL4NcPhSAKY3BgJ-L16W94ZOobyO0KUGob1J79pH9A
Uxxd25zdN6qKrObFKLDEXRiMD6wE5iUstf3gIRv3aiFs1p90pKB6wSign
https://accounts.google.com/InteractiveLogin?authuser=0&continue=https://takeout.g
oogle.com/takeout/download?j%3Deceb1af7-2f4f-4842-91bd-495d70f6eebf%26i%3D5%26user
%3D100163304658953442343%26rapt%3DAEjHL4OtZ9uNX9Is0CbrT7Rr7eWmMGy7FOkEO8Vm6QN6YO8k
MNTwAyytfy57mOtUakBY7nI58I7XmwWyUxdmwAyYd50KGIT2zg&ffgf=1&followup=https://takeout
.google.com/takeout/download?j%3Deceb1af7-2f4f-4842-91bd-495d70f6eebf%26i%3D5%26us
er%3D100163304658953442343%26rapt%3DAEjHL4OtZ9uNX9Is0CbrT7Rr7eWmMGy7FOkEO8Vm6QN6YO
8kMNTwAyytfy57mOtUakBY7nI58I7XmwWyUxdmwAyYd50KGIT2zg&osid=1&passive=1209600&rart=A
NgoxceWFffHRlN6UuGAWyiMjLvjkUr8YlqQGLJALjUX1cnvkBtXWPomwQci1uTbtOXiM8BvOO4wJHwta2I
i0TuuqpdH-7WlWg&ifkv=Af_xneEPgh3hNMtJjWiaa6zzmSEnKp5pGGkdq8laZSTP_fmoXTcgEKdarO0ry
Z1XpVbUc47nwmF0Sign
https://export-download.canva.com/4HeNc/DAE6Fe4HeNc/16/0/0001-20480963805.png?X-Am
z-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAJHKNGJLC2J7OGJ6Q%2F20220304%2Fus
-east-1%2Fs3%2Faws4_request&X-Amz-Date=20220304T084759Z&X-Amz-Expires=77041&X-Amz-
Signature=cb2cec9f0018b8a1bb26186405cedad80ea46ea23b660b6ab9cc2f4a929ddb08&X-Amz-S
ignedHeaders=host&response-content-disposition=attachment%3B%20filename%2A%3DUTF-8
%27%27Colorful%2520Pastel%2520Abstract%2520Line%2520Paint%2520Blank%2520Page%2520B
order%2520A4.png&response-expires=Sat%2C%2005%20Mar%202022%2006%3A12%3A00%20GMT0
https://export-download.canva.com/DpkI8/DAFA9wDpkI8/40/0/0003-26391836069.png?X-Am
z-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAJHKNGJLC2J7OGJ6Q%2F20220516%2Fus
-east-1%2Fs3%2Faws4_request&X-Amz-Date=20220516T224836Z&X-Amz-Expires=64388&X-Amz-
Signature=b7ae456006a0e8700a09f80a789d9d85c95ff682fc0460d1964c446cbc1491ae&X-Amz-S
ignedHeaders=host&response-content-disposition=attachment%3B%20filename%2A%3DUTF-8
%27%27Sneha.png&response-expires=Tue%2C%2017%20May%202022%2016%3A41%3A44%20GMT
https://takeout.google.com/settings/takeout/downloads?user=100163304658953442343&r
apt=AEjHL4NcPhSAKY3BgJ-L16W94ZOobyO0KUGob1J79pH9AUxxd25zdN6qKrObFKLDEXRiMD6wE5iUst
f3gIRv3aiFs1p90pKB6whttps://takeout.google.com/settings/takeout/downloads?user=100
163304658953442343&rapt=AEjHL4NcPhSAKY3BgJ-L16W94ZOobyO0KUGob1J79pH9AUxxd25zdN6qKr
ObFKLDEXRiMD6wE5iUstf3gIRv3aiFs1p90pKB6whttps://accounts.google.com/CMrxoO/9vP8CEA
M=application/x-zip-compressedapplication/x-zip
https://takeout.google.com/settings/takeout/downloads?user=100163304658953442343&r
apt=AEjHL4OOPV7t0p2Pd0M-tc8jKG62RR4kzb5eouHykzspeiczpdh_YyEhhjq-8nV2_FH-WMZFU2V0eO
KexfoEI189beyAPmEM9Ahttps://takeout.google.com/settings/takeout/downloads?user=100
163304658953442343&rapt=AEjHL4OOPV7t0p2Pd0M-tc8jKG62RR4kzb5eouHykzspeiczpdh_YyEhhj
q-8nV2_FH-WMZFU2V0eOKexfoEI189beyAPmEM9Ahttps://accounts.google.com/COnOhO/9vP8CEA
M=application/x-zip-compressedapplication/x-zip
https://takeout.google.com/settings/takeout/downloads?user=100163304658953442343&r
apt=AEjHL4OtZ9uNX9Is0CbrT7Rr7eWmMGy7FOkEO8Vm6QN6YO8kMNTwAyytfy57mOtUakBY7nI58I7Xmw
WyUxdmwAyYd50KGIT2zghttps://takeout.google.com/settings/takeout/downloads?user=100
163304658953442343&rapt=AEjHL4OtZ9uNX9Is0CbrT7Rr7eWmMGy7FOkEO8Vm6QN6YO8kMNTwAyytfy
57mOtUakBY7nI58I7XmwWyUxdmwAyYd50KGIT2zghttps://accounts.google.com/COnOhO/9vP8CEA
M=application/x-zip-compressedapplication/x-zip
https://takeout.google.com/settings/takeout/downloads?user=100163304658953442343&r
apt=AEjHL4NWW1AGj3JtpFs-8dboW6XQ8V_I7RQUhLP057AP23wwK8vP93iGTMXjG8Lr5hjePf-W8rPtvZ
DRlepOCCxG1BAZzKmbFQhttps://takeout.google.com/settings/takeout/downloads?user=100
163304658953442343&rapt=AEjHL4NWW1AGj3JtpFs-8dboW6XQ8V_I7RQUhLP057AP23wwK8vP93iGTM
XjG8Lr5hjePf-W8rPtvZDRlepOCCxG1BAZzKmbFQhttps://takeout.google.com/settings/takeou
t/downloads?user=100163304658953442343&rapt=AEjHL4NWW1AGj3JtpFs-8dboW6XQ8V_I7RQUhL
P057AP23wwK8vP93iGTMXjG8Lr5hjePf-W8rPtvZDRlepOCCxG1BAZzKmbFQCNbRlO79vP8CEAM=applic
ation/x-zip-compressedapplication/x-zip
https://takeout.google.com/settings/takeout/downloads?user=100163304658953442343&r
apt=AEjHL4NWW1AGj3JtpFs-8dboW6XQ8V_I7RQUhLP057AP23wwK8vP93iGTMXjG8Lr5hjePf-W8rPtvZ
DRlepOCCxG1BAZzKmbFQhttps://takeout.google.com/settings/takeout/downloads?user=100
163304658953442343&rapt=AEjHL4NWW1AGj3JtpFs-8dboW6XQ8V_I7RQUhLP057AP23wwK8vP93iGTM
XjG8Lr5hjePf-W8rPtvZDRlepOCCxG1BAZzKmbFQhttps://takeout.google.com/settings/takeou
t/downloads?pli=1&rapt=AEjHL4NWW1AGj3JtpFs-8dboW6XQ8V_I7RQUhLP057AP23wwK8vP93iGTMX
jG8Lr5hjePf-W8rPtvZDRlepOCCxG1BAZzKmbFQCOGj2e/9vP8CEAM=application/x-zip-compresse
dapplication/x-zip
https://accounts.google.com/ServiceLogin?passive=1209600&osid=1&continue=https://t
akeout.google.com/settings/takeout/download?j%3Deceb1af7-2f4f-4842-91bd-495d70f6ee
bf%26i%3D7%26pli%3D1&followup=https://takeout.google.com/settings/takeout/download
?j%3Deceb1af7-2f4f-4842-91bd-495d70f6eebf%26i%3D7%26pli%3D1&rart=ANgoxceSBHEUnlvxC
IZOQXH4qK_DeP_i2Ch0e75LFM3dvtMN4ZWnRAEvsXODFE3W28nfhFcs7qsJD8ao7WYU82Wk9ac_LeOkeg&
authuser=0Manage
https://export-download.canva.com/b3ZYU/DAFXWsb3ZYU/33/0-45009973376.pdf?X-Amz-Alg
orithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAJHKNGJLC2J7OGJ6Q%2F20230110%2Fus-east
-1%2Fs3%2Faws4_request&X-Amz-Date=20230110T210632Z&X-Amz-Expires=58675&X-Amz-Signa
ture=1ddf531d43a681b311126aa5180605b092d3504093864b2fb37b73b27206cc17&X-Amz-Signed
Headers=host&response-content-disposition=attachment%3B%20filename%2A%3DUTF-8%27%2
7V-Seva%2520Maiyam%2520Janarthanan%2520L%2520JLP%2520Farms%2520Vedapatty%2520-%252
0Perur%2520Main%2520Road%2520Vedapatty%252C%2520Coimbatore%2520641007%252098842300

04%2520BILL%2520TO%2520INVOICE%2520%23%2520101%2520CHINMAYA%2520INTERNATIONAL%2520
RESIDENTIAL%2520SCHOOL%252C%2520SWAMI%2520CHINMAYANANDA%2520LANE%252C%2520NALLUR%2
520VAYAL%2520POST%252C%2520.pdf&response-expires=Wed%2C%2011%20Jan%202023%2013%3A2
4%3A27%20GMT
https://export-download.canva.com/b3ZYU/DAFXWsb3ZYU/30/0-45009706421.pdf?X-Amz-Alg
orithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAJHKNGJLC2J7OGJ6Q%2F20230111%2Fus-east
-1%2Fs3%2Faws4_request&X-Amz-Date=20230111T030841Z&X-Amz-Expires=36938&X-Amz-Signa
ture=3835dc3938ad415db3292af900e315c009dbc67d17944638853a7d441fdb62ae&X-Amz-Signed
Headers=host&response-content-disposition=attachment%3B%20filename%2A%3DUTF-8%27%2
7V-Seva%2520Maiyam%2520Janarthanan%2520L%2520JLP%2520Farms%2520Vedapatty%2520-%252
0Perur%2520Main%2520Road%2520Vedapatty%252C%2520Coimbatore%2520641007%252098842300
04%2520BILL%2520TO%2520INVOICE%2520%23%2520101%2520CHINMAYA%2520INTERNATIONAL%2520
RESIDENTIAL%2520SCHOOL%252C%2520SWAMI%2520CHINMAYANANDA%2520LANE%252C%2520NALLUR%2
520VAYAL%2520POST%252C%2520.pdf&response-expires=Wed%2C%2011%20Jan%202023%2013%3A2
4%3A19%20GMT
https://export-download.canva.com/b3ZYU/DAFXWsb3ZYU/27/0-45009365609.pdf?X-Amz-Alg
orithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAJHKNGJLC2J7OGJ6Q%2F20230111%2Fus-east
-1%2Fs3%2Faws4_request&X-Amz-Date=20230111T101718Z&X-Amz-Expires=9795&X-Amz-Signat
ure=a8b86d1f53b9c3be7934d878c4dca013cfea423f05f55835ace732f081ed0441&X-Amz-SignedH
eaders=host&response-content-disposition=attachment%3B%20filename%2A%3DUTF-8%27%27
V-Seva%2520Maiyam%2520Janarthanan%2520L%2520JLP%2520Farms%2520Vedapatty%2520-%2520
Perur%2520Main%2520Road%2520Vedapatty%252C%2520Coimbatore%2520641007%2520988423000
4%2520BILL%2520TO%2520INVOICE%2520%23%2520101%2520CHINMAYA%2520INTERNATIONAL%2520R
ESIDENTIAL%2520SCHOOL%252C%2520SWAMI%2520CHINMAYANANDA%2520LANE%252C%2520NALLUR%25
20VAYAL%2520POST%252C%2520.pdf&response-expires=Wed%2C%2011%20Jan%202023%2013%3A00
%3A33%20GMTm
https://doc-3o-8k-photos-data-export.googleusercontent.com/download/8s1lbg6at9flgd
e0sb95gnk4lsoqnavv/fg7pmpbvkjhbnn66vijvetnk6ucccbh2/1663987500000/2ec5ea9b-14b8-45
84-bb34-6d667ae0a61f/100163304658953442343/ADt3v-MttGi_AZa4ijvXsL1VBkHmhDrFte6UI8o
6nRsM5tpHurcZhhBPMgg2qBMOJgxPk41EsGknQEx-AAZCzzdURQarp_AqyjE8ko-ZXh9606nC6eUgcKuCL
2mJtyai5p6XV3liDxbP4dYCAWet4hGOXjEs88RWnl-uR9lAiQrifKwRVWuUV0ijxnO7ntkJ8Sn-JHhkuHX
cqveTPgw548jitxmT4kq5yMMa4ozgthaJHkM5rq2xyS4AFTDokljbhuWazJn-iNs7foVZy24RBAjt6BcaK
ug0WsyzAn9bEaXCpPHUonzaZbE=?authuser=0&nonce=str9uiogr3ad8&user=100163304658953442
343&hash=dem5s7kfv6c00aq28roqtirtgseiq86u
https://takeout.google.com/settings/takeout/downloads?user=100163304658953442343&r
apt=AEjHL4O624A_WelKnPtNuFcczolfsal2YOvwQrabRHFjm3kuvPSMMkXfyJd-TAKJmUkD1-47TJqfYR
-HYTs8FfuVByb5M5C7rA
https://accounts.google.com/CheckCookie?continue=https%3A%2F%2Ftakeout.google.com%
2Fsettings%2Ftakeout%2Fdownload%3Fj%3Deceb1af7-2f4f-4842-91bd-495d70f6eebf%26i%3D0
%26pli%3D1%26rapt%3DAEjHL4O624A_WelKnPtNuFcczolfsal2YOvwQrabRHFjm3kuvPSMMkXfyJd-TA
KJmUkD1-47TJqfYR-HYTs8FfuVByb5M5C7rA&hl=en&checkedDomains=youtube&checkConnection=
youtube%3A290%3A0&pstMsg=1&osid=1&rart=ANgoxcdlLdjzFb2Laa3Ad3FQjdvzowlXMq3VOQb4PDF
huCBto8ZjROAfewpaz3CLE_4-asoonitRHWIGMevYMFJDyLMUNzCRfg&flowName=GlifWebSignIn&ifk
v=Af_xneH-sh9iT-dZfUImHpygpisnJIKBkQyuHKBCOzgPXFL5S2thfc6aZcgr7e4DRapw_Vp7MtVYMw&c
html=LoginDoneHtml&gidl=EgIIAAManage
https://takeout.google.com/accounts/SetOSID?authuser=0&continue=https%3A%2F%2Facco
unts.youtube.com%2Faccounts%2FSetSID%3Fssdc%3D1%26sidt%3DALWU2cue8%252F1KG6kYTLlOz
wcweml7NNhthp3iEXL2teVVqFtV9kbt5CNH6droXD3d112DxR2AmaUkY7gPxkgelcDVEiw6XwCiDuWaldI
ItxMHcmuxTBh%252BNJKglPvknnkmreARbCLW1PhS5HrJvewHz%252BdqHkUZazH9AqvA9uUjB16aT40Jc
D%252BQJXjRjWVhYZOof2tM%252Bfh4EXRF9Hv9wVUFNfUe0w%252FNp5FktG0aTUbJMCJ91Q6q9Gsbcr0
K6amzAS%252BcSVs05ny17HhplCf8Z%252Bh5W9uFQ3lmhcydwANxr0SCPC8AtMYwQo6YjZqyYMootJGj7
exc4phhdI8Zuoxse44LlOuaAhgNWI7ZIqmAYL1L01kIii8RXbqIAG6F1vAlcNOAdncGnvw2hH%252BAsgX
B%252Fq4pOUeti6CLR9IrMuxq59Qj7amWtgmulUQGXmqmDlqjNczDdemwUNMnBSt61LXuRIInUimuSI7aE
Rw85EnSeb%252BdcLmYAuPG0W1Rfl94AFWDV4X0cPXZjCZ6fb%252BW8JnBA%252F9pJEMrWUm9eRenGky
w5d6qD%252BGw7dWOMZ1zK0U%253D%26continue%3Dhttps%253A%252F%252Ftakeout.google.com%
252Fsettings%252Ftakeout%252Fdownload%253Fj%253Deceb1af7-2f4f-4842-91bd-495d70f6ee
bf%2526i%253D0%2526pli%253D1%2526rapt%253DAEjHL4O624A_WelKnPtNuFcczolfsal2YOvwQrab
RHFjm3kuvPSMMkXfyJd-TAKJmUkD1-47TJqfYR-HYTs8FfuVByb5M5C7rA%26tcc%3D1%26dbus%3DIN&o
sidt=ALWU2cu0cBzFmDCk1w8Gki9WNS9ISuAoZNKSZQbf1YzJ3anjFYh5PWjRtlzlY_Kv3xZx8Yp17MbUL
JLSfAZbyjWLyV50qZgpIldobZT60MzKKCGAH8Ug8yO4vwQsy508gInBvPFLrNP7mNZD2ApTQVlVxYSKst4
cheWaEa_Tkf6kBJ-imIGuMNq4rkKUImBDwQhvYYn4FNsGYolJUq6lIwACwpHHcIfYvcCUEJbulzl_UVBed
ZU9-XU&tcc=1&ifkv=Af_xneFcgikBo7QuGqDl1_YYCmYypUXC1-M7hFKTaJucTsgrgTNrCjI0SguzZsvP
SicxJ3Gz06VoIgManage
https://doc-9k-5k-photos-data-export.googleusercontent.com/download/8s1lbg6at9flgd
e0sb95gnk4lsoqnavv/erk5qjfdme1ajr8jmdtgip7dkoih6dd5/1664685000000/6287a63c-1fd2-41
20-9af4-f47c2969cc14/100163304658953442343/ADt3v-O6gL29GFYGMIazfi6Bw293niiT2FIn8ZA
rFwNX8CgnFA60TpXT0LgzW6ngquoJ1Qsm6ZqsNueMlHOqVjrh0bVi37OSMDTaOBr2JpLYLOo7ZEyc70aEx
Bgx-55MqfVn8F1GGCS_jdJb-DG4ppzBak-hokOZKwhiZucgCiJGqbJHR0iO9glsVFm-V8_T8X5dz8dPtZg
jiKui_NX_bAXD4r2QG_j2uzhrlHI5l8C6iw-92eTWSXY7z7iqzYv81uMhj9duKxyq40HWUqT32w1RZjPRD
8UKBNfLn1SFLS4MjFZzRde-1QU=?authuser=0&nonce=jclvmldobusje&user=100163304658953442
343&hash=b4fva8rv77oup0ck4aqmrvb265egmtnp
https://doc-c0-6g-photos-data-export.googleusercontent.com/download/8s1lbg6at9flgd
e0sb95gnk4lsoqnavv/e2c1s5mfi3rs8nau3ajql1rm34grnen0/1664685000000/97f76cc9-5dba-44
73-9fd8-0f01f9f6d41c/100163304658953442343/ADt3v-NgqaWmeOfCMFX5Veh2Nk-wNiFvYhvOMpd
ke_qBoTmj0r7x2Id1sqa0_sl9jjKwhgZoGChuYPffiO7VNryv1uG7S_Cx_FhILeKpXrBXBQARKjCjK--85
f-MEzKXYuNQFYRlun_GzRonR5zUjJfQMRyedNfdrpVRXYKAYsYG7FaUNuQuluqHA2IuPNuJzYAtcmDzeXR
3gGh18LDbDBK1ZvUagIHlmg1J2s5g4j2-VrglB4q6AKT4bijslbbPXupYzCKaAjWNtsP9mRFUo54VwNO0o
9n7M3nTKxKbB8Ym7eVkTqMtzcU=?authuser=0&nonce=ujb6bdguo0mli&user=100163304658953442
343&hash=ag6jk0rmmckvfa5okihll9g58espmlcf

https://takeout.google.com/takeout/download?j=eceb1af7-2f4f-4842-91bd-495d70f6eebf
&i=4&user=100163304658953442343&rapt=AEjHL4Pb-JTIX5RcJRpoJ1r4dyxvRUge5X0CnYJUvwPtP
cUIgf_1YDM_kwn1KGXv-QhMhtifpQRHx3HXEcIrdomh86qdCvrvowManage
https://doc-5g-30-photos-data-export.googleusercontent.com/download/8s11bg6at9flgd
e0sb95gnk41soqnavv/1c7kn3lv77mbkc98ogoiut8nv37qsreo/1687144500000/9ad8d71a-aaff-45
4b-8ce2-8a3a6682eb9e/100163304658953442343/ADt3v-NmSaKInjOwb2yMbMgu6ljQZ0jJZUZO_k7
L_E72NiPwBfivAf7a9Mh01tqyCOe5jRFiyZrEyMjDw-zIIMcb9AKdp3DJR9a50-6emPBqzP51CAvWtisIl
bDSGJvzvrgtqkoOogKQcfwx0MymYnLOFIvVVTkaiU--Lzk28L_qeWykdH86VZKsJ0GLVeUYzifgCsImp5v
z0Vo0F945_uLH7fdZUCain7STVFnYxaZv3Vx4isEqF-aRkOxHrpw5fDaP2mFtloxOu60QkncqIGimMA4_H
MQ4koR15BPfDYzGdPCk4QSRLaY=?authuser=0&nonce=bcc740127dj12&user=100163304658953442
343&hash=9n2in78q5cv9tpco4ieep13pjl81pbq3
https://accounts.google.com/signin/v2/challenge/dp?login_hint&prompt=login&respons
e_type=code&redirect_uri=https%3A%2F%2Fauth0.openai.com%2Flogin%2Fcallback&scope=e
mail%20profile&state=makPXaQpM7TzqUGjpqrwMmT8fwYbmuRt&client_id=799222349882-ne3i0
s9jdm5s0p7ll2d7tlsi1vc1halt.apps.googleusercontent.com&service=lso&o2v=1&flowName=
GeneralOAuthFlow&cid=2&navigationDirection=forward&TL=AG7eRGAeW1uzyoPjQ6avRWNQyy2Q
jdojNQF6mRHJuNG7qpPo-bqwXhk3N3y9Pgqz
https://accounts.google.com/signin/v2/challenge/pwd?TL=AG7eRGD62HrfQ10CYjVLeQD7T-i
1X52CXHdg5DSWkj8OLEVljQNY9so_XmNTPFFF&cid=1&continue=https%3A%2F%2Ftakeout.google.
com%2Ftakeout%2Fdownload%3Fj%3Deceb1af7-2f4f-4842-91bd-495d70f6eebf%26i%3D5%26user
%3D100163304658953442343%26rapt%3DAEjHL4NWW1AGj3JtpFs-8dboW6XQ8V_I7RQUhLP057AP23ww
K8vP93iGTMXjG8Lr5hjePf-W8rPtvZDRlepOCCxG1BAZzKmbFQ&flowName=GlifWebSignIn&followup
=https%3A%2F%2Ftakeout.google.com%2Ftakeout%2Fdownload%3Fj%3Deceb1af7-2f4f-4842-91
bd-495d70f6eebf%26i%3D5%26user%3D100163304658953442343%26rapt%3DAEjHL4NWW1AGj3JtpF
s-8dboW6XQ8V_I7RQUhLP057AP23wwK8vP93iGTMXjG8Lr5hjePf-W8rPtvZDRlepOCCxG1BAZzKmbFQ&i
fkv=Af_xneEDptunVR0DmqiYOrqsZjr9U4QfKfkF0Zay4EQf053oBZ4EAcLpYGdsEgYzwtJvhpGH9xsz-w
&osid=1&rart=ANgoxcfw-TtMt8r9v32j6nloaKE1Y2M8bdYGUSeIztALo5knT-gNFXjit3CFT8olYVBuA
t4YYtr7jo2h8wyqZBh0p08M2BD1RgSign
https://accounts.google.com/CheckCookie?continue=https%3A%2F%2Ftakeout.google.com%
2Fsettings%2Ftakeout%2Fdownload%3Fj%3Deceb1af7-2f4f-4842-91bd-495d70f6eebf%26i%3D0
%26pli%3D1%26rapt%3DAEjHL4M6ZpstK0D59UE_Rd4uT_n4LyIDZAMG-VH_l2J3dL2nZTufU8E_ujWhJi
LyYVvEAITK-lsowT2ejXm_l_by8dlX-AdJwQ&hl=en&checkedDomains=youtube&checkConnection=
youtube%3A737%3A0&pstMsg=1&osid=1&rart=ANgoxccoWHolY4Dd5Z6nvahnfrIp9OUZA5gythIBwdJ
7m6voa_JH8FvazxNxrbuEbJnH1opsOPmDU8Cnu3sjRFM51ykwDe234w&flowName=GlifWebSignIn&ifk
v=Af_xneEFaCko6DuF1qewomOHBQ64mBtjxbweqsVnEcsI6KiDJju_k8v8Aus7mha4GNllg7WDnEfWqg&c
html=LoginDoneHtml&gidl=EgIIAAManage
https://accounts.google.com/signin/v2/challenge/pwd?TL=AG7eRGA4kqnFBqQL_8tYhWEJpFi
r_B1RMLz3lklWrUZvEMMqpN54mGFtBIeNaFMf&cid=1&continue=https%3A%2F%2Ftakeout.google.
com%2Fsettings%2Ftakeout%2Fdownload%3Fj%3Deceb1af7-2f4f-4842-91bd-495d70f6eebf%26i
%3D0%26pli%3D1&flowName=GlifWebSignIn&followup=https%3A%2F%2Ftakeout.google.com%2F
settings%2Ftakeout%2Fdownload%3Fj%3Deceb1af7-2f4f-4842-91bd-495d70f6eebf%26i%3D0%2
6pli%3D1&ifkv=Af_xneEFaCko6DuF1qewomOHBQ64mBtjxbweqsVnEcsI6KiDJju_k8v8Aus7mha4GNll
g7WDnEfWqg&osid=1&rart=ANgoxccoWHolY4Dd5Z6nvahnfrIp9OUZA5gythIBwdJ7m6voa_JH8FvazxN
xrbuEbJnH1opsOPmDU8Cnu3sjRFM51ykwDe234w&flowEntry=ServiceLoginSign
https://accounts.google.com/o/oauth2/auth?login_hint=&prompt=login&response_type=c
ode&redirect_uri=https%3A%2F%2Fauth0.openai.com%2Flogin%2Fcallback&scope=email%20p
rofile&state=ZE6XSxy5HI-keTqdv4Kh6Tcaag-A19Ab&client_id=799222349882-ne3i0s9jdm5s0
p7ll2d7tlsi1vc1halt.apps.googleusercontent.com
https://accounts.google.com/o/oauth2/auth?login_hint=&prompt=login&response_type=c
ode&redirect_uri=https%3A%2F%2Fauth0.openai.com%2Flogin%2Fcallback&scope=email%20p
rofile&state=xqJlDllHKZID_bxoP_FhadVLzhDnGUN5&client_id=799222349882-ne3i0s9jdm5s0
p7ll2d7tlsi1vc1halt.apps.googleusercontent.com
https://accounts.google.com/CheckCookie?continue=https%3A%2F%2Ftakeout.google.com%
2Ftakeout%2Fdownload%3Fj%3Deceb1af7-2f4f-4842-91bd-495d70f6eebf%26i%3D4%26user%3D1
00163304658953442343%26rapt%3DAEjHL4NcPhSAKY3BgJ-L16W94ZOoby00KUGob1J79pH9AUxxd25z
dN6qKrObFKLDEXRiMD6wE5iUstf3gIRv3aiFs1p90pKB6w&hl=en&checkedDomains=youtube&checkC
onnection=youtube%3A471%3A0&pstMsg=1&osid=1&rart=ANgoxce-BNgFexYa18XlTJ3tWye9JjUm5
xMaa7dMHNMfp5-cxsvuPqlV0M0x3SuwohSQVRvdI6g1bCK3pbi-Ro6r50a5XadUaw&flowName=GlifWeb
SignIn&ifkv=Af_xneHmk4Dl-BHMSXcGL8bpDs2sD6hIWBVThGSWqCVx2XMp6jK-wAQPbTi0xtt59Hrr-U
L173WXmQ&chtml=LoginDoneHtml&gidl=EgIIAAManage
https://hotels.eglobe-solutions.com/directhotels/googlehotelads_landing?roomid=308
74&checkin=2023-06-11&nights=1&currency=INR&googlesite=mapresults&userdevice=deskt
op&bookingSource=GoogleCPC&adType=0CRESCENT
https://amazon.in/https://www.amazon.in/ap/signin?openid.pape.max_auth_age=0&openi
d.return_to=https%3A%2F%2Fmusic.amazon.in%2F%3FrefMarker%3Dnull&openid.identity=ht
tp%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0%2Fidentifier_select&openid.assoc_handle=a
mzn_webamp_in&openid.mode=checkid_setup&language=en_IN&openid.claimed_id=http%3A%2
F%2Fspecs.openid.net%2Fauth%2F2.0%2Fidentifier_select&pageId=login&openid.ns=http%
3A%2F%2Fspecs.openid.net%2Fauth%2F2.0amazon.in/ap/signin?openid.pape.max_auth_age=
0&openid.return_to=https%3A%2F%2Fmusic.amazon.in%2F%3FrefMarker%3Dnull&openid.iden
tity=http%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0%2Fidentifier_select&openid.assoc_h
andle=amzn_webamp_in&openid.mode=checkid_setup&language=en_IN&openid.claimed_id=ht
tp%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0%2Fidentifier_select&pageId=login&openid.n
s=http%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0
https://takeout.google.com/accounts/SetOSID?authuser=0&continue=https%3A%2F%2Facco
unts.youtube.com%2Faccounts%2FSetSID%3Fssdc%3D1%26sidt%3DALWU2cvVW%252FXQdYFlduDK6
RFqd7YdDEnBm5TBLRh8VgxrcL0KS0VeNFrEXYUa1KPMye0wqHrD5ibUS1n2uypyj8XHf8G%252BYpX0SsM
%252B2DOqrsfNHUmpqNreEoQxn0UoKV1fvd2WRQVtglytyjNZT8rWEVdFaD%252BrHeVwzdwJg9ntu%252

B3jjRzchD6CpDzo68WBa7ZU2dIF9XRAjdoHW%252BPbDvJR9VXwaAojeGtpAXy5JRGBLXYNxWfJeTojI%2
52Bfp3DMinDhb0NAVSTex5yoqtwHGXZRjH2aUZ00c2rBmFJo6%252BvHE3b8zAadMaoSBiXq0x4N%252Fc
QRyne6S%252FcfDZvD49xCZsls6yP7e45pBenX1BmVXz3yPFEVtaUiF4IqvnsyLXp9yukXvKh5bJ16xtqA
9gA1IvBK7ImtiYtW8DpNmPxFOrMOWpVzLa%252FaT7nBFMFqPmJDTlZEnqkg1UNh0URdvnDxgeUVTFT%25
2BbGrFeooiBsfET9xyNlPzywavYRnLoe0KJ%252B4SVh1DJvQbAHwoDxRD%252Fx%252FoUZQTU%252BWI
y62bsRH7tf6NNyoO1VYdoURUCqoqMYIU%253D%26continue%3Dhttps%253A%252F%252Ftakeout.goo
gle.com%252Ftakeout%252Fdownload%253Fj%253Deceb1af7-2f4f-4842-91bd-495d70f6eebf%25
26i%253D4%2526user%253D100163304658953442343%2526rapt%253DAEjHL4Pb-JTIX5RcJRpoJ1r4
dyxvRUge5X0CnYJUvwPtPcUIgf_1YDM_kwn1KGXv-QhMhtifpQRHx3HXEcIrdomh86qdCvrvow%26tcc%3
D1%26dbus%3DIN&osidt=ALWU2cvq4iCkalNsZpMS55X836h4YWRZlN-exJlz91Lh0gB_ywO2mZDifI8cS
DhOeZlQce___xO9LtExqvyK_0FXTvd7z6j4tr06FcMrtGzlIdclSMb3RoekMmHQE0LXf6wLrXd0ZM0jUh6
WtVPfDQZbcN5KucmNHvV-ebO7xFwAPTi8gYn1BCiXXCU4_Dh4b0t7RdJQHn8rtkcNTnb1tsx-P4GNlgebj
JwP0rkqWRl2u4nZq1JpE2Y&tcc=1&ifkv=Af_xneEhWebGAj6yLUQaqzXOwBM6QYJeNK7Ff_Z4vvWmh_pE
xEEBXEtgJfzK-UFE9h9Kb2zdIg8gvwManage
https://accounts.google.com/CheckCookie?continue=https%3A%2F%2Ftakeout.google.com%
2Ftakeout%2Fdownload%3Fj%3Deceb1af7-2f4f-4842-91bd-495d70f6eebf%26i%3D4%26user%3D1
00163304658953442343%26rapt%3DAEjHL4Pb-JTIX5RcJRpoJ1r4dyxvRUge5X0CnYJUvwPtPcUIgf_1
YDM_kwn1KGXv-QhMhtifpQRHx3HXEcIrdomh86qdCvrvow&hl=en&checkedDomains=youtube&checkC
onnection=youtube%3A299%3A0&pstMsg=1&osid=1&rart=ANgoxceQxMbk59PHpS3iwE_VIWXvOz5cN
7MBxI0aYeCU_dawKrZb49-XjA1NhB2KD1Er5oIYviurOMLtpX20EUb_VplqrjaAEQ&flowName=GlifWeb
SignIn&ifkv=Af_xneHjXMJ8PKWRpiGOZf2jEFkQ-JVgFJTaAKNAomRdUUa-KQvMnhXM9FOSg-HjBYCBjO
oH34htag&chtml=LoginDoneHtml&gidl=EgIIAAManage
https://takeout.google.com/https://takeout.google.com/settings/takeout/downloads?u
ser=100163304658953442343&rapt=AEjHL4Pb-JTIX5RcJRpoJ1r4dyxvRUge5X0CnYJUvwPtPcUIgf_
1YDM_kwn1KGXv-QhMhtifpQRHx3HXEcIrdomh86qdCvrvowtakeout.google.com/settings/takeout
/downloads?user=100163304658953442343&rapt=AEjHL4Pb-JTIX5RcJRpoJ1r4dyxvRUge5X0CnYJ
UvwPtPcUIgf_1YDM_kwn1KGXv-QhMhtifpQRHx3HXEcIrdomh86qdCvrvow
https://takeout.google.com/https://takeout.google.com/settings/takeout/downloads?u
ser=100163304658953442343&rapt=AEjHL4Pb-JTIX5RcJRpoJ1r4dyxvRUge5X0CnYJUvwPtPcUIgf_
1YDM_kwn1KGXv-QhMhtifpQRHx3HXEcIrdomh86qdCvrvow#i=4&j=eceb1af7-2f4f-4842-91bd-495d
70f6eebftakeout.google.com/settings/takeout/downloads?user=100163304658953442343&r
apt=AEjHL4Pb-JTIX5RcJRpoJ1r4dyxvRUge5X0CnYJUvwPtPcUIgf_1YDM_kwn1KGXv-QhMhtifpQRHx3
HXEcIrdomh86qdCvrvow#i=4&j=eceb1af7-2f4f-4842-91bd-495d70f6eebf
https://takeout.google.com/https://takeout.google.com/settings/takeout/downloads?u
ser=100163304658953442343&rapt=AEjHL4Pb-JTIX5RcJRpoJ1r4dyxvRUge5X0CnYJUvwPtPcUIgf_
1YDM_kwn1KGXv-QhMhtifpQRHx3HXEcIrdomh86qdCvrvowtakeout.google.com/settings/takeout
/downloads?user=100163304658953442343&rapt=AEjHL4Pb-JTIX5RcJRpoJ1r4dyxvRUge5X0CnYJ
UvwPtPcUIgf_1YDM_kwn1KGXv-QhMhtifpQRHx3HXEcIrdomh86qdCvrvow
https://takeout.google.com/https://takeout.google.com/settings/takeout/downloads?u
ser=100163304658953442343&rapt=AEjHL4Pb-JTIX5RcJRpoJ1r4dyxvRUge5X0CnYJUvwPtPcUIgf_
1YDM_kwn1KGXv-QhMhtifpQRHx3HXEcIrdomh86qdCvrvowtakeout.google.com/settings/takeout
/downloads?user=100163304658953442343&rapt=AEjHL4Pb-JTIX5RcJRpoJ1r4dyxvRUge5X0CnYJ
UvwPtPcUIgf_1YDM_kwn1KGXv-QhMhtifpQRHx3HXEcIrdomh86qdCvrvow
https://takeout.google.com/https://takeout.google.com/settings/takeout/downloads?u
ser=100163304658953442343&rapt=AEjHL4Pb-JTIX5RcJRpoJ1r4dyxvRUge5X0CnYJUvwPtPcUIgf_
1YDM_kwn1KGXv-QhMhtifpQRHx3HXEcIrdomh86qdCvrvow#i=4&j=eceb1af7-2f4f-4842-91bd-495d
70f6eebftakeout.google.com/settings/takeout/downloads?user=100163304658953442343&r
apt=AEjHL4Pb-JTIX5RcJRpoJ1r4dyxvRUge5X0CnYJUvwPtPcUIgf_1YDM_kwn1KGXv-QhMhtifpQRHx3
HXEcIrdomh86qdCvrvow#i=4&j=eceb1af7-2f4f-4842-91bd-495d70f6eebf
https://takeout.google.com/https://takeout.google.com/settings/takeout/downloads?u
ser=100163304658953442343&rapt=AEjHL4M6ZpstK0D59UE_Rd4uT_n4LyIDZAMG-VH_l2J3dL2nZTu
fU8E_ujWhJiLyYVvEAITK-lsowT2ejXm_l_by8dlX-AdJwQ#i=0&j=eceb1af7-2f4f-4842-91bd-495d
70f6eebftakeout.google.com/settings/takeout/downloads?user=100163304658953442343&r
apt=AEjHL4M6ZpstK0D59UE_Rd4uT_n4LyIDZAMG-VH_l2J3dL2nZTufU8E_ujWhJiLyYVvEAITK-lsowT
2ejXm_l_by8dlX-AdJwQ#i=0&j=eceb1af7-2f4f-4842-91bd-495d70f6eebf
https://takeout.google.com/https://takeout.google.com/settings/takeout/downloads?u
ser=100163304658953442343&rapt=AEjHL4M6ZpstK0D59UE_Rd4uT_n4LyIDZAMG-VH_l2J3dL2nZTu
fU8E_ujWhJiLyYVvEAITK-lsowT2ejXm_l_by8dlX-AdJwQ#i=1&j=eceb1af7-2f4f-4842-91bd-495d
70f6eebftakeout.google.com/settings/takeout/downloads?user=100163304658953442343&r
apt=AEjHL4M6ZpstK0D59UE_Rd4uT_n4LyIDZAMG-VH_l2J3dL2nZTufU8E_ujWhJiLyYVvEAITK-lsowT
2ejXm_l_by8dlX-AdJwQ#i=1&j=eceb1af7-2f4f-4842-91bd-495d70f6eebf
https://takeout.google.com/https://takeout.google.com/settings/takeout/downloads?u
ser=100163304658953442343&rapt=AEjHL4M6ZpstK0D59UE_Rd4uT_n4LyIDZAMG-VH_l2J3dL2nZTu
fU8E_ujWhJiLyYVvEAITK-lsowT2ejXm_l_by8dlX-AdJwQ#i=1&j=eceb1af7-2f4f-4842-91bd-495d
70f6eebftakeout.google.com/settings/takeout/downloads?user=100163304658953442343&r
apt=AEjHL4M6ZpstK0D59UE_Rd4uT_n4LyIDZAMG-VH_l2J3dL2nZTufU8E_ujWhJiLyYVvEAITK-lsowT
2ejXm_l_by8dlX-AdJwQ#i=1&j=eceb1af7-2f4f-4842-91bd-495d70f6eebf
https://takeout.google.com/https://takeout.google.com/settings/takeout/downloads?u
ser=100163304658953442343&rapt=AEjHL4M6ZpstK0D59UE_Rd4uT_n4LyIDZAMG-VH_l2J3dL2nZTu
fU8E_ujWhJiLyYVvEAITK-lsowT2ejXm_l_by8dlX-AdJwQtakeout.google.com/settings/takeout
/downloads?user=100163304658953442343&rapt=AEjHL4M6ZpstK0D59UE_Rd4uT_n4LyIDZAMG-VH
_l2J3dL2nZTufU8E_ujWhJiLyYVvEAITK-lsowT2ejXm_l_by8dlX-AdJwQ
https://takeout.google.com/https://takeout.google.com/settings/takeout/downloads?u
ser=100163304658953442343&rapt=AEjHL4M6ZpstK0D59UE_Rd4uT_n4LyIDZAMG-VH_l2J3dL2nZTu
fU8E_ujWhJiLyYVvEAITK-lsowT2ejXm_l_by8dlX-AdJwQtakeout.google.com/settings/takeout
/downloads?user=100163304658953442343&rapt=AEjHL4M6ZpstK0D59UE_Rd4uT_n4LyIDZAMG-VH
_l2J3dL2nZTufU8E_ujWhJiLyYVvEAITK-lsowT2ejXm_l_by8dlX-AdJwQ
https://takeout.google.com/https://takeout.google.com/settings/takeout/downloads?u
ser=100163304658953442343&rapt=AEjHL4M6ZpstK0D59UE_Rd4uT_n4LyIDZAMG-VH_l2J3dL2nZTu

fU8E_ujWhJiLyYVvEAITK-lsowT2ejXm_l_by8dlX-AdJwQ#i=0&j=eceb1af7-2f4f-4842-91bd-495d
70f6eebftakeout.google.com/settings/takeout/downloads?user=100163304658953442343&r
apt=AEjHL4M6ZpstK0D59UE_Rd4uT_n4LyIDZAMG-VH_l2J3dL2nZTufU8E_ujWhJiLyYVvEAITK-lsowT
2ejXm_l_by8dlX-AdJwQ#i=0&j=eceb1af7-2f4f-4842-91bd-495d70f6eebf
https://takeout.google.com/https://takeout.google.com/settings/takeout/downloads?u
ser=100163304658953442343&rapt=AEjHL4M6ZpstK0D59UE_Rd4uT_n4LyIDZAMG-VH_l2J3dL2nZTu
fU8E_ujWhJiLyYVvEAITK-lsowT2ejXm_l_by8dlX-AdJwQtakeout.google.com/settings/takeout
/downloads?user=100163304658953442343&rapt=AEjHL4M6ZpstK0D59UE_Rd4uT_n4LyIDZAMG-VH
_l2J3dL2nZTufU8E_ujWhJiLyYVvEAITK-lsowT2ejXm_l_by8dlX-AdJwQ
https://takeout.google.com/https://takeout.google.com/settings/takeout/downloads?u
ser=100163304658953442343&rapt=AEjHL4M6ZpstK0D59UE_Rd4uT_n4LyIDZAMG-VH_l2J3dL2nZTu
fU8E_ujWhJiLyYVvEAITK-lsowT2ejXm_l_by8dlX-AdJwQtakeout.google.com/settings/takeout
/downloads?user=100163304658953442343&rapt=AEjHL4M6ZpstK0D59UE_Rd4uT_n4LyIDZAMG-VH
_l2J3dL2nZTufU8E_ujWhJiLyYVvEAITK-lsowT2ejXm_l_by8dlX-AdJwQ
https://www.youtube.com/redirect?event=video_description&redir_token=QUFFLUhqbDA4U
HF3OC05Mkpwa19NRXdGY2UyX3FMaEZnQXxBQ3Jtc0tuTHBxR3dlS2hJOFFjQ192aDlYSEljOGdkX0N6dEF
hZUNJTzRzenpURFhDWlJXc0pURVZaZGE2Vl1lemVEVG1tNEJYVU9fTjk1emlMR2VpNHJBb3VBUWRDSUxPN
3JQU19oS2ItWlB6aUtQNkdFZFM2RQ&q=https%3A%2F%2Fwww.feedingamerica.org%2Fpenny&v=JEq
i3VVLYkg1
https://login.microsoftonline.com/https://login.microsoftonline.com/common/oauth2/
v2.0/authorize?client_id=a81d90ac-aa75-4cf8-b14c-58bf348528fe&redirect_uri=https%3
A%2F%2Fanswers.microsoft.com&response_type=code%20id_token&scope=openid%20profile&
state=OpenIdConnect.AuthenticationProperties%3D2Yc9ATRFGJJ72p8YJlsWx2_nWjbJBbIklSo
nPZkVN7dOAoDvhQYDnwttkFlsKxMlrLZEdpEe-Lj8nMSkKmS47ngXiu4CEwaWlwAMtmnlMLlvpJcPSSvqr
Pu5y05-BRGKwDlJ0nrIs1uShIlOlTRb3ooWEI8OwU8-nkzvqdTFvs8lSu0AoXYLTE
https://login.microsoftonline.com/https://login.microsoftonline.com/common/oauth2/
v2.0/authorize?client_id=a81d90ac-aa75-4cf8-b14c-58bf348528fe&redirect_uri=https%3
A%2F%2Fanswers.microsoft.com&response_type=code%20id_token&scope=openid%20profile&
state=OpenIdConnect.AuthenticationProperties%3D2Yc9ATRFGJJ72p8YJlsWx2_nWjbJBbIklSo
nPZkVN7dOAoDvhQYDnwttkFlsKxMlrLZEdpEe-Lj8nMSkKmS47ngXiu4CEwaWlwAMtmnlMLlvpJcPSSvqr
Pu5y05-BRGKwDlJ0nrIs1uShIlOlTRb3ooWEI8OwU8-nkzvqdTFvs8lSu
https://export-download.canva.com/b3ZYU/DAFXWsb3ZYU/64/0/0001-1359792104.png?X-Amz
-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAJHKNGJLC2J7OGJ6Q%2F20230322%2Fus-
east-1%2Fs3%2Faws4_request&X-Amz-Date=20230322T040914Z&X-Amz-Expires=84292&X-Amz-S
ignature=c544757977a463e16c2cc8806628ea7ee1f8739db3fa414720649b496fe218da&X-Amz-Si
gnedHeaders=host&response-content-disposition=attachment%3B%20filename%2A%3DUTF-8%
27%27V-Seva%2520Maiyam%2520Janarthanan%2520L%2520JLP%2520Farms%2520Vedapatty%2520-
%2520Perur%2520Main%2520Road%2520Vedapatty%252C%2520Coimbatore%2520641007%25209884
230004%2520BILL%2520TO%2520INVOICE%2520%23%2520101%2520CHINMAYA%2520INTERNATIONAL%
2520RESIDENTIAL%2520SCHOOL%252C%2520SWAMI%2520CHINMAYANANDA%2520LANE%252C%2520NALL
UR%2520VAYAL%2520POST%252C%2520.png&response-expires=Thu%2C%2023%20Mar%202023%2003
%3A34%3A06%20GMT
https://amazon.in/https://www.amazon.in/ap/signin?openid.pape.max_auth_age=0&openi
d.return_to=https%3A%2F%2Fmusic.amazon.in%2F%3FrefMarker%3Dnull&openid.identity=ht
tp%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0%2Fidentifier_select&openid.assoc_handle=a
mzn_webamp_in&openid.mode=checkid_setup&language=en_IN&openid.claimed_id=http%3A%2
F%2Fspecs.openid.net%2Fauth%2F2.0%2Fidentifier_select&pageId=login&openid.ns=http%
3A%2F%2Fspecs.openid.net%2Fauth%2F2.0amazon.in/ap/signin?openid.pape.max_auth_age=
0&openid.return_to=https%3A%2F%2Fmusic.amazon.in%2F%3FrefMarker%3Dnull&openid.iden
tity=http%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0%2Fidentifier_select&openid.assoc_h
andle=amzn_webamp_in&openid.mode=checkid_setup&language=en_IN&openid.claimed_id=ht
tp%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0%2Fidentifier_select&pageId=login&openid.n
s=http%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0
https://poe.com/https://poe.com/continue_chat?quora_auth_code=WVSVWotcByEgOeao8AJQ
Z_NV0XSkn2e5JiH7HqFwZ-fmJfvWDFPuc2lLAfdYleEMYfGdQYgCosqYg5CE0Ru75w&context_content
_oid=1477743646352178&context_content_type=answer&reply=What%20is%20the%20fare%20f
or%20the%20metro%20rail%3F&scroll_to=bottom&bot_name=Sagepoe.com/continue_chat?quo
ra_auth_code=WVSVWotcByEgOeao8AJQZ_NV0XSkn2e5JiH7HqFwZ-fmJfvWDFPuc2lLAfdYleEMYfGdQ
YgCosqYg5CE0Ru75w&context_content_oid=1477743646352178&context_content_type=answer
&reply=What
https://poe.com/https://poe.com/continue_chat?quora_auth_code=WVSVWotcByEgOeao8AJQ
Z_NV0XSkn2e5JiH7HqFwZ-fmJfvWDFPuc2lLAfdYleEMYfGdQYgCosqYg5CE0Ru75w&context_content
_oid=1477743646352178&context_content_type=answer&reply=What%20is%20the%20fare%20f
or%20the%20metro%20rail%3F&scroll_to=bottom&bot_name=Sagepoe.com/continue_chat?quo
ra_auth_code=WVSVWotcByEgOeao8AJQZ_NV0XSkn2e5JiH7HqFwZ-fmJfvWDFPuc2lLAfdYleEMYfGdQ
YgCosqYg5CE0Ru75w&context_content_oid=1477743646352178&context_content_type=answer
&reply=What
https://amazon.in/https://www.amazon.in/ap/signin?openid.pape.max_auth_age=3600&op
enid.return_to=https%3A%2F%2Fmusic.amazon.in%2F%3FrefMarker%3Dnull&openid.identity
=http%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0%2Fidentifier_select&openid.assoc_handl
e=amzn_webamp_in&openid.mode=checkid_setup&language=en_IN&openid.claimed_id=http%3
A%2F%2Fspecs.openid.net%2Fauth%2F2.0%2Fidentifier_select&pageId=login&openid.ns=ht
tp%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0amazon.in/ap/signin?openid.pape.max_auth_a
ge=3600&openid.return_to=https%3A%2F%2Fmusic.amazon.in%2F%3FrefMarker%3Dnull&openi
d.identity=http%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0%2Fidentifier_select&openid.a
ssoc_handle=amzn_webamp_in&openid.mode=checkid_setup&language=en_IN&openid.claimed
_id=http%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0%2Fidentifier_select&pageId=login&op
enid.ns=http%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0

## Chrome history -- limit 50

```
http://amazon.com/s
http://archiveofourown.org/works/24007973-
http://archiveofourown.org/works/14466273:-
https://www.youtube.com/results?search_query=that+girl+playlist&page=&utm_source=o
pensearchthat
https://www.youtube.com/results?search_query=bad+bitch+play+list&page=&utm_source=
opensearchbad
http://archiveofourown.org/works/4793360A
https://twitter.com/larryffprompts/status/1664244330104496135Larry
https://archiveofourown.org/works/47609569/chapters/119995906#workskinhope
https://archiveofourown.org/works/47609569/chapters/119995846#workskinhope
https://archiveofourown.org/works/47609569/chapters/119995813#workskinhope
https://archiveofourown.org/works/47609569/chapters/119995732#workskinhope
https://archiveofourown.org/works/47609569/chapters/119995687#workskinhope
https://archiveofourown.org/works/47609569/chapters/119995630#workskinhope
https://archiveofourown.org/works/47609569/chapters/119995570#workskinhope
https://archiveofourown.org/works/47609569/chapters/119995489#workskinhope
https://youtube.com/https://www.youtube.com/shorts/UakPhCp9aSAyoutube.com/shorts/U
akPhCp9aSA
https://www.google.com/search?q=crackers+in+barrels&sourceid=chrome&ie=UTF-8https:
//www.google.com/search?q=crackers+in+barrels&sourceid=chrome&ie=UTF-8google.com/s
earch?q=crackers+in+barrels&sourceid=chrome&ie=UTF-8
https://twitter.com/https://twitter.com/alarryshelf/status/1670885134147416067?s=4
6&t=4HQ8ljJcuberkUwmAr2VtQtwitter.com/alarryshelf/status/1670885134147416067?s=46&
t=4HQ8ljJcuberkUwmAr2VtQ
https://takeout.google.com/https://takeout.google.com/settings/takeout/downloads?p
li=1&rapt=AEjHL4M6ZpstK0D59UE_Rd4uT_n4LyIDZAMG-VH_l2J3dL2nZTufU8E_ujWhJiLyYVvEAITK
-lsowT2ejXm_l_by8dlX-AdJwQtakeout.google.com/settings/takeout/downloads?pli=1&rapt
=AEjHL4M6ZpstK0D59UE_Rd4uT_n4LyIDZAMG-VH_l2J3dL2nZTufU8E_ujWhJiLyYVvEAITK-lsowT2ej
Xm_l_by8dlX-AdJwQ
https://translate.google.com/https://translate.google.com/?sl=hi&tl=en&text=%E0%A4
%86%E0%A4%AA%20%E0%A4%95%E0%A5%87%20%E0%A4%A8%E0%A4%9C%E0%A4%BC%E0%A4%B0%E0%A5%8B%
E0%A4%82%20%E0%A4%B8%E0%A4%AE%E0%A4%9D%E0%A4%BE%20%E0%A4%AA%E0%A5%8D%E0%A4%AF%E0%A4
%BE%E0%A4%B0%20%E0%A4%95%E0%A4%BE%E0%A4%AC%E0%A4%BF%E0%A4%B2%20&op=translatetrans
late.google.com/?sl=hi&tl=en&text=??
https://youtube.com/https://www.youtube.com/watch?v=MFpqMh6M5L4youtube.com/watch?v
=MFpqMh6M5L4
https://www.youtube.com/results?search_query=do+the+dance&page=&utm_source=opensea
rchhttps://www.youtube.com/results?search_query=do+the+dance&page=&utm_source=open
searchyoutube.com/results?search_query=do+the+dance&page=&utm_source=opensearch
https://www.google.com/search?q=tannenbaum&sourceid=chrome&ie=UTF-8https://www.goo
gle.com/search?q=tannenbaum&sourceid=chrome&ie=UTF-8google.com/search?q=tannenbaum
&sourceid=chrome&ie=UTF-8
https://google.com/https://www.google.com/maps/search/Hotels/@13.064626,80.2218026
,14.72z/data=
https://amazon.com/https://www.amazon.com/New-House-Same-Underwear-excited/dp/1774
470101/ref=pd_vtp_h_vft_none_pd_vtp_h_vft_none_sccl_10/141-4607784-9508953?pd_rd_w
=ybmSs&content-id=amzn1.sym.a5610dee-0db9-4ad9-a7a9-14285a430f83&pf_rd_p=a5610dee-
0db9-4ad9-a7a9-14285a430f83&pf_rd_r=G95J0A9MVMH9JYPJF5NG&pd_rd_wg=8nXvs&pd_rd_r=44
5a59f6-3f8d-44b1-9fcb-8c1449e57213&pd_rd_i=1774470101&psc=1&asin=1774470101&revisi
onId=&format=4&depth=1amazon.com/New-House-Same-Underwear-excited/dp/1774470101/re
f=pd_vtp_h_vft_none_pd_vtp_h_vft_none_sccl_10/141-4607784-9508953?pd_rd_w=ybmSs&co
ntent-id=amzn1.sym.a5610dee-0db9-4ad9-a7a9-14285a430f83&pf_rd_p=a5610dee-0db9-4ad9
-a7a9-14285a430f83&pf_rd_r=G95J0A9MVMH9JYPJF5NG&pd_rd_wg=8nXvs&pd_rd_r=445a59f6-3f
8d-44b1-9fcb-8c1449e57213&pd_rd_i=1774470101&psc=1&asin=1774470101&revisionId=&for
mat=4&depth=1
https://twitter.com/https://twitter.com/anneketruus/status/1653804263913422848/pho
to/4twitter.com/anneketruus/status/1653804263913422848/photo/4
https://www.google.com/sorry/index?continue=https://www.google.com/search%3Fq%3Dao
3%26oq%3Dao3%26aqs%3Dchrome.0.69i59j0i131i433i512l3j0i512l2j0i131i433i512j5.3763j0
j7%26sourceid%3Dchrome%26ie%3DUTF-8&q=EgRn4CNUGMqBqKQGIjD4gIY9Qkk3KNumMXP89tr8_JMC
HmH2UrkJYkkMNOV9oqHDFiDehkodeVKju78ItIEyAXJaAUM
https://www.youtube.com/YouTube
https://archiveofourown.org/works/12225561#mainA
https://archiveofourown.org/works/8342227/chapters/19110898knock
https://archiveofourown.org/works/5157680/chapters/11877494California
https://archiveofourown.org/works/3525578/chapters/7754546Every
https://archiveofourown.org/works/4089382#mainShould
https://archiveofourown.org/works/4093060/chapters/9219502?view_adult=truethese
https://archiveofourown.org/works/1023265Zayn
https://archiveofourown.org/works/8036800?view_adult=trueShades
```

```
https://archiveofourown.org/works/659065keeping
https://accounts.google.co.in/accounts/SetSID?ssdc=1&sidt=ALWU2csIfc4Pk/tlanS/OMj2
x4/T5QcJuykYKrHvAZNV5wOUdtJa5o83aMTIWuw65cv5s2viIMrWOw6tuwWkNYQPR9VZOYXSwBTJOzv8jw
MzwkB0fnWlVtgU9JK9eSJbOrGhGXvbdyds195OHRH0/nmA1NhLPcXOldxTCYstRpq854%2BXnvGFtDossM
EtaflbSocu9Cg5mBrn56sTKzjRDtsbG55ARIAlgUEpw2DjmefqRGZZ/XLc1yhGyJ0gmITU5SHED/YDvWuZ
RD/9tZbb0Wn5cXs4QNhO65HEJK46jOUNR61ZPLmpg1PWpu1fzlctYrRZYc6Ov2994BGwhu5%2B2W5KGkmA
6xw1wsHkf0huH2e4gnSW0A0r7lYjc3sPAPgM1KYptsU0x2ScGNdZwIlBKdMLo36thZfRpMD7pVfINgmULo
nvwWjpxmyULOQU8j0uZzPNTqzkZI45hqLAw82GmJle/K%2B/5axz8%2BQQqO2WfeQfVBa9HnfEWmJ9Z5N5
4xG6IvcBCxroC9AfdYE567Q/EeEKDD86jCfK9Y23zhbrtTFiehQlkJWGviE%3D&continue=https://ta
keout.google.com/settings/takeout/download?j%3Deceb1af7-2f4f-4842-91bd-495d70f6eeb
f%26i%3D0%26pli%3D1%26rapt%3DAEjHL4M6ZpstK0D59UE_Rd4uT_n4LyIDZAMG-VH_l2J3dL2nZTufU
8E_ujWhJiLyYVvEAITK-lsowT2ejXm_l_by8dlX-AdJwQ&tcc=1&ifkv=Af_xneGkYTRFvXNRzq0bIhTe5
NsDQ3eYLoZuRssvrb0rXyMjjP6Mke_pmGFpBbRWSMzUoqCdZlmJZg=3
http://archiveofourown.org/works/98486788l-
http://archiveofourown.org/works/32852560
https://accounts.google.co.in/accounts/SetSID?ssdc=1&sidt=ALWU2ctwJ8/szU8G9yZGHLpD
WJ%2BkcWZPqdo6QLJSHjSs0w38ogAjjP5ZNwHLxrvHepOeYP6b621jSNTN/aD%2BRb4mkZqcaQe2DMHC9K
RBzSH8DDIRGI18y1lLAMN0K0dZEuh8HxoanGoQp2B5r0lSpRXTemv5oOBmky0md4s32eQNcmbxThHnakXf
RcJ71Wi8XsuhceISaMoVKQEFrSvHUV%2B0azmUH1xJXlBQodiIHR2WKJFqqo6eMcYLmDDORysIjh3G4jqc
RYSKnzXN96WCXwDFkSda2b08%2BoiC0FNV02zcYrwxJvBEEuqiu85x/vanvKe37C8s7NDepz6QwQsJaDCw
n3qPV%2BA2zk2794wXt%2BGi5qYzXXlGhEMux%2BlamQb/jVA900oc7ZeG2NnwBAUh9dcTzgE%2BrhjF5U
Slx8JN5dfa%2B/qqkpUq2UYEGByxtAuxOQSvKUcFNe8aIw2bxUBsf0Yypno2ukgpIKGl/SRwdaXcWtVIcr
xKzuDplLTIZ4/Ud1v9U40zsLK1gj2Js5SyDL3cH4%2Bl7ay5kJXFfsVrWvP6LTLbn1et6tQ%3D&continu
e=https://takeout.google.com/takeout/download?j%3Deceb1af7-2f4f-4842-91bd-495d70f6
eebf%26i%3D4%26user%3D100163304658953442343%26rapt%3DAEjHL4Pb-JTIX5RcJRpoJ1r4dyxvR
Uge5X0CnYJUvwPtPcUIgf_1YDM_kwn1KGXv-QhMhtifpQRHx3HXEcIrdomh86qdCvrvow&tcc=1&ifkv=A
f_xneFSx3xniuz5oa_MQuASUOm6N8O1SSAQ3DKORk7FA6qGPEV9ukHj3KRUZhRkIleeFqM38mk1ow
https://accounts.google.com/CheckCookie?continue=https%3A%2F%2Ftakeout.google.com%
2Ftakeout%2Fdownload%3Fj%3Deceb1af7-2f4f-4842-91bd-495d70f6eebf%26i%3D4%26user%3D1
00163304658953442343%26rapt%3DAEjHL4Pb-JTIX5RcJRpoJ1r4dyxvRUge5X0CnYJUvwPtPcUIgf_1
YDM_kwn1KGXv-QhMhtifpQRHx3HXEcIrdomh86qdCvrvow&hl=en&checkedDomains=youtube&checkC
onnection=youtube%3A299%3A0&pstMsg=1&osid=1&rart=ANgoxceQxMbk59PHpS3iwE_VIWXvOz5cN
7MBxI0aYeCU_dawKrZb49-XjA1NhB2KD1Er5oIYviurOMLtpX20EUb_VplqrjaAEQ&flowName=GlifWeb
SignIn&ifkv=Af_xneHjXMJ8PKWRpiGOZf2jEFkQ-JVgFJTaAKNAomRdUUa-KQvMnhXM9FOSg-HjBYCBjO
oH34htag&chtml=LoginDoneHtml&gidl=EgIIAA
https://accounts.google.com/AccountChooser?continue=https://takeout.google.com/set
tings/takeout/download?j%3Deceb1af7-2f4f-4842-91bd-495d70f6eebf%26i%3D7&Email=sneh
ajanarthanan123456@gmail.com=
https://accounts.google.com/AccountChooser?continue=https://takeout.google.com/set
tings/takeout/download?j%3Deceb1af7-2f4f-4842-91bd-495d70f6eebf%26i%3D0&Email=sneh
ajanarthanan123456@gmail.com=
https://in.search.yahoo.com/search?fr=mcafee&type=E211IN826G0&p=how+to+make+mac+an
d+cheese+powder+at+homehow
https://www.youtube.com/results?search_query=diy+instat+mac+and+cheese+powder&page
=&utm_source=opensearchdiy
https://in.search.yahoo.com/search?fr=mcafee&type=E211IN826G0&p=how+to+make+mac+an
d+cheese+powder+at+homehow
https://mail.google.com/mail/u/0
https://shelbys-advice-blog.tumblr.com/post/111965409857/calming-masterpostShelby
https://www.google.com/search?q=isidore+name+meaning&sourceid=chrome&ie=UTF-8isido
re
```

## Chrome bookmarks

```
https://accounts.google.com/b/0/AddMailService
https://youtube.com/
https://maps.google.com/
https://translate.google.com/
https://www.google.co.in/
https://music.amazon.in/
https://games.usatoday.com/games/easy-crossword
```

## IE history -- limit 50

```
http://go.microsoft.com/fwlink/p/?LinkId=255142
http://www.dellauction.com/
http://www1.ap.dell.com/content/default.aspx?c=in&l=en&s=gen
http://www.dell.com/support/home
```

# Interesting files and registry

## Putty Sessions

```
=== Putty Saved Session Information (All Users) ===
Not Found
```

## Putty SSH Host keys

```
=== Putty SSH Host Hosts (All Users) ===
Not Found
```

## Enumerating Office 365 endpoints synced by OneDrive.

```
SID: S-1-5-19
================================================================================
==============
SID: S-1-5-20
================================================================================
==============
SID: S-1-5-21-3918106844-1363930152-1516286804-1001
Name: Business1
UserEmail snehjanarthanan@outlook.com
UserFolder C:\Users\snehj\OneDrive
Name: Personal
UserEmail snehjanarthanan@outlook.com
UserFolder C:\Users\snehj\OneDrive
LibraryType personal
LastModifiedTime 2023-07-20T09:41:21 (Thu 20 Jul 2023 09:41:21)
MountPoint C:\Users\snehj\OneDrive
UrlNamespace https://d.docs.live.net
================================================================================
==============
SID: S-1-5-18
Name: Business1
UserEmail snehjanarthanan@outlook.com
UserFolder C:\Users\snehj\OneDrive
================================================================================
==============
```

## 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
```

## Enumerating machine and user certificate files

```
Issuer : CN=localhost
Subject : CN=localhost
ValidDate : 17-04-2022 10:51:59
ExpiryDate : 17-04-2027 05:30:00
HasPrivateKey : True
StoreLocation : LocalMachine
KeyExportable : True
Thumbprint : 683796237A6AFECCC694D0170E43BEB4D57FFFBF
Enhanced Key Usages
Server Authentication
================================================================================
===============
```

## Office Most Recent Files -- limit 50

```
Last Access Date User Application Document
2023-07-23 03:26 DESKTOP-SNEHA\snehj Word C:\Users\snehj\Downloads\Resume file
(India).docx
2023-06-28 10:02 DESKTOP-SNEHA\snehj Word C:\Users\snehj\Downloads\Resume file.docx
2023-06-25 04:37 DESKTOP-SNEHA\snehj Word C:\Users\snehj\Downloads\Global_Candidat
e_Privacy_Notice_English_Final_August_18.docx
2023-06-24 05:12 DESKTOP-SNEHA\snehj Word C:\Users\snehj\Downloads\CV.docx
2023-06-20 14:43 DESKTOP-SNEHA\snehj Word C:\Users\snehj\Downloads\Epic.docx
2023-06-18 14:04 DESKTOP-SNEHA\snehj Excel C:\Users\snehj\Downloads\Lab slot.xlsx
2023-06-12 05:29 DESKTOP-SNEHA\snehj Word C:\Users\snehj\OneDrive\Documents\CV.docx
2023-06-11 05:57 DESKTOP-SNEHA\snehj Word D:\MOD - wheats croft road.docx
2023-05-16 13:13 DESKTOP-SNEHA\snehj Word
C:\Users\snehj\Downloads\6436ceb922ca4_CyberX_problem_statements_rev2 (1).docx
2023-05-16 12:03 DESKTOP-SNEHA\snehj Excel
C:\Users\snehj\Downloads\rekognition-violentimages_accessKeys.csv
2023-05-12 17:12 DESKTOP-SNEHA\snehj Word
C:\Users\snehj\Downloads\6436ceb922ca4_CyberX_problem_statements_rev2 (2).docx
2023-05-12 14:52 DESKTOP-SNEHA\snehj Word C:\Users\snehj\Downloads\DGO QB ans.docx
2023-05-12 11:47 DESKTOP-SNEHA\snehj Word C:\Users\snehj\Downloads\AWS 16M-QB.docx
2023-05-12 11:47 DESKTOP-SNEHA\snehj Word C:\Users\snehj\Downloads\CIA II QB.docx
2023-05-10 14:52 DESKTOP-SNEHA\snehj Word
C:\Users\snehj\Downloads\SeleniumQB-16Marks (1).docx
2023-05-09 15:11 DESKTOP-SNEHA\snehj Word C:\Users\snehj\Downloads\selenium
(1).docx
2023-05-09 15:09 DESKTOP-SNEHA\snehj Word C:\Users\snehj\Downloads\selenium.docx
2023-05-08 14:02 DESKTOP-SNEHA\snehj Word C:\Users\snehj\Downloads\16MARKS -
20qns.docx
2023-05-07 07:17 DESKTOP-SNEHA\snehj Word C:\Users\snehj\Downloads\MODULE
2&3-QUESTION BANK.docx
2023-05-07 03:22 DESKTOP-SNEHA\snehj Word C:\Users\snehj\Downloads\CIA2 DGO QB.docx
2023-05-07 03:22 DESKTOP-SNEHA\snehj Word C:\Users\snehj\Downloads\CIA2 DGO QB
(1).docx
2023-05-02 05:37 DESKTOP-SNEHA\snehj Excel C:\Users\snehj\Downloads\DAY 1.xlsx
2023-05-02 05:35 DESKTOP-SNEHA\snehj Word C:\Users\snehj\Downloads\DAY 3.docx
2023-05-02 05:35 DESKTOP-SNEHA\snehj Word C:\Users\snehj\Downloads\DAY 5.docx
2023-05-02 05:35 DESKTOP-SNEHA\snehj Word C:\Users\snehj\Downloads\DAY 1.docx
2023-05-02 05:35 DESKTOP-SNEHA\snehj Word C:\Users\snehj\Downloads\DAY 7.docx
2023-05-02 03:53 DESKTOP-SNEHA\snehj Word C:\Users\snehj\Downloads\DAY 4.docx
2023-05-01 13:35 DESKTOP-SNEHA\snehj Excel D:\RAJESH DMD.xls
2023-04-27 08:26 DESKTOP-SNEHA\snehj PowerPoint
C:\Users\snehj\Downloads\643511aa7f65e_CyberX_PPT_Template_.pptx
2023-04-19 04:42 DESKTOP-SNEHA\snehj Word
C:\Users\snehj\Downloads\6436ceb922ca4_CyberX_problem_statements_rev2.docx
2023-04-18 05:03 DESKTOP-SNEHA\snehj Excel C:\Users\snehj\Downloads\hacks.xlsx
2023-04-17 06:36 DESKTOP-SNEHA\snehj PowerPoint
C:\Users\snehj\Downloads\BlockDocs-Blockheads-Binance ideathon (1).pptx
2023-04-10 09:59 DESKTOP-SNEHA\snehj Excel C:\Users\snehj\Downloads\s1.xlsx
2023-03-27 05:51 DESKTOP-SNEHA\snehj PowerPoint C:\Users\snehj\Hack Wizards -
PS-KVH-012(1).pptx
2023-03-14 05:43 DESKTOP-SNEHA\snehj Word C:\Users\snehj\Downloads\G20 OD LIST.docx
2023-03-14 05:43 DESKTOP-SNEHA\snehj Word C:\Users\snehj\Downloads\G20 OD LIST
(1).docx
2023-03-11 12:08 DESKTOP-SNEHA\snehj Word C:\Users\snehj\Downloads\G20 PROMO VIDEO
BUDGET.docx
2023-03-11 09:37 DESKTOP-SNEHA\snehj Word
C:\Users\snehj\Downloads\1678527284222_Induction program budget.docx
2023-02-25 18:44 DESKTOP-SNEHA\snehj Word C:\Users\snehj\Downloads\SKILLATHON
GUIDE.docx
2023-02-25 18:44 DESKTOP-SNEHA\snehj Word C:\Users\snehj\Downloads\Unisys
```

```
Innovation Program.docx
2023-02-15 16:37 DESKTOP-SNEHA\snehj Excel C:\Users\snehj\Downloads\Sem 4 Group
split up data.xlsx
2023-02-03 08:51 DESKTOP-SNEHA\snehj Excel C:\Users\snehj\Downloads\She Codes _
shortlisted for L2 rd.xlsx
2023-01-11 10:54 DESKTOP-SNEHA\snehj Word C:\Users\snehj\Downloads\101-CHINMAYA-IN
TERNATIONAL-RESIDENTIAL-SCHOOL-SWAMI-CHINMAYANANDA-LANE-NALLUR-VAYAL-POST-SIRUVANI
-ROAD-COIMBATORE-641-114 (1).docx
2022-12-26 02:34 DESKTOP-SNEHA\snehj Excel C:\Users\snehj\Downloads\CSE, IT & AIDS
- C++ Students List.xlsx
2022-12-12 17:31 DESKTOP-SNEHA\snehj Word C:\Users\snehj\OneDrive\Desktop\LAB SEM
3\DIA LAB.docx
2022-12-12 16:52 DESKTOP-SNEHA\snehj Word C:\Users\snehj\OneDrive\Desktop\LAB SEM
3\Tries.docx
2022-11-24 14:08 DESKTOP-SNEHA\snehj Excel C:\Users\snehj\Downloads\26.xlsx
2022-11-19 12:51 DESKTOP-SNEHA\snehj Word C:\Users\snehj\Downloads\Company Specific
Problem solving set 2.docx
2022-11-19 10:36 DESKTOP-SNEHA\snehj Excel C:\Users\snehj\Downloads\HackerEarth
Test Results - 17-11-2022.xls
2022-11-10 09:32 DESKTOP-SNEHA\snehj PowerPoint C:\Users\snehj\Downloads\Emids -
IIIT Hackathon Rules and Guidelines.pptx
```

## Recent files --limit 70--

```
snehj :
C:\Users\snehj\.aws(23-07-2023 10:22:57)
C:\Users\snehj\Downloads\.jpg(23-07-2023 10:22:57)
C:\Users\snehj\Downloads\10be6b21-6259-43b3-903d-0d8e5d1c4f37.jpg(23-07-2023
10:22:57)
C:\Users\snehj\Downloads\6259154d46edc_InnoHacks_idea_ppt_format.pptx(23-07-2023
10:22:57)
C:\Users\snehj\Downloads\6436ceb922ca4_CyberX_problem_statements_rev2
(1).docx(23-07-2023 10:22:57)
C:\Users\snehj\OneDrive\Desktop\727721eucs146(23-07-2023 10:22:57)
C:\Users\snehj\OneDrive\Desktop\727721eucs146(23-07-2023 10:22:57)
C:\Users\snehj\Downloads\83023081-d51e-4394-9bc6-03e68b19bd28.jpg(23-07-2023
10:22:57)
C:\Users\snehj\Downloads\95de4703-4e39-4f48-a72f-dfab0fb4d534.jpg(23-07-2023
10:22:57)
C:\Users\snehj\Downloads\aadhar card.pdf(23-07-2023 10:22:57)
C:\Users\snehj\Downloads\Adobe Scan 11 Jul 2023.pdf(23-07-2023 10:22:57)
C:\Users\snehj\vit\amplify-pkg-win-x64.tgz(23-07-2023 10:22:57)
C:\Users\snehj\hotelbooking\src\App.test.js(23-07-2023 10:22:57)
C:\Users\snehj\Downloads\Appointment.pdf(23-07-2023 10:22:57)
C:\Users\snehj\Downloads\archive.zip(23-07-2023 10:22:57)
E:\August(23-07-2023 10:22:57)
C:\Users\snehj\OneDrive\Desktop\Burgeon(23-07-2023 10:22:57)
C:\Users\snehj\OneDrive\Desktop\Burgeon(23-07-2023 10:22:57)
C:\Users\snehj\Downloads\Businesses.pdf(23-07-2023 10:22:57)
C:\Users\snehj\Downloads\call_log (1).csv(23-07-2023 10:22:57)
C:\Users\snehj\Downloads\call_log.csv(23-07-2023 10:22:57)
C:\Users\snehj\vit\imagebasedmodels\camerarollimages(23-07-2023 10:22:57)
D:\class assembly(23-07-2023 10:22:57)
C:\Users\snehj\Downloads\CLASSDIAGRAM.jpg(23-07-2023 10:22:57)
C:\Users\snehj\cmp(23-07-2023 10:22:57)
C:\Users\snehj\.aws\config(23-07-2023 10:22:57)
C:\Users\snehj\OneDrive\Desktop\Python Assignments\Count numbers(23-07-2023
10:22:57)
C:\Users\snehj\crm(23-07-2023 10:22:57)
C:\Users\snehj\Downloads\CRMapp.pdf(23-07-2023 10:22:57)
C:\Users\snehj\Downloads\CV.docx(23-07-2023 10:22:57)
C:\Users\snehj\Downloads\CV.docx.pdf(23-07-2023 10:22:57)
C:\Users\snehj\Downloads\CyberCore - KVH 018.pdf(23-07-2023 10:22:57)
C:\Users\snehj\Downloads\DAY1(23-07-2023 10:22:57)
C:\Users\snehj\Downloads\DAY1(23-07-2023 10:22:57)
C:\Users\snehj\Downloads\dependency-check-8.3.1-release.zip(23-07-2023 10:22:57)
C:\Users\snehj\OneDrive\Desktop(23-07-2023 10:22:57)
C:\Users\snehj\OneDrive\Desktop(23-07-2023 10:22:57)
C:\Users\snehj\OneDrive\Desktop(23-07-2023 10:22:57)
C:\Users\snehj\Downloads\DN Technoverse 2023 I Contest guidelines.pdf(23-07-2023
10:22:57)
C:\Users\snehj\OneDrive\Documents(23-07-2023 10:22:57)
C:\Users\snehj\Downloads\download (1).jpg(23-07-2023 10:22:57)
C:\Users\snehj\Downloads\download-removebg-preview.png(23-07-2023 10:22:57)
```

```
C:\Users\snehj\Downloads\download.jpg(23-07-2023 10:22:57)
C:\Users\snehj\Downloads(23-07-2023 10:29:40)
C:\Users\snehj\Downloads(23-07-2023 10:22:57)
C:\Users\snehj\Downloads\EP LAB.xls(23-07-2023 10:22:57)
C:\Users\snehj\Downloads\Epic.docx(23-07-2023 10:22:57)
C:\Users\snehj\Downloads\DAY1\ER.jpeg(23-07-2023 10:22:57)
C:\Program Files\Sublime Text 3\EXP 9.html(23-07-2023 10:22:57)
C:\Users\snehj\vit\facerecognition(23-07-2023 10:22:57)
C:\Users\snehj\OneDrive\Desktop\HTML\Flippy(23-07-2023 10:22:57)
C:\Users\snehj\OneDrive\Documents\FlutterDev\flutter(23-07-2023 10:22:57)
C:\Users\snehj\OneDrive\Documents\FlutterDev(23-07-2023 10:22:57)
C:\Users\snehj\Downloads\Global_Candidate_Privacy_Notice_English_Final_August_18.d
ocx(23-07-2023 10:22:57)
C:\Users\snehj\Downloads\google-services.json(23-07-2023 10:22:57)
C:\Users\snehj\Hackathons(23-07-2023 10:22:57)
C:\Users\snehj\vit\imagebasedmodels\camerarollimages\harrystyles2.jpg(23-07-2023
10:22:57)
C:\Users\snehj\vit\imagebasedmodels\camerarollimages\harrystyles3.jpg(23-07-2023
10:22:57)
C:\Users\snehj\vit\imagebasedmodels\camerarollimages\harrystyles5.jpg(23-07-2023
10:22:57)
C:\Users\snehj\vit\hatespeech.py(23-07-2023 10:22:57)
C:\Users\snehj\Downloads\image (1).txt(23-07-2023 10:22:57)
C:\Users\snehj\Downloads\image (2).txt(23-07-2023 10:22:57)
C:\Users\snehj\Downloads\image (3).txt(23-07-2023 10:22:57)
C:\Users\snehj\Downloads\image.txt(23-07-2023 10:22:57)
C:\Users\snehj\vit\imagebasedmodels(23-07-2023 10:22:57)
C:\Users\snehj\vit\imageconvert.py(23-07-2023 10:22:57)
C:\Users\snehj\vit\imgStore.py(23-07-2023 10:22:57)
D:\2023\Takeout\Google Photos\Photos from 2022\IMG_5334.MOV(23-07-2023 10:22:57)
C:\Users\snehj\OneDrive\Desktop\JAVA(23-07-2023 10:22:57)
C:\Users\snehj\OneDrive\Desktop\JAVA(23-07-2023 10:22:57)
```

159