

# Cyber Security Audit Report

**Name:** bat

**Lab:** cat

**Audit Timestamp:** 2025-08-20 22:42:24

## Table of Contents

1. Cyber Security Health Score
2. System Information
3. Network Details
4. Security Information
5. Critical Port Exposure
6. Users Accounts
7. Last Windows Update
8. RDP & Remote Services
9. Critical Windows Services
10. Desktop Files
11. USB Device Connection History
12. Smartphone / Dongle Connection History
13. Installed Programs
14. Startup Applications
15. Shared Folders
16. Unwanted Softwares
17. Logs

This report contains confidential information intended solely for the recipient. Unauthorized use or distribution is prohibited.

## CYBER SECURITY HEALTH SCORE

**Overall Security Health: 38% (■ At Risk)**

**Compulsory Parameters Passed: 4 / 9**

**Desirable Parameters Passed: 2 / 7**

**Compulsory Parameters:**

Parameter	Status
Antivirus Installed	YES
Firewall Enabled	YES
USB Storage Media Blocked	NO
AutoPlay Disabled	NO
Remote Desktop Disabled (RDP)	YES
Telnet Service Disabled	YES
Default Share Disabled	NO
No Shared Folders Configured	NO
Wi-Fi Disabled	NO

**Desirable Parameters:**

Parameter	Status
Geo-Location Disabled	NO
Plug and Play Disabled	NO
Clear Desktop Maintained	NO
System Lockout Policy Configured	NO
Password Policy Configured	NO
Open TCP Ports < 10	YES
Open UDP Ports < 10	YES

# CYBER SECURITY AUDIT REPORT

## System Information

S.No	Parameter	Value
1	System Serial Number	Not Available
2	PC Name	JoeyTheDog
3	OS Name	Microsoft Windows 11 Pro
4	Windows Version	10.0.26100
5	BIOS Version	1.K0
6	Machine Type	64-bit
7	Processor	12th Gen Intel(R) Core(TM) i7-12700F
8	Product ID	00331-10000-00001-AA250
9	Service Pack Status	No Service Pack Installed
10	OS Configuration	Standalone Workstation
11	Plug and Play Status	Plug and Play Enabled (Manual Start)
12	Windows Directory	C:\WINDOWS
13	System Directory	C:\WINDOWS\system32
14	Clear Desktop Status	Desktop is Cluttered (110 files/folders)
15	OS Install Date	2025-01-29
16	Domain	WORKGROUP
17	System Last Updated On	13 August 2025
18	Windows License Status	Notification
19	BitLocker Status	Error: (Requires Admin Privileges)
20	Internet Connectivity	Connected
21	Geo-Location Status	Geo-Location Services Enabled
22	Bluetooth Status	No Bluetooth Adapter Found
23	Local IP Address	192.168.0.153
24	Public IP Address	49.204.20.82
25	CPU Usage	8.3%
26	Memory Usage	42.5%

## **Network Details**

S.No	Parameter	Value
1	MAC Address	D8-BB-C1-A3-90-FE
2	Connection Type	Ethernet
3	Active Network Interface	Realtek Gaming 2.5GbE Family Controller #2
4	Wi-Fi Interface	No Wi-Fi Adapter Found
5	Wi-Fi Status	Wi-Fi Status Unknown
6	Wi-Fi SSID	No Wi-Fi Connection
7	IP Address	192.168.0.153
8	Network Type	Project Network or Unknown

## **Security Information**

S.No	Parameter	Value
1	Timestamp	2025-08-20 22:42:24
2	Antivirus Installed	Windows Defender
3	Windows Firewall Status	Domain Profile: Enabled Private Profile: Enabled Public Profile: Enabled
4	Last Windows Defender Scan Time	13 August 2025 14:21:49
5	USB Storage Device Access	USB Access: Allowed
6	AutoPlay Status	AutoPlay is Enabled
7	Remote Desktop Protocol (RDP)	Disabled (RDP is OFF)
8	Telnet	Not Installed
9	Default Share Status	Enabled (Security Risk)
10	Shared Folder Status	Configured (Security Risk) - Users
11	BIOS Password	Manual Check Required
12	Saved Browser Passwords	Manual Check Required
13	Windows Login Password	Windows Login Password Set (User: amaan)
14	Password Policy	Weak Password Policy (Minimum length is 0)
15	System Lockout Policy	No Lockout Policy (Accounts never lock)

## Open Ports Overview (Critical / TCP / UDP)

S.No	Port	Protocol	Service	Status	PIDs
1	445	TCP	SMB	OPEN	N/A
2	139	TCP	NetBIOS Session	OPEN	N/A
3	138	TCP	NetBIOS Datagram	OPEN	N/A
4	137	TCP	NetBIOS Name	OPEN	N/A
5	135	TCP	RPC	OPEN	N/A
6	49665	TCP	Unknown	OPEN	N/A
7	49666	TCP	Unknown	OPEN	N/A
8	49668	TCP	Unknown	OPEN	N/A
9	49667	TCP	Unknown	OPEN	N/A
10	139	TCP	NetBIOS	OPEN	N/A
11	445	TCP	SMB	OPEN	N/A
12	49669	TCP	Unknown	OPEN	N/A
13	52534	UDP	Unknown	OPEN	6996
14	52533	UDP	Unknown	OPEN	6996
15	5355	UDP	Unknown	OPEN	2676
16	5353	UDP	mDNS	OPEN	28328, 4264, 9956
17	2177	UDP	Unknown	OPEN	9388
18	1900	UDP	UPnP	OPEN	9956, 6996
19	138	UDP	NetBIOS Datagram	OPEN	4
20	137	UDP	NetBIOS Name	OPEN	4

**Total Open TCP Ports: 12**

**Total Open UDP Ports: 8**

**Total Critical Ports Found: 7**

## Users Accounts

Administrator, amaan, DefaultAccount, Guest, WDAGUtilityAccount

## Last Windows Update

- KB5056579 7/10/2025
- KB5063878 8/13/2025
- KB5063666 7/9/2025
- KB5065381 8/13/2025

## **RDP & Remote Services Status**

**Total Services Checked: 10**

S.No	Service Name	Status
1	Bluetooth Support Service	Stopped
2	Geolocation Service	Running
3	Plug and Play	Running
4	HV Host Service	Stopped
5	Remote Desktop Services	Stopped
6	Remote Procedure Call (RPC)	Running
7	Routing and Remote Access	Stopped
8	Wi-Fi Direct Services	Stopped
9	Xbox Game Monitoring	Unknown
10	Default Share Status	Running

## **Critical Windows Services Status**

**Total Services Checked: 18**

S.No	Service Name	Status
1	DNS Client	Running
2	DNS Server	Unknown
3	Geolocation Service	Running
4	Distributed Transaction Coordinator	Stopped
5	Plug and Play	Running
6	Remote Access Auto Connection Manager	Stopped
7	Remote Access Connection Manager	Running
8	Routing and Remote Access	Stopped

9	Remote Registry	Stopped
10	RPC Endpoint Mapper	Running
11	Remote Procedure Call (RPC) Locator	Stopped
12	Remote Procedure Call (RPC)	Running
13	Remote Desktop Configuration	Stopped
14	Microsoft Storage Spaces SMP	Stopped
15	OpenSSH Authentication Agent	Unknown
16	Remote Desktop Services	Stopped
17	Problem Reports Control Panel Support	Stopped
18	Telnet Client	Unknown

## **Desktop Files**

**Number of Desktop Files: 110**

S.No	File Name
1	1337230.jpeg
2	15-05-2025-LATEST-main
3	17-04-2025-main
4	2025-07-09 14-32-55.00_02_15_01.Still001.jpg
5	2025-07-21_00-52-59.00_00_27_20.Still001.jpg
6	22-04-2025-main
7	3.jpeg
8	360_F_319202173_IChFjDK92X4FwE7pbzFjFueIRrRjkJiL.jpg
9	360_F_567048053_ItaBMIfuV6sE583KnWeJuruJyPJbmg1D.jpg
10	360_F_836756205_cRNRqUu5VGCSyYbdncDKvrQGKkWahrAh.jpg

## **USB Device Connection History**

*No USB storage devices found.*

## **Smartphone and Dongle Connection History**

S.No	Device	Vendor	Type	Serial Number
1	Apple Device	Apple	Smartphone	VID_05AC&PID_12A8&MI_00
2	Apple Device	Apple	Smartphone	VID_05AC&PID_12A8&MI_02

## **Installed Programs**

**Total Installed Programs: 210**

S.No	Program Name	Version
1	AIDA64 Extreme v7.50	7.50
2	Adobe After Effects 2022	22.2.1
3	Adobe Media Encoder 2022	22.3.1
4	Adobe Photoshop 2024	25.3.1.241
5	Adobe Premiere Pro 2022	22.1.2
6	Adobe Redeem Launcher	1.0.0.11
7	Advanced Installer 22.7	22.7
8	Android Studio	2021.3
9	Balatro	Unknown Version
10	Battle.net	Unknown Version
11	Bonjour	3.1.0.1
12	CPUID CPU-Z MSI 2.11	2.11
13	Cyberpunk 2077 Bonus Content	Unknown Version
14	DARK SOULS™: REMASTERED	Unknown Version
15	DELTARUNE	Unknown Version
16	Discord	1.0.9004
17	Dropbox Redeem Launcher	1.0.0.04
18	Dynamic Application Loader Host Interface Service	1.0.0.0
19	ELDEN RING NIGHTREIGN	Unknown Version
20	ENE IO Driver	3.3.0
21	ENE Video Capture Box HAL	1.0.5.15
22	ENE Video Capture Box HAL	1.0.5.15
23	ENE_EHD_M2_HAL	1.0.14.0
24	ENE_EHD_M2_HAL	1.0.14.0
25	ENE_External_Device_HAL	1.0.14.0
26	ENE_External_Device_HAL	1.0.14.0
27	ENE_MousePad_HAL	1.0.2.0



28	ENE_MousePad_HAL	1.0.2.0
29	ENE_X_AIC_HAL	1.0.6.3
30	ENE_X_AIC_HAL	1.0.6.3
31	Epic Games Launcher	1.3.93.0
32	Epic Games Launcher Prerequisites (x64)	1.0.0.0
33	Epic Online Services	2.0.44.0
34	Genshin Impact	2.33.7.0
35	Geometry Dash	Unknown Version
36	Git	2.37.3
37	Google Chrome	139.0.7258.128
38	Hamachi	2.3.0.111
39	Hamachi	2.3.0.111
40	HoYoPlay	1.5.2.229
41	Intel Driver && Support Assistant	25.3.24.7
42	Intel(R) C++ Redistributables on Intel(R) 64	15.0.179
43	Intel(R) Chipset Device Software	10.1.19627.8423
44	Intel(R) Chipset Device Software	10.1.19627.8423
45	Intel(R) Computing Improvement Program	2.4.09084
46	Intel(R) ME WMI Provider	1.0.0.0
47	Intel(R) Management Engine Components	2225.16.0.2820
48	Intel(R) Management Engine Components	1.0.0.0
49	Intel(R) Management Engine Driver	1.0.0.0
50	Intel(R) Serial IO	30.100.2131.26
51	Intel(R) Serial IO	30.100.2131.26
52	Intel® Driver & Support Assistant	25.3.24.7
53	Intel® Hardware Accelerated Execution Manager	7.6.5
54	Kinect for Windows Speech Recognition Language Pack (de-DE)	11.0.7413.611
55	Kinect for Windows Speech Recognition Language Pack (en-AU)	11.0.7400.336
56	Kinect for Windows Speech Recognition Language Pack (en-CA)	11.0.7400.336
57	Kinect for Windows Speech Recognition Language Pack (en-GB)	11.0.7400.336
58	Kinect for Windows Speech Recognition Language Pack (en-IE)	11.0.7400.336
59	Kinect for Windows Speech Recognition Language Pack (en-NZ)	11.0.7400.336
60	Kinect for Windows Speech Recognition Language Pack (en-US)	11.0.7400.336
61	Kinect for Windows Speech Recognition Language Pack (es-ES)	11.0.7400.336
62	Kinect for Windows Speech Recognition Language Pack (es-MX)	11.0.7400.336
63	Kinect for Windows Speech Recognition Language Pack (fr-CA)	11.0.7400.336
64	Kinect for Windows Speech Recognition Language Pack (fr-FR)	11.0.7400.336

65	Kinect for Windows Speech Recognition Language Pack (it-IT)	11.0.7400.336
66	Kinect for Windows Speech Recognition Language Pack (ja-JP)	11.0.7400.336
67	Launcher Prerequisites (x64)	1.0.0.0
68	Lies of P	Unknown Version
69	MSI Center SDK	3.2025.0116.01
70	Mage Arena	Unknown Version
71	Maono Link 3.3.5	3.3.5
72	Microsoft .NET Core Host - 3.1.28 (x64)	24.112.31513
73	Microsoft .NET Core Host FX Resolver - 3.1.28 (x64)	24.112.31513
74	Microsoft .NET Core Runtime - 3.1.28 (x64)	24.112.31513
75	Microsoft .NET Core Runtime - 3.1.28 (x64)	3.1.28.31513
76	Microsoft .NET Host - 5.0.15 (x64)	40.60.31015
77	Microsoft .NET Host - 6.0.11 (x64)	48.47.50420
78	Microsoft .NET Host - 8.0.14 (x64)	64.56.29490
79	Microsoft .NET Host - 8.0.14 (x86)	64.56.29490
80	Microsoft .NET Host FX Resolver - 5.0.15 (x64)	40.60.31015
81	Microsoft .NET Host FX Resolver - 6.0.11 (x64)	48.47.50420
82	Microsoft .NET Host FX Resolver - 8.0.14 (x64)	64.56.29490
83	Microsoft .NET Host FX Resolver - 8.0.14 (x86)	64.56.29490
84	Microsoft .NET Runtime - 5.0.15 (x64)	40.60.31015
85	Microsoft .NET Runtime - 6.0.11 (x64)	48.47.50420
86	Microsoft .NET Runtime - 8.0.14 (x64)	64.56.29490
87	Microsoft .NET Runtime - 8.0.14 (x64)	8.0.14.34611
88	Microsoft .NET Runtime - 8.0.14 (x86)	64.56.29490
89	Microsoft ASP.NET Core 8.0.14 - Shared Framework (x86)	8.0.14.25112
90	Microsoft ASP.NET Core 8.0.14 Shared Framework (x86)	8.0.14.25112
91	Microsoft Edge	139.0.3405.102
92	Microsoft Edge WebView2 Runtime	139.0.3405.102
93	Microsoft GameInput	10.1.22621.3036
94	Microsoft OneDrive	25.140.0720.0001
95	Microsoft Server Speech Platform Runtime (x64)	11.0.7400.345
96	Microsoft Server Speech Recognition Language - TELE (en-IN)	11.0.7400.335
97	Microsoft Server Speech Recognition Language - TELE (pl-PL)	11.0.7400.335
98	Microsoft Server Speech Recognition Language - TELE (pt-BR)	11.0.7400.335
99	Microsoft Server Speech Recognition Language - TELE (ru-RU)	11.0.7400.335
100	Microsoft Server Speech Recognition Language - TELE (zh-CN)	11.0.7400.335
101	Microsoft Update Health Tools	5.72.0.0

102	Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.17	9.0.30729
103	Microsoft Visual C++ 2010 x64 Redistributable - 10.0.40219	10.0.40219
104	Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219	10.0.40219
105	Microsoft Visual C++ 2012 Redistributable (x64) - 11.0.61030	11.0.61030.0
106	Microsoft Visual C++ 2012 Redistributable (x86) - 11.0.60610	11.0.60610.1
107	Microsoft Visual C++ 2012 Redistributable (x86) - 11.0.61030	11.0.61030.0
108	Microsoft Visual C++ 2012 x64 Additional Runtime - 11.0.61030	11.0.61030
109	Microsoft Visual C++ 2012 x64 Minimum Runtime - 11.0.61030	11.0.61030
110	Microsoft Visual C++ 2012 x86 Additional Runtime - 11.0.61030	11.0.61030
111	Microsoft Visual C++ 2012 x86 Minimum Runtime - 11.0.61030	11.0.61030
112	Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.30501	12.0.30501.0
113	Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.40664	12.0.40664.0
114	Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.30501	12.0.30501.0
115	Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.40664	12.0.40664.0
116	Microsoft Visual C++ 2013 x64 Additional Runtime - 12.0.40664	12.0.40664
117	Microsoft Visual C++ 2013 x64 Minimum Runtime - 12.0.40664	12.0.40664
118	Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.40664	12.0.40664
119	Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.40664	12.0.40664
120	Microsoft Visual C++ 2015-2022 Redistributable (x64) - 14.44.35211	14.44.35211.0
121	Microsoft Visual C++ 2015-2022 Redistributable (x86) - 14.44.35211	14.44.35211.0
122	Microsoft Visual C++ 2022 X64 Additional Runtime - 14.44.35211	14.44.35211
123	Microsoft Visual C++ 2022 X64 Minimum Runtime - 14.44.35211	14.44.35211
124	Microsoft Visual C++ 2022 X86 Additional Runtime - 14.44.35211	14.44.35211
125	Microsoft Visual C++ 2022 X86 Minimum Runtime - 14.44.35211	14.44.35211
126	Microsoft Visual Studio Code (User)	1.103.1
127	Microsoft Windows Desktop Runtime - 5.0.15 (x64)	40.60.31016
128	Microsoft Windows Desktop Runtime - 5.0.15 (x64)	5.0.15.31016
129	Microsoft Windows Desktop Runtime - 6.0.11 (x64)	48.47.50419
130	Microsoft Windows Desktop Runtime - 6.0.11 (x64)	6.0.11.31823
131	Microsoft Windows Desktop Runtime - 8.0.14 (x86)	64.56.29521
132	Microsoft Windows Desktop Runtime - 8.0.14 (x86)	8.0.14.34613
133	Microsoft XNA Framework Redistributable 4.0 Refresh	4.0.30901.0
134	NVIDIA AIUser Container	1.42
135	NVIDIA App 11.0.4.526	11.0.4.526
136	NVIDIA Backend	11.0.4.526
137	NVIDIA Container	1.42
138	NVIDIA FrameView SDK 1.5.10920.35420203	1.5.10920.35420203

139	NVIDIA Graphics Driver 581.08	581.08
140	NVIDIA HD Audio Driver 1.4.5.0	1.4.5.0
141	NVIDIA Install Application	2.1002.434.0
142	NVIDIA LocalSystem Container	1.42
143	NVIDIA MessageBus 3 for NvApp	3.15
144	NVIDIA NvDLISR	1.0
145	NVIDIA PhysX System Software 9.23.1019	9.23.1019
146	NVIDIA Session Container	1.42
147	NVIDIA ShadowPlay 11.0.4.500	11.0.4.500
148	NVIDIA Telemetry Client	19.4.23.0
149	NVIDIA User Container	1.42
150	NVIDIA Virtual Audio 4.65.0.3	4.65.0.3
151	NVIDIA Watchdog Plugin for NvContainer	1.42
152	Nefarius Virtual Gamepad Emulation Bus Driver	1.17.333.0
153	Notepad++ (64-bit x64)	8.8.3
154	Notion 4.16.0	4.16.0
155	NvCpl	1.0
156	OBS Studio	31.0.4
157	OneBrowser	115.0.5790.171
158	Python 3.13.2 (64-bit)	3.13.2150.0
159	Python 3.13.2 Add to Path (64-bit)	3.13.2150.0
160	Python 3.13.2 Core Interpreter (64-bit)	3.13.2150.0
161	Python 3.13.2 Development Libraries (64-bit)	3.13.2150.0
162	Python 3.13.2 Documentation (64-bit)	3.13.2150.0
163	Python 3.13.2 Executables (64-bit)	3.13.2150.0
164	Python 3.13.2 Standard Library (64-bit)	3.13.2150.0
165	Python 3.13.2 Tcl/Tk Support (64-bit)	3.13.2150.0
166	Python 3.13.2 Test Suite (64-bit)	3.13.2150.0
167	Python 3.13.2 pip Bootstrap (64-bit)	3.13.2150.0
168	Python Launcher	3.13.2150.0
169	REDlauncher	3.2.1.1
170	Realtek Audio Driver	6.0.9768.1
171	Realtek Ethernet Controller Driver	10.73.815.2024
172	ReelSmart Motion Blur v5 for After Effects and Premiere Pro	5.1.8
173	Resident Evil 4	Unknown Version
174	Riot Vanguard	Unknown Version
175	Roblox Player for amaan	Unknown Version

176	Roblox Studio for amaan	Unknown Version
177	Rockstar Games Launcher	1.0.102.2459
178	Rockstar Games SDK	2.4.0.77
179	Steam	2.10.91.91
180	Streamlabs Desktop 1.17.0	1.17.0
181	Terraria	Unknown Version
182	UXP WebView Support	1.1.0
183	Ubisoft Connect	140.0.10857
184	Undertale	Unknown Version
185	VALORANT	Unknown Version
186	Verbatim_SureFireGaming_Product	1.0.3.11
187	Verbatim_SureFireGaming_Product	1.0.3.11
188	Voicemod	1.5.1
189	Voxengo Marvel GEQ	1.15
190	WD P40 Game Drive	1.0.2.18
191	WD P40 Game Drive	1.0.2.18
192	WD_BLACK AN1500	1.0.12.0
193	WD_BLACK AN1500	1.0.12.0
194	WD_BLACK D50	1.0.9.0
195	WD_BLACK D50	1.0.9.0
196	Web Companion	8.9.0.1201
197	WiX Toolset v3.14 Core	3.14.8722
198	WiX Toolset v3.14 Managed SDK	3.14.8722
199	WiX Toolset v3.14 Native 2010 SDK	3.14.8722
200	WiX Toolset v3.14 Native 2012 SDK	3.14.8722
201	WiX Toolset v3.14 Native 2013 SDK	3.14.8722
202	WiX Toolset v3.14 Native 2015 SDK	3.14.8722
203	WiX Toolset v3.14 Native 2017 SDK	3.14.8722
204	WiX Toolset v3.14 X64	3.14.8722
205	WiX Toolset v3.14.1.8722	3.14.1.8722
206	WinRAR 6.11 (64-bit)	6.11.0
207	cFosSpeed 12.01	12.01
208	obs-backgroundremoval version 1.1.13	1.1.13
209	osu!	latest
210	vertical-canvas version 1.5.2	1.5.2

## Startup Applications

Total Startup Applications: 258

S.No	Application Name	Path	Source
1	Discord	"C:\Users\amaan\AppData\Local\Discord\Update.exe" --processStart Discord.exe	Registry
2	EpicGamesLauncher	"C:\Program Files (x86)\Epic Games\Launcher\Portal\Binaries\Win64\EpicGamesLauncher.exe" -silent -launchcontext=boot	Registry
3	GoogleChromeAutoLaunch_7163853C09849CE938E06634FF0CEF44	"C:\Program Files\Google\Chrome\Application\chrome.exe" --no-startup-window /prefetch:5	Registry
4	MicrosoftEdgeAutoLaunch_75EEE27B96CB44DF3D365E0D42034901	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --win-session-start	Registry
5	OneDrive	"C:\Users\amaan\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background	Registry
6	Riot Vanguard	"C:\Program Files\Riot Vanguard\vgtray.exe"	Registry
7	RtkAudUService	"C:\WINDOWS\System32\DriverStore\FileRepository\realtekservice.inf_amd64_e54441f6cc56b0cb\RtkAudUService64.exe" -background	Registry
8	SecurityHealth	%windir%\system32\SecurityHealthSystray.exe	Registry
9	Steam	"C:\Program Files (x86)\Steam\steam.exe" -silent	Registry
10	Synapse3	C:\Program Files (x86)\Razer\Synapse3\WPFUI\Framework\Razer Synapse 3 Host\Razer Synapse 3.exe /StartMinimized	Registry
11	VoicemodV3	"C:\Program Files\Voicemod V3\Voicemod.exe" --boot	Registry
12	Web Companion	C:\Program Files (x86)\Lavasoftware\Web Companion\Application\WebCompanion.exe --minimize	Registry
13	\Agent Activation Runtime\S-1-5-21-3513449910-1489054591-2946980587-1001	C:\Users\amaan\AppData\Local\Microsoft\OneDrive\25.140.0720.0001\OneDriveLauncher.exe /startInstances	Task Scheduler
14	\Microsoft\Windows\.NET Framework\.NET Framework NGEN v4.0.30319	C:\WINDOWS\System32\AgentActivationRuntimeStarter.exe	Task Scheduler
15	\Microsoft\Windows\.NET Framework\.NET Framework NGEN v4.0.30319 64	COM handler	Task Scheduler

16	\Microsoft\Windows\NET Framework\NET Framework NGEN v4.0.30319 64 Critical	COM handler	Task Scheduler
17	\Microsoft\Windows\NET Framework\NET Framework NGEN v4.0.30319 Critical	COM handler	Task Scheduler
18	\Microsoft\Windows\AccountHealth\RecoverabilityToastTask	COM handler	Task Scheduler
19	\Microsoft\Windows\Active Directory Rights Management Services Client\AD RMS Rights Policy Template Management (Automated)	COM handler	Task Scheduler
20	\Microsoft\Windows\Active Directory Rights Management Services Client\AD RMS Rights Policy Template Management (Automated)	COM handler	Task Scheduler
21	\Microsoft\Windows\Active Directory Rights Management Services Client\AD RMS Rights Policy Template Management (Manual)	COM handler	Task Scheduler
22	\Microsoft\Windows\AppID\Policies\PolicyConverter	COM handler	Task Scheduler
23	\Microsoft\Windows\AppID\VerifiedPublisherCertStoreCheck	%windir%\system32\appidpolicyconverter.exe	Task Scheduler
24	\Microsoft\Windows\AppListBackup\Backup	%windir%\system32\dstokenclean.exe	Task Scheduler
25	\Microsoft\Windows\AppListBackup\BackupNonMaintenance	COM handler	Task Scheduler
26	\Microsoft\Windows\Application Experience\MareBackup	%windir%\system32\appidcertstorecheck.exe	Task Scheduler
27	\Microsoft\Windows\Application Experience\Microsoft Compatibility Appraiser	Multiple actions	Task Scheduler
28	\Microsoft\Windows\Application Experience\Microsoft Compatibility Appraiser Exp	%windir%\system32\sc.exe start InventorySvc	Task Scheduler
29	\Microsoft\Windows\Application Experience\PcaPatchDbTask	%windir%\system32\compattelrunner.exe -m:appraiser.dll -f:DoScheduledTelemetryRun express	Task Scheduler
30	\Microsoft\Windows\Application Experience\SdbinstMergeDbTask	%windir%\system32\rundll32.exe %windir%\system32\PcaSvc.dll,PcaPatchSdbTask	Task Scheduler

31	\Microsoft\Windows\Application Experience\SdbinstMergeDb Task	%windir%\system32\sdbinst.exe -mm	Task Scheduler
32	\Microsoft\Windows\Application Experience\StartupAppTask	%windir%\system32\sdbinst.exe -mm	Task Scheduler
33	\Microsoft\Windows\Application Data\CleanupTemporaryState	%windir%\system32\AppHostRegistrationVerifier.exe	Task Scheduler
34	\Microsoft\Windows\Application Data\DsSvcCleanup	%windir%\system32\rundll32.exe Windows.Storage.ApplicationData.dll,CleanupTemporaryState	Task Scheduler
35	\Microsoft\Windows\Application Data\appuriverifierdaily	%windir%\system32\rundll32.exe Startupscan.dll,SusRunTask	Task Scheduler
36	\Microsoft\Windows\Application Data\appuriverifierinstall	%windir%\system32\AppHostRegistrationVerifier.exe	Task Scheduler
37	\Microsoft\Windows\AppxDeploymentClient\Pre-staged app cleanup	COM handler	Task Scheduler
38	\Microsoft\Windows\Autochk\Proxy	%windir%\system32\rundll32.exe %windir%\system32\AppxDeploymentClient.dll,AppxPreStageCleanupRunTask	Task Scheduler
39	\Microsoft\Windows\BitLocker\BitLocker Encrypt All Drives	%windir%\system32\rundll32.exe /d acproxy.dll,PerformAutochkOperations	Task Scheduler
40	\Microsoft\Windows\BitLocker\BitLocker MDM policy Refresh	COM handler	Task Scheduler
41	\Microsoft\Windows\Bluetooth\UninstallDeviceTask	COM handler	Task Scheduler
42	\Microsoft\Windows\BrokerInfrastructure\BgTaskRegistrationMaintenanceTask	BthUdTask.exe \$(Arg0)	Task Scheduler
43	\Microsoft\Windows\Certificate ServicesClient\UserTask	%windir%\system32\rundll32.exe %windir%\system32\CapabilityAccessManager.dll,CapabilityAccessManagerDoStoreMaintenance	Task Scheduler
44	\Microsoft\Windows\Certificate ServicesClient\UserTask	COM handler	Task Scheduler
45	\Microsoft\Windows\Certificate ServicesClient\UserTask	COM handler	Task Scheduler
46	\Microsoft\Windows\Certificate ServicesClient\UserTask	COM handler	Task Scheduler
47	\Microsoft\Windows\Certificate ServicesClient\UserTask-Roam	COM handler	Task Scheduler
48	\Microsoft\Windows\Certificate ServicesClient\UserTask-Roam	COM handler	Task Scheduler



49	\Microsoft\Windows\Chkdsk\ProactiveScan	COM handler	Task Scheduler
50	\Microsoft\Windows\Chkdsk\SyspartRepair	COM handler	Task Scheduler
51	\Microsoft\Windows\CloudExperienceHost\CreateObjectTask	%windir%\system32\bcdboot.exe %windir% /sysrepair	Task Scheduler
52	\Microsoft\Windows\CloudRestore\Backup	COM handler	Task Scheduler
53	\Microsoft\Windows\CloudRestore\Backup	COM handler	Task Scheduler
54	\Microsoft\Windows\CloudRestore\Restore	COM handler	Task Scheduler
55	\Microsoft\Windows\ConsentUX\UnifiedConsent\UnifiedConsentSyncTask	COM handler	Task Scheduler
56	\Microsoft\Windows\ConsentUX\UnifiedConsent\UnifiedConsentSyncTask	COM handler	Task Scheduler
57	\Microsoft\Windows\Containers\CmCleanup	COM handler	Task Scheduler
58	\Microsoft\Windows\Customer Experience Improvement Program\Consolidator	COM handler	Task Scheduler
59	\Microsoft\Windows\Customer Experience Improvement Program\UsbCeip	%SystemRoot%\System32\wsqmcons.exe	Task Scheduler
60	\Microsoft\Windows\DUSM\dusmtask	COM handler	Task Scheduler
61	\Microsoft\Windows\Data Integrity Scan\Data Integrity Check And Scan	COM handler	Task Scheduler
62	\Microsoft\Windows\Data Integrity Scan\Data Integrity Check And Scan	COM handler	Task Scheduler
63	\Microsoft\Windows\Data Integrity Scan\Data Integrity Scan	COM handler	Task Scheduler
64	\Microsoft\Windows\Data Integrity Scan\Data Integrity Scan for Crash Recovery	COM handler	Task Scheduler
65	\Microsoft\Windows\Defrag\ScheduledDefrag	COM handler	Task Scheduler
66	\Microsoft\Windows\Device Information\Device	%windir%\system32\defrag.exe -c -h -o -\$	Task Scheduler

67	\Microsoft\Windows\Device Information\Device	%windir%\system32\devicecensus.exe SystemCxt	Task Scheduler
68	\Microsoft\Windows\Device Information\Device User	%windir%\system32\devicecensus.exe SystemCxt	Task Scheduler
69	\Microsoft\Windows\Device Setup\Driver Recovery on Reboot	%windir%\system32\devicecensus.exe UserCxt	Task Scheduler
70	\Microsoft\Windows\Diagnosis\RecommendedTroubleshootingScanner	COM handler	Task Scheduler
71	\Microsoft\Windows\Diagnosis\RecommendedTroubleshootingScanner	COM handler	Task Scheduler
72	\Microsoft\Windows\Diagnosis\RecommendedTroubleshootingScanner	COM handler	Task Scheduler
73	\Microsoft\Windows\Diagnosis\RecommendedTroubleshootingScanner	COM handler	Task Scheduler
74	\Microsoft\Windows\Diagnosis\Scheduled	COM handler	Task Scheduler
75	\Microsoft\Windows\Diagnosis\UnexpectedCodepath	COM handler	Task Scheduler
76	\Microsoft\Windows\DirectX\DXGIDataAdapterCache	%windir%\system32\directxdatabaseupdater.exe	Task Scheduler
77	\Microsoft\Windows\DirectX\DXGIDataAdapterCache	%windir%\system32\dxgiadaptercache.exe	Task Scheduler
78	\Microsoft\Windows\DirectX\DXGIDataAdapterCache	%windir%\system32\dxgiadaptercache.exe	Task Scheduler
79	\Microsoft\Windows\DirectX\DirectXDatabaseUpdater	%windir%\system32\UCConfigTask.exe	Task Scheduler
80	\Microsoft\Windows\DirectX\DirectXDatabaseUpdater	%windir%\system32\directxdatabaseupdater.exe	Task Scheduler
81	\Microsoft\Windows\DiskCleanup\SilentCleanup	%windir%\system32\dxgiadaptercache.exe	Task Scheduler
82	\Microsoft\Windows\DiskDiagnostic\Microsoft-Windows-DiskDiagnosticDataCollector	%windir%\system32\cleanmgr.exe /autocleanstoragesense /d %systemdrive%	Task Scheduler
83	\Microsoft\Windows\DiskDiagnostic\Microsoft-Windows-DiskDiagnosticResolver	%windir%\system32\rundll32.exe dfdts.dll,DfdGetDefaultPolicyAndSMART	Task Scheduler
84	\Microsoft\Windows\DiskFootprint\Diagnostics	%windir%\system32\DFDWiz.exe	Task Scheduler

85	\Microsoft\Windows\DiskFootprint\StorageSense	%windir%\system32\disksnapshot.exe -z	Task Scheduler
86	\Microsoft\Windows\EDP\EDP App Launch Task	%SystemRoot%\System32\dusmtask.exe	Task Scheduler
87	\Microsoft\Windows\EDP\EDP Auth Task	COM handler	Task Scheduler
88	\Microsoft\Windows\EDP\EDP Inaccessible Credentials Task	COM handler	Task Scheduler
89	\Microsoft\Windows\EDP\StorageCardEncryption Task	COM handler	Task Scheduler
90	\Microsoft\Windows\ExploitGuard\ExploitGuard MDM policy Refresh	COM handler	Task Scheduler
91	\Microsoft\Windows\ExploitGuard\ExploitGuard MDM policy Refresh	COM handler	Task Scheduler
92	\Microsoft\Windows\ExploitGuard\ExploitGuard MDM policy Refresh	COM handler	Task Scheduler
93	\Microsoft\Windows\Feedback\Siuf\DmClient	COM handler	Task Scheduler
94	\Microsoft\Windows\Feedback\Siuf\DmClientOnScenarioDownload	%windir%\system32\dmclient.exe	Task Scheduler
95	\Microsoft\Windows\File Classification Infrastructure\Property Definition Sync	%windir%\system32\dmclient.exe utcwnf	Task Scheduler
96	\Microsoft\Windows\FileHistory\File History (maintenance mode)	COM handler	Task Scheduler
97	\Microsoft\Windows\Flighting\FeatureConfig\BootstrapUsage DataReporting	COM handler	Task Scheduler
98	\Microsoft\Windows\Flighting\FeatureConfig\GovernedFeatureUsageProcessing	COM handler	Task Scheduler
99	\Microsoft\Windows\Flighting\FeatureConfig\ReconcileConfigs	COM handler	Task Scheduler
100	\Microsoft\Windows\Flighting\FeatureConfig\ReconcileFeatures	COM handler	Task Scheduler

101	\\Microsoft\\Windows\\Flighting\\FeatureConfig\\ReconcileFeatures	COM handler	Task Scheduler
102	\\Microsoft\\Windows\\Flighting\\FeatureConfig\\ReconcileFeatures	COM handler	Task Scheduler
103	\\Microsoft\\Windows\\Flighting\\FeatureConfig\\ReconcileFeatures	COM handler	Task Scheduler
104	\\Microsoft\\Windows\\Flighting\\FeatureConfig\\ReconcileFeatures	COM handler	Task Scheduler
105	\\Microsoft\\Windows\\Flighting\\FeatureConfig\\ReconcileFeatures	COM handler	Task Scheduler
106	\\Microsoft\\Windows\\Flighting\\FeatureConfig\\UsageDataFlushing	COM handler	Task Scheduler
107	\\Microsoft\\Windows\\Flighting\\FeatureConfig\\UsageDataFlushing	COM handler	Task Scheduler
108	\\Microsoft\\Windows\\Flighting\\FeatureConfig\\UsageDataFlushing	COM handler	Task Scheduler
109	\\Microsoft\\Windows\\Flighting\\FeatureConfig\\UsageDataReceiver	COM handler	Task Scheduler
110	\\Microsoft\\Windows\\Flighting\\FeatureConfig\\UsageDataReporting	COM handler	Task Scheduler
111	\\Microsoft\\Windows\\Flighting\\OneSettings\\RefreshCache	COM handler	Task Scheduler
112	\\Microsoft\\Windows\\Flighting\\OneSettings\\RefreshCache	COM handler	Task Scheduler
113	\\Microsoft\\Windows\\Flighting\\OneSettings\\RefreshCache	COM handler	Task Scheduler
114	\\Microsoft\\Windows\\Hotpatch\\Monitoring	COM handler	Task Scheduler
115	\\Microsoft\\Windows\\Hotpatch\\Monitoring	%systemroot%\\system32\\cmd.exe /d /c %systemroot%\\system32\\hpatchmonTask.cmd	Task Scheduler
116	\\Microsoft\\Windows\\Hotpatch\\Monitoring	%systemroot%\\system32\\cmd.exe /d /c %systemroot%\\system32\\hpatchmonTask.cmd	Task Scheduler
117	\\Microsoft\\Windows\\InstallService\\RestoreDevice	COM handler	Task Scheduler

118	\Microsoft\Windows\InstallService\ScanForUpdates	COM handler	Task Scheduler
119	\Microsoft\Windows\InstallService\ScanForUpdates	COM handler	Task Scheduler
120	\Microsoft\Windows\InstallService\ScanForUpdates	COM handler	Task Scheduler
121	\Microsoft\Windows\InstallService\ScanForUpdatesAsUser	COM handler	Task Scheduler
122	\Microsoft\Windows\InstallService\WakeUpAndContinueUpdates	COM handler	Task Scheduler
123	\Microsoft\Windows\InstallService\WakeUpAndScanForUpdates	COM handler	Task Scheduler
124	\Microsoft\Windows\International\Synchronize Language Settings	COM handler	Task Scheduler
125	\Microsoft\Windows\International\Synchronize Language Settings	COM handler	Task Scheduler
126	\Microsoft\Windows\Kernel\La57Cleanup	COM handler	Task Scheduler
127	\Microsoft\Windows\LanguageComponents\Installer\Installation	%windir%\system32\la57setup.exe	Task Scheduler
128	\Microsoft\Windows\LanguageComponents\Installer\ReconcileLanguageResources	COM handler	Task Scheduler
129	\Microsoft\Windows\Location\Notifications	COM handler	Task Scheduler
130	\Microsoft\Windows\Location\WindowsActionDialog	%windir%\System32\LocationNotificationWindows.exe	Task Scheduler
131	\Microsoft\Windows\MUI\LPremove	COM handler	Task Scheduler
132	\Microsoft\Windows\Maintenance\WinSAT	%windir%\System32\WindowsActionDialog.exe	Task Scheduler
133	\Microsoft\Windows\Management\Autopilot\DetectHardwareChange	COM handler	Task Scheduler
134	\Microsoft\Windows\Management\Autopilot\DetectHardwareChange	COM handler	Task Scheduler

135	\\Microsoft\\Windows\\Management\\Autopilot\\RemediateHardwareChange	COM handler	Task Scheduler
136	\\Microsoft\\Windows\\Management\\Provisioning\\Cellular	COM handler	Task Scheduler
137	\\Microsoft\\Windows\\Management\\Provisioning\\Logon	%windir%\\system32\\ProvTool.exe /turn 7 /source CellStateChangeTask	Task Scheduler
138	\\Microsoft\\Windows\\Management\\Provisioning\\MdmDiagnosticsCleanup	%windir%\\system32\\ProvTool.exe /turn 5 /source LogonIdleTask	Task Scheduler
139	\\Microsoft\\Windows\\Management\\Provisioning\\Retry	%windir%\\system32\\MdmDiagnosticsTool.exe /clean	Task Scheduler
140	\\Microsoft\\Windows\\Management\\Provisioning\\RunOnReboot	%windir%\\system32\\ProvTool.exe /turn 5 /source ProvRetryTask	Task Scheduler
141	\\Microsoft\\Windows\\Maps\\MapsToastTask	%windir%\\system32\\ProvTool.exe /turn 5 /source ContinueSessionTask	Task Scheduler
142	\\Microsoft\\Windows\\Maps\\MapsUpdateTask	COM handler	Task Scheduler
143	\\Microsoft\\Windows\\MemoryDiagnostic\\AutomaticOfflineMemoryDiagnostic	COM handler	Task Scheduler
144	\\Microsoft\\Windows\\MemoryDiagnostic\\ProcessMemoryDiagnosticEvents	COM handler	Task Scheduler
145	\\Microsoft\\Windows\\MemoryDiagnostic\\ProcessMemoryDiagnosticEvents	COM handler	Task Scheduler
146	\\Microsoft\\Windows\\MemoryDiagnostic\\ProcessMemoryDiagnosticEvents	COM handler	Task Scheduler
147	\\Microsoft\\Windows\\MemoryDiagnostic\\ProcessMemoryDiagnosticEvents	COM handler	Task Scheduler
148	\\Microsoft\\Windows\\MemoryDiagnostic\\RunFullMemoryDiagnostic	COM handler	Task Scheduler
149	\\Microsoft\\Windows\\Multimedia\\SystemSoundsService	%windir%\\system32\\lpremove.exe	Task Scheduler
150	\\Microsoft\\Windows\\NetworkConnectivityStatusIndicator\\NcsIdentifyUserProxies	COM handler	Task Scheduler
151	\\Microsoft\\Windows\\NetworkConnectivityStatusIndicator\\NcsIdentifyUserProxies	COM handler	Task Scheduler

152	\\Microsoft\\Windows\\Network Connectivity Status Indicator\\NcsIdentifyUserProxies	COM handler	Task Scheduler
153	\\Microsoft\\Windows\\NlaSvc\\WiFiTask	COM handler	Task Scheduler
154	\\Microsoft\\Windows\\Offline Files\\Background Synchronization	%SystemRoot%\\System32\\WiFiTask.exe nla	Task Scheduler
155	\\Microsoft\\Windows\\Offline Files\\Logon Synchronization	COM handler	Task Scheduler
156	\\Microsoft\\Windows\\PCRPF\\PCR Prediction Framework Firmware Update Task	COM handler	Task Scheduler
157	\\Microsoft\\Windows\\PerformanceTrace\\RequestTrace	%windir%\\system32\\rundll32.exe %windir%\\system32\\pcrpf.dll,NotifyFirmwareUpdateStaged	Task Scheduler
158	\\Microsoft\\Windows\\Plug and Play\\Device Install Group Policy	COM handler	Task Scheduler
159	\\Microsoft\\Windows\\Plug and Play\\Device Install Reboot Required	COM handler	Task Scheduler
160	\\Microsoft\\Windows\\Plug and Play\\Device Install Reboot Required	COM handler	Task Scheduler
161	\\Microsoft\\Windows\\Plug and Play\\Sysprep Generalize Drivers	COM handler	Task Scheduler
162	\\Microsoft\\Windows\\Power Efficiency Diagnostics\\AnalyzeSystem	%SystemRoot%\\System32\\drvinst.exe 6	Task Scheduler
163	\\Microsoft\\Windows\\Printing\\EduPrintProv	COM handler	Task Scheduler
164	\\Microsoft\\Windows\\Printing\\PrintJobCleanupTask	COM handler	Task Scheduler
165	\\Microsoft\\Windows\\Printing\\PrinterCleanupTask	%windir%\\system32\\eduprintprov.exe	Task Scheduler
166	\\Microsoft\\Windows\\ReFsDedupSvc\\Initialization	COM handler	Task Scheduler
167	\\Microsoft\\Windows\\Recovery Environment\\VerifyWinRE	COM handler	Task Scheduler
168	\\Microsoft\\Windows\\Registry\\RegIdleBackup	COM handler	Task Scheduler
169	\\Microsoft\\Windows\\Servicing\\OOBEFodSetup	COM handler	Task Scheduler

170	\Microsoft\Windows\Servicing\StartComponentCleanup	%windir%\system32\OOBEFodSetup.exe	Task Scheduler
171	\Microsoft\Windows\SharedPC\Account Cleanup	COM handler	Task Scheduler
172	\Microsoft\Windows\Shell\Crea teObjectTask	COM handler	Task Scheduler
173	\Microsoft\Windows\Shell\Fami lySafetyMonitor	COM handler	Task Scheduler
174	\Microsoft\Windows\Shell\Fami lySafetyRefreshTask	%windir%\System32\wpcmon.exe	Task Scheduler
175	\Microsoft\Windows\Shell\Inde xerAutomaticMaintenance	COM handler	Task Scheduler
176	\Microsoft\Windows\Shell\The mesSyncedImageDownload	COM handler	Task Scheduler
177	\Microsoft\Windows\SoftwareP rotectionPlatform\SvcRestartT askLogon	COM handler	Task Scheduler
178	\Microsoft\Windows\SpacePort \SpaceAgentTask	COM handler	Task Scheduler
179	\Microsoft\Windows\SpacePort \SpaceAgentTask	%windir%\system32\SpaceAgent.exe	Task Scheduler
180	\Microsoft\Windows\SpacePort \SpaceManagerTask	%windir%\system32\SpaceAgent.exe	Task Scheduler
181	\Microsoft\Windows\SpacePort \SpaceManagerTask	%windir%\system32\spaceman.exe /Work	Task Scheduler
182	\Microsoft\Windows\StateRepo sitory\MaintenanceTasks	%windir%\system32\spaceman.exe /Work	Task Scheduler
183	\Microsoft\Windows\Storage Tiers Management\Storage Tiers Management Initialization	%windir%\system32\rundll32.exe %windir%\system3 2\Windows.StateRepositoryClient.dll,StateRepository DoMaintenanceTasks	Task Scheduler
184	\Microsoft\Windows\Storage Tiers Management\Storage Tiers Optimization	COM handler	Task Scheduler
185	\Microsoft\Windows\Subscripti on\EnableLicenseAcquisition	%windir%\system32\defrag.exe -c -h -g -# -m 8 -i 13500	Task Scheduler
186	\Microsoft\Windows\Subscripti on\EnableLicenseAcquisition	%SystemRoot%\system32\ClipRenew.exe -e	Task Scheduler
187	\Microsoft\Windows\Subscripti on\EnableLicenseAcquisition	%SystemRoot%\system32\ClipRenew.exe -e	Task Scheduler
188	\Microsoft\Windows\Subscripti on\LicenseAcquisition	%SystemRoot%\system32\ClipRenew.exe -e	Task Scheduler



189	\Microsoft\Windows\Subscription\LicenseAcquisition	%SystemRoot%\system32\ClipRenew.exe	Task Scheduler
190	\Microsoft\Windows\Subscription\LicenseAcquisition	%SystemRoot%\system32\ClipRenew.exe	Task Scheduler
191	\Microsoft\Windows\Sustainability\PowerGridForecastTask	%SystemRoot%\system32\ClipRenew.exe	Task Scheduler
192	\Microsoft\Windows\Sustainability\PowerGridForecastTask	COM handler	Task Scheduler
193	\Microsoft\Windows\Sustainability\SustainabilityTelemetry	COM handler	Task Scheduler
194	\Microsoft\Windows\Sysmain\HybridDriveCachePrepopulate	COM handler	Task Scheduler
195	\Microsoft\Windows\Sysmain\HybridDriveCacheRebalance	COM handler	Task Scheduler
196	\Microsoft\Windows\Sysmain\ResPriStaticDbSync	COM handler	Task Scheduler
197	\Microsoft\Windows\Sysmain\WsSwapAssessmentTask	COM handler	Task Scheduler
198	\Microsoft\Windows\SystemRestore\SR	%windir%\system32\rundll32.exe sysmain.dll,PfSvWsSwapAssessmentTask	Task Scheduler
199	\Microsoft\Windows\Task Manager\Interactive	%windir%\system32\srtasks.exe ExecuteScheduledSPPCreation	Task Scheduler
200	\Microsoft\Windows\TextServicesFramework\MsCtfMonitor	COM handler	Task Scheduler
201	\Microsoft\Windows\Time Synchronization\ForceSynchronize Time	COM handler	Task Scheduler
202	\Microsoft\Windows\Time Synchronization\ForceSynchronize Time	COM handler	Task Scheduler
203	\Microsoft\Windows\Time Synchronization\SynchronizeTime	COM handler	Task Scheduler
204	\Microsoft\Windows\Time Zone\SynchronizeTimeZone	%windir%\system32\sc.exe start w32time task_started	Task Scheduler
205	\Microsoft\Windows\UPnP\UPnPHostConfig	%windir%\system32\tzsync.exe	Task Scheduler
206	\Microsoft\Windows\USB\Usb-Notifications	sc.exe config upnphost start= auto	Task Scheduler
207	\Microsoft\Windows\USB\Usb-Notifications	COM handler	Task Scheduler
208	\Microsoft\Windows\USB\Usb-Notifications	COM handler	Task Scheduler

209	\Microsoft\Windows\USB\Usb-Notifications	COM handler	Task Scheduler
210	\Microsoft\Windows\WCM\WiFi Task	COM handler	Task Scheduler
211	\Microsoft\Windows\WDI\ResolutionHost	%SystemRoot%\System32\WiFiTask.exe	Task Scheduler
212	\Microsoft\Windows\Windows Defender\Windows Defender Cache Maintenance	COM handler	Task Scheduler
213	\Microsoft\Windows\Windows Defender\Windows Defender Cleanup	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.25070.5-0\MpCmdRun.exe -IdleTask -TaskName WdCacheMaintenance	Task Scheduler
214	\Microsoft\Windows\Windows Defender\Windows Defender Scheduled Scan	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.25070.5-0\MpCmdRun.exe -IdleTask -TaskName WdCleanup	Task Scheduler
215	\Microsoft\Windows\Windows Defender\Windows Defender Verification	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.25070.5-0\MpCmdRun.exe Scan -ScheduleJob -ScanTrigger 55 -IdleScheduledJob	Task Scheduler
216	\Microsoft\Windows\Windows Error Reporting\QueueReporting	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.25070.5-0\MpCmdRun.exe -IdleTask -TaskName WdVerification	Task Scheduler
217	\Microsoft\Windows\Windows Error Reporting\QueueReporting	%windir%\system32\wermgr.exe -upload	Task Scheduler
218	\Microsoft\Windows\Windows Error Reporting\QueueReporting	%windir%\system32\wermgr.exe -upload	Task Scheduler
219	\Microsoft\Windows\Windows Error Reporting\QueueReporting	%windir%\system32\wermgr.exe -upload	Task Scheduler
220	\Microsoft\Windows\Windows Error Reporting\QueueReporting	%windir%\system32\wermgr.exe -upload	Task Scheduler
221	\Microsoft\Windows\Windows Filtering Platform\BfeOnServiceStartTypeChange	%windir%\system32\wermgr.exe -upload	Task Scheduler
222	\Microsoft\Windows\Windows Media Sharing\UpdateLibrary	%windir%\system32\rundll32.exe bfe.dll,BfeOnServiceStartTypeChange	Task Scheduler
223	\Microsoft\Windows\Windows ColorSystem\Calibration Loader	"%ProgramFiles%\Windows Media Player\wmpnscfg.exe"	Task Scheduler
224	\Microsoft\Windows\Windows ColorSystem\Calibration Loader	COM handler	Task Scheduler

225	\Microsoft\Windows\WindowsUpdate\Scheduled Start	COM handler	Task Scheduler
226	\Microsoft\Windows\WindowsUpdate\Scheduled Start	%systemroot%\System32\sc.exe start wuauserv	Task Scheduler
227	\Microsoft\Windows\WindowsUpdate\Scheduled Start	%systemroot%\System32\sc.exe start wuauserv	Task Scheduler
228	\Microsoft\Windows\WindowsUpdate\Scheduled Start	%systemroot%\System32\sc.exe start wuauserv	Task Scheduler
229	\Microsoft\Windows\Wininet\CacheTask	%systemroot%\System32\sc.exe start wuauserv	Task Scheduler
230	\Microsoft\Windows\WlanSvc\CDSSync	COM handler	Task Scheduler
231	\Microsoft\Windows\WlanSvc\MoProfileManagement	COM handler	Task Scheduler
232	\Microsoft\Windows\WlanSvc\MoProfileManagement	COM handler	Task Scheduler
233	\Microsoft\Windows\Work Folders\Work Folders Logon Synchronization	COM handler	Task Scheduler
234	\Microsoft\Windows\Work Folders\Work Folders Maintenance Work	COM handler	Task Scheduler
235	\Microsoft\Windows\Workplace Join\Automatic-Device-Join	COM handler	Task Scheduler
236	\Microsoft\Windows\Workplace Join\Automatic-Device-Join	%SystemRoot%\System32\dsregcmd.exe \$(Arg0) \$(Arg1) \$(Arg2)	Task Scheduler
237	\Microsoft\Windows\Workplace Join\Device-Sync	%SystemRoot%\System32\dsregcmd.exe \$(Arg0) \$(Arg1) \$(Arg2)	Task Scheduler
238	\Microsoft\Windows\Workplace Join\Recovery-Check	COM handler	Task Scheduler
239	\Microsoft\Windows\Workplace Join\Recovery-Check	%SystemRoot%\System32\dsregcmd.exe /checkrecovery	Task Scheduler
240	\Microsoft\Windows\WwanSvc\NotificationTask	%SystemRoot%\System32\dsregcmd.exe /checkrecovery	Task Scheduler
241	\Microsoft\Windows\WwanSvc\OobeDiscovery	%SystemRoot%\System32\WiFiTask.exe wwan	Task Scheduler
242	\Microsoft\Windows\WwanSvc\OobeDiscovery	COM handler	Task Scheduler
243	\Microsoft\Windows\WwanSvc\OobeDiscovery	COM handler	Task Scheduler
244	\Microsoft\Windows\capabilityaccessmanager\maintenancetasks	COM handler	Task Scheduler

245	\\Microsoft\\Windows\\input\\InputSettingsRestoreDataAvailable	%systemroot%\\system32\\cmd.exe /d /c %systemroot%\\system32\\hpatchmonTask.cmd	Task Scheduler
246	\\Microsoft\\Windows\\input\\LocalUserSyncDataAvailable	COM handler	Task Scheduler
247	\\Microsoft\\Windows\\input\\MouseSyncDataAvailable	COM handler	Task Scheduler
248	\\Microsoft\\Windows\\input\\PenSyncDataAvailable	COM handler	Task Scheduler
249	\\Microsoft\\Windows\\input\\RemoteMouseSyncDataAvailable	COM handler	Task Scheduler
250	\\Microsoft\\Windows\\input\\RemotePenSyncDataAvailable	COM handler	Task Scheduler
251	\\Microsoft\\Windows\\input\\RemoteTouchpadSyncDataAvailable	COM handler	Task Scheduler
252	\\Microsoft\\Windows\\input\\TouchpadSyncDataAvailable	COM handler	Task Scheduler
253	\\Microsoft\\Windows\\input\\syncpensettings	COM handler	Task Scheduler
254	\\Microsoft\\XblGameSave\\XblGameSaveTask	COM handler	Task Scheduler
255	\\OneDrive Reporting Task-S-1-5-21-3513449910-1489054591-2946980587-1001	"C:\\Program Files\\NVIDIA Corporation\\NVIDIA App\\CEF\\NVIDIA App.exe"	Task Scheduler
256	\\OneDrive Standalone Update Task-S-1-5-21-3513449910-1489054591-2946980587-1001	%localappdata%\\Microsoft\\OneDrive\\OneDriveStandaloneUpdater.exe /reporting	Task Scheduler
257	\\OneDrive Startup Task-S-1-5-21-3513449910-1489054591-2946980587-1001	%localappdata%\\Microsoft\\OneDrive\\OneDriveStandaloneUpdater.exe	Task Scheduler
258	electron.app.Notion	C:\\Users\\amaan\\AppData\\Local\\Programs\\Notion\\Notion.exe --open-at-login	Registry

## **Shared Folders**

**Total Shared Folders: 4**

S.No	Shared Name	Local Path	Description
1	C\$	C:\\	Default share
2	E\$	E:\\	Default share
3	IPC\$	Remote	IPC

4	Users	C:\Users	No description available
---	-------	----------	--------------------------

## Unwanted Software Detection

Total Unwanted Software Found: 3

S.No	Software Name
1	ENE Video Capture Box HAL
2	ENE Video Capture Box HAL
3	Dropbox Redeem Launcher

## USB Logs

- **Event ID:** Unknown  
**Timestamp:** Unknown  
**Source:** Unknown  
**Description:** No Description Found

## Security Logs

- **Event ID:** Unknown  
**Timestamp:** Unknown  
**Source:** Unknown  
**Description:** No Description Found

## System Logs

- **Event ID:** \*\* 111  
**Timestamp:** \*\* Unknown  
**Source:** \*\* Unknown  
**Description:** No Description Found
- **Event ID:** \*\* 113  
**Timestamp:** \*\* Unknown

**Source:** \*\* Unknown  
**Description:** No Description Found

- **Event ID:** \*\* 10016  
**Timestamp:** \*\* Unknown  
**Source:** \*\* Unknown  
**Description:** No Description Found
- **Event ID:** \*\* 1014  
**Timestamp:** \*\* Unknown  
**Source:** \*\* Unknown  
**Description:** No Description Found
- **Event ID:** \*\* 16  
**Timestamp:** \*\* Unknown  
**Source:** \*\* Unknown  
**Description:** No Description Found
- **Event ID:** \*\* 16  
**Timestamp:** \*\* Unknown  
**Source:** \*\* Unknown  
**Description:** No Description Found
- **Event ID:** \*\* 16  
**Timestamp:** \*\* Unknown  
**Source:** \*\* Unknown  
**Description:** No Description Found
- **Event ID:** \*\* 113  
**Timestamp:** \*\* Unknown  
**Source:** \*\* Unknown  
**Description:** No Description Found
- **Event ID:** \*\* 114  
**Timestamp:** \*\* Unknown  
**Source:** \*\* Unknown  
**Description:** No Description Found
- **Event ID:** \*\* 113  
**Timestamp:** \*\* Unknown  
**Source:** \*\* Unknown  
**Description:** No Description Found

- **Event ID:** \*\* 7040  
**Timestamp:** \*\* Unknown  
**Source:** \*\* Unknown  
**Description:** No Description Found
- **Event ID:** \*\* 114  
**Timestamp:** \*\* Unknown  
**Source:** \*\* Unknown  
**Description:** No Description Found
- **Event ID:** \*\* 10016  
**Timestamp:** \*\* Unknown  
**Source:** \*\* Unknown  
**Description:** No Description Found
- **Event ID:** \*\* 16  
**Timestamp:** \*\* Unknown  
**Source:** \*\* Unknown  
**Description:** No Description Found
- **Event ID:** \*\* 15  
**Timestamp:** \*\* Unknown  
**Source:** \*\* Unknown  
**Description:** No Description Found
- **Event ID:** \*\* 44  
**Timestamp:** \*\* Unknown  
**Source:** \*\* Unknown  
**Description:** No Description Found
- **Event ID:** \*\* 43  
**Timestamp:** \*\* Unknown  
**Source:** \*\* Unknown  
**Description:** No Description Found
- **Event ID:** \*\* 19  
**Timestamp:** \*\* Unknown  
**Source:** \*\* Unknown  
**Description:** No Description Found
- **Event ID:** \*\* 10016  
**Timestamp:** \*\* Unknown  
**Source:** \*\* Unknown  
**Description:** No Description Found
- **Event ID:** \*\* 10016  
**Timestamp:** \*\* Unknown  
**Source:** \*\* Unknown

**Description:** No Description Found

## Application Logs

- **Event ID:** \*\* 1003  
**Timestamp:** \*\* Unknown  
**Source:** \*\* Unknown  
**Description:** No Description Found
- **Event ID:** \*\* 8198  
**Timestamp:** \*\* Unknown  
**Source:** \*\* Unknown  
**Description:** No Description Found
- **Event ID:** \*\* 1003  
**Timestamp:** \*\* Unknown  
**Source:** \*\* Unknown  
**Description:** No Description Found
- **Event ID:** \*\* 8198  
**Timestamp:** \*\* Unknown  
**Source:** \*\* Unknown  
**Description:** No Description Found
- **Event ID:** \*\* 1003  
**Timestamp:** \*\* Unknown  
**Source:** \*\* Unknown  
**Description:** No Description Found
- **Event ID:** \*\* 8198  
**Timestamp:** \*\* Unknown  
**Source:** \*\* Unknown  
**Description:** No Description Found
- **Event ID:** \*\* 12288  
**Timestamp:** \*\* Unknown  
**Source:** \*\* Unknown  
**Description:** No Description Found
- **Event ID:** \*\* 1003  
**Timestamp:** \*\* Unknown  
**Source:** \*\* Unknown  
**Description:** No Description Found



- **Event ID:** \*\* 1003  
**Timestamp:** \*\* Unknown  
**Source:** \*\* Unknown  
**Description:** No Description Found
- **Event ID:** \*\* 8198  
**Timestamp:** \*\* Unknown  
**Source:** \*\* Unknown  
**Description:** No Description Found
- **Event ID:** \*\* 12288  
**Timestamp:** \*\* Unknown  
**Source:** \*\* Unknown  
**Description:** No Description Found
- **Event ID:** \*\* 1003  
**Timestamp:** \*\* Unknown  
**Source:** \*\* Unknown  
**Description:** No Description Found
- **Event ID:** \*\* 1003  
**Timestamp:** \*\* Unknown  
**Source:** \*\* Unknown  
**Description:** No Description Found
- **Event ID:** \*\* 8198  
**Timestamp:** \*\* Unknown  
**Source:** \*\* Unknown  
**Description:** No Description Found
- **Event ID:** \*\* 0  
**Timestamp:** \*\* Unknown  
**Source:** \*\* Unknown  
**Description:** No Description Found
- **Event ID:** \*\* 1026  
**Timestamp:** \*\* Unknown  
**Source:** \*\* Unknown  
**Description:** No Description Found
- **Event ID:** \*\* 1000  
**Timestamp:** \*\* Unknown  
**Source:** \*\* Unknown  
**Description:** No Description Found
- **Event ID:** \*\* 1001  
**Timestamp:** \*\* Unknown  
**Source:** \*\* Unknown

**Description:** No Description Found

- **Event ID:** \*\* 1001  
**Timestamp:** \*\* Unknown  
**Source:** \*\* Unknown  
**Description:** No Description Found
- **Event ID:** \*\* 256  
**Timestamp:** \*\* Unknown  
**Source:** \*\* Unknown  
**Description:** No Description Found

## **DNS Logs**

- **Event ID:** Unknown  
**Timestamp:** Unknown  
**Source:** Unknown  
**Description:** No Description Found
- **Event ID:** Unknown  
**Timestamp:** Unknown  
**Source:** Unknown  
**Description:** No Description Found
- **Event ID:** Unknown  
**Timestamp:** Unknown  
**Source:** Unknown  
**Description:** No Description Found
- **Event ID:** Unknown  
**Timestamp:** Unknown  
**Source:** Unknown  
**Description:** No Description Found
- **Event ID:** Unknown  
**Timestamp:** Unknown  
**Source:** Unknown  
**Description:** No Description Found
- **Event ID:** Unknown  
**Timestamp:** Unknown  
**Source:** Unknown  
**Description:** No Description Found

- **Event ID:** Unknown  
**Timestamp:** Unknown  
**Source:** Unknown  
**Description:** No Description Found
- **Event ID:** Unknown  
**Timestamp:** Unknown  
**Source:** Unknown  
**Description:** No Description Found
- **Event ID:** Unknown  
**Timestamp:** Unknown  
**Source:** Unknown  
**Description:** No Description Found
- **Event ID:** Unknown  
**Timestamp:** Unknown  
**Source:** Unknown  
**Description:** No Description Found
- **Event ID:** Unknown  
**Timestamp:** Unknown  
**Source:** Unknown  
**Description:** No Description Found
- **Event ID:** Unknown  
**Timestamp:** Unknown  
**Source:** Unknown  
**Description:** No Description Found
- **Event ID:** Unknown  
**Timestamp:** Unknown  
**Source:** Unknown  
**Description:** No Description Found
- **Event ID:** Unknown  
**Timestamp:** Unknown  
**Source:** Unknown  
**Description:** No Description Found
- **Event ID:** Unknown  
**Timestamp:** Unknown  
**Source:** Unknown  
**Description:** No Description Found
- **Event ID:** Unknown  
**Timestamp:** Unknown  
**Source:** Unknown

**Description:** No Description Found

- **Event ID:** Unknown  
**Timestamp:** Unknown  
**Source:** Unknown  
**Description:** No Description Found
- **Event ID:** Unknown  
**Timestamp:** Unknown  
**Source:** Unknown  
**Description:** No Description Found
- **Event ID:** Unknown  
**Timestamp:** Unknown  
**Source:** Unknown  
**Description:** No Description Found

--- END OF REPORT ---

This concludes the Cyber Security Audit Report.