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 (60 files/folders)
15	OS Install Date	2025-01-29
16	Domain	WORKGROUP
17	System Last Updated On	12 February 2025
18	Windows License Status	Notification Mode
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	192.168.0.154
24	Public IP Address	49.204.16.61
25	CPU Usage	5.8%
26	Memory Usage	32.5%

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	IP Address	192.168.0.154

Security Information

S.No	Parameter	Value
1	Timestamp	2025-03-11 19:36:11
2	Antivirus Installed	Antivirus Installed: Windows Defender
3	Last Windows Defender Scan Time	09 March 2025 12:35:31
4	USB Storage Device Access	USB Access: Allowed
5	AutoPlay Status	AutoPlay is Enabled
6	Remote Desktop Protocol (RDP)	Disabled (RDP is OFF)
7	Telnet	Not Installed
8	Default Share Status	Enabled (Security Risk)
9	Shared Folder Status	Not Configured (Safe)
10	Passwords not saved in web/system	Passwords Saved (See Credential Manager)
11	BIOS Password	BIOS Password May Be Set (Check BIOS Manually)
12	Windows Login Password	Windows Login Password Set (User: amaan)
13	Password Policy	Weak (Users can set empty passwords) Minimum password age (days): 0■ Maximum password age (days): 42■ Minimum password length: 0■ Length of password history maintained: None
14	System Lockout Policy	No System Lockout Policy (Accounts never lock) Lockout Threshold: Never Lockout Duration (minutes): 30 Lockout Observation Window (minutes): 30

Users Accounts

Administrator, amaan, DefaultAccount, Guest, WDAGUtilityAccount

Last Windows Update

- KB5049622 1/29/2025 - KB5051987 2/12/2025 - KB5052085 2/12/2025

Desktop Files

0etp4sa0nex91.png 2025-01-17 20-55-03.00_18_08_55.Still001.jpg 2025-01-17
20-55-03.00_18_25_08.Still002.jpg 2025-01-17 20-55-03.00_23_41_21.Still003.jpg 2025-01-26
06-33-23.00_00_21_28.Still002.jpg 360_F_319202173_IChFjDK92X4FwE7pbzfjFueIRrRjkJiL.jpg
360_F_567048053_ItaBMlfuV6sE583KnWeJuruJyPJbmg1D.jpg
3fec5bef-5280-49d3-b984-51d8ee044bbf.jpg 5fwolb04i2ae1.jpeg Adobe After Effects 2022.lnk 60

Security Logs

System Logs

Event[0] Log Name: System Source: EventLog Date: 2025-01-29T22:03:27.0860000Z Event ID: 6009
Task: None■ Level: Information■ Opcode: N/A Keyword: Classic,■ User: N/A User Name: N/A
Computer: JoeyTheDog Description: Microsoft (R) Windows (R) 10.00. 26100 Multiprocessor Free.■
Event[1] Log Name: System Source: EventLog Date: 2025-01-29T22:03:27.0860000Z Event ID: 6005
Task: None■ Level: Information■ Opcode: N/A Keyword: Classic,■ User: N/A User Name: N/A
Computer: JoeyTheDog Description: The Event log service was started.■ Event[2] Log Name: System
Source: EventLog Date: 2025-01-29T22:03:27.0870000Z Event ID: 6013 Task: None■ Level:
Information■ Opcode: N/A Keyword: Classic,■ User: N/A User Name: N/A Computer: JoeyTheDog
Description: The system uptime is 26 seconds.■ Event[3] Log Name: System Source:
Microsoft-Windows-Kernel-General Date: 2025-01-29T22:03:01.1350000Z Event ID: 12 Task: N/A
Level: Information■ Opcode: Info■■ Keyword: N/A User: S-1-5-18 User Name: NT
AUTHORITY\SYSTEM Computer: JoeyTheDog Description: The operating system started at system
time ?2025?-?01?-?29T16:33:00.500000000Z.■ Event[4] Log Name: System Source:
Microsoft-Windows-Kernel-General Date: 2025-01-29T22:03:01.1350000Z Event ID: 25 Task: N/A
Level: Information■ Opcode: Info■■ Keyword: Time,■ User: S-1-5-18 User Name: NT
AUTHORITY\SYSTEM Computer: JoeyTheDog Description: The system time was initialized to
?2025?-?01?-?29T16:33:00.500000000Z. Loader time: ?2025?-?01?-?29T16:32:59.000000000Z
Internal boot flags: 0x2 HAL RTC error code: 0x0 RTC time is in UTC: false Soft boot: false Success:
true Phase: 0■

Application Logs

Event[0] Log Name: Application Source: Microsoft-Windows-User Profiles Service Date: 2025-01-29T22:03:15.8650000Z Event ID: 1531 Task: N/A Level: Information■ Opcode: Info■■ Keyword: N/A User: S-1-5-18 User Name: NT AUTHORITY\SYSTEM Computer: JoeyTheDog Description: The User Profile Service has started successfully. ■ Event[1] Log Name: Application Source: Microsoft-Windows-WMI Date: 2025-01-29T22:03:21.6050000Z Event ID: 5615 Task: N/A Level: Information■ Opcode: Info■■ Keyword: N/A User: S-1-5-18 User Name: NT AUTHORITY\SYSTEM Computer: JoeyTheDog Description: Windows Management Instrumentation Service started sucessfully■ Event[2] Log Name: Application Source: Microsoft-Windows-WMI Date: 2025-01-29T22:03:21.8630000Z Event ID: 5617 Task: N/A Level: Information■ Opcode: Info■■ Keyword: N/A User: S-1-5-18 User Name: NT AUTHORITY\SYSTEM Computer: JoeyTheDog Description: Windows Management Instrumentation Service subsystems initialized successfully■ Event[3] Log Name: Application Source: Microsoft-Windows-WMI Date: 2025-01-29T22:03:22.0820000Z Event ID: 63 Task: N/A Level: Warning■ Opcode: Info■■ Keyword: N/A User: S-1-5-18 User Name: NT AUTHORITY\SYSTEM Computer: JoeyTheDog Description: A provider, Win32_OfflineFilesConfigurationProvider, has been registered in the Windows Management Instrumentation namespace ROOT\CIMV2 to use the LocalSystem account. This account is privileged and the provider may cause a security violation if it does not correctly impersonate user requests.■ Event[4] Log Name: Application Source: Microsoft-Windows-WMI Date: 2025-01-29T22:03:22.0870000Z Event ID: 63 Task: N/A Level: Warning■ Opcode: Info■■ Keyword: N/A User: S-1-5-18 User Name: NT AUTHORITY\SYSTEM Computer: JoeyTheDog Description: A provider, InvProv, has been registered in the Windows Management Instrumentation namespace ROOT\CIMV2 to use the LocalSystem account. This account is privileged and the provider may cause a security violation if it does not correctly impersonate user requests.■

DNS Logs

USB Logs