```
[*] Start Date/Time: 20240222T23133193+05
[*] Script running with Administrator rights.
[*] Dumping System Info to seperate file\n
[*] Windows Version: Microsoft Windows NT 10.0.22621.0
[*] Windows Default Path for LENOVO : C:\Program Files\Common
Files\Oracle\Java\javapath;C:\Program Files (x86)\VMware\VMware
Workstation\bin\;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;
C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Windows\System32\OpenSSH\;
C:\Users\LENOVO\AppData\Local\Programs\Python\Python312\Scripts\;C:\Users
\LENOVO\AppData\Local\Programs\Python\Python312\;C:\Users\LENOVO\AppData\
Local\Microsoft\WindowsApps;C:\Users\LENOVO\AppData\Local\Programs\Micros
oft VS Code\bin
[*] Host network interface assigned: 192.168.56.1
[*] Host network interface assigned: 192.168.142.1
[*] Host network interface assigned: 169.254.163.39
[*] Host network interface assigned: 169.254.58.64
[*] Host network interface assigned: 169.254.161.78
[*] Host network interface assigned: 192.168.43.103
[*] Checking IPv6 Network Settings
[-] Host IPv6 network interface assigned (gwmi): fe80::7e76:cf6:299c:1df5
[-] Host IPv6 network interface assigned (gwmi):
fe80::7204:2bb1:5dc5:d11b
[-] Host IPv6 network interface assigned (gwmi):
fe80::1c52:2a2b:de01:1582
[*] Checking Windows AutoUpdate Configuration
[+] Windows AutoUpdate is set to 4 : System.Collections.Hashtable.4
[*] Checking for missing Windows patches with Critical or Important
MsrcSeverity values. NOTE: This make take a few minutes.
[+] Windows system appears to be up-to-date for Critical and Important
patches.
[*] Checking BitLocker Encryption
[+] BitLocker detected and Operating System Volume is: FullyEncrypted
[*] Checking if users can install software as NT AUTHORITY\SYSTEM
[+] Users cannot install software as NT AUTHORITY\SYSTEM.
[*] Testing if PowerShell Commandline Audting is Enabled
[-] ProcessCreationIncludeCmdLine_Enabled Is Not Set
[*] Testing if PowerShell Moduling is Enabled
[-] EnableModuleLogging Is Not Set
[*] Testing if PowerShell EnableScriptBlockLogging is Enabled
[-] EnableScriptBlockLogging Is Not Set
[*] Testing if PowerShell EnableScriptBlockInvocationLogging is Enabled
[-] EnableScriptBlockInvocationLogging Is Not Set
[*] Testing if PowerShell EnableTranscripting is Enabled
[-] EnableTranscripting Is Not Set
[*] Testing if PowerShell EnableInvocationHeader is Enabled
[-] EnableInvocationHeader Is Not Set
[*] Testing if PowerShell ProtectedEventLogging is Enabled
[-] EnableProtectedEventLogging Is Not Set
[*] Event logs settings defaults are too small. Test that max sizes have
been increased.
[-] Microsoft-Windows-SMBServer/Audit max log size is smaller than
System.Collections.Hashtable[Microsoft-Windows-SMBServer/Audit] GB: 0.008
GB
[-] Security max log size is smaller than
System.Collections.Hashtable[Security] GB: 0.02 GB
[-] Microsoft-Windows-PowerShell/Operational max log size is smaller than
System.Collections.Hashtable[Microsoft-Windows-PowerShell/Operational]
GB: 0.015 GB
```

```
[-] Microsoft-Windows-TaskScheduler/Operational max log size is smaller
than System.Collections.Hashtable[Microsoft-Windows-
TaskScheduler/Operational] GB: 0.01 GB
[-] Microsoft-Windows-WinRM/Operational max log size is smaller than
System.Collections.Hashtable[Microsoft-Windows-WinRM/Operational] GB:
0.001 GB
[-] Microsoft-Windows-Security-Netlogon/Operational max log size is
smaller than System.Collections.Hashtable[Microsoft-Windows-Security-
Netlogon/Operational] GB: 0.001 GB
[-] Microsoft-Windows-WMI-Activity/Operational max log size is smaller
than System.Collections.Hashtable[Microsoft-Windows-WMI-
Activity/Operational] GB: 0.001 GB
[-] Windows PowerShell max log size is smaller than
System.Collections.Hashtable[Windows PowerShell] GB: 0.015 GB
[-] System max log size is smaller than
System.Collections.Hashtable[System] GB: 0.02 GB
[-] Application max log size is smaller than
System.Collections.Hashtable[Application] GB: 0.02 GB
[-] Microsoft-Windows-TerminalServices-LocalSessionManager/Operational
max log size is smaller than System.Collections.Hashtable[Microsoft-
Windows-TerminalServices-LocalSessionManager/Operational] GB: 0.001 GB
[*] Testing if PowerShell Version is at least version 5
[+] Current PowerShell Version: 5.1.22621.2506
[*] Testing if PowerShell Version 2 is permitted
[-] PowerShell Version 2 should be disabled: Enabled
[*] Testing if .NET Framework version supports PowerShell Version 2
[+] .NET Framework greater than 3.0 installed: 4.8.09032
[+] .NET Framework greater than 3.0 installed: 4.8.09032
[+] .NET Framework greater than 3.0 installed: 4.8.09032
[+] .NET Framework greater than 3.0 installed: 4.8.09032
[+] .NET Framework greater than 3.0 installed: 4.0.0.0
[*] Testing if PowerShell is configured to use Constrained Language.
[-] Execution Langugage Mode Is Not ConstrainedLanguage: FullLanguage
[*] Testing if system is configured to limit the number of stored
credentials.
[-] CachedLogonsCount Is Not Set to 0 or 1: 10
[*] Testing if system is configured to prevent RDP service.
[+] AllowRemoteRPC is set to deny RDP: 0
[*] Testing if system is configured to deny remote access via Terminal
Services.
[+] fDenyTSConnections is set to deny remote connections: 1
[*] Testing if WinFW Service is running.
[+] WinRM Services is not running: Get-Service check.
[*] Testing if Windows Network Firewall rules allow remote connections.
[+] WinRM Firewall Rule MSFT_NetFirewallRule (CreationClassName =
"MSFT?FW?FirewallRule?WINRM-HTTP-In-TCP", PolicyRuleName = "",
SystemCreationClassName = "", SystemName = "").Name is disabled.
[+] WinRM Firewall Rule MSFT_NetFirewallRule (CreationClassName =
"MSFT?FW?FirewallRule?WINRM-HTTP-In-TCP-..., PolicyRuleName = "",
SystemCreationClassName = "", SystemName = "").Name is disabled.
[*] Testing Local Administrator Accounts.
[-] More than one account is in local Administrators group: 2
[*] Account in local Administrator group: DESKTOP-0520P8I\Administrator
[*] Account in local Administrator group: DESKTOP-0520P8I\LENOVO
[*] Testing if AppLocker is configured.
[x] Testing for Microsoft AppLocker failed.
[*] EMET Service components are built into Windows 10.
[*] Testing if Local Administrator Password Solution (LAPS) is installed.
```

```
[x] Testing for Microsoft LAPS failed.
[*] Testing if Group Policy Objects.
[*] System may not be assigned GPOs.
[*] Testing Net Session Enumeration configuration using the TechNet
script NetSessEnumPerm.ps1
[*] Testing for WPAD entry in C:\Windows\System32\Drivers\etc\hosts
[-] No WPAD entry detected. Should contain: wpad 255.255.255.255
[*] Testing for WPADOverride registry key.
[*] System not configured with the WpadOverride registry key.
[*] Testing WinHttpAutoProxySvc configuration.
[-] WinHttpAutoProxySvc service is: Running
[*] Testing if KB3165191 is installed to harden WPAD by check
installation date.
[-] KB3165191 to harden WPAD is not installed.
[*] Testing if Network Adapters are configured to enable WINS Resolution:
DNSEnabledForWINSResolution
[-] DNSEnabledForWINSResolution is enabled
[*] Testing if Network Adapters are configured to enable WINS Resolution:
WINSEnableLMHostsLookup
[-] WINSEnableLMHostsLookup is enabled
[*] Testing if LLMNR is disabled.
[-] DNSClient.EnableMulticast does not exist or is enabled:
[*] Testing if Computer Browser service is disabled.
[-] Computer Browser service is: Running
[*] Testing if NetBios is disabled.
[x] Testing for NetBios failed.
[*] Testing if Windows Scripting Host (WSH) is disabled.
[-] WSH Setting Enabled key does not exist.
[*] Testing if security back-port patch KB2871997 is installed by check
installation date.
[-] KB2871997 is not installed.
[*] Testing if PowerShell LocalAccountTokenFilterPolicy in Policies is
Disabled
[+] LocalAccountTokenFilterPolicy Is Not Set
[*] Testing if PowerShell LocalAccountTokenFilterPolicy in Wow6432Node
Policies is Disabled
[+] LocalAccountTokenFilterPolicy in Wow6432Node Is Not Set
[-] WDigest UseLogonCredential key does not exist.
[*] Testing if SMBv1 is disabled.
[*] Testing if SMBv1 is disabled.
[-] SMBv1 is Enabled
[*] Testing if system is configured to audit SMBv1 activity.
[+] SMBv1 Auditing should be Enabled: Enabled
[*] Testing if Untrusted Fonts are disabled using the Kernel
MitigationOptions.
[-] Kernel MitigationOptions key does not exist.
[*] Testing for Credential Guard.
[x] Testing for Credential Guard failed.
[*] Testing for Device Guard.
[x] Testing for Device Guard failed.
[*] Testing Lanman Authentication for NoLmHash registry key.
[+] NoLmHash registry key is configured: 1
[*] Testing Lanman Authentication for LM Compatability Level registry
key.
[-] LM Compatability Level registry key is not configured.
[*] Testing Domain and Local Anonymous Enumeration settings:
RestrictAnonymous.
[-] RestrictAnonymous registry key is not configured: 0
```

```
[*] Testing Domain and Local Anonymous Enumeration settings:
RestrictAnonymoussam
[+] RestrictAnonymoussam registry key is configured: 1
[*] Testing Restrict RPC Clients settings.
[-] RestrictRemoteClients registry key is not configured:
[*] Testing NTLM Session Server Security settings.
[-] NTLM Session Server Security settings is not configured to require
NTLMv2 and 128-bit encryption: 536870912
[*] Testing NTLM Session Client Security settings.
[-] NTLM Session Client Security settings is not configured to require
NTLMv2 and 128-bit encryption: 536870912
[*] Completed Date/Time: 20240222T23141051+05
```