```
[*] 20/08/2025 16:11:09 - Starting HardeningKitty
[*] 20/08/2025 16:11:09 - Getting machine information
[*] Hostname: TFM-VM-S2
[*] Domain: WORKGROUP
[*] Domain role: StandaloneServer
[*] Install date: 07/09/2025 15:10:39
[*] Last Boot Time: 08/20/2025 16:04:01
[*] Uptime: 00:07:08.4927875
[*] Windows: Microsoft Windows Server 2022 Standard Evaluation
[*] Windows edition: ServerStandardEval
[*] Windows version: 2009
[*] Windows build: 20348.1.amd64fre.fe_release.210507-1500
[*] System-locale: es-ES
[*] Powershell Version: 5.1
[*] 20/08/2025 16:11:12 - Language warning
[?] 20/08/2025 16:11:12 - HardeningKitty was developed for the system language 'en-US'. This system uses 'es-ES'
Language-dependent analyses can sometimes produce false results. Please create an issue if this occurs.
[*] 20/08/2025 16:11:12 - Getting user information
[*] Username: TFM-VM-S2\SecureAdmin
[*] Is Admin: True
[*] 20/08/2025 16:11:12 - Starting Category Features
ID 1000, SMBv1 Support, Result=Disabled, Recommended=Disabled, Severity=Passed
[*] 20/08/2025 16:11:13 - Starting Category Account Policies
ID 1103, Store passwords using reversible encryption, Result=0, Recommended=0, Severity=Passed
ID 1101, Account lockout duration, Result=30, Recommended=15, Severity=Passed
ID 1100, Account lockout threshold, Result=5, Recommended=10, Severity=Passed
ID 1104, Allow Administrator account lockout, Result=0, Recommended=1, Severity=Medium
ID 1102, Reset account lockout counter, Result=15, Recommended=15, Severity=Passed
[*] 20/08/2025 16:11:13 - Starting Category User Rights Assignment
ID 1200, Access this computer from the network, Result=Todos;BUILTIN\Administradores;BUILTIN\Usuarios;BUILTIN\Operadores
de copia de seguridad, Recommended=BUILTIN\Administrators, Severity=Medium
ID 1201, Allow log on locally, Result=BUILTIN\Administradores;BUILTIN\Usuarios;BUILTIN\Operadores de copia de seguridad,
Recommended=BUILTIN\Users;BUILTIN\Administrators, Severity=Medium
ID 1202, Debug programs, Result=BUILTIN\Administradores, Recommended=, Severity=Medium
ID 1203, Deny access to this computer from the network, Result=, Recommended=BUILTIN\Guests;NT AUTHORITY\Local account,
Severity=Medium
ID 1204, Deny log on as a batch job, Result=, Recommended=BUILTIN\Guests, Severity=Medium
ID 1205, Deny log on as a service, Result=, Recommended=BUILTIN\Guests, Severity=Medium
ID 1206, Deny log on through Remote Desktop Services, Result=, Recommended=BUILTIN\Guests;NT AUTHORITY\Local account,
Severity=Medium
[*] 20/08/2025 16:11:14 - Starting Category Security Options
ID 1300, Accounts: Block Microsoft accounts, Result=0, Recommended=3, Severity=Low
```

```
ID 1301, Audit: Force audit policy subcategory settings to override audit policy category settings, Result=1,
Recommended=1, Severity=Passed
ID 1302, Interactive logon: Do not require CTRL+ALT+DEL, Result=0, Recommended=0, Severity=Passed
ID 1303, Interactive logon: Don't display last signed-in, Result=0, Recommended=1, Severity=Low
ID 1304, Interactive logon: Don't display username at sign-in, Result=0, Recommended=1, Severity=Low
ID 1305, Microsoft network client: Digitally sign communications (always), Result=0, Recommended=1, Severity=Medium
ID 1306, Microsoft network client: Digitally sign communications (if server agrees), Result=1, Recommended=1,
Severity=Passed
ID 1307, Microsoft network server: Digitally sign communications (always), Result=0, Recommended=1, Severity=Medium
ID 1308, Microsoft network server: Digitally sign communications (if client agrees), Result=0, Recommended=1,
Severity=Medium
ID 1309, Network access: Do not allow anonymous enumeration of SAM accounts, Result=1, Recommended=1, Severity=Passed
ID 1310, Network access: Do not allow anonymous enumeration of SAM accounts and shares, Result=1, Recommended=1,
Severity=Passed
ID 1311, Network access: Do not allow storage of passwords and credentials for network authentication, Result=0,
Recommended=1, Severity=Medium
ID 1324, Network access: Restrict anonymous access to Named Pipes and Shares, Result=1, Recommended=1, Severity=Passed
ID 1325, Network access: Restrict clients allowed to make remote calls to SAM, Result=, Recommended=O:BAG:BAD:
(A;;RC;;;BA), Severity=Medium
ID 1312, Network security: Allow LocalSystem NULL session fallback, Result=0, Recommended=0, Severity=Passed
ID 1326, Network security: Do not store LAN Manager hash value on next password change, Result=1, Recommended=1,
Severity=Passed
ID 1313, Network security: LAN Manager authentication level, Result=5, Recommended=5, Severity=Passed
ID 1314, Network security: LDAP client signing requirements, Result=1, Recommended=1, Severity=Passed
ID 1315, Network security: Minimum session security for NTLM SSP based (including secure RPC) clients, Result=536870912,
Recommended=537395200, Severity=Medium
ID 1316, Network security: Minimum session security for NTLM SSP based (including secure RPC) servers, Result=536870912,
Recommended=537395200, Severity=Medium
ID 1317, Network security: Restrict NTLM: Audit Incoming NTLM Traffic, Result=0, Recommended=2, Severity=Medium
ID 1318, Network security: Restrict NTLM: Audit NTLM authentication in this domain, Result=0, Recommended=7,
Severity=Medium
ID 1319, Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers, Result=0, Recommended=1,
Severity=Medium
ID 1320, Shutdown: Allow system to be shut down without having to log on, Result=0, Recommended=0, Severity=Passed
ID 1321, User Account Control: Admin Approval Mode for the Built-in Administrator account, Result=0, Recommended=1,
Severity=Medium
ID 1322, User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode, Result=2,
Recommended=2, Severity=Passed
ID 1323, User Account Control: Behavior of the elevation prompt for standard users, Result=3, Recommended=1,
Severity=Medium
[*] 20/08/2025 16:11:15 - Starting Category Windows Firewall
ID 1400, EnableFirewall (Domain Profile, Policy), Result=0, Recommended=1, Severity=Medium
ID 1418, EnableFirewall (Domain Profile), Result=1, Recommended=1, Severity=Passed
```

```
ID 1401, Inbound Connections (Domain Profile, Policy), Result=1, Recommended=1, Severity=Passed
ID 1419, Inbound Connections (Domain Profile), Result=1, Recommended=1, Severity=Passed
ID 1402, Outbound Connections (Domain Profile, Policy), Result=0, Recommended=0, Severity=Passed
ID 1420, Outbound Connections (Domain Profile), Result=0, Recommended=0, Severity=Passed
ID 1403, Log size limit (Domain Profile, Policy), Result=4096, Recommended=16384, Severity=Medium
ID 1421, Log size limit (Domain Profile), Result=32767, Recommended=16384, Severity=Passed
ID 1404, Log dropped packets (Domain Profile, Policy), Result=0, Recommended=1, Severity=Medium
ID 1422, Log dropped packets (Domain Profile), Result=1, Recommended=1, Severity=Passed
ID 1405, Log successful connections (Domain Profile, Policy), Result=0, Recommended=1, Severity=Low
ID 1423, Log successful connections (Domain Profile), Result=1, Recommended=1, Severity=Passed
ID 1406, EnableFirewall (Private Profile, Policy), Result=0, Recommended=1, Severity=Medium
ID 1424, EnableFirewall (Private Profile), Result=1, Recommended=1, Severity=Passed
ID 1407, Inbound Connections (Private Profile, Policy), Result=1, Recommended=1, Severity=Passed
ID 1425, Inbound Connections (Private Profile), Result=1, Recommended=1, Severity=Passed
ID 1408, Outbound Connections (Private Profile, Policy), Result=0, Recommended=0, Severity=Passed
ID 1426, Outbound Connections (Private Profile), Result=0, Recommended=0, Severity=Passed
ID 1409, Log size limit (Private Profile, Policy), Result=4096, Recommended=16384, Severity=Medium
ID 1427, Log size limit (Private Profile), Result=32767, Recommended=16384, Severity=Passed
ID 1410, Log dropped packets (Private Profile, Policy), Result=0, Recommended=1, Severity=Medium
ID 1428, Log dropped packets (Private Profile), Result=1, Recommended=1, Severity=Passed
ID 1411, Log successful connections (Private Profile, Policy), Result=0, Recommended=1, Severity=Low
ID 1429, Log successful connections (Private Profile), Result=1, Recommended=1, Severity=Passed
ID 1412, EnableFirewall (Public Profile, Policy), Result=0, Recommended=1, Severity=Medium
ID 1430, EnableFirewall (Public Profile), Result=1, Recommended=1, Severity=Passed
ID 1413, Inbound Connections (Public Profile, Policy), Result=1, Recommended=1, Severity=Passed
ID 1431, Inbound Connections (Public Profile), Result=1, Recommended=1, Severity=Passed
ID 1414, Outbound Connections (Public Profile, Policy), Result=0, Recommended=0, Severity=Passed
ID 1432, Outbound Connections (Public Profile), Result=0, Recommended=0, Severity=Passed
ID 1415, Log size limit (Public Profile, Policy), Result=4096, Recommended=16384, Severity=Medium
ID 1433, Log size limit (Public Profile), Result=32767, Recommended=16384, Severity=Passed
ID 1416, Log dropped packets (Public Profile, Policy), Result=0, Recommended=1, Severity=Medium
ID 1434, Log dropped packets (Public Profile), Result=1, Recommended=1, Severity=Passed
ID 1417, Log successful connections (Public Profile, Policy), Result=0, Recommended=1, Severity=Low
ID 1435, Log successful connections (Public Profile), Result=1, Recommended=1, Severity=Passed
[*] 20/08/2025 16:11:15 - Starting Category Advanced Audit Policy Configuration
ID 1500, Credential Validation, Result=Success and Failure, Recommended=Success and Failure, Severity=Passed
ID 1501, Security Group Management, Result=Success and Failure, Recommended=Success, Severity=Passed
ID 1502, User Account Management, Result=Success and Failure, Recommended=Success and Failure, Severity=Passed
ID 1503, DPAPI Activity, Result=Success and Failure, Recommended=Success and Failure, Severity=Passed
ID 1504, Plug and Play Events, Result=Success and Failure, Recommended=Success, Severity=Passed
ID 1505, Process Creation, Result=Success and Failure, Recommended=Success, Severity=Passed
ID 1506, Account Lockout, Result=Success and Failure, Recommended=Failure, Severity=Passed
ID 1507, Group Membership, Result=Success and Failure, Recommended=Success, Severity=Passed
```

```
ID 1508, Logon, Result=Success and Failure, Recommended=Success and Failure, Severity=Passed
ID 1509, Other Logon/Logoff Events, Result=Success and Failure, Recommended=Success and Failure, Severity=Passed
ID 1510, Special Logon, Result=Success and Failure, Recommended=Success, Severity=Passed
ID 1511, Detailed File Share, Result=Success and Failure, Recommended=Failure, Severity=Passed
ID 1512, File Share, Result=Success and Failure, Recommended=Success and Failure, Severity=Passed
ID 1513, Kernel Object, Result=Success and Failure, Recommended=Success and Failure, Severity=Passed
ID 1514, Other Object Access Events, Result=Success and Failure, Recommended=Success and Failure, Severity=Passed
ID 1515, Removable Storage, Result=Success and Failure, Recommended=Success and Failure, Severity=Passed
ID 1516, SAM, Result=Success and Failure, Recommended=Success and Failure, Severity=Passed
ID 1517, Audit Policy Change, Result=Success and Failure, Recommended=Success, Severity=Passed
ID 1518, Authentication Policy Change, Result=Success and Failure, Recommended=Success, Severity=Passed
ID 1519, MPSSVC Rule-Level Policy Change, Result=Success and Failure, Recommended=Success and Failure, Severity=Passed
ID 1520, Other Policy Change Events, Result=Success and Failure, Recommended=Failure, Severity=Passed
ID 1521, Sensitive Privilege Use, Result=Success and Failure, Recommended=Success and Failure, Severity=Passed
ID 1522, Other System Events, Result=Success and Failure, Recommended=Success and Failure, Severity=Passed
ID 1523, Security State Change, Result=Success and Failure, Recommended=Success, Severity=Passed
ID 1524, Security System Extension, Result=Success and Failure, Recommended=Success, Severity=Passed
ID 1525, System Integrity, Result=Success and Failure, Recommended=Success and Failure, Severity=Passed
[*] 20/08/2025 16:11:16 - Starting Category Administrative Templates: Control Panel
ID 1600, Personalization: Prevent enabling lock screen camera, Result=0, Recommended=1, Severity=Low
[*] 20/08/2025 16:11:16 - Starting Category Administrative Templates: Network
ID 1601, DNS Client: Turn off multicast name resolution (LLMNR), Result=1, Recommended=0, Severity=Medium
ID 1602, Lanman Workstation: Enable insecure guest logons, Result=1, Recommended=0, Severity=Medium
ID 1603, Turn off Microsoft Peer-to-Peer Networking Services, Result=0, Recommended=1, Severity=Medium
ID 1604, WLAN Settings: Allow Windows to automatically connect to suggested open hotspots, to networks shared by
contacts, and to hotspots offering paid services, Result=1, Recommended=0, Severity=Medium
[*] 20/08/2025 16:11:16 - Starting Category Administrative Templates: PowerShellCore
ID 2108, Turn on PowerShell Module Logging, Result=0, Recommended=1, Severity=Low
ID 2109, Turn on PowerShell Module Logging (PowerShell Policy), Result=0, Recommended=1, Severity=Low
ID 2110, Turn on PowerShell Module Logging - Module Names, Result=, Recommended=*, Severity=Low
ID 2111, Turn on PowerShell Script Block Logging, Result=0, Recommended=1, Severity=Medium
ID 2112, Turn on PowerShell Script Block Logging (Invocation), Result=0, Recommended=1, Severity=Low
ID 2113, Turn on PowerShell Script Block Logging (PowerShell Policy), Result=0, Recommended=1, Severity=Low
ID 2116, Turn on PowerShell Transcription, Result=0, Recommended=1, Severity=Low
ID 2114, Turn on PowerShell Transcription (Invocation), Result=0, Recommended=1, Severity=Low
ID 2115, Turn on PowerShell Transcription (PowerShell Policy), Result=0, Recommended=1, Severity=Medium
[*] 20/08/2025 16:11:16 - Starting Category Administrative Templates: Printers
ID 1772, Configure Redirection Guard, Result=, Recommended=1, Severity=Medium
ID 1768, Only use Package Point and Print (CVE-2021-36958), Result=, Recommended=1, Severity=Medium
ID 1769, Package Point and Print - Approved servers (CVE-2021-36958), Result=, Recommended=1, Severity=Medium
ID 1764, Point and Print Restrictions: When installing drivers for a new connection (CVE-2021-34527), Result=0,
Recommended=0, Severity=Passed
```

ID 1765, Point and Print Restrictions: When updating drivers for an existing connection (CVE-2021-34527), Result=0, Recommended=0, Severity=Passed
[*] 20/08/2025 16:11:16 - Starting Category Administrative Templates: Start Menu and Taskbar
ID 1771, Notifications: Turn off notifications network usage, Result=0, Recommended=1, Severity=Medium
[*] 20/08/2025 16:11:16 - Starting Category Administrative Templates: System
ID 1605, Credentials Delegation: Allow delegation default credentials, Result=1, Recommended=0, Severity=Medium
ID 1606, Credentials Delegation: Encryption Oracle Remediation, Result=0, Recommended=0, Severity=Passed
ID 1699, Credentials Delegation: Remote host allows delegation of non-exportable credentials, Result=0, Recommended=1, Severity=Medium
ID 1607, Device Installation: Device Installation Restrictions: Prevent installation of devices that match an ID, Result=0, Recommended=1, Severity=Medium
ID 1608, Device Installation: Device Installation Restrictions: Prevent installation of devices that match an ID (Retroactive), Result=0, Recommended=1, Severity=Medium
ID 1609, Device Installation: Device Installation Restrictions: Prevent installation of devices that match ID PCI\CC_0C0010 (Firewire), Result=0, Recommended=PCI\CC_0C0010, Severity=Medium
ID 1610, Device Installation: Device Installation Restrictions: Prevent installation of devices that match ID PCI\CC_0C0A (Thunderbolt), Result=0, Recommended=PCI\CC_0C0A, Severity=Medium
ID 1611, Device Installation: Device Installation Restrictions: Prevent installation of devices using drivers that match an device setup class, Result=0, Recommended=1, Severity=Medium
ID 1612, Device Installation: Device Installation Restrictions: Prevent installation of devices using drivers that match an device setup class (Retroactive), Result=0, Recommended=1, Severity=Medium
ID 1613, Device Installation: Device Installation Restrictions: Prevent installation of devices using drivers that match d48179be-ec20-11d1-b6b8-00c04fa372a7 (SBP-2 drive), Result=0, Recommended=d48179be-ec20-11d1-b6b8-00c04fa372a7, Severity=Medium
ID 1614, Device Guard: Virtualization Based Security Status, Result=Not available, Recommended=2, Severity=Medium
ID 1615, Device Guard: Available Security Properties: Secure Boot, Result=2, Recommended=2, Severity=Passed
ID 1616, Device Guard: Available Security Properties: DMA protection, Result=Not available, Recommended=3, Severity=Medium
ID 1617, Device Guard: Security Services Configured: Credential Guard, Result=Not available, Recommended=1, Severity=Medium
ID 1619, Device Guard: Security Services Running: Credential Guard, Result=Not available, Recommended=1, Severity=Medium
ID 1618, Device Guard: Security Services Configured: HVCI, Result=Not available, Recommended=2, Severity=Medium
ID 1620, Device Guard: Security Services Running: HVCI, Result=Not available, Recommended=2, Severity=Medium
ID 1623, Device Guard: Require UEFI Memory Attributes Table (Policy), Result=, Recommended=1, Severity=Medium
ID 1621, Device Guard: Secure Launch Configuration (Policy), Result=0, Recommended=1, Severity=Medium
ID 1622, Device Guard: Windows Defender Application Control deployed (Policy), Result=0, Recommended=1, Severity=Medium
ID 1630, Early Launch Antimalware: Boot-Start Driver Initialization Policy, Result=0, Recommended=3, Severity=Medium
ID 1631, Group Policy: Process even if the Group Policy objects have not changed, Result=1, Recommended=0, Severity=Low
ID 1632, Group Policy: Do not apply during periodic background processing, Result=0, Recommended=0, Severity=Passed
ID 1640, Internet Communication Management: Internet Communication settings: Turn off the Windows Messenger Customer Experience Improvement Program, Result=0, Recommended=2, Severity=Medium
ID 1641, Internet Communication Management: Internet Communication settings: Turn off downloading of print drivers over HTTP, Result=0, Recommended=1, Severity=Medium

ID 1642, Internet Communication Management: Internet Communication settings: Turn off Windows Error Reporting 1, Result=1, Recommended=0, Severity=Medium
ID 1643, Internet Communication Management: Internet Communication settings: Turn off Windows Error Reporting 2, Result=0, Recommended=1, Severity=Medium
ID 1644, Internet Communication Management: Internet Communication settings: Turn off Internet download for Web publishing and online ordering wizards, Result=0, Recommended=1, Severity=Medium
ID 1645, Internet Communication Management: Internet Communication settings: Turn off Windows Customer Experience Improvement Program, Result=1, Recommended=0, Severity=Medium
ID 1650, Kernel DMA Protection: Enumeration policy for external devices incompatible with Kernel DMA Protection, Result=2, Recommended=0, Severity=Medium
ID 1660, Logon: Turn on convenience PIN sign-in, Result=1, Recommended=0, Severity=Medium
ID 1661, Logon: Turn off app notifications on the lock screen, Result=0, Recommended=1, Severity=Medium
ID 1662, Logon: Do not display network selection UI, Result=0, Recommended=1, Severity=Medium
ID 1670, Mitigation Options: Untrusted Font Blocking, Result=0, Recommended=1000000000000, Severity=Medium
ID 1680, OS Policies: Allow Clipboard synchronization across devices, Result=1, Recommended=0, Severity=Medium
ID 1685, Sleep Settings: Require a password when a computer wakes (plugged in), Result=0, Recommended=1, Severity=Medium
ID 1686, Sleep Settings: Require a password when a computer wakes (on battery), Result=0, Recommended=1, Severity=Medium
ID 1687, Sleep Settings: Allow standby states (S1-S3) when sleeping (plugged in), Result=1, Recommended=0, Severity=Medium
ID 1688, Sleep Settings: Allow standby states (S1-S3) when sleeping (on battery), Result=1, Recommended=0, Severity=Medium
ID 1690, Remote Assistance: Configure Offer Remote Assistance, Result=1, Recommended=0, Severity=Medium
ID 1691, Remote Assistance: Configure Solicited Remote Assistance, Result=1, Recommended=0, Severity=Medium
ID 1692, Remote Procedure Call: Enable RPC Endpoint Mapper Client Authentication, Result=0, Recommended=1, Severity=Medium
ID 1693, Remote Procedure Call: Restrict Unauthenticated RPC clients, Result=0, Recommended=2, Severity=Medium
ID 1694, Security Settings: Enable svchost.exe mitigation options, Result=0, Recommended=1, Severity=Medium
ID 1695, Windows Performance PerfTrack: Enable/Disable PerfTrack, Result=1, Recommended=0, Severity=Medium
ID 1696, User Profiles: Turn off the advertising ID, Result=0, Recommended=1, Severity=Medium
ID 1697, Time Providers: Enable Windows NTP Client, Result=0, Recommended=1, Severity=Medium
ID 1698, Time Providers: Enable Windows NTP Server, Result=0, Recommended=0, Severity=Passed
[*] 20/08/2025 16:11:18 - Starting Category Administrative Templates: Windows Components
ID 1700, App Package Deployment: Allow a Windows app to share application data between users, Result=1, Recommended=0, Severity=Medium
ID 1701, App Privacy: Let Windows apps activate with voice while the system is locked, Result=0, Recommended=2, Severity=Medium
ID 1702, App runtime: Block launching Universal Windows apps with Windows Runtime API access from hosted content, Result=0, Recommended=1, Severity=Medium
ID 1703, Application Compatibility: Turn off Application Telemetry, Result=1, Recommended=0, Severity=Medium
ID 1704, AutoPlay Policies: Turn off Autoplay, Result=255, Recommended=255, Severity=Passed
ID 1705, AutoPlay Policies: Disallow Autoplay for non-volume devices, Result=0, Recommended=1, Severity=Medium
ID 1706, AutoPlay Policies: Set the default behavior for AutoRun, Result=1, Recommended=1, Severity=Passed
ID 1707, Biometrics: Allow the use of biometrics, Result=1, Recommended=0, Severity=Medium

ID 1773, Biometrics: Facial Features: Configure enhanced anti-spoofing, Result=, Recommended=1, Severity=Medium
ID 1708, BitLocker Drive Encryption: Volume status, Result=FullyEncrypted, Recommended=FullyEncrypted, Severity=Passed
ID 1761, BitLocker Drive Encryption: Choose drive encryption method and cipher strength (for operating system drives), Result=6, Recommended=6, Severity=Passed
ID 1762, BitLocker Drive Encryption: Drive encryption method (for operating system drives), Result=XtsAes256, Recommended=XtsAes128, Severity=Medium
ID 1709, BitLocker Drive Encryption: Disable new DMA devices when this computer is locked, Result=0, Recommended=1, Severity=Medium
ID 1710, BitLocker Drive Encryption: Operating System Drives: Allow Secure Boot for integrity validation, Result=0, Recommended=1, Severity=Medium
ID 1711, BitLocker Drive Encryption: Operating System Drives: Require additional authentication at startup, Result=0, Recommended=1, Severity=Medium
ID 1715, BitLocker Drive Encryption: Operating System Drives: Require additional authentication at startup: Allow BitLocker without a compatible TPM, Result=1, Recommended=0, Severity=Medium
ID 1716, BitLocker Drive Encryption: Operating System Drives: Require additional authentication at startup: Configure TPM startup, Result=0, Recommended=0, Severity=Passed
ID 1717, BitLocker Drive Encryption: Operating System Drives: Require additional authentication at startup: Configure TPM startup PIN, Result=0, Recommended=1, Severity=Medium
ID 1718, BitLocker Drive Encryption: Operating System Drives: Require additional authentication at startup: Configure TPM startup key, Result=0, Recommended=0, Severity=Passed
ID 1719, BitLocker Drive Encryption: Operating System Drives: Require additional authentication at startup: Configure TPM startup key and PIN, Result=0, Recommended=0, Severity=Passed
ID 1712, BitLocker Drive Encryption: Operating System Drives: Allow enhanced PINs for startup, Result=0, Recommended=1, Severity=Medium
ID 1713, BitLocker Drive Encryption: Operating System Drives: Configure use of hardware-based encryption for operating system drives, Result=0, Recommended=0, Severity=Passed
ID 1763, BitLocker Drive Encryption: Operating System Drives: Configure minimum PIN length for startup, Result=, Recommended=8, Severity=Medium
ID 1720, Cloud Content: Do not show Windows tips, Result=0, Recommended=1, Severity=Medium
ID 1721, Cloud Content: Turn off Microsoft consumer experiences, Result=0, Recommended=1, Severity=Medium
ID 1722, Credential User Interface: Do not display the password reveal button, Result=0, Recommended=1, Severity=Medium
ID 1724, Credential User Interface: Enumerate administrator accounts on elevation, Result=1, Recommended=0, Severity=Medium
ID 1725, Data Collection and Preview Builds: Allow Diagnostic Data, Result=2, Recommended=1, Severity=Medium
ID 1726, Data Collection and Preview Builds: Allow device name to be sent in Windows diagnostic data, Result=1, Recommended=0, Severity=Medium
ID 1727, Delivery Optimization: Download Mode, Result=1, Recommended=99, Severity=Medium
ID 1728, Event Log Service: Application: Specify the maximum log file size (KB), Result=4096, Recommended=32768, Severity=Medium
ID 1729, Event Log Service: Security: Specify the maximum log file size (KB), Result=4096, Recommended=196608, Severity=Medium
ID 1730, Event Log Service: System: Specify the maximum log file size (KB), Result=4096, Recommended=32768, Severity=Medium

```
ID 1774, Event Log Service: Microsoft-Windows-PowerShell/Operational: Specify the maximum log file size (KB),
Result=15728640, Recommended=268435456, Severity=Medium
ID 1775, Event Log Service: PowerShellCore/Operational: Specify the maximum log file size (KB), Result=15728640,
Recommended=268435456, Severity=Medium
ID 1731, File Explorer: Allow the use of remote paths in file shortcut icons, Result=0, Recommended=0, Severity=Passed
ID 1732, HomeGroup: Prevent the computer from joining a homegroup, Result=0, Recommended=1, Severity=Medium
[*] 20/08/2025 16:11:21 - Starting Category Microsoft Defender Antivirus
ID 1800, Turn off Microsoft Defender Antivirus, Result=0, Recommended=0, Severity=Passed
ID 1826, Enable Tamper Protection (Status), Result=False, Recommended=True, Severity=Medium
ID 1801, Configure detection for potentially unwanted applications, Result=0, Recommended=1, Severity=Medium
ID 1806, Exclusions: Extension Exclusions (Policy), Result=, Recommended=, Severity=Passed
ID 1813, Exclusions: Extension Exclusions (Intune), Result=, Recommended=, Severity=Passed
ID 1807, Exclusions: Extension Exclusions, Result=, Recommended=, Severity=Passed
ID 1808, Exclusions: Path Exclusions (Policy), Result=, Recommended=, Severity=Passed
ID 1814, Exclusions: Path Exclusions (Intune), Result=, Recommended=, Severity=Passed
ID 1809, Exclusions: Path Exclusions, Result=, Recommended=, Severity=Passed
ID 1810, Exclusions: Process Exclusions (Policy), Result=, Recommended=, Severity=Passed
ID 1815, Exclusions: Process Exclusions (Intune), Result=, Recommended=, Severity=Passed
ID 1811, Exclusions: Process Exclusions, Result=, Recommended=, Severity=Passed
ID 1816, MAPS: Join Microsoft MAPS, Result=0, Recommended=2, Severity=Medium
ID 1817, MAPS: Configure the 'Block at First Sight' feature, Result=, Recommended=0, Severity=Medium
ID 1818, MAPS: Send file samples when further analysis is required, Result=, Recommended=0, Severity=Medium
ID 1819, MpEngine: Enable file hash computation feature, Result=, Recommended=1, Severity=Medium
ID 1820, MpEngine: Select cloud protection level, Result=0, Recommended=2, Severity=Medium
ID 1821, Real-time Protection: Scan all downloaded files and attachments, Result=0, Recommended=0, Severity=Passed
ID 1822, Real-time Protection: Turn off real-time protection, Result=0, Recommended=0, Severity=Passed
ID 1823, Real-time Protection: Turn on behavior monitoring (Policy), Result=0, Recommended=0, Severity=Passed
ID 1824, Real-time Protection: Turn on script scanning, Result=0, Recommended=0, Severity=Passed
ID 1825, Scan: Scan removable drives, Result=1, Recommended=0, Severity=Medium
ID 1812, Enable sandboxing for Microsoft Defender Antivirus, Result=0, Recommended=1, Severity=Medium
[*] 20/08/2025 16:11:23 - Starting Category Microsoft Defender Exploit Guard
ID 1900, Attack Surface Reduction rules, Result=0, Recommended=1, Severity=Medium
ID 1901, ASR: Block executable content from email client and webmail (Policy), Result=0, Recommended=1, Severity=Medium
ID 1916, ASR: Block executable content from email client and webmail, Result=0, Recommended=1, Severity=Medium
ID 1933, ASR: Block executable content from email client and webmail (Intune), Result=0, Recommended=1, Severity=Medium
ID 1902, ASR: Block all Office applications from creating child processes (Policy), Result=0, Recommended=1,
Severity=Medium
ID 1917, ASR: Block all Office applications from creating child processes, Result=0, Recommended=1, Severity=Medium
ID 1934, ASR: Block all Office applications from creating child processes (Intune), Result=0, Recommended=1,
Severity=Medium
ID 1903, ASR: Block Office applications from creating executable content (Policy), Result=0, Recommended=1,
Severity=Medium
ID 1918, ASR: Block Office applications from creating executable content, Result=0, Recommended=1, Severity=Medium
```

ID 1935, ASR: Block Office applications from creating executable content (Intune), Result=0, Recommended=1, Severity=Medium
ID 1904, ASR: Block Office applications from injecting code into other processes (Policy), Result=0, Recommended=1, Severity=Medium
ID 1919, ASR: Block Office applications from injecting code into other processes, Result=0, Recommended=1, Severity=Medium
ID 1936, ASR: Block Office applications from injecting code into other processes (Intune), Result=0, Recommended=1, Severity=Medium
ID 1905, ASR: Block JavaScript or VBScript from launching downloaded executable content (Policy), Result=0, Recommended=1, Severity=Medium
ID 1920, ASR: Block JavaScript or VBScript from launching downloaded executable content, Result=0, Recommended=1, Severity=Medium
ID 1937, ASR: Block JavaScript or VBScript from launching downloaded executable content (Intune), Result=0, Recommended=1, Severity=Medium
ID 1906, ASR: Block execution of potentially obfuscated scripts (Policy), Result=0, Recommended=1, Severity=Medium
ID 1921, ASR: Block execution of potentially obfuscated scripts, Result=0, Recommended=1, Severity=Medium
ID 1938, ASR: Block execution of potentially obfuscated scripts (Intune), Result=0, Recommended=1, Severity=Medium
ID 1907, ASR: Block Win32 API calls from Office macros (Policy), Result=0, Recommended=1, Severity=Medium
ID 1922, ASR: Block Win32 API calls from Office macros, Result=0, Recommended=1, Severity=Medium
ID 1939, ASR: Block Win32 API calls from Office macros (Intune), Result=0, Recommended=1, Severity=Medium
ID 1908, ASR: Block executable files from running unless they meet a prevalence, age, or trusted list criterion (Policy), Result=0, Recommended=1, Severity=Medium
ID 1923, ASR: Block executable files from running unless they meet a prevalence, age, or trusted list criterion, Result=0, Recommended=1, Severity=Medium
ID 1940, ASR: Block executable files from running unless they meet a prevalence, age, or trusted list criterion (Intune), Result=0, Recommended=1, Severity=Medium
ID 1909, ASR: Use advanced protection against ransomware (Policy), Result=0, Recommended=1, Severity=Medium
ID 1924, ASR: Use advanced protection against ransomware, Result=0, Recommended=1, Severity=Medium
ID 1941, ASR: Use advanced protection against ransomware (Intune), Result=0, Recommended=1, Severity=Medium
ID 1910, ASR: Block credential stealing from the Windows local security authority subsystem (lsass.exe) (Policy), Result=0, Recommended=1, Severity=Medium
ID 1925, ASR: Block credential stealing from the Windows local security authority subsystem (lsass.exe), Result=0, Recommended=1, Severity=Medium
ID 1942, ASR: Block credential stealing from the Windows local security authority subsystem (lsass.exe) (Intune), Result=0, Recommended=1, Severity=Medium
ID 1911, ASR: Block process creations originating from PSExec and WMI commands (Policy), Result=0, Recommended=1, Severity=Medium
ID 1926, ASR: Block process creations originating from PSExec and WMI commands, Result=0, Recommended=1, Severity=Medium
ID 1943, ASR: Block process creations originating from PSExec and WMI commands (Intune), Result=0, Recommended=1, Severity=Medium
ID 1912, ASR: Block untrusted and unsigned processes that run from USB (Policy), Result=0, Recommended=1, Severity=Medium
ID 1927, ASR: Block untrusted and unsigned processes that run from USB, Result=0, Recommended=1, Severity=Medium
ID 1944, ASR: Block untrusted and unsigned processes that run from USB (Intune), Result=0, Recommended=1, Severity=Medium

```
ID 1913, ASR: Block Office communication application from creating child processes (Policy), Result=0, Recommended=1,
Severity=Medium
ID 1928, ASR: Block Office communication application from creating child processes, Result=0, Recommended=1,
Severity=Medium
ID 1945, ASR: Block Office communication application from creating child processes (Intune), Result=0, Recommended=1,
Severity=Medium
ID 1914, ASR: Block Adobe Reader from creating child processes (Policy), Result=0, Recommended=1, Severity=Medium
ID 1929, ASR: Block Adobe Reader from creating child processes, Result=0, Recommended=1, Severity=Medium
ID 1946, ASR: Block Adobe Reader from creating child processes (Intune), Result=0, Recommended=1, Severity=Medium
ID 1915, ASR: Block persistence through WMI event subscription (Policy), Result=0, Recommended=1, Severity=Medium
ID 1930, ASR: Block persistence through WMI event subscription, Result=0, Recommended=1, Severity=Medium
ID 1947, ASR: Block persistence through WMI event subscription (Intune), Result=0, Recommended=1, Severity=Medium
ID 1931, ASR: Block abuse of exploited vulnerable signed drivers (Policy), Result=0, Recommended=1, Severity=Medium
ID 1932, ASR: Block abuse of exploited vulnerable signed drivers, Result=0, Recommended=1, Severity=Medium
ID 1948, ASR: Block abuse of exploited vulnerable signed drivers (Intune), Result=0, Recommended=1, Severity=Medium
ID 1966, ASR: Exclude files and paths from Attack Surface Reduction Rules (Policy), Result=, Recommended=,
Severity=Passed
ID 1967, ASR: Exclude files and paths from Attack Surface Reduction Rules, Result=, Recommended=, Severity=Passed
ID 1968, ASR: Exclude files and paths from Attack Surface Reduction Rules (Intune), Result=, Recommended=,
Severity=Passed
ID 1965, Network Protection: Prevent users and apps from accessing dangerous websites, Result=, Recommended=1,
Severity=Medium
[*] 20/08/2025 16:11:25 - Starting Category Administrative Templates: Windows Components
ID 1767, News and interests: Enable news and interests on the taskbar, Result=, Recommended=0, Severity=Medium
ID 1733, OneDrive: Prevent the usage of OneDrive for file storage, Result=0, Recommended=1, Severity=Medium
ID 1734, Remote Desktop Connection Client: Do not allow passwords to be saved, Result=0, Recommended=1, Severity=Medium
ID 1735, Remote Desktop Session Host: Allow users to connect remotely by using Remote Desktop Services, Result=0,
Recommended=1, Severity=Medium
ID 1736, Remote Desktop Session Host: Device and Resource Redirection: Do not allow drive redirection, Result=0,
Recommended=1, Severity=Medium
ID 1737, Remote Desktop Session Host: Security: Always prompt for password upon connection, Result=0, Recommended=1,
Severity=Medium
ID 1738, Remote Desktop Session Host: Security: Require secure RPC communication, Result=0, Recommended=1,
Severity=Medium
ID 1739, Remote Desktop Session Host: Security: Set client connection encryption level, Result=0, Recommended=3,
Severity=Medium
ID 1740, Search: Allow Cloud Search, Result=1, Recommended=0, Severity=Medium
ID 1741, Search: Allow Cortana, Result=1, Recommended=0, Severity=Medium
ID 1742, Search: Allow Cortana above lock screen, Result=1, Recommended=0, Severity=Medium
ID 1743, Search: Allow indexing of encrypted files, Result=1, Recommended=0, Severity=Medium
ID 1744, Search: Allow search and Cortana to use location, Result=1, Recommended=0, Severity=Medium
ID 1745, Search: Set what information is shared in Search, Result=1, Recommended=3, Severity=Medium
ID 1746, Windows Error Reporting: Disable Windows Error Reporting, Result=0, Recommended=1, Severity=Medium
```

```
ID 1747, Windows Game Recording and Broadcasting: Enables or disables Windows Game Recording and Broadcasting, Result=1,
Recommended=0, Severity=Low
ID 1748, Windows Ink Workspace: Allow Windows Ink Workspace, Result=1, Recommended=0, Severity=Medium
ID 1749, Windows Installer: Always install with elevated privileges, Result=0, Recommended=0, Severity=Passed
ID 1750, Windows Installer: Allow user control over installs, Result=1, Recommended=0, Severity=Medium
ID 1751, Windows Installer: Prevent Internet Explorer security prompt for Windows Installer scripts, Result=1,
Recommended=0, Severity=Medium
ID 1752, Windows Logon Options: Sign-in and lock last interactive user automatically after a restart, Result=1,
Recommended=1, Severity=Passed
ID 1770, Windows Installer: Disable Co-Installer (USB AutoInstall), Result=, Recommended=1, Severity=Medium
ID 1753, WinRM Client: Allow Basic authentication, Result=1, Recommended=0, Severity=Medium
ID 1754, WinRM Client: Allow unencrypted traffic, Result=1, Recommended=0, Severity=Medium
ID 1755, WinRM Client: Disallow Digest authentication, Result=1, Recommended=0, Severity=Medium
ID 1756, WinRM Service: Allow remote server management through WinRM, Result=1, Recommended=0, Severity=Medium
ID 1757, WinRM Service: Allow Basic authentication, Result=1, Recommended=0, Severity=Medium
ID 1758, WinRM Service: Allow unencrypted traffic, Result=1, Recommended=0, Severity=Medium
ID 1759, WinRM Service: Disallow WinRM from storing RunAs credentials, Result=0, Recommended=1, Severity=Medium
ID 1760, Windows Remote Shell: Allow Remote Shell Access, Result=1, Recommended=0, Severity=Medium
ID 2000, File Explorer: Configure Windows Defender SmartScreen, Result=1, Recommended=1, Severity=Passed
ID 2001, File Explorer: Configure Windows Defender SmartScreen to warn and prevent bypass, Result=Warn,
Recommended=Block, Severity=Medium
[*] 20/08/2025 16:11:26 - Starting Category PowerShell
ID 2105, Turn on PowerShell Module Logging, Result=0, Recommended=1, Severity=Low
ID 2106, Turn on PowerShell Module Logging - Module Names, Result=, Recommended=*, Severity=Low
ID 2100, Turn on PowerShell Script Block Logging, Result=0, Recommended=1, Severity=Medium
ID 2101, Turn on PowerShell Script Block Logging (Invocation), Result=0, Recommended=1, Severity=Low
ID 2102, Turn on PowerShell Transcription, Result=0, Recommended=1, Severity=Low
ID 2107, Turn on PowerShell Transcription (Invocation), Result=0, Recommended=1, Severity=Low
ID 2103, Disable PowerShell version 2, Result=Enabled, Recommended=Disabled, Severity=Medium
ID 2104, Disable PowerShell version 2 (root), Result=, Recommended=Disabled, Severity=Medium
[*] 20/08/2025 16:11:27 - Starting Category MS Security Guide
ID 2200, LSA Protection, Result=, Recommended=1, Severity=Medium
ID 2201, Lsass.exe audit mode, Result=, Recommended=8, Severity=Low
ID 2202, NetBT NodeType configuration, Result=0, Recommended=2, Severity=Medium
ID 2203, WDigest Authentication, Result=0, Recommended=0, Severity=Passed
ID 2209, Enable Structured Exception Handling Overwrite Protection (SEHOP), Result=0, Recommended=0, Severity=Passed
ID 2210, Limits print driver installation to Administrators, Result=, Recommended=1, Severity=Medium
ID 2211, Configure RPC packet level privacy setting for incoming connections, Result=, Recommended=1, Severity=Medium
ID 2212, Manage processing of Queue-specific files, Result=, Recommended=1, Severity=Medium
[*] 20/08/2025 16:11:27 - Starting Category MSS (Legacy)
ID 2204, MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended), Result=0, Recommended=1, Severity=Medium
ID 2205, MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing),
Result=0, Recommended=2, Severity=Medium
```

```
ID 2206, MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing), Result=1,
Recommended=2, Severity=Medium
ID 2207, MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes, Result=1, Recommended=0,
Severity=Medium
ID 2208, MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS
servers, Result=1, Recommended=1, Severity=Passed
[*] 20/08/2025 16:11:27 - Starting Category Scheduled Task
ID 2400, XblGameSave Standby Task, Result=, Recommended=Disabled, Severity=Medium
[*] 20/08/2025 16:11:29 - Starting Category System Services
ID 2411, Disable mDNS in Dnscache service, Result=, Recommended=0, Severity=Medium
ID 2401, Print Spooler (Spooler), Result=4, Recommended=4, Severity=Passed
ID 2402, Print Spooler (Spooler) (Service Startup type), Result=Disabled, Recommended=Disabled, Severity=Passed
ID 2412, WebClient (WebClient), Result=3, Recommended=4, Severity=Medium
ID 2413, WebClient (WebClient) (Service Startup type), Result=, Recommended=Disabled, Severity=Medium
ID 2403, Xbox Accessory Management Service (XboxGipSvc), Result=3, Recommended=4, Severity=Medium
ID 2404, Xbox Accessory Management Service (XboxGipSvc) (Service Startup type), Result=, Recommended=Disabled,
Severity=Medium
ID 2405, Xbox Live Auth Manager (XblAuthManager), Result=3, Recommended=4, Severity=Medium
ID 2406, Xbox Live Auth Manager (XblAuthManager) (Service Startup type), Result=, Recommended=Disabled, Severity=Medium
ID 2407, Xbox Live Game Save (XblGameSave), Result=3, Recommended=4, Severity=Medium
ID 2408, Xbox Live Game Save (XblGameSave) (Service Startup type), Result=, Recommended=Disabled, Severity=Medium
ID 2409, Xbox Live Networking Service (XboxNetApiSvc), Result=3, Recommended=4, Severity=Medium
ID 2410, Xbox Live Networking Service (XboxNetApiSvc) (Service Startup type), Result=, Recommended=Disabled,
Severity=Medium
[*] 20/08/2025 16:11:29 - Starting Category Microsoft Defender Exploit Guard
ID 1950, Exploit protection: Control flow guard (CFG), Result=NOTSET, Recommended=ON, Severity=Medium
ID 1951, Exploit protection: Data Execution Prevention (DEP), Result=NOTSET, Recommended=ON, Severity=Medium
ID 1952, Exploit protection: Override Data Execution Prevention (DEP), Result=False, Recommended=False, Severity=Passed
ID 1954, Exploit protection: Force randomization for images (Mandatory ASLR), Result=NOTSET, Recommended=ON,
Severity=Medium
ID 1955, Exploit protection: Override force randomization for images (Mandatory ASLR), Result=False, Recommended=False,
Severity=Passed
ID 1956, Exploit protection: Randomize memory allocations (Bottom-up ASLR), Result=NOTSET, Recommended=ON,
Severity=Medium
ID 1957, Exploit protection: Override randomize memory allocations (Bottom-up ASLR), Result=False, Recommended=False,
Severity=Passed
ID 1958, Exploit protection: High-entropy ASLR, Result=NOTSET, Recommended=ON, Severity=Medium
ID 1959, Exploit protection: Override high-entropy ASLR, Result=False, Recommended=False, Severity=Passed
ID 1960, Exploit protection: Validate exception chains (SEHOP), Result=NOTSET, Recommended=ON, Severity=Medium
ID 1961, Exploit protection: Validate exception chains (SEHOP (Telemetry only), Result=NOTSET, Recommended=OFF,
Severity=Medium
ID 1962, Exploit protection: Override validate exception chains (SEHOP), Result=False, Recommended=False, Severity=Passed
ID 1963, Exploit protection: Validate heap integrity, Result=NOTSET, Recommended=ON, Severity=Medium
```

```
ID 1964, Exploit protection: Override validate heap integrity, Result=False, Recommended=False, Severity=Passed
ID 1953, Force use of Data Execution Prevention (DEP), Result=OptIn, Recommended=AlwaysOn, Severity=Medium
[*] 20/08/2025 16:11:30 - Starting Category Windows Firewall
ID 2300, HardeningKitty-Block-TCP-NetBIOS, Result=, Recommended=True, Severity=Low
ID 2301, HardeningKitty-Block-TCP-RDP, Result=, Recommended=True, Severity=Low
ID 2302, HardeningKitty-Block-TCP-RPC, Result=, Recommended=True, Severity=Low
ID 2303, HardeningKitty-Block-TCP-SMB, Result=, Recommended=True, Severity=Low
ID 2304, HardeningKitty-Block-TCP-WinRM, Result=, Recommended=True, Severity=Low
ID 2305, HardeningKitty-Block-UDP-NetBIOS, Result=, Recommended=True, Severity=Low
ID 2306, HardeningKitty-Block-UDP-RPC, Result=, Recommended=True, Severity=Low
ID 2307, HardeningKitty-Block-calc-x64, Result=, Recommended=True, Severity=Low
ID 2308, HardeningKitty-Block-calc-x86, Result=, Recommended=True, Severity=Low
ID 2309, HardeningKitty-Block-certutil-x64, Result=, Recommended=True, Severity=Low
ID 2310, HardeningKitty-Block-certutil-x86, Result=, Recommended=True, Severity=Low
ID 2311, HardeningKitty-Block-conhost-x64, Result=, Recommended=True, Severity=Low
ID 2312, HardeningKitty-Block-conhost-x86, Result=, Recommended=True, Severity=Low
ID 2313, HardeningKitty-Block-cscript-x64, Result=, Recommended=True, Severity=Low
ID 2314, HardeningKitty-Block-cscript-x86, Result=, Recommended=True, Severity=Low
ID 2315, HardeningKitty-Block-mshta-x64, Result=, Recommended=True, Severity=Low
ID 2316, HardeningKitty-Block-mshta-x86, Result=, Recommended=True, Severity=Low
ID 2317, HardeningKitty-Block-notepad-x64, Result=, Recommended=True, Severity=Low
ID 2318, HardeningKitty-Block-notepad-x86, Result=, Recommended=True, Severity=Low
ID 2319, HardeningKitty-Block-RunScriptHelper-x64, Result=, Recommended=True, Severity=Low
ID 2320, HardeningKitty-Block-RunScriptHelper-x86, Result=, Recommended=True, Severity=Low
ID 2321, HardeningKitty-Block-wscript-x64, Result=, Recommended=True, Severity=Low
ID 2322, HardeningKitty-Block-wscript-x86, Result=, Recommended=True, Severity=Low
[*] 20/08/2025 16:11:35 - HardeningKitty is done
[*] 20/08/2025 16:11:41 - Your HardeningKitty score is: 3.49. HardeningKitty Statistics: Total checks: 388 - Passed: 113,
Low: 45, Medium: 230, High: 0.
```