# Windows Atomic Tests by ATT&CK Tactic & Technique

# defense-evasion

- T1134 Access Token Manipulation
  - Atomic Test #1: Access Token Manipulation [windows]
- T1197 BITS Jobs
  - Atomic Test #1: Download & Execute [windows]
  - Atomic Test #2: Download & Execute via PowerShell BITS [windows]
  - Atomic Test #3: Persist, Download, & Execute [windows]
- T1009 Binary Padding
- T1088 Bypass User Account Control
  - Atomic Test #1: Bypass UAC using Event Viewer [windows]
  - Atomic Test #2: Bypass UAC using Event Viewer - PowerShell [windows]
  - Atomic Test #3: Bypass UAC using Fodhelper [windows]
  - Atomic Test #4: Bypass UAC using Fodhelper - PowerShell [windows]
- T1191 CMSTP
  - Atomic Test #1: CMSTP Executing Remote Scriptlet [windows]
  - Atomic Test #2: CMSTP Executing UAC Bypass [windows]
- T1116 Code Signing CONTRIBUTE A TEST
- T1223 Compiled HTML File
  - Atomic Test #1: Compiled HTML Help Local Payload [windows]
  - Atomic Test #2: Compiled HTML Help Remote Payload [windows]
- T1109 Component Firmware CONTRIBUTE A TEST
- T1122 Component Object Model Hijacking
  - Atomic Test #1: Component Object Model Hijacking [windows]

- T1196 Control Panel Items CONTRIBUTE A TEST
- T1207 DCShadow
  - Atomic Test #1: DCShadow - Mimikatz [windows]
- T1038 DLL Search Order Hijacking CONTRIBUTE A TEST
- T1073 DLL Side-Loading CONTRIBUTE A TEST
- T1140 Deobfuscate/Decode Files or Information
  - Atomic Test #1: Deobfuscate/Decode Files Or Information [windows]
  - Atomic Test #2: Certutil Rename and Decode [windows]
- T1089 Disabling Security Tools
  - Atomic Test #8: Unload Sysmon Filter Driver [windows]
  - Atomic Test #9: Disable Windows IIS HTTP Logging [windows]
- T1211 Exploitation for Defense Evasion CONTRIBUTE A TEST
- T1181 Extra Window Memory Injection CONTRIBUTE A TEST
- T1107 File Deletion
  - Atomic Test #4: Delete a single file - Windows cmd [windows]
  - Atomic Test #5: Delete an entire folder - Windows cmd [windows]
  - Atomic Test #6: Delete a single file - Windows PowerShell [windows]
  - Atomic Test #7: Delete an entire folder - Windows PowerShell [windows]
  - Atomic Test #8: Delete VSS - vssadmin [windows]
  - Atomic Test #9: Delete VSS - wmic [windows]
  - Atomic Test #10: bcdedit [windows]
  - Atomic Test #11: wbadmin [windows]
- T1222 File Permissions Modification
  - Atomic Test #1: Take ownership using takeown utility [windows]
  - Atomic Test #2: Take ownership recursively using takeown utility [windows]

    - Atomic Test #3: cacls - Grant permission to specified user or group [windows]
    - Atomic Test #4: cacls - Grant permission to specified user or group recursively [windows]
    - Atomic Test #5: icacls - Grant permission to specified user or group [windows]
    - Atomic Test #6: icacls - Grant permission to specified user or group recursively [windows]
    - Atomic Test #7: attrib - Remove read-only attribute [windows]
- T1006 File System Logical Offsets CONTRIBUTE A TEST
- T1158 Hidden Files and Directories
    - Atomic Test #4: Create Windows System File with Attrib [windows]
    - Atomic Test #5: Create Windows Hidden File with Attrib [windows]
    - Atomic Test #11: Create ADS command prompt [windows]
    - Atomic Test #12: Create ADS PowerShell [windows]
- T1183 Image File Execution Options Injection
    - Atomic Test #1: IFEO Add Debugger [windows]
    - Atomic Test #2: IFEO Global Flags [windows]
- T1054 Indicator Blocking CONTRIBUTE A TEST
- T1066 Indicator Removal from Tools CONTRIBUTE A TEST
- T1070 Indicator Removal on Host
    - Atomic Test #1: Clear Logs [windows]
    - Atomic Test #2: FSUtil [windows]
- T1202 Indirect Command Execution
    - Atomic Test #1: Indirect Command Execution - pcalua.exe [windows]
    - Atomic Test #2: Indirect Command Execution - forfiles.exe [windows]
- T1130 Install Root Certificate
- T1118 InstallUtil
    - Atomic Test #1: InstallUtil uninstall method call [windows]

- T1036 Masquerading
  - Atomic Test #1: Masquerading as Windows LSASS process [windows]
- T1112 Modify Registry
  - Atomic Test #1: Modify Registry of Current User Profile - cmd [windows]
  - Atomic Test #2: Modify Registry of Local Machine - cmd [windows]
  - Atomic Test #3: Modify Registry of Another User Profile [windows]
- T1170 Mshta
  - Atomic Test #1: Mshta executes JavaScript Scheme Fetch Remote Payload With GetObject [windows]
- T1096 NTFS File Attributes
  - Atomic Test #1: Alternate Data Streams (ADS) [windows]
- T1126 Network Share Connection Removal
  - Atomic Test #1: Add Network Share [windows]
  - Atomic Test #2: Remove Network Share [windows]
  - Atomic Test #3: Remove Network Share PowerShell [windows]
- T1027 Obfuscated Files or Information
- T1186 Process Doppelgänging CONTRIBUTE A TEST
- T1093 Process Hollowing CONTRIBUTE A TEST
- T1055 Process Injection
  - Atomic Test #1: Process Injection via mavinject.exe [windows]
  - Atomic Test #2: Process Injection via PowerSploit [windows]
  - Atomic Test #4: Process Injection via C# [windows]
- T1108 Redundant Access CONTRIBUTE A TEST
- T1121 Regsvcs/Regasm
  - Atomic Test #1: Regasm Uninstall Method Call Test [windows]
  - Atomic Test #2: Regsvs Uninstall Method Call Test [windows]

- T1117 Regsvr32
  - Atomic Test #1: Regsvr32 local COM scriptlet execution [windows]
  - Atomic Test #2: Regsvr32 remote COM scriptlet execution [windows]
  - Atomic Test #3: Regsvr32 local DLL execution [windows]
- T1014 Rootkit
  - Atomic Test #3: Windows Signed Driver Rootkit Test [windows]
- T1085 Rundll32
  - Atomic Test #1: Rundll32 execute JavaScript Remote Payload With GetObject [windows]
- T1198 SIP and Trust Provider Hijacking CONTRIBUTE A TEST
- T1064 Scripting
- T1218 Signed Binary Proxy Execution
  - Atomic Test #1: mavinject - Inject DLL into running process [windows]
  - Atomic Test #2: SyncAppvPublishingServer - Execute arbitrary PowerShell code [windows]
  - Atomic Test #3: Register-CimProvider - Execute evil dll [windows]
- T1216 Signed Script Proxy Execution
  - Atomic Test #1: PubPrn.vbs Signed Script Bypass [windows]
- T1045 Software Packing CONTRIBUTE A TEST
- T1221 Template Injection CONTRIBUTE A TEST
- T1099 Timestomp
- T1127 Trusted Developer Utilities
  - Atomic Test #1: MSBuild Bypass Using Inline Tasks [windows]
- T1078 Valid Accounts CONTRIBUTE A TEST
- T1102 Web Service CONTRIBUTE A TEST
- T1220 XSL Script Processing
  - Atomic Test #1: MSXSL Bypass using local files [windows]

- Atomic Test #2: MSXSL Bypass using remote files [windows]
- Atomic Test #3: WMIC bypass using local XSL file [windows]
- Atomic Test #4: WMIC bypass using remote XSL file [windows]

# privilege-escalation

- T1134 Access Token Manipulation
  - Atomic Test #1: Access Token Manipulation [windows]
- T1015 Accessibility Features
  - Atomic Test #1: Attaches Command Prompt As Debugger To Process - osk [windows]
  - Atomic Test #2: Attaches Command Prompt As Debugger To Process - sethc [windows]
  - Atomic Test #3: Attaches Command Prompt As Debugger To Process - utilman [windows]
  - Atomic Test #4: Attaches Command Prompt As Debugger To Process - magnify [windows]
  - Atomic Test #5: Attaches Command Prompt As Debugger To Process - narrator [windows]
  - Atomic Test #6: Attaches Command Prompt As Debugger To Process - DisplaySwitch [windows]
  - Atomic Test #7: Attaches Command Prompt As Debugger To Process - AtBroker [windows]
- T1182 AppCert DLLs CONTRIBUTE A TEST
- T1103 AppInit DLLs
  - Atomic Test #1: Install AppInit Shim [windows]
- T1138 Application Shimming
  - Atomic Test #1: Application Shim Installation [windows]
- T1088 Bypass User Account Control
  - Atomic Test #1: Bypass UAC using Event Viewer [windows]
  - Atomic Test #2: Bypass UAC using Event Viewer - PowerShell [windows]
  - Atomic Test #3: Bypass UAC using Fodhelper [windows]

    - Atomic Test #4: Bypass UAC using Fodhelper - PowerShell [windows]
- T1038 DLL Search Order Hijacking CONTRIBUTE A TEST
- T1068 Exploitation for Privilege Escalation CONTRIBUTE A TEST
- T1181 Extra Window Memory Injection CONTRIBUTE A TEST
- T1044 File System Permissions Weakness CONTRIBUTE A TEST
- T1179 Hooking
    - Atomic Test #1: Hook PowerShell TLS Encrypt/Decrypt Messages [windows]
- T1183 Image File Execution Options Injection
    - Atomic Test #1: IFEO Add Debugger [windows]
    - Atomic Test #2: IFEO Global Flags [windows]
- T1050 New Service
    - Atomic Test #1: Service Installation [windows]
    - Atomic Test #2: Service Installation PowerShell Installs A Local Service using PowerShell [windows]
- T1034 Path Interception CONTRIBUTE A TEST
- T1013 Port Monitors CONTRIBUTE A TEST
- T1055 Process Injection
    - Atomic Test #1: Process Injection via mavinject.exe [windows]
    - Atomic Test #2: Process Injection via PowerSploit [windows]
    - Atomic Test #4: Process Injection via C# [windows]
- T1178 SID-History Injection CONTRIBUTE A TEST
- T1053 Scheduled Task
    - Atomic Test #1: At.exe Scheduled task [windows]
    - Atomic Test #2: Scheduled task Local [windows]
    - Atomic Test #3: Scheduled task Remote [windows]
- T1058 Service Registry Permissions Weakness CONTRIBUTE A TEST

- T1078 Valid Accounts CONTRIBUTE A TEST
- T1100 Web Shell
  - Atomic Test #1: Web Shell Written to Disk [windows]

# persistence

- T1015 Accessibility Features
  - Atomic Test #1: Attaches Command Prompt As Debugger To Process - osk [windows]
  - Atomic Test #2: Attaches Command Prompt As Debugger To Process - sethc [windows]
  - Atomic Test #3: Attaches Command Prompt As Debugger To Process - utilman [windows]
  - Atomic Test #4: Attaches Command Prompt As Debugger To Process - magnify [windows]
  - Atomic Test #5: Attaches Command Prompt As Debugger To Process - narrator [windows]
  - Atomic Test #6: Attaches Command Prompt As Debugger To Process - DisplaySwitch [windows]
  - Atomic Test #7: Attaches Command Prompt As Debugger To Process - AtBroker [windows]
- T1098 Account Manipulation
  - Atomic Test #1: Admin Account Manipulate [windows]
- T1182 AppCert DLLs CONTRIBUTE A TEST
- T1103 AppInit DLLs
  - Atomic Test #1: Install AppInit Shim [windows]
- T1138 Application Shimming
  - Atomic Test #1: Application Shim Installation [windows]
- T1131 Authentication Package CONTRIBUTE A TEST
- T1197 BITS Jobs
  - Atomic Test #1: Download & Execute [windows]
  - Atomic Test #2: Download & Execute via PowerShell BITS [windows]

    - Atomic Test #3: Persist, Download, & Execute [windows]
- T1067 Bootkit CONTRIBUTE A TEST
- T1176 Browser Extensions
    - Atomic Test #1: Chrome (Developer Mode) [linux, windows, macos]
    - Atomic Test #2: Chrome (Chrome Web Store) [linux, windows, macos]
    - Atomic Test #3: Firefox [linux, windows, macos]
- T1042 Change Default File Association
    - Atomic Test #1: Change Default File Association [windows]
- T1109 Component Firmware CONTRIBUTE A TEST
- T1122 Component Object Model Hijacking
    - Atomic Test #1: Component Object Model Hijacking [windows]
- T1136 Create Account
    - Atomic Test #3: Create a new user in a command prompt [windows]
    - Atomic Test #4: Create a new user in PowerShell [windows]
- T1038 DLL Search Order Hijacking CONTRIBUTE A TEST
- T1133 External Remote Services CONTRIBUTE A TEST
- T1044 File System Permissions Weakness CONTRIBUTE A TEST
- T1158 Hidden Files and Directories
    - Atomic Test #4: Create Windows System File with Attrib [windows]
    - Atomic Test #5: Create Windows Hidden File with Attrib [windows]
    - Atomic Test #11: Create ADS command prompt [windows]
    - Atomic Test #12: Create ADS PowerShell [windows]
- T1179 Hooking
    - Atomic Test #1: Hook PowerShell TLS Encrypt/Decrypt Messages [windows]
- T1062 Hypervisor

    - Atomic Test #1: Installing Hyper-V Feature [windows]
- T1183 Image File Execution Options Injection
    - Atomic Test #1: IFEO Add Debugger [windows]
    - Atomic Test #2: IFEO Global Flags [windows]
- T1177 LSASS Driver CONTRIBUTE A TEST
- T1037 Logon Scripts
    - Atomic Test #1: Logon Scripts [windows]
- T1031 Modify Existing Service
    - Atomic Test #1: Modify Fax service to run PowerShell [windows]
- T1128 Netsh Helper DLL
    - Atomic Test #1: Netsh Helper DLL Registration [windows]
- T1050 New Service
    - Atomic Test #1: Service Installation [windows]
    - Atomic Test #2: Service Installation PowerShell Installs A Local Service using PowerShell [windows]
- T1137 Office Application Startup
    - Atomic Test #1: DDEAUTO [windows]
- T1034 Path Interception CONTRIBUTE A TEST
- T1013 Port Monitors CONTRIBUTE A TEST
- T1108 Redundant Access CONTRIBUTE A TEST
- T1060 Registry Run Keys / Startup Folder
    - Atomic Test #1: Reg Key Run [windows]
    - Atomic Test #2: Reg Key RunOnce [windows]
    - Atomic Test #3: PowerShell Registry RunOnce [windows]
    - Atomic Test #4: Startup Folder [windows]
- T1198 SIP and Trust Provider Hijacking CONTRIBUTE A TEST

- T1053 Scheduled Task
  - Atomic Test #1: At.exe Scheduled task [windows]
  - Atomic Test #2: Scheduled task Local [windows]
  - Atomic Test #3: Scheduled task Remote [windows]
- T1180 Screensaver
  - Atomic Test #1: Set Arbitrary Binary as Screensaver [windows]
- T1101 Security Support Provider
  - Atomic Test #1: Modify SSP configuration in registry [windows]
- T1058 Service Registry Permissions Weakness CONTRIBUTE A TEST
- T1023 Shortcut Modification CONTRIBUTE A TEST
- T1019 System Firmware CONTRIBUTE A TEST
- T1209 Time Providers CONTRIBUTE A TEST
- T1078 Valid Accounts CONTRIBUTE A TEST
- T1100 Web Shell
  - Atomic Test #1: Web Shell Written to Disk [windows]
- T1084 Windows Management Instrumentation Event Subscription
  - Atomic Test #1: Persistence [windows]
  - Atomic Test #2: Persistence Cleanup [windows]
- T1004 Winlogon Helper DLL
  - Atomic Test #1: Winlogon Shell Key Persistence - PowerShell [windows]
  - Atomic Test #2: Winlogon Userinit Key Persistence - PowerShell [windows]
  - Atomic Test #3: Winlogon Notify Key Logon Persistence - PowerShell [windows]

# discovery

- T1087 Account Discovery
  - Atomic Test #7: Enumerate all accounts [windows]
  - Atomic Test #8: Enumerate all accounts via PowerShell [windows]
  - Atomic Test #9: Enumerate logged on users [windows]
  - Atomic Test #10: Enumerate logged on users via PowerShell [windows]
- T1010 Application Window Discovery
  - Atomic Test #1: List Process Main Windows - C# .NET [windows]
- T1217 Browser Bookmark Discovery
- T1083 File and Directory Discovery
  - Atomic Test #1: File and Directory Discovery [windows]
  - Atomic Test #2: File and Directory Discovery [windows]
- T1046 Network Service Scanning
- T1135 Network Share Discovery
  - Atomic Test #2: Network Share Discovery command prompt [windows]
  - Atomic Test #3: Network Share Discovery PowerShell [windows]
- T1040 Network Sniffing
  - Atomic Test #3: Packet Capture Windows Command Prompt [windows]
  - Atomic Test #4: Packet Capture PowerShell [windows]
- T1201 Password Policy Discovery
- T1120 Peripheral Device Discovery CONTRIBUTE A TEST
- T1069 Permission Groups Discovery
  - Atomic Test #2: Permission Groups Discovery Windows [windows]
  - Atomic Test #3: Permission Groups Discovery PowerShell [windows]
- T1057 Process Discovery
- T1012 Query Registry

    - Atomic Test #1: Query Registry [windows]
- T1018 Remote System Discovery
    - Atomic Test #1: Remote System Discovery - net [windows]
    - Atomic Test #2: Remote System Discover - ping sweep [windows]
    - Atomic Test #3: Remote System Discover - arp [windows]
- T1063 Security Software Discovery
    - Atomic Test #1: Security Software Discovery [windows]
    - Atomic Test #2: Security Software Discovery - powershell [windows]
    - Atomic Test #4: Security Software Discovery - Sysmon Service [windows]
- T1082 System Information Discovery
    - Atomic Test #1: System Information Discovery [windows]
- T1016 System Network Configuration Discovery
    - Atomic Test #1: System Network Configuration Discovery [windows]
- T1049 System Network Connections Discovery
    - Atomic Test #1: System Network Connections Discovery [windows]
    - Atomic Test #2: System Network Connections Discovery with PowerShell [windows]
- T1033 System Owner/User Discovery
    - Atomic Test #1: System Owner/User Discovery [windows]
- T1007 System Service Discovery
    - Atomic Test #1: System Service Discovery [windows]
    - Atomic Test #2: System Service Discovery - net.exe [windows]
- T1124 System Time Discovery
    - Atomic Test #1: System Time Discovery [windows]
    - Atomic Test #2: System Time Discovery - PowerShell [windows]

# credential-access

- T1098 Account Manipulation
  - Atomic Test #1: Admin Account Manipulate [windows]
- T1110 Brute Force
  - Atomic Test #1: Brute Force Credentials [windows]
- T1003 Credential Dumping
  - Atomic Test #1: Powershell Mimikatz [windows]
  - Atomic Test #2: Gsecdump [windows]
  - Atomic Test #3: Windows Credential Editor [windows]
  - Atomic Test #4: Registry dump of SAM, creds, and secrets [windows]
  - Atomic Test #5: Dump LSASS.exe Memory using ProcDump [windows]
  - Atomic Test #6: Dump LSASS.exe Memory using Windows Task Manager [windows]
  - Atomic Test #7: Offline Credential Theft With Mimikatz [windows]
  - Atomic Test #8: Dump Active Directory Database with NTDSUtil [windows]
- T1081 Credentials in Files
  - Atomic Test #3: Mimikatz & Kittenz [windows]
  - Atomic Test #4: Extracting credentials from files [windows]
- T1214 Credentials in Registry
  - Atomic Test #1: Enumeration for Credentials in Registry [windows]
- T1212 Exploitation for Credential Access CONTRIBUTE A TEST
- T1187 Forced Authentication CONTRIBUTE A TEST
- T1179 Hooking
  - Atomic Test #1: Hook PowerShell TLS Encrypt/Decrypt Messages [windows]

- T1056 Input Capture
  - Atomic Test #1: Input Capture [windows]
- T1208 Kerberoasting CONTRIBUTE A TEST
- T1171 LLMNR/NBT-NS Poisoning CONTRIBUTE A TEST
- T1040 Network Sniffing
  - Atomic Test #3: Packet Capture Windows Command Prompt [windows]
  - Atomic Test #4: Packet Capture PowerShell [windows]
- T1174 Password Filter DLL
  - Atomic Test #1: Install and Register Password Filter DLL [windows]
- T1145 Private Keys
  - Atomic Test #1: Private Keys [windows]
- T1111 Two-Factor Authentication Interception CONTRIBUTE A TEST

# lateral-movement

- T1017 Application Deployment Software CONTRIBUTE A TEST
- T1175 Distributed Component Object Model CONTRIBUTE A TEST
- T1210 Exploitation of Remote Services CONTRIBUTE A TEST
- T1037 Logon Scripts
  - Atomic Test #1: Logon Scripts [windows]
- T1075 Pass the Hash
  - Atomic Test #1: Mimikatz Pass the Hash [windows]
  - Atomic Test #2: Mimikatz Kerberos Ticket Attack [windows]
- T1097 Pass the Ticket CONTRIBUTE A TEST
- T1076 Remote Desktop Protocol

    - Atomic Test #1: RDP [windows]
- T1105 Remote File Copy
    - Atomic Test #7: certutil download (urlcache) [windows]
    - Atomic Test #8: certutil download (verifyctl) [windows]
- T1021 Remote Services CONTRIBUTE A TEST
- T1091 Replication Through Removable Media CONTRIBUTE A TEST
- T1051 Shared Webroot CONTRIBUTE A TEST
- T1080 Taint Shared Content CONTRIBUTE A TEST
- T1072 Third-party Software CONTRIBUTE A TEST
- T1077 Windows Admin Shares
    - Atomic Test #1: Map admin share [windows]
    - Atomic Test #2: Map Admin Share PowerShell [windows]
- T1028 Windows Remote Management
    - Atomic Test #1: Enable Windows Remote Management [windows]
    - Atomic Test #2: PowerShell Lateral Movement [windows]
    - Atomic Test #3: WMIC Process Call Create [windows]
    - Atomic Test #4: Psexec [windows]
    - Atomic Test #5: Invoke-Command [windows]

# collection

- T1123 Audio Capture
    - Atomic Test #1: SourceRecorder via Windows command prompt [windows]
    - Atomic Test #2: PowerShell Cmdlet via Windows command prompt [windows]

- T1119 Automated Collection
  - Atomic Test #1: Automated Collection Command Prompt [windows]
  - Atomic Test #2: Automated Collection PowerShell [windows]
- T1115 Clipboard Data
  - Atomic Test #1: Utilize Clipboard to store or execute commands from [windows]
  - Atomic Test #2: PowerShell [windows]
- T1074 Data Staged
- T1213 Data from Information Repositories CONTRIBUTE A TEST
- T1005 Data from Local System
- T1039 Data from Network Shared Drive CONTRIBUTE A TEST
- T1025 Data from Removable Media CONTRIBUTE A TEST
- T1114 Email Collection
  - Atomic Test #1: T1114 Email Collection with PowerShell [windows]
- T1056 Input Capture
  - Atomic Test #1: Input Capture [windows]
- T1185 Man in the Browser CONTRIBUTE A TEST
- T1113 Screen Capture
- T1125 Video Capture CONTRIBUTE A TEST

# exfiltration

- T1020 Automated Exfiltration CONTRIBUTE A TEST
- T1002 Data Compressed
  - Atomic Test #1: Compress Data for Exfiltration With PowerShell [windows]
  - Atomic Test #2: Compress Data for Exfiltration With Rar [windows]

- T1022 Data Encrypted
  - Atomic Test #2: Compress Data and lock with password for Exfiltration with winrar [windows]
  - Atomic Test #3: Compress Data and lock with password for Exfiltration with winzip [windows]
  - Atomic Test #4: Compress Data and lock with password for Exfiltration with 7zip [windows]
- T1030 Data Transfer Size Limits
- T1048 Exfiltration Over Alternative Protocol
- T1041 Exfiltration Over Command and Control Channel CONTRIBUTE A TEST
- T1011 Exfiltration Over Other Network Medium CONTRIBUTE A TEST
- T1052 Exfiltration Over Physical Medium CONTRIBUTE A TEST
- T1029 Scheduled Transfer CONTRIBUTE A TEST

# execution

- T1191 CMSTP
  - Atomic Test #1: CMSTP Executing Remote Scriptlet [windows]
  - Atomic Test #2: CMSTP Executing UAC Bypass [windows]
- T1059 Command-Line Interface
- T1223 Compiled HTML File
  - Atomic Test #1: Compiled HTML Help Local Payload [windows]
  - Atomic Test #2: Compiled HTML Help Remote Payload [windows]
- T1196 Control Panel Items CONTRIBUTE A TEST
- T1173 Dynamic Data Exchange
  - Atomic Test #1: Execute Commands [windows]
- T1106 Execution through API CONTRIBUTE A TEST

- T1129 Execution through Module Load CONTRIBUTE A TEST
- T1203 Exploitation for Client Execution CONTRIBUTE A TEST
- T1061 Graphical User Interface CONTRIBUTE A TEST
- T1118 InstallUtil
  - Atomic Test #1: InstallUtil uninstall method call [windows]
- T1177 LSASS Driver CONTRIBUTE A TEST
- T1170 Mshta
  - Atomic Test #1: Mshta executes JavaScript Scheme Fetch Remote Payload With GetObject [windows]
- T1086 PowerShell
  - Atomic Test #1: Mimikatz [windows]
  - Atomic Test #2: BloodHound [windows]
  - Atomic Test #3: Obfuscation Tests [windows]
  - Atomic Test #4: Mimikatz - Cradlecraft PsSendKeys [windows]
  - Atomic Test #5: Invoke-AppPathBypass [windows]
  - Atomic Test #6: PowerShell Add User [windows]
  - Atomic Test #7: Powershell MsXml COM object - no prompt [windows]
  - Atomic Test #8: Powershell MsXml COM object - with prompt [windows]
  - Atomic Test #9: Powershell XML requests [windows]
  - Atomic Test #10: Powershell invoke mshta.exe download [windows]
  - Atomic Test #11: Powershell Invoke-DownloadCradle [windows]
  - Atomic Test #12: PowerShell Fileless Script Execution [windows]
- T1121 Regsvcs/Regasm
  - Atomic Test #1: Regasm Uninstall Method Call Test [windows]
  - Atomic Test #2: Regsvs Uninstall Method Call Test [windows]

- T1117 Regsvr32
  - Atomic Test #1: Regsvr32 local COM scriptlet execution [windows]
  - Atomic Test #2: Regsvr32 remote COM scriptlet execution [windows]
  - Atomic Test #3: Regsvr32 local DLL execution [windows]
- T1085 Rundll32
  - Atomic Test #1: Rundll32 execute JavaScript Remote Payload With GetObject [windows]
- T1053 Scheduled Task
  - Atomic Test #1: At.exe Scheduled task [windows]
  - Atomic Test #2: Scheduled task Local [windows]
  - Atomic Test #3: Scheduled task Remote [windows]
- T1064 Scripting
- T1035 Service Execution
  - Atomic Test #1: Execute a Command as a Service [windows]
- T1218 Signed Binary Proxy Execution
  - Atomic Test #1: mavinject - Inject DLL into running process [windows]
  - Atomic Test #2: SyncAppvPublishingServer - Execute arbitrary PowerShell code [windows]
  - Atomic Test #3: Register-CimProvider - Execute evil dll [windows]
- T1216 Signed Script Proxy Execution
  - Atomic Test #1: PubPrn.vbs Signed Script Bypass [windows]
- T1072 Third-party Software CONTRIBUTE A TEST
- T1127 Trusted Developer Utilities
  - Atomic Test #1: MSBuild Bypass Using Inline Tasks [windows]
- T1204 User Execution CONTRIBUTE A TEST
- T1047 Windows Management Instrumentation
  - Atomic Test #1: WMI Reconnaissance Users [windows]

    - Atomic Test #2: WMI Reconnaissance Processes [windows]
    - Atomic Test #3: WMI Reconnaissance Software [windows]
    - Atomic Test #4: WMI Reconnaissance List Remote Services [windows]
- T1028 Windows Remote Management
    - Atomic Test #1: Enable Windows Remote Management [windows]
    - Atomic Test #2: PowerShell Lateral Movement [windows]
    - Atomic Test #3: WMIC Process Call Create [windows]
    - Atomic Test #4: Psexec [windows]
    - Atomic Test #5: Invoke-Command [windows]
- T1220 XSL Script Processing
    - Atomic Test #1: MSXSL Bypass using local files [windows]
    - Atomic Test #2: MSXSL Bypass using remote files [windows]
    - Atomic Test #3: WMIC bypass using local XSL file [windows]
    - Atomic Test #4: WMIC bypass using remote XSL file [windows]

# command-and-control

- T1043 Commonly Used Port CONTRIBUTE A TEST
- T1092 Communication Through Removable Media CONTRIBUTE A TEST
- T1094 Custom Command and Control Protocol CONTRIBUTE A TEST
- T1024 Custom Cryptographic Protocol CONTRIBUTE A TEST
- T1132 Data Encoding
- T1001 Data Obfuscation CONTRIBUTE A TEST
- T1172 Domain Fronting CONTRIBUTE A TEST

- T1008 Fallback Channels CONTRIBUTE A TEST
- T1104 Multi-Stage Channels CONTRIBUTE A TEST
- T1188 Multi-hop Proxy CONTRIBUTE A TEST
- T1026 Multiband Communication CONTRIBUTE A TEST
- T1079 Multilayer Encryption CONTRIBUTE A TEST
- T1219 Remote Access Tools CONTRIBUTE A TEST
- T1105 Remote File Copy
  - Atomic Test #7: certutil download (urlcache) [windows]
  - Atomic Test #8: certutil download (verifyctl) [windows]
- T1071 Standard Application Layer Protocol
  - Atomic Test #1: Malicious User Agents [windows]
- T1032 Standard Cryptographic Protocol CONTRIBUTE A TEST
- T1095 Standard Non-Application Layer Protocol CONTRIBUTE A TEST
- T1065 Uncommonly Used Port
  - Atomic Test #1: Testing usage of uncommonly used port with PowerShell [windows]
- T1102 Web Service CONTRIBUTE A TEST

# initial-access

- T1189 Drive-by Compromise CONTRIBUTE A TEST
- T1190 Exploit Public-Facing Application CONTRIBUTE A TEST
- T1200 Hardware Additions CONTRIBUTE A TEST
- T1091 Replication Through Removable Media CONTRIBUTE A TEST
- T1193 Spearphishing Attachment

    - Atomic Test #1: Download Phishing Attachment - VBScript [windows]
- T1192 Spearphishing Link CONTRIBUTE A TEST
- T1194 Spearphishing via Service CONTRIBUTE A TEST
- T1195 Supply Chain Compromise CONTRIBUTE A TEST
- T1199 Trusted Relationship CONTRIBUTE A TEST
- T1078 Valid Accounts CONTRIBUTE A TEST