Seatbelt

Seatbelt is a C# project that performs a number of security oriented host-survey "safety checks" relevant from both offensive and defensive security perspectives.

@andrewchiles' HostEnum.ps1 script and @tifkin_'s Get-HostProfile.ps1 provided inspiration for many of the artifacts to collect.

@harmj0y and @tifkin_ are the primary authors of this implementation.

Seatbelt is licensed under the BSD 3-Clause license.

Table of Contents

Command Line Usage

```
                        %&&@@@&&
                        &&&&&&&%%,                          #&&@@@@@@%%
                        &%&   %&%%                          &////(((&%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%  &%%**#                      @////(((&%%
#%%%%%%%%%%%%%%%%%%%%%%%%%%%%  %&%,,,,,,,,,,,,,,,,        @////(((&%%
#%%%%%%%%%%%%%%%%%%%%%%%%%%%%  %%%,,,,,,  ,,,.   ,,        @////(((&%%
##########################%%%%  &%%......  ...   ..        @////(((&%%
###########################%%%  %%%......  ...   ..        @////(((&%%
##########################%%%%  &%%..............          @////(((&%%
#########################%%%%%  %%%..                       @////(((&%%
                        &%%   %%%%%      Seatbelt           %////(((&%%
                        &%%&&%%%%%%        v1.2.1           ,(((&%%%%%%
                         #%%%%%#,


Available commands (+ means remote usage is supported):

  + AMSIProviders          - Providers registered for AMSI
  + AntiVirus              - Registered antivirus (via WMI)
  + AppLocker              - AppLocker settings, if installed
    ARPTable               - Lists the current ARP table and adapt
    AuditPolicies          - Enumerates classic and advanced audit
  + AuditPolicyRegistry    - Audit settings via the registry
  + AutoRuns               - Auto run executables/scripts/programs
    azuread                - Return AzureAD info
    Certificates           - Finds user and machine personal certi
    CertificateThumbprints - Finds thumbprints for all certificate
  + ChromiumBookmarks      - Parses any found Chrome/Edge/Brave/Op
  + ChromiumHistory        - Parses any found Chrome/Edge/Brave/Op
  + ChromiumPresence       - Checks if interesting Chrome/Edge/Bra
  + CloudCredentials       - AWS/Google/Azure/Bluemix cloud creden
  + CloudSyncProviders     - All configured Office 365 endpoints (
    CredEnum               - Enumerates the current user's saved c
  + CredGuard              - CredentialGuard configuration
    dir                    - Lists files/folders. By default, list
  + DNSCache               - DNS cache entries (via WMI)
  + DotNet                 - DotNet versions
  + DpapiMasterKeys        - List DPAPI master keys
    EnvironmentPath        - Current environment %PATH$ folders an
  + EnvironmentVariables   - Current environment variables
  + ExplicitLogonEvents    - Explicit Logon events (Event ID 4648)
    ExplorerMRUs           - Explorer most recently used files (la
  + ExplorerRunCommands    - Recent Explorer "run" commands
    FileInfo               - Information about a file (version inf
  + FileZilla              - FileZilla configuration files
  + FirefoxHistory         - Parses any found FireFox history file
  + FirefoxPresence        - Checks if interesting Firefox files e
  + Hotfixes               - Installed hotfixes (via WMI)
    IdleTime               - Returns the number of seconds since t
  + IEFavorites            - Internet Explorer favorites
    IETabs                 - Open Internet Explorer tabs
  + IEUrls                 - Internet Explorer typed URLs (last 7
  + InstalledProducts      - Installed products via the registry
    InterestingFiles       - "Interesting" files matching various
  + InterestingProcesses   - "Interesting" processes - defensive p
    InternetSettings       - Internet settings including proxy con
  + KeePass                - Finds KeePass configuration files
  + LAPS                   - LAPS settings, if installed
  + LastShutdown           - Returns the DateTime of the last syst
    LocalGPOs              - Local Group Policy settings applied t
  + LocalGroups            - Non-empty local groups, "-full" displ
  + LocalUsers             - Local users, whether they're active/d
  + LogonEvents            - Logon events (Event ID 4624) from the
  + LogonSessions          - Windows logon sessions
    LOLBAS                 - Locates Living Off The Land Binaries
  + LSASettings            - LSA settings (including auth packages
  + MappedDrives           - Users' mapped drives (via WMI)
    McAfeeConfigs          - Finds McAfee configuration files
    McAfeeSiteList         - Decrypt any found McAfee SiteList.xml
    MicrosoftUpdates       - All Microsoft updates (via COM)
```

```
      MTPuTTY                - MTPuTTY configuration files
      NamedPipes             - Named pipe names, any readable ACL in
    + NetworkProfiles        - Windows network profiles
    + NetworkShares          - Network shares exposed by the machine
    + NTLMSettings           - NTLM authentication settings
      OfficeMRUs             - Office most recently used file list (
      OneNote                - List OneNote backup files
    + OptionalFeatures       - List Optional Features/Roles (via WMI
      OracleSQLDeveloper     - Finds Oracle SQLDeveloper connections
    + OSInfo                 - Basic OS info (i.e. architecture, OS
    + OutlookDownloads       - List files downloaded by Outlook
    + PoweredOnEvents        - Reboot and sleep schedule based on th
    + PowerShell             - PowerShell versions and security sett
    + PowerShellEvents       - PowerShell script block logs (4104) w
    + PowerShellHistory      - Searches PowerShell console history f
      Printers               - Installed Printers (via WMI)
    + ProcessCreationEvents  - Process creation logs (4688) with sen
      Processes              - Running processes with file info comp
    + ProcessOwners          - Running non-session 0 process list wi
    + PSSessionSettings      - Enumerates PS Session Settings from t
    + PuttyHostKeys          - Saved Putty SSH host keys
    + PuttySessions          - Saved Putty configuration (interestin
      RDCManFiles            - Windows Remote Desktop Connection Man
    + RDPSavedConnections    - Saved RDP connections stored in the r
    + RDPSessions            - Current incoming RDP sessions (argume
    + RDPsettings            - Remote Desktop Server/Client Settings
      RecycleBin             - Items in the Recycle Bin deleted in t
      reg                    - Registry key values (HKLM\Software by
      RPCMappedEndpoints     - Current RPC endpoints mapped
    + SCCM                   - System Center Configuration Manager (
    + ScheduledTasks         - Scheduled tasks (via WMI) that aren't
      SearchIndex            - Query results from the Windows Search
      SecPackageCreds        - Obtains credentials from security pac
    + SecureBoot             - Secure Boot configuration
      SecurityPackages       - Enumerates the security packages curr
      Services               - Services with file info company names
    + SlackDownloads         - Parses any found 'slack-downloads' fi
    + SlackPresence          - Checks if interesting Slack files exi
    + SlackWorkspaces        - Parses any found 'slack-workspaces' f
    + SuperPutty             - SuperPutty configuration files
    + Sysmon                 - Sysmon configuration from the registry
    + SysmonEvents           - Sysmon process creation logs (1) with
      TcpConnections         - Current TCP connections and their ass
      TokenGroups            - The current token's local and domain
      TokenPrivileges        - Currently enabled token privileges (e
    + UAC                    - UAC system policies via the registry
      UdpConnections         - Current UDP connections and associate
      UserRightAssignments   - Configured User Right Assignments (e.
      WifiProfile            - Enumerates the saved Wifi profiles an
    + WindowsAutoLogon       - Registry autologon information
      WindowsCredentialFiles - Windows credential DPAPI blobs
    + WindowsDefender        - Windows Defender settings (including
    + WindowsEventForwarding - Windows Event Forwarding (WEF) settin
    + WindowsFirewall        - Non-standard firewall rules, "-full"
      WindowsVault           - Credentials saved in the Windows Vaul
    + WMI                    - Runs a specified WMI query
      WMIEventConsumer       - Lists WMI Event Consumers
      WMIEventFilter         - Lists WMI Event Filters
      WMIFilterBinding       - Lists WMI Filter to Consumer Bindings
    + WSUS                   - Windows Server Update Services (WSUS)


Seatbelt has the following command groups: All, User, System, Slack,

    You can invoke command groups with         "Seatbelt.exe <group>


    Or command groups except specific commands "Seatbelt.exe <group>

   "Seatbelt.exe -group=all" runs all commands

   "Seatbelt.exe -group=user" runs the following commands:

        azuread, Certificates, CertificateThumbprints, ChromiumPrese
        CloudSyncProviders, CredEnum, dir, DpapiMasterKeys,
```

```
        ExplorerMRUs, ExplorerRunCommands, FileZilla, FirefoxPresenc
        IdleTime, IEFavorites, IETabs, IEUrls,
        KeePass, MappedDrives, MTPuTTY, OfficeMRUs,
        OneNote, OracleSQLDeveloper, PowerShellHistory, PuttyHostKey
        PuttySessions, RDCManFiles, RDPSavedConnections, SecPackageC
        SlackDownloads, SlackPresence, SlackWorkspaces, SuperPutty,
        TokenGroups, WindowsCredentialFiles, WindowsVault

    "Seatbelt.exe -group=system" runs the following commands:

        AMSIProviders, AntiVirus, AppLocker, ARPTable, AuditPolicies,
        AuditPolicyRegistry, AutoRuns, Certificates, CertificateThumb
        CredGuard, DNSCache, DotNet, EnvironmentPath,
        EnvironmentVariables, Hotfixes, InterestingProcesses, Interne
        LAPS, LastShutdown, LocalGPOs, LocalGroups,
        LocalUsers, LogonSessions, LSASettings, McAfeeConfigs,
        NamedPipes, NetworkProfiles, NetworkShares, NTLMSettings,
        OptionalFeatures, OSInfo, PoweredOnEvents, PowerShell,
        Processes, PSSessionSettings, RDPSessions, RDPsettings,
        SCCM, SecureBoot, Services, Sysmon,
        TcpConnections, TokenPrivileges, UAC, UdpConnections,
        UserRightAssignments, WifiProfile, WindowsAutoLogon, WindowsU
        WindowsEventForwarding, WindowsFirewall, WMI, WMIEventConsume
        WMIEventFilter, WMIFilterBinding, WSUS

    "Seatbelt.exe -group=slack" runs the following commands:

        SlackDownloads, SlackPresence, SlackWorkspaces

    "Seatbelt.exe -group=chromium" runs the following commands:

        ChromiumBookmarks, ChromiumHistory, ChromiumPresence

    "Seatbelt.exe -group=remote" runs the following commands:

        AMSIProviders, AntiVirus, AuditPolicyRegistry, ChromiumPrese
        DNSCache, DotNet, DpapiMasterKeys, EnvironmentVariables,
        ExplicitLogonEvents, ExplorerRunCommands, FileZilla, Hotfixes
        InterestingProcesses, KeePass, LastShutdown, LocalGroups,
        LocalUsers, LogonEvents, LogonSessions, LSASettings,
        MappedDrives, NetworkProfiles, NetworkShares, NTLMSettings,
        OptionalFeatures, OSInfo, PoweredOnEvents, PowerShell,
        ProcessOwners, PSSessionSettings, PuttyHostKeys, PuttySessio
        RDPSavedConnections, RDPSessions, RDPsettings, SecureBoot,
        Sysmon, WindowsDefender, WindowsEventForwarding, WindowsFire


    "Seatbelt.exe -group=misc" runs the following commands:

        ChromiumBookmarks, ChromiumHistory, ExplicitLogonEvents, File
        InstalledProducts, InterestingFiles, LogonEvents, LOLBAS,
        McAfeeSiteList, MicrosoftUpdates, OutlookDownloads, PowerShe
        Printers, ProcessCreationEvents, ProcessOwners, RecycleBin,
        reg, RPCMappedEndpoints, ScheduledTasks, SearchIndex,
        SecurityPackages, SysmonEvents


Examples:
    'Seatbelt.exe <Command> [Command2] ...' will run one or more spe
    'Seatbelt.exe <Command> -full' will return complete results for
    'Seatbelt.exe "<Command> [argument]"' will pass an argument to a
    'Seatbelt.exe -group=all' will run ALL enumeration checks, can b
    'Seatbelt.exe -group=all -AuditPolicies' will run all enumeratio
    'Seatbelt.exe <Command> -computername=COMPUTER.DOMAIN.COM [-user
    'Seatbelt.exe -group=remote -computername=COMPUTER.DOMAIN.COM [-
    'Seatbelt.exe -group=system -outputfile="C:\Temp\out.txt"' will
    'Seatbelt.exe -group=user -q -outputfile="C:\Temp\out.json"' wil
```

Note: searches that target users will run for the current user if not-elevated and for ALL users if elevated.

Command Groups

Note: many commands do some type of filtering by default. Supplying the `-full` argument prevents filtering output. Also, the command group `all` will run all current checks.

For example, the following command will run ALL checks and returns ALL output:

```
Seatbelt.exe -group=all -full
```

system

Runs checks that mine interesting data about the system.

Executed with: `Seatbelt.exe -group=system`

Command	Description
AMSIProviders	Providers registered for AMSI
AntiVirus	Registered antivirus (via WMI)
AppLocker	AppLocker settings, if installed
ARPTable	Lists the current ARP table and adapter information(equivalent to arp -a)
AuditPolicies	Enumerates classic and advanced audit policy settings
AuditPolicyRegistry	Audit settings via the registry
AutoRuns	Auto run executables/scripts/programs
Certificates	User and machine personal certificate files
CertificateThumbprints	Thumbprints for all certificate store certs on the system
CredGuard	CredentialGuard configuration
DNSCache	DNS cache entries (via WMI)
DotNet	DotNet versions
EnvironmentPath	Current environment %PATH$ folders and SDDL information
EnvironmentVariables	Current user environment variables
Hotfixes	Installed hotfixes (via WMI)
InterestingProcesses	"Interesting" processes - defensive products and admin tools
InternetSettings	Internet settings including proxy configs
LAPS	LAPS settings, if installed
LastShutdown	Returns the DateTime of the last system shutdown (via the registry)
LocalGPOs	Local Group Policy settings applied to the machine/local users
LocalGroups	Non-empty local groups, "full" displays all groups (argument == computername to enumerate)
LocalUsers	Local users, whether they're active/disabled, and pwd last set (argument == computername to enumerate)
LogonSessions	Logon events (Event ID 4624) from the security event log. Default of 10 days, argument == last X days.
LSASettings	LSA settings (including auth packages)

McAfeeConfigs	Finds McAfee configuration files
NamedPipes	Named pipe names and any readable ACL information
NetworkProfiles	Windows network profiles
NetworkShares	Network shares exposed by the machine (via WMI)
NTLMSettings	NTLM authentication settings
OptionalFeatures	TODO
OSInfo	Basic OS info (i.e. architecture, OS version, etc.)
PoweredOnEvents	Reboot and sleep schedule based on the System event log EIDs 1, 12, 13, 42, and 6008. Default of 7 days, argument == last X days.
PowerShell	PowerShell versions and security settings
Processes	Running processes with file info company names that don't contain 'Microsoft', "full" enumerates all processes
PSSessionSettings	Enumerates PS Session Settings from the registry
RDPSessions	Current incoming RDP sessions (argument == computername to enumerate)
RDPsettings	Remote Desktop Server/Client Settings
SCCM	System Center Configuration Manager (SCCM) settings, if applicable
Services	Services with file info company names that don't contain 'Microsoft', "full" dumps all processes
Sysmon	Sysmon configuration from the registry
TcpConnections	Current TCP connections and their associated processes and services
TokenPrivileges	Currently enabled token privileges (e.g. SeDebugPrivilege/etc.)
UAC	UAC system policies via the registry
UdpConnections	Current UDP connections and associated processes and services
UserRightAssignments	Configured User Right Assignments (e.g. SeDenyNetworkLogonRight, SeShutdownPrivilege, etc.) argument == computername to enumerate
WifiProfile	TODO
WindowsAutoLogon	Registry autologon information
WindowsDefender	Windows Defender settings (including exclusion locations)
WindowsEventForwarding	Windows Event Forwarding (WEF) settings via the registry
WindowsFirewall	Non-standard firewall rules, "full" dumps all (arguments == allow/deny/tcp/udp/in/out/domain/private/public)
WMIEventConsumer	Lists WMI Event Consumers
WMIEventFilter	Lists WMI Event Filters
WMIFilterBinding	Lists WMI Filter to Consumer Bindings

WSUS	Windows Server Update Services (WSUS) settings, if applicable

user

Runs checks that mine interesting data about the currently logged on user (if not elevated) or ALL users (if elevated).

Executed with: `Seatbelt.exe -group=user`

Command	Description
Certificates	User and machine personal certificate files
CertificateThumbprints	Thumbprints for all certificate store certs on the system
ChromiumPresence	Checks if interesting Chrome/Edge/Brave/Opera files exist
CloudCredentials	AWS/Google/Azure cloud credential files
CloudSyncProviders	TODO
CredEnum	Enumerates the current user's saved credentials using CredEnumerate()
dir	Lists files/folders. By default, lists users' downloads, documents, and desktop folders (arguments == <directory> <depth> <regex>
DpapiMasterKeys	List DPAPI master keys
Dsregcmd	TODO
ExplorerMRUs	Explorer most recently used files (last 7 days, argument == last X days)
ExplorerRunCommands	Recent Explorer "run" commands
FileZilla	FileZilla configuration files
FirefoxPresence	Checks if interesting Firefox files exist
IdleTime	Returns the number of seconds since the current user's last input.
IEFavorites	Internet Explorer favorites
IETabs	Open Internet Explorer tabs
IEUrls	Internet Explorer typed URLs (last 7 days, argument == last X days)
KeePass	TODO
MappedDrives	Users' mapped drives (via WMI)
OfficeMRUs	Office most recently used file list (last 7 days)
OneNote	TODO
OracleSQLDeveloper	TODO
PowerShellHistory	Iterates through every local user and attempts to read their PowerShell console history if successful will print it
PuttyHostKeys	Saved Putty SSH host keys
PuttySessions	Saved Putty configuration (interesting fields) and SSH host keys

RDCManFiles	Windows Remote Desktop Connection Manager settings files
RDPSavedConnections	Saved RDP connections stored in the registry
SecPackageCreds	Obtains credentials from security packages
SlackDownloads	Parses any found 'slack-downloads' files
SlackPresence	Checks if interesting Slack files exist
SlackWorkspaces	Parses any found 'slack-workspaces' files
SuperPutty	SuperPutty configuration files
TokenGroups	The current token's local and domain groups
WindowsCredentialFiles	Windows credential DPAPI blobs
WindowsVault	Credentials saved in the Windows Vault (i.e. logins from Internet Explorer and Edge).

misc

Runs all miscellaneous checks.

Executed with: `Seatbelt.exe -group=misc`

Command	Description
ChromiumBookmarks	Parses any found Chrome/Edge/Brave/Opera bookmark files
ChromiumHistory	Parses any found Chrome/Edge/Brave/Opera history files
ExplicitLogonEvents	Explicit Logon events (Event ID 4648) from the security event log. Default of 7 days, argument == last X days.
FileInfo	Information about a file (version information, timestamps, basic PE info, etc. argument(s) == file path(s)
FirefoxHistory	Parses any found FireFox history files
InstalledProducts	Installed products via the registry
InterestingFiles	"Interesting" files matching various patterns in the user's folder. Note: takes non-trivial time.
LogonEvents	Logon events (Event ID 4624) from the security event log. Default of 10 days, argument == last X days.
LOLBAS	Locates Living Off The Land Binaries and Scripts (LOLBAS) on the system. Note: takes non-trivial time.
McAfeeSiteList	Decrypt any found McAfee SiteList.xml configuration files.
MicrosoftUpdates	All Microsoft updates (via COM)
OutlookDownloads	List files downloaded by Outlook
PowerShellEvents	PowerShell script block logs (4104) with sensitive data.
Printers	Installed Printers (via WMI)
ProcessCreationEvents	Process creation logs (4688) with sensitive data.
ProcessOwners	Running non-session 0 process list with owners. For remote use.

RecycleBin	Items in the Recycle Bin deleted in the last 30 days - only works from a user context!
reg	Registry key values (HKLM\Software by default) argument == [Path] [intDepth] [Regex] [boolIgnoreErrors]
RPCMappedEndpoints	Current RPC endpoints mapped
ScheduledTasks	Scheduled tasks (via WMI) that aren't authored by 'Microsoft', "full" dumps all Scheduled tasks
SearchIndex	Query results from the Windows Search Index, default term of 'passsword'. (argument(s) == <search path> <pattern1,pattern2,...>
SecurityPackages	Enumerates the security packages currently available using EnumerateSecurityPackagesA()
SysmonEvents	Sysmon process creation logs (1) with sensitive data.

Additional Command Groups

Executed with: `Seatbelt.exe -group=GROUPNAME`

Alias	Description
Slack	Runs modules that start with "Slack*"
Chromium	Runs modules that start with "Chromium*"
Remote	Runs the following modules (for use against a remote system): AMSIProviders, AntiVirus, AuditPolicyRegistry, ChromiumPresence, CloudCredentials, DNSCache, DotNet, DpapiMasterKeys, EnvironmentVariables, ExplicitLogonEvents, ExplorerRunCommands, FileZilla, Hotfixes, InterestingProcesses, KeePass, LastShutdown, LocalGroups, LocalUsers, LogonEvents, LogonSessions, LSASettings, MappedDrives, NetworkProfiles, NetworkShares, NTLMSettings, OptionalFeatures, OSInfo, PoweredOnEvents, PowerShell, ProcessOwners, PSSessionSettings, PuttyHostKeys, PuttySessions, RDPSavedConnections, RDPSessions, RDPsettings, Sysmon, WindowsDefender, WindowsEventForwarding, WindowsFirewall

Command Arguments

Command that accept arguments have it noted in their description. To pass an argument to a command, enclose the command an arguments in double quotes.

For example, the following command returns 4624 logon events for the last 30 days:

```
Seatbelt.exe "LogonEvents 30"
```

The following command queries a registry three levels deep, returning only keys/valueNames/values that match the regex `.*defini.*`, and ignoring any errors that occur.

```
Seatbelt.exe "reg \"HKLM\SOFTWARE\Microsoft\Windows Defender\" 3 .*defini.* true"
```

Output

Seatbelt can redirect its output to a file with the `-outputfile="C:\Path\file.txt"` argument. If the file path ends in .json, the output will be structured json.

For example, the following command will output the results of system checks to a txt file:

```
Seatbelt.exe -group=system -outputfile="C:\Temp\system.txt"
```

Remote Enumeration

Commands noted with a + in the help menu can be run remotely against another system. This is performed over WMI via queries for WMI classes and WMI's StdRegProv for registry enumeration.

To enumerate a remote system, supply `-computername=COMPUTER.DOMAIN.COM` - an alternate username and password can be specified with `-username=DOMAIN\USER -password=PASSWORD`

For example, the following command runs remote-focused checks against a remote system:

```
Seatbelt.exe -group=remote -computername=192.168.230.209 -username=THESHIRE\sam -password="yum \"po-ta-toes\""
```

Building Your Own Modules

Seatbelt's structure is completely modular, allowing for additional command modules to be dropped into the file structure and loaded up dynamically.

There is a commented command module template at `.\Seatbelt\Commands\Template.cs` for reference. Once built, drop the module in the logical file location, include it in the project in the Visual Studio Solution Explorer, and compile.

Compile Instructions

We are not planning on releasing binaries for Seatbelt, so you will have to compile yourself.

Seatbelt has been built against .NET 3.5 and 4.0 with C# 8.0 features and is compatible with Visual Studio Community Edition. Simply open up the project .sln, choose "release", and build. To change the target .NET framework version, modify the project's settings and rebuild the project.

Acknowledgments

Seatbelt incorporates various collection items, code C# snippets, and bits of PoCs found throughout research for its capabilities. These ideas, snippets, and authors are highlighted in the appropriate locations in the source code, and include:

- @andrewchiles' HostEnum.ps1 script and @tifkin_'s Get-HostProfile.ps1 provided inspiration for many of the artifacts to collect.
- Boboes' code concerning NetLocalGroupGetMembers
- ambyte's code for converting a mapped drive letter to a network path
- Igor Korkhov's code to retrieve current token group information
- RobSiklos' snippet to determine if a host is a virtual machine
- JGU's snippet on file/folder ACL right comparison
- Rod Stephens' pattern for recursive file enumeration
- SwDevMan81's snippet for enumerating current token privileges
- Jared Atkinson's PowerShell work on Kerberos ticket caches
- darkmatter08's Kerberos C# snippet
- Numerous PInvoke.net samples <3
- Jared Hill's awesome CodeProject to use Local Security Authority to Enumerate User Sessions
- Fred's code on querying the ARP cache
- ShuggyCoUk's snippet on querying the TCP connection table

- yizhang82's example of using reflection to interact with COM objects through C#
- @djhohnstein's SharpWeb project
- @djhohnstein's EventLogParser project
- @cmaddalena's SharpCloud project, BSD 3-Clause
- @_RastaMouse's Watson project, GPL License
- @_RastaMouse's Work on AppLocker enumeration
- @peewpw's Invoke-WCMDump project, GPL License
- TrustedSec's HoneyBadger project, BSD 3-Clause
- CENTRAL Solutions's Audit User Rights Assignment Project, No license
- Collection ideas inspired from @ukstufus's Reconerator
- Office MRU locations and timestamp parsing information from Dustin Hurlbut's paper Microsoft Office 2007, 2010 - Registry Artifacts
- The Windows Commands list, used for sensitive regex construction
- Ryan Ries' code for enumeration mapped RPC endpoints
- Chris Haas' post on EnumerateSecurityPackages()
- darkoperator's work on the HoneyBadger project
- @airzero24's work on WMI Registry enumeration
- Alexandru's answer on RegistryKey.OpenBaseKey alternatives
- Tomas Vera's post on JavaScriptSerializer
- Marc Gravell's note on recursively listing files/folders
- @mattifestation's Sysmon rule parser
- Some inspiration from spolnik's Simple.CredentialsManager project, Apache 2 license
- This post on Credential Guard settings
- This thread on network profile information
- Mark McKinnon's post on decoding the DateCreated and DateLastConnected SSID values
- This Specops post on group policy caching
- sa_ddam213's StackOverflow post on enumerating items in the Recycle Bin
- Kirill Osenkov's code for managed assembly detection
- The Mono project for the SecBuffer/SecBufferDesc classes
- Elad Shamir and his Internal-Monologue project, Vincent Le Toux for his DetectPasswordViaNTLMInFlow project, and Lee Christensen for this