Sign in

GhostPack / **Seatbelt** Public

Notifications Fork 687 Star 3.8k

Code Issues 8 Pull requests 1 Actions Projects Security Insights

master

Go to file Code

- .github/ISSUE_TEMPL...
- Seatbelt
- .gitignore
- CHANGELOG.md
- LICENSE
- README.md
- Seatbelt.sln

README License

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.

About

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

csharp situational-awareness

- Readme
- View license
- Activity
- Custom properties
- 3.8k stars
- 106 watching
- 687 forks

Report repository

Releases

No releases published

Packages

No packages published

Contributors 16

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

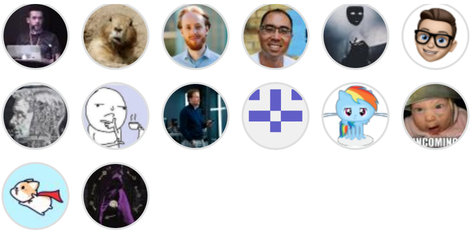
@harmj0y and @tifkin_ are the primary authors of this implementation.

Seatbelt is licensed under the BSD 3-Clause license.

Table of Contents

Command Line Usage

```
                        %&&@@@&&
                        &&&&&&&%%%,
                        &%&   %&%%
%%%%%%%%%%%######%%%#%%####%  &%%**#
#%#%%%%%%%#######%#%%#######  %&%,,,,,,,,,,,,,,.
#%#%%%%%%#####%%#%#%%#######  %%%,,,,,,  ,,.   .
#####%%%####################  &%%......  ...
```



+ 2 contributors

Languages

C# 100.0%

```
#######%##########%#########  %%%......  ...
###%##%#####################  &%%..............
#####%######################  %%%..
                        &%&   %%%%%      Seatbe
                        &%%&&&%%%%%        v1.2
                         #%%%%##,


Available commands (+ means remote usage is sup

    + AMSIProviders          - Providers regist
    + AntiVirus              - Registered antiv
    + AppLocker              - AppLocker settin
      ARPTable               - Lists the curren
      AuditPolicies          - Enumerates class
    + AuditPolicyRegistry    - Audit settings v
    + AutoRuns               - Auto run executa
      azuread                - Return AzureAD i
      Certificates           - Finds user and m
      CertificateThumbprints - Finds thumbprint
    + ChromiumBookmarks      - Parses any found
    + ChromiumHistory        - Parses any found
    + ChromiumPresence       - Checks if intere
    + CloudCredentials       - AWS/Google/Azure
    + CloudSyncProviders     - All configured O
      CredEnum               - Enumerates the c
    + CredGuard              - CredentialGuard
      dir                    - Lists files/fold
    + DNSCache               - DNS cache entrie
    + DotNet                 - DotNet versions
    + DpapiMasterKeys        - List DPAPI maste
      EnvironmentPath        - Current environm
    + EnvironmentVariables   - Current environm
    + ExplicitLogonEvents    - Explicit Logon e
      ExplorerMRUs           - Explorer most re
    + ExplorerRunCommands    - Recent Explorer
      FileInfo               - Information abou
    + FileZilla              - FileZilla config
    + FirefoxHistory         - Parses any found
    + FirefoxPresence        - Checks if intere
    + Hotfixes               - Installed hotfix
      IdleTime               - Returns the numb
    + IEFavorites            - Internet Explore
      IETabs                 - Open Internet Ex
    + IEUrls                 - Internet Explore
    + InstalledProducts      - Installed produc
```

```
      InterestingFiles        - "Interesting" fi
    + InterestingProcesses    - "Interesting" pr
      InternetSettings        - Internet setting
    + KeePass                 - Finds KeePass co
    + LAPS                    - LAPS settings, i
    + LastShutdown            - Returns the Date
      LocalGPOs               - Local Group Poli
    + LocalGroups             - Non-empty local
    + LocalUsers              - Local users, whe
    + LogonEvents             - Logon events (Ev
    + LogonSessions           - Windows logon se
      LOLBAS                  - Locates Living O
    + LSASettings             - LSA settings (in
    + MappedDrives            - Users' mapped dr
      McAfeeConfigs           - Finds McAfee con
      McAfeeSiteList          - Decrypt any foun
      MicrosoftUpdates        - All Microsoft up
      MTPuTTY                 - MTPuTTY configur
      NamedPipes              - Named pipe names
    + NetworkProfiles         - Windows network
    + NetworkShares           - Network shares e
    + NTLMSettings            - NTLM authenticat
      OfficeMRUs              - Office most rece
      OneNote                 - List OneNote bac
    + OptionalFeatures        - List Optional Fe
      OracleSQLDeveloper      - Finds Oracle SQL
    + OSInfo                  - Basic OS info (i
    + OutlookDownloads        - List files downl
    + PoweredOnEvents         - Reboot and sleep
    + PowerShell              - PowerShell versi
    + PowerShellEvents        - PowerShell scrip
    + PowerShellHistory       - Searches PowerSh
      Printers                - Installed Printe
    + ProcessCreationEvents   - Process creation
      Processes               - Running processe
    + ProcessOwners           - Running non-sess
    + PSSessionSettings       - Enumerates PS Se
    + PuttyHostKeys           - Saved Putty SSH
    + PuttySessions           - Saved Putty conf
      RDCManFiles             - Windows Remote D
    + RDPSavedConnections     - Saved RDP connec
    + RDPSessions             - Current incoming
    + RDPsettings             - Remote Desktop S
      RecycleBin              - Items in the Rec
      reg                     - Registry key val
      RPCMappedEndpoints      - Current RPC endp
    + SCCM                    - System Center Co
    + ScheduledTasks          - Scheduled tasks
      SearchIndex             - Query results fr
      SecPackageCreds         - Obtains credenti
    + SecureBoot              - Secure Boot conf
      SecurityPackages        - Enumerates the s
      Services                - Services with fi
    + SlackDownloads          - Parses any found
    + SlackPresence           - Checks if intere
    + SlackWorkspaces         - Parses any found
    + SuperPutty              - SuperPutty confi
    + Sysmon                  - Sysmon configura
    + SysmonEvents            - Sysmon process c
      TcpConnections          - Current TCP conn
      TokenGroups             - The current toke
      TokenPrivileges         - Currently enable
    + UAC                     - UAC system polic
      UdpConnections          - Current UDP conn
      UserRightAssignments    - Configured User
      WifiProfile             - Enumerates the s
    + WindowsAutoLogon        - Registry autolog
      WindowsCredentialFiles - Windows credenti
    + WindowsDefender         - Windows Defender
    + WindowsEventForwarding - Windows Event Fo
    + WindowsFirewall         - Non-standard fir
      WindowsVault            - Credentials save
    + WMI                     - Runs a specified
      WMIEventConsumer        - Lists WMI Event
      WMIEventFilter          - Lists WMI Event
      WMIFilterBinding        - Lists WMI Filter
    + WSUS                    - Windows Server U


Seatbelt has the following command groups: All,

    You can invoke command groups with


    Or command groups except specific commands

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

   "Seatbelt.exe -group=user" runs the followin

        azuread, Certificates, CertificateThumb
        CloudSyncProviders, CredEnum, dir, Dpap
```

```
         ExplorerMRUs, ExplorerRunCommands, FileZ
         IdleTime, IEFavorites, IETabs, IEUrls,
         KeePass, MappedDrives, MTPuTTY, OfficeM
         OneNote, OracleSQLDeveloper, PowerShellH
         PuttySessions, RDCManFiles, RDPSavedConn
         SlackDownloads, SlackPresence, SlackWork
         TokenGroups, WindowsCredentialFiles, Win

    "Seatbelt.exe -group=system" runs the follow

         AMSIProviders, AntiVirus, AppLocker, ARP
         AuditPolicyRegistry, AutoRuns, Certifica
         CredGuard, DNSCache, DotNet, Environment
         EnvironmentVariables, Hotfixes, Interest
         LAPS, LastShutdown, LocalGPOs, LocalGrou
         LocalUsers, LogonSessions, LSASettings,
         NamedPipes, NetworkProfiles, NetworkShar
         OptionalFeatures, OSInfo, PoweredOnEvent
         Processes, PSSessionSettings, RDPSession
         SCCM, SecureBoot, Services, Sysmon,
         TcpConnections, TokenPrivileges, UAC, Us
         UserRightAssignments, WifiProfile, Windo
         WindowsEventForwarding, WindowsFirewall,
         WMIEventFilter, WMIFilterBinding, WSUS

    "Seatbelt.exe -group=slack" runs the followin

         SlackDownloads, SlackPresence, SlackWork

    "Seatbelt.exe -group=chromium" runs the follo

         ChromiumBookmarks, ChromiumHistory, Chro

    "Seatbelt.exe -group=remote" runs the follow

         AMSIProviders, AntiVirus, AuditPolicyReg
         DNSCache, DotNet, DpapiMasterKeys, Envir
         ExplicitLogonEvents, ExplorerRunCommands
         InterestingProcesses, KeePass, LastShutd
         LocalUsers, LogonEvents, LogonSessions,
         MappedDrives, NetworkProfiles, NetworkSh
         OptionalFeatures, OSInfo, PoweredOnEvent
         ProcessOwners, PSSessionSettings, PuttyH
         RDPSavedConnections, RDPSessions, RDPset
         Sysmon, WindowsDefender, WindowsEventFor
    "Seatbelt.exe -group=misc" runs the followin

         ChromiumBookmarks, ChromiumHistory, Exp
         InstalledProducts, InterestingFiles, Lo
         McAfeeSiteList, MicrosoftUpdates, Outlo
         Printers, ProcessCreationEvents, Proces
         reg, RPCMappedEndpoints, ScheduledTasks
         SecurityPackages, SysmonEvents


Examples:
    'Seatbelt.exe <Command> [Command2] ...' wil
    'Seatbelt.exe <Command> -full' will return 
    'Seatbelt.exe "<Command> [argument]"' will 
    'Seatbelt.exe -group=all' will run ALL enum
    'Seatbelt.exe -group=all -AuditPolicies' wi
    'Seatbelt.exe <Command> -computername=COMPU
    'Seatbelt.exe -group=remote -computername=C
    'Seatbelt.exe -group=system -outputfile="C:
    'Seatbelt.exe -group=user -q -outputfile="C
```

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	Descriptior
AMSIProviders	Providers registered for AMSI
AntiVirus	Registered antivirus (via WMI)
AppLocker	AppLocker settings, if installed
ARPTable	Lists the current ARP table and information(equivalent to arp -
AuditPolicies	Enumerates classic and advanc settings
AuditPolicyRegistry	Audit settings via the registry
AutoRuns	Auto run executables/scripts/pr
Certificates	User and machine personal cer
CertificateThumbprints	Thumbprints for all certificate s system
CredGuard	CredentialGuard configuration
DNSCache	DNS cache entries (via WMI)
DotNet	DotNet versions
EnvironmentPath	Current environment %PATH$ f information
EnvironmentVariables	Current user environment varia
Hotfixes	Installed hotfixes (via WMI)
InterestingProcesses	"Interesting" processes - defens admin tools
InternetSettings	Internet settings including prox
LAPS	LAPS settings, if installed
LastShutdown	Returns the DateTime of the las (via the registry)

LocalGPOs	Local Group Policy settings app machine/local users
LocalGroups	Non-empty local groups, "full" (argument == computername
LocalUsers	Local users, whether they're act pwd last set (argument == com enumerate)
LogonSessions	Logon events (Event ID 4624) f event log. Default of 10 days, a days.
LSASettings	LSA settings (including auth pa
McAfeeConfigs	Finds McAfee configuration file
NamedPipes	Named pipe names and any re information
NetworkProfiles	Windows network profiles
NetworkShares	Network shares exposed by the
NTLMSettings	NTLM authentication settings
OptionalFeatures	TODO
OSInfo	Basic OS info (i.e. architecture,
PoweredOnEvents	Reboot and sleep schedule bas event log EIDs 1, 12, 13, 42, and days, argument == last X days.
PowerShell	PowerShell versions and securi
Processes	Running processes with file inf that don't contain 'Microsoft', " processes
PSSessionSettings	Enumerates PS Session Setting

RDPSessions	Current incoming RDP sessions computername to enumerate)
RDPsettings	Remote Desktop Server/Client
SCCM	System Center Configuration M settings, if applicable
Services	Services with file info company contain 'Microsoft', "full" dump
Sysmon	Sysmon configuration from the
TcpConnections	Current TCP connections and th processes and services
TokenPrivileges	Currently enabled token privile SeDebugPrivilege/etc.)
UAC	UAC system policies via the reg
UdpConnections	Current UDP connections and a processes and services
UserRightAssignments	Configured User Right Assignm SeDenyNetworkLogonRight, SeShutdownPrivilege, etc.) argu computername to enumerate
WifiProfile	TODO
WindowsAutoLogon	Registry autologon information
WindowsDefender	Windows Defender settings (in locations)
WindowsEventForwarding	Windows Event Forwarding (W registry
WindowsFirewall	Non-standard firewall rules, "fu (arguments == allow/deny/tcp/udp/in/out/dor
WMIEventConsumer	Lists WMI Event Consumers

WMIEventFilter	Lists WMI Event Filters
WMIFilterBinding	Lists WMI Filter to Consumer B
WSUS	Windows Server Update Servic 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

Terms Privacy Security Status Docs Contact Manage cookies Do not share my personal information

© 2024 GitHub, Inc.