GitHub - BloodHoundAD/SharpHound3: C# Data Collector for the BloodHound Project, Version 3

By rvazarkar

Archived: 2026-04-05 18:32:32 UTC

THIS IS NOW DEPRECATED IN FAVOR OF SHARPHOUND. DATA COLLECTED USING THIS METHOD WILL NOT WORK WITH BLOODHOUND 4.1+

SharpHound - C# Rewrite of the BloodHound Ingestor

Get SharpHound

The latest build of SharpHound will always be in the BloodHound repository here

Compile Instructions

SharpHound is written using C# 9.0 features. To easily compile this project, use Visual Studio 2019.

If you would like to compile on previous versions of Visual Studio, you can install the Microsoft.Net.Compilers nuget package.

Building the project will generate an executable as well as a PowerShell script that encapsulates the executable. All dependencies are rolled into the binary.

Requirements

SharpHound is designed targetting .Net 4.5. Sharphound must be run from the context of a domain user, either directly through a logon or through another method such as RUNAS.

More Information

Usage

Enumeration Options

- **CollectionMethod** - The collection method to use. This parameter accepts a comma separated list of values. Has the following potential values (Default: Default):
    - **Default** - Performs group membership collection, domain trust collection, local group collection, session collection, ACL collection, object property collection, and SPN target collection

    - **Group** - Performs group membership collection
    - **LocalAdmin** - Performs local admin collection
    - **RDP** - Performs Remote Desktop Users collection
    - **DCOM** - Performs Distributed COM Users collection
    - **PSRemote** - Performs Remote Management Users collection
    - **GPOLocalGroup** - Performs local admin collection using Group Policy Objects
    - **Session** - Performs session collection
    - **ComputerOnly** - Performs local admin, RDP, DCOM and session collection
    - **LoggedOn** - Performs privileged session collection (requires admin rights on target systems)
    - **Trusts** - Performs domain trust enumeration
    - **ACL** - Performs collection of ACLs
    - **Container** - Performs collection of Containers
    - **DcOnly** - Performs collection using LDAP only. Includes Group, Trusts, ACL, ObjectProps, Container, and GPOLocalGroup.
    - **ObjectProps** - Performs Object Properties collection for properties such as LastLogon or PwdLastSet
    - **All** - Performs all Collection Methods except GPOLocalGroup
- **Domain** - Search a particular domain. Uses your current domain if null (Default: null)
- **Stealth** - Performs stealth collection methods. All stealth options are single threaded.
- **ExcludeDomainControllers** - Excludes domain controllers from enumeration (avoids Microsoft ATA flags :))
- **ComputerFile** - Specify a file to load computer names/IPs from
- **LdapFilter** - LDAP Filter to apppend to search
- **OverrideUserName** - Overrides user name for session enumeration (advanced)
- **RealDNSName** - Overrides DNS name for API calls
- **CollectAllProperties** - Collect all string LDAP properties instead of a subset
- **WindowsOnly** - Limit computer collection to systems with an operating system that matches *Windows*

Loop Options

- **Loop** - Loop computer collections
- **LoopDuration** - How long to loop for
- **LoopInterval** - Duration to wait between loops

Connection Options

- **DomainController** - Specify which Domain Controller to connect to (Default: null)
- **LdapPort** - Specify what port LDAP lives on (Default: 0)
- **SecureLdap** - Connect to AD using Secure LDAP instead of regular LDAP. Will connect to port 636 by default.
- **LdapUsername** - Username to connect to LDAP with. Requires the LDAPPassword parameter as well (Default: null)

- **LdapPassword** - Password for the user to connect to LDAP with. Requires the LDAPUser parameter as well (Default: null)
- **DisableKerberosSigning** - Disables LDAP encryption. Not recommended.

Performance Options

- **PortScanTimeout** - Specifies the timeout for ping requests in milliseconds (Default: 2000)
- **SkipPortScan** - Instructs Sharphound to skip ping requests to see if systems are up
- **Throttle** - Adds a delay after each request to a computer. Value is in milliseconds (Default: 0)
- **Jitter** - Adds a percentage jitter to throttle. (Default: 0)

Output Options

- **OutputDirectory** - Folder in which to store JSON files (Default: .)
- **OutputPrefix** - Prefix to add to your JSON files (Default: "")
- **NoZip** - Don't compress JSON files to the zip file. Leaves JSON files on disk. (Default: false)
- **EncryptZip** - Add a randomly generated password to the zip file.
- **ZipFileName** - Specify the name of the zip file
- **RandomizeFilenames** - Randomize output file names
- **PrettyJson** - Outputs JSON with indentation on multiple lines to improve readability. Tradeoff is increased file size.
- **DumpComputerStatus** - Dumps error codes from connecting to computers

Cache Options

- **CacheFileName** - Filename for the Sharphound cache. (Default: .bin)
- **NoSaveCache** - Don't save the cache file to disk. Without this flag, .bin will be dropped to disk
- **InvalidateCache** - Invalidate the cache file and build a new cache

Misc Options

- **StatusInterval** - Interval to display progress during enumeration in milliseconds (Default: 30000)
