Veil - Framework

- The Veil-Framework

Veil-Evasion Veil-Ordnance Veil-Catapult PowerTools Veil-Pillage

- Guides/Videos
- Repository

Hunting for Sensitive Data with the Veil-Framework

July 22, 2014 by Harm J0y

Data mining available file shares for sensitive data is a staple of red teaming. We've found everything from password lists, to full employee directories, salary information, network diagrams and more, all due to network shares with incorrectly configured permissions. Veil-PowerView has a few functions (Invoke-Netview and Invoke-Sharefinder) that have helped us quickly find and explore shares our current user has access to. I've talked in the past about using Powershell to triage file servers during engagements, and realized that robust, recursive file listing would make a great addition into PowerView. Those two functions (Invoke-SearchFiles and Invoke-FileFinder) were recently added, and I wanted to demonstrate how this new functionality can help you find sensitive files on the network as quickly as possible.

Invoke-ShareFinder has had its output recently reworked so it spits out any "\\HOST\share – COMMENT" found, instead of the status output similar to Invoke-Netview. The reason for this is to easily chain together Invoke-ShareFinder and Invoke-FileFinder, while preserving as much information we might want as possible. Here's how I usually run sharefinder:

- PS C:\> Invoke-ShareFinder -Ping -CheckShareAccess -Verbose | Out-File -Encoding ascii found_shares.txt

This will query AD for all machine objects, ping each one to ensure the host is up before enumeration, check each found share for read access, and output everything to found_shares.txt. The -Verbose flag gives some status output as it chews through all the retrieved servers, and the output will look something like this:

```
\\WIN2K8.company.com\MSBuild    - test
\\WIN2K8.company.com\NETLOGON   - Logon server share
\\WIN2K8.company.com\SYSVOL     - Logon server share
\\WIN2K8.company.com\test       -
\\WIN2K8.company.com\Users      - User share
\\WINDOWS7.company.com\secret   - don't look here
...snip...
```

I’ll save off an original copy of the file off for reference, and then will glance over the output, manually trimming out certain shares that seem like they likely won’t be interesting. I can then feed that output file straight into Invoke-FileFinder. This will recursively search given shares for sensitive files:

- PS C:> Invoke-FileFinder -ShareList .\found_shares.txt -OutFile found_files.csv

This will take the share input list from sharefinder and recursively list each share, filtering for files with ‘*pass*’, ‘*sensitive*’, ‘*admin*’, ‘*secret*’, ‘*login*’, ‘*unattend*.xml’, ‘*.vmdk’, ‘*creds*’, or ‘*credential*’ in the file name. Anything found is then output to a CSV with the full path, owner, last access time, last write time, and length. If I want/need to search for other terms, I’ll use something like this:

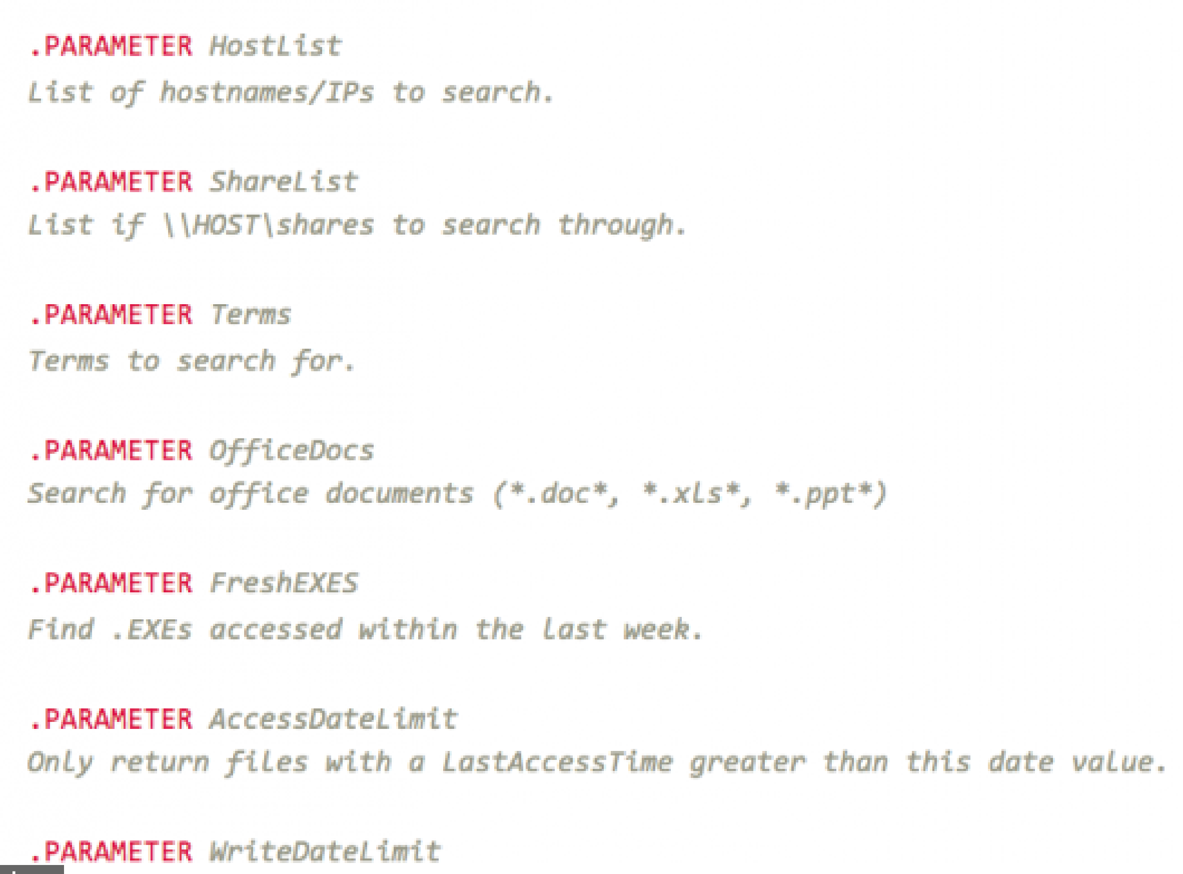
- PS C:> Invoke-FileFinder -ShareList .\found_shares.txt -OutFile found_files.csv -Terms payroll,CEO,…

This will replace the default terms with the wildcarded terms specified. If you want to run Invoke-FileFinder without enumerating shares ahead of time, the following function will query

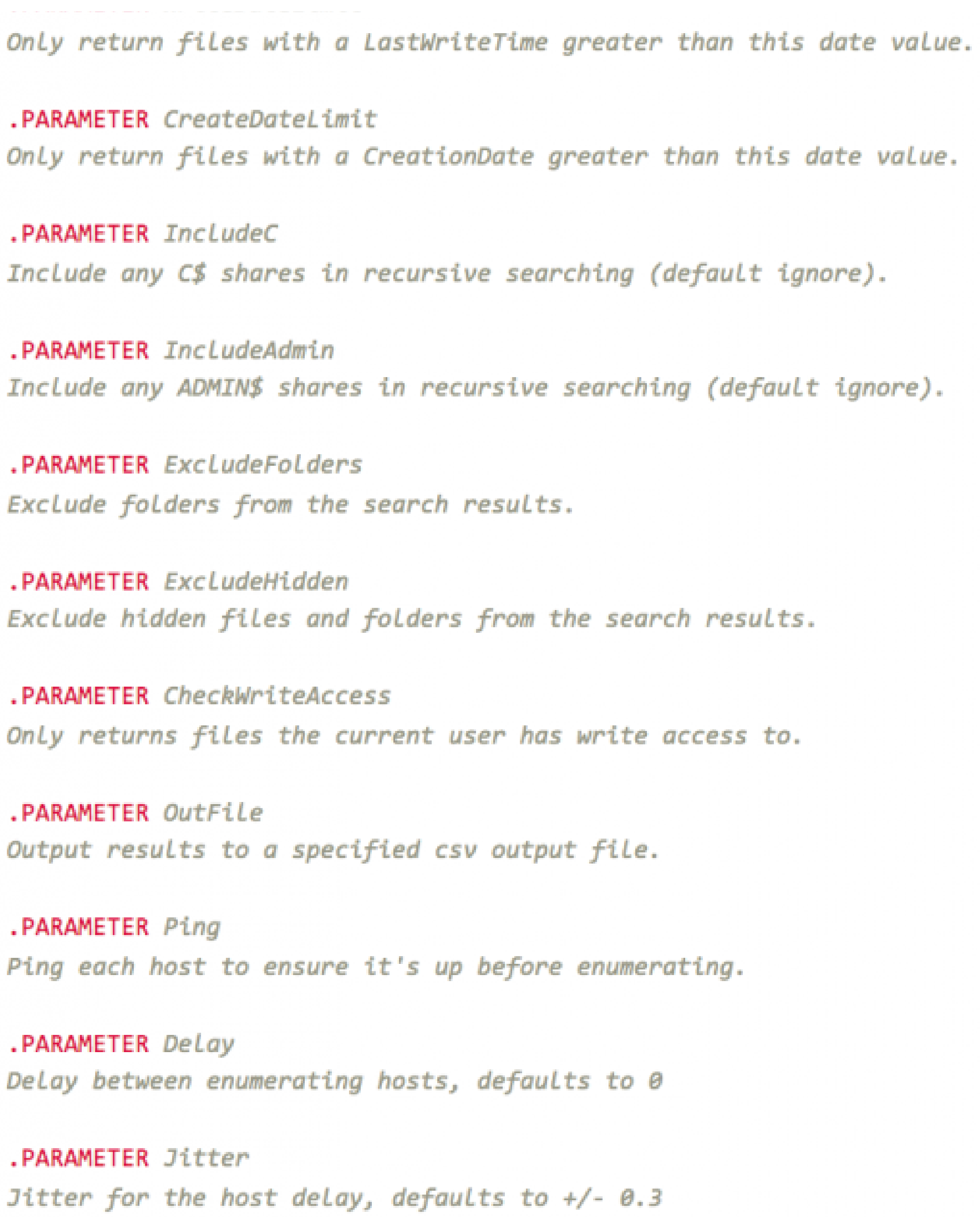
AD for active machines like the rest of PowerView's Invoke-* cmdlets. It will then enumerate all shares it finds, excluding C$ and ADMIN$ by default (these can be included with the -IncludeC and -IncludeAdmin flags). I still advise running Invoke-ShareFinder first and pruning your results a bit for speed reasons, but kicking off the following command will find everything sensitive it can in the network:

- PS C:> Invoke-FileFinder -OutFile all_files.csv -Verbose

There are several more flags available, including filters for office documents, last creation/write/access times, etc. Check out Invoke-FileFinder's function documentation if you're interested in more of the options:



```
.PARAMETER HostList
List of hostnames/IPs to search.

.PARAMETER ShareList
List if \\HOST\shares to search through.

.PARAMETER Terms
Terms to search for.

.PARAMETER OfficeDocs
Search for office documents (*.doc*, *.xls*, *.ppt*)

.PARAMETER FreshEXES
Find .EXEs accessed within the last week.

.PARAMETER AccessDateLimit
Only return files with a LastAccessTime greater than this date value.

.PARAMETER WriteDateLimit
```



```
Only return files with a LastWriteTime greater than this date value.

.PARAMETER CreateDateLimit
Only return files with a CreationDate greater than this date value.

.PARAMETER IncludeC
Include any C$ shares in recursive searching (default ignore).

.PARAMETER IncludeAdmin
Include any ADMIN$ shares in recursive searching (default ignore).

.PARAMETER ExcludeFolders
Exclude folders from the search results.

.PARAMETER ExcludeHidden
Exclude hidden files and folders from the search results.

.PARAMETER CheckWriteAccess
Only returns files the current user has write access to.

.PARAMETER OutFile
Output results to a specified csv output file.

.PARAMETER Ping
Ping each host to ensure it's up before enumerating.

.PARAMETER Delay
Delay between enumerating hosts, defaults to 0

.PARAMETER Jitter
Jitter for the host delay, defaults to +/- 0.3
```

Happy hunting :)

Share this:

Share

This entry was posted in Informational, Veil-Powerview and tagged Veil-Powerview. Bookmark the permalink.

← July 15th V-Day

August 15th V-Day: Smash and Pillage →

2 thoughts on “Hunting for Sensitive Data with the Veil-Framework”

Pingback: Veil – Framework - Meta Thrunks Security Blog

Robin Wood says:

May 6, 2015 at 4:39 pm

To save anyone else reporting it, the -Ping argument has been removed from Invoke-ShareFinder and it is now the default action.

Reply

Leave a Reply

Enter your comment here...

Search …

Follow me on Twitter

My Tweets

Recent Posts

- A Perl of Hope – January V-Day 2016
- November 2015 V-Day
- September 2015 V-Day
- June 2015 V-Day!
- On Your Mark, Get Set, Go! – May V-Day

Recent Comments

- Braz on A Perl of Hope – January V-Day 2016
- George on Self-Expiring Payloads
- Use Cobalt Strike's Beacon with Veil's Evasion | Strategic Cyber LLC on How to use Cobalt Strike's Beacon with Veil
- Brandon on Veil-Evasion
- Common Windows Privilege Escalation Vectors | Smart PC Expert-Service PC Online on Veil-Evasion

running on WordPress | Theme: Mog by hndr.