threatexpress / **red-team-scripts**

Watch 15 Star 173 Fork 41

Code Issues 0 Pull requests 0 Projects 0 Insights

A collection of Red Team focused tools, scripts, and notes

11 commits **1** branch **0** releases **2** contributors

Branch: **master** New pull request Find file Clone or download

joevest Beacon Handler Latest commit `b9a6e5d` on Jan 29

beacon-handler	Beacon Handler	4 months ago
.gitignore	Update .gitignore	a year ago

HostEnum.ps1	Cleanup README and remove unused function	4 months ago
LICENSE	Update LICENSE language to reflect BSD-3-Clause	4 months ago
README.md	Cleanup README and remove unused function	4 months ago
hostenum.py	Change function outputs to PS objects vs strings (mostly)	4 months ago

README.md

Red Team Scripts

Red Team Scripts is a collection of red teaming related tools, scripts, techniques, and notes developed or discovered over time during engagements. Related tool release blog posts can be found at Threat Express an Information Security and Red Teaming Blog

Situational Awareness

Perform situational awareness on a local host or domain upon initial compromise.

`Invoke-HostEnum`

Author: Andrew Chiles (@andrewchiles) with code by harmj0y, Joe Bialek, rvrsh3ll, Beau Bullock, Tim Medin

A PowerShell v2.0 compatible script comprised of multiple system enumeration / situational awareness techniques collected over time. If system is a member of a Windows domain, it can also perform limited domain enumeration with the -Domain switch. However, domain enumeration is significantly limited with the intention that PowerView or BoodHound could also be used.

Enumerated Information:

- OS Details, Hostname, Uptime, Installdate
- Installed Applications and Patches
- Network Adapter Configuration, Network Shares, Connections, Routing Table, DNS Cache
- Running Processes and Installed Services
- Interesting Registry Entries
- Local Users, Groups, Administrators
- Personal Security Product Status
- Interesting file locations and keyword searches via file indexing
- Interesting Windows Logs (User logins)
- Basic Domain enumeration (users, groups, trusts, domain controllers, account policy, SPNs)

Privilege Escalation

Optionally performs Privilege Escalation functions from PowerUp in the PowerSploit project.

Empire 2.0 Integration

Use the accompanying hostenum.py script to include Invoke-HostEnum as post-exploitation situational awarness module in Empire. Both files need to be copied to the appropriate locations in Empire.

Credits:

Several functions are inspired or pulled directly from the following projects and are referenced in the code where applicable:

- Invoke-HostRecon by Beau Bullock
- Get-ComputerDetails from Joe Bialek in PowerSploit
- Get-BrowserInformation by rvrsh3ll
- Get-UserSPNS by Tim Medin
- PowerUp by @harmj0y

Usage

Refer to the help and comments in each script for detailed usage information.

License

This project and all individual scripts are under the BSD 3-Clause license

Links

threatexpress.com http://threatexpress.com/2018/01/hostenum-updates-usage/ http://threatexpress.com/2017/05/invoke-hostenum/