

Product

Solutions

Resources

Open Source

Enterprise

Pricing

Sign in

Sign up

redcanaryco / atomic-red-team

Public

Notifications

Fork2.8k

Star9.7k

<>Code

Issues6

Pull requests5

Actions

Wiki

Security

Insights

atomic-red-team / atomics / T1110.002 / T1110.002.md

Atomic Red Team doc generat...

Generated docs from job=generate-d...819934c · 2 years ago

History

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

atomic-red-team / atomics / T1110.002 / T1110.002.md

↑Top

PreviewCodeBlame

71 lines (45 loc) · 3.23 KB

RawCopyDownloadMenu

Atomic tests

- [Atomic Test #1 - Password Cracking with Hashcat](#)

Atomic Test #1 - Password Cracking with Hashcat

Execute Hashcat.exe with provided SAM file from registry of Windows and Password list to crack against

Supported Platforms: Windows

auto_generated_guid: 6d27df5d-69d4-4c91-bc33-5983ffe91692

Inputs:

Name	Description	Type	Default Value
hashcat_exe	Path to Hashcat executable	String	%temp%\hashcat6\hashcat-6.1.1\hashc
input_file_sam	Path to SAM file	String	PathToAtomicsFolder\T1110.002\src\sa


























T1110.002 - Password Cracking

Description from ATT&CK

Adversaries may use password cracking to attempt to recover usable credentials, such as plaintext passwords, when credential material such as password hashes are obtained. [OS Credential Dumping](https://attack.mitre.org/techniques/T1003) can be used to obtain password hashes, this may only get an adversary so far when [Pass the Hash](https://attack.mitre.org/techniques/T1550/002) is not an option. Further, adversaries may leverage [Data from Configuration Repository](https://attack.mitre.org/techniques/T1602) in order to obtain hashed credentials for network devices.(Citation: US-CERT-TA18-106A)

Techniques to systematically guess the passwords used to compute hashes are available, or the adversary may use a pre-computed rainbow table to crack hashes. Cracking hashes is usually done on adversary-controlled systems outside of the target network.(Citation: Wikipedia Password cracking) The resulting plaintext password

Page 1 of 2

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

input_file_passwords	Path to password list	String	PathToAtomicsFolder\T1110.002\src\pa
----------------------	-----------------------	--------	--------------------------------------

Attack Commands: Run with `command_prompt` ! Elevation Required (e.g. root or admin)

```
cd #{hashcat_exe}\..  
#{hashcat_exe} -a 0 -m 1000 -r .\rules\Incisive-leetspeak.rule #{input_f
```

Cleanup Commands:

```
del %temp%\hashcat6.7z >nul 2>&1  
del %temp%\7z1900.exe >nul 2>&1  
del %temp%\7z /Q /S >nul 2>&1  
del %temp%\hashcat-unzip /Q /S >nul 2>&1
```

Dependencies: Run with `powershell` !

Description: Hashcat must exist on disk at specified location (#{hashcat_exe})

Check Prereq Commands:

```
if (Test-Path $(cmd /c echo #{hashcat_exe})) {exit 0} else {exit 1}
```

Get Prereq Commands:

```
Invoke-WebRequest "https://www.7-zip.org/a/7z1900.exe" -OutFile "$env:TE  
Start-Process -FilePath "$env:Temp\7z1900.exe" -ArgumentList "/S /D=$env  
Invoke-WebRequest "https://hashcat.net/files/hashcat-6.1.1.7z" -OutFile  
Start-Process cmd.exe -Args "/c %temp%\7z\7z.exe x %temp%\hashcat6.7z -  
New-Item -ItemType Directory (Split-Path $(cmd /c echo #{hashcat_exe}))  
Move-Item $env:Temp\hashcat-unzip\hashcat-6.1.1\* $(cmd /c echo #{hashca
```