

71 lines (45 loc) · 3.23 KB

# 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 resulting from a successfully cracked hash may be used to log into systems, resources, and services in which the account has access.

## Atomic Tests

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

Preview

Code

Blame

Raw



## 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\hashcat.exe
input_file_sam	Path to SAM file	String	PathToAtomicsFolder\T1110.002\src\sam.txt
input_file_passwords	Path to password list	String	PathToAtomicsFolder\T1110.002\src\password.lst

**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_file_sam} #
```



**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 "$env:TEMP\7z1900.exe"
Start-Process -FilePath "$env:Temp\7z1900.exe" -ArgumentList "/S /D=$env:temp\7zi"
Invoke-WebRequest "https://hashcat.net/files/hashcat-6.1.1.7z" -OutFile "$env:TEMP\hashcat-6.1.1.7z"
Start-Process cmd.exe -Args "/c %temp%\7z\7z.exe x %temp%\hashcat6.7z -aoa -o%temp%\hashcat-unzip"
New-Item -ItemType Directory (Split-Path $(cmd /c echo #{hashcat_exe})) -Force | Out-Null
Move-Item $env:Temp\hashcat-unzip\hashcat-6.1.1\* $(cmd /c echo #{hashcat_exe}\..)
```

