

# T1007 - System Service Discovery

## **Description from ATT&CK**

Adversaries may try to gather information about registered local system services. Adversaries may obtain information about services using tools as well as OS utility commands such as sc query , tasklist /svc , systemctl --type=service , and net start .

Adversaries may use the information from <u>System Service Discovery</u> during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

## **Atomic Tests**

- Atomic Test #1 System Service Discovery
- Atomic Test #2 System Service Discovery net.exe
- Atomic Test #3 System Service Discovery systemctl

# Atomic Test #1 - System Service Discovery

Identify system services.

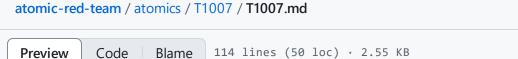
Upon successful execution, cmd.exe will execute service commands with expected result to stdout.

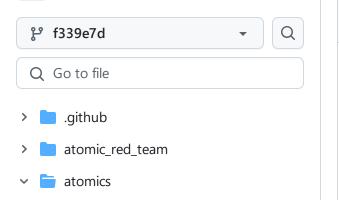
**Supported Platforms:** Windows

auto\_generated\_guid: 89676ba1-b1f8-47ee-b940-2e1a113ebc71

Attack Commands: Run with command\_prompt! Elevation Required (e.g. root or admin)

Raw [ 🖵 🔽





**●** Files

Indexes

T1003.001

Atomic Test #2 - System Service Discovery - net.exe



T1036

T1037.001

> T1037.002

> T1037.004

> T1037.005

Enumerates started system services using net.exe and writes them to a file. This technique has been used by multiple threat actors.

Upon successful execution, net.exe will run from cmd.exe that queries services. Expected output is to a txt file in c:\Windows\Temp\service-list.txt.s

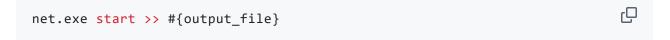
Supported Platforms: Windows

auto\_generated\_guid: 5f864a3f-8ce9-45c0-812c-bdf7d8aeacc3

#### Inputs:

Name	Description	Туре	Default Value
output_file	Path of file to hold net.exe output	Path	C:\Windows\Temp\service- list.txt

### Attack Commands: Run with command\_prompt!



### Cleanup Commands:

del /f /q /s #{output\_file} >nul 2>&1

## Atomic Test #3 - System Service Discovery - systemctl

Enumerates system service using systemctl

Supported Platforms: Linux

auto\_generated\_guid: f4b26bce-4c2c-46c0-bcc5-fce062d38bef

Attack Commands: Run with bash!

systemctl --type=service