

# T1057 - Process Discovery

# **Description from ATT&CK**

Adversaries may attempt to get information about running processes on a system. Information obtained could be used to gain an understanding of common software/applications running on systems within the network. Adversaries may use the information from [Process Discovery](https://attack.mitre.org/techniques/T1057) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. In Windows environments, adversaries could obtain details on running processes using the Tasklist utility via cmd or Get-Process via PowerShell. Information about processes can also be extracted from the output of Native API calls such as CreateToo1he1p32Snapshot. In Mac and Linux, this is accomplished with the ps command. Adversaries may also opt to enumerate processes via /proc.

#### **Atomic Tests**

- Atomic Test #1 Process Discovery ps
- Atomic Test #2 Process Discovery tasklist
- Atomic Test #3 Process Discovery Get-Process
- Atomic Test #4 Process Discovery get-wmiObject
- Atomic Test #5 Process Discovery wmic process

### Atomic Test #1 - Process Discovery - ps

Utilize ps to identify processes.

Upon successful execution, sh will execute ps and output to /tmp/loot.txt.

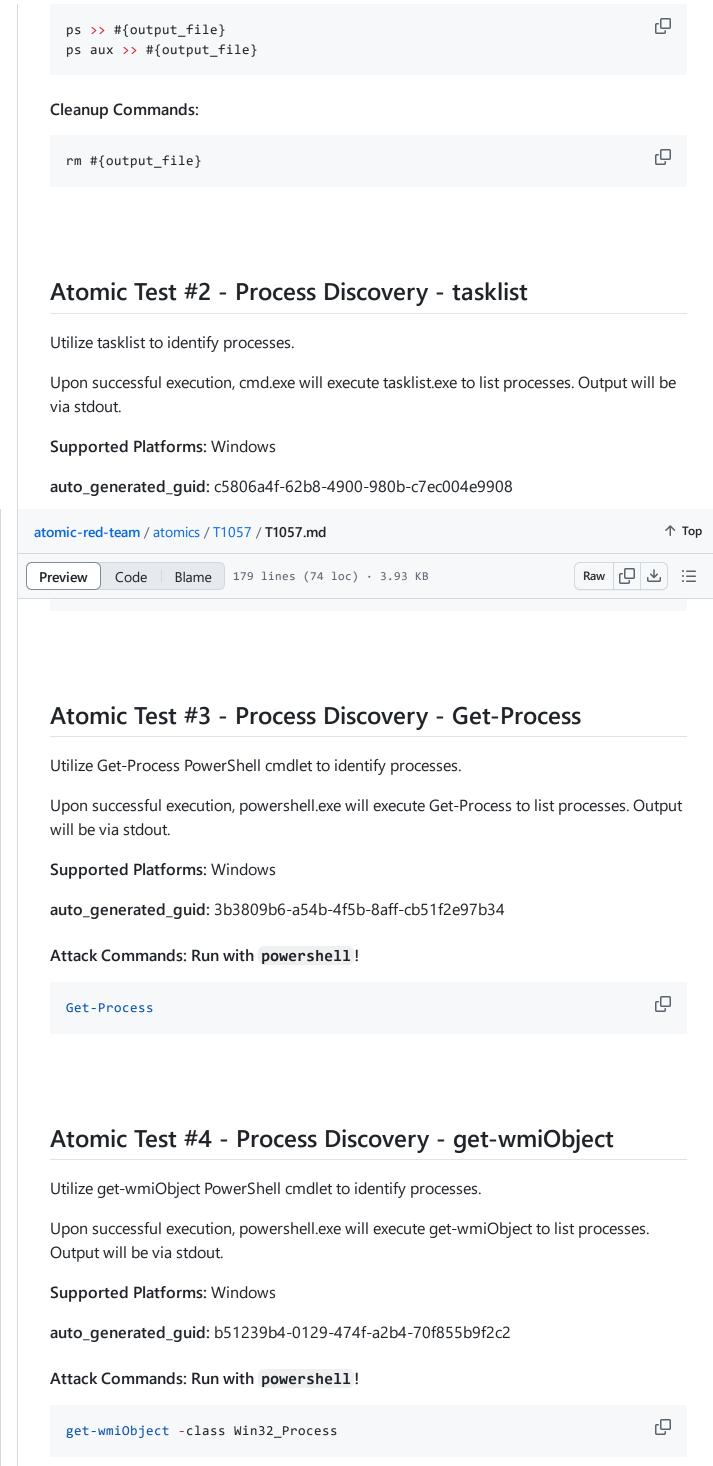
Supported Platforms: macOS, Linux

auto\_generated\_guid: 4ff64f0b-aaf2-4866-b39d-38d9791407cc

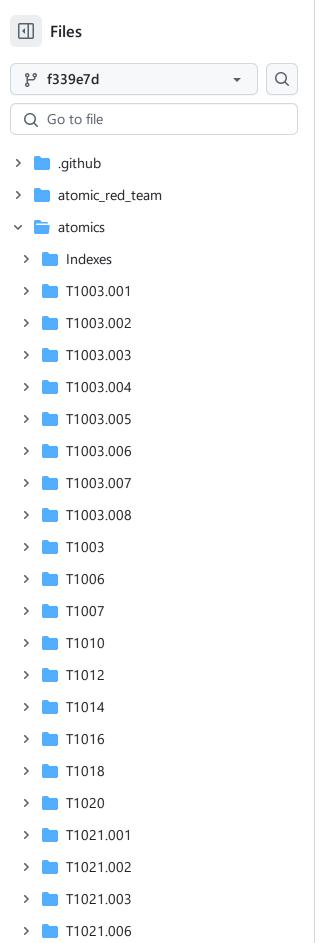
### Inputs:

Name	Description	Туре	Default Value
output_file	path of output file	path	/tmp/loot.txt

Attack Commands: Run with sh!



Page 2 of 3



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

# Atomic Test #5 - Process Discovery - wmic process

Utilize windows management instrumentation to identify processes.

Upon successful execution, WMIC will execute process to list processes. Output will be via stdout.

**Supported Platforms:** Windows

auto\_generated\_guid: 640cbf6d-659b-498b-ba53-f6dd1a1cc02c

Attack Commands: Run with command\_prompt!

wmic process get /format:list

Q