# .. /ssh.exe

Execute

Ssh.exe is the OpenSSH compatible client can be used to connect to Windows 10 (build 1809 and later) and Windows Server 2019 devices.

**Paths:**
c:\windows\system32\OpenSSH\ssh.exe

**Resources:**

- https://gtfobins.github.io/gtfobins/ssh/

**Acknowledgements:**

- Akshat Pradhan
- Felix Boulet

**Detections:**

- Sigma: https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_lolbin_ssh.yml
- IOC: Event ID 4624 with process name C:\Windows\System32\OpenSSH\sshd.exe.
- IOC: command line arguments specifying execution.

## Execute

. Execute calc.exe on host machine. The prompt for password can be eliminated by adding the host's public key in the user's authorized_keys file. Adversaries can do the same for execution on remote machines.

```
ssh localhost calc.exe
```

| | |
|---|---|
| **Use case:** | Execute specified command, can be used for defense evasion. |
| **Privileges required:** | User |
| **Operating systems:** | Windows 10 1809, Windows Server 2019 |
| **ATT&CK® technique:** | T1202 |

. Executes calc.exe from ssh.exe

```
ssh -o ProxyCommand=calc.exe .
```

| | |
|---|---|
| **Use case:** | Performs execution of specified file, can be used as a defensive evasion. |
| **Privileges required:** | User |
| **Operating systems:** | Windows 10 |
| **ATT&CK® technique:** | T1202 |