

# T1529 - System Shutdown/Reboot

## Description from ATT&CK

Adversaries may shutdown/reboot systems to interrupt access to, or aid in the destruction of, those systems. Operating systems may contain commands to initiate a shutdown/reboot of a machine or network device. In some cases, these commands may also be used to initiate a shutdown/reboot of a remote computer or network device.(Citation: Microsoft Shutdown Oct 2017)(Citation: alert\_TA18\_106A) Shutting down or rebooting systems may disrupt access to computer resources for legitimate users.

Adversaries may attempt to shutdown/reboot a system after impacting it in other ways, such as [Disk Structure Wipe](#) or [Inhibit System Recovery](#), to hasten the intended effects on system availability.(Citation: Talos Nyetya June 2017)(Citation: Talos Olympic Destroyer 2018)

## Atomic Tests

- [Atomic Test #1 - Shutdown System - Windows](#)
- [Atomic Test #2 - Restart System - Windows](#)

- [Atomic Test #3 - Restart System via shutdown](#) - macOS/Linux
- [Atomic Test #4 - Shutdown System via shutdown](#) - macOS/Linux
- [Atomic Test #5 - Restart System via reboot](#) - macOS/Linux
- [Atomic Test #6 - Shutdown System via halt](#) - Linux
- [Atomic Test #7 - Reboot System via halt](#) - Linux
- [Atomic Test #8 - Shutdown System via poweroff](#) - Linux
- [Atomic Test #9 - Reboot System via poweroff](#) - Linux
- [Atomic Test #10 - Logoff System - Windows](#)

## Atomic Test #1 - Shutdown System - Windows

This test shuts down a Windows system.

**Supported Platforms:** Windows

**auto\_generated\_guid:** ad254fa8-45c0-403b-8c77-e00b3d3e7a64

**Inputs:**

Name	Description	Type	Default Value
timeout	Timeout period before shutdown (seconds)	Integer	1

**Attack Commands:** Run with `command_prompt` ! Elevation Required (e.g. root or admin)

```
shutdown /s /t #{timeout}
```



## Atomic Test #2 - Restart System - Windows

This test restarts a Windows system.

**Supported Platforms:** Windows

**auto\_generated\_guid:** f4648f0d-bf78-483c-bafc-3ec99cd1c302

**Inputs:**

Name	Description	Type	Default Value
timeout	Timeout period before restart (seconds)	Integer	1

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

```
shutdown /r /t #{timeout}
```



## Atomic Test #3 - Restart System via **shutdown** - macOS/Linux

This test restarts a macOS/Linux system.

**Supported Platforms:** macOS, Linux

**auto\_generated\_guid:** 6326dbc4-444b-4c04-88f4-27e94d0327cb

**Inputs:**

Name	Description	Type	Default Value
timeout	Time to restart (can be minutes or specific time)	String	now

**Attack Commands:** Run with **bash** ! Elevation Required (e.g. root or admin)

```
shutdown -r #{timeout}
```



## Atomic Test #4 - Shutdown System via **shutdown** - macOS/Linux

This test shuts down a macOS/Linux system using a halt.

**Supported Platforms:** macOS, Linux

**auto\_generated\_guid:** 4963a81e-a3ad-4f02-adda-812343b351de

**Inputs:**

Name	Description	Type	Default Value
timeout	Time to shutdown (can be minutes or specific time)	String	now

**Attack Commands:** Run with **bash** ! Elevation Required (e.g. root or admin)

```
shutdown -h #{timeout}
```



## Atomic Test #5 - Restart System via **reboot** - macOS/Linux

This test restarts a macOS/Linux system via **reboot** .

**Supported Platforms:** macOS, Linux

**auto\_generated\_guid:** 47d0b042-a918-40ab-8cf9-150ffe919027

**Attack Commands:** Run with **bash** ! Elevation Required (e.g. root or admin)

```
reboot
```



## Atomic Test #6 - Shutdown System via **halt** - Linux

This test shuts down a Linux system using `halt` .

**Supported Platforms:** Linux

**auto\_generated\_guid:** 918f70ab-e1ef-49ff-bc57-b27021df84dd

**Attack Commands:** Run with `bash` ! Elevation Required (e.g. root or admin)

```
halt -p
```



## Atomic Test #7 - Reboot System via `halt` - Linux

---

This test restarts a Linux system using `halt` .

**Supported Platforms:** Linux

**auto\_generated\_guid:** 78f92e14-f1e9-4446-b3e9-f1b921f2459e

**Attack Commands:** Run with `bash` ! Elevation Required (e.g. root or admin)

```
halt --reboot
```



## Atomic Test #8 - Shutdown System via `poweroff` - Linux

---

This test shuts down a Linux system using `poweroff` .

**Supported Platforms:** Linux

**auto\_generated\_guid:** 73a90cd2-48a2-4ac5-8594-2af35fa909fa

**Attack Commands:** Run with `bash` ! Elevation Required (e.g. root or admin)

```
poweroff
```



## Atomic Test #9 - Reboot System via `poweroff` - Linux

This test restarts a Linux system using `poweroff`.

Supported Platforms: Linux

auto\_generated\_guid: 61303105-ff60-427b-999e-efb90b314e41

Attack Commands: Run with `bash` ! Elevation Required (e.g. root or admin)

```
poweroff --reboot
```



## Atomic Test #10 - Logoff System - Windows

This test performs a Windows system logoff as seen in [dcrat backdoor capabilities](#)

Supported Platforms: Windows

auto\_generated\_guid: 3d8c25b5-7ff5-4c9d-b21f-85ebd06654a4

Attack Commands: Run with `command_prompt` ! Elevation Required (e.g. root or admin)

```
shutdown /1
```

