Command and Scripting Interpreter: Unix Shell, Sub-technique T1623.001 - Mobile

Archived: 2026-04-05 18:29:16 UTC

Adversaries may abuse Unix shell commands and scripts for execution. Unix shells are the underlying command prompts on Android and iOS devices. Unix shells can control every aspect of a system, with certain commands requiring elevated privileges that are only accessible if the device has been rooted or jailbroken.

Unix shells also support scripts that enable sequential execution of commands as well as other typical programming operations such as conditionals and loops. Common uses of shell scripts include long or repetitive tasks, or the need to run the same set of commands on multiple systems.

Adversaries may abuse Unix shells to execute various commands or payloads. Interactive shells may be accessed through command and control channels or during lateral movement such as with SSH. Adversaries may also leverage shell scripts to deliver and execute multiple commands on victims or as part of payloads used for persistence.

If the device has been rooted or jailbroken, adversaries may locate and invoke a superuser binary to elevate their privileges and interact with the system as the root user. This dangerous level of permissions allows the adversary to run special commands and modify protected system files.

Source: https://attack.mitre.org/techniques/T1623/001