Privilege Escalation, Tactic TA0111 - ICS

Archived: 2026-04-05 18:36:59 UTC

The adversary is trying to gain higher-level permissions.

Privilege Escalation consists of techniques that adversaries use to gain higher-level permissions on a system or network. Adversaries can often enter and explore a network with unprivileged access but require elevated permissions to follow through on their objectives. Common approaches are to take advantage of system weaknesses, misconfigurations, and vulnerabilities.

ID: TA0111

Created: 10 April 2021

Last Modified: 16 April 2025

Techniques

Techniques: 2

ID	Name	Description
T0890	Exploitation for Privilege Escalation	Adversaries may exploit software vulnerabilities in an attempt to elevate privileges. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Security constructs such as permission levels will often hinder access to information and use of certain techniques, so adversaries will likely need to perform privilege escalation to include use of software exploitation to circumvent those restrictions.
T0874	Hooking	Adversaries may hook into application programming interface (API) functions used by processes to redirect calls for execution and privilege escalation means. Windows processes often leverage these API functions to perform tasks that require reusable system resources. Windows API functions are typically stored in dynamic-link libraries (DLLs) as exported functions.