# File and Directory Permissions Modification: Windows File and Directory Permissions Modification, Sub-technique T1222.001 - Enterprise

Archived: 2026-04-05 16:00:04 UTC

Adversaries may modify file or directory permissions/attributes to evade access control lists (ACLs) and access protected files.[1][2] File and directory permissions are commonly managed by ACLs configured by the file or directory owner, or users with the appropriate permissions. File and directory ACL implementations vary by platform, but generally explicitly designate which users or groups can perform which actions (read, write, execute, etc.).

Windows implements file and directory ACLs as Discretionary Access Control Lists (DACLs).[3] Similar to a standard ACL, DACLs identifies the accounts that are allowed or denied access to a securable object. When an attempt is made to access a securable object, the system checks the access control entries in the DACL in order. If a matching entry is found, access to the object is granted. Otherwise, access is denied.[4]

Adversaries can interact with the DACLs using built-in Windows commands, such as `icacls`, `cacls`, `takeown`, and `attrib`, which can grant adversaries higher permissions on specific files and folders. Further, PowerShell provides cmdlets that can be used to retrieve or modify file and directory DACLs. Specific file and directory modifications may be a required step for many techniques, such as establishing Persistence via Accessibility Features, Boot or Logon Initialization Scripts, or tainting/hijacking other instrumental binary/configuration files via Hijack Execution Flow.

---

Source: https://attack.mitre.org/techniques/T1222/001