

# CAPEC-561: Windows Admin Shares with Stolen Credentials (Version 3.9)

Archived: 2026-04-05 15:56:14 UTC

ChildOf **S** Standard Attack Pattern - A standard level attack pattern in CAPEC is focused on a specific methodology or technique used in an attack. It is often seen as a singular piece of a fully executed attack. A standard attack pattern is meant to provide sufficient details to understand the specific technique and how it attempts to accomplish a desired goal. A standard level attack pattern is a specific type of a more abstract meta level attack pattern.<sup>653</sup>[Use of Known Operating System Credentials](#) CanFollow **D** Detailed Attack Pattern - A detailed level attack pattern in CAPEC provides a low level of detail, typically leveraging a specific technique and targeting a specific technology, and expresses a complete execution flow. Detailed attack patterns are more specific than meta attack patterns and standard attack patterns and often require a specific protection mechanism to mitigate actual attacks. A detailed level attack pattern often will leverage a number of different standard level attack patterns chained together to accomplish a goal.<sup>16</sup>[Dictionary-based Password Attack](#) CanFollow **S** Standard Attack Pattern - A standard level attack pattern in CAPEC is focused on a specific methodology or technique used in an attack. It is often seen as a singular piece of a fully executed attack. A standard attack pattern is meant to provide sufficient details to understand the specific technique and how it attempts to accomplish a desired goal. A standard level attack pattern is a specific type of a more abstract meta level attack pattern.<sup>49</sup>[Password Brute Forcing](#) CanFollow **S** Standard Attack Pattern - A standard level attack pattern in CAPEC is focused on a specific methodology or technique used in an attack. It is often seen as a singular piece of a fully executed attack. A standard attack pattern is meant to provide sufficient details to understand the specific technique and how it attempts to accomplish a desired goal. A standard level attack pattern is a specific type of a more abstract meta level attack pattern.<sup>50</sup>[Password Recovery Exploitation](#) CanFollow **D** Detailed Attack Pattern - A detailed level attack pattern in CAPEC provides a low level of detail, typically leveraging a specific technique and targeting a specific technology, and expresses a complete execution flow. Detailed attack patterns are more specific than meta attack patterns and standard attack patterns and often require a specific protection mechanism to mitigate actual attacks. A detailed level attack pattern often will leverage a number of different standard level attack patterns chained together to accomplish a goal.<sup>55</sup>[Rainbow Table Password Cracking](#) CanFollow **D** Detailed Attack Pattern - A detailed level attack pattern in CAPEC provides a low level of detail, typically leveraging a specific technique and targeting a specific technology, and expresses a complete execution flow. Detailed attack patterns are more specific than meta attack patterns and standard attack patterns and often require a specific protection mechanism to mitigate actual attacks. A detailed level attack pattern often will leverage a number of different standard level attack patterns chained together to accomplish a goal.<sup>70</sup>[Try Common or Default Usernames and Passwords](#) CanFollow **D** Detailed Attack Pattern - A detailed level attack pattern in CAPEC provides a low level of detail, typically leveraging a specific technique and targeting a specific technology, and expresses a complete execution flow. Detailed attack patterns are more specific than meta attack patterns and standard attack patterns and often require a specific protection mechanism to mitigate actual attacks. A detailed level attack pattern often will leverage a number of different standard level attack patterns chained together to accomplish a goal.<sup>565</sup>[Password Spraying](#) CanFollow **D** Detailed Attack Pattern - A detailed level attack pattern in CAPEC

provides a low level of detail, typically leveraging a specific technique and targeting a specific technology, and expresses a complete execution flow. Detailed attack patterns are more specific than meta attack patterns and standard attack patterns and often require a specific protection mechanism to mitigate actual attacks. A detailed level attack pattern often will leverage a number of different standard level attack patterns chained together to accomplish a goal.<sup>568</sup>[Capture Credentials via Keylogger](#) CanFollow **D** Detailed Attack Pattern - A detailed level attack pattern in CAPEC provides a low level of detail, typically leveraging a specific technique and targeting a specific technology, and expresses a complete execution flow. Detailed attack patterns are more specific than meta attack patterns and standard attack patterns and often require a specific protection mechanism to mitigate actual attacks. A detailed level attack pattern often will leverage a number of different standard level attack patterns chained together to accomplish a goal.<sup>643</sup>[Identify Shared Files/Directories on System](#) CanPrecede **M** Meta Attack Pattern - A meta level attack pattern in CAPEC is a decidedly abstract characterization of a specific methodology or technique used in an attack. A meta attack pattern is often void of a specific technology or implementation and is meant to provide an understanding of a high level approach. A meta level attack pattern is a generalization of related group of standard level attack patterns. Meta level attack patterns are particularly useful for architecture and design level threat modeling exercises.<sup>151</sup>[Identity Spoofing](#) CanPrecede **M** Meta Attack Pattern - A meta level attack pattern in CAPEC is a decidedly abstract characterization of a specific methodology or technique used in an attack. A meta attack pattern is often void of a specific technology or implementation and is meant to provide an understanding of a high level approach. A meta level attack pattern is a generalization of related group of standard level attack patterns. Meta level attack patterns are particularly useful for architecture and design level threat modeling exercises.<sup>165</sup>[File Manipulation](#) CanPrecede **S** Standard Attack Pattern - A standard level attack pattern in CAPEC is focused on a specific methodology or technique used in an attack. It is often seen as a singular piece of a fully executed attack. A standard attack pattern is meant to provide sufficient details to understand the specific technique and how it attempts to accomplish a desired goal. A standard level attack pattern is a specific type of a more abstract meta level attack pattern.<sup>545</sup>[Pull Data from System Resources](#) CanPrecede **M** Meta Attack Pattern - A meta level attack pattern in CAPEC is a decidedly abstract characterization of a specific methodology or technique used in an attack. A meta attack pattern is often void of a specific technology or implementation and is meant to provide an understanding of a high level approach. A meta level attack pattern is a generalization of related group of standard level attack patterns. Meta level attack patterns are particularly useful for architecture and design level threat modeling exercises.<sup>549</sup>[Local Execution of Code](#)

---

Source: <https://capec.mitre.org/data/definitions/561.html>