Search Open Technical Databases: Scan Databases, Sub-technique T1596.005 - Enterprise

Archived: 2026-04-05 17:13:10 UTC

Adversaries may search within public scan databases for information about victims that can be used during targeting. Various online services continuously publish the results of Internet scans/surveys, often harvesting information such as active IP addresses, hostnames, open ports, certificates, and even server banners.[1]

Adversaries may search scan databases to gather actionable information. Threat actors can use online resources and lookup tools to harvest information from these services. Adversaries may seek information about their already identified targets, or use these datasets to discover opportunities for successful breaches. Information from these sources may reveal opportunities for other forms of reconnaissance (ex: Active Scanning or Search Open Websites/Domains), establishing operational resources (ex: Develop Capabilities or Obtain Capabilities), and/or initial access (ex: External Remote Services or Exploit Public-Facing Application).

Source: https://attack.mitre.org/techniques/T1596/005