Data from Configuration Repository: SNMP (MIB Dump), Sub-technique T1602.001 - Enterprise

Archived: 2026-04-05 14:49:46 UTC

Adversaries may target the Management Information Base (MIB) to collect and/or mine valuable information in a network managed using Simple Network Management Protocol (SNMP).

The MIB is a configuration repository that stores variable information accessible via SNMP in the form of object identifiers (OID). Each OID identifies a variable that can be read or set and permits active management tasks, such as configuration changes, through remote modification of these variables. SNMP can give administrators great insight in their systems, such as, system information, description of hardware, physical location, and software packages[1]. The MIB may also contain device operational information, including running configuration, routing table, and interface details.

Adversaries may use SNMP queries to collect MIB content directly from SNMP-managed devices in order to collect network information that allows the adversary to build network maps and facilitate future targeted exploitation.[2][3]

Source: https://attack.mitre.org/techniques/T1602/001