Networking

SNMP and Network Device Logs

CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

SNMP

- Simple Network Management Protocol (SNMP)
  - Collects and manipulates valuable network information
    - Agents send an alert to the management station if something isn't functioning properly
      - These alerts are called traps
- Versions
  - SNMPv1
    - Supports plaintext authentication, only uses UDP
  - SNMPv2c
    - Supports plaintext authentication with MD5 or SHA, uses UDP but can be configured to use TCP
  - SNMPv3
    - Supports strong authentication with MD5 or SHA, uses TCP

OIDs and MIBs

- Object Identifiers (OIDs)
  - Mechanism for naming any object, concept, or “thing” with a globally unambiguous persistent name
- Management Information Base (MIB)
  - Contains nodes that are identified by the OIDs

Types of Logs

- Network Device Log
  - Collection of all network data, traffic, issues, etc…
    - Verifies the network is working properly
- Traffic Log
  - Captures the network traffic
    - Dates, times, source, destination, ports, etc…
- Audit Log
  - Records all events in an IT system
- Syslog
  - Standard for sending and receiving notification messages from various network devices