Networking

Networking Operations

3.1.2 - SNMP and Network Device Logs

What is the SNMP protocol and what are some common network device logs?

Overview

Given a scenario, the student will use the appropriate statistics and sensors to ensure network availability

Grade Level(s)

10, 11, 12

Cyber Connections

- Threats & Vulnerabilities
- Networks & Internet
- Hardware & Software

This content is based upon work supported by the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency under the Cybersecurity Education Training and Assistance Program (CETAP).

Teacher Notes:

CompTIA N10-008 Network+ Objectives

Objective 3.1

- Given a scenario, use the appropriate statistics and sensors to ensure network availability
    - SNMP
        - Traps
        - Object identifiers (OIDs)
        - Management information bases (MIBs)
    - Network device logs
        - Log reviews
            - Traffic logs
            - Audit logs
            - Syslog
        - Logging levels/severity levels

SNMP and Network Device Logs

SNMP

Simple Network Management Protocol (SNMP) collects and manipulates valuable network information. SNMP uses concurrent ports 161 and 162. SNMP gathers data by polling devices on a network. A baseline is received when everything is functioning as normal. Network watchdogs called agents send an alert called a ***trap*** to the management station if something isn't functioning properly. There are three versions of SNMP:

- 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) are an identifier mechanism standardized by the International Telecommunications Union (ITU) and ISO/IEC for naming any object, concept, or "thing" with a globally unambiguous persistent name.

Teacher Notes:

In SNMP, every node in a ***management information base (MIB)*** is identified by an OID. A managed object is one of any number of specific characteristics of a managed device.

Network Device Logs

Network device logs are important in networking for understanding what is happening and diagnosing/troubleshooting issues. A baseline should be documented so it is known what "normal" looks like for a network. We can review logs to verify the network is working properly, the network conforms with all internal and external regulations, and that management procedures and security policies are in place for future reference.

Types of Logs

Traffic logs display an entry for the start and end of every session. All entries include: date and time, source and destination zones, addresses and ports, application name, security rule applied to the traffic flow, rule action (allow, deny, or drop), ingress and egress interface, number of bytes, and session end reason.

An ***audit log*** is a document that records an event in an IT system. Audit logs include what resources were accessed, destination and source addresses, a timestamp and user login information.

Syslog is a standard for sending and receiving notification messages from various network devices. The messages include time stamps, event messages, severity, host IP addresses, diagnostics and more. In terms of its built-in ***severity level***, it can communicate a range among level 0 through 7. In order, these are Emergency, Alert, Critical, Error, Warning, Notification, Information, and Debugging.