SNMP Polling:

SNMP polling is the process of periodically sending SNMP `GET` (or `GET-NEXT`) requests from a network management system (NMS) to SNMP-enabled devices to retrieve information.

Polling Steps:

- NMS sends SNMP GET requests to a device.
- The device (SNMP agent) responds with the requested data.
- The NMS collects, stores, and analyzes the data.
- This happens on a regular schedule (e.g., every 5 minutes).

SNMP commands:

Polls a single OID from a device:

snmpget -v<version> -c<community> <target-ip> <OID>

Example: snmpget -v2c -c public <IP> .1.3.6.1.2.1.1.5.0

Explanation:

- `-v2c`: Use SNMP version 2c
- `-c public`: Community string (like a password; default is `public`)
- <IP>: IP of the SNMP agent (your Windows host)
- `.1.3.6.1.2.1.1.5.0`: OID for system name (sysName)

Walks through an SNMP subtree (gets multiple related OIDs):

Syntax: snmpwalk -v<version> -c<community> <target-ip> [<base-OID>]

Example:

snmpwalk -v2c -c public <target-ip> .1.3.6.1.2.1.1

Explanation:

`.1.3.6.1.2.1.1` = system info, basic info about the device for discovering what data is available in the system.

`.1.3.6.1.2.1.12 =` This OID is the **root** of all SNMP data related to **network interfaces** on the device (e.g., Ethernet, Wi-Fi, loopback, etc.)

Displays tabular SNMP data (like interface lists) in a table format:

Syntax: snmptable -v<version> -c<community> <target-ip> <table-OID>

Example: snmptable -v2c -c public 192.168.1.100 IF-MIB::ifTable

Interface status, uptime:

snmpstatus -v2c -c public <target-ip>

Simulation 1: Using Kali to poll localhost (Kali as NMS, localhost as Agent):

Set up snmp in kali linux:

sudo apt update

sudo apt install snmpd –y

Configure the SNMP agent:

sudo nano /etc/snmp/snmpd.conf

Add the lines:

rocommunity public

agentAddress udp:161,udp6:[::1]:161

Comment the line: <these lines are for removing access restriction>:

#AgentAddress 127.0.0.1,[::1]

Restart and enable the SNMP agent:

sudo systemctl restart snmpd

sudo systemctl enable snmpd

Execute the command for testing snmp polling:

snmpget -v2c -c public 127.0.0.1 .1.3.6.1.2.1.1.5.0

snmpwalk -v2c -c public 127.0.0.1

Simulation 2: Use Kali to **poll SNMP data from the Windows host**

Snmp agent : Windows host machine

NMS : Kali Linux VM

SNMP Setup:

Windows :

Enable SNMP on the Windows Host:

- Open **Control Panel → Programs and Features → Turn Windows features on or off**.
- Click **"Add a feature"** (in Windows 10/11, under “Optional Features”).
- Search for and install:
  `Simple Network Management Protocol (SNMP)`
  `SNMP WMI Provider` *(optional)*
- After installation, open: **Services → Allow connection any service**
- In **SNMP Properties**:
  Under **Security tab**, add a community string (e.g. `public`) with **READ ONLY access**.
- Allow access from your **Kali VM IP** (or all hosts, for testing).
- Start or restart the SNMP service.

Configure SNMP Service:

1. Press `Windows + R`, type: `services.msc`, press Enter
2. Find and open **SNMP Service**
3. Go to **Security** tab:
    a. Add **community name** (e.g., `public`) with **READ ONLY** permission
    b. In "Accept SNMP packets from these hosts":
        i. Add your **Kali VM IP** (or select **Accept SNMP packets from any host** just for testing)
4. Apply and **start the SNMP service**

Allow SNMP through Windows Firewall:

1. Open **Windows Defender Firewall with Advanced Security**
2. Click **Inbound Rules**
3. Find or create rule for:
    a. **Protocol:** UDP
    b. **Port:** 161
    c. **Action:** Allow

d. **Profile:** All (Domain, Private, Public)
e. **Name:** "Allow SNMP"

Configure Kali Networking (in VMware):

In **VMware Workstation or Player**, check your Kali VM's network adapter:

- Go to VM settings → **Network Adapter**
- Set it to:
  - **Bridged** *(if you want to poll across your LAN — best option)*

Linux – SNMP configuration:

sudo apt update

sudo apt install snmp

sudo apt install snmp snmp-mibs-downloader

TESTING:

snmpget -v2c -c public 192.168.1.100 .1.3.6.1.2.1.1.3.0