Below is a detailed report formatted similarly to the provided example, incorporating the updated commands, macro, type, description, and flag. The report assumes the objective is to discover an SNMP service on the standard UDP port and retrieve the flag.

Detailed Steps to Solve the Machine

Machine Information

- **Macro**: NS
- **Type**: Scanning
- **Description**: The machine requires network scanning to identify active hosts and an SNMP service running on the standard UDP port (161). The flag is obtained after querying the SNMP service using the appropriate community string.
- **Objective**: Discover an SNMP service on the standard UDP port (161) and retrieve the flag.

Step-by-Step Process

Step 1: Network Scanning with Nmap

- **Command**: nmap -n --min-parallelism 100 --max-retries 1 192.168.0.0/16
- **Description**:
    - **Purpose**: Perform a broad network scan to identify live hosts within the 192.168.0.0/16 subnet.
    - **Details**:
        - Executed from a machine with IP 192.168.0.5.
        - nmap -n disables DNS resolution to speed up the scan.
        - --min-parallelism 100 ensures at least 100 probes are sent in parallel for efficiency.
        - --max-retries 1 limits retry attempts to 1 to reduce scan time.
        - The scan targets the 192.168.0.0/16 subnet (65,536 addresses) to discover active hosts.
    - **Assumption**: The scan identifies 192.168.3.2 as a live host, which is targeted for further scanning.

    - **Output**: A list of active IPs, including 192.168.3.2.

Step 2: UDP Port Scanning for SNMP

- **Command**: nmap -sU -p 161 -n --min-parallelism 100 --max-retries 1 192.168.3.2
- **Description**:
    - **Purpose**: Identify whether the SNMP service is running on the standard UDP port (161) on the target machine (192.168.3.2).
    - **Details**:
        - Executed from 192.168.0.5.
        - -sU specifies a UDP scan.
        - -p 161 targets the standard SNMP port.
        - -n disables DNS resolution.
        - --min-parallelism 100 and --max-retries 1 optimize the scan for speed and reliability.
    - **Assumption**: The scan confirms that UDP port 161 is open and running an SNMP service.
    - **Output**: A report confirming UDP port 161 is open on 192.168.3.2.

Step 3: Query SNMP Service

- **Command**: snmpwalk -v 2c -c public 192.168.3.2
- **Description**:
    - **Purpose**: Query the SNMP service to retrieve system information, including the flag.
    - **Details**:
        - Executed from 192.168.0.5.
        - snmpwalk retrieves a tree of information from the SNMP service.
        - -v 2c specifies SNMP version 2c.
        - -c public uses the default community string public for access.
        - Targets the IP 192.168.3.2.

    - **Assumption**: The SNMP query is successful, and the flag is embedded in the retrieved data (e.g., in the system description or a custom OID).
    - **Output**: SNMP data containing the flag jDdHyCkr9iJENWFz.

Final Answer

- **Flag**: jDdHyCkr9iJENWFz