Threat Category: Reconnaissance, SNMP Enumeration

Threat Description: The SNORT rule with SID 1000013 is designed to detect SNMP (Simple Network Management Protocol) request traffic targeting UDP port 161. This protocol is commonly used for network management and monitoring. However, it can also be exploited by attackers to gather sensitive information about devices on a network, such as system descriptions, interface details, routing tables, and more.

Indicators of Compromise (IoCs):

Protocol: UDP

Destination Port: 161

SNMP Request PDU detected in payload

Detection Mechanism:

This rule triggers when a UDP packet is sent to port 161, the default port for SNMP. It does not examine packet content in depth but relies on protocol and port matching to flag potential SNMP query activity. The detection occurs regardless of the source or destination IP, making it suitable for monitoring across various segments of a network.

Possible Attribution & Use Cases:

Could be used by attackers performing SNMP sweeps to gather information on networked devices.

Also triggered by legitimate network management tools performing SNMP monitoring.

Recommended Actions:

Monitor and Investigate: Verify whether the SNMP request originates from authorized network monitoring tools.

Restrict Access: Limit SNMP access to trusted management networks using ACLs or firewall rules.

Author & Attribution:

Rule Author: community

Rule Source: Custom/Community Rule Set

SID: 1000013

Revision: 1