Threat Category: Reconnaissance, ICMP Scanning

Threat Description: The SNORT rule is designed to detect ICMP echo requests, commonly known as "ping" requests. ICMP echo requests are typically used to check the availability of a host and measure round-trip time.

Indicators of Compromise (IoCs):

ICMP Type: 8 (Echo Request)

Protocol: ICMP

No specific source or destination ports (ICMP is portless)

Detection Mechanism:

This rule uses the Snort alert action to generate an alert when any host sends an ICMP echo request to any other host.

Matches ICMP packets from any source IP and any source port to any destination IP and any destination port.

The rule triggers specifically on ICMP echo request messages.

Possible Attribution & Use Cases:

Associated with reconnaissance activities by threat actors mapping a target network.

Recommended Actions:

Monitor and Investigate: Identify the source of the ICMP request and verify if it is from a known or trusted system.

Rate Limiting: Implement rate-limiting on ICMP traffic to reduce risk of reconnaissance without affecting diagnostics.

suspicious activity.

Author & Attribution:

Rule Author: community

Rule Source:

SID: 1000016

Revision: 1