Threat Category: Reconnaissance, Information Gathering

Threat Description: The SNORT rule rule1_e.txt is designed to detect ICMP ping requests. This type of traffic is commonly used for network reconnaissance to determine the reachability of a host. While pinging is a legitimate network utility, it can also be used by attackers to discover active hosts within a network before launching more targeted attacks.

Protocol: ICMP

Detection Mechanism: This rule identifies potential ICMP ping requests by monitoring for any ICMP traffic.

Possible Attribution & Use Cases: Detection of network scanning or reconnaissance activity.

Identification of potential attackers attempting to map the network.

Legitimate network troubleshooting.

Recommended Actions: Monitor and Investigate: Analyze the source of the ICMP traffic. High volumes of pings from a single source may indicate reconnaissance.

Rate Limiting: Implement rate limiting on ICMP traffic if excessive pinging is detected.

Firewall Review: Review firewall rules to ensure that ICMP traffic is allowed only when necessary.

Author & Attribution:

SID: 1000001

Revision: 1