Threat Category: Network Traffic, NTP Protocol

Threat Description: The rule is designed to detect NTP (Network Time Protocol) requests. NTP is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. Detecting NTP requests can be useful for monitoring network time synchronization activity.

Indicators of Compromise (IoCs)

Protocol: UDP

Destination Port: 123

Detection Mechanism: This rule identifies NTP requests by monitoring for UDP traffic destined for port 123.

Possible Attribution & Use Cases:

Monitoring network time synchronization activity.

Detecting potential NTP-based attacks or abuse.

Troubleshooting time synchronization issues.

Recommended Actions:

Monitor and Investigate: Analyze NTP traffic for anomalies, such as excessive NTP requests or requests from unauthorized sources.

Secure NTP: Implement secure NTP configurations to prevent NTP-based attacks.

NTP Server Authentication: If possible, authenticate NTP servers to ensure time synchronization from trusted sources.

Author & Attribution:

SID: 1000010

Revision: 1