Threat Category: Reconnaissance, File Transfer Protocol Abuse

Threat Description: The SNORT rule sid:1000018 is designed to detect attempts to initiate file transfers using the Trivial File Transfer Protocol (TFTP) over UDP port 69.

Indicators of Compromise (IoCs):

Protocol: UDP

Destination Port: 69

Traffic Direction: Any source to destination on port 69

Payload containing TFTP read/write request (e.g., RRQ or WRQ)

Detection Mechanism:

This rule detects any UDP packet sent to port 69 regardless of source port or IP. Since TFTP operates over UDP and does not require a connection setup like TCP, the rule listens for potential read or write requests typically found at the beginning of a TFTP session.

Possible Attribution & Use Cases:

May indicate lateral movement or payload delivery during exploitation or post-exploitation phases.

Could be used by attackers to exfiltrate data from compromised systems.

Recommended Actions:

Determine if the TFTP usage is expected in the environment. Investigate unusual sources or destinations.

Block or limit access to UDP port 69 on firewall and network perimeter devices.

Author & Attribution:

Rule Author: community

Rule Source: Custom Rule

SID: 1000018

Revision: 1