Threat Category: Reconnaissance, SMB Protocol

Threat Description: The SNORT rule is designed to detect attempts to initiate connections over TCP port 445, which is commonly used by the Server Message Block (SMB) protocol on Windows systems.

Indicators of Compromise (IoCs):

Destination Port: 445

Protocol: TCP

Direction: Outbound (from any source to any destination)

Detection Mechanism:

This rule detects any TCP traffic destined for port 445, regardless of the source or destination IP address. It does not analyze packet contents but simply matches traffic based on port and protocol.

Possible Attribution & Use Cases:

This activity could originate from legitimate SMB clients or administrators conducting routine tasks.

However, it is also commonly observed during:

Reconnaissance or scanning for SMB-enabled systems

Lateral movement by malware or attackers

Exploitation of SMB vulnerabilities

Recommended Actions:

Track SMB connection attempts, especially from unexpected sources.

Limit SMB access to trusted zones only.

Ensure all hosts using SMB are up-to-date with security patches.

Disable legacy SMB versions to reduce attack surface.

Author & Attribution:

Rule Author: community

Rule Source: Custom rule

SID: 1000019

Revision: 1