Threat Category: Network Traffic, SMTP Protocol

Threat Description: The rule is designed to detect SMTP connection attempts. SMTP is an internet standard for e-mail transmission. Detecting SMTP connections is essential for monitoring email traffic and identifying potential email-borne threats.

Indicators of Compromise (IoCs)

Protocol: TCP

Destination Port: 25

Detection Mechanism: This rule identifies SMTP connection attempts by monitoring for TCP traffic destined for port 25.

Possible Attribution & Use Cases:

Monitoring email traffic for spam or malicious content.

Detecting potential email server compromises.

Troubleshooting email delivery issues.

Recommended Actions: Monitor and Investigate: Analyze SMTP traffic for suspicious email activity, such as large volumes of emails, emails with malicious attachments, or emails from unknown sources.

Email Filtering: Implement email filtering solutions to block spam, phishing emails, and malware.

SMTP Authentication: Enforce SMTP authentication to prevent email spoofing and unauthorized email relaying.

Author & Attribution:

SID: 1000007

Revision: 1