Threat Category: Remote Access, Protocol Abuse

Threat Description: The SNORT rule is designed to detect Remote Desktop Protocol (RDP) connection attempts over TCP port 3389. RDP is a proprietary protocol developed by Microsoft, commonly used for remote access to Windows systems. While legitimate in enterprise environments, unauthorized RDP access is frequently used by threat actors during the initial access or lateral movement stages of an attack. This rule helps security teams identify when RDP connections are initiated, which can be an indicator of either administrative activity or potential unauthorized access attempts.

Indicators of Compromise (IoCs)

Destination Port: 3389

Protocol: TCP

Connection Direction: From any source to any destination on port 3389

Detection Mechanism:

This rule inspects TCP traffic and triggers an alert when a connection is made to TCP port 3389, which is the default port for RDP. It does not analyze packet content but relies on port-based detection.

Possible Attribution & Use Cases:

Common in corporate environments for remote administration.

Used by attackers to gain access to internal systems if exposed externally or poorly secured.

Recommended Actions:

Monitor and Investigate: Review logs and alert data to determine the source and intent of the RDP connection.

Access Control: Restrict external RDP access using firewall rules or VPN requirements.

Detection Tuning: Whitelist known and authorized RDP connections to reduce false positives.

Author & Attribution:

Rule Author: community

Rule Source:

SID: 1000012

Revision: 1