Threat Category: Network Traffic, SSH Protocol

Threat Description: The SNORT rule rule6_e.txt is designed to detect SSH (Secure Shell) connection attempts. SSH is a cryptographic network protocol for operating network services securely over an unsecured computer network. Detecting SSH connections is crucial for monitoring secure remote access and identifying potential unauthorized access attempts.

Indicators of Compromise (IoCs)

Protocol: TCP

Destination Port: 22

Detection Mechanism: This rule identifies SSH connection attempts by monitoring for TCP traffic destined for port 22.

Possible Attribution & Use Cases: Monitoring secure remote access to systems.

Detecting unauthorized SSH access attempts.

Auditing SSH activity for compliance purposes.

Author & Attribution:

SID: 1000006

Revision: 1