Threat Category: Network Traffic, HTTP Protocol

Threat Description: The SNORT rule is designed to detect HTTP traffic. HTTP (Hypertext Transfer Protocol) is the foundation of data communication for the World Wide Web. Detecting HTTP traffic is essential for network monitoring and security analysis.

Indicators of Compromise (IoCs)

Protocol: TCP

Destination Port: 80

Detection Mechanism:

This rule identifies HTTP traffic by monitoring for TCP traffic destined for port 80.

Possible Attribution & Use Cases:

Monitoring web browsing activity.

Detecting potential web-based attacks.

Troubleshooting web connectivity issues.

Recommended Actions:

Monitor and Investigate: Analyze HTTP traffic for suspicious activity, such as access to known malicious websites or unusual traffic patterns.

Web Filtering: Implement web filtering to block access to malicious or inappropriate content.

Intrusion Detection: Use intrusion detection systems (IDS) to inspect HTTP traffic for signs of attacks.

Author & Attribution:

SID: 1000002

Revision: 1