Threat Category: Reconnaissance, Alternate Port Scanning

Threat Description: The SNORT rule is designed to detect network traffic directed to TCP port 8080, which is commonly used as an alternate HTTP port.

Indicators of Compromise (IoCs)

Destination Port: 8080

Protocol: TCP

Detection Mechanism:

The rule uses the alert action to trigger a notification.

The msg keyword provides context in the alert: "Alternate HTTP port traffic detected".

The sid (Snort ID) uniquely identifies the rule as 1000014.

The rev keyword indicates this is the first revision of the rule.

Possible Attribution & Use Cases:

Attackers may use alternate ports like 8080 for web traffic to avoid traditional security monitoring.

Web proxies and administrative interfaces often operate on port 8080.

Recommended Actions:

Review traffic on port 8080 to determine if the activity is legitimate or indicative of malicious behavior.

Limit access to port 8080 through firewall or access control rules.

Ensure traffic on non-standard ports is logged and alerts are investigated.

Verify whether any internal or external services are listening on port 8080 and whether they should be.

Author & Attribution:

Rule Author: community

Rule Source:

SID: 1000014

Revision: 1