Threat Category: Malware, Backdoor, Attempted Administrator Access

Threat Description: The SNORT rule is designed to detect attempts to gain unauthorized "root" or administrative access to systems, often targeting Telnet services. This detection focuses on identifying TCP traffic containing the specific string "r00t," a common misspelling used to evade simple filters.

Indicators of Compromise (IoCs)

Content: "r00t"

Detection Mechanism:

The traffic is TCP.

The traffic flow is from the server to the client and the TCP connection must be established (to_server,established).

The destination port is 23 (Telnet).

The rule checks for the presence of the string "r00t" in the packet's content.

Possible Attribution & Use Cases:

The detection indicates a possible attempt to gain unauthorized "root" or administrative access.

Attackers often use misspellings like "r00t" to bypass basic security measures.

This rule can be used to identify and block attempts to gain elevated privileges, particularly those targeting Telnet.

Recommended Actions:

Monitor and Investigate: Analyze the traffic and the involved systems to confirm the attempted unauthorized access.

Containment & Mitigation: Isolate the affected system to prevent further spread. Secure the Telnet

service or discontinue its use if possible.

Threat Hunting & Intelligence Sharing: Use this rule to proactively hunt for similar activity. Share information with the security community to improve detection and prevention efforts.

Author & Attribution:

Rule Author: community

Ruleset: community

SID: 211

Revision: 7