Threat Category: Protocol Anomaly, Telnet Exploit

Threat Description: This rule is designed to detect a specific exploit attempt against Telnet servers, possibly a BSD-related exploit. This rule focuses on traffic from an external network to internal Telnet servers on port 23. The detection mechanism involves checking for a specific byte sequence within the TCP packet payload at a specific offset and depth. Specifically, it checks for the presence of "|FF F6 FF F6 FF FB 08 FF F6|" at a depth of 50 and an offset of 200. The rule also uses isdataat and raw_data keywords. This pattern is indicative of a Telnet exploit attempting to execute commands or cause a denial of service.

Indicators of Compromise (IoCs):

TCP Port: 23 (Telnet)

Content Pattern: "|FF F6 FF F6 FF FB 08 FF F6|" (depth 50, offset 200)

Detection Mechanism:

The network protocol must be TCP.

The traffic direction must be from $EXTERNAL_NET to $TELNET_SERVERS.

The destination port must be 23.

The TCP connection must be established.

The rule checks if there is data at 200 bytes using isdataat.

Possible Attribution & Use Cases:

The detection can be used to identify attempts to exploit Telnet servers, potentially gaining unauthorized access.

Recommended Actions:

Monitor and Investigate: If this rule is triggered, investigate the targeted Telnet server for signs of

compromise.

Disable Telnet: If possible, disable the Telnet service and use more secure alternatives such as SSH.

Patching: Ensure that Telnet servers are patched against known vulnerabilities.

Intrusion Prevention: Utilize intrusion prevention systems to block Telnet exploit attempts.

Author & Attribution:

Rule Author: Community

Rule Source: Community

Rule SID: 1253

Rule Revision: 24

Service: telnet

Reference: Bugtraq-3064, CVE-2001-0554, Nessus-10709