Threat Category: Protocol Anomaly, Suspicious Login, FTP

Threat Description: This rule is designed to detect attempts to log in to an FTP server using the username "w0rm". This rule focuses on traffic from an external network to an internal network on TCP port 21 (the standard FTP port). The detection mechanism involves checking for the "USER" command (case-insensitive) followed by the username "w0rm" (case-insensitive) with a distance of 1. It also uses a PCRE to match the pattern /^USER\s+w0rm/ims. This combination of checks is used to identify potential unauthorized access attempts.

Indicators of Compromise (IoCs):

TCP Port: 21 (FTP)

Content 1: "USER" (case-insensitive)

Content 2: "w0rm" (case-insensitive, distance 1)

PCRE Pattern: ?/^USER\s+w0rm/ims?

Detection Mechanism: This rule identifies potential "w0rm" FTP login attempts using the following conditions:

The network protocol must be TCP.

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

The destination port must be 21.

The TCP connection must be established (established).

The content must contain "USER" (case-insensitive).

The content must contain "w0rm" (case-insensitive) within 1 byte of the "USER" command.

The PCRE pattern must match, indicating a "USER w0rm" command.

Possible Attribution & Use Cases:

Recommended Actions:

Strengthen Authentication: Enforce strong passwords and consider using multi-factor authentication for FTP access.

Restrict Access: Implement firewall rules to restrict access to FTP services from untrusted networks.

Author & Attribution:

Rule Author: Community

Rule Source: Community

Rule SID: 144

Rule Revision: 16

Service: ftp