Threat Category: Protocol Anomaly, RPC Portmap Decode

Threat Description:

The SNORT rule is designed to detect attempts to list services using the UDP portmapper service. This rule focuses on traffic from an external network to an internal network on UDP port 32771. The detection mechanism involves checking for specific byte sequences within the UDP packet payload at specific offsets and depths. Specifically, it checks for "|00 01 86 A0|" at a depth of 4 and offset of 12, "|00 00 00 04|" within 4 bytes with a distance of 4, and "|00 00 00 00|" at a depth of 4 and offset of 4. These patterns are indicative of a request to the portmapper service to list available services.

Indicators of Compromise (IoCs):

UDP Port: 32771

Content Pattern 1: "|00 01 86 A0|" (depth 4, offset 12)

Content Pattern 2: "|00 00 00 04|" (within 4, distance 4)

Content Pattern 3: "|00 00 00 00|" (depth 4, offset 4)

Detection Mechanism:

The network protocol must be UDP.

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

The destination port must be 32771.

Possible Attribution & Use Cases:

The detection can be used to identify reconnaissance activity targeting RPC services.

This rule is useful for monitoring network traffic for attempts to map network services, which is often a precursor to exploitation.

Recommended Actions:

Monitor and Investigate: If this rule is triggered, investigate the source of the traffic and the targeted system to determine the intent of the portmap request.

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

Author & Attribution:

Rule Author: Community

Rule Source: Community

Rule SID: 1281

Rule Revision: 15

Metadata: policy max-detect-ips drop