Threat Category: Reconnaissance, DNS Tunneling

Threat Description: The SNORT rule TCP DNS traffic detected is designed to detect instances of Domain Name System (DNS) traffic being sent over the TCP protocol to port 53. While DNS traffic typically uses UDP, DNS over TCP is used for zone transfers or when responses exceed 512 bytes. However, attackers may also leverage TCP-based DNS for covert communication, data exfiltration, or command and control (C2) through DNS tunneling. This rule helps identify such anomalies, which may indicate reconnaissance activities or abuse of DNS for stealthy operations.

Indicators of Compromise (IoCs):

Protocol: TCP

Destination Port: 53 (DNS)

Any source/destination IP and port

Detection Mechanism:

This rule generates an alert when any TCP traffic is directed to port 53, which is reserved for DNS services.

Possible Attribution & Use Cases:

May be associated with attackers using DNS for data exfiltration or C2.

Useful for detecting abnormal DNS behavior in environments where TCP-based DNS is uncommon.

Recommended Actions:

Monitor and Analyze: Investigate the source and destination of TCP DNS traffic. Determine whether the activity is normal or suspicious.

Restrict if Necessary: If not needed in your network, limit DNS over TCP using firewall rules or access control lists.

Inspect Payload: Deep packet inspection may reveal if DNS is being used for tunneling or exfiltration.

Author & Attribution:

Rule Author: community

Rule Source: Custom

SID: 1000015

Revision: 1