Network Traffic Analysis

Tcpdump Analyzer Results

13:24:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A? yummyrecipesforme.com. (24)
13:24:36.098564 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2 udp port 53 unreachable length 254

13:26:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A? yummyrecipesforme.com. (24)
13:27:15.934126 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2 udp port 53 unreachable length 320

13:28:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A? yummyrecipesforme.com. (24)
13:28:50.022967 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2 udp port 53 unreachable length 150

Log Analysis

Details:

- Source IP: **192.51.100.15**
- Destination IP: **203.0.113.2**
- DNS Request for: **yummyrecipesforme.com**
- ICMP Protocol Used: ICMP is used to communicate errors and operational information. The ICMP messages here indicate an error, specifically that the **UDP port 53** is unreachable.

Issues Interpreted from the Logs:
The provided logs depict a series of DNS requests originating from the IP address **192.51.100.15** to the IP **203.0.113.2** on port **53**, which is typically associated with DNS. Following each DNS request, there is an ICMP packet indicating that the requested **UDP port 53** on the destination IP **203.0.113.2** is unreachable.

Incident Reporting, Investigation, and Solutions

Initial Reporting:
The problem was first reported at 13:24:32 or 1:24pm based on the timestamp of the first log entry.

Scenario, Events, and Symptoms:
Upon first observation, the system at IP **192.51.100.15** made DNS requests to the server at IP **203.0.113.2**. This was consistently met with ICMP error messages, indicating that the DNS

service was inaccessible. The symptoms are clear: DNS queries for **yummyrecipesforme.com** are not being resolved and are leading to ICMP error responses.

Investigation Findings:

- All attempts from the source IP to access the DNS service on the destination IP failed.
- ICMP responses consistently indicate that the **UDP port 53** on **203.0.113.2** is unreachable.
- The ICMP error lengths are variable, which might suggest differing payload sizes or potential variations in error messages.

Current Status:

DNS resolution for **yummyrecipesforme.**com via server **203.0.113.2** remains unsuccessful as of the last logged attempt at 13:28:50 or 1:28pm.

Suspected Root Cause:

The DNS service on **203.0.113.2** might be down, misconfigured, or there might be a network issue preventing access to **UDP port 53** on this server. It is possible that this is an indication of a malicious attack on the web server.

Suggested Solutions:

- Validate the network routes and firewall rules between **192.51.100.15** and **203.0.113.2** to ensure there are no blocks or misconfigurations.
- Check the status of the DNS service on **203.0.113.2**. If it's down, restart it. If it's misconfigured, correct the configuration. Ensure that the server's firewall or security group settings allow traffic on **port 53**.
- If the issue persists, consider using an alternative DNS server or seek insights from the administrators of **203.0.113.2**.

In Case of Malicious Activity:

- Network Monitoring and Traffic Analysis: Implement network monitoring solutions to identify anomalous or increased traffic to **203.0.113.2**. This will help in identifying any patterns that suggest a DDoS attack or other forms of malicious activities.
- Rate Limiting: To counter potential DDoS attacks, set rate limits on incoming requests to the DNS server. This helps in preventing the server from being overwhelmed by a flood of requests.
- DNS Security Extensions: Implement DNSSEC to add an extra layer of trust to DNS queries and responses. This prevents DNS cache poisoning and ensures that the DNS data has not been tampered with.
- Implement Intrusion Detection Systems and Intrusion Prevention Systems: IDS and IPS can help in identifying and blocking malicious traffic in real-time. Set rules specific to DNS attack patterns.

- Honeypots: Deploy honeypots in your network. If attackers target the honeypot, you can gain valuable insights into their methods, tools, and intent, while diverting their attention from actual critical assets.
- Ensure Regular Backups: Have regular backups of your DNS configurations and server settings. This allows for a quicker recovery in case of any malicious alterations.
- Update and Patch: Regularly update and patch your DNS server software to protect against known vulnerabilities.
- Incident Response Plan: If you suspect a malicious attack, activate your incident response team and plan. This should include isolating affected systems, conducting forensic analysis, and coordinating with relevant stakeholders (like ISPs or law enforcement if necessary).