

ARAIZ NAQVI



INCIDENT REPORT

yummyrecipesforme.com

02ND OCTOBER, 2024


2024-2025



ARAIZ NAQVI

TABLE OF CONTENT

- Problems Found
- Issue Analysis
- About me :)



2024-2025

DISCLAIMER

This incident report is a project-based simulation for the fictional organization yummyrecipesforme.com, as part of the "Fundamentals of Cybersecurity" course on Google's Coursera platform.

While the details may resemble real-world scenarios, all data, systems, and findings are entirely fictitious and created for educational purposes. This incident report does not reflect any actual incidents or vulnerabilities affecting any real organization, including yummyrecipesforme.com.

Though based on practical analysis and protocols, the assessments are conducted in a simulated environment and should not be considered representative of any real entity's security posture.

INCIDENT SUMMARY

Time of Incident: 13:24:32:192571 (1:24pm)

Summary of Incident: Several clients of *yummyrecipesforme.com* reported they could not reach the website, which showed the error 'destination port unreachable'.
When a UDP packet is sent to the DNS server, an ICMP response of 'UDP port 53 unavailable' is observed.

NETWORK TRAFFIC ANALYSIS

```
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
```

Protocols Involved:

ICMP, UDP, DNS

(PTO)

Summary of Log Data :

After the incoming issue, an attempt was made to ping the DNS server under tcpdump. Three attempts were made to record outgoing and incoming traffic.

The first attempt at 1:24 (converted time) sent a UDP packet to the DNS server from IP 192.51.100.15 port 52444 to destination DNS server 203.0.113.2 to yummyrecipesforme.com. This returned a 'UDP port 53 unavailable' error status response.

An additional 2 consequent responses were sent at 1:26 pm and 1:28 pm respectively with the exact same response.

There is a high possibility of high traffic due to Threat Actors or technical faults that are causing the DNS server to reject incoming queries and giving above error response.

IMPACT ASSESSMENT

Affected Services :

As a result of this issue, the Organisation *yummprecipesforme* is unable to carry out its regular services and the various website users are not able to enter the website to access existing information or browse more information of their interest from the website.

This may result in a huge hit in reputation, severe time and money to fix the issue, and legal penalties for any underlying lack of compliance.

ROOT CAUSE ANALYSIS

Potential Threat Actor Related Causes

This can be due to a possible DOS attack in one of the possible manners:

DNS Server Overload

The threat actor may have sent an overwhelming amount of traffic to the DNS server itself which could have caused it to drop legitimate queries and crash.

Network Infrastructure Overload

The threat actor may have sent an overwhelming amount of traffic to all of the Network Infrastructures like its routers, switches, firewalls, or load balancers, causing it to be unable to respond to UDP requests.

Resource Exhaustion

The threat actor may end up using all computational resources causing systems to crash and be useless.

(PTO)

Targeted Port 53 Attack

Additionally, port 53 may have been targeted and loaded with all/some of the above-mentioned attacks.

This can be due to a possible DDOS attack in one of the possible manners:

SYN Flood Attacks

The threat actor could've simulated a TCP connection by overloading SYN packets in the three handshake.

ICMP Pool

The threat actor may have sent multiple ICMP error messages to the network server, making it shut down, and keeping legitimate queries out.

Ping of Death

The threat actor could've sent an oversized ICMP packet that is greater than 64KB in size hence making execution time per packet very high.

(PTO)

This can also be due to a possible technical issue:

Firewall or Network Security Rules

The firewall may be improperly configured, resulting in requests being naturally declined.

DNS Server Not Listening

The DNS server might be running on port 53 but not listening on it, its configuration might have changed to a different port.

Physical Faults in Network

There might be physical faults in the network, like broken links, dysfunctional routers, etc that could be blocking incoming requests.

Improperly Configured DNS

The DNS server may be improperly configured and might not be pointing to the correct IP address.

(PTO)

CONCLUSION

The organization's Security Engineers are working towards concluding a plausible reason for the issue in question.

Once the reason and source are established, proper protocols and recovery procedures will be put in place for the smooth sailing of the organization's websites again.

Until then forensics and investigation are still underway.

Araiz Naqvi

Network Security Engineer

If you
find this
helpful, you'll
love my
content!

M @araiz-naqvi

in @araiznaqvi

