Security incident report

Maria Audu

Section 1: Identify the network protocol involved in the incident
The network protocol involved in the incident is **DNS (Domain Name System)**, which uses **UDP on port 53**. The error messages shown in the tcpdump log (“udp port 53 unreachable”) indicate that DNS traffic over UDP was failing, preventing the domain name from being resolved to an IP address.

Section 2: Document the incident
Cybersecurity Incident Report **Incident Title** DNS Service Disruption Causing Website Access Failure **Date/Time Reported** Approximately **1:24 p.m.**, based on tcpdump timestamps **Reported By** Cybersecurity Analyst **Affected Asset** Client website: **www.yummyrecipesforme.com**
Incident Summary Multiple users reported being unable to access the website *www.yummyrecipesforme.com* and receiving a “destination port unreachable” error. Network traffic analysis revealed that DNS requests sent from client systems were failing due to an unreachable DNS service.
Protocols and Services Involved • **DNS (Domain Name System)** – impacted service • **UDP (User Datagram Protocol)** – transport protocol used for DNS queries • **ICMP (Internet Control Message Protocol)** – used to return error messages

Technical Findings

- Client systems sent DNS queries over **UDP port 53** to the DNS server (IP: 203.0.113.2).
- The DNS server responded with **ICMP error messages** stating **"udp port 53 unreachable."**
- Multiple attempts resulted in the same ICMP error, indicating a persistent issue.
- Because DNS resolution failed, the browser could not obtain an IP address, preventing HTTPS communication with the web server.

Impact

- Users were unable to resolve the domain name.
- Website access was unavailable for affected users.
- Business services relying on the website were disrupted.

Suspected Root Cause

The DNS server was not accepting traffic on **UDP port 53**, likely due to:

- DNS service not running
- Firewall or network security rule blocking port 53
- DNS server misconfiguration

Current Status

The issue has been identified and escalated to security engineers for remediation. DNS traffic remains disrupted at the time of reporting.

Recommended Next Steps

1. Verify that the DNS service is active and listening on UDP port 53.
2. Review firewall and network security configurations.
3. Restart or reconfigure DNS services if necessary.
4. Test DNS resolution after changes are applied.
5. Monitor traffic to ensure normal DNS responses resume.

Conclusion

The incident was caused by a failure of **DNS over UDP (port 53)**, resulting in ICMP "port unreachable" errors and preventing users from accessing the website.

Section 3: Recommend one remediation for brute force attacks
Recommended remediation: Implement **account lockout policies** that temporarily lock an account after a

defined number of failed login attempts.

Explanation:

Account lockout policies prevent attackers from repeatedly guessing passwords by limiting the number of authentication attempts. This significantly reduces the effectiveness of brute force attacks and alerts administrators to suspicious login activity so it can be investigated quickly.