The Exemplar Explained  
Cybersecurity Incident Report: Network Traffic Analysis

|  |  |
| --- | --- |
| Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log | Explanation |
| 1. The tcpdump log showed that my computer sent a DNS request using UDP to the DNS server 203.0.113.2 to get the IP for yummyrecipesforme.com. The response came back with ICMP errors saying “udp port 53 unreachable.” Since port 53 is used for DNS, that basically means the DNS request didn’t go through and the server wasn’t responding like it should. 2. The log showed UDP packets being sent out from my IP (192.51.100.15) to the DNS server and ICMP messages coming back right after. The query number 35084 and the “A?” flag showed that it was a normal DNS lookup. The ICMP error showed up a few times, so it wasn’t just one failed attempt, the connection to the DNS server was completely failing. 3. Because port 53 wasn’t responding, it’s clear that something was wrong with the DNS service. It could mean the server was down, the traffic was being blocked, or maybe there was a DoS attack hitting it. Either way, it stopped the DNS from working, which caused the website to be unreachable. | 1. After checking the tcpdump log, I saw that my computer sent a DNS request using UDP to the DNS server at 203.0.113.2 to get the IP address for yummyrecipesforme.com. The DNS server replied with ICMP messages saying “udp port 53 unreachable.” Since port 53 is used for DNS, this means the DNS request didn’t go through and the server wasn’t responding properly. Provide a few details on what was indicated in the log. 2. The first few lines in the log show the outgoing UDP packets from my IP address (192.51.100.15) to the DNS server (203.0.113.2.domain). Then, there are ICMP responses from the server back to my computer with the error “udp port 53 unreachable.” The query ID number 35084 with the “+” and “A?” flags shows it was a DNS A record lookup. Since the ICMP responses happened multiple times, it confirms that there was a consistent issue with DNS communication. 3. Because port 53 was unreachable, and that port is used for DNS, the problem clearly has to do with the DNS server not responding. This could mean the server was down or something was blocking traffic to it. It might also be the result of a DoS attack that flooded the server, or a network issue like a firewall blocking UDP traffic on that port. |
|

|  |  |
| --- | --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident | Explanation |
| 1. When the problem was first reported the timestamp in the tcpdump log, 13:24:32.192571, shows that the issue happened around 1:24 p.m. 2. A few customers reached out because they couldn’t get on yummyrecipesforme.com, and they kept getting the same port unreachable message. When I tried it myself, the page didn’t load either, so I ran tcpdump to see what was going on. That’s when I saw the UDP requests going out and the ICMP errors coming back. 3. The problem has been reported and passed on to the security engineers. They’re currently checking if the DNS server is actually down or if there’s some kind of block on the network side. For now, the DNS is still not responding, so users can’t reach the website. 4. Every time a UDP request goes out, it’s followed by an ICMP “port 53 unreachable” message. That tells us the DNS server isn’t responding at all, which is likely the main reason the website isn’t loading for anyone. 5. The next thing to check is whether the DNS server itself is offline or crashed. If it’s running, then we’ll look at the firewall settings to make sure port 53 isn’t being blocked. If both of those are fine, we might need to check for any signs of a DoS attack or another kind of network disruption. 6. The most likely cause is either a Denial of Service (DoS) attack that flooded the DNS server and made it stop responding, or a firewall misconfiguration that’s blocking traffic on port 53. | 1. The timestamps in the tcpdump log show the time 13:24:32.192571, which means the issue happened around 1:24 p.m. today. Around that time, users started saying they couldn’t reach the website and got the “destination port unreachable” error. 2. A few customers contacted the company saying they couldn’t access yummyrecipesforme.com and saw the “destination port unreachable” message after waiting for the page to load. When I tested it myself, I got the same result. That’s when I used tcpdump to check the traffic and found the DNS errors. 3. At this point, the issue has been reported to management, and the security engineers are handling it. They’re trying to figure out if it’s the DNS server itself or something blocking the traffic. 4. By analyzing the tcpdump results, I confirmed that UDP packets were sent out but the only replies were ICMP messages saying port 53 was unreachable. That means the DNS server wasn’t answering, which explains why users couldn’t reach the website. 5. The next steps are to check whether the DNS server is offline or unresponsive. If it’s running fine, then the firewall settings need to be checked in case someone accidentally blocked traffic on port 53. If it’s not a config issue, the team might need to check for signs of a DoS attack on the DNS server. 6. Right now, the most likely cause is either a Denial of Service (DoS) attack that took down or overloaded the DNS server, or a firewall misconfiguration that blocked UDP traffic on port 53. Both would stop DNS queries from getting through and explain why users couldn’t access the site. |