Cybersecurity Incident Report:

Network Traffic Analysis

|  |
| --- |
| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log. |
| The UDP protocol reveals that:  The UDP packet sent to port 53 of the DNS server was undeliverable. In the first line of the error log, the query identification number appears as 35084, along with associated flags. The "A?" flag indicates that the request was for an A record, which is used to map a domain name to an IP address.  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message:  "UDP port 53 unreachable", indicating that the DNS request could not reach a listening service on the destination server.  The port noted in the error message is used for:  Port 53, which is dedicated to DNS services. In this case, it was being used to resolve the domain "yummyrecipesforme.com" through the DNS server at 203.0.113.2.  The most likely issue is:  A problem with the DNS provider is preventing requests from being processed, likely due to the DNS service being down, misconfigured, or blocked, resulting in port 53 being unreachable. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred: the incident began at 13:24:32.192571 (1:24 PM and 32.192571 seconds), as indicated by the timestamp of the first outgoing DNS request.  Explain how the IT team became aware of the incident: through these 3 steps:  1. User reports of an inability to access the website (yummyrecipesforme.com).  2. Network monitoring alerts detecting repeated failed DNS requests.  3. Log analysis showing ICMP error messages indicating that UDP port 53 was unreachable.  Explain the actions taken by the IT department to investigate the incident:  1. Log review: The IT team analyzed network traffic logs to identify failed DNS requests and ICMP error responses.  2. DNS server check: They verified if the DNS server at 203.0.113.2 was operational and listening on port 53.  3. Network connectivity test: They performed tests (e.g., ping, traceroute, or nslookup) to check connectivity between 192.51.100.15 (client) and 203.0.113.2 (DNS server).  4. Firewall and security policies: They checked for any firewall rules or security settings that might have blocked DNS traffic.  5. Service status check: They ensured that the DNS service was running properly on 203.0.113.2.  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):  1. Port affected: UDP port 53 (DNS service).  2. Source IP: 192.51.100.15 (Client trying to resolve the domain name).  3. Destination IP: 203.0.113.2 (DNS server).  4. Issue detected: The DNS server at 203.0.113.2 responded with an ICMP error (port unreachable), meaning no service was listening on port 53.  5. epeated failure: The same issue occurred multiple times at 13:24:32, 13:26:32, and 13:28:32.  Note a likely cause of the incident:  1. DNS server failure: The DNS server at 203.0.113.2 was likely down, misconfigured, or not running a DNS service on port 53.  2. Firewall or security settings: A firewall or network policy might have been blocking incoming or outgoing DNS requests.  3. Network connectivity issue: Routing issues or misconfigurations might have prevented access to the DNS server. |