Cybersecurity Incident Report Yummi Recipes

Part 1: Summary of the Problem Found in the DNS and ICMP Traffic Log

Upon analyzing the network protocol analyzer logs, it was observed that attempts to access the secure employee background check website resulted in the inability to reach port 443, which is typically used for HTTPS traffic. This indicates a potential issue with either the web server or the firewall configuration. The possibility of a malicious attack on the web server cannot be ruled out.

Part 2: Analysis of the Data and Proposed Solution

Earlier this morning, the human resources (HR) team reported an issue with accessing the background check web portal. In response, the network security team conducted tests using the network protocol analyzer tool tcpdump. The analysis of the resulting logs revealed that port 443, responsible for handling HTTPS traffic, was found to be unreachable.

To address this incident, further investigation is underway to identify the root cause and restore access to the secure web portal. Our immediate course of action includes examining the firewall configuration to determine if port 443 is blocked. Additionally, we will contact the system administrator responsible for the web server to investigate any signs of a potential attack.

It is worth mentioning that the HR team suspects a particular new hire who may have motives to obstruct the background check process. The network security team has also considered the possibility of an intentional attack aimed at disrupting the background check website.

To mitigate the incident and restore normal operations, the following steps will be taken:

1. Verify the firewall configuration to ensure that port 443 is open and properly configured to allow HTTPS traffic.
2. Engage the system administrator responsible for the web server to investigate any indicators of an attack, such as unusual log entries or suspicious system behavior.
3. Implement additional security measures, such as intrusion detection systems (IDS) or web application firewalls (WAF), to enhance the protection of the background check website.
4. Conduct a thorough review of access controls and user permissions for the web portal to prevent unauthorized access.

By following these steps, we aim to identify and resolve the issue promptly, ensuring the availability and integrity of the background check website while addressing any potential security concerns.

DNS & ICMP Traffic Log

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