**Incident report**

SCENERIO

Review the scenerio’s below, then complete the step-by-step instructions.

You arer a cybersecurity analyst working for a multimedia company that offers web design service, graphic design and social media marketing solutions to small businesses. Your organizations recently experiences a DDoS attack which compromised the internal network for two hours until it was resolved.

During the attack, your organization’s network suddenly stopped responding due to an incoming flood of packets. normal internal network traffic could not access any network resources, the incident management team responded by blocking incoming ICMP packets stopping all non ciritical network services offline, and restoring critical network access.

The company’s cybersecurity team then investigated the security event, they found that a malicious actor had sent a flood of ICMP pings into the company’s network through unconfigured firewall. this vulnerability allowed the malicious attacker to overwhelm the company’s network through a DISTRIBUTED DENIAL OF SERVICE (DDoS) attack.

To address this security event, the network security team implenmented:

* A new firewall rule to limit the incoming ICMP packets.
* Source IP address verification on the firewall to check for spofed IP afddressses on incoming ICMP packets.
* Networkmonitoring software to detect abnormal traffic patterns.
* An IDS/IPS system to filter out some ICMP traffic based on suspicioys characteristics.

As a cybersecurity analyst, you are tasked with using this security event to create a plan to improve your company’s network security, following the National Institute of Standard and technology (NIST) cybersecurity framework (CSF). you will use the CSF to help you navigate through different steps of analyzing the cybersecurity event and integrate your analysis into a general security strategy.

Step-byStep instructions

1. Acess the incident report analysis
2. Summarize the security event
3. Identify the type of attack and the systems affected
4. Protect the assets in your organization fron being compromised
5. Detect similar incidents in the future
6. Respond to future cybersecurity incidents
7. Recover from the incident
8. You will complete a self assesment for your incident report porfolio activity

**Incident Responce Analysis:** Applying the NIST framework to the incident report

|  |  |
| --- | --- |
| **Summary** | The company experienced a security event when all network services suddenly stopped responding. The security team found the disruption was caused by a distributed denial of services (DDoS) attack through a flood of incoming ICMP packets. The team responded by blocking the attack and stopping all non-critical network services, so that critical network services could be restored. |
| Identify | A malicious/threat actor targeted the company using DDoS attack flooding the network system with ICMP packets,the entire internal network was affected. all critical network resources needed to the secured and restored to a functioning state. |
| Protect | **the security team implemented a new firewall rule to limit/filter the rate of incoming ICMP packets, and an IDS/IPS to filter out some ICMP traffic based on suspicious activity/characteristics.** |
| Detect | The security team configured source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets and implemented network monitoring software to detect abnormal traffic patterns. |
| Respond | For future security attacks/threats, the cybersecurity team will isolate affected systems to prevent further disruption to the network. They will attempt to restore any critical systems and services that were disrupted by the event. Then, the team will analyze network logs to check for suspicious and abnormal activity. The team will also report all incidents to upper management and appropriate legal authorities, if applicable. |
| Recover | To recover from a DDoS attack, access to network services need to be restored to a normal functioning state. In the future external icmp flood attacks can be blocked at the firewall, then all non-critical network services  should be stopped to reduce internal network traffic. NEXT, critical network services should be restored first. FINALLY once the flood of incoming ICMP packets are timed out , all non-critical network services should be brought back online. |

|  |
| --- |
| Reflections/Notes: The NIST CSF core functions provide a framework of planning proactive to applying reactive measures to cybersecurity threats. These functions are essential for ensuring that an organization has effective security strategies in place. An organization must have the ability to quickly recover from any damage caused by an incident to minimize their level of risk. |
|  |