Incident report analysis

Instructions

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this chart as a way to practice applying the NIST framework to different situations you encounter.

Summary	The organization’s network services suddenly stopped responding due to an incoming flood of ICMP packets. Normal internal network traffic could not access any network resources disabling the regular functions of the company. The suspicious overwhelm of network traffic was investigated by the security team. It was found that there was a flood of ICMP packets, rendering the server inactive. As a result, no one in the company was able to access the resources.
Identify	The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. Upon review, it seems like a malicious actor had sent a flood of ICMP pings into the company’s network through an unconfigured firewall. This vulnerability allowed the malicious attacker to overwhelm the company’s network through a distributed denial of service (DDoS) attack.
Protect	To ensure that the organization’s assets are adequately secured, the company should set policies to make sure that most attack surfaces are mitigated through security measures. Making sure no setting is misconfigured in the network space, for example, and thorough port

	filtering can help decrease the chances of a malicious actor accessing a device. It is highly recommended to institutionalize network segmentation to ensure that it becomes harder for an attacker to have a huge impact with their DDoS attack.
Detect	To address this security event, the network security team implemented A new firewall rule to limit the rate of incoming ICMP packets. They also implemented Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets. There is also a network monitoring software put in place to detect abnormal traffic patterns. An IDS/IPS system is configured to filter out some ICMP traffic based on suspicious characteristics.
Respond	If there is a case where a server is attacked through denial of service, the security team will respond by trying to contain the impact by isolating that network that is impacted from the general company network. Next time an attacker tries to attack through an unconfigured security setup, we will make sure to update patches and mitigate the issue at hand, and similar issues in other branches of the department. To analyze this incident, security personnel can use a SIEM tool, or use packet sniffing tools like Wireshark or Tcpdump to analyze the network traffic and look for suspicious activity in the logs. The company should keep updating the baseline configurations and incident playbooks to better handle future cybersecurity incidents,
Recover	To recover from a DDoS attack by ICMP flooding, 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 ICMP packets have timed out, all non-critical network systems and services can be brought back online.

Reflections/Notes: