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 company faced a security incident when all network services suddenly became unresponsive. The cybersecurity team traced the issue to a distributed denial of service (DDoS) attack, triggered by a surge of incoming ICMP packets. In response, the team blocked the attack and temporarily shut down non-essential services to ensure the restoration of critical network operations.
Identify	The company was targeted by one or more malicious actors using an ICMP flood attack, which impacted the entire internal network. As a result, all critical network resources had to be secured and brought back to a fully functional state
Protect	The cybersecurity team set up a new firewall rule to restrict the influx of ICMP packets and deployed an IDS/IPS system to filter out suspicious ICMP traffic
Detect	The cybersecurity team set up source IP address validation on the firewall to identify spoofed IP addresses in incoming ICMP packets and deployed network monitoring software to detect unusual traffic patterns
Respond	Going forward, the cybersecurity team will isolate compromised systems to

	prevent further network disruption. They will focus on restoring any critical systems and services impacted by the incident. Afterward, the team will analyze network logs to identify any unusual or suspicious activity. All incidents will also be reported to senior management and, when applicable, to the appropriate legal authorities
Recover	To recover from an ICMP flood DDoS attack, it's essential to restore network services to normal operation. Non-essential services should then be temporarily halted to reduce internal traffic, allowing critical services to be restored first. Once the ICMP packet flood no longer in effect, non-essential systems and services can be brought back online.

Reflections/Notes: As a junior analyst, I gained valuable insight from responding to a DDoS attack caused by an ICMP flood. When the network services went down, I watched as the cybersecurity team quickly identified the threat and took action. They implemented firewall rules to limit the flow of ICMP packets and deployed an IDS/IPS system to filter out suspicious traffic. I was particularly fascinated by the use of source IP verification to detect spoofed IP addresses and how network monitoring helped identify abnormal traffic patterns.

Reflecting on the process, I've learned that isolating affected systems quickly can prevent further disruptions. Restoring critical services first is essential, followed by a detailed analysis of network logs to spot any suspicious activity. It's also important to report incidents to management and legal authorities. Going forward, blocking external ICMP flood attacks at the firewall, temporarily shutting down non-essential services, and focusing on critical operations are key steps to handling these situations more effectively. Once the flood subsides, the restoration of non-critical services can proceed gradually.

This experience has reinforced the importance of a proactive, methodical approach to security. It's an invaluable learning opportunity that has sharpened my skills and understanding, helping me grow as an analyst in the field of cybersecurity.