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	Earlier today, the network experienced a company-wide stoppage of services. For two hours, employees could not access the internal network resources, and company operations came to a halt. After logging into a station, any attempt to run company tools or applications would be followed by an error message or they would simply not run. The security team believed that this denial of service was either caused by a hardware issue or a malicious attack. In response to the incident, our cybersecurity team added a configuration rule to the firewall to prevent ICMP packet requests from being accepted into our network. Additionally, all non-critical network services were temporarily disabled.
Identify	Using our network traffic analysis tool, we found that there was an excessive amount of incoming ICMP request packets originating from multiple distinct IP addresses. The flood of ICMP pings passed through the network's firewall, undetected, and left no available ports to allow for normal tasks or activities. The firewall was not configured to detect excessive ICMP pings. The analysis led us to conclude that our network was overwhelmed by a malicious actor conducting a distributed denial of service (DDoS) attack against the organization.

Protect	To prevent future attacks, the cybersecurity team configured a new firewall rule that limits the rate of incoming ICMP packets. The firewall was also equipped with IP address verification to ensure any incoming ICMP packets with spoofed IP addresses would be denied entry. An intrusion protection system was added to filter out any suspicious ICMP traffic by dropping these type of requests before they reach our internal network.
Detect	To detect future DDoS ICMP ping flooding attacks, a new intrusion detection system was implemented. This IDS will filter out ICMP packets with any suspicious characteristics. In addition to this, we invested in network monitoring software that detects abnormal traffic patterns, which our analysts can use as needed.
Respond	In response to the DDoS attack, our management team temporarily blocked all incoming ICMP packets, and rendered all non-critical network services offline. In the 2 hours of network downtime, employees were given an impromptu refresher training on the importance of keeping company information and access credentials confidential, and the negative impact a DDoS attack can have on company operations. For future DDoS attacks, our team now has the additional tools IDS/IPS and network monitoring tools, as well as new firewall configurations to examine to respond more quickly and efficiently.
Recover	Critical network services were restored from backups once ports became available after stopping the ICMP flooding. Any clients of our multimedia services who were expecting our products or services within those hours of downtime should be contacted and made aware of the issue, to ensure transparency and maintain trust.

Reflections/Notes: