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	This morning, the company experienced a security event that resulted in the sudden unresponsiveness of all network services. Initial analysis indicated that the incident may have been a denial of service (DoS) attack. However, further investigation revealed that it was, in fact, a distributed denial of service (DDoS) attack, resulting in the disruption of the internal network and services for approximately two hours. The incident was caused by an unconfigured firewall that allowed the threat actor to overwhelm the server with ICMP packets. The response team took immediate action to contain and eradicate the threat by blocking all ICMP packets, stopping all non-critical network services offline, and restoring critical network services.
Identify	The security team conducted an audit of the company's internal networks, systems, devices, and access privileges to identify potential security vulnerabilities. The audit revealed that an unconfigured firewall had been exploited by a threat actor, allowing them to send a significant volume of ICMP packets that resulted in the disruption of the company's internal network. This resulted in employees being unable to access any network resources.
Protect	The cybersecurity team implemented a new firewall rule to restrict the rate of incoming ICMP packets and integrated an IPS/IDS to assist in filtering

	certain traffic from an unknown IP address and based on suspicious activity.
Detect	The cybersecurity team has implemented an IP address verification process on the firewall. This process allows the security team to check for spoofed IP addresses on incoming ICMP packets, helping them to verify any unusual activity and respond with greater efficiency.
Respond	In the event of a security incident, the cybersecurity team will take immediate action to isolate and contain the affected areas to prevent the threat from spreading to other systems and networks. All incidents will be promptly reported to relevant stakeholders and upper management. If necessary, the relevant federal and governmental authorities will also be informed.
Recover	It is critical to restore network services to a normal functioning state in order to recover from a DDoS attack by ICMP flooding. Once the firewall rules have been updated to allow for the blocking of external ICMP flood attacks, it is advisable to stop all non-critical network services in order to reduce internal network traffic. Following this, critical network services should be restored, and finally, once the flood of ICMP packets has timed out, all non-critical network systems and services can be brought back online.