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	Today, we received information that company employees could not log into their emails. The team of analysts began an investigation, which revealed that the company was the victim of a DDoS attack. The internal network of the company was compromised, resulting in all services being unavailable for approximately 2 hours. The team stopped the stream of ICMP requests that were causing the overload. Analysts blocked incoming requests, shut down all non-critical services, and restored critical services to their baseline state. It was determined that the cause was an ICMP flood. This resulted from the lack of proper firewall configuration.
Identify	The attack carried out was a DDoS attack. It involves "flooding" the company's server with a large number of ICMP requests from multiple sources simultaneously. In the flood of incoming requests, the server becomes overloaded and stops responding to any other requests. As a result, the entire internal network, including the company's website, corporate email, and databases, stops functioning.
Protect	Security analysts recommend strengthening the security and resilience of the internal network against external attacks. First and foremost, they recommend

	updating firewall rules to block all unnecessary ports and unknown packet sources. They also advise using Intrusion Prevention Systems (IPS), which significantly enhance network security by actively blocking suspicious traffic.
Detect	Analysts also recommend using Intrusion Detection Systems (IDS) to detect suspicious traffic or queries from unknown sources early on. Security Information and Event Management (SIEM) tools are also advised, as they enable analysts to more effectively, quickly, and preemptively detect potential threats, and consequently, respond to them faster.
Respond	Strengthening Security and Detection Speed. Firstly, frequent firewall updates for new data. Have an action plan/procedures in place for a similar incident (shutting down non-critical services to minimize losses, quickly analyzing critical services, and restoring them to operation). Analyzing logs using tools such as tcmdump. Having a baseline configuration. Frequently updating backup copies of servers.
Recover	To be able to quickly restore a compromised system, a baseline configuration is essential to compare the source code for any potential changes. Up-to-date backups of servers are also crucial to swiftly restore them to operation.

Reflections/Notes: