Incident report analysis

Introduction

In today's interconnected world, businesses and organizations face various security threats, including distributed denial-of-service (DDoS) attacks. In this incident report analysis, we will examine a DDoS attack that targeted a company's network, disrupting critical services. We will explore the incident's impact, the response and recovery measures taken by the cybersecurity team, and the lessons learned from the experience. This analysis aims to provide insights into the importance of robust cybersecurity measures and the need for organizations to have a well-defined incident response plan in place.

Summary	The company experienced a security event when all network services suddenly stopped responding. The cybersecurity team found the disruption was caused by a distributed denial of services (DDoS) attack through a flood of incoming ICMP packets. The team responded by blocking the attack and stopping all non-critical network services, so that critical network services could be restored.
Identify	The cybersecurity team discovered malicious attackers or an attack has targeted the company with ICMP flood attack. The internal network was affected .All critical network assets needed to be secured and restored to functioning state
Protect	The cybersecurity team implemented a new firewall rule to limit the rate of incoming ICMP packets and an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
Detect	The cybersecurity team configured source ip address verification on the firewall to check for spoofed ip addresses on incoming ICMP packets and

	implemented network monitoring software to detect abnormal traffic patterns.
Respond	To mitigate the impact of future security incidents, the cybersecurity team will isolate affected systems, preventing further disruption to the network. They will prioritize restoring critical systems and services that were affected by the incident. Subsequently, the team will analyze network logs for suspicious or abnormal activities. Additionally, the team will report all incidents to senior management and the appropriate legal authorities, as necessary.
Recover	To recover from a distributed denial-of-service (DDoS) attack resulting from ICMP flooding, network services must be restored to normal functioning. In the future, external ICMP flood attacks can be blocked at the firewall. Then, non-critical network services should be stopped to minimize internal network traffic. Afterward, critical network services should be restored as a priority. Finally, after the ICMP packet flood times out, all non-critical network systems and services can be brought back online.

Reflections/Notes:

- DDoS attack disrupted network services, emphasizing the need for security measures.
- Cybersecurity team blocked attack and restored critical services.
- Implemented security measures to prevent future attacks.
- Plan includes isolating affected systems, restoring critical services, and reporting incidents.
- The recovery plan outlines steps to restore services and minimize future attacks.
- Incident report analysis provides insights into the company's response, highlighting the importance of a defined incident response plan.