Incident report analysis

Summary	Our company recently experienced a DDoS attack that disrupted our internal network for two hours. The attack involved a flood of ICMP pings sent by a malicious actor through an unconfigured firewall, causing our network services to stop responding. The incident management team reacted by blocking incoming ICMP packets, stopping non-critical network services, and restoring critical ones. To address this event, the cybersecurity team implemented new security measures like a firewall rule to limit incoming ICMP packets, source IP address verification, network monitoring software, and an IDS/IPS system to filter out suspicious ICMP traffic.
Identify	The type of attack experienced was a Distributed Denial of Service (DDoS) attack, which overwhelmed the company's network with a flood of ICMP pings. The attack compromised the internal network, causing network services to stop responding.
Protect	To protect the organization's assets from being compromised in the future, it is important to implement strong network security measures such as firewall configurations, intrusion detection systems, and regular security updates. Additionally, conducting regular security assessments and employee training on phishing awareness can help prevent future attacks. Setting up a response plan for DDoS attacks and utilizing DDoS protection services can also help in mitigating the impact of such attacks.
Detect	One way to detect similar incidents in the future is by implementing a robust incident detection and response system. This system should include continuous monitoring of network activity using intrusion detection systems, security information and event management (SIEM) tools, and data loss

	prevention (DLP) solutions. By monitoring network traffic and user behavior patterns, as well as setting up alerts for suspicious activity, organizations can quickly identify and respond to potential security incidents before they escalate. Regular security audits and penetration testing can also help identify vulnerabilities and potential threats to the organization's assets.
Respond	- Develop an incident response plan outlining the steps to be taken in the event of a cybersecurity incident. - Conduct regular tabletop exercises to test the effectiveness of our incident response plan.
Recover	- Develop a system recovery plan to restore affected systems to normal operation and recover any impacted data or assets. - Implement regular backups of critical data and systems to ensure quick recovery in case of a security incident.

Reflections/Notes: