**Incident report analysis**

| **Summary** | Our company experienced a DDos attack, which caused the systems to be down for two hours. This attack caused the network services to be down due to an influx of ICMP packets. After investigation, the cybersecurity team found that a malicious actor had sent a flood of ICMP pings to the company’s network through an unconfigured firewall. | | |
| --- | --- | --- | --- |
| Identify | The attack that occurred was a DDoS attack, due to the flooding of ICMP pings. We identified that the attack was an ICMP flood targeting our entire internal network. All our essential services were affected, so our first priority was securing and bringing those back up. | | |
| Protect | To prevent this in the future, we added a firewall rule to limit how many ICMP packets could come in at once. We also set up an IDS/IPS system to filter suspicious ICMP traffic before it could cause problems. | | |
| Detect | We configured our firewall to verify source IPs to catch spoofed addresses and deployed network monitoring tools to help us spot unusual traffic patterns quickly. | | |
| Respond | Next time this happens, we’ll isolate the affected systems right away to contain the issue. Our plan is to get critical services up first, then dig through the logs to understand what happened. We’ll also make sure to notify leadership and legal if needed. | | |
| Recover | To recover from an ICMP flood, we first need to bring network access back to normal. That means blocking the flood at the firewall, pausing non-essential services, and restoring critical ones first. Once the attack fades, we can safely bring everything else back online. | | |

| Reflections/Notes: |
| --- |