# 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 experienced a denial of service attack which caused the network to suddenly stop functioning. During this time, the internal network department was unable to access any network resources. This attack affected our internal network operations for two hours. The incident management team limited the use of the network for non critical activities and blocked incoming ICMP packets until normal operations were restored. |
| Identify | The cybersecurity team investigated the incident and determined that a malicious actor flooded the internal network with ICMP packets through an unconfigured firewall, resulting in a DDoS attack. |
| Protect | The cybersecurity team applied configurations to the firewall to limit the amount of ICMP packets a server can receive. Additionally they implemented IDS/IPS systems to monitor traffic, block senders and drop suspicious packets. |
| Detect | The security team introduced a network monitoring software, updated the firewall to verify IP addresses and to check for spoofed IP addresses on incoming ICMP packets. |
| Respond | To prevent future DDoS attacks utilizing a packet sniffer such as tcpdump can |

| | |
|---|---|
| | help monitor the traffic in the network and identify suspicious activity. Any ports and devices that are not being used for normal operations can be removed or disabled. A proxy server can also be used to determine what packets are safe to be transmitted.  Penetration tests can be conducted to determine vulnerabilities that require hardening within the network prior to attacks occurring. The organization can use network segmentation to prevent each department from being affected during attacks. Finally the use of VPNs, encryption, and HTTPS protocols can harden the network. |
| Recover | The normal operations of the internal network were restored after two hours of investigation and implementation of additional security measurements. Recovering from a DDoS attack, normal business operations were paused, incoming ICMP packets were disabled, and the firewall was configured to limit the amount of ICMP requests. The IPS was integrated to monitor activities, block senders and drop suspicious ICMP packets. Normal operations were restored and resources are now available for use. |

---

Reflections/Notes: