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	We recently experienced a DDoS attack that brought down our internal network for about two hours. The attack was carried out using a flood of ICMP packets and was able to get through because of an unconfigured firewall. During the attack, our systems couldn't communicate internally, which really affected productivity. The incident response team acted quickly by blocking incoming ICMP traffic and shutting down non-essential services, then restored the critical ones. Afterward, we made some changes to help prevent this from happening again.
Identify	• Our firewall wasn't properly configured to block or limit ICMP traffic. • We hadn't done a recent audit of our firewall rules or network settings. • There was no clear picture of what "normal" network activity looked like, which made the attack harder to spot at first.
Protect	• We added a rule to limit how much ICMP traffic we accept. • We also set up source IP verification to help catch fake IP addresses. **Still needed:** • Better staff training on securing network configurations. • More thorough documentation of our network and security setups. • Stronger access control policies to minimize risks.

Detect	• We installed monitoring software to track unusual traffic patterns. • We also added an IDS/IPS to filter out suspicious traffic. **Next steps:** • Set up alerts for things like ICMP spikes or strange traffic from one IP. • Create a “normal traffic” baseline so we can spot weird behavior faster. • Start pulling logs into a central place where we can review them more easily.
Respond	• We blocked ICMP traffic as soon as we spotted the problem. • We shut down non-essential services to keep bandwidth available for recovery. • Then we focused on bringing critical systems back online. **What we should improve:** • A formal incident response plan that clearly outlines who does what. • Regular practice drills so we’re not scrambling next time. • A communication process for letting key people know what’s going on during an incident.
Recover	• Once the flood traffic was filtered out, we restored the systems. • The fix worked, but it showed we need better planning for recovery scenarios. **Recovery goals for the future:** • Test our backup and recovery plans regularly. • Write a recovery checklist for incidents like this. • Review what happened and make sure we update our defences.

Reflections/Notes:
This incident was a wake-up call. It showed how one missed configuration can have a big impact and how important it is to think ahead. I saw how useful the NIST Cybersecurity Framework can be

in guiding not just our responses, but how we think about our entire approach to security. Going forward, I want to focus more on prevention, planning, and visibility.