Incident report analysis

Scenario

You are a cybersecurity analyst working for a multimedia company that offers web design services, graphic design, and social media marketing solutions to small businesses. Your organization recently experienced a DDoS attack, which compromised the internal network for two hours until it was resolved.

During the attack, your organization’s network services suddenly stopped responding due to an incoming flood of ICMP packets. Normal internal network traffic could not access any network resources. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.

The company’s cybersecurity team then investigated the security event. They found that a malicious actor had sent a flood of ICMP pings into the company’s network through an unconfigured firewall. This vulnerability allowed the malicious attacker to overwhelm the company’s network through a distributed denial of service (DDoS) attack.

To address this security event, the network security team implemented:

- A new firewall rule to limit the rate of incoming ICMP packets
- Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets
- Network monitoring software to detect abnormal traffic patterns
- An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics

As a cybersecurity analyst, you are tasked with using this security event to create a plan to improve your company’s network security, following the National Institute of

Standards and Technology (NIST) Cybersecurity Framework (CSF). You will use the CSF to help you navigate through the different steps of analyzing this cybersecurity event and integrate your analysis into a general security strategy. We have broken the analysis into different parts in the template below. You can explore them here:

- Identify security risks through regular audits of internal networks, systems, devices, and access privileges to identify potential gaps in security.
- Protect internal assets through the implementation of policies, procedures, training and tools that help mitigate cybersecurity threats.
- Detect potential security incidents and improve monitoring capabilities to increase the speed and efficiency of detections.
- Respond to contain, neutralize, and analyze security incidents; implement improvements to the security process.

Recover affected systems to normal operation and restore systems data and/or assets that have been affected by an incident.

Summary	● Understand the organization's environment to manage cybersecurity risks. ● Implement safeguards to ensure delivery of critical services. ● Identify the occurrence of a cybersecurity event. ● Take action after detecting a cybersecurity event. ● Restore services and reduce the impact of similar future incidents.
Identify	**Conduct regular security audits** of firewalls, routers, and other network devices to ensure they are properly configured. **Review and document network architecture** to identify unprotected entry points, like the unconfigured firewall exploited in the attack.

	Evaluate and update asset inventories (hardware, software, systems). **Assess risk exposure** related to protocols like ICMP and identify areas where restrictions should be applied. **Establish a baseline for normal network activity** to help distinguish malicious traffic
Protect	**Configure firewalls properly** and apply rate-limiting for protocols like ICMP to prevent flooding**.** **Enforce least privilege access to internal systems** to prevent lateral movement after an attack**.** **Train staff to recognize symptoms of a DDoS attack** and follow incident response procedures. **Deploy anti-DDoS solutions**, such as cloud-based filtering or scrubbing services. **Implement network segmentation** to isolate critical systems from general traffic.
Detect	**Deploy network monitoring tools** that trigger alerts when traffic volume spikes or follows abnormal patterns. **Install and tune an Intrusion Detection/Prevention System (IDS/IPS)** to detect and filter suspicious ICMP or network flood activity.

	Review and adjust logging policies to ensure critical events are captured in real time. **Perform threat hunting** and log analysis to identify early indicators of attack.
Respond	**Follow a documented incident response plan** to contain and mitigate the attack quickly. **Block malicious IPs or traffic sources** identified during the DDoS. **Stop non-critical services** during an attack to preserve bandwidth for critical systems. **Document the attack** and response actions to inform future improvements. **Conduct a post-incident analysis** to identify lessons learned and enhance the response plan
Recover	**Bring systems back online gradually**, starting with mission-critical services. **Validate integrity of data and systems** after restoration. **Apply patches or configuration changes** identified during the response phase. **Update business continuity and disaster recovery plans** to reflect DDoS mitigation procedures.

	Communicate clearly with stakeholders and clients about the resolution and steps taken to prevent recurrence.

Reflections/Notes: The recent DDoS attack was a critical reminder of how a single misconfigured firewall can create a major vulnerability within an organization's network. Although the attack only lasted two hours, it revealed weaknesses in our perimeter defenses and monitoring capabilities. By analyzing the incident through the lens of the NIST Cybersecurity Framework, I gained a structured approach to identifying, addressing, and preventing future threats.

In the **Identify** phase, I learned the importance of routine security audits and comprehensive network documentation. If we had thoroughly reviewed our firewall configurations earlier, we might have prevented the attack entirely.

The **Protect** function emphasized the need for proactive defense, such as implementing rate limiting for ICMP traffic and training staff on response protocols. This reinforced the idea that technology alone isn't enough — policy and awareness play an equally vital role in hardening our environment.

From the **Detect** phase, I saw how essential real-time monitoring and well-configured IDS/IPS systems are to recognize threats early. This will be a major focus in our ongoing improvements.

During the **Respond** phase, the team showed effectiveness in containing the attack, but we also recognized areas for improvement in coordination and communication. Post-incident reviews will now be a formalized part of our process.

Finally, in the **Recover** phase, I understood that system restoration must go hand-in-hand with a thorough assessment of damage, configuration reviews, and transparent communication with stakeholders.

Overall, this incident deepened my appreciation for structured cybersecurity practices. It also motivated me to strengthen our organization's ability to prevent and withstand future cyber threats by focusing on both technical controls and process maturity.