Multimedia Company – ICMP Flood DDoS Attack

Using the NIST Cybersecurity Framework to respond to a security incident

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:

A DDoS attack flooded the company’s network with ICMP packets, causing internal services to go down for 2 hours. The attack succeeded because the firewall was not properly configured. After the attack, the team blocked ICMP traffic, added firewall rules, monitoring tools, and IDS/IPS to prevent similar incidents in the future.

NIST Cybersecurity Framework Application

Step 1: Identify

Objective: Understand current cybersecurity posture, assets, and risks.

Actions Taken:

- Conducted asset inventory of critical systems and networking equipment.
- Identified firewall misconfiguration that allowed the attack.
- Reviewed user access permissions to firewall settings.
- Mapped network exposure points to assess ICMP traffic flow.
- Performed risk analysis on the impact of ICMP-based DDoS threats.

Outcome:

Key weaknesses in firewall configuration and lack of ICMP traffic control were identified, prompting an immediate need for stronger protective measures.

Step 2: Protect

Objective: Develop and implement safeguards to ensure delivery of critical services.

Actions Taken:

- Implemented a firewall rule to limit incoming ICMP packets.
- Enabled source IP address verification to block spoofed packets.
- Updated network access policies and firewall configurations.
- Conducted training for IT staff on secure firewall management.

- Hardened systems by disabling non-essential network services.

Outcome:

The attack surface was significantly reduced, and proper firewall controls were enforced to prevent recurrence.

Step 3: Detect

Objective: Identify cybersecurity events quickly and accurately.

Actions Taken:

- Deployed network monitoring tools to detect abnormal traffic patterns.
- Integrated Intrusion Detection and Prevention Systems (IDS/IPS) to filter malicious ICMP traffic.
- Configured alerting systems to notify security teams of suspicious activity.

Outcome:
Improved visibility into network behavior and enhanced the organization's ability to detect threats early.

Step 4: Respond

Objective: Contain and eliminate the impact of the attack.

Actions Taken During the Incident:

- Blocked all incoming ICMP traffic at the firewall.
- Stopped non-critical network services to reduce system load.
- Restored critical systems in a controlled and prioritized manner.
- Documented incident actions and performed a post-incident review.

Outcome:
The threat was neutralized promptly, and normal operations were partially restored within two hours.

Step 5: Recover

Objective: Restore systems and operations to normal while minimizing impact.

Actions Taken:

- Rebooted affected systems and verified service integrity.
- Conducted a full system health check and restored services step-by-step.
- Updated incident response documentation.
- Scheduled regular firewall reviews and configuration audits.

Outcome:
All services were restored, and procedures were refined to improve resilience in future incidents.

Recommendations

- Conduct monthly firewall configuration audits.
- Enforce least privilege access for network and security device management.
- Maintain current threat intelligence to monitor evolving DDoS methods.
- Perform routine penetration testing to uncover hidden vulnerabilities.
- Train staff regularly on incident response procedures.

Conclusion

This DDoS incident highlighted the importance of proper firewall configuration and proactive monitoring. By applying the NIST CSF, the organization responded effectively and has taken significant steps toward a more secure and resilient network infrastructure.