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	Our multi-media company was attacked via DDOS, The attack involved our servers being flooded with ICMP packets which compromised our internal networks and kept them unresponsive for 2 hours. The Incident Management team reacted by blocking incoming ICMP packets and stopping all non-critical network services while restoring the critical ones.
Identify	Network infrastructures were affected during the attack, and the attack utilized the unconfigured firewall to send packets. During the attack, non-critical protocols were affected like our design services. Additionally, the ones that have been granted access to the networks are the administrators, IT security staff, and critical business personnel.
Protect	Some Actions that have been taken are configuring the firewall to regulate the rate of ICMP packets and validate source IP addresses, using network monitoring software with deployment, and installing IDS/IPS systems that can

	filter any traffic considered suspicious. Access rights to critical systems will be denied to those unauthorized and security staff will be given authorization along with business personnel. Data security will further be improved through the reviewing of backup procedures as well as encryption of data. Regular security audits will be enforced for updated procedures, as well as a prompt incident response. In addition, the systems will all be kept up-to-date with the latest security patches.
Detect	To identify suspicious activity the organization will implement a SIEM system to analyze and track data anomalies. User accounts will be monitored and traced and intrusion detection Systems will be implemented, therefore, detection will be present even if the firewall is not properly configured (which it will be).
Respond	Firstly, we will create a better network and management protocols. For example, a management protocol we will incorporate is the SNMP to better monitor issues, moreover implementing the Internet Control Message Protocol ICMP will allow the devices to send error messages if there is an issue with the transmission. Some data that can be used in this situation to analyze the incident is network traffic flow, as this incident occurred via the transmissions of ICMP packets, a SEIM tool can better monitor this incident. In order to recover, a Disaster Recovery Plan should be implemented,
Recover	To restore the system from the cybersecurity incident, the organization should use the most current backups, the details of the system configuration, and the logs of the incident. The disaster recovery plan will be invoked for restoring critical systems and data, with preference given to essential business functions. A properly trained recovery team will implement such a plan while ensuring communication protocols are maintained. Systems will be assessed and hardened post-recovery to address vulnerabilities, and a thorough post-incident analysis will be carried out to understand the root cause and to improve future efforts. It is by this broad approach that a more effective recovery and stronger resilience can be achieved from the attacks.

Reflections/Notes: