Incident report analysis

Instructions

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.

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 incident and integrate your analysis into a general security strategy

Identify	The incident management team audited the systems, devices, and access policies involved in the attack to identify the gaps in security. With an

	unconfigured firewall, the threat actor could easily take advantage of the unfiltered network traffic and open ports to overwhelm the network with ICMP packets.
Protect	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. ● Firewall configuration to allow only essential traffic into the network and filter out unwanted traffic as well as close unnecessary ports. On the client side: MFA is implemented and login attempts are reduced to 3.
Detect	To detect new unauthorized access attacks in the future, the team will use a firewall logging tool and an intrusion detection system (IDS) to monitor all incoming traffic from the internet.
Respond	As mentioned, The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.
Recover	Assuming the company keeps a backup of its data, systems and data will be restored to the latest backup version up until the incident. Any data recorded on the day of the incident will need to be re-entered.

Reflections/Notes: The recent DDoS attack exposed vulnerabilities stemming from an unconfigured firewall, emphasizing the critical need for robust network security. Following the NIST Cybersecurity Framework, our team swiftly implemented measures like limiting ICMP traffic, source IP verification, and enhanced client-side security through MFA and login restrictions. Strengthening detection with firewall logging and an IDS bolsters our ability to identify future threats. Our response strategy effectively mitigated the attack's impact by blocking ICMP packets and restoring critical services. Moving forward, regular backups will aid swift recovery, emphasizing the importance of a proactive, multi-layered security approach aligned with industry best practices to safeguard our digital assets and maintain uninterrupted services for our clients.