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	On July 18, 2023, the cybersecurity team identified a security incident, then investigated the security event. The team 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. Our organization experienced a DDoS attack, which compromised the internal network for two hours until it was resolved. During the attack, the 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.Tthe team has configured the firewall, which was the source of the attack and performed a security audit of all devices, systems and processes.to prevent future attacks. Finally, The team has returned all systems to business operations with hardened security configuration
Identify	The incident management team audited the systems, devices, and access policies involved in the attack to identify the gaps in security. The team 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 result, compromised the internal network for two hours until it was resolved Upon initial review, it appears that no customer data was deleted from the database.
Protect	The team has configured the firewall, which was the source of the attack and performed a security audit of all devices, systems and processes.to prevent future attacks. The Security team has updated security polices to include training for all employees on how to configure properly new devices in accordance to the baseline security specifications. Additionally, we will implement a new protective firewall configuration and invest in an intrusion prevention system (IPS).
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	The team has configured the firewall, which was the source of the attack and performed a security audit of all devices, systems and processes.to prevent future attacks. The Security team has updated security polices to include training for all employees on how to configure properly new devices in accordance to the baseline security specifications. We informed upper management of this event and they will contact our customers by mail to inform them about the security breach
Recover	The team has returned all systems to business operations with hardened security configuration. The Security Team has analyzed how the malicious attackers used the vulnerability in the unconfigured firewall, . They found that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall. As a result of this experience, the security team has recommended to the executive officers, that we engage in a monthly penetration testing to conduct stress test to ensure we have a robust security system. To address this security event, the network security team implemented: 1. A new firewall rule to limit the rate of incoming ICMP packets

	2. Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets. 3. Network monitoring software to detect abnormal traffic patterns. 4. An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics

---

Reflections/Notes:As a person committed to a cultural mindset of lifelong learning of continuous improvement, I see the value of an approach to learning at the point of need, and structuring regular cybersecurity best practices training in how to configure hardware properly and the latest phishing tactics by malicious actors