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	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. It could be concluded that the organization experienced a DDoS attack, which compromised the internal network for two hours until it was resolved. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.
Identify	● Technology/ Asset Management : The recently experienced DDoS attack compromised the internal network for two hours until it was resolved. ● Process/ Business Environment : The multimedia company offers web design services, graphic design, and social media marketing solutions to small businesses. Hence, due to the two hours of inability to perform the necessary functions, the day to day scheduled tasks would have been delayed, and maybe deadlines missed. ● People : The company's cybersecurity team needs access to the affected systems
Protect	● Access Control : The company's cybersecurity team got access to the

	affected systems and the incident management team responded by blocking incoming ICMP packets. ● Awareness/ Training : The incident management team needs to be given complete information and need to be kept aware about this security incident. Training is required so that such incidents can be avoided in the future. ● Data Security : According to the incident reports, there has been no data breach. Data security needs to be re-checked to detect any vulnerabilities that this attack may have exposed. ● Information Protection and Procedures : Authorization permissions need to be checked again in order to prevent any data breaches in the future. MFA (Multi Factor Authentication) needs to be implemented, if not implemented already ● Maintenance : A patch update is required that addresses the security vulnerabilities within the program or product that may have been unknown, or exposed due to this attack. ● Protective Technology : An IDS/IPS system needs to be installed to filter out some ICMP traffic based suspicious characteristics alongside having a new firewall rule to limit the rate of incoming ICMP packets. Network monitoring software also needs to be installed to detect abnormal traffic patterns.
Detect	● Anomalies and Events : SIEM tools could be used to detect and alert IT security staff of anomalies and security events. ● Security Continuous Monitoring : Network monitoring needs to be done to detect any abnormal traffic patterns. ● Detection Process : A new firewall rule to limit the rate of incoming ICMP packets and IDS/IPS system to filter out some ICMP traffic based suspicious characteristics
Respond	The cybersecurity team responded by the following actions :

	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 suspicious characteristics
Recover	Recovery Planning : Server backups need to be brought into play to recover any data abnormalities, if any, during the attack. Improvements : Network hardening tasks need to be performed regularly to prevent such an attack in the future Communications : The restoration procedures carried out by the cybersecurity team needs to be communicated to the incident management team and training needs to happen accordingly. The clients also need to be notified about the attack and mails need to be sent once everything is back to normal.

Reflections/Notes: