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	My organization is working on a multimedia company however we experience a DDoS attack that compramised the intermal netwrok that took 2 hours to resolve. In the beginning of the attack my organization network services suddenly stoped responding due to an incoming flood of icmp packets.
Identify	The cybersecurity team investigating the event and found that a malicious actor had sent a flood of icmp pings into the companys network through an unconfigured firewall. This vulnerability made it easy for the malicious attacker to attack our network with a DDoS attack.
Protect	The network security temam plan to implement a a source IP address verification and a new firewall rule to limit the amount of ICMP packets and spoofed IP address for the incoming ICMP packets. A network monitoring software to detect any abnormal traffic patters. An ID/IPS system to filttered and check for ICMP traffic and find any suspicious activities
Detect	To detect any abnormal or suspicious activities we will implement an ID/IPS to help filtered and check ICMP traffic and a source IP address verification to check where the ICMP packets are cominig from
Respond	The incedent management team responded by blocking the incoming ICMP

	packets which stopped all non-ctritical network services offilne and restoring network services.
Recover	My team will first report the incident to upper managment to ensure that they know what happened. Then we will address the customers about the incident and let them know that there was an attack that made the system to stop responding which is why they werent able to access the company resources. Once everything has calm down and insure that everything is good to go then we will reboot our system and restore critical network services and non critical network services active

---

Reflections/Notes: