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	Recently, our organization was attacked by an adversary, causing our network to crash. During this 2 hour period before responding, normal internal network traffic could not access any network resources. This left plenty of employees stuck not completing any work. The incident management team responded by blocking incoming ICMP packets, stopping all non critical network services offline, and restoring critical network services.
Identify	This was an ICMP flood attack, This is when an outsider sends a bunch of requests to our network, so much that the network crashes. This happened through an unconfigured firewall and left any machines connected to the network impacted.
Protect	To protect against this attack, the organization can take steps to filter certain network traffic where this attack is coming from, block adversary ips and create a rule in the firewall that limits the amount of icmp packets that can be sent in a certain amount of time so our network does not crash.
Detect	To detect further adversaries, we can install IDS software on our network in order to detect attacks and look into them in a more timely matter. We can also implement a IPS software to protect against known threats and build another layer of protection. A SIEM tool would be another great addition in order to

	view attacks across many different types of logs. This can broaden our knowledge and view of our attack field.
Respond	It is important to use these tools we plan to implement to respond to attacks in the future. Checking logs to assess the attack type early on will be key to responding to the incident. Once we recognize the attack type, we can then take measures to prevent the attacker from further action through isolating parts of our infrastructure that are affected.
Recover	When a future attack is detected, we'll want to isolate affected systems quickly and check logs to confirm what kind of attack we're dealing with. Once we know the source and pattern, we can shut down vulnerable services and apply updated rules to contain the threat. Acting quickly and focusing on restoring critical systems first will keep disruption to a minimum.

Reflections/Notes: