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	A multimedia company that provides various services to small businesses experienced a DDoS attack that lasted approximately two (2) hours. While the attack was happening it was determined that the attack that caused the organization's network services to stop responding was due to an incoming flood of ICMP packets. The flood of ICMP/ping packets did not allow normal internal network traffic to access any of the network resources that were normally used. An incident management team was able to respond to this ping flood attack by blocking all incoming ICMP packets, bringing down all non-critical network services, and restoring only critical network services. A cybersecurity team later discovered, after the attack, that the DDoS attack was possible because of an unconfigured firewall that allowed a threat actor to send the flood of ICMP packets into the company's network.
Identify	The biggest gap in security that is apparent in this situation is the implementation of an unconfigured firewall. The firewall should, at the least, be configured to monitor suspicious activity and filter it out if possible.
Protect	The firewall should be configured to filter traffic, specifically incoming traffic, to make sure that it does not contain any suspicious or known threat signatures. For example, a packet that has the IP address of the internal network coming

	from outside of the network should be filtered to prevent attacks like this. The firewall can also be used to limit the rate of ICMP traffic that is coming into the network. An IDS/IPS should also be used to filter out ICMP traffic with suspicious signatures.
Detect	There are a couple of options that can be implemented for this organization that would help them detect threats like this in the future. First, a SIEM can be put into place to monitor security alert activity for the entire network so that anybody in charge of monitoring the network can have easier access to view any potential or active threats. Second, an IPS or an IDS can be implemented to detect and potentially stop - with an IPS - threats from doing any significant harm to the network.
Respond	Network segmentation can be implemented in the future to help isolate cybersecurity incidents, threats, and affected devices. Whenever a threat is discovered, the segment of the network that the affected device is on can be quarantined from the rest of the network to stop it from spreading. The SIEM and/or IDS or IPS can be used to alert network administrators of these threats more quickly so that response time can be lower and help to minimize the damage done by any cybersecurity incidents.
Recover	After the threat has been taken care of and the network is secure, all of the network services that were taken offline because of the attack should be brought back online. Any information that may have been lost or compromised should be restored from any backups available so that business may continue to operate as it was before the incident.

Reflections/Notes: This incident occurring boils down to having an unconfigured firewall in place. If a firewall is in place to protect a network it should be configured at least to the bare minimum.