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	Network services went down for the company. The small business was receiving a DDoS attack for approximately two hours. The organization's network services were stopped due to an incoming flood of ICMP packets. Incident management team stopped the DDoS attack, implemented measures to get the business back up and running, then the cybersecurity team investigated the security event.
Identify	Malicious actor/actors targeted the company’s employees and then attacked with an ICMP flood attack. Internal network traffic was cut off from network resources. Critical resources needed to be restored to continue business operations.
Protect	There were new rules created for the firewall to limit incoming ICMP packets. Network monitoring software was used to detect abnormal traffic. Lastly, IDS/IPS filtered ICMP traffic according to suspicious activity.
Detect	IP address verification is now checked for spoofed IP addresses from incoming ICMP packets. Network monitoring software is used to assist with detecting abnormal traffic.
Respond	To triage events in the future, isolating affected systems to keep further

	infections is recommended. Maintaining uptime of critical resources will be top of the list to continue business operations. Next the teams will audit the systems to look for suspicious activity. Lastly, notifying appropriate upper management and legal authorities as needed.
Recover	To get back to normal operations from a DDoS attack by ICMP flooding, it’s recommended to stop the packets at the firewall first. Then, stop all non-critical network services, restart critical network services, and finish the recovery by bringing back all non-critical network resources after ICMP flooding has been stopped.

Reflections/Notes: Educating staff members that the company will not verify information in a third party fashion can lower the chances of this happening in the future.