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	We recently experienced a DDoS (Distributed Denial of Services) attack. This attack compromised the internal network for two(2) hours before resolution was achieved. During the attack, network services stopped responding. It was discovered that it was d ue to an ICMP flooding attack. This caused normal network traffic to be unable to access network resources. The team responded by blocking all incoming ICMP packets, stopping all non -critical network services offline and then restoring critical network se rvices.
Identify	This was a DdoS attack that affected the network's ability to handle legitimate incoming traffic.
Protect	**To address this, the security team plans the following implementations:** **1. New firewall rule to limit the rate of incoming ICMP packets.** **2. Source IP address verification on the firewall to check for IP Spoofing on incoming ICMP packets.**
Detect	In order to aid in future detection of this – and other types – of attacks the following will be done: **1. Network monitoring software will be installed/updated to detect abnormal traffic patterns.**

	2. **An IDS/IPS will be installed to filter out some ICMP traffic based on suspicious traits.**
Respond	The team initially shut down affected areas of the network but were able to restore critical needs after a short period. For future security events, the team will isolate affected systems to prevent fu rther disruption of the network. Focus will be given to critical systems and services first in order to restore them quickly. Network logs will be analyzed for suspicious and abnormal activity and a report of all incidents will be provided to upper management. Going forward we will be performing regular penetration tests to check for areas of vulnerability within the network and establishing audit procedures for the firewall and OS as well as looking into broader network segmentation to reduce the potential impact of another breach.
Recover	To recover from a DDoS attack by ICMP flooding, access to network services need to be restored to a normal functioning state. In the future, external ICMP flood attacks can be blocked at the firewall. All non-critical network services should be stopped to reduce internal network traffic. Next, critical network services should be restored first. Finally, once the flood of ICMP packets have all timed out, all non-critical network systems and services can be brough back online.

Reflections/Notes: