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	Earlier today our organization’s network services suddenly stopped responding, and our internal network was compromised for over two hours until we finally resolved the problem. The cybersecurity team found that ICMP packets were being sent into the company’s network through an unconfigured firewall at high enough volumes to overwhelm the network through a distributed denial of service (DDoS) attack. Our team responded by blocking ICMP packets, which stopped the incoming packets from overwhelming the system, allowing it to be restored and for services to respond to normal traffic.
Identify	Our cybersecurity team determined that an unconfigured firewall allowed the attacker to send packets into our internal network which disrupted our internal network. Multiple external systems flooded our network with ICMP packets which prevented internal network traffic from accessing resources on the internal network. Our immediate response to regain control of the situation was to block all incoming ICMP packets, and stopping all non-critical network services, and restoring all critical network services. These changes allowed us to resume basic internal network operations.
Protect	To address the security incident and prevent future attacks, we developed new firewall policies and ensure all firewalls were updated. Specifically, we utilized a rate limit for incoming ICMP packets that ensures the network cannot be flooded with ICMP requests. Another reason the attack was successful was that we accepted external packets with a spoofed internal IP address, therefore we implemented source IP address verification on the firewall to check for spoofed addresses on incoming ICMP packet and reject them. We also implemented a number of methods to monitor network traffic

	and enable detection of suspicious activity. These include network monitoring software to detect abnormal traffic patterns, as well as an Intrusion Prevention System (IPS) and Intrusion Detection (IDS) system providing multiple layers of protection.
Detect	To detect future network attacks, we will make use of network monitoring software to log and monitor network traffic for unusual events. We will also use both an IPS and IDS to monitor all traffic, detect suspicious activity, and automatically respond to potential intrusions to prevent the attack from proceeding any further and alert the cybersecurity team to investigate the potential attack. We also check for spoofed IP addresses to stop external users from sending packets that appear to be from inside the local network.
Respond	In this case, the team blocked the type of traffic used in the attack, ICMP packets, which isolated the local network from the attack. This can be done to help mitigate the effect of future attacks and allow the systems to be restored. Once this is done, the team will try to restore the main services that the attack affected. The team can then undertake analysis of network logs to understand the suspicious activity. The main vulnerability in this attack was the unconfigured firewall that allowed traffic with spoofed IPs access to the internal network. In the future we will need to develop plans to monitor firewall configurations and ensure none are unconfigured. We need to ensure each is configured, and configured correctly for its role in the network. Therefore, we need to develop improved network asset tracking methods.
Recover	Since data is not affected, we do not need to restore any systems based on backups. Recovery requires the team to block traffic from the DDoS attack, shutting down non-critical network services, and then restoring all critical network services before the non-critical ones are also restarted.

Reflections/Notes: