Incident report analysis

Instructions

Think about the concepts covered in the course and reflect on the scenario to determine what type of attack occurred and which systems were affected.

Summary	Our company experienced a DDoS (distributed denial of services) attack today morning, which caused severe problems and compromised our internal network.
Identify	Our team found that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall. This caused a flood of ICMP packets and made our network services unavailable for a couple of hours.
Protect	In order to protect our network, our security team decided to implement a new firewall rule that limits the amount of ICMP packets and IDS/IPS system to filter out ICMP traffic based on any suspicious activity,
Detect	In addition, our team also included a source IP address verification on the firewall to catch any ICMP packet that shows any kind of abnormal traffic patterns.
Respond	The company decided to incorporate deep analysis into network logs and check for suspicious and abnormal activity. For future reference, the firewalls will also be strengthened so we do not see ourselves in the same hard situation later on.
Recover	To bring everything back to normal, we had to make sure that all of our

	network services are now working at full capacity, and that all the resources that had to be strengthened are effectively fulfilling their purposes.

Reflections/Notes: