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	Your company has suffered a Distributed Denial-of-Service (DDoS) attack recently. During this attack your organization's network services suddenly stopped responding due the flood of Internet Control Message Protocol (ICMP) packets.
Identify	The attack was a Distributed Denial-of-service, DDoS, this happened when a malicious actor sent a flood of ICMP pings into your company network, these packets passed your unconfigured firewall, resulting in a bad network service behavior.
Protect	In order to prevent a future similar incident the first step will be to configure your firewall in order to limit the number of ICMP packets per second, we can also implement ingress filtering on your network devices to block or filter out spoofed IP addresses.
Detect	With your new Intrusion Detection System/Intrusion Prevent System (IDS/IPS) we can monitor your network traffic in order to actively perform a protect measure when a malicious actor starts a possible DDoS attack against us. We can also apply a Security Information and Event Manage (SIEM) tool to real-time monitoring your network and be alerted when the tool notices an anomaly.

Respond	The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. In future your team will get all the respond measures documented on a Playbook to be more prepared for a quick response action in a future event.
Recover	After containing the attack and stopping the network services affected, ensure that the firewall is correctly configured and your ingress filtering is filtering spoofed IP addresses we can restart your services. First we restart the critical services and after all ICMP packets timed out we restart non-critical services.

Reflections/Notes: This DDoS attack perform a damage to your organization, but also hardening your security measures, with a playbook, firewall and ingress filtering, monitoring tools like IDS/IPS and SIEM tools, and the expertise to quickly response a future incident we will be much more prepared to keep your business customer-focused.