NIST CSF - Incident Report Analysis

Summary	The organization experienced a DDoS attack that compromised the internal network for 2 hours. Network services suddenly stopped responding due to an incoming flood of Internet Control Message Protocol (ICMP) packets (bandwidth was overwhelmed causing the crash). The Incident Management team blocked incoming ICMP packets, stopping all non-critical network services offline, and restored critical network services.
Identify	The Cybersecurity Team investigated the security event and found a malicious actor sent a flood of ICMP pings, affecting the entire internal network. It was identified as a Distributed Denial of Service (DDoS), ICMP flood attack.
Protect	Following this security event, the Security Team implemented: • A new firewall rule to limit the rate of incoming ICMP packets • An Intrusion Detection System (IDS)/Intrusion Protection System (IPS) to filter out some ICMP traffic based on suspicious characteristics
Detect	The Security Team configured source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets and implemented network monitoring software to detect abnormal traffic patterns.
Respond	For future security events, the Security Team will isolate affected systems to prevent further disruption to the network. They will attempt to restore any critical systems and services disrupted by the event, then, will analyze network logs to check for suspicious and abnormal activity. The team will also report all incidents to upper management and appropriate legal authorities, if applicable or necessary.
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. Then, 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 timed out, all non-critical network systems

	and services can be brought back online.

Reflections/Notes:

- A Next Generation Firewall (NGSW) should be considered to conduct deep packet inspection. It also has intrusion prevention features that detect security threats and notify firewall administrators.
- A Virtual Private Network (VPN) should also be considered to encapsulate any unencrypted data to prevent malicious actors who may attempt various network interception attacks, such as packet sniffing or on-path attacks.
- The organization should consider subnetting to create security zones and assist in network efficiency.