TANNER S VAN SLYKE **1-208-697-7197**

NIST CSF Incident Report Analysis

Summary	The company experienced a sudden disruption in network services as a result of a DDoS attack. The cybersecurity team determined that the disruption was caused by a flood of ICMP packets. The team then blocked the attack and stopped all non-critical network services until critical services could be restored.
Identify	The attacker(s) targeted the company with an ICMP flood, affecting the entire internal network. Critical resources needed to be secured and restored to a functional state.
Protect	The team implemented a new firewall rule to limit the rate of incoming ICMP packets, as well as an IDS/IPS system to filter out suspicious ICMP traffic.
Detect	The team configured source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets, as well as network monitoring software to screen for abnormal traffic patterns.
Respond	For future security events, the team will attempt to isolate affected systems to prevent network-wide disruption, while working to restore any critical systems or services affected by the event. The team will then analyze network logs for suspicious or abnormal activity before reporting all incidents to upper management or the applicable authorities.
Recover	Access to network services needs to be restored to a normal, functional state. Future ICMP flood attacks will be blocked by the reconfigured firewall, then non-critical network services should be stopped to limit traffic on the internal network. Critical network services should be restored first, with all non-critical systems and services being brought back online once the flood packets have timed out.