Incident report analysis

Summary	A large number of employees reported that they were no longer having access to the internal network of the organization. Not much later than that there was a network shutdown for the entire organization. The IT team reported that there was a flood of ICMP packets received that flooded the network. There was a vulnerability found at an unsecured firewall which was flooded by ICMP packets from an adversary, leading to the company's network shutdown by DDoS attack. So far, we have blocked the incoming ICMP packets to restore critical network services.
Identify	An unsecured firewall was exploited which allowed the threat actor to overflow the network server with ICMP packets causing the internal network to shutdown.
Protect	The IT team has implemented procedures to better improve the security defenses by adding: ● Firewall rule to limit the rate of incoming ICMP packets ● Source IP address verification on the firewall ● Network monitoring software ● AN IDS/IPS In addition, there should be regularly performed audits on the firewall to ensure there are no vulnerabilities in the server.
Detect	In order to reduce this type of attack from occurring again, there have been IDS and IPS systems in place to filter out ICMP traffic based on suspicious characteristics. We will also be utilizing full packet capture devices with the SIEM to aid us in investigating alerts created by the IDS.
Respond	The system was shut down for roughly 2 hours after the attack. The IT team responded by blocking the incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. There have been immediate procedures implemented to improve the security defenses and

	regular audits will be conducted to ensure there are no lapses in security. In addition to that, there have been upgrades to the firewall, added IDS and IPS systems to better monitor suspicious network traffic.
Recover	There will be a a configuration check to ensure that we are in full control of the operating system, and will conduct a baseline configuration as to restore any or all unauthorized changes