Jasper Davis

Incident Report analysis

Summary	Recently, the company's network services suddenly stopped responding and internal network traffic was not able to access any network resources. The network experienced a flood of Internet Control Message Protocol (ICMP) packets which we believe caused the access issues.
Identify	Receiving a flood of ICMP packets is a common type of distributed denial of service (DDoS) attacks. When the network is flooded with these packets it can become unresponsive and disrupt regular business operations. The cybersecurity team investigated the security event and found that the malicious actor had exploited an unconfigured firewall.
Protect	In order to better protect against these potential attacks in the future, the company has created a new firewall rule to limit the rate of incoming ICMP packets. In addition, source IP address verification has been enabled to check for potentially spoofed IP addresses.
Detect	To detect these attacks in the future, an intrusion detection/prevention system (IDS/IPS) has been brought online to monitor all incoming traffic and filter out ICMP traffic deemed suspicious.
Respond	The incident management team blocked incoming ICMP packets and stopped all non-critical services. After resetting the system, the incident management team restored critical network services. Following investigation and root cause analysis, firewall configuration and IDS/IPS implementation was performed to prevent this type of incident from reoccurring.
Recover	With the new preventative measures in place, the system was brought back

	online. The previous night's database backup will be used to restore any missing/compromised data. This recovery will mean that data entered the morning of the attack will likely need to be re-submitted.