M.Kesten-january ‘24

Incident report analysis

Applying the NIST CSF

Summary	There was a security event in the company when all organization’s network services suddenly stopped responding. The team found that company’s network was overwhelmed through distributed denial of service (DDoS) attack with incoming flood of ICMP packets. Team responded by blocking incoming ICMP attack, stopping all non-critical network services, so that critical network services could be restored.
Identify	A malicious actors targeted company with an ICMP flood attack. Entire internal network was affected. All critical network services needed to be secured and restored.
Protect	The team implemented a new firewall rule to limit the rate of incoming ICMP packets and an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
Detect	The team implemented network monitoring software to detect abnormal traffic patterns and configured source IP address verification on the firewall to check for spoofed IP addresses.
Respond	In the future, team will isolate affected systems to prevent further attack on network. They will try to restore any critical systems and services that were affected by the event. Then, they will analyze network logs to check for abnormal activity. If applicable, team will also respond all incidents to upper

	management and legal authorities.
Recover	Access to network services need to be restored to normal functioning state, to recover from DDoS attack by ICMP flooding. In the future, external ICMP flood attack can be blocked at the firewall. After that, all non-critical network services should be stopped to reduce internal traffic on network. Then, critical services should be restored first and when the flood of ICMP packets have timed-out, all non-critical services and network systems could be brought back online.

Reflections/Notes: