

NIST Framework Incident Report

Summary

Earlier this week, multimedia company YourGenericMMC experienced an outage of its internal network for two hours. During those two hours, all network services suddenly stopped responding, and after using network analyzer tools, determined it was an incoming flood of ICMP packets. We believe this to be a Ping Flood Attack performed by a malicious actor who wished to halt all operations at YourGenericMMC. Our security team traced the packets through the company's firewall leading us to believe the firewall was misconfigured, thus not able to filter out the Ping Flood Attack.

Identify

The incident management team audited the systems, devices, and access policies involved in the attack to identify the gaps in security. The team found that the ICMP packets were being let through the company's firewall. Upon further inspection, it was found that the firewall had not been configured when it was installed. This attack paralyzed the entire company for two hours as the entire internal network was unresponsive.

Protect

The company has since implemented many safeguards to protect the company's system from any future attacks. The firewall has now been configured with a rule that limits the rate of incoming ICMP packets at any given time. The firewall has also been configured to verify source IP addresses to check for spoofed IP addresses on incoming ICMP packets. A network monitoring software has been installed to detect abnormal traffic patterns in the system. An IDS/IPS system has also been implemented to filter out some ICMP traffic based on suspicious characteristics before they are allowed into the DNS server (Controlled Zone). The company's security team is responsible to ensuring that all these measures are implemented correctly and that they are maintained and monitored.

Detect

To detect any new attacks, the company will have a properly configured firewall to limit incoming ICMP packets along with verifying source IP addresses. A network monitoring software will also be monitored frequently to catch any suspicious-looking packets and to detect abnormal traffic patterns. An IDS/IPS system will also filter out suspicious ICMP packets, detecting any packets with suspicious characteristics.

Respond

The security team had to block all ICMP packets, stop all non-critical network services, and restore critical network services. We informed upper management of this occurrence

and established a plan to upgrade our security system. The security team will begin implementing these security upgrades ASAP.

Recover

The team will continue to restore the network services of the remaining sections of the company system in order to get everything operational. We have informed staff that their network services may not be fully operational until the next work day as our team continues to dig into the attack and restart all services back to operational normal.

Reflections/Notes: