Incident report analysis

Instructions

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this chart as a way to practice applying the NIST framework to different situations you encounter.

Summary	Given information on the scenario , preparation for the incident started with a phishing email delivered to an intern, the email contained a link to an external website in which the intern entered their internal network credentials, thus giving the attacks a way into the network. The attacks then used this information to start an ICMP Flood DDoS attack, overwhelming the internal network with ICMP requests. The firewall which should have been able to detect and stop/alert sysAdmins failed to do so due to a misconfiguration. sysAdmin responded by blocking the ICMP from outside network IP addresses All systems were affected, non-critical and critical causing them to be taken offline.
Identify	Intern internal network credentials were stolen through a phishing email that passed all detection devices. ICMP Flood DDoS attack causing all network devices and services to be taken offline to be secured and restored

Protect	Implementation of MFA, requiring all users on an internal network to provide additional forms of authentication to gain access to the network as well as limiting password attempts can help reduce the effect of stolen credentials. Priority systems in need of review is the misconfigured firewall, the firewall must have its updated rules to limit the rate of ICMP packets entering a network
Detect	The introduction of an IDS can aid network engineers by alerting them to any abnormalities found in network traffic. Source IP verification to check for spoofed IP addresses from outside the network and letting the firewall block connections from outside the network with those addresses Introduction of log monitoring software such as a SIEM to monitor network traffic and abnormalities
Respond	Interns can all be trained on how to properly protect credentials from being stolen or leaked. Affected systems will be isolated to prevent further disruption to services and the business Management was contacted to inform them of breach and customers will also be informed in accordance with compliance and laws
Recover	Backups will be used to restore network to operational form, informing customers to re-enter any information that they have entered today, after the backup has been initialized Critical systems will first be brought back online and then non-critical safety waiting for ICMP packets to timeout

Reflections/Notes: