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	At XX:XX, all network services at COMPANY X stopped responding. Incident Management Team (IMT) was notified immediately. IMT was able to restore service after 2 hours by Identifying an ICMP flood DDOS attack, then implemented a rate-limit filter on ICMP packets, then turned off non-critical network services and rebooted critical network services.
Identify	IMT identified incoming ICMP flood DDOS attack in progress from SIEM. Entire internal network was affected.
Protect	IMT added rate-limit ICMP filtering to firewall, then disabled non-critical services and rebooted critical services to restore operation. In the future, a “kill switch” that disconnects the internal network from Internet may allow restoration of limited function.
Detect	CS team found firewall did not block ICMP packets, which allowed DDOS attack through. CS did not find any evidence that data had been compromised in the attack. In the future, IDS/IPS should be able to detect such ICMP packets and thus,

	respond to incidents faster as well as network monitoring software to detect odd incoming traffic patterns.
Respond	CS team verified new firewall rule, then audited the rest of firewall config to close off any other unused ports. Also, firewall is additionally configured to verify source IP address to stop any IP spoofing attacks. CS team also added network monitoring software to detect abnormal traffic patterns as well as IDS/IPS to speed up response to suspicious characteristics. Together, they should stop such attacks from interrupting the internal network, and if interruption happens, keep downtime to a minimum.
Recover	IMT was able to restore services after roughly 2 hours of downtime after the new firewall rule went into effect. The rest of non-critical services were restored after a thorough audit by the CS team to minimize attack surfaces. Priority was to a) block the flood, b) stop non-critical network functions, c) restore critical network functions, d) restore non-critical network functions when conditions allow.

Reflections/Notes: