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	The organisation recently experienced a 2 hour disruption to business as a result of internal network compromisation during a suspected ddos attack. A flood of incoming ICMP packets meant legitimate user interaction was prevented because network services suddenly stopped responding. The immediate response of the security team prevented incoming ICMP packets, stopped all non-critical network services offline, and restored critical network services. After the security incident occurred investigations were carried out to establish which areas of the network had vulnerabilities that allowed the malicious actor to attack the network.
Identify	It was established that the malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall. This meant that the system was overwhelmed and therefore could not operate as part of normal business. This was a distributed denial of service attack (ddos). Assets were not compromised in terms of privacy, however, the 2 hour disruption to the normal functioning of organisation services can have a negative impact on finance and customer relations.
Protect	The security team carried out remediation measures consisting of establishing a new firewall rule to limit the rate of incoming ICMP packets, implementing

	source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets, installing Network monitoring software to detect abnormal traffic patterns and implementing an IDS/IPS to filter out some ICMP traffic based on suspicious characteristics.
Detect	As mentioned, source IP address verification was implemented to detect spoofed IP addresses and ICMP packets. Further remediation strategies implemented an intrusion detection system (IDS) to alert network administrators of potential breaches, as well as an intrusion prevention system (IPS) that helps to prevent unauthorised access suplimentary to detection.
Respond	The first response of the incident management team included blocking incoming ICMP packets, stopping all non-critical network services offline and restoring critical network services.
Recover	Resumption of normal network traffic was restored after 2 hours. The organisation can resume normal business operations following ddos attacks provided they immediately restrict non-critical network services,, implement a firewall that can block further ICMP flood attacks and eventually restore all non-critical network systems .

Reflections/Notes: It is important to correctly configure firewalls to keep networks safe. Stateful firewalls keep track of information passing through it and helps filter out threats. Firewalls that operate on predefined rules (stateless) may not be up-to-scratch in terms of security because they do not actively analyse the contents of incoming data packets. If using a stateless firewall they must be regularly configured, however they're the least favourable. It might be even better to implement a next generation firewall that offers intrusion protection as well as deep packet inspection.

The implementation of IDS/IPS as well as installation of network monitoring is a positive step forward. Multiple strategies that help mitigate vulnerabilities establish an overall defense-in-depth approach to cybersecurity.