Incident report analysis

Summary	
Identify	• The incident involved a Distributed Denial of Service (DDoS) attack on the organization's network. • The attack disrupted network services for two hours. • The attack vector was a flood of ICMP pings through an unconfigured firewall. • The incident management team blocked incoming ICMP packets, halted non-critical network services, and restored critical services.
Protect	• A new firewall rule was implemented to limit the rate of incoming ICMP packets. • Source IP address verification on the firewall was implemented to prevent spoofed IP addresses. • Network monitoring software was deployed to detect abnormal traffic patterns. • An Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) was employed to filter out suspicious ICMP traffic
Detect	• The abnormal increase in incoming ICMP traffic was detected during the incident. • Network monitoring software played a crucial role in identifying the attack. • The IDS/IPS system was able to filter out some malicious ICMP traffic.
Respond	• The incident management team took immediate action by blocking incoming ICMP packets. • Non-critical network services were temporarily taken offline to mitigate the impact. • Critical network services were restored promptly. • Investigation and analysis of the security event were carried out to identify the attacker and the vulnerability exploited. • New security measures were implemented to address the identified vulnerabilities.
Recover	• Affected systems were restored to normal operation after the incident. • Data and assets that were affected by the DDoS attack were recovered.

Reflections/Notes:

The incident highlights the importance of proactive security measures. Regular audits and vulnerability assessments should be conducted to identify and address potential security gaps. Policies and procedures should be in place to respond swiftly to security incidents. Training and awareness programs for employees can help in recognizing and reporting security incidents. The incident also underscores the significance of network monitoring and intrusion detection systems in detecting abnormal activities. Ongoing improvements to security processes are necessary to adapt to evolving threats.

Luca Forma