Incident report analysis

Summary	It was found that the company suffered a DDoS attack and the impact of this attack resulted in the internal network of the company being unresponsive due to an incoming flood of ICMP packets. The investigations conducted by this cyber security team found that the malicious actor flooded the companies network with the ICMP packets via an unconfigured firewall vulnerability. Hence, resulting in the company's internal network being unresolved for two hours. The incident was resolved by blocking the ICMP packets, stopping all non-critical network services, and then restoring the critical network services.
Identify	It was identified that the source of this vulnerability that caused the attack was due to the firewall of the network being unconfigured to handle such an attack.
Protect	To protect the company from an DDoS attack like this in the future, the cyber security team must configure the rules of the firewall so that it limits the rate of ICMP packets that can come through the network.
Detect	In order to detect such and attack like this in the future the company must integrate a SIEM tool into their company's cyber security framework. This tool will allow the cyber-security team to analyze network traffic, software applications, track authorized versus unauthorized users, and detect any unusual activity on user accounts. Also the company should install an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
Respond	Hence when another DDoS ICMP packet flood attack such as this occurs again the following steps can be taken to reduce the impact of the attack and maybe prevent it from happening in the first place. 1. First configure the firewall of the network so that a certain rate of ICMP

	packets can be let in so the the network does not get overwhelmed from the large number of packets causing it to become unresponsive. 2. Integrate an SIEM tool to all of the company's applications and networks to log the data and see the network traffic, software applications, track authorised and unauthorised users and detect any unusual activity on user accounts. 3. Install an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics. 4. Add this list of steps to a section called response to "DDoS attack with ICMP flood" to a cybersecurity playbook.
Recover	The road to recovery from this incident requires the testing of the critical network systems after they become online again and also the non-critical network systems should be turned on again. This recovery is recommended to be made after the necessary steps are taken in 'Respond' section of this report.

Completed by Yedukondalu Alias Rasavihari Markonda Patnaikuni on the 28th of May 2024