Incident report analysis

Summary	Our organization recently experienced a Ddos attack. Unfortunately we were not able to stop that attack. Our website was down for 2 hours. The threat actor used a simple kind of technique to overload our server with more requests than the capacity of the server. Due to the large number of requests in a seconds time frame, our server crashed and was not able to respond to each and every request. The threat actor was continuously sending these requests for 2 hours until we encountered the situation and brought back the server to working. This attack was due to ICMP flooding.
Identify	Our team was constantly working on the attack since it happened and was able to remove the attacker and restore the server in 2 hours by examining the logs using a packet sniffer known as tcpdump. We were able to understand that this was an Ddos attack in which the hacker used ICMP Flooding technique. The hacker was sending more ping command to the server than it could handle at a time.
Protect	The tools implemented by the security team to encounter upcoming attacks on the organization are; 1. A new firewall to limit the rate of incoming ICMP packets, 2. Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets, 3. Network monitoring software to detect abnormal traffic patterns 4. An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics
Detect	By using the new tools which are implemented after this attack we will be able to protect against these types of attacks in future.

	1. The firewall will help us to limit the incoming packages so if it encounters any overflow in packet rate then it will automatically stop the flow of packets to protect the system. 2. Another firewall port setting will stop the spoofed IP address which has been manipulated before to gain authorization. 3. Intrusion Detection system are installed which will alert the administrator incase of any abnormality in packets sent across the network. 4. Intrusion Prevention System Will help to stop the malicious activity on the network by stopping the packets and dropping them.
Respond	The team responded by enabling firewalls and stopping the threat actor from malicious activity which he was trying to do. For Future attacks the Response Team should consult the playbook immediately and follow the prescribed steps given. For further improvement, the firewalls should be corrected and Penetration Testing should be performed on the server to find any vulnerabilities which need to be addressed ASAP.
Recover	Fortunately, Nothing was destroyed. The Hacker only did a Ddos attack but was not able to get into the server. When the ping requests from the hacker stopped. The server was restarted and started working normally.