Incident report analysis

Summary	A company who provides web design, graphic design, and social media marketing solutions services has experienced a DDoS (*Distributed Denial of Service*) attack. During this incident, the company's network stopped working because a high incoming amount of ICMP (Internet Control Message Protocol) packets were blocking the regular network package streams. The response team, in order to reestablish the organization's business continuity, blocked all the ICMP income packages, brought down the non-essential network service in order to restart the vital ones, thus restoring the network access.
Identify	The DDoS faced by the organization is known as an *ICMP Flood* attack. This specific type of attack is done by exploiting vulnerabilities within the network system, allowing the threat actor to send a high amount of ICMP packets through the network to a specific server. The criminal usually uses bots to attack the targeted server. The server then becomes unable to respond to any other kind of network connection because it is overwhelmed with ICMP replies, going from the attacked server to the bots that are sending ICMP requests. After accessing the incident, it was determined that this attack was made possible by a security flaw in the firewall used by the organization, it wasn't properly configured. This vulnerability affected the company's entire network system, bringing down the services and stopping the overall business continuity.

Protect	In order to protect the organization from future similar attacks certain precaution measures need to be established. They are the following: ● The firewall needs to be properly configured and frequently updated to the new security vulnerabilities; ● New rules need to be set within the firewall, creating a limit to the incoming amount of ICMP packets; ● The IP addresses who access the network need to be verified, this will prevent spoofing attacks and regulate the ICMP streams; ● A network monitoring system needs to be implemented in order to analyze unusual network traffic; ● Detection systems also need to be implemented, IDS (*Intrusion Detection System*) and IPS (*Intrusion Prevention System*) will be a valuable ally when it comes to monitoring the network and preventing threats. ● A network segmentation infrastructure should be implemented into the company's internal network, this will make sure that if future network breaches or attacks occur, the problem can be isolated and dealt with.

Detect	The protective measures implemented into the company’s security system (previously discussed) are essential to prevent threat actors from breaking into the system and disrupting the company’s workflow. However, preemptive measures aren’t the only important things when it comes to guaranteeing the safety of the organization’s assets and business continuity. Detecting systems are a key aspect when it comes to safety and should be used in conjunction with preemptive systems, such as firewalls. It is recommended the following detection systems to be implemented into the company’s security infrastructure: - **SIEM tools**: SIEM (*Security Information and Event Management*) tools are often used to monitor the integrity of systems by analyzing the event logs. But these tools can also be implemented to analyze one's network system, and, in case of any unusual activity, report to the administrator so the security event can be verified and corrected, if it is the case. Therefore, SIEM tools can also be used as network monitoring systems, which for this event could have been an essential tool to prevent such attacks. - **IDS and IPS tools**: IDS are used to detect unusual network traffic, that’s where the tools get its name: *Intrusion Detection System*. When an insecure connection is made or a not-seen-before amount of traffic is detected within the network, the tool will generate an alert which can be evaluated by the analyst and assessed if there’s a real threat or not. The IPS tools are very much alike the IDS tools, the only difference is that the IPS tool will actively prevent the threat as soon as it is detected. Those tools can come as a good addition to the organization’s security framework, helping to prevent and monitor the network system.

Respond	In case similar security problems arise, a response protocol should be developed and implemented by the company. This response protocol should contain the following steps: 1. **Contain**: To contain a security issue, the response team should isolate the affected system from the network. This will make sure other assets won’t be affected by the problem. 2. **Neutralize**: Neutralizing a threat can be done by ensuring that the preemptive measures are properly working. In case of future ICMP flood attacks, this step is making sure the firewall is filtering all the ICMP packets. 3. **Analyze**: By analyzing the collected data from future incidents, the security team can improve the system’s reliability and avoid problems. This can be done by analyzing the data stored at the SIEM tools and the IDS and IPS alerts. 4. **Document**: This step is vital to make sure the procedures are up-to-date with current cyberthreats. If the current used protocol didn’t cover how to work around new problems during responding to the incident, the documentation should be updated.

Recover	The recovery step is essential to maintain the organization’s continuity and avoid data loss. In case of future DDoS attacks that use the ICMP flood methods, the first step to be taken is to isolate the affected network. After the isolation is done, the security team should block all income ICMP packets and bring down any non-essential services, avoiding the overload of the already affected network. After all the packets are timed out, the non-essential services can be brought back up.