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 attack was performed by a malicious party operating from outside of the company. They gained access to the internal network through a firewall that was not properly configured. • The impact of the attack was that critical network infrastructure within the company was rendered non-operational due to the large amount of network traffic. • The response to the incident was to verify the location of, and limit the number of ICMP packets that could traverse the network at one time. • IDS/IPS systems were also set up to monitor traffic and verify the location of the traffic so that an alert could be sent, and any traffic originating from external sources could be denied by the firewall.
Identify	• The event that occurred was an attack known as an ICMP flood • This type of attack occurs when a malicious party sends a large number of ICMP (Internet Control Message Protocol) packets to a target device in order to cause disruption to the system • The ICMP flood attack was combined with a Distributed Denial of Service (DDoS) attack to allow for sending the large quantity of packets to the target • The attack targeted the company's network and successfully brought

	down a large amount of the network infrastructure within the company
Protect	● To protect against this type of attack in the future, it is important to make sure that only the ports that are necessary for critical operations are open ● It is also important to make sure that the rate of packet delivery is controlled, in order to prevent the successful delivery of a large number of packets at once. ● All network devices should be configured correctly, and all configurations should be verified and confirmed to be correct and that they achieve the goals set out by the organisation
Detect	● Suspicious activity on a network can be detected by verifying the source IP address of the request. If the source IP address originates from outside the company network, then the traffic can be assumed to be malicious ● To track and verify the IP addresses of incoming packets, a SIEM tool such as Google's Chronicle could be used, and a record kept of any IP addresses flagged as malicious so that they can be blocked from future accesses ● The activity patterns of authorised users should also be monitored in order to be able to recognise when their behaviour deviates from the usual behaviour that has been seen coming from their IP address.
Respond	● If the situation described were to occur in the future, a suitable response would be to isolate the affected device from the network, so that any attempt to compromise the network through the use of the target device does not spread to the entire organisation ● To analyse the event in the future, network logs could be viewed through the use of a SIEM tool, which would provide a comprehensive overview of the logs and enable network admins to use the information in the logs to quickly recognise the attack and quarantine the affected

	systems - Backups should be kept of any device configurations, so that the configuration can be easily restored in the future, once any security vulnerabilities present in the configuration have been addressed.
Recover	- To be able to recover from a security incident, it is important to keep up-to-date backups of any critical information or device configurations, ensuring that they are free of security vulnerabilities

---

Reflections/Notes: