**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** | Internal users reported not being able to access any internal network resources. Network servers were not responding to normal traffic. The incident management team identified a large amount of incoming ICMP packets sent to a firewall that was incorrectly configured. The malicious actor was able to flood the network and cause a DDoS attack. |
| Identify | The incident management team examined access logs and discovered the flood of ICMP packets to a firewall that was incorrectly configured to allow for ICMP traffic. Examination of the source of the packets showed multiple IP addresses. The team determined that this vulnerability in the firewall allowed for a DDoS attack. |
| Protect | The team will make necessary configuration change on the firewall to limit the number of ICMP packets coming into the network. Additionally, regular audits are to take place to test configuration of the firewall and all network assets. The firewall will also be configured to detect if any of the source IP addresses for ICMP packets have been spoofed – the originating IP addresses do not match with the IPs of the systems that performed the proper TCP/IP handshake for establishing connectivity with our systems. |
| Detect | Measures are to be put in place regularly monitor incoming traffic to the firewall for suspicious activity. The firewall needs to be configured to check for any spoofed IP addresses for ICMP packets and log the information to be used in the SIEM tool. Similarly, SIEM will monitor for any suspicious changes in network activity such as ICMP packets arriving quickly from multiple source IPs. The team installed an intrusion detection and prevention system that would determine if incoming ICMP traffic is suspicious and filter out some of the traffic so the system would not be overwhelmed with requests. |
| Respond | For any future DDoS attacks on our systems using ICMP flood, we can take the following measures to respond:   1. Identify the affected asset, whether it is a firewall or other device that faces the internet. 2. Bring down the machine and isolate it for future investigation. 3. If needed and given the ability to do so, bring up a new instance and configure it to protect against the threat but do not let it handle network traffic. If applicable, assign new IP addresses and update DNS. |
| Recover | After responding to a security incident and neutralizing the threat, the team shoud:   1. Recover any damage due to loss of data by recovering filesystems and databases to the last known good full backup. 2. Reconnect affected devices and servers. Update DNS if applicable and addressing has changed. 3. Generate an incident report for company stakeholders. |

|  |
| --- |
| Reflections/Notes: |