**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 organization’s network services suddenly stopped responding. After being made aware of this, the security investigated the incident and found that network traffic was flooded with ICMP packets. So, the security team blocked all ICMP packets, halted all non critical network services, and restored critical network services. Upon further inspection, the security team determined that the company was a victim of a type of DDoS (Distributed Denial of Service) attack called “ICMP flood”. Indeed, a malicious actor sent a flood of ICMP requests with different IP addresses through an unconfigured firewall, thus bypassing security measures and forcing the network server to stop responding altogether.  The impact of this DDoS attack must not be undermined, since the servers were down for two hours costing the company precious financial resources and time, and even worse, consumer trust. To prevent another DDoS attack the security team configured the previously unconfigured firewall. |
| Identify | The security team audited the company’s network to find vulnerabilities. It found that network servers stopped responding after a flood of ICMP requests sent by a malicious actor with different IP addresses through an unconfigured firewall. Thus, it was concluded that the company was a victim of a type of DDoS attack called “ICMP flood”, where a malicious actor floods a network with ICMP packets sent from various IP addresses to disrupt business continuity. |
| Protect | To prevent future attacks, the security team configured the firewall by implementing a new firewall rule to limit ICMP packet receptions, and an Intrusion prevention system (IPS) and Intrusion detection system (IDS) to filter incoming packets based on suspicious characteristics. |
| Detect | To detect new threats the security team implemented IP address verification for ICMP packets, a SIEM tool to detect abnormal incoming traffic patterns. Also, regular security audits of the network were implemented. |
| Respond | To respond to future similar attacks, the security team should block all ICMP packets, halt noncritical network services and restore critical ones. After that, they should investigate further by checking network traffic logs in the SIEM tool for vulnerabilities. When said vulnerability is found, they should report it and implement measures to avoid further disruption, like isolating affected systems. For this, it would be good to implement network segmentation.  The company must also, on the one hand, inform the competent authorities, and inform their clients and employees of the reason they can’t access network services and apologize.  Finally, the security team must regularly check if systems are updated and configured correctly to detect and block unwanted and malicious traffic, while allowing desired traffic. |
| Recover | To recover business continuity the security team must restore all network services, that are currently unable to process requests. So, ICMP traffic should be blocked with the firewall. Then, all non-critical services must be stopped for servers to recuperate. After that, critical services must be restored. When the packet flow stops, and the server can process requests again, all noncritical network systems can be restored. Thus, restoring business continuity. |

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