**CYBER SECURITY WEEK 4 ASSIGNMENT**

**OLANREWAJU ADESINA FE/23/10260344**

**Incident report analysis**

|  |  |
| --- | --- |
| **Summary** | The internal network of the company experienced an attack which affected the network services of the company making it stop working and responding. It appears the network services have been overwhelmed by a (DDoS) attack which lead to flooding of ICMP packets causing the server to shut down as a result of exhausted network bandwidth. |
| **Identify** | The incident management team has identified the attack as a possible ICMP Flood attack. The team found that a malicious actor had sent a flood of ICMP pings into the company’s network through an un-configured firewall. This vulnerability allowed the malicious attacker to overwhelm the company’s network through a distributed denial of service (DDoS) attack.  The ICMP packets have been repeatedly sent to the server in order to exhaust the bandwidth for incoming and outgoing traffic. |
| **Protect** | The cybersecurity team installed an IPS system to filter out and drop malicious ICMP traffic based on suspicious characteristics. We also came up with new firewall rules reduce malicious incoming ICMP packets. |
| **Detect** | The cybersecurity team installed an IDS to monitor the network and detect abnormal traffic patterns. We also identified un-configured firewalls and implemented Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets. |
| **Respond** | The team responded by implementing strong security policies that include port filtering, network monitoring and proper firewall configuration. We isolated the affected systems, blocked incoming ICMP packets and stopped all non-critical network services offline. Then, the team analyzed network logs to check for suspicious and abnormal activity. We informed upper management of this event and they will contact our customers by mail to inform them about the attack. Management will also need to inform law enforcement and other organizations as required by the law. |
| **Recover** | After blocking incoming ICMP packets, the cybersecurity team stopped non-critical network services to reduce internal network traffic and restored critical network services. After the ICMP packets have timed out, non-critical network systems, services and the database from the last backup were also restored. This type of attack can be prevented from happening again by regularly scanning the network & systems, filtering and monitoring for open ports and irregular patterns in the network traffic and incoming ICMP packets. |

|  |
| --- |
| **Reflections/Notes:** An incident response plan should be established with the help of the NIST framework to provide clear guidelines for responding to several potential security incidents. The plan should include the organization’s procedures, steps, and responsibilities of each member of its incident response team. This will help to minimize the impact of a security incident faster and keep the business running. |