**Assignment 1: Use the NIST CSF to respond to a Security Incident on Module 4 of Course 3**

**Incident report analysis**

|  |  |
| --- | --- |
| **Summary** | The company (Multimedia) experienced a network disruption due to a DDoS attack via ICMP packets. The cybersecurity team mitigated the attack by blocking it and temporarily suspending non-critical network services to restore critical ones. |
| Identify | The company faced an ICMP flood attack orchestrated by malicious actors, leading to a widespread disruption across the internal network. Efforts were concentrated on securing and reinstating critical network resources for operational continuity. |
| Protect | The cybersecurity team put in place a fresh firewall regulation to control the influx of incoming ICMP packets and implemented an IDS/IPS system to screen out certain ICMP traffic with suspicious attributes. |
| Detect | The cybersecurity team made sure the firewall checks incoming ICMP packets for fake IP addresses and used network monitoring software to spot unusual traffic patterns. |
| Respond | .In upcoming security events, the cybersecurity team plans to isolate affected systems to stop further network disruption. They will prioritize restoring disrupted critical systems and services. Afterwards, they will analyze network logs for any suspicious or abnormal activity and report all incidents to upper management and legal authorities if needed. |
| Recover | To recover from an ICMP flooding DDoS attack, restoring normal functioning of network services is crucial. For future prevention, external ICMP flood attacks can be blocked at the firewall. Then, stopping all non-critical network services reduces internal network traffic. Critical network services should be restored first. After the ICMP packet flood times out, non-critical network systems and services can be brought back online. |