**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** | Earlier today, the organization’s network services suddenly stopped responding due to an incoming flood of ICMP packets. As a result of this, normal internal network traffic could not access any network resources. So our team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. |
| Identify | Following our investigation, we found out that a malicious actor had sent a flood of ICMP pings into the company’s network through an unconfigured firewall. This vulnerability allowed the malicious attacker to overwhelm the company’s network through a distributed denial of service (DDoS) attack. |
| Protect | For us to address this security event:  -A new firewall rule was implemented to limit the rate of incoming ICMP packets  - We also ensure Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets  - We install Network monitoring software to detect abnormal traffic patterns  - An IDS/IPS system were also installed to filter out some ICMP traffic based on suspicious characteristics |
| Detect | To detect this form of attack in the future, we will install an intrusion detection system (IDS) to monitor all incoming traffic from the internet. We will also install intrusion prevention system(IPS) to prevent the system against this kind of attack. Firewall will also be configured properly |
| Respond | For this type of security event in the future, we will isolate the affected systems to prevent further disruption to the network, and thenattempt to restore any critical systems and services that were disrupted by the event.  Interns will also be trained about how to respond to this kind of security incident. We will also report all incidents to upper management and appropriate legal authorities. |
| Recover | To recover from this kind of attack in the future, network services will be promptly restored to its normal functioning state by stopping all non-critical network services first to reduce network traffic.  The firewall will also be strengthened to block external ICMP flood attacks. |

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