**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** | On 06/05/23 at approximately 0900 hrs the organization network stopped responding. Employees could not access network resources on the internal network. It was determined a distributed denial of service (DDoS) attack consisting of a flood of ICMP pings was responsible. The ICMP packets were blocked and network services were restarted. The attack was abated at 1100 hrs (two hour duration). | | |
| --- | --- | --- | --- |
| Identify | The incident management team reviewed network traffic logs and identified a flood on inbound ICMP packets. This packet flood overloaded the network resources and prevented use of the internal network. An unconfigured firewall had allowed the ICMP pings into the company’s internal network. Multiple source destinations were identified and it was determined the organization has suffered a distributed denial of service (DDoS) attack. | | |
| Protect | The IMT contacted the firewall administrator regarding the unconfigured firewall. Recommendations were made to add rules to limit the rate of incoming ICMP packets and to verify source IP addresses to detect spoofed IP addresses on incoming ICMP packets. The firewall was configured to implement these new rules.  The IMT contacted the network administrator regarding installation of networking monitoring software and an intrusion prevention system (IPS) or intrusion detection system (IDS) to detect or detect and prevent suspicious ICMP and other traffic. | | |
| Detect | Network monitoring software will allow the team to aggregate log data into more easily understood dashboards as well as alert the team to potential threats. IDS/IPS will also monitor incoming traffic for suspicious packets and circumstances. Additionally, an IPS can be configured to automatically respond to many kinds of suspicious circumstances without requiring human intervention. | | |
| Respond | The IMT blocked all ICMP packets at the firewall and stopped all non-critical network services. This served to eliminate the flood of traffic that was disabling the network and allowed services to restart so they would again be responsive. This event will need to be reported to proper authorities as required by law, regulation, and company policy. | | |
| Recover | After all ICMP traffic was stopped and non-critical network services shutdown, new firewall rules were put in place and network services were restarted one by one and confirmed to be functioning normally. Blocking ICMP pings at the firewall then stopping and restarting network services in order of importance should be used to address future ICMP ping attacks. | | |

| Reflections/Notes: None. |
| --- |