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 to practice applying the NIST framework to different situations you encounter.

|  |  |
| --- | --- |
| **Summary** | The company experienced a DdoS attack via an unconfigured firewall, which compromised the internal network for 2 hours . During the attack the network stopped responding, the incident management team responded by blocking incoming ICMP packets, restarting non-crititcal services and restored critical network services. |
| Identify | The company was targeted by an ICMP flood attack. The entire internal network was affected, with all critical network resources needing to be secured and restored to a functional state. |
| Protect | The cybersecurity team implemented new firewall rules to limit the rate of ICMP packets as well as an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics. |
| Detect | The cybersecurity team added IP address verification to check for spoofed IP addresses on incoming ICMP packets as well as monitoring software to detect abnormal traffic. |
| Respond | For future events the cyber security team will isolate the attacked systems to prevent further disruption to the network. Attempts will be made to restore any systems that were disrupted (critical / non-critical). After any attacks the team will analyze network logs to check for any abnormal activity and report any incidents to managements and legal authorities, if applicable. |
| Recover | To recover from a DDoS attack by ICMP flooding, access to network services needs to be restored to a normal functioning state.  In the future, configure firewalls to block external ICMP flood attacks Then, all non-critical network services should be stopped to reduce internal network traffic. Next, critical network services should be restored first. Finally, once the flood of ICMP packets have timed out, all non-critical network systems and services can be brought back online. |

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