**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** | Today, our internal network was compromised for two hours. We received several reports from customers that our network services were not working. It is suspected to be malicious intent by an unknown group. Our security team responded quickly by taking down servers and repairing them before quickly setting them back up again. This event exposed many issues with security within our network. | | |
| --- | --- | --- | --- |
| Identify | The security team investigated the servers, internal networks, and logs. They found that a group of malicious actors sent ICMP pings and flooded our network servers, resulting in a DDoS attack. Our services had to be taken down for hours, resulting in a monetary loss, and a loss in reputation from our clients. | | |
| Protect | The security team reconfigured the firewall to limit the rate of ICMP packets, which should block any further DDoS attack using the same method. The baseline configuration documentations were updated to ensure this standard is kept in the future. The firewall will also now check the IP addresses from the packets to make sure they are from verified sources, and not fakes due to IP spoofing. An IPS system was implemented, which automatically prevents very suspicious types of network traffic. | | |
| Detect | To detect attacks in the future, a monitoring software was implemented which can detect and alert our security team to potential attacks. An IDS system was also implemented to alert to some suspicious, but not critical threats. | | |
| Respond | Systems were taken down to prevent further damage, and analyze the incident. Clients will be notified about what happened, and about the steps we are taking to ensure that this doesn’t happen again. Our playbook will be updated with more clear steps on how to deal with situations like this. Our security systems will be scrutinized to ensure they fall under cybersecurity and risk frameworks. | | |
| Recover | The servers will go back up, after we wipe all the ICMP packets and implement some of the security tools/procedures discussed. No data was lost, but we have informed staff to create a backup for the software of our services while we harden our security. | | |

| Reflections/Notes: |
| --- |