**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** | Recently, our organization experienced a DDoS attack which compromised the internal network for two hours. | | |
| --- | --- | --- | --- |
| Identify | The DDoS attack was done through a flood of ICMP packets that exceeded the server’s capacity, thus progressively overcharging it’s processing load, until it stopped responding altogether. We did not have correct firewall measures to reject the suspicious amount of traffic or to even flag it via an SIEM tool. | | |
| Protect | **The vulnerability was exploited through an unconfigured firewall. Thus, we audited every internal firewall to make sure they are up to date, activated, and comply with the baseline for the company. Firewalls now limit the rate and size of incoming ICMP packets, and verify the source address to deter IP Spoofing.**  **On the other hand, we have now installed Splunk Enterprise as our SIEM tool.**  **Finally, we have added an IDS to our internal network in order to help us with preventing new cases in the future.** | | |
| Detect | In order to detect similar threats in the future, we will use an SIEM tool (Splunk Enterprise) to alert us to suspicious traffic from the same IP. In this case, if any traffic, even from a trusted IP, has a size that considerably varies from the standard, or happens at a rate above average, it will be automatically flagged. Furthermore, as this was a DDoS attack, we will also monitor for trends where we receive the same number of requests from different sources, as the requests are all the same. A blacklist of IPs will also be implemented going forward. | | |
| Respond | The firewall’s response will be automatic from now on, so in the best case scenario, this shouldn’t happen anymore.  In the case a threat makes it past the firewall and is picked up by our IDS, we will first analize incoming traffic with a packet sniffer to make sure it’s not a false positive. In the case it is a normal attack, we will proceed as a first measure to block the incoming IPs causing the traffic and move them to our blacklist.  While that is a temporary measure, it should give us enough time to analize where the backdoor is and be able to block it. If it does not, and the attack resumes before we can plug the gap, we will shut the server down until we can fix it. | | |
| Recover | A backup of the server should be made every 24 hours so we can restore the server to its most recent state. This backup should be kept separately and be easily accessible in case we need it.  The backup should not only include settings, but also files. | | |

| Reflections/Notes: |
| --- |