**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 company experienced a DDoS attack in the form of an ICMP flood. As a result, internal networks were down for roughly two hours while engineers took extensive measures to restore regular and secure function. Following this attack, inspection of SIEM logs revealed that this attack was performed through an unconfigured firewall. |
| Identify | Inspections performed by the cybersecurity team revealed that this attack was performed through an improperly configured firewall, giving the threat actor an opportunity to contact our server and perform a DDoS ICMP flood attack. This compromised our internal network for two hours, interfering with both employee access to critical software and data needed for job function, and user access to our website. |
| Protect | To prevent a repeat of this event or similar attacks, we have reconfigured the vulnerable firewall as well as implementing more thorough packet sniffing and network monitoring to limit external IP spoofing ability. |
| Detect | To detect suspicious activity in the future, the cybersecurity team will monitor network monitoring logs and use more secure network access protocols to be able to detect IP spoofing before threat actors have access to our internal network and prevent future smurf attacks. |
| Respond | In response, all non-critical network services were taken offline and all incoming ICMP traffic was blocked until critical network services were restored. |
| Recover | As no data was damaged or manipulated during the attack, thorough checks and comparisons will be made with backup data before declaring that regular function has been restored, while a majority of recovery efforts go towards preventing future attacks and reducing attack surface. |

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