**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** | A multimedia company just had a DDoS attack, which disturbed the natural flow of the internal network for two hours until it got resolved. While the attack was going on, the company’s network services did not respond to the request of the user because of the incoming flood of ICMP packets, which resulted to normal internal network traffic not accessing any network resources. The incident management team blocked incoming ICMP packets, stopped all non-critical network services offline, as well as restoring critical network services just to stop the unnecessary incoming flood of ICMP packets.  The company’s cybersecurity team discovered that a malicious actor had sent a flood of ICMP pings into the company’s network through an unconfigured firewall, which is the vulnerability that allowed the malicious attacker to do damage to the company’s network by a distributed denial of service (DDoS) attack.  In response to this security event, the network security team decided to implement a new firewall rule to restrict the rate of incoming ICMP packets, a source IP address verification on the firewall to check for spoofed IP address on incoming ICMP packets, a network monitoring software to detect abnormal traffic patterns, an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics. | | |
| --- | --- | --- | --- |
| Identify | A DDoS attack occurred in the company’s system due to the unnecessary incoming flood of ICMP packets caused by a malicious actor sending a flood of ICMP pings into the company’s network through an unconfigured firewall. This type of attack is mostly like an occurrence of the smurf attack in which the malicious actor sniffs an authorized user’s IP address and floods it with packets. The smurf attack can occur with the use of the ICMP ping which the attacker can use that type of packet to overwhelm the servers on the network to shut them down, which creates a denial of service causing the company’s operations to a halt. | | |
| Protect | An advanced firewall needs to be included in order to monitor any unusual traffic on the network to protect against a smurf attack. | | |
| Detect | Majority of the next generation firewalls (NCFW) contain features that detect network anomalies in order to ensure that oversized broadcasts are detected before they have a chance to bring down the network. | | |
| Respond | We can use either the four devices or tools, which are firewalls, intrusion detection systems, intrusion prevention systems, and security incident and event management tools, depending on the level of security that we hope to achieve. We can go with using the Intrusion Detection System (IDS) to detect known attacks with its ability to sniff data packets while they move across the network as well as to analyze them for the characteristics of known attacks. The IDS systems can also review anomalies which are potential signs of malicious activities. When the IDS discovers an anomaly, it sends an alert to the network administrator so that they can investigate further.  The network administrator also needs to catch the malicious activity before it does any damage to the network since the limitation of the system is that it doesn't actually stop the incoming traffic if it detects something not right.  When the IDS system is combined with a firewall, then an IDS adds another layer of defense. The IDS is placed behind the firewall and before entering the LAN, which allows the IDS to analyze data streams after network traffic that is disallowed by the firewall has been filtered out which is done to reduce false positives in IDS alerts. | | |
| Recover | Port filtering is good for blocking or allowing certain port numbers to limit unwanted communication which protects against port vulnerabilities and higher encryption should also be included to make accessing the system more difficult. | | |

| Reflections/Notes: |
| --- |