**Incident report analysis**

**Scenario**



Review the scenario below. Then complete the step-by-step instructions.

You are a cybersecurity analyst working for a multimedia company that offers web design services, graphic design, and social media marketing solutions to small businesses. Your organization recently experienced a DDoS attack, which compromised the internal network for two hours until it was resolved.

During the attack, your organization’s network services suddenly stopped responding due to an incoming flood of ICMP packets. Normal internal network traffic could not access any network resources. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.

The company’s cybersecurity team then investigated the security event. They found that a malicious actor had sent a flood of ICMP pings into the company’s network through an unconfigured firewall. This vulnerability allowed the malicious attacker to overwhelm the company’s network through a distributed denial of service (DDoS) attack.

**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** | This noon an employee reported to the IT team that she was unable to access any of her internal tools, nor could she access her web development tools, she reported having a time out error every time she tried to access a tool. She indicated that she got an email this morning with an attachment, however once the file was downloaded nothing happened. A couple of employees noticed the same outage a few minutes after the initial report. |
| Identify | The incident management team gathered and analyzed the network logs report we found that a malicious actor had sent a flood of ICMP pings into the company’s network through an unconfigured firewall. This vulnerability seems to have allowed the malicious attacker to overwhelm the company’s network through a distributed denial of service (DDoS) attack. |
| Protect | The team has set up some new rules on the company´s network firewall, one of those rules includes a limit rate of ICMP packets, in order to avoid possible future ICMP flood attacks. In the other hand, source IP address verification will be set up in the firewall as well in order to restrict spoofed IP addressed on incoming ICMP packets. Also, there is a plan to implement an IDS system so the security team can have a fast response in future attack scenarios. |
| Detect | To detect new unauthorized access attacks, the team will use a firewall logging tool and an intrusion detection system (IDS), to monitor all incoming traffic from the internet. As well we provide training for all the employees on how to protect login credentials in the future. We informed upper management of this event, and they will contact our customers by mail to inform them about the data breach. Management will also need to inform law enforcement and other organizations as required by local laws. |
| Respond | The incident management team responded by blocking incoming ICMP packets and stopping all non-critical network services offline |
| Recover | The team will restore critical network services after blocking the ICMP packets and making sure there are not more requests coming into the network, before restoring the network services, in order to make sure the services will be available to be operated as usual. |

|  |
| --- |
| Reflections/Notes: Security team will reinforce their training in order to properly response and take action against attacks that may occur in the future. |