**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** | We experienced a disruptive ICMP flood attack due to an unconfigured firewall, causing a complete halt in internal network traffic. To mitigate the attack, we took immediate actions by blocking incoming ICMP packets and temporarily taking non-critical network services offline. While this response successfully restored normal network operations, the incident's impact was a downtime of approximately two hours. | | |
| --- | --- | --- | --- |
| Identify | We experienced an ICMP flood attack that exploited a vulnerability in an unconfigured firewall, leading to a disruption in our network infrastructure. This attack had a significant impact on various systems within our organization, affecting the following:   1. Internal Network Traffic: The attack completely halted normal internal network operations, preventing our employees from accessing essential network resources and services. 2. Non-Critical Network Infrastructure: As a response to the attack, we took the precautionary step of temporarily taking non-critical network services offline. This measure was necessary to prioritize critical services and ensure their restoration. 3. Critical Infrastructure: The attack posed a threat to our critical network infrastructure, potentially jeopardizing vital business operations and data. | | |
| Protect | In order to further protect against similar attacks and others we should first order a security audit to give an overall picture of our current security posture with a focus on finding any more unsecured infrastructure currently in deployment. Including quarterly security audits to make sure no new vulnerabilities have been introduced.  We should then Segment the network to separate the critical and non-critical infrastructure along with segmenting regular business data from the proprietary company information and set up security zones given the nature of our business. This will further reduce the impact of an attack from taking out all of our infrastructure at once.  While also introducing encryption into the new segmented zones of our network, with our proprietary information having the heaviest and latest methods and the other segments a less strict method.  All employee work related data will now be shared on personal network drives and/or department drives.  We will also create and store backups of our critical infrastructure and keep a baseline image for every network asset and computer. This will first allow us to get up and running quickly after an incident and enable us to compare images and configurations to ensure systems remain clean.  A new and revised IRP, BCP, and DRP should be in place moving forward in order to further reduce active downtime and increase response time during an incident.  Currently we have done the following:   * implemented a firewall rule to limit incoming ICMP traffic in order to protect against another ICMP flood. * Implemented source IP verification to check for spoofed IP addresses on any incoming ICMP packets. * Network monitoring software to detect abnormal traffic patterns * IPS and IDS systems are now in place to filter out ICMP traffic based on suspicious charastics. | | |
| Detect | We have network monitoring software in place to help detect abnormal traffic patterns along with an IDS to help us identify and understand threats as they are happening or attempted with an IPS in place to help us prevent the actual attack from happening. This will prevent attacks while also giving us information we can then use to further enhance our security posture and Defence in-depth strategy. | | |
| Respond | We will be giving out a basic employee training on cyber security, touching upon what to do or not do during or after an incident (such as referring all questions from customers or media to the proper place), phishing, good basic security habits such as not allowing others to walk through a secured door with you, locking the workstation if you are getting up for any amount of time, not sharing passwords.  This also includes training for our IT, network, and security teams on the current playbooks and BCP, DRP, and IRP’s along with weekly information about emerging attack trends. This enables a fast reaction to any incident at the onset and reducing response time and downtime. | | |
| Recover | With our new backup plan, we will be taking weekly backups of all critical infrastructure and keeping the last two backups on rotation, the newest one replacing the oldest.  Baseline images for all assets that will be revised after any changes.  The backups will allow us to be up and running in the case of any incident and will allow us to continue operations in the shortest amount of time by restoring any last data on our critical systems.  The baseline images will allow us to cut down on incidence response time and allow us to avoid potentially leaving attack surfaces open. In case of an infected asset we can wipe and reimage the asset to bring it up in running within a hour or in the case that is not possible we can now compare the images for changes to clean the asset. | | |

| Reflections/Notes: |
| --- |