**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** | The incident involved the disabling of normal internal network traffic in the organization’s network due to a DDoS attack, specifically a ICMP flood attack. The attack consisted of routing ICMP packets to destinations within the organization’s network from multiple sources. The result was that the internal network was compromised for 2 hours, i.e. the network services were unable to respond during this time. To mitigate the effects of the attack, all ICMP packets were blocked from entering the network, all non-critical network services were put offline in order to prioritize restoring critical services. The cause was the exploitation of an unconfigured firewall, which, being unconfigured, did not prevent an excessive amount of ICMP packets from entering the network. Measures were taken to secure the organization’s network from future DDoS attacks, as shall be discussed below. |
| Identify | Incident: DDoS attack, specifically ICMP flood attack. ICMP (Internet Control Message Protocol) is a protocol designed to inform devices within the network about the status of transmissions within a network, e.g. transmission success or failure. Hence, a system that receives an ICMP packet is likely to be programmed to always process it in order to learn about the status of its transmissions. The attacker took advantage of an unconfigured firewall that allowed an amount of ICMP packets to be sent to the network. The result of the attack was that, due to trying to process such a large amount of ICMP packets, the systems hosting the network services were prevented from responding to normal requests. |
| Protect | To safeguard the organization’s network from future DDoS attacks, specifically ICMP flood attacks, a natural first step was to configure the firewall – the door between the internal network and the internet – to control how many ICMP packets being routed to the network must be allowed to enter the network at a time. Additionally, since a spoofed IP address (i.e. an IP address that is from an illegitimate source but is made to appear legitimate) is indicative of an attempt to gain unauthorized access to a network, i.e. indicative of an attacker/threat actor. Hence, a key method to protect the network is to identify and block communications from spoofed IP addresses. This is done via source IP address verification in the firewall. Finally, an intrusion prevention system (IPS) both detects and prevents suspicious traffic from entering the network; while there is a risk of false positives, this measure can ensure that obvious attack patterns are identified and counteracted. |
| Detect | To detect suspicious network activity, 3 key measures have been taken:   * An intrusion detection system (IDS) to alert network operators about suspicious network activity * An intrusion prevention system (IPS), that both detects and prevents suspicious traffic from entering the network * A network monitoring software to detect abnormal patterns, in order to ascertain whether they are threats or not   For the last case, a SIEM tool (security incident event monitoring tool) is a viable option, as SIEM tools operate by making and consolidating logs of the activities within an organization, and analyzing these logs to create alerts and/or a digestible presentation of high priority risks (via dashboards).  In addition, packet sniffers could be implemented, that inspect traffic coming into the network and thereby get a more detailed understanding of the nature of the incoming traffic. |
| Respond | In this incident, the incident management team responded by:   * Blocking incoming ICMP packets * Stopping all non-critical network services offline * Restoring critical network services   However, such a response plan means critical services are at risk being put on hold before the attack can be properly contained. Adding additional safeguards to critical systems could avoid damage to the organization’s operations while giving the incident management team’s more time and breathing room to identify and contain the attack. Hence, if viable, the **network can be segmented**, giving critical services a more highly secured subnet with stricter authorization and traffic control compared to less critical services that need to be more easily accessible. |
| Recover | Currently, the recovery only involves restoring critical services first, before trying to restore non-critical services. However, this does not account for the data loss that may have occurred due to interrupted services, especially once they are taken offline before being brought back online later. To this end, regularly **backing up the data** generated by network services during their operation, especially for longer services, can ensure that an attack does not result in excessive data loss. This allows activities to resume and return to their pre-attack stage more efficiently.  Additionally, for critical services, if viable, additional systems can be configured as backup systems that run these services if the main systems are forced to go offline due to an attack. Traffic can be redirected to the backup systems via switches. |

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