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 management team had found that an excessive amount of ICMP packets were flooding into the network services of the organization, resulting in normal traffic being unable to access the network. The team had since blocked incoming ICMP packets, stopped all non-critical network services, and restored critical network services. The team had also found that the ICMP packets were coming from a malicious actor by exploiting an unconfigured firewall.
Identify	The team had found a flood of ICMP packets into the organization's networks. We have identified that the source of the ICMP packets originated from a malicious actor who is using a DDoS attack to overwhelm the network. Network crashes could lead to an impediment in the organization's business flow, resulting in potential customers being unable to access the organization website. This incident would harm the organization's revenue in the process.
Protect	The team has implemented: ● A new firewall rule to limit rate of ICMP packets ● Source IP address verification to disallow spoofed IP addresses from accessing the network In making these changes, the network would filter unauthorized and illegitimate access while still allowing legitimate users to access network services.

Detect	To detect future illegitimate access to the network, the team has implemented various detection procedures: ● Network monitoring software to detect anomalies or abnormal network access ● An IDS/IPS system to filter out ICMP traffic
Respond	The team responded to the issue by checking the network logs through our SIEM to determine the cause of the issue. We found an overwhelming amount of ICMP packets through our logs. We have examined the ICMP packets individually to determine that the cause of the issue was from a malicious actor. Subsequently, we blocked incoming ICMP packets and took non-critical services offline. We have also informed law enforcement of the issue and will liaise with them to follow-up on further investigations.
Recover	To recover the network, we restored critical services. We informed the staff that we have restored the network from back-up of the system which means they would have to re-enter any new information they would have made since the date of the back-up. In the future, the organization will use the same procedures to respond to subsequent incidents of similar nature.

Reflections/Notes: