**Incident report analysis**

**Repor analysis of a DDoS atack applying NIST CSF.**

|  |  |
| --- | --- |
| **Summary** | This morning, employees reported an inability to access the company's internal network to the IT team. The IT team promptly observed a significant influx of ICMP packets originating from various IP addresses. The security team was promptly mobilized to respond to the incident. After 2 hours of business operations being down and investigations utilizing logs and employee reports, the incident management team mitigated the issue by blocking all ICMP packets. This action temporarily halted non-critical network services but successfully restored critical network services.  Post-incident, the cybersecurity team conducted an investigation to determine the root cause of the incident. The team discovered that an improperly configured firewall had been exploited. This vulnerability enabled a malicious actor to launch a distributed denial-of-service (DDoS) attack, flooding the company's network. |
| Identify | The incident management team conducted a comprehensive audit of systems, devices, and configurations to identify security gaps. The team determined that the root cause of the incident was an improperly configured firewall, which allowed malicious actors to overwhelm the company's network with ICMP packets. The incident constituted a DDoS attack that compromised the company's network, resulting in a disruption of business operations. |
| Protect | The team has implement new firewall roles to limit the rate of ICMP packets. Source IP verification on the firewall to check for spoofed IP adresses on incoming ICMP packets. Network monitoring software to detect abnormal traffic patterns. An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics. |
| Detect | To proactively detect potential future incidents, the team will employ the following strategies:  Network Traffic Monitoring:  Utilize packet sniffer software to continuously monitor network traffic. This will enable the identification of anomalies or suspicious patterns that may indicate a potential security incident.  IDS/IPS System Alert Monitoring:  Regularly monitor alerts generated by Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). This proactive approach ensures swift identification and response to potential security threats.  Log Data Analysis:  Analyze log data from all network sources to identify unusual activities or patterns. By examining logs comprehensively, the team can spot potential indicators of compromise and take preemptive action.  SIEM Implementation:  Implement a Security Information and Event Management (SIEM) solution to centralize and correlate log data from various sources. This integrated approach enhances the team's ability to detect and respond to security incidents by providing a holistic view of the network.  By combining these monitoring and analysis techniques, the team aims to enhance the organization's overall cybersecurity posture and respond effectively to any potential future incidents. |
| Respond | The organization's response plan involves the following key steps:  Incident Reporting and Communication:  Initiate the response plan by promptly reporting any potential incident to the responsible personnel and communicating the situation to stakeholders. This ensures a swift and coordinated response.  Log Data Utilization for Investigation:  Leverage log data to facilitate the investigation process and determine the root cause of the incident. Analyzing logs provides valuable insights into the nature and scope of the security event.  Protocol Disallowance:  Proactively disallow protocols that have been exploited in the attack to safeguard critical network infrastructure. This measure helps prevent further exploitation and mitigate the impact on essential services.  Blocking Attacker Signature IP Addresses (DoS Attack):  In cases of a Denial-of-Service (DoS) attack, promptly block the attacker's signature IP addresses to mitigate the impact on network availability and performance. This action aims to disrupt the attacker's capability to launch further attacks.  IPS Systems for Attack Characteristic Marking:  Employ Intrusion Prevention Systems (IPS) to mark characteristics associated with the attacker, facilitating the identification and breaking of persistence. This helps in preventing sustained malicious activities and enhances the overall resilience of the network.  By implementing these measures, the organization aims to enhance incident response capabilities, minimize the impact of incidents, and actively deter and thwart malicious activities. |
| Recover | To facilitate the recovery of business operations, the incident management team will rely on established processes, guidelines, and technologies. The key components include:  Disaster Recovery Plans:  Activate and follow established disaster recovery plans to ensure a systematic and organized restoration of critical business functions. These plans should encompass procedures for data recovery, system restoration, and overall business continuity.  Incident Response Plan:  Refer to the incident response plan to guide the team in executing predefined actions and procedures. This includes the identification of the incident, containment measures, eradication of threats, recovery processes, and post-incident analysis.  Technological Measures:  Utilize technological tools, such as firewalls, to block protocols that were exploited during the incident. By restricting traffic outside the organization's network and implementing firewall rules, the team can prevent further exploitation and secure the network.  Limiting Traffic:  Implement measures to limit outbound and inbound traffic to essential communication only. This helps to contain the incident and reduce the risk of further compromise while focusing on critical communication necessary for business operations.  Technology Resources:  Leverage technology resources, including backup systems and redundant infrastructure, to expedite the recovery process. This ensures that essential services can be restored efficiently and with minimal downtime.  By combining these processes, guidelines, and technologies, the incident management team aims to expedite the recovery of business operations while ensuring the security and integrity of the organization's network and systems. |

|  |
| --- |
| Reflections/Notes:https://www.nist.gov/cyberframework |