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 company recently experienced a **DDoS attack** which resulted in the disruption of internal network services for approximately two hours. The atta occurred due to a **flood of ICMP packets**, which overwhelmed the network This made normal internal network traffic unable to access critical network resources. Upon investigation, the cybersecurity team found that the compa firewall had been unconfigured, allowing malicious actors to launch a flood o ICMP packets, resulting in the attack. The incident was eventually resolved blocking incoming ICMP packets, stopping non-critical services, and restorir critical network resources.
Identify	**Type of Attack: DDoS (Distributed Denial of Service) attack**, specifically through a flood of ICMP packets. **Affected Systems:** The attack compromised **all internal network services** disrupting access to normal resources for internal users. **Impact:** The internal network became unresponsive for **two hours**, severely disrupting operations. The **unconfigured firewall** created a vulnerability tha allowed the attack to occur.

Protect	**The cybersecurity team implemented:** • **Firewall rule implementation:** A new rule was added to **limit incon ICMP packets**, preventing future DDoS attacks of a similar nature. • **Source IP verification: Source IP address verification** was implemented to identify and block **spoofed IP addresses** attempting exploit vulnerabilities. • **Network monitoring:** New **network monitoring software** was insta to detect abnormal traffic patterns and prevent future intrusions. • **IDS/IPS system: Intrusion Detection/Prevention Systems** (IDS/IP were set up to filter suspicious ICMP traffic and identify malicious patterns in real-time.
Detect	To improve detection of similar threats in the future: **Firewall Logging:** All incoming traffic will be logged to monitor and detect unusual ICMP flood patterns in real-time. **Abnormal traffic detection:** The **network monitoring software** will alert t team to any traffic anomalies. **IDS/IPS utilisation:** The newly implemented **IDS/IPS system** will help dete and block suspicious traffic or patterns that match the characteristics of DD attacks.
Respond	**Immediate Response:** • **Blocked incoming ICMP packets** to stop the attack. • **Stopped non-critical services** to reduce network load and maintain functionality of critical services. • **Restored critical services** to resume business operations. **Future Response Plan:** • **Containment:** For future incidents, the team will **isolate affected systems** immediately to prevent further network disruption. • **Neutralising threat:** The team will **block malicious IP addresses** a firewall and deploy emergency **DDoS mitigation services** if needed • **Log analysis:** After each incident, network logs will be analysed to identify suspicious patterns and ensure no further breaches occur. • **Reporting:** The cybersecurity team will report incidents to upper management and authorities per **legal and regulatory requirement**

Recover	• **Restore critical systems first** to ensure business continuity. • Once ICMP flood traffic has subsided, the team will begin bringing **non-critical services** back online. • **Backup data restoration** will be carried out if any data was lost during th attack. • **Review configurations** to ensure **firewall settings** and other preventive measures are correctly implemented before bringing the network to full functionality.

Reflections/Notes: