Incident report analysis

Stephen Langford

2/18/25

Summary	Our organization recently experienced a **Distributed Denial-of-Service (DDoS) attack**, which compromised the internal network for **two hours** before it was mitigated. During the attack, network services became unresponsive due to an overwhelming flood of **ICMP packets**, preventing normal internal traffic from accessing network resources. The **incident management team** responded by: • Blocking incoming **ICMP packets** • Taking **non-critical network services** offline • Restoring **critical network services** A subsequent investigation revealed that the **firewall was unconfigured**, allowing the malicious actor to exploit this vulnerability and flood the network with traffic.
Identify	The **incident response team** conducted an audit to assess system vulnerabilities. They identified that: • The **firewall was not configured** to limit the rate of incoming ICMP packets. • The **internal network** was **overwhelmed and became unresponsive** due to the attack.

Protect	To enhance security and prevent future occurrences, the **network security team** implemented: ● **Firewall rules** to **limit ICMP packet rates**. ● **Source IP address verification** to detect and block **spoofed ICMP packets**. ● **Network monitoring software** to identify **abnormal traffic patterns**. ● An **Intrusion Detection/Prevention System (IDS/IPS)** to filter ICMP traffic based on suspicious characteristics.
Detect	To ensure early detection of unauthorized access attempts in the future, the cybersecurity team will: ● Utilize **network monitoring software** to identify anomalies. ● Deploy an **IDS/IPS system** to detect **suspicious network traffic patterns**.
Respond	The **incident management team** took the following steps to mitigate the attack: ● **Blocked all ICMP packets** to stop the ongoing DDoS attack. ● **Took non-critical services offline** to prevent further damage. ● **Restored critical services** within **two hours** after the initial outage.
Recover	The organization successfully recovered by: ● **Configuring the firewall** to limit ICMP packet rates. ● Implementing **Source IP address verification** to block **spoofed traffic**. ● Deploying **network monitoring software and IDS/IPS** for real-time

	detection and prevention. ● Ensuring the **incident response team is better prepared** for future attacks.