DDOS Incident report

**Date and Time of Incident: Not specified

Incident Overview:
Recently the organization experienced a DDos attack compromising the internal network for two hours. Network services were interrupted due to a flood of ICMP packets from a malicious actor. Normal network traffic was unable to access any resources during this time. In response the security team blocked all incoming ICMP packets and restarted critical network services.

After investigation, it was found that a malicious actor sent a flood of ICMP pings into the network through an unconfigured firewall. This vulnerability allowed the attacker to completely compromise the network through a distributed denial of service (DDos) attack.

Incident Details:
- **Incident Trigger: Unusual amount of ICMP packets to the network through a firewall
- **Duration of Incident: Two Hours
- **Affected Systems: normal network users, total internal network
- **Type of Traffic:** ICMP flood

Incident Analysis:

1. **Traffic Patterns:**
   - Analyzed traffic patterns to identify deviations from baseline norms.
   - Observed an incoming flood of ICMP packets, indicating potential irregularities.

3. **Potential Threat Vectors:**
   - Examined potential threat vectors, such as malware, DDoS attacks, or unauthorized access attempts.
   - Considered vulnerabilities in network architecture and systems. Mainly the unconfigured firewall through which the flood was sent.

4. **Impact Assessment:**
   - After assessment critical network infrastructure was affected by the flood resulting in a complete network shutdown.

Incident Response Actions:

1. **Isolation:**
   - Isolated affected systems or segments to prevent further spread.

2. **Traffic Blocking:**
   - all incoming ICMP packets blocked

3. **Forensic Analysis:**
   - Conducted forensic analysis to determine the origin and purpose of malicious traffic.

   - Malicious actor sent flood of ICMP pings into network through an unconfigured firewall

4. **Communication:**
   - Notified relevant stakeholders, including IT teams, security personnel, and management.
   - Provided regular updates on the incident response progress.

5. **Patch and Remediation:**
   - New firewall rule implemented to limit rate of incoming ICMP packets
   - Source IP address verification added to firewall to check for spoofed IP addresses on incoming ICMP packets
   - Network monitoring software installed to detect abnormal traffic
   - IDS/IPS system installed to filter out suspicious ICMP traffic

Recommendations:

1. **Enhanced Monitoring:**
   - Implement continuous monitoring for early detection of suspicious activities.
   - Invest in advanced threat detection and prevention solutions.

2. **Employee Training:**
   - Conduct security awareness training for employees to recognize and report suspicious activities.
   - Emphasize the importance of adherence to security policies.

3. **Regular Audits:**
   - Schedule regular network audits to identify and address potential vulnerabilities.
   - Ensure all systems are up-to-date with security patches.

4. **Firewall configuration**
   - Update firewalls to latest configuration standards
   - Implement firewall rules to block/allow port access from certain individuals
5. **Security Incident and Event Monitoring**
   - Installation of a SIEM tool to further enhance detection and response time

Conclusion:
The incident has been successfully contained and remediated. Ongoing monitoring and proactive security measures are recommended to prevent similar incidents. (See recommendations)

A potential response plan for future attacks is as follows:

1. Assess the incident and verify by analyzing logs and appropriate metrics by using a SIEM tool or other detection means
2. Contain the damage by isolating appropriate systems and networks to prevent spread. In this case block all incoming ICMP traffic until said traffic times-out or subsides.

3. Eliminate the cause of the damage and recover the affected system/network to operating Once traffic has subsided, restart critical network services first.
4. Document and reflect on the incident and coordinate with stakeholders or authorities to insure application of gleaned information.