Google certificate project

Use the NIST Cybersecurity Framework to respond to a security incident (Academic Simulation)

Realized by:

Nada Maach

Contents

1 Summary

The organization experienced a Distributed Denial of Service (DDoS) attack targeting its internal network through an ICMP flood. The attack lasted approximately two hours and rendered the company's server unavailable to legitimate traffic. This directly impacted the availability of critical network resources and services.
The incident management team mitigated the attack by blocking incoming ICMP packets, disabling non-critical network services, and restoring critical services to resume business operations.

2 Identify

The cybersecurity team determined that the company's web server was overwhelmed by an ICMP flood (Ping flood) originating from spoofed IP addresses. Due to a misconfigured firewall, the traffic was able to bypass controls and disrupt internal access to the organization's website and related services.

Impact

- **Confidentiality:** No compromise detected.
- **Integrity:** No data alteration observed.
- **Availability:** Critical services were disrupted for approximately two hours.

3 Protect

To strengthen defenses and reduce the likelihood of similar incidents, the team implemented:

- **Firewall Hardening:** Added rules to limit the rate of incoming ICMP requests.
- **Source IP Verification:** Configured the firewall to check for spoofed IP addresses on ICMP packets.
- **Service Prioritization:** Segmented critical and non-critical services for faster response in case of similar attacks.

4 Detect

To ensure faster detection of future ICMP flooding attempts, the following measures were deployed:

- **IDS/IPS Integration:** Configured to analyze ICMP traffic and drop malicious packets based on suspicious patterns.
- **Network Monitoring:** Implemented monitoring software to identify abnormal traffic volumes, spikes, and anomalies in real-time.
- **Alerting:** Enhanced alerting thresholds for ICMP anomalies to speed up response time.

5 Respond

The response actions during the incident included:

- Blocking malicious ICMP traffic at the firewall.
- Disabling non-critical network services to preserve resources.
- Allowing only essential services to operate while mitigation was in progress.
- Blacklisting identified malicious IPs to prevent further connection attempts.

6 Recover

The affected server was temporarily taken offline, firewall configurations were updated, and services were gradually restored to normal operation. Recovery was successful with no data loss and minimal disruption after mitigation.

7 Continuous Improvement

- Regular firewall audits to detect misconfigurations early.
- Periodic DDoS tabletop exercises to test the readiness of the response team.
- Review of service-level agreements (SLAs) to ensure uptime guarantees.

8 Conclusion

This incident highlighted a critical firewall misconfiguration that allowed malicious ICMP traffic to disrupt availability. The organization has since reinforced its Protect, Detect, and Respond capabilities. Ongoing monitoring and proactive testing will ensure resilience against future DDoS attempts.