NIST Cybersecurity Incident Report.

Summary

Recently the company experienced a DDOS attack, which compromised the internal network for 2 hours. During the attack, network services suddenly stopped responding due to an incoming flood of ICMP packets. Normal internal network traffic could not access any network resource.

Identify

The incident management team responded by blocking the incoming ICMP FLOOD of packets, stopping all non-critical network services offline, and restoring critical network services. The company's cyber security team then investigated the security event. They found that a malicious actor had sent a flood of ICMP pings into the company's unconfigured firewall. This vulnerability allowed the malicious attacker to overwhelm the company's network through a distributed denial of service (DDOS) attack.

Protect

To address this security event the network security team implemented:

- A new firewall rule to limit the rate of incoming ICMP packets
- Source IP address verification on the firewall to check for spoofed IP addresses 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 detect and help prevent future attacks. Security teams will use an Intrusion detection system to monitor all incoming traffic from the internet to filter out some of the ICMP traffic based on suspicious characteristics. Network monitoring software has been installed and configured to detect abnormal traffic patterns. Source IP address verification on the firewall to check for spoofed IP address.

Respond

New firewall configurations and IDS/IPS will help detect or eliminate future attacks. Security teams and network teams are not monitoring for penetrations into systems to prevent further disruptions to the network. SEIM tools are now monitoring current

NIST Cybersecurity Incident Report.

traffic logs and the team is working to identify any other gaps in security that may need addressing.

Recover

Once the attack was identified the team responded by blocking incoming ICMP packets. New firewall policies and SEIM tool monitoring should help prevent future network shutdowns from malicious actors. Currently teams are checking the baseline images of the network and database to ensure any discrepancies that are discovered are fixed and brought up to date. With the threat neutralized the internal networks are working properly.

.