



Incident report analysis

Summary	<p>Earlier today, our network services were suddenly cut off due to a compromise, which in turn shut off critical internal network services. The incident management team found that the event was caused due to an incoming flood of ICMP packets to the network, indicating a Distributed Denial of Service attack (DDoS). The incident response team quickly responded by blocking the incoming ICMP packets, stopping all non critical network services offline, and restoring critical network services. The total time of the attack was 2 hours before it was resolved. Through further investigation after resolution, the cybersecurity team found that a malicious actor sent a flood of ICMP packets to the network by breaking through an unconfigured firewall, which left the network vulnerable. This vulnerability allowed the malicious actor to overwhelm our network by initiating a DDoS attack.</p>
Identify	<p>The cybersecurity team was able to investigate the incident by evaluating current policies and configurations of software that may lead to vulnerabilities. Through reevaluating current configurations of our current firewalls, they discovered that we had an unconfigured firewall which created the vulnerability that allowed the malicious actor to initiate their attack to overwhelm the company network. This gap in the network's firewall allowed the malicious actor to send a flood of ICMP packets into the network known as a Distributed Denial of Service attack, overwhelming the system and inevitably shutting off critical network services for 2 hours.</p>
Protect	<p>After the event was resolved, the network security team implemented a new network hardening tactics to prevent future intrusions and attacks: a new</p>

	<p>firewall rule to limit 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, and an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.</p>
Detect	<p>To detect new DDoS and DoS attacks in the future, the team will use an Intrusion Detection System, firewall reconfigurations, and network monitoring software to monitor incoming ICMP traffic and detect suspicious activity on the network, to then filter out that suspicious activity through the use of rules to limit the rate of incoming ICMP packets and check for spoofed IP addresses of those packets</p>
Respond	<p>We can prevent future attacks like this. By implementing network segmentation, we can minimize the impact of intrusion to certain areas of the network to prevent the entire network from shutting down and isolating the event. We can also implement regular software and patch updates to fix current vulnerabilities, and make sure that our data is safe through making sure our firewalls configurations are up-to-date on the latest models for security. Implementing regular penetration testing can also help detect vulnerabilities that are unknown to us, thus making it possible for us to address them before attacks take place and decreasing our attack surface.</p>
Recover	<p>To recover from a DDoS attack by ICMP flooding, access to network services need to be restored to a normal functioning state. In the future, external ICMP flood attacks can be blocked at the firewall. Then, all non-critical network services should be stopped to reduce internal network traffic. Next, critical network services should be restored first. Finally, once the flood of ICMP packets have timed out, all non-critical network systems and services can be brought back online.</p>

Reflections/Notes: