



Incident report analysis

Summary	<p>This morning, an employee informed the IT department that he was unable to access the company's network when the security team investigated the network logs they find that the network was full of ICMP packet pings from multiple IP addresses from different locations after further investigation the team confirmed that the company's network was struck by a DDOS attack which took the servers down the team found out that the malicious actor took advantage of an unconfigured firewall.</p> <p>The team quickly took down the network to make sure that critical service can be quickly restored.</p> <p>The internal network was down for two hours until it was resolved.</p>
Identify	The security team audited the security status of the company network and they found that the malicious actor took advantage of an unconfigured firewall. They also found several gaps in the security which helped the malicious actor to successfully orchestrate a DDOS (Distributed Denial Of Service) attack .
Protect	The security team has implemented several measures to prevent these kinds of attacks in future like a new firewall rule to limit the rate of incoming ICMP packets, additionally we will invest in an intrusion prevention system (IPS).
Detect	To detect any future DDOS attempt the team has implemented a new intrusion detection system (IDS) and there will be regular network monitoring to make sure there is no abnormal activity on the company network ,also source IP address verification on the firewall has been set up to check for spoofed IP addresses on incoming ICMP packets to make sure that these attacks can be prevented.

Respond	To respond to a future attack the team created a response plan including all the necessary steps to recover the system and the whole incident will be reported to the higherups and government authorities as required by the law. This will make sure that they can respond to the attack before it can escalate to a bigger level.
Recover	<p>After confirming that it is a DDOS attack the team quickly blocked the malicious ip addresses sending the ICMP packets and took the systems down to recover them and make sure that there are no backdoors that can be used by the attacker for any other type of attack .And gradually got the systems only all within 2 hours.</p> <p>In future the ICMP packets will be blocked by the firewall , then team will confirm that it is indeed a DDOS attack afterwards all non necessary services will be taken down to reduce network traffic , then critical services will be recovered first.</p>

Reflections/Notes: The attack happened due to the flaws in our security as there was a unconfigured firewall which gave the attacker an easy way to attack the system. To prevent future attacks the team will make sure that they will remain vigilant and will make sure that network security measures are strong so that events like this do not happen again as they can cause serious harm to the company.