Incident Report Analysis

Summary	Recently, an organization who offers web design services, graphic design, and social media marketing solutions to small business reports that the organization's network services suddenly stopped responding. This action compromised the internal networks for two hours blocking normal internal network traffic from accessing any network resources.
Identify	The company's cybersecurity team audited the hardware devices, the operating systems, and the internal network. The team found that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall. This vulnerability allowed the malicious attacker to overwhelm the company's network through a distributed denial of service (DDoS) attack.
Protect	The team has implemented a new firewall rule to limit the rate of incoming ICMP packets with an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
Detect	The team will implement configured source of IP address verification on the firewall to check for spoofed IP address on incoming ICMP packets and network monitoring software to detect abnormal traffic patterns.
Respond	For future security events, the cybersecurity team will isolate affected systems to prevent further disruption to the network. They will attempt to restore any critical systems and services that were disrupted by the event. Then, the team will analyze network logs to check for suspicious and abnormal activity. The team will also report all incidents to upper management and appropriate legal authorities, if applicable.
Recover	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.

Reflections/Notes:

Security Incident Report

Identify the network protocol involved in the incident.	The incident involved the application layer which is responsible for making networks requests or responding to requests. Specifically, the HTTP and DNS protocols.
Document the incident	The incident occurred today at 1:18 p.m. Multiple customers emailed company's helpdesk complaining about that the company's website had prompted them to download a file to update their browsers. After running the file, the address of the website changed, and their personal computers began running more slowly. The website owner tried to log in to the admin panel but was unable to, so decided to reach out to the website hosting provider. The reason for being unable to log in to the admin panel was due to the attacker managed to guess the password and access to the admin panel. The cybersecurity team was alert about the incident and began to investigate the security incident. Using a sandbox environment to observe the suspicious website behavior the network protocol analyzer tcpdump was ran typing the URL for the website yummyrecipesforme.com. As soon the website loads, this prompted to download an executable file to update the browser. The file was downloaded and ran. After this action, the browser redirects to a different URL,

	greatrecipesforme.com, which design is identical to the original site. However, the company's recipes from yummyrecipesforme.com were available to be downloaded for free on the new website. After analyzing the DND and HTTP log file provided by the network protocol analyzer, we can determine that the IP address and port were effectively changed after the executable file was downloaded and ran it at 1:20 p.m. The legitimate IP address 203.0.113.22 was replaced by the IP address 192.0.2.17 used by the attack, as well as the ports used. The executable file contains a script that redirects the visitor's browsers from yummyrecipesforme.com to greatrecipesforme.com. We categorize this incident as a brute force attack.
Recommend one remediation for brute force attacks	The main reason this brute force attack was successful was due to the password was still set as default. Facilitating the attacker's access. We strongly recommend implementing a two-factor authentication (2FA) to verify the identity of the user attempting to login. Even if the attacker managed to guess the currently password, will not be able to access due to be unable to complete the second verification step that could a one-time password (OTP) send to the email or phone number of the true website admin.

Security Risk Assessment Report

Select up to three hardening tools and methods to implement	The following tools and methods are the best to implement: 1. Password policies 2. Firewall maintenance 3. Multifactor authentication (MFA)
Explain your recommendations	1. Stronger passwords policies are used to prevent attackers from easily guessing user passwords, either manually or by using a script to attempt thousands of stolen passwords. This hardening

	technique requires low frequently to be updated, especially is hashing and salting methods are used. 2. Setting firewall rules can and need to be check to update security configurations regularly. This hardening technique allows to prevent abnormal network traffic into the network. Blocking DDoS attacks for example. 3. A multifactor authentication or MFA requires a use to verify their identity in two or more ways to access a system or network. This can help protect against brute force attacks and similar security events. This hardening technique can be implemented at any time and is set up once.