Security incident report

Section 1: Identify the network protocol involved in the incident				
Time	**Source IP**	**Destination IP**	**Protocol**	**Description**
14:18:32.192571	your.machine.52444	dns.google.domain	DNS	DNS query for yummyrecipesforme.com
14:18:32.204388	dns.google.domain	your.machine.52444	DNS	DNS response with IP address 203.0.113.22
14:18:36.786501	your.machine.36086	yummyrecipesforme.com	HTTP	HTTP GET request to yummyrecipesforme.com
14:20:32.192571	your.machine.52444	dns.google.domain	DNS	DNS query for greatrecipesforme.com
14:20:32.204388	dns.google.domain	your.machine.52444	DNS	DNS response with IP address 192.0.2.17
14:25:29.576493	your.machine.56378	greatrecipesforme.com	HTTP	HTTP GET request to greatrecipesforme.com

Section 2: Document the incident
A former employee conducted a brute force attack on YummyRecipesForMe's web host by guessing the default administrative password. After gaining access, they modified the website's source code to embed a malicious JavaScript function, which prompted visitors to download and execute a malware file. This file redirected users to a fake website, greatrecipesforme.com, causing their computers to slow down. Multiple customers reported the issue, leading to the discovery of the breach. The investigation confirmed the security flaw was due to the use of a default password and lack of brute force attack prevention mechanisms.

Section 3: Recommend one remediation for brute force attacks
Implement Two-Factor Authentication (2FA): Enforcing 2FA adds an extra layer of security by requiring users to provide two forms of identification before gaining access. This makes it significantly harder for attackers to gain unauthorized access, even if they manage to guess the password.