Security incident report

Section 1: Identify the network protocol involved in the incident
The Network protocol for this incident is HTTP. Since the issue was accessing the web server for the organization. When we looked at the tcpdump traffic log, it showed usage of the http protocol when contacting the website. The malicious file was then transported to users computers using the HTTP protocol, which is at the application layer.

Section 2: Document the incident
The attacker, a former employee, gained access to the admin panel of the company by using a brute force attack. A brute force attack is a trial-and-error process of discovering private information. They repeatedly entered several known default passwords for the administrative account until they correctly guessed the right one. This kind of attack was a Cross-site scripting or XSS attack. They embedded a javascript function in the source code that prompted visitors to download and run a file upon visiting the website. After embedding the malware, the baker changed the password to the administrative account. When customers downloaded the file, they were redirected to a fake version of the website that contains the malware. After which, users complained their computers were running slowly. Several hours after the attacker had embedded this code, multiple customers had emailed the company's helpdesk. This time scale indicates that improvements to noticing security threats and alerts is needed. After receiving these emails, the cybersecurity analysts set up a sandbox environment to investigate the matter. They connected to the website and checked the tcpdump traffic log. Here it was observed that, after successfully connecting, the browser was requesting data from the company's website with the HTTP:GET method using HTTP protocol. This is when the malicious file was downloaded, which prompted an update of the browser. After which, traffic was then rerouted to the DNS server again to make another DNS request.

However this time the DNS routes traffic to a different IP, the attacker's malicious site.

Section 3: Recommend one remediation for brute force attacks
The attacker was able to gain access and change the admin password via a brute force attack. This was because the Admin password was still set to default, which is a weak security measure. The organization needs to address this by implementing a strong password policy, and more frequent password changes to help maintain security. Securing access to confidential information can also be improved with enforcing two-factor or multi-factor authentication. Thus adding extra layers of security. Since this attack took hours to be noticed, login attempts should be monitored more frequently e.g. alerts via SIEM tools. As the attacker had to make multiple guesses for the password, limiting the number of incorrect attempts would also add an extra layer of defense against these kinds of attacks.