Security incident report

Section 1: Identify the network protocol involved in the incident
Upon capturing packets to and from the website “http://yummyrecipes forme.com” and analyzing them, we can see that the protocol that is being affected is the ‘HyperText Transmission Protocol”(usually uses port 80)

Section 2: Document the incident
The Start -> Connection to the legitimate site goes through just as it is meant to and takes the user to the proper site "http://yummyrecipesfrome.com” Upon connection to the site, the user is prompted to authorize a download from the site, this is done through the HTTP GET call(This is how data is sent to the user). Malware activates -> After the malware is downloaded, 2 minutes pass before it activates. When the malware activates, the DNS server is prompted on behalf of the user to connect to the spoofed site “http://greatrecipesforme.com”. This site now displays all the recipes on the original site with no need to pay for them, greatly hindering the business of the site. Additional problems -> The malware that was downloaded to the host has been reported to slow down the operations of the hosts computer, prompting many users to be justifiably upset. This can lead to a loss in reputation for the site and company; damaging the image of the company How this happened -> Upon investigation the problem stemmed from a rogue employee with malicious intent to do harm to the company and potentially the users as well. This employee was able to get elevated privileges by running a brute force attack on the admins account, discovering that they have had a weak password. The security team is currently attempting to strip the rogue employee of his unauthorized access to

Section 3: Recommend one remediation for brute force attacks
There are a wide variety of options to stop brute force attacks from happening and thwart threat actors from gaining administrator privileges and lateral movement. The best remediations for this are: -MultiFactor Authentication(MFA) This will ensure that anyone who isn't the administrator or with proper access has no ability to gain control of the system. This is done by using the authentication principle of 'Something you have' or"Something you are" by using: -Biometric data(Fingerprints, palm scans(vein scan), iris scanning, ect) -Single-use key(SMS, authenticator App, ect) Can greatly reduce the chance of a breach using admin passwords -Single Sign On(SSO) This is a form of authentication where the user is given a key to log in and is constantly verifying that its from the same device using a key infrastructure -Strong password requirements and expiration Since the problem originated from the admin having an insecure password, ensure that they can only use a strong and secure password for entering a privileged account. Password expiration ensures that no old and potentially compromised passwords are used -Lockout policies This is a policy in which multiple unsuccessful login attempts will lock the account down and require it to be reset by a privileged member. This ensures that a brute force attempt on a privileged account will be inaccessible to the threat actor Out of these options the best to ensure that a brute force attack doesn't happen would be to use lockout policies and Strong password requirements