Security incident report

Section 1: Identify the network protocol involved in the incident
Incident involves HTTPS and HTTP protocols where website was compromised to prompt install something that redirect DNS of yummyrecipesforme.com to greatrecipesforme.com

Section 2: Document the incident
Helpdesk received multiple customer emails that our website prompted them to download a file to update their web browsers. After that, attempt to go to our website went to a look-alike, and their computer is also slower. I have created a sandboxed environment to tcpdump the traffic between my sandboxed browser and our website. Our website did indeed prompt me to download an EXE. I run that, and the browser has indeed forwarded me to a new url, greatrecipesforme.com which is a lookalike for our original site. I suspect our website had been compromised to prompt users to download malware. Judging by the content of the other website, which contains our paid recipe for free, it was probably done by a disgruntled former employee. Senior analyst Smith confirmed that our website was compromised, and checking web admin log shows a brute force attack on passwords was used to gain admin access. Admin password was never changed from default .

Section 3: Recommend one remediation for brute force attacks

Recommend auditing all passwords for public-facing servers to conform to existing password strength policy, and not left on default.
Another way is to limit failed login attempts to 3, then that IP address attempting to login will be TIMED OUT, and alert in SIEM triggered.

Further hardening can be done by setting our firewall to reject any attempt to log into web server admin from outside the company network. Any legitimate remote access would be using VPN, thus appearing to be local.

One can also implement MFA/2FA for website's admin functions and limit it to only people who *should* have access, not just anyone with password.