Security incident report

Section 1: Identify the network protocol involved in the incident
The protocols used were the usual for connecting to a website: DNS domain name translation request for finding the ip address associated with the domain name www.yummyrecipesforme.com, TCP SYN for establishing tcp/ip connection, HTTP for accessing the website contents and

Section 2: Document the incident
At around 14:20 the website www.yummyrecipesforme.com was compromised. A threat actor got access to an admin account. They then proceeded to inject the site with a Javascript snippet that downloads and runs a malware sample on the victim's computer when they try to enter the website. They are then redirected to a website of domain name www.greatrecipesforme.com, which is identical to the original website. The IT team was brought aware of this situation when the victims reported to the webdesk the domain name change and the sudden download of the malware sample, with promises of more free recipes, but then promptly made their computers run slowly. Based on the slowing down of the affected computers, the IT team suspects the malware to be a botnet, infostealer or a cryptominer. Subsequently to the attack, some system administrators could not log into their accounts because their passwords got changed. It is suspected that the threat actor used a brute-force attack, based on unusually high failed log-in attempts coming from one single IP address that showed on the logs, and based on the relatively low number of attempts it took

to compromise the account successfully, the threat actor probably used a dictionary type of brute-force attack.

Section 3: Recommend one remediation for brute force attacks
To mitigate the risk of brute force attacks on the future the company n to update it's password policy for system administrators, requiring industry standard strong passwords (at least 8 characters, at least one number, uppercase letter and special symbol); immediate password change from the default admin one; and requiring MFA to be set up. Additionally, whenever an user unsuccessfully tries to log-in three times, that account becomes disabled temporarily, with the only method of reactivation being manually by anothe system administrator.