Security incident report

Section 1: Identify the network protocol involved in the incident

The network protocol involved in the incident is DNS, HTTP

Section 2: Document the incident

The attacker has somehow managed to get access to admin page , the initial findings have been directing it is possibly a brute force attack and the Password was a default one which was not upto Security Standards. The weakness of regular auditing is evident. After accessing the admin page attacker has been setting up a malware and instructed the users who visited the page to download and install it, the users who have done the same has been redirected to another malicious page named getrecipiesforme.com

The above findings are backed by

```
14:18:36.786589 IP your.machine.36086 > yummyrecipesforme.com.http: Flags [P.], seq 1:74, ack 1, win 512, options [nop,nop,TS val 3302576859 ecr 3302576859], length 73: HTTP: GET / HTTP/1.1
```

The give log info which clearly depicts the user browser has put forward a GET request to download the malware

```
14:25:29.576493 IP your.machine.56378 > greatrecipesforme.com.http: Flags [S], seq 1020702883, win 65495, options [mss 65495,sackOK,TS val 3302989649
ecr 0,nop,wscale 7], length 0
```

The above log findings prove that the users have been redirected to another page which fooled the legitimate users

Section 3: Recommend one remediation for brute force attacks

Immediate password controls has to be initiated

2 factor authentication must be enabled
Regular audit must ensure the Passwords are changed regularly and upto the mark of Security Standards (preferably in NIST)