Security incident report

Section 1: Identify the network protocol involved in the incident
The protocol involved in the incident is the HTTP request (Hypertext transfer protocol). The issue stemmed from after accessing the web server for yummyrecipesforme.com. The tcpdump logs show that it was after the connection to yummyrecipesforme.com that it sent out another HTTP request that loaded the malicious application.

Section 2: Document the incident
Several customers contacted the website's helpdesk stating that when visiting yummyrecipesforme.com, they would be prompted to download a file and their computers would operate slowly afterward. The website owner tried logging into their admin account and noticed it was locked out. The cybersecurity analyst used a sandbox environment to analyze the website. Tcpdump was then used to analyze the network traffic packets from the steps given and they were able to recreate the steps of downloading a file and being redirected to a fake website (greatrecipesforme.com). The browser would initially connect to yummyrecipesforme.com after the initial DNS query and TCP handshake. After the downloading and execution of the file, the logs show it would then DNS query for greatrecipesforme.com with a TCP handshake before sending a HTTP request for it. Since the admin account was also locked out, there is suspicion a brute force attack was used to access the account and change the password. There could also be an attempt at XSS which is why there is code prompting for installation of a malicious file.

Section 3: Recommend one remediation for brute force attacks

One remediation to protect against brute force attacks is to make sure password length, complexity, and history are properly implemented. This makes sure that easily guessable passwords are less likely to be used. There can also be a set amount of time for frequent password changes so stolen passwords have a shorter period of being valid. Implementing MFA would also be useful to confirm the user's identity, with an OTP (one-time passcode) being sent to the user via another method to verify.

```
14:18:32.192571 IP your.machine.52444 > dns.google.domain: 35084+ A?
yummyrecipesforme.com. (24)
14:18:32.204388 IP dns.google.domain > your.machine.52444: 35084 1/0/0 A
203.0.113.22 (40)


14:18:36.786501 IP your.machine.36086 > yummyrecipesforme.com.http: Flags
[S], seq 2873951608, win 65495, options [mss 65495,sackOK,TS val 3302576859
ecr 0,nop,wscale 7], length 0
14:18:36.786517 IP yummyrecipesforme.com.http > your.machine.36086: Flags
[S.], seq 3984334959, ack 2873951609, win 65483, options [mss 65495,sackOK,TS
val 3302576859 ecr 3302576859,nop,wscale 7], length 0
14:18:36.786529 IP your.machine.36086 > yummyrecipesforme.com.http: Flags
[.], ack 1, win 512, options [nop,nop,TS val 3302576859 ecr 3302576859],
length 0
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
14:18:36.786595 IP yummyrecipesforme.com.http > your.machine.36086: Flags
[.], ack 74, win 512, options [nop,nop,TS val 3302576859 ecr 3302576859],
length 0
...<a lot of traffic on the port 80>...


14:20:32.192571 IP your.machine.52444 > dns.google.domain: 21899+ A?
greatrecipesforme.com. (24)
14:20:32.204388 IP dns.google.domain > your.machine.52444: 21899 1/0/0 A
192.0.2.17 (40)

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
14:25:29.576510 IP greatrecipesforme.com.http > your.machine.56378: Flags
[S.], seq 1993648018, ack 1020702884, win 65483, options [mss 65495,sackOK,TS
val 3302989649 ecr 3302989649,nop,wscale 7], length 0
14:25:29.576524 IP your.machine.56378 > greatrecipesforme.com.http: Flags
[.], ack 1, win 512, options [nop,nop,TS val 3302989649 ecr 3302989649],
length 0
14:25:29.576590 IP your.machine.56378 > greatrecipesforme.com.http: Flags
[P.], seq 1:74, ack 1, win 512, options [nop,nop,TS val 3302989649 ecr
3302989649], length 73: HTTP: GET / HTTP/1.1
```

```
14:25:29.576597 IP greatrecipesforme.com.http > your.machine.56378: Flags
[.], ack 74, win 512, options [nop,nop,TS val 3302989649 ecr 3302989649],
length 0
…<a lot of traffic on the port 80>...
```