Review the scenario below. Then complete the step-by-step instructions.

You are a cybersecurity analyst for yummyrecipesforme.com, a website that sells recipes and cookbooks. A former employee has decided to lure users to a fake website with malware.

The former employee/ hacker executed a brute force attack to gain access to the web host. They repeatedly entered several known default passwords for the administrative account until they correctly guessed the right one. After they obtained the login credentials, they were able to access the admin panel and change the website's source code. They embedded a javascript function in the source code that prompted visitors to download and run a file upon visiting the website. After embedding the malware, the hacker changed the password to the administrative account. When customers download the file, they are redirected to a fake version of the website that contains the malware.

Several hours after the attack, multiple customers emailed yummyrecipesforme's helpdesk. They complained that the company's website had prompted them to download a file to access free recipes. The customers claimed that, after running the file, the address of the website changed and their personal computers began running more slowly.

In response to this incident, the website owner tries to log in to the admin panel but is unable to, so they reach out to the website hosting provider. You and other cybersecurity analysts are tasked with investigating this security event.

To address the incident, you create a sandbox environment to observe the suspicious website behavior. You run the network protocol analyzer tcpdump, then type in the URL for the website, yummyrecipesforme.com. As soon as the website loads, you are prompted to download an executable file to update your browser. You accept the download and allow the file to run. You then observe that your browser redirects you to a different URL, greatrecipesforme.com, which contains the malware.

The logs show the following process:

1. The browser initiates a DNS request: It requests the IP address of the yummyrecipesforme.com URL from the DNS server.
2. The DNS replies with the correct IP address.
3. The browser initiates an HTTP request: It requests the yummyrecipesforme.com webpage using the IP address sent by the DNS server.
4. The browser initiates the download of the malware.
5. The browser initiates a DNS request for greatrecipesforme.com.
6. The DNS server responds with the IP address for greatrecipesforme.com.
7. The browser initiates an HTTP request to the IP address for greatrecipesforme.com.

A senior analyst confirms that the website was compromised. The analyst checks the source code for the website. They notice that javascript code had been added to prompt website visitors to download an executable file. Analysis of the downloaded file found a script that redirects the visitors' browsers from yummyrecipesforme.com to greatrecipesforme.com.

The cybersecurity team reports that the web server was impacted by a brute force attack. The disgruntled hacker was able to guess the password easily because the admin password was still set to the default password. Additionally, there were no controls in place to prevent a brute force attack.

Your job is to document the incident in detail, including identifying the network protocols used to establish the connection between the user and the website. You should also recommend a security action to take to prevent brute force attacks in the future.

Log Data

```
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>...
```

How to read the tcpdump traffic log

This reading explains how to identify the brute force attack using tcpdump.

```
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)
```

The first section of the DNS & HTTP traffic log file shows the source computer (**your.machine.52444**) using port **52444** to send a DNS resolution request to the DNS server (**dns.google.domain**) for the destination URL (**yummyrecipesforme.com**). Then the reply comes back from the DNS server to the source computer with the IP address of the destination URL **(203.0.113.22**).

```
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
```

The next section shows the source computer sending a connection request (**Flags [S]**) from the source computer (**your.machine.36086**) using port **36086** directly to the destination (**yummyrecipesforme.com.http**). The **.http** suffix is the port number; **http** is commonly associated with port 80. The reply shows the destination acknowledging it received the connection request (**Flags [S.]**). The communication between the source and the intended destination continues for about 2 minutes, according to the timestamps between this block (**14:18**) and the next DNS resolution request (see below for the **14:20** timestamp).

TCP Flag codes include:

Flags [S] - Connection **S**tart
Flags [F] - Connection **F**inish
Flags [P] - Data **P**ush
Flags [R] - Connection **R**eset
Flags [.] - Acknowledgment

```
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 log entry with the code **HTTP: GET / HTTP/1.1** shows the browser is requesting data from **yummyrecipesforme.com** with the **HTTP: GET** method using **HTTP** protocol version **1.1**. This could be the download request for the malicious file.

```
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 192.0.2.172 (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
```

Then, a sudden change happens in the logs. The traffic is routed from the source computer to the DNS server again using port **.52444** (**your.machine.52444 > dns.google.domain**) to make another DNS resolution request. This time, the DNS server routes the traffic to a new IP address (**192.0.2.172)** and its associated URL (**greatrecipesforme.com.http**). The traffic changes to a route between the source computer and the spoofed website (outgoing traffic: **IP your.machine.56378 > greatrecipesforme.com.http** and incoming traffic: **greatrecipesforme.com.http > IP your.machine.56378**). Note that the port number (**.56378**) on the source computer has changed again when redirected to a new website.

Security incident report

Section 1: Identify the network protocol involved in the incident

The primary network protocols involved in this incident are **DNS (Domain Name System)** and **HTTP (Hypertext Transfer Protocol)**. DNS was used to resolve the domain names `yummyrecipesforme.com` and `greatrecipesforme.com` into their respective IP addresses. HTTP was used to transfer web content between the browser and both websites, including the request to download the malicious file and the redirection to the attacker-controlled website.

Section 2: Document the incident

On May 14, multiple customers reported unusual behavior on the company website, yummyrecipesforme.com. Users were prompted to download a file claiming to offer free recipes, after which their browsers were redirected to greatrecipesforme.com and their computers began performing slowly. Investigation revealed that a former employee had performed a brute force attack on the web server by repeatedly attempting default passwords until access was gained to the admin panel. Once logged in, the attacker modified the website's source code by embedding JavaScript that triggered a file download. The attacker then changed the admin password to lock out legitimate access. The cybersecurity team confirmed the attack by analyzing traffic in a sandbox environment using `tcpdump`, which showed a DNS request for yummyrecipesforme.com, followed by an HTTP request to download a malicious file, and subsequent redirection via DNS and HTTP to greatrecipesforme.com. The incident was traced through packet captures, server logs, and source code review, confirming unauthorized access and malware deployment.

Section 3: Recommend one remediation for brute force attacks

To prevent brute force attacks in the future, the organization should

implement two-factor authentication (2FA) for all administrative access. 2FA adds an essential layer of security beyond just a username and password by requiring a second verification method such as a mobile-generated code. This significantly reduces the chances of unauthorized access, even if a password is guessed or compromised, thereby strengthening account protection against brute force and credential stuffing attacks.