Security incident report

Section 1: Identify the network protocol involved in the incident
From the tcpdump, it's pretty clear that DNS (Domain Name System) is the network protocol that is being used to divert network traffic to a different website.

Section 2: Document the incident
The tcpdump given here starts at timestamp - 14:18:32.192571 The first two lines are how a normal network log should look like. User's machine using the port number: *52444* sends the DNS resolution request to the DNS server (*dns.google.domain*) for the URL (*yummyrecipesforme.com*) In the next line, the server replies with the IP of the website (*203.0.113.22*) After a few seconds, the user's machines sends a request with a different port number: 36086 to *yummyrecipesforme.com.http* The flag [S] represents the start of the connection In reply we get another flag [S.] which indicates connection request acknowledged User's machine remains connected to the website for the next two minutes and you can see some more flags in between. [.] represents acknowledgement. At timestamp 14:20:32.192571 we see the original port number: 52444 asking for a DNS resolution request for a new URL (*greatrecipesforme.com*). And we get a new IP address (*192.0.2.17*)

After five minutes at timestamp 14:25:29.576493 we see a new port number sending a connection request from the User's machine. The log at timestamp 14:25:29.576590 shows HTTP: GET / HTTP/1.1 which indicates that the browser is requesting data from the website. With the HTTP:GET method, using HTTP protocol version 1.1. It could be an attempt at downloading a malicious file.

Section 3: Recommend one remediation for brute force attacks
For this case in particular it's better to use websites with HTTPS in their address. They are more secure and thus may prevent attacks like these. But brute force attacks in general can be prevented using MFA or 2FA. It gives the end user multiple ways to secure their device and ensure that only they can access their accounts and other important websites.