Security incident report

What happened and network protocol involved in the incident
I was put in a situation where I had to analyze what was happening on a website that sells cookbooks. According to the case, users were reporting that they were having problems with the website, because as soon as they accessed the site they were asked to download a document, and after that document was downloaded their computer started to slow down. So I had to analyze the LOG to see what was happening. My analysis, the protocol involved in the incident is the Hypertext transfer protocol (HTTP).

Incident documented
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). 14:20:32.192571 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) And here, two minutes later, it was also noticed that (your.machine.52444) using port 52444 to send a DNS resolution request to the DNS server (dns.google.domain) for a different destination URL (greatrecipesforme.com). Realizing that the destination URL is being sent to another website.

Recommendation in this case (brute force attacks)
According to the case, this attack was carried out by a former employee, who managed to log into the web host after several password attempts. He managed to log in because the password remained the same, it was the factory default. In this case, it is highly recommended that default passwords be changed and 2FA should also be implemented, to prevent situations like this from happening again.