Security incident report

Section 1: Identify the network protocol involved in the incident
The network protocol involved in the incident was the Hypertext Transfer Protocol. By using tcpdump while accessing yummyrecipesforme.com, a log of DNS and HTTP traffic was recorded and analyzed to come to this conclusion. The malicious file was shown to get the VM using the HTTP protocol in the application layer.

Section 2: Document the incident
Security Analysts used a sandbox on a virtual machine to test the website's suspicious behavior. The tcpdump log was able to record the virtual machines multiple request which were the following: ● At 14:18:32 the VM sent a DNS query for yummyrecipesforme.com and received a legitimate IP for the website ● At 14:18:36 the VM initiates a TCP connection to HTTP on the website and connects successfully. ● At 14:18:36.786589, the VM sends an HTTP GET request to yummyrecipesforme.com, this could be the download request for the malicious .exe file. ● At 14:20 the VM is redirected to a new IP address for greatrecipesforme.com. Following the same DNS, and TCP connections to the new IP.

Section 3: Recommend one remediation for brute force attacks
One remediation for brute force attacks is to implement password policies. For example, password requirements for capital letters, numbers, and special characters. As well as, implementing a periodical password change policy.