Security Incident Report

Section 1: Identify the network protocol involved in the incident
The network protocol involved in the incident is HTTP. The traffic logs indicate communication between the affected machine and two domains, yummyrecipesforme.com and greatrecipesforme.com, over port 80 standard port for HTTP.

Section 2: Document the incident
At 14:18:32 and 14:20:32, the affected machine initiated DNS queries to resolve the IP addresses of the domains yummyrecipesforme.com and greatrecipesforme.com, respectively using the DNS protocol (port 53). DNS responses were received for both queries. At 14:25:29 the affected machine established TCP connection to the respective HTTP servers of the mentioned domain on port 80 requests were made to access their web resources. Based on the provided tcpdump traffic log, it appears that the affected machine is communicating with external HTTP servers via DNS queries, followed by HTTP requests. This activity suggests potential web browsing or web-based application usage of the affected machine.

Section 3: Recommend one remediation for brute force attacks
To mitigate the risk of brute force attacks targeting the HTTP services, one recommended remediation is to implement account lockout mechanisms. This involves temporarily locking out user accounts after a certain number of failed login attempts within a defined period. Additionally, implementing strong password policy, such as requiring complex passwords and enforcing regular password changes, can further reduce the likelihood to successful brute force attacks