Security incident report

Section 1: Identify the network protocol involved in the incident
The protocols used are DNS and HTTP. Both protocols use the TCP/IP to operate over. The issue is that after trying to reach yummyrecepiesforme.com the user is redirected to different web site imitating the initial one. After running a tcpdump, the log file shows that after finishing the handshake process after initiating HTTP protocol and exchanging significant amount of data another DNS request from another port is initiated for another similar web site.

Section 2: Document the incident
After users try to reach yummyrecepiesforme.com are redirected to greatrecepiesforme.com. Ater examining the tcpdump log file, we can trace a request sent from a user to the DNS server for reaching yummyrecepiesforme.com, after the 3 step handshake is complete. After initiating a HTTP request with push protocol, from yummyrecepies.com acknowledged the request and sends data which is indicated as a lot of traffic on port 80, which is a red flag, even though there is a possibility the content of the site to be with a lot of data. Right after that data transfer, from the user device new request from new port is initiated to the DNS server for new web site greatrecepiesforme.com which ends in 3 way handshake and http request acknowledged from the greatrecepiesforme.com and ending with a lot of traffic. A further investigation is needed and logs must be inspected to determine what is the attack exactly. One possible scenario is a brute force attacks in which threat actor has provided an invisible link that leads to downloading malicious code, that redirects the user to a different site with identical look so they can enter their credentials and those get stollen.

Section 3: Recommend one remediation for brute force attacks

Recommendations:
Enforce HTTPS connections, implementation of Control Security Policies, regular pen testing and audits, Update and modify Firewalls, and update systems and antivirus. Implement strong password policies and limit the login attempts, implement MFA, regularly inform users for threats and different ways to prevent exploitational checking for the padlock icon in the address bar, before entering credentials to verify they are on the correct site, update their antivirus, don’t klick on suspicious links, have strong and different passwords for different sites.