# Security incident report

| **Section 1: Identify the network protocol involved in the incident** | |
| --- | --- |
| The network protocol used in the incident is the HTTP. The issue involved was accessing the web server, and these involve http traffic. When tcpdump was run, the log file showed that the http protocol was used when the malware was installed. This was done using the http protocol in the application layer. | |
|

| **Section 2: Document the incident** |
| --- |
| The traffic log file shows that when attempting to connect to the IP address associated with ‘yummyrecipesforme.com’, everything runs as normal to begin with. Using port 52444, a DNS resolution request is sent to the DNS server for the URL. The reply comes back and gives the IP address for the destination URL. The source computer sends the connection request using port 36086 to the destination ‘yummyrecipesforme.com.http’. The http suffix is associated with port 80. This continues back and forth for a time. Then the log entry shows a request for data from the URL with the HTTP.GET method. This is likely the download request for the malware. Next, the traffic is routed to the DNS server again using port 52444 to make another DNS resolution request. The DNS this time routes the traffic to a new IP address that is associated with the URL ‘greatrecipesforme.com.http’. The port number on the source computer has now changed to 56378. |

| **Section 3: Recommend one remediation for brute force attacks** |
| --- |
| After reviewing the incident and how the attack was carried out, it seems that a sufficient password policy is lacking. Malware was inserted to the source code of the website, installing itself on users establishing a connection. This could have been avoided if passwords were changed and a strong password policy was enforced. No passwords should be given to employees without the proper authorization. It would also increase security posture if passwords were changed when employees are let go or quit. |