# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| The network protocol involved in the incident is **HTTP (HyperText Transfer Protocol)**. This is evident from the traffic captured on port 80, where the HTTP GET requests (GET / HTTP/1.1) were observed. HTTP is an unencrypted protocol used for communication between a client (such as a web browser) and a web server, and it is commonly associated with web browsing activities. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| **Incident Discovery:**   * This incident was discovered during routine network traffic monitoring, likely using a tool such as tcpdump or Wireshark. The presence of large volumes of HTTP traffic over unencrypted port 80 raised concerns about data security and the legitimacy of the domains.   **Incident Response:**   * Further investigation is required to determine whether the traffic was part of a legitimate activity or if the domains represent a security threat (e.g., phishing or malware-hosting sites). Traffic logs will be analyzed for unusual patterns or any unauthorized data transmission.   **Incident Recovery:**   * After mitigating the incident, steps should be taken to ensure that machines and the network are properly secured. Review firewall rules, and update the security policies if necessary to prevent recurrence. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| **Security Measure Recommended:**   * **Enforce HTTPS for All Traffic:** Implement policies that require the use of HTTPS, ensuring that all communication between the organization and external servers is encrypted. * **Web Filtering and Network Controls:** Block access to suspicious or unauthorized domains at the network level to prevent such incidents in the future. |