# Security incident report

| **Section 1: Identify the network protocol involved in the incident** | |
| --- | --- |
| network protocol analyzer tcpdump | |
|

| **Section 2: Document the incident** |
| --- |
| there was a brute force attack on a website |

| **Section 3: Recommend one remediation for brute force attacks** |
| --- |
| create sandbox environment , run the network protocol analyzer tcpdump and then type URL of the website you observe that the website contains malware . |