Frothly is a small premium beer brewing company with intensions of making it big. Competition in the brewing industry has become intense. Other companies are looking to get intellectual property from Frothly by whatever means possible. It looks like the previous web scan was only the beginning.

Your job now is to investigate the possible breach to determine what was stolen or if a breach occurred. The Chief Information Officer is also concerned about cyber security practice and management within the organisation and has asked you to provide a review of these processes and procedures in line with recent relevant vulnerabilities.

Task 1 - Splunk Based Incident Investigation

Frothly competitors are looking to take intellectual property from them, and the Chief Information Officer believes that they may try to compromise online Frothly systems. The following questions are related to possible attack on the Frothly computer systems. As part of the answer for each of these questions, your report must include:

- A clear description of the reasoning for your answer.
- A detailed description of the process that you followed and the searches that you used to obtain the answer. It is expected that you will include screenshots in your description.

- Provide a list of suspicious IP addresses that attempt to make an unauthorized web connection to Frothly systems. Only list connections that have a duration of longer than 1 minute.
- Identify and display the US states that contribute the most client registrations on the Frothly web site. Which states have the most unauthorised web connections?
- Which web pages are directing Frothly's customers to their web site? Identify the top external websites that contribute the most referrals to the Frothly web site and display the number of referrals in a table?
- The server running www.brewertalk.com experienced temporary unavailability. When did this happen and for how long?
- This temporary unavailability was caused by a vulnerability scanner which was running a web vulnerability scan against www.brewertalk.com. Provide the range of ports that were scanned by this vulnerability scanner?
- An important file is transferred from Kevin Lagerfield's laptop. What is this important file?
- Kevin Lagerfield claims that this file was stolen from his computer because he received a warning a few weeks ago. Is there any evidence to agree or disagree with his claim?
- Frank Ester claims that his password on http://www.brewertalk.com/ was leaked. Frank lets you know his password is Aa12345. Is there evidence that this password was extracted?

- The leak of passwords is caused by the misuse of the updatexml SQL function. Apart from updatexml function, an attacker also misuses another function for reconnaissance purposes. What is this function?