1. 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.
2. 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?
3. 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?
4. The server running www.brewertalk.com experienced temporary unavailability. When did this happen and for how long?
5. 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?
6. An important file is transferred from Kevin Lagerfield's laptop. What is this important file?
7. 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?
8. 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?
9. 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?