7808ICT Cyber Security Management Assignment 2 Specification

Due Date: 25th May 2020
Weighting: 30%

This assignment is worth 30% of the total assessment for 7808ICT. It is individual work. While you can discuss the assignment with your peers, your submission should be your own work. You should provide evidence of your own work incorporated in your submission (e.g. screenshots with your login name showing).

The objective of this assignment is to gain knowledge and understanding of the security information and event management tool Splunk through research and practical experience. This understanding is to be demonstrated by submission of a formal technical report of a threat hunting exercise and the development of a Splunk dashboard.

All assignment related data can be found in the botsv2 index (you must include "index=botsv2" in all your searches) on the http://splunk.ict.griffith.edu.au:8000 Splunk Enterprise server. Login using the following credentials if you have not logged into this server before.

Username: sXXXXXXX
Password: changeme

If you are trying to connect to the server from off campus, you must connect through a VPN first. Details of how to VPN into the Griffith Network can be found here:
https://intranet.secure.griffith.edu.au/computing/remote-access/virtual-private-network

Please note that the assignment data is **much bigger** and more realistic than your tutorial data, so you must limit your searches, otherwise you will be waiting for a long time for a response as well as slowing down everyone else.

Background

Frothly is a small premium beer brewing company with intensions of making it big. New homebrew kits with Frothly proprietary recipes are due to launch later in the year. The FBI has heard chatter from a nation state sponsored hacking group that claim to have successfully compromised the Frothly network and exfiltrated sensitive data. As luck would have it Frothly's Head of IT, Kevin Lagerfield, has just left the company. Your job is to investigate the breach to determine what was stolen or if a breach actually occurred.

Task 1

1. Amber Turing was hoping for Frothly to be acquired by a potential competitor which fell through, but visited their website to find contact information for their executive team. What is the website domain that she visited?
2. Amber found the executive contact information and sent him an email. What is the CEO's name? Provide the first and last name.
3. After the initial contact with the CEO, Amber contacted another employee at this competitor. What is that employee's email address?
4. What is the name of the file attachment that Amber sent to a contact at the competitor?
5. What is Amber's personal email address?
6. What version of TOR did Amber install to obfuscate her web browsing? Answer guidance: Numeric with one or more delimiter.
7. What is the public IPv4 address of the server running www.brewertalk.com?
8. Provide the IP address of the system used to run a web vulnerability scan against www.brewertalk.com.
9. The IP address from Question 8 is also being used by a likely different piece of software to attack a URI path. What is the URI path?
10. What SQL function is being abused on the URI path from Question 9?
11. What is Frank Ester's password salt value on www.brewertalk.com?
12. What is user btun's password on brewertalk.com?
13. What was the value of the cookie that Kevin Lagerfield's browser transmitted to the malicious URL as part of a XSS attack?
14. The brewertalk.com web site employed Cross Site Request Forgery (CSRF) techniques. What was the value of the anti-CSRF token that was stolen from Kevin Lagerfield's computer and used to help create an unauthorized admin user on brewertalk.com?
15. What brewertalk.com username was maliciously created by a spear phishing attack?
16. According to Frothly's records, what is the likely MAC address of Mallory's corporate MacBook? HINT: Her corporate MacBook has the hostname MACLORY-AIR13.
17. What episode of Game of Thrones is Mallory excited to watch?
18. What is Mallory Krauesen's phone number?
19. Enterprise Security contains a threat list notable event for MACLORY-AIR13 and suspect IP address 5.39.93.112. What is the name of the threat list (i.e. Threat Group) that is triggering the notable event?
20. Considering the threat list you found in Question 19, and related data, what protocol often used for file transfer is actually responsible for the generated traffic?

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.

Task 2

Develop a Splunk dashboard for the Frothly data. The dashboard should include 5 panels with a variation of visualisations with at least one single value display. The dashboard should use the following Splunk functions:

- Chart
- Timechart
- Macros
- Pivot
- Eval
- Search
- Where
- Stats
- Count
- Transaction

As well as showing the output of the dashboard, your report must include:

- A clear description of the design of your dashboard, explanations of the searches used, and the importance and purpose of each panel.
- A detailed description of how you incorporated command functionality into the dashboard and the reasoning for why the commands are required for the panel.

Submission

Please submit your assignment via the 7808ICT Blackboard web site under the Assessment section. Reports may be submitted as one zip file or as a single file.

The quality of the presentation of a formal technical report is as important as the quality of the technical content of the report in the profession. Your assignment will be assessed on:

1. The body text of your report should be no more than 25 pages in length excluding appendices;
2. The text of your report should be in 12-point Times New Roman or 11-point Arial font or something equivalent, and in single space;
3. Page size is A4 with 2cm in margins on all sides;
4. The report is suggested to be organised with executive summary within one page, table of contents, body text, and appendices;
5. The report body text consists of your overall analysis of each question, description of how you went about completing each task and your conclusions.