Using the website(s) assigned to you in Unit 1, carry out the following exercise and answer the questions listed below.

Your results and responses should be posted on the wiki, created by you and your fellow students. As this is a wiki activity, please [**see guidance here on using a wiki**](https://docs.moodle.org/38/en/Wiki_activity) on the Moodle platform.

**Note:** this is a collaborative exercise, please only add to the wiki and do not delete other student's work.

Perform scans against your assigned website(s) using the tools available in Kali Linux. Answer as many of the following questions as you can:

1. What Operating System does the website utilise?
2. What web server software is it running?
3. Is it running a CMS (Wordpress, Drupal, etc?)
4. What protection does it have (CDN, Proxy, Firewall?)
5. Where is it hosted?
6. Does it have any open ports? Which did you expect to be open?

The wiki should consist of two sections:

1. The first section should be a FAQ (frequently asked questions) where you can post questions. In addition, if you have encountered and solved any of the questions/ issues, you should post your responses to the queries.
2. The second section involves the results - each of you should post a compilation of the results they have obtained in the wiki. Doing so will allow your fellow students to evaluate the kind of results available and ask questions (in the FAQ section) about how certain results were obtained. Offer constructive feedback on the results posted.

For advice on constructive feedback and understanding other peoples' points of view, look at the [**guidelines on the Department’s homepage**](https://www.my-course.co.uk/course/view.php?id=4634) on peer review.

**Learning Outcomes**

* Identify and analyse security threats and vulnerabilities in network systems and determine appropriate methodologies, tools and techniques to manage and/or solve them.
* Design and critically appraise computer programs and systems to produce solutions that help manage and audit risk and security issues.
* Gather and synthesise information from multiple sources (including internet security alerts and warning sites) to aid in the systematic analysis of security breaches and issues.

**Reflection**

Reflect on this activity by answering the following questions:

* Did you have any issues or challenges with the scans?
* How did you overcome them?
* How will they affect your final report?

Record all reflections in your e-portfolio.

Website: loadedwithstuff.co.uk/

What Operating System does the website utilise?

Apache

What web server software is it running?

Apache

Is it running a CMS (Wordpress, Drupal, etc?)

No. The server is running PHP and Apache

What protection does it have (CDN, Proxy, Firewall?)

The website is not using CDN

Where is it hosted?

https://www.a2hosting.com/

Does it have any open ports? Which did you expect to be open?

The following ports were open / closed

21/tcp open ftp

22/tcp closed ssh

25/tcp open smtp

53/tcp open domain

80/tcp open http

88/tcp closed kerberos-sec

110/tcp open pop3

143/tcp open imap

443/tcp open https

445/tcp closed microsoft-ds

465/tcp open smtps

587/tcp open submission

993/tcp open imaps

995/tcp open pop3s

3306/tcp open mysql

5432/tcp open postgresql

Did you have any issues or challenges with the scans?

It was fairly easy to scan the website. I used Nmap software to map out open ports and information about the website.

How will they affect your final report?

The research I’ve conducted in this assignment will help me in the final executive assignment.

References:

Nmap network scanning: The Official Nmap Project Guide ... - researchgate (no date). Available at: https://www.researchgate.net/publication/234829346\_Nmap\_Network\_Scanning\_The\_Official\_Nmap\_Project\_Guide\_to\_Network\_Discovery\_and\_Security\_Scanning (Accessed: February 25, 2023).