**Network and Information Security Management E-portfolio Reflection Assignment**

In this Network and Information Security Management Modules I have learnt and done different concepts like how to scan and penetration tool and activities like collaborative discussions, pen scanning exercise and practical and team activity. With these all process I got knowledge and experiences as an individual and as a group. Just here below I would like to reflect about it.

In the first collaborative discussion part I have posted and discussed about the health care cybersecurity industries threats and focused on Brute force attacks and denial-of-service. Right now, it has come the momentous threats in the medical center. And most of medical center susceptibilities can concession clients’ statistics. Once observing at possible fears, Brute force attacks and denial-of-service are common.

In addition to my point my classmates ([David Luvaha](https://www.my-course.co.uk/user/view.php?id=14337&course=6756) from [Jan Küffner](https://www.my-course.co.uk/user/view.php?id=14259&course=6756)) also added their ideas on network hard ware replacement to support modern crypto algorithms to secure it . Since NHS Digital (2020) acknowledges that breaches related to security of associated medical hardware may lead to substantial interruption to the service operation in medical center. Besides the technical issues, another class mate [Kin Wong](https://www.my-course.co.uk/user/view.php?id=14575&course=6756) considered human factor as a highest potential risk of health care cybersecurity industries. According to the Sky News today (2021) the IT systems of the Ireland’s health service are all being shut down because of significant ransomware attack, which maybe happened due to any human error. According to Joseph (2021), he stated 5 network security risks which are happened by human error. So that in my first collaborative discussion what I understand is that to make health care cybersecurity industries are stable and secure we should consider all issues which describe in the above.

In my collaborative discussion 3 I raised an issue about CCTV data in a disciplinary This case study concerns on unfair use of CCTV data in a corrective procedure practicing on one staff. The foundation of the opposition being was unethically attained.And our tutor, Doug Millward also gave the following comments on this regard “it is good to highlights about processes, procedures, and the human element also It is worth considering how the data itself can be encoded as part of security precautions as well as looking at alternative mechanisms that may be usable”.So, I totally agreed with in the above comment.

we have practiced on how to make basic penetration scan test individually and as a group. In this test as group, we agreed that each individual person would conduct a basic scan each on the opposing groups website so that we could compare the results with each other. And Some of the results were vastly different across the board.

In regards to my own individual results I used this web site “WEBSITE- <http://nismphp-env.eba-ytbpbyww.us-east-1.elasticbeanstalk.com/>” and I Perform a basic scan test using standard tools such as ping, traceroute, dig and nslookup in order to answer the following information:

How many hops from your machine to your assigned website? - I got Traceroute detected 21 hops, which step causes the biggest delay in the route? I got Hop 13, What is the average duration of that delay? -; I got Average duration- 96 ms (found from the ping test results), What are the main nameservers for the website? -I got Whois 'markmonitor.com', Who is the registered contact? – I got Amazon Technologies Inc. (AT-88-Z), What is the MX record for the website? – I got No MX record found and where is the website hosted? and I got Ashburn, Virginia, United States. In this exercise I have gained skill how to scan different website with different tools within different operating system.

In our design part of a Network and Information Security Management (NISM) Assessment Project. In this design part we have explained a lot of issues as we have attached at group assignment. As an individual I have contributed something on the appropriate related standards part. In the summery part we have explained a lot of issues as we have attached at group assignment. As an individual here I contribute something in the recommendation and conclusion parts. Since we did scan inspection, then we got several security intimidations that should be alleviated so based on this finding I recommended the following for it.

* penetrations result indicated ports 21 and 80 are exposed. It is HTTP port, mean no encryption among the client and server once they communicating. HTTP are more susceptible for attacker and DoS (Acunetix, 2014).
* Some CMS working on the webserver this may expose the scheme to cyber-attack like SQL injections and database attacks. Social factor in this case will be the possible source of the risk. (FutureEnTech, 2020).

Based on the above conclusions and after analysing the website, here below are the recommendations.

* The first recommendation should be Practise SSL and port 443 can avert any unsecured data transient over.
* To avert SQL shot to toxic the medical site record, the site would be threatened practicing solutions like next generation security device, ACL protocols and other security procedures.
* Port 20 and 80 should be encrypted and other redundant exposed port would be evading from any treat.

In conclusion I have seen that using security tools, network security protocol and huma factors is very critical to build better security strategies and these could be the key to preventing some of the worst attacks. At the end as my understanding Cyber-attacks can originate from all diverse positions, consequently our safety procedures should be advanced.

**References**

1.Acunetix (2014) Danger: Open Ports – Trojan is as Trojan does, Available at: https://www.acunetix.com/blog/articles/danger-open-ports-trojan-trojan/ (Accessed: 6th July 2021).

2.Appcheck (2020) Common e-commerce vulnerabilities and how to remedy. Available at: https://appcheck-ng.com/common-ecommerce-vulnerabilities/# [Accessed 10 July 2021].

3.BBC (2021) Newspaper headlines: Hancock hangs on - but is it a 'Barnard Castle moment?', Available at: https://www.bbc.co.uk/news/blogs-the-papers-57619698 (Accessed: 29th June 2021).

4.Brian, K (2016) *Hikvision Backdoor Confirmed,*Available at: https://ipvm.com/reports/hikvision-cloudv (Accessed: 29th June 2021).

5.FutureEnTech (2020) 9 Default Security Threats in WordPress and How to Fix Them, Available at: https://futureentech.com/9-default-security-threats-wordpress-fix/# [Accessed: 6th July 2021].

6.Joseph, G (2021) *5 risks in protecting medical devices and how to meet them,*Available at: https://www.healthdatamanagement.com/list/5-risks-in-protecting-medical-devices-and-how-to-meet-them (Accessed: 14th May 2021).

7.NHS Digital (2020) The problem with medical devices Available from:

<https://digital.nhs.uk/cyber-and-data-security/guidance-and> assurance/guidance-on-protecting-medical-devices [Accessed 13 May 2021].

8.Sky News (2021) Ireland's health service shuts down IT systems over 'significant ransomware attack', Available at: https://news.sky.com/story/irelands-health-service-shuts-down-it-systems-over-significant-ransomware-attack-12305982 (Accessed: 14th May 2021).

9.Unfair Use of CCTV Data. Available from: <https://dataprotection.ie/en/pre-gdpr/case-studies> [Accessed 26 June 2021]