Reflection:
Collaborative Learning Discussion 1:

Background:

I have researched a scenario, which involves a medical checking system, with a few devices and one monitor, are connected and communicate with a Wi-Fi network.

Also, we need to analysis our peer's website if there is any vulnerability by using STRIDE and DREAD tools, with solutions.

Description:

I need to figure out any potential security threat of the system, including every individual device and the Wi-Fi network, and create posts for discussion

My peers have given me the peer response to enhance the context of my post. I will also learn new ideas from their posts.

Analysis:

I have created an initial post, which have pointed out the major threats and vulnerabilities, based on the scenario. I suggested to use MFA to minimise the potential threat of the brute attack.

In peer response, one of my peers has raised the usability of MFA, although it is very secured, but the balance between security and usability is also a challenge when deploying an effective cyber security solution. (Braz & Robert, 2006).

Evaluation:

As the technology become more advanced, more choices for enterprises and users when deploying the MFA.

Microsoft (2021) has proposed different ways and medias for the MFA, including SMS, Voice phone calls, authenticator app, software and hardware tokens, security key and her own Windows Hello technology. I can choose which authentication is easy and suitable for myself and other staffs.

During the discussion, my peer has mentioned about the usability and flexibility of MFA. Microsoft (2021) recommends Microsoft Authenticator app for MFA deployment. Authenticator app is the easiest for users to use, it also built-in different authentication methods, including passwordless, OATH codes and MFA push notifications.

With different choices of authentication method, MFA will become more flexible and easier to deploy. I also can choose which authentication method depends on the cost. For example, I can install authentication app and SMS for one time password as my authentication method, instead of hardware token and FIDO2 security key, which need to be purchased with extra cost.

To achieve the highest security protection with usability, passwordless is the best solution. Microsoft's Windows Hello (2021) is a biometric authentication, can be fingerprints or facial recognition. With addition of 2 more authentication methods, it is unnecessary to use any password for login, which can eliminate the brute force attack completely.

Collaborative Learning Discussion 2 and Team Project:

Background:

I need to inspect and find out any security vulnerability and threat of the web site which is created by another group of classmates.

Description:

I started from simple TCP/IP testing, discover the network related details of the web site, including nslookup, ping and tracert, etc. After that I need to do some Pen tests and discover any security threat of the web site.

Evaluation:

I found that the basic TCP/IP tools, such PING, TRACERT, NSLOOKUP in Windows CMD are not in-adequate for findings. I need to use Domaintools (2021) for more findings, including the location, main DNS servers, the owner of the server and their contacts, which are required to answer in the basic scanning activity.

Every teammate has created different results. Some of them have found that the delay of the route at some hops. In fact, some of them are not UK based. The geolocation and the distance between me and the website are also another issue of network performance.

As the technologies rise, the traditional mitigation solutions may not catch up with the latest hacking techniques. For example, a stateful firewall is not enough to defend a DDOS attack. Attack tools are easy to access, and attackers don't need an expert knowledge to do an attack. The common use of IoTs cause the threat of the largest DDoS attack in history, which can be up to 1Tbps DDOS level (Checkpoint, 2020).

Also, the widely use of Wi-Fi may cause different network security threat happens easily. Unlike a wired network, attackers can attack a Wi-Fi network at any point where has a signal; they will be able to capture, crack and connect the Wi-Fi network through the air. Once the credentials of the Wi-Fi network is cracked, the attacker can do everything inside it, from DDOS to data loss.

Although the Penetration Test can discover lots of security threats and vulnerabilities, but there are limitations. Cypress Data Press (2020) stated the limitations:

1. Pen Testing can only do for a period, which is limited.

2. The network may not allow us to do every testing, due to budget, policies, or resources.

3. A production network may not allow us to do a test which may exploit and crash the systems.

4. We may not have every skill set to do every test, especially a test aims to a specific application or system.

Even we have completed a Pen test, it does not mean we are away from every threat, there are cons of the Pen Test (Alice, 2021):

1. A Pen Test may crash servers and data loss during the testing process.
2. We need to trust the Pen Tester, but there is a risk of human error or any intention of the person, as he/she is invited to hack in our system for testing.
3. The result will be invalid and misleading if the test condition is unrealistic.

References

Braz, C. & Robert, J. M. (2006) Security and Usability: the Case of the User Authentication Methods. IHM 6: 199–203.

Microsoft (2021) *Secure access to resources with multifactor authentication,* Available at: *https://www.microsoft.com/en-gb/security/business/identity-access-management/mfa-multi-factor-authentication* (Accessed: 11 May 2021).

Microsoft (2021) *What authentication and verification methods are available in Azure Active Directory?,* Available at: *https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods* (Accessed: 12 May 2021).

Microsoft (2021) *Windows Hello,* Available at: *https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/windows-hello* (Accessed: 12 May 2021).

Domaintools (2021) *Whois Lookup,* Available at: *https://whois.domaintools.com/* (Accessed: 19th May 2021).

Checkpoint (2020) *DDOS ATTACKS ARE ON THE RISE. DDoS Protector DDoS Protection and Attack Mitigation* [Online]. Available at: *https://www.checkpoint.com/downloads/products/ddos-protector-appliance-datasheet.pdf* (Accessed: 25th May 2021).

Aaron, C (2020) *Major Limitations of Penetration Testing You Need to Know,* Available at: *https://www.cypressdatadefense.com/blog/limitations-of-penetration-testing/* (Accessed: 27th May 2021).

Alice, B (2021) *Pros and cons of penetration testing,* Available at: *https://www.itgovernance.eu/blog/en/pros-and-cons-of-penetration-testing* (Accessed: 27th May 2021).