During the collaborative discussion 1, I found the usability is another important factor of cyber security. I was surprised some classmates have raised the MFA is difficult to deploy, and the users will have difficulties as using password becomes their habit.

This prompted me to research if the MFA is so difficult to deploy and not usable. I found that Microsoft (2021) has developed many options for the MFA, not only traditional tokens. Various 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. The fact is, I can choose which authentication is easy and suitable for myself and other staffs.

To investigate the usability of MFA, if it is difficult for a user to use. I have tried to use the MFA on Microsoft Azure AD and 365. I have setup MFA by using SMS, Authenticator app, and Hello. The login process is step by step, which has clear instruction for a user. But a security admin may need to give a short course, or instruction to the staffs how to install the Authenticator app or read a text message and get the 5 digital OTP from SMS.

After these findings and realisations, I found a cyber security measure, not only secure but also has to be user friendly. I found it will be helpful for the users if provide basic training or short course, how to login with each authentication method, what they should be aware to, such as their mobile phone's security. As their mobile phones will play a role as a door key. After MFA has gone live. A proper end-user training will make the deployment easier and usable.

In the discussion, I also have discovered a classmate suggested by using static ARP to prevent Man-in-a-middle attack, besides deploying a passwordless MFA. I am confused how can we target so many MAC addresses on the allowed list of the routers and AP; also, how can we add or delete any guest users' devices dynamically. For example, doctor's private mobile phone or tablet, which may need to connect the medical Wi-Fi network in urgent. Also, there are many IoTs on the network. I concern how to deploy this technique effectively but at the same time, the network security measure is under managed.

This prompted me to read into how I can defend the man-of-the-middle attack effective, but make sure every trusted device can be connected to the network seamlessly, if there is any solution.

I found the Cisco Wireless Lan Controller (WLC) also able to do Dynamic ARP Inspection (DAI), which is a solution to stop any Man-in-the-middle attack. DAI is enabled on per-VLAN basis, the WLC records and compare ARP requests and responses, including the gratuitous ARPs (GARPs), only those clients with a valid MAC-IP mapping on the DHCP binding table will be able to continue the authentication process. Any ARP message and packet will be dropped and logged if there is no valid entry on the DHCP binding table. This will prevent any further ARP spoofing attack, but also eliminates any further network attack, such as SYNflood and DDOS, etc. (Cisco, 2021)

After the discussion, I realised ARP is another tool to defend the security of a network, besides of by using a secured authentication method, which can minimise the probability of password cracking by the attackers. A secured ARP measure is helpful for me to deploy one more secure layer against every potential attack by the hackers. ARP also can eliminate untrusted devices to access our network. I also can make an account, how many devices are connecting to my network, by check the DHCP bind table and logs of the WLC.

During the basic testing and design document session with our team, I found myself need a better understanding of the Pen test tools, despite of basic scanning tools such as ping, traceroute and nslookup. I was surprised at how other classmates and team members of my

group have used more advanced tool to do the testing, such as OWSAP and Nmap. I felt my knowledge of Pen Test and its tools are in-adequate.

This prompted me to research different tools I can use on the Pen test and their characteristics. I have done a clean install of Kali Linux (2021) OS on a notebook computer, which contains most of the tools for the Pen Test. The tools I have tested are Nmap, OWASP zap and what web. Furthermore, I also have installed Nessus manually for advanced Pen testing.

The testing and discovery of the Pen test tools helped me to prepare for the Pen test assignment in Unit 7. I also understand the specialisation of every tool, from Web server application and OS detection to the host location. I also found that OWASP zap and Nessus can do a comprehensive testing with detailed report.

After these trials, I found the Kali Linux is very helpful to do a deep, aggressive Pen test, I found that the tools have given much more detailed information than the 1st level scanning tools, such as ping, traceroute and nslookup.

I also did the PEN test with Nessus. Nessus able to detect over 100 zero-day vulnerabilities, able to figure out which threats have the highest priority, which is the top 10 reporting function, also I can install any necessary plugin for a live scan (Nessus, 2021).

Although Nessus is an effective PEN test software, with intelligence which able to detect different kinds of vulnerabilities, but it cannot display some of the basic host information. For example, the location of the host, any firewall can be detected. I need to rely on other web site and tools to complete these tests. For example, traceroute and IP2Location web site.

During the teamwork process, I was responsible on recommendations and conclusions, about the risk mitigation technically, also the PEN Testing on the major PEN test software, such as NESSUS and OWSAP. Other members of my team were responsible for management process. It would be better if I can participate more about the management and legal aspect, such as the security standards like GPDR, HIPAA, ECM, etc.

In the final seminar, the debate helped me to have a better understanding of IPv6. IPv6 not only can increase the pool of IP addresses, but also provides end-to-end data encryption (SOPHOS, 2021). It is much more secure and safer than IPv4, prevent any potential cyber-attack and data loss effectively, even there is no on-top encryption protocol. IPv6 gives protection to users who have no networking and cyber security knowledge.

References:

Microsoft (2021) How it works: Azure AD Multi-Factor Authentication, Available at: https://docs.microsoft.com/en-GB/azure/active-directory/authentication/concept-mfa-howitworks (Accessed: 28th May 2021).

Cisco (2021) Cisco Unified Wireless Network Architecture—Base Security Features. Enterprise Mobility 4.1 Design Guide [Online]. Available at: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper/ch4_Secu.html (Accessed: 13th May 2021).

OffSec Services Limited (2021) The Most Advanced Penetration Testing Distribution, Available at: https://www.kali.org/ (Accessed: 11th June 2021).

Tenable (2021) THE NESSUS FAMILY, Available at: https://www.tenable.com/products/nessus (Accessed: 22nd June 2021).

SOPHOS (2021) Why IPv6 Matters for Your Security, Available at: https://www.sophos.com/en-us/security-news-trends/security-trends/why-switch-to-ipv6.aspx (Accessed: 25th July 2021).