## Seminar 2: TCP/IP v ISO/OSI

Question:

Would the Internet we have today be much better if it was based on the ISO/ OSI 7-layer model rather than TCP/IP?

Answer:

The OSI and TCP/IP are reference models. The OSI has 7 layers whereas the TCP/IP has 5 layers. I think it may be better as the OSI model can be used in different type of networks, whereas the TCP/IP model depends on the protocols. Which means the TCP can only solve a specific problem whereas the OSI model can be implemented on various networks. The OSI model is also well documented compared to the TCP/IP model, which means that the OSI models can be easier to implement to a network as referring the simple documentation and guidance of it would be much more helpful possibly. On the other hand TCP/IP model has 5 layers which have accurate functionalities. Regarding protocols if we use OSI model we would be able to execute protocols that fit our specific requirements which is not possible with the TCP/IP model as it is difficult to make changes to the protocols because there is already a defined set of protocols for it.(Russell, 2006)

**Reference**

Russell, A., 2006. 'Rough Consensus and Running Code' and the Internet-OSI Standards War. *IEEE Annals of the History of Computing*, 28(3), pp.48-61.

**E portfolio content:**

This relates to the fourth module aim *Articulate the legal, social, ethical and professional issues faced by information security professionals* as if the information security professional needs to be aware of this question they can relate to this answer. This also relates to the first module aim *Identify and analyse security risks and vulnerabilities in IT network systems and determine appropriate methodologies, tools and techniques to manage and/or solve them* as I have identified the issues with the two models

## Unit 7-E portfolio Activity

**Question:**

What does the article teach you about carrying out vulnerability scans using Kali?

**Answer:**

I have learnt that Kali is pre-packaged with Linux Kernel, a group of essential utilities/applications and default settings. Many software’s can be installed on Kali. (Leroux, 2020) It has over six hundred tools to use. (Bhatt, 2018)

Kali is designed so that it is very quiet opposite to sending network packets at regular intervals such as through user applications or background services which is noisy. The reason why it is quiet is because this feature allows it to hide itself from showing on the network, and to protect itself from any potential attacks. (Leroux, 2020)

Kali can be used on many different computer systems, and be used on cell phones and tablets through the cloud which enables portable penetration testing. (Bhatt, 2018)

By deciding to use Kali we should realise that it is not simple and easy to use, it is a huge learning opportunity. If we would like something more beginner friendly then we can consider using for example Ubuntu derivative (Leroux, 2020)

**Question:**

What issues might you encounter?

**Answer:**

Adding extra repositories to download further software’s than what is already available could potentially break your system. It is a little complicated to use, you should know what you are doing otherwise complicated issues can occur

**Question:**

How would you overcome them?

**Answer**

Don’t further download software’s as there are already many available. You should research properly about the task you want to carry out and know well how to do it.

**Reference**

Leroux, S. (2020) The Kali Linux Review You Must Read Before You Start Using It. It's FOSS. Available from: <https://itsfoss.com/kali-linux-review/>

Bhatt, D. (2018) Modern Day Penetration Testing Distribution Open Source Platform - Kali Linux - Study Paper. *International Journal of Scientific & Technology Research* 7(4): 233-237. (2)

**Question:**

How do their results compare with your initial evaluation?

**Answer:**

The 6 open source security tools mentioned, Nmap, Metaploit, Wireshark, Aircack, John the Ripper, and Sql Map are easy to get started with, effective and well supported. The paper compared the 6 tools, and revealed Nmap being the most useful as it fit the criteria of being, flexible, powerful, easy, free, well documented, supported, acclaimed, popular, more than the other tools mentioned. If we compare this with the Kali Linux we can say that these tools are more beginner friendly resulting it in being popular whereas Kali linux are more for advanced expertise. Kali linux have over 600 different tools to use, even though this may seem useful it could be confusing. However, Nmap, as Kali is, is portable, and free, and even powerful. (Bhingardeve et al.,2018)

**Question:**

What do you think of their criteria?

**Answer**

The results of the 8 criteria used to judge the various tools were based on secondary data. However, I believe there should be more clarity for example what would seem easy for one person might not be easy for someone else.

**Reference**

Bhingardeve, N. & Franklin, S. (2018) A Comparison Study of Open Source Penetration Testing Tools. *International Journal of Trend in Scientific Research and Development* 2(4): 2595-2597.

**Question:**

Based on your evaluation in the previous session and the articles above, consider the recommendation given above:

What are the pros and cons of using Kali Linux vs. Nessus?

Has this changed your original evaluation score?

**Answer:**

Nessus is easier to use than Kali, Kali has variety of tools where some of them are easier to use than others. Regarding flexibility Kali has 100’s of tools available and can be used on different platforms as well, whereas Nessus scans for discovery of vulnerabilities. Majority of Kali’s tools are free as compared to Nessus which offers limited functionality in the free version. In terms of privacy Nessus is better at protection than Kali which relies on the penetration testers’ skills of avoiding any privacy issues.

In the original evaluation score in Seminar 3 evaluation exercise, we gave Kali the score of 3.4, and Nessus the score of 2.2. The above articles did not change my perception of the Kali evaluation score given in the seminar as compared to Nessus. However, the university’s’ decision of requiring us to use Kali can be a drawback because of our inexperience in using it however, the Msc course is all about learning so it is a good learning opportunity.

**Reference**

Tests, P., Tests, C., (2021). *Nessus VS OpenVAS Advantages and Disadvantages Explained*. [online] Hackingloops.com. Available at: <https://www.hackingloops.com/nessus-vs-openvas/> [Accessed 20 July 2021].

**E-portfolio content:**

This exercise meets the first module aim “*Identify and analyse security risks and vulnerabilities in IT network systems and determine appropriate methodologies, tools and techniques to manage and/or solve them”,* as we were required to analyse the tool, Kali Linux thoroughly, and also compare it to Nessus in order to find out the most appropriate tool and to also figure out if the university chose the right scan for us to carry out the scans.

This exercise also meets the second module aim “*Design and critically appraise computer programs and systems to produce solutions that help manage and audit risk and security issue*”, as we are identifying and analysing the tools to carry out the scans which is in a way carrying out a design of how we are going to solve the problem (which is of carrying out the scan)

This can also possibly relate to the fourth module aim “*Articulate the legal, social, ethical and professional issues faced by information security professionals*” as by using the tools to carry out scans we will face legal social ethical professional issues in a way for example we would need to ensure we are using the tools legally and not using the tools in order to hack a website. We are staying professional by doing this. If we do use the tools in a harmful way we understand that ethical issues can arise.

## Seminar 5

**Yahoo Data Breach 2014-** (Swinhoe, 2020).

**Question:**

What types of data were affected?

**Answer:**

3 billion User Account Information such as security question and answers

**Question:**

What happened?

**Answer:**

The hacking group used Yahoo’s user database which they stole and initially used account management tool but then turned to using recovery email addresses to identify the accounts which were more effective than the account management tool for them. They managed to generate cookies which gave the hackers free access to the users accounts without having to type in passwords

**Question**

Who was responsible?

**Answer:**

A phishing email was sent in 2014 to a company employee through which they were hacked

Were affected individuals notified?

It first started in 2014, but only in December 2016 did everyone get informed of the breach and users had to change their passwords

**Question**

What were the social, legal and ethical implications of the decisions made?

**Answer**

Yahoo initially did not inform anyone of the breach including the SEC, Investors and the public. The CEO was against the idea of asking the customers to change their passwords in case they lose the customers which is a huge ethical, social, legal issue. The customers when they were finally told about the breach did loose trust in the company. This data breach affected the reputation of the company by a hugely.

**Question**

If you had been the ISM for the organisation you selected what mitigations would you have put in place to stop any reoccurrences?

**Answer**

I would provide training to employees to inform them of security practises and what would happen if you click on phishing emails. I would install anti-phishing tools and firewall. Possibly inform everyone in the organisation to regularly change their password.

**Reference**

Swinhoe, D., (2020). The 15 Biggest Data Breaches Of The 21St Century. [online] CSO Online.

**Eportfolio Content:**

This exercise relates to the all module aims. As for the First and second module aim “*Identify and analyse security risks and vulnerabilities in IT network systems and determine appropriate methodologies, tools and techniques to manage and/or solve them”.and “Identify and analyse security risks and vulnerabilities in IT network systems and determine appropriate methodologies, tools and techniques to manage and/or solve them*”

I identified the data breach of Yahoo, and I gave my opinion of the mitigation actions if I was the ISM of the organisation.

As for the third module aim *“Gather and synthesise information from multiple sources (including internet security alerts & warning sites) to aid in the systematic analysis of security breaches and issues”.*

I used the source provided to answer the analysis of the security breach and issue of the Yahoo Data breach.

As for the fourth module aim “*Articulate the legal, social, ethical and professional issues faced by information security professionals*”,

I used the Yahoo data breach information to explain in all my answers about the legal social ethical and professional issues that occurred as a result of the Data breach.

## Final Seminar

**Question**

Debate: It is our belief that the future of the Internet is based on the MobilityFirst architecture

**Answer:**

Major issues in todays world of technology is When downloading videos, and it is required to move to one place and another the download does not run smoothly, When receiving calls on the internet if you are at home, and go to outside, the call does not smoothly switch over from the WIFI to 4g, performance wise the TCP/IP protocol is weak in terms of wireless network circumstances. MobilityFirst is a future internet architecture. It claims to give a solution to all these issues. It improves mobility as it separates names from network addresses, these names and network addresses are then referred to Globally Unique Identifies. It enhances security by preventing spoofing and hijacking, and it transforms the network-layer functionality. It is definitely required due to the increase of smart phones and the originally designed tethered hosts architecture and protocols have not changed much that can be and will be an issue for the end users, and will effect the long-term innovations of technology. (Venkataramani et al., 2014)

**Reference**

Venkataramani, A., Kurose, J., Raychaudhuri, D., Nagaraja, K., Mao, M. and Banerjee, S., (2014). MobilityFirst. *ACM SIGCOMM Computer Communication Review*, 44(3), pp.74-80.

**Eportfolio Content:**

This debate relates to all the learning outcomes. As for the first module aim, “Identify and analyse security risks and vulnerabilities in IT network systems and determine appropriate methodologies, tools and techniques to manage and/or solve them.” The risks of not moving to the mobillityfirst architecture is mentioned, and the solution recommended is of course mobilityfirst, this also relates to the second learning outcome too “Design and critically appraise computer programs and systems to produce solutions that help manage and audit risk and security issues”.

As for the third learning outcome “Gather and synthesise information from multiple sources (including internet security alerts & warning sites) to aid in the systematic analysis of security breaches and issues”

I have used this source which included some studies within it too.

As for the fourth learning outcome, “Articulate the legal, social, ethical and professional issues faced by information security professionals” are all mentioned in my answer.