Niru’s Points

Thank you Abaraajith. So, I will now be talking about the vulnerabilities we have encountered during the assessment.

I would like to highlight the fact that there is no network set up within the organization and all the employees or members of the company work from home. The cases I will be presenting may seem very simple, but they can still cause **huge problems** to the company.

1. The **first problem** we encountered was the communication line. Email and instant messaging apps were the main tools that were used in this project. These tools are cost effective and simple to use, but there are not so good when it comes to information security. There have been many instances of information leaks and tampering through these platforms.
   1. There are numerous issues with Email, some of these are **malware, spams, phishing** and **attackers with not so good intentions.**
   2. And when it comes to IM apps like WhatsApp the threats are **viruses and worms over IM, identity theft/authentication spoofing, firewall tunneling and spim.**
2. **The next problem was with the complexity of passwords that have been set by the users. The only security measure they have set up is 4-digit pin number. These days it is very easy to find software that can be used to hack into any unauthorized systems. Also, these types of pins are used in more than one instance. But even through social engineering the attacker can easily guess the pins. Eg: One of the employees had a pin that was used for the PC login was the same pin used in the mobile. (Can skip this if you want)**
3. **The absence of an anti-virus guards causes numerous problems. It is like keeping the door of your wide open for intruders to enter and steal things from your house. Similarly, viruses enter the PCs and cause numerous problems like slowing down the computer, reformatting the hard disk, crashing the OS etc.**
4. **There is no proper networks setup. Files are stored locally in each members’ PC. By using the public network to send their files and receive files there is a high probability that files can be intercepted during transmission. Without a private network the whole system is vulnerable to many outside attacks.**
5. **The company maintains a level of availability using cloud storage services like Google drive to maintain sync of file management like updating, deleting and adding. But some problems with cloud storage is that there is no control over data, meaning that the third-party service providers handling of data is beyond the company’s control. Data leakage and snooping are also some of the problems caused by cloud storage.**

**With that said some of the cases have been tested for exploitation and it will be explained by Dhanurjan.**

[**https://www.networkworld.com/article/2323048/top-5-im-security-risks.html**](https://www.networkworld.com/article/2323048/top-5-im-security-risks.html)

[**http://library.ahima.org/doc?oid=99319**](http://library.ahima.org/doc?oid=99319)

[**https://www.pewresearch.org/internet/2017/01/26/2-password-management-and-mobile-security/**](https://www.pewresearch.org/internet/2017/01/26/2-password-management-and-mobile-security/)

[**https://solutionsreview.com/data-storage/pros-and-cons-is-cloud-storage-right-for-you/**](https://solutionsreview.com/data-storage/pros-and-cons-is-cloud-storage-right-for-you/)

[**https://www.promax.com/blog/10-advantages-and-disadvantages-of-cloud-storage**](https://www.promax.com/blog/10-advantages-and-disadvantages-of-cloud-storage)