A7010E Homework 3

Nico Ferrari (nicfer-0@student.ltu.se)

September 28, 2020

1. The HiM enterprise that hired you in the last assignment is now looking for upgrading (not updating!) the operating systems within the whole company. HiM allows Bring Your Own Device (BYOD) model where employees can use their own computers from homes or from inside the company location.The company sends you a request to offer advice and guidelines on the upgrading process by preparing the following points

---

Nowdays, chosing an operating system takes into account several factors, including: security, interface, recovery, costs, disk space etc. The most common OSs in for computer clients, are Linux-based Operating Systems, Windows, MacOS. Here a brief comparisin between the different OSs:

Linux based operating systems are based on the Linux kernel. Linux is the core of the operating systems and, according to some definitions of Operating System, can be defined as one itself. Linux is free and open-source so anyone can have access to the source code, modify it, analyze and contribute to the development. This allows to have contributors around the world which audit the software packages and can improve performances and security issues, which is something not possible with proprietary software. Various distributions have been developed based on this, for example Ubuntu. Most of the distributions available are community-driven project, some times even from a single person leading to maintainability problems and none of the distributions is as spread as Windows. During the last decades, most of the Linux distribution started to become more and more user friendly, with easy to understand GUIs and simple and guided installation processes. Nevertheless, the Linux terminal is a fundamental part of the user experience in most of the cases. In fact, some applications can be installed by CLI, using the terminal emulator. Through CLI it is possible to have complete power over the OS, having everything accessible (if the user has the right privileges) and making easier to "break" things in the OS and making it hard to repair. Support comes via huge communities online and online searches. With the years the GUI has improved and it is becoming easier to customize. In fact, thanks to the complete controls over the system, the user is able to personalize it in every aspect. Multiple Desktop Environments available and the users can customize them according to their needs. Another aspect which differentiate Linux based OSs is their stability. Due to the openness of its software and the lower amount of users, the amount of cyberattacks agains Linux OSs is lower. Some Linux distributions are differentiated by addressing security concerns, designed with the goal of mitigating security threats and/or focusing on the privacy and anonymity of the users. Moreover, by default, administrator privileges are not available to the users, having a better privileges model compared to other OS like Windows where users, by default, pretty much have access to everything on the system.

Windows is developed by Microsoft and is a closed-source OS. Each Windows OS has different versions which try to satisfy the needs of the different types of user. In order to install Windows, users need a license with a price which differs between the different versions. Windows tries to be as user friendly as possible, including an easy and guided installation process, a user-oriented design and an incredible wide range of software available. In fact windows is on the market since several years and is in most of the cases the default operating system on computers. The users then got used to this environment and the other Microsoft and/or Windows only products, creating a kind of ecosystem. Due to its widespread and target, which often is users without an in depth IT-knowledge, it is more subject to cyberattacks. Since the OS is not open source, there is not such a huge community contributing to the security issues analysis as big as in Linux based systems. Users usually have administrator privileges by default and this can bring to security problems related to user's errors. Support comes as well as Linux on forums/websites but it is possible to have paid support as well.

MacOS is the OS developed by Apple for Macintoshes. In fact, while Windows and Linux can run on thousands of different machines from hundreds of different vendors, MacOS is distributed by Apple to run solely on Apple hardware. Also MacOS is extremely user friendly with a lot of free application available by default and many unique features. Apple has created a great ecosystem among the Macintoshes, allowing great functionalities among differnt devices (i.e. sharing clipboards or files between devices with IOS and MacBooks with MacOS). MacOS is based on Unix, and it is possible to control the system by CLI. Systems based on MacOS are less affected by cyberattacks compared with Windows ones, adopting the concept of security through obscurity. In fact, MacOS keeps the inner parts of the system proprietary, keeping them secrets from the hackers. Its security still remains not comparable with the one offered by the Linux systems, which result the most secure systems.

In order to keep the system secure, becomes fundamental to install the software updates. In fact, security patches must be installed as soon as possible in order to avoid attacks based on those vulnerabilities. Another important aspect is to check software which is going to be installed. Many times, attackers make install software on the machine of an user. In order to avoid this kind of problems is necessary to scan the files in the computer, received electronically, downloaded,.. for viruses. There are different antivirus available on the market and usually made to protect from attacks over the network and/or viruses. This kind of software is usually proprietary, and I think would be necessary to ask ourselves : "should I trust them?". This is a question which can be referred also to any other kind of proprietary software. In fact we are not able to check the code for vulnerabilities or malicious behaviours. In order to be protect the user from the "outside", user must control also the open ports on the computer and close the unused ones, to avoid data breach or different attacks. The password must follow some policies regarding length and complexity and not being stored in clear anywhere. When possible it is better to avoid passwords as only authentication method for the different services.

During the last years and especially during the last period, BYOD is exploding, allowing employees to work using their own devices and from distance. In order to minimize as much as possible the security threads possible while using the employee's devices from distance, security policies must be applied. First of all, all documents related to work present on the device must be encrypted. In fact, in case the user lose the device used for work or it gets stolen, the documents must be not accessible from unauthorized third parties. The company data belong to the company, even if they are on a private device, meaning that these data needs to be accessible. The company data must be transferred only through the company's mandate application in order to mitigate data breaches. Fundamentals are policies to apply when a person leaves the company, like the data wipe procedure. More over the user must apply the security patches in order to mitigate the attacks which exploit software vulnerabilities. Beside policies, which sometimes are not followed and are heavily affected by the human factor, a secure infrastructure must be established in order to protect the company data when BYOD is enabled. In order to mitigate the security threads, I propose the following structure:

- In the company there is a server acting as a **identity and access manager**. The entity manager will establish the policies and the credentials of each user able to login into the workstations connected to the internal network. In this way, the credentials will be stored in the server, and not into each workstation in the network. For this purpose there are services like Active Directory (for Windows) and FreeIPA (UNIX like systems and Windows). The authentication must support MultiFactor Authentication in order to not rely just on passwords. If the budget allows it, secure keys are preferred (i.e. Yubikey).
- In order to access from outside and establishing a secure connection, a **VPN server** must be created in the company. The VPN server should allow multi factor authentication as well, for the same reason provided before. OpenVPN could be an option and can be configured to use the same credentials used to access to the personal account.
- The user must install a **VPN client** and a **Desktop Sharing application** (for example, RealVNC or, otherwise, Windows has already included the Remote Desktop Connection software, which allows to connect to an IP address and share the desktop) in order to remotely work on his workspace.

In this way, installing a simple VPN client and a desktop sharing application , the user will be able to work from remote on his workspace and the files do not need to be saved on the personal device. All the information will be now encrypted using two factor authentication. Moreover, this tools are not dependant from the platform and they are available for all the major operating systems. Some policies can be now implemented making sure that the user cannot share the company information (i.e. taking pictures of sensible data, leaving session open when he is not working...).

2. Please prepare a 5-10 minutes recorded demonstration on biometric technologies. The demonstration should be technical, so please do not present research papers

3. What is your own reflection on the entire week of the course?

Interesting results from the research for this homework. I think that the instructions where not clear, leaving different possible interpretations. Anyway, continuing to be satisfied for this course.