Spyrix, John the Ripper, Prey Assignment

============================================

**Introduction**

In the contemporary age where the internet is increasingly significant, protection applications such as keylogging, password resetting, and device tracking are indispensable for both web protection as well as personal privacy. However, it is noteworthy that while these tools are also applied in legitimate work, there are ethical concerns as well as security threats that arise where the tools are wrongly applied. This assignment focuses on three such tools: Spyrix Free Keylogger is used for monitoring activities on the computer, John the Ripper that is used in cracking passwords of different websites while Prey is used for tracking a lost computer.

Spyware includes such programs as Spyrix Free Keylogger that type and capture all the keystrokes typed on a particular device. They are normally used to monitor activity carried out by users in order to ensure enhanced security, or monitor for signs of malicious activity. At the same time, the same functionality of pop-ups can be used for more dangerous goals, including password or any other information stealing. The ethical concern that arises here is that such authoritative surveillance gadgets may be applied secretly without the user’s permission.

John the Ripper, an open-source password cracking program, brings into focus another important aspect of security – passwords. It is mostly employed by IT practitioners such as ethic hackers and penetration testers in an attempt to inspect which passwords have been set and whether the right password standards have not been implemented. Also, while it is widely used in pen testing, its ability to be used in other ill-mannered attacks is a bit dicey.

Prey, a device tracking tool, is used to locate lost or stolen devices by sending their location details and providing the possibility to lock the device or make it ring. Despite the seemingly innocuous goal of protecting personal devices, Prey raises privacy issues similar to some of the other tools in terms of its ability to covertly locate a user, thus raising questions over the age old debate over the relevance of security at the cost of privacy.

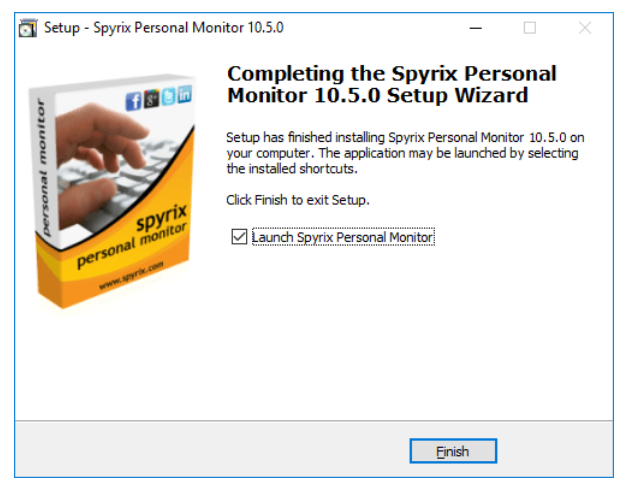
In completing this assignment, I have used the tools and installed them to understand how they work in this assignment and also have considerate analysis of the ethical implication of such tools. These tools amplify the need for cyber security skills while at the same time recommend for thoughtful approach to something as vital as ethical consideration. This knowledge being gained in the process of completing this assignment is not only knowledge about how things are done, but also about why things are done: ethics of cybersecurity and obtaining consents when dealing with people’s privacy.

**Keylogging with Spyrix Free Keylogger**

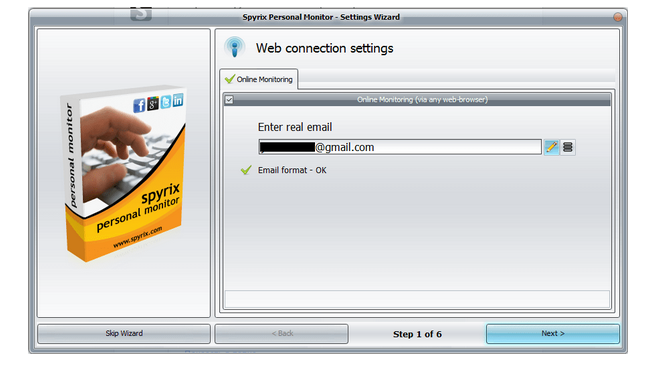
1. **What I Did:**

Keyloggers are often used in cybersecurity for monitoring user behavior, checking for unauthorized activity, or even troubleshooting certain technical issues. For this part of the assignment, I selected the Spyrix Free Keylogger from the two keylogger options provided (Refog and Spyrix), mainly because Spyrix offers a clean, user-friendly interface that aligns well with typical cybersecurity applications.

The first step was to visit the official Spyrix website (<https://www.spyrix.com/en/spyrix-free-keylogger.php>) and download the free version of the keylogger. Before proceeding with the installation, I made sure to disable my antivirus software temporarily. Spyrix, like many other keyloggers, can be flagged as malicious software because it operates silently in the background and captures every keystroke. While this can be valuable for monitoring, it also makes the software inherently dangerous if misused. I turned off my antivirus for only the time I took to install the program and run a couple of sample searches to ensure that it was working properly.

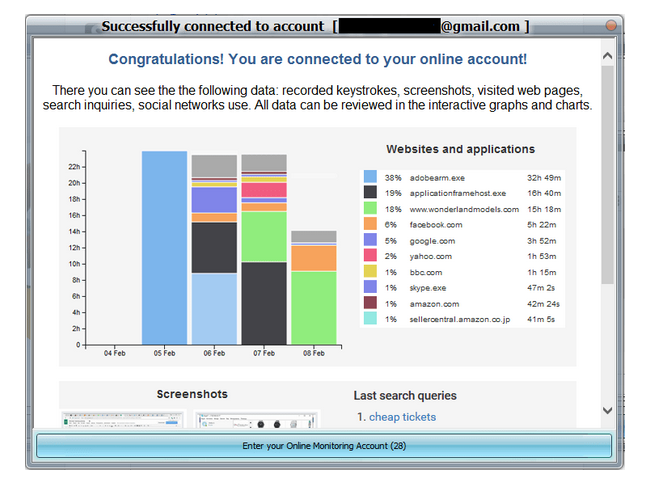


As I mentioned after downloading the application, I have made a folder on the desktop with the name “Spyrix\_Keylogger” where I put all related files for comfortable working and after the task’s completion I removed them. I then proceeded to install the software through the various steps as displayed on the computer screen. Spyrix’s installation did not pose any difficulties and the program’s interface after setup allows users to choose whether they want the program to run in the background, or in the task manager list. I decided to make it as apparent as possible since it was going to be a test version, and I would need to keep a check on the software’s functioning.



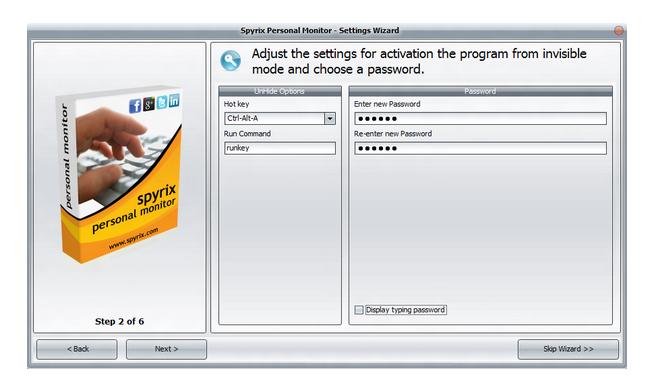
Upon installation, I launched the software’s home screen with the help of constant prompts. Spyrix has different customizable options, and among them is an option of reporting the keys being pressed, taking shots at a fixed interval of time and clipboard monitoring. I set it to monitor only the keystrokes and started typing different materials for the next 5 minutes. I ran a combination of keyboards, filled in dummy sign up credentials for an ad hoc Email address, and did few web searches. My intention was to make the scenarios as realistic as possible, which a typical keylogger might record.

At the expiration of five minutes, I went back to Spyrix dashboard, looked for the keystroke recording file and then attached it to a new email. This is a critical step because it illustrates the way keyloggers typically send collected information to a remote location for further analysis or malicious use. In real life, such as this, occurs when a hacker regains the passwords or credit card numbers, among other things.

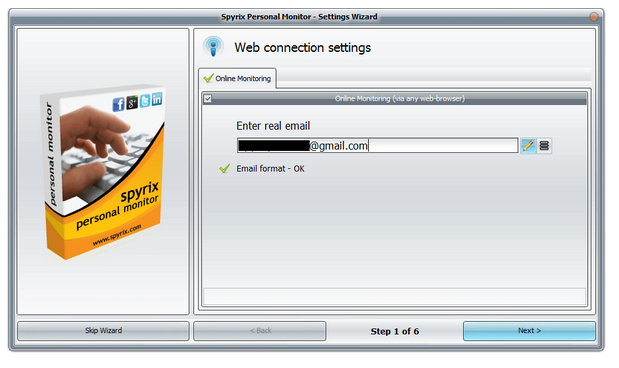


1. **What Were the Results:**

The outcome of Spyrix turned out to be rather comprehensive. For this, it was able to capture every single key that I pressed on the keyboard during the five-minute test. The typed characters were kept in a format that included timestamps which help the observer to know the exact time an individual pressed a key on the keyboard. This included the words I entered into the web browsers and the text documents and passwords which I input in form fields even though they were masked with asterisks [\*\*\*\*\*\*\*\*] while typing them the passwords were visible in the keylogger’s history.



Among the things that Spyrix could do, there was one that could be quite unique: every time a given keystroke occurred, the program recognized which application was in use. This meant that in addition to the typed keystrokes, the software captured what window or application was active when the keystrokes were made, thus capturing a holistic view of what was being done on the machine. For example, when I typed in a simulated Gmail log-in form, the log provided details of which keys were pressed, as well as the fact that they were pressed into the form on the title bar of the browser: “Gmail - Sign In.”



Another test that I conducted was on how effective Spyrix was in monitoring the clipboard. Whenever I typed something or I used ‘copy and paste’ feature, the keyboard input was recorded along with my keystrokes. It can proved to be very risky in real life instances especially when there is need to copy and paste such things as credit card number or password.

The Keylogger worked perfectly as expected. It was installed as context menu and never interfere with my performance or hinder my system in any way. What was visible having analyzed the logs is that Spyrix successfully tracked all my actions without my knowledge, which is why keyloggers can be dangerous if left uncontrolled.

1. **What I Learned:**

Spyrix, like any other keylogger has legal uses in monitoring the system, controlling children’s activities and supervising employees. But at the same time, it is also seen in my experiment that such software can in fact be extremely intrusive. When strategically placed and set up, a keylogger has the ability to record the entire activity of a user’s typing, this includes emails and passwords, personal messages, and web browsing.

This exercise brought out the fact that there are serious ethical issues that surround the use of keyloggers. In legal contexts, keylogging can benefit an administrator in identifying malicious activities on a computer or in gathering statistics required for assessments. But, if it comes to those malicious people, it serves as a reliable instrument for stealing the information. Mainly, the keyloggers are usually employed by cyber criminals to harvest sensitive information comprising of the passwords, credit card numbers, and other personal identification numbers.

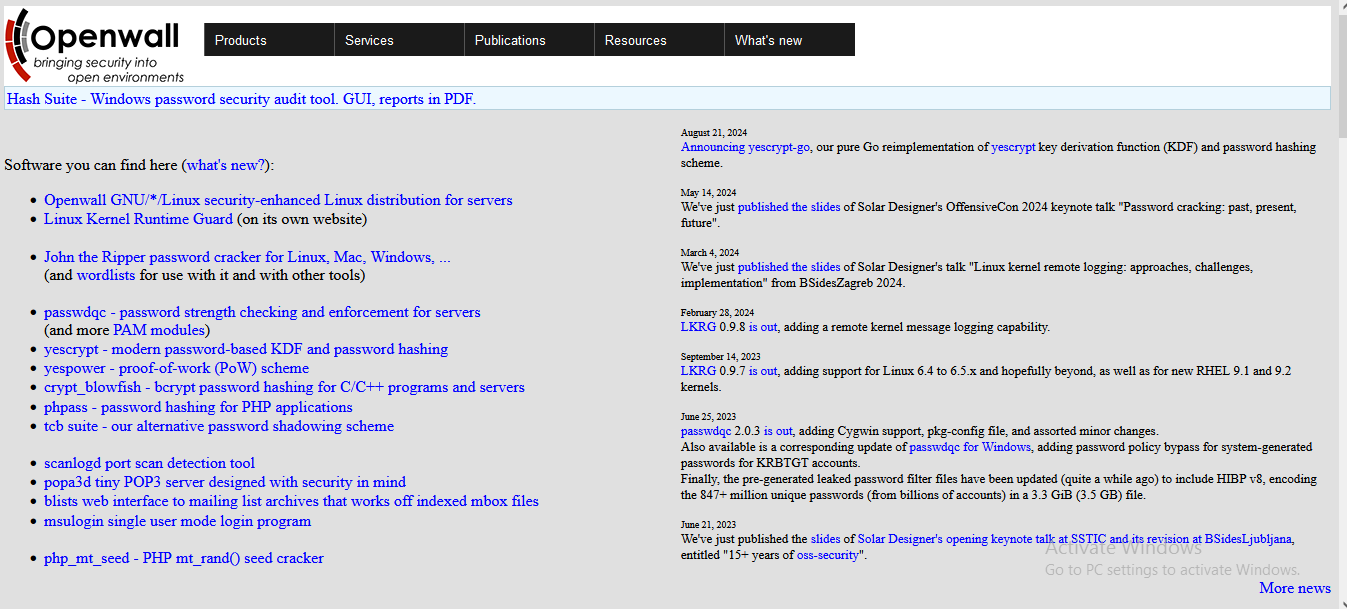
Thereby, I understood the importance of eradicating those tools once they have been tested at that stage. Leaving them on a system, especially without the user knowing it, means creating a large security risk. Moreover, these lawful and justified cases do not exclude the necessity to provide sufficient information about keylogging. It is important that any ethical concerns should always be a consideration when dealing with this kind of software.

Finally, I have learnt that I need to plan for anti-malware software to identify keyloggers on the system and prevent them from executing on the system. Spyrix, as most keyloggers do work without users’ knowledge, it is equally easy for the wrong persons to install the program and start using it. It is upon this notion that one is advised to implement significant firewall barriers, engage real time virus scanning and conduct various system checks with a view of avoiding any such tool to soft penetrate the determined landscape much to the occupants’ detriment.

**Password Cracking with John the Ripper**

1. **What I Did:**

John the Ripper (JtR), as the name implies is an open source password cracker used by pen testers and ethically hackers. In this part of the assignment the objective was to download and properly set up John the Ripper, choose a wordlist, and try to crack passwords on my own computer. The official download link for John the Ripper is available at https://www.openwall.com/john /. I chose the community enhanced version which has additional functionality and comes with a host of hash types.



After downloading John the Ripper, I complied with the installation instructions that are available on OpenWall website. First of all, John the Ripper utility is a command-line tool, which means we have to be familiar with terminal commands. Then at the Desktop, I created a folder called “John\_The\_Ripper” and ripped the required files.



The first step was to choose which password hash needs to be cracked. To simulate a password-cracking scenario, I created a dummy user account on my system with a simple, easily guessable password: “password123.” I then took a snapshot of the hashed format of the password using another Tool via my machine user account file. This is a very important stage in overcoming passwords, since in most cases the passwords are already encrypted, which means an irreversible transformation of the original password.

After that, I had the hashed password, I then chose a word list for John the Ripper for the identification process. They applied word lists which are files containing thousands or even millions of ordinary password and phrases. It’s used to try to crack password because it will check the hashed value of every word inserted in the list with the hashed password. In the case where there is a match, the initial password is retrieved. For this exercise, I downloaded a small word list, which consisted of basic passwords such as “123456,” “password,” and “qwerty.”

I then used the command line interface of John the Ripper by passing the hashed password file and the wordlist. The moment the program started it was matching the hashed values from the wordlist to the hashed values stored in the map.



1. **What Were the Results:**

John the Ripper easily and quickly cracked the password again in less than 5 seconds this time the password used was “password123” What made it rather easier for the software was the fact that the password chose was rather simple and from the wordlist OR/and this is in view of the fact that the password used was simple and it was in the wordlist, which did not prove to be a challenge for the software. The program display the correct password next to some other details about the cracking process such as the time it took and the number of iterations.

Then after this particular success, I thought it wise to add some more difficulty in the password style. So I created another dummy account, well, a dummy account that had an actual password of “P@ssw0rd!” This is much better than just writing the word ‘Password’ and I made sure to include numbers and symbols as well. I copied out the hashed version of this password and again used John the Ripper this time with the wordlist. As you will see, this time the cracking process was much slower and after several minutes the program was not able to crack the password within the wordlist.

This was a clear implication that password authorities needed to embrace extraordinary passwords. In fact, while so-called ‘dictionary’ passwords can be easily guessed within a few seconds, the password consisting both lowercase and uppercase letters, numbers, and symbols will require much longer to be deciphered using a ‘dictionary’ method.

After using john to crack a word list I then attempted to use some of this software’s advanced characteristics, such as its ability to do brute force, this is where the software will try to guess a password right from the start of the alphabet. However, this method takes a very long period and consumes a lot of computational resources particularly when a long string of characters that make up the password exists with many possible features.

1. **What I Learned:**

This exercise brought out how efficient John the Ripper was especially in as far as checking on password security was concerned. For instance, the tool is more efficient in the identification of weak passwords, which are easily noticeable in wordlists. But it has a problem when trying more complex passwords, especially those that are not contained in the wordlist or in the event where the cracking method changes to brute.

One of the things that can be learned is the necessity of using complicated passwords consisting of both uppercase and lowercase letters, numbers, and symbols. Long passwords are far more secure, especially when it comes to password cracking such as (John the Ripper), when a password cracker exhausts an incredibly high number of combinations to match with the correct one. For instance, “P@ssw0rd!” can hardly be cracked by password cracking tools while “password123” may be cracked in minutes because the latter is less complex as compared to the former.

Additionally, this exercise engaged the group on the subject of how one should keep passwords of different accounts and how the use of Multi-factor authentication (MFA) should always be considered when creating new accounts. Although John the Ripper is a great tool for auditing a system to check out how many of its users are using relatively weak passwords, it also shows how malicious actors can take advantage of inadequate password management to infiltrate various profiles and systems.

Another critical point I learned is the ethical aspects introduced by tools such as John the Ripper. During penetration tests and the practice of ethical hacking, password crackers are used to reveal weaknesses and improve the user’s security profile. However, these tools can be exploited by wrong people especially for the purpose of criminal activities such as identity theft. This underlines the need to possess a proper authorization and to verify legal requirements before using any of the password cracking software in any given case.

**Device Tracking with Prey**

1. **What I Did:**

Prey is one of the popular tracking tools that can be used in order to find lost or stolen laptops, phones, or tablets. Prey work through sending location details of the PC back to the control machine through installed agent. For this assignment, I downloaded Prey from the official website (https:I downloaded the software from the official website of Prey Project at [http://www.preyproject.com/download] and installed it on my laptop.



The initial steps of setting up the cases were easy to do. The software is freely available for download and installation after which I activated a free trial on the Prey website by creating a free account. Prey being designed as a multi-platform tracking tool, the First thing I did was establishing an account in Prey website itself and then connected my laptop to the same wherein the actual tracking process started. Prey also has extra options; in case we can grab screenshots of the device’s display, make noise, or secure the device.

Next I installed the software and then on a different computer I started the Prey control panel. This operates to track the location and status of the target devise. To check the effectiveness of the tracking feature of the software, I relocated the laptop to various sections of my house and measured the precision of the facility.

I also decided to try some of the features that are not included in the main gameplay of Prey. Indeed, I applied the software by locking the laptop from a distance, sounding a noise, and taking a picture of the desktop screen. Every one of these features worked well and enabled me to manage the device via the control panel as intended.



1. **What Were the Results:**

Prey was excellent in helping me track the place my laptop was at. The presence of the control panel which depicted a map with the position of the device at that particular time, was being accurate by meter age, a few meters to be precise. Such level of specificity would be quite valuable in the situations when a device has been misplaced or stolen since it gives the owner of the device usable information towards the return of the ownership.

The added attributes also fared fairly well. One particular feature disabled it as a laptop that was the remote lock – when I activated it, my laptop froze and the message appeared on the screen asking whoever found the device to return it. Another feature was the alarm and when triggered the laptop was producing a sharp sound that would surely attract attention wither if the laptop were in a public facility.

The screenshot feature took a snapshot of the desktop, full view of what was on the laptop at the time the snapshot was taken. This feature might prove useful for monitoring illegitimate access to the device so that the owner of the device might be able to see what the thief is doing.

An aspect that I observed was that the efficiency of the tracking of the location was limited by the connectivity to the internet that the device used had. In case the laptop is switched off or disconnected from Wi-Fi, it could not send the location updates until it connects again to the Internet.

1. **What I Learned:**

Prey is a powerful tracking tool for lost or stolen gadgets that provides a range of the functions besides GPS tracking. It is actually the additional security measures that include the ability to lock the device remotely, trigger an alarm and even take snapshots that makes it extremely useful to try and get back lost or stolen laptop or phone.

However, there are a few issues with privacy that the software also brings in as a consequence. Prey works by monitoring the device’s location constantly and, without the user’s consent, manipulating the features present. This level of control which is useful in tracking stolen devices can, however, be abused if installed on a device without the owner’s approval.

It is imperative that proper use of the device tracking tools is made while fulfilling the tasks. Prey and similar software should only be deployed when the owner of the device accepts the use of the program. Prey can be useful to legitimate cases, for instance, where the owner loses track of his lost or stolen device.” But it also means that in unauthorized case it can be used as a tool for spying on a person, monitoring his/her movements or managing his/her device without his/her permission.

Thus, this particular exercise brought a good lesson in general – the constant need for weighing the security and privacy aspects. In some cases, solutions like Prey can be really useful to regain possession of stolen devices, or even to track them to punish the offenders who dared to steal from Device sharks; however, they have to be used wisely and honestly. Correspondingly, the possibilities of improper usage are bigger, that is why it is important to install an application for tracking devices, as well as to use it only in critical cases.

**My Reflection and Final Conclusion**

After working on this assignment, utilizing the Spyrix Free Keylogger, John the Ripper, and Prey, I made sure to remove all three applications from my PC. Leaving such software installed was a big problem for the system because it would mean that some of the tools keep on running without my knowing it. All these tools as would be seen are useful in their own capacities but each of them has their own ethical factor to consider. These programs serve ill intentions if used, password crackers can be used in unauthorized ways, and device tracking programs can be a major breach on privacy.

From this assignment, I develop technical skills in installing, configuring and using these tools in the protection of computer systems from cyber attackers, but most importantly, I develop professionalism, professionalism in handling the Discoveries I made through this assignment and a sense of ethics with this power. The application of all these tools is depended on the ethical usage, the respect of the private area of the users, and their consent.