Hello Everyone! In this exercise, you will learn What Are Key loggers & how to prevent ourselves from Key loggers.

What is Key logger ?

- Key logger is a malicious program that is specifically designed to monitor and log the keystrokes made by the user on their keyboards.
- It is a form of spyware program used by cybercriminals to fetch sensitive information like banking details, login credentials of social media accounts, credit card number, etc.
- A key logger can monitor and log such information and send those to the cybercriminal behind it. A key logger can not only monitor the keystrokes, but it can also take note of every click and touch on your system.

So what information is captured by Key loggers?

When key loggers run, they track every keystroke entered and save the data in a file. Hackers can access this file later, or the key logger software can automatically email the file to the hacker. Some key loggers, which are called screen recorders, can capture your full screen at random intervals as well. Key loggers can recognize patterns in keystrokes to make it easier to identify sensitive information. If a hacker is looking for password information, they can program the key logger to monitor for a particular keystroke, such as the at sign (@). Then, the software only notifies them when you are likely entering password credentials alongside an email username. This technique helps malicious users quickly

identify sensitive information without needing to sift through all your keystroke data.

Let's see what are the dangers of Key logger?

- Hackers can steal credit card information and make unauthorized purchases.
- Malicious users can log in to your email accounts and steal information or scam your contacts.
- Hackers can log in to your bank accounts and transfer money out.
- Malicious users can access your company's network and steal confidential information.

Here are various ways Key loggers are infecting Devices:

- Visiting and downloading software from untrustworthy, suspicious sites would create a doorway for malicious programs like Key loggers.
- Clicking on malicious links of text messages or unknown emails can trigger the download of Key logger in the background.
- Cybercriminals use social engineering tricks to force users to install the Keylogger into their devices. They would attract the users by offering too good to be true proposals like getting a paid software for free by clicking a particular link or pop-up.
- Downloading the applications, movies, music, etc., from torrent sites might initiate the Key logger installation. Torrents are one of the most common sources of malware infections.

There are two types of Keyloggers:

- **Hardware:** Hardware keyloggers are physical devices that record every keystroke. Cybercriminals can disguise them in the computer cabling or in a USB adapter, making it hard for the victim to detect. However, because you need physical access to the device to install a hardware keylogger, it isn't as commonly used in cyberattacks.
- **Software:** Software keyloggers don't require physical access to a device. Instead, users download software keyloggers onto the device. A user might download a software keylogger intentionally or inadvertently along with malware.

Here are some of the attack indicators, if your device has been targeted by Keyloggers You may see the following:

- You may notice that your computer is unusually slow or unstable. This is usually a sign of malicious software running in the background.
- You might also find that your keyboard is typing the wrong characters or keys are not working properly.
- Another sign is if you notice any strange software installed on your device that you don't remember downloading.
- You could also receive suspicious pop-up windows on your screen that you don't recognize.
- You might notice that your online accounts have been accessed without your knowledge, which could be a sign of key loggers or another compromise. In this Exercise, Hacker will execute Keylogger in Victim device and hence

it will store all the keystrokes types by victim in plain text format.

Some of prevention tips from such type of attacks are:
Remember that any file you receive on any digital device could be embedded with keylogger software. In turn, pay close attention to the sender's address, and only open files from those you can trust. A strong antivirus program should be scanning all files for viruses before opening them to help prevent key loggers and other malware. Implement Multifactor Authentication. The whole point of enabling multi-factor authentication (MFA) is to strengthen and enhance user logins. Doing this will add multiple steps within the login process, increasing security and making it difficult for any malicious agent to gain entry to your accounts without your permission. Use software or on-screen keyboards for inputting your banking details wherever possible. If you do have a keylogger, it won't be able to recognize your sensitive information. Most computers come with an onscreen keyboard option already installed, which you'll find in your list of program accessories in the Start menu. Set up a Firewall and always keep your devices up to date.

Thank You