**DAY-12**

**Anti keyloggers:**

Identify whether there is a keylogger in a system or not

Two types:

1. Identify and delete keyloggers

2. Identify and encrypt the data and block the data collection

One of the anti keylogger tool is KeyScramble by qfxsoftware.com

Fea keylogger🡪chrome browser extension

🡪This can bypass anti keylogger

🡪It will grab the text you type in the website input forms

Browser extensions are called as **premium business programs**

🡪Process viewer by Microsoft is used to view all running processes. Helps in identifying any malicious processes or key loggers

🡪This is available to download

Execute processexp64.exe

Click options

Click virustotal.com and check virustotal.com and submit unknown executables

Use virustotal.com to scan for viruses in downloaded files

**Clearing tracks/logs:**

Last phase of ethical hacking

The hacker will delete/remove all the logs that are recorded the moment hacker compromised the system in order not to get detected

How to clear the application logs in windows os:

1. Event viewer accessing

Clear logs in event viewer

2. Auditpol

To access auditpol:

cmd(admin)🡪 auditpol /?

cmd(admin)🡪 auditpol /get /category:\*

cmd(admin)🡪auditpol /clear

cmd(admin)🡪auditpol /set /category: “logon/logoff”

/success:enable [to set/enable auditing]

For linux:

The logs are created and stored in folder /etc/var/logs

The logs in linux os are stored in plain text and are text files, so the hacker can remove logs in linux also.

Linux logs are not encrypted, so it is easy to delete or modify logs