Task 8

Develop ethical hacking tools using Python

This task gives a formal introduction to ethical hacking. The course provided in this task gives insights into ethical hacking.

The term ethical hacking, more commonly referred to as White Hat in the industry today, is a skill that ranks among the top 3 skills. Organizations and corporations have to ensure that their infrastructure and systems are secured and that breaches/attacks are kept at bay. Ethical Hacking takes you from the starting point through the finishing point of everything you need to know about this domain and getting started on the journey to master it.

This free introduction to ethical hacking course gave me an insight and its functions under the top 3 domains in the industry today. This course gives you the scoop into what are the foundations, processes, domains and outcomes of Ethical Hacking. In every domain of ethical hacking, I understood the domain, its common attacks, and its hacking methodology. I also learned about SQL injection and bWAPP along with its features and architecture. Apart from that, I also had hands-on demonstrations of three different types Broken Authentication, Blind SQL Injections and Cross-site scripting.

This course introduced me to various new terminologies in the field of ethical hacking. They were really like a whole new world of ethical hacking. I got to learn about various computer security threats which is a major problem in the internet era. I also learned about the goals of ethical hacking and the skills and tools required for ethical hacking. I also learned in detail about the process of ethical hacking with demonstrations. I realised that there are various domains under ethical hacking among which the web application domain faces common attacks. I also learned about every domain in Detail and its hacking methodologies. I found that bWAAP is a really useful tool to learn ethical hacking. I also learned about Kali Linux and various web application attacks in depth.

The below link gives my course completion certificate:

https://olympus1.mygreatlearning.com/course_certificate/UFZCEFHR

Keylogger:

Keystroke logging is the process of recording (logging) the keys pressed on a keyboard (usually when the user is unaware). It is also known as keylogging or keyboard capturing.

These programs are used for troubleshooting technical problems with computers and business networks. It can also be used to monitor network usage but more often than not it is used for malicious intentions like stealing passwords.

Keylogger for Linux:
Download some python libraries

1) pywin32
2) pyhook

pyxhook requires python-Xlib. Install it if you don't have it already.

sudo apt-get install python-xlib
Download pyhook library
Following is the code to create a keylogger in python:

https://docs.google.com/document/d/1VtrOCpj7jU9tUKtQqcHjsP9BWFiTQDOOE71d4TQP7nI/edit?usp=drivesdk

Output:
The keylogger will be started in the background and save all the data on the file.log file "/home/Akash/Desktop".

Password cracking:

John the Ripper is an offline password cracker. In other words, it tries to find passwords from captured files without having to interact with the target. By doing this, it does not generate suspicious traffic since the process is generally performed locally, on the attacker's machine.

Although it's primarily used to crack password hashes, John can also be used to crack protected archive files, encrypted private keys, and many more.

Steps:

1) Create a zip file in Kali Linux
   https://imgur.com/a/xSpIweF

2) Get hash file
   https://imgur.com/a/Xiaykew

3) Convert hash into hash.txt
   https://imgur.com/a/SHPhpQE

4) Use John to get the password
   https://imgur.com/a/kwEPL7y

5) Extract the password from the actual zip file to check whether it is correct or not
https://imgur.com/a/C0hMI8r

I faced many problems during the process of building keyloggers and also learning about ethical hacking. But I also learned a lot while solving problems each time.
I want to learn more about hacking in the upcoming days. I am planning to watch YouTube videos about using bWAAP. I believe I can learn more knowledge from this.