

Over the past couple of weeks, it has been quite difficult to properly use AWS educate account. A number of tools have been suggested to use so as to exhaust and to have an appreciation of various tools and their results. Of interest Kali Linux and Shhgit were shared with us to add on the other tools we had used to do our scans in unit 4.

Kali Linux is a penetration testing platform which includes a number of tools and utilities. Interestingly, Kali Linux is used by both the bad and the good guys. It has over 600 already installed penetration testing tools. The number of tools configured and preinstalled on the operating system, make Kali Linux the Swiss Army knife in any security professionals toolbox (Guru99, 2021) I made several attempts to scan using this platform but they all failed.

On the other hand is Shhgit. As stated by Toshendra-Kumar Sharma (2019)

“Shhgit’ is the new web app that will search for sensitive secrets such as private crypto keys by scanning the web-based Github code repository. The new tool ‘Shhgit’ was introduced by Paul Price, the programmer and security expert. Shhgit’s function is to scan public code repositories for secrets that might sometimes end up in the hands of bad actors or malicious users and may ultimately have the potential of causing significant data breaches.”

As most of us have accounts on Github, this is a perfect tool to use just to keep our secrets safe.

References

Guru99 (N.D) Kali Linux Tutorial for Begginers. Available from <https://www.guru99.com/kali-linux-tutorial.html>

Toshendra Kumar Sharma (2019) Shhgit web app will scan Github repository for private crypto keys Available from: <https://www.blockchain-council.org/blockchain/shhgit-web-app-will-scan-github-repository-for-private-crypto-keys/>