***Synopsis***

**Name of project: -Hack Box *(A complete penetration testing tool kit)***

**Team Members**

Siddharth Khandelwal (leader)

Kartik Bajpay

Somuya Sharma

Sumit Prajapat

Sneha Shukla

***Introduction:-***

***Important terms to be understood***

***What is penetration testing?***

A penetration test, also called a pen test or ethical hacking, is a cybersecurity technique organizations use to identify, test and highlight vulnerabilities in their [security posture](https://searchsecurity.techtarget.com/definition/security-posture). These penetration tests are often carried out by ethical hackers. These in-house employees or third parties mimic the strategies and actions of an attacker in order to evaluate the hackability of an organization's computer systems, network or web applications. Organizations can also use pen testing to test their adherence to compliance regulations.

***What is Red Team test?***

Red Team Exercise is an imitation of multi-layered cyber-attack targeting agreed upon objectives that include networks, technical and physical assets, storage devices and many more. The exercise and assessment performed helps in improving your security defenses by letting you experience a real-world data breach and thereby giving a bigger picture of your organization’s risk posture, security architecture, and your team’s readiness in detecting and mitigating the threat proactively. Red Team Exercise unfolds security vulnerabilities by penetrating your networks, assessing your processes, and testing the defensive capabilities of your security teams in all possible ways. This helps in taking the necessary steps to update your security layers accordingly.

***HACK BOX***

Hack box is a simple debian based penetration testing toolkit which works on CLI & Gui both it is beginner friendly and can work on low end hardware it includes almost all type of attack tested in a Red team exercises such as Xss payload injection and reverse shell etc.

With this toolkit we no longer need to search or remember different types of hacking tools present in the system. This is beginner friendly tool as the newbies don’t know much about the tools and other then the default tools present in the os’s such as KALI LINUX and PERROT OS

It is highly customizable as all the tool are scripted in shell and python which are much easier to understand.

**Required hardware**

The hardware required for this os is very low although there are some basic requirements for proper functioning of this toolkit.

1. Dual core processor
2. 2GB RAM
3. At least 40GB hard disk
4. Wi-Fi adaptor for internet access (With 802.11 IEEE for wireless attack recommended)

**Current function**

* [Anonymously Hiding Tools](https://github.com/Z4nzu/hackingtool#anonymously-hiding-tools)
* [Information gathering tools](https://github.com/Z4nzu/hackingtool#information-gathering-tools)
* [Wordlist Generator](https://github.com/Z4nzu/hackingtool#wordlist-generator)
* [Wireless attack tools](https://github.com/Z4nzu/hackingtool#wireless-attack-tools)
* [SQL Injection Tools](https://github.com/Z4nzu/hackingtool#sql-injection-tools)
* [Phishing attack tools](https://github.com/Z4nzu/hackingtool#phishing-attack-tools)
* [Web Attack tools](https://github.com/Z4nzu/hackingtool#web-attack-tools)
* [Post exploitation tools](https://github.com/Z4nzu/hackingtool#post-exploitation-tools)
* [Forensic tools](https://github.com/Z4nzu/hackingtool#forensic-tools)
* [Payload creation tools](https://github.com/Z4nzu/hackingtool#payload-creation-tools)
* [Exploit framework](https://github.com/Z4nzu/hackingtool#exploit-framework)
* [Reverse engineering tools](https://github.com/Z4nzu/hackingtool#reverse-engineering-tools)
* [DDOS Attack Tools](https://github.com/Z4nzu/hackingtool#ddos-attack-tools)
* [Remote Administrator Tools (RAT)](https://github.com/Z4nzu/hackingtool#remote-administrator-tools--rat-)
* [XSS Attack Tools](https://github.com/Z4nzu/hackingtool#xss-attack-tools)
* [Steganography tools](https://github.com/Z4nzu/hackingtool#steganograhy-tools)

**Innovation and usefulness**

1) It can run on a very low end hardware.

2) Al the required tools are at one place.

3) Easy to install your favourite tools.

4) Command line interface based alternative for Graphical user interface tools for low end cli based operating system

5) Highly customizable

**Need for HACK BOX**

1. **Who should use: -**

Although this tool kit is perfect for any pentester or red team member the tool is recomended for new comers as all the tools required are at one place and they don’t need to remember every tool (just select the tool kit and run the tool).

1. **Reduce cost: -**

As it run’s on any Linux distribution (which is open source) & can run on a low end hardware, a perfect hacking setup can be easily build at a low cost.

1. **Highly customizable: -**

As all the script are written in shell or python which are much easier to understand and all the code is open source hence it can be customized.

**Conclusion: -**

We as a group of ethical hackers recommend HACK BOX for its customizability, user friendly UI, simplicity and being a beginner’s friendly complete hacking tool kit.