Securezy - A Penetration Testing Toolbox

Vinit Motghare[1] ,Aniket Kasturi[1] ,Akash Kokare[1] , Amruta Sankhe[2]

[1]Dept. of Information Technology, Atharva College of Engineering, Maharashtra, India
[2]Assistant Professor, Dept. of Information Technology, Atharva College of Engineering, Maharashtra, India

---***---

Abstract - ***In this online era, where absolutely everything is on the internet. Cyber Security has come forward as one of the most vital and high-priority agendas. To ensure our virtual security, Ethical Hackers have come into the picture. But, becoming a fully-fledged Ethical Hacker is a complicated journey and usually takes years of experience. As the entry criteria for Cyber Security are so high, many students and professionals are skipping this fundamental field. As a beginner in the Cyber Security domain, people can find its techniques and tools quite daunting. There are numerous tools available on the Internet, each with its specific use case and with its complex working and complex commands. This complexity could make or break someone's interest in this particular field. To make the initial journey of young Ethical Hackers, we have built 3 Security tools wrapped in one Graphical User Interface software. This paper talks about the following toolbox containing a Port scanner, Text encryption/decryption tool, and along with a password cracker.***

***Key Words*:** **Cyber Security, Ethical Hackers, Graphical User Interface, Penetration Testing, Cyber Kill Chain, Reconnaissance, Encryption, Decryption and Hashing, PTES, VAPT.**

1. INTRODUCTION

Cyber Security is one of the most underemployed domains in the IT industry at this current time. Jobs are left unfilled all over the world and the demand for qualified individuals is as high as it gets. [7] The job market, as well as National jobs for this domain, is going to increase by 30% by 2030 [6]. This leads to a conundrum as there's an increased requirement of individuals but no one to qualify for it. Cyber security jobs require years of knowledge and experience along with certifications to back them up. For beginner Ethical Hackers, they have to commit and learn different kinds of tools for Penetration Testing from different places, which have complex command structures [1]. Hoping from tool to tool can turn into a hassle for a novice Ethical Hacker. Such hassle and inability to have a certain job in Cyber security can be demotivating for many and lead to ditching this field completely. This paper states a need for easy to use software for some Penetration Testing tools in one GUI window. The paper also mentions the Cyber Kill Chain phases, which is an essential cyber security-based model that traces cyber attacks. It helps the security researchers to stop attacks at every stage of the chain.

There are 7 phases namely-
Reconnaissance, Weaponization, Delivery, Exploitation, Installation, installation, Command & Control, Actions and objectives.

2. LITERATURE SURVEY

IIn [1] the authors discussed nmap and its ability to find the available ports and services. The authors of this particular paper used different kinds of command variations present in nmap. They also looked into the traffic and time calculations of each command variation. Depending on the amount or volume of the network, there are timing options within nmap. In the end, the paper proposes a scan strategy taking into consideration the different constraints mentioned above.

In [2] the authors talk about different types of sweeping, also known as Port scanning. In it, they focus on Vertical scans i.e. single IP address of the network being tested on multiple ports. The paper chooses to analyze how hackers try to enter a network using vertical scanning and build a relationship amongst the commonly scanned ports.

In [3] the authors looked into port scanning using the TOR browser, which was developed by the US Navy to surf the Internet anonymously. Through TOR, the target of the port scan can't retaliate at us, due to the uncertainty created. This is necessary knowledge to be aware of while protecting our information and interest, as Hackers can make use of this methodology.

In [4] the paper examines the many sorts of attacks and techniques used in password cracking, as well as the general, do's and don'ts for safeguarding sensitive data against unauthorized users. The author also mentions different password cracking tools and their working. Especially demonstrating attacking FTP and SSH servers using THC Hydra.

In [5] the authors put forth the importance and need of cybersecurity for the countries around the world. In the past, battles took place on actual battlefields. But in recent years, battles have shifted to virtual areas. The paper also shed some light on the cyber capabilities of some major countries. It is very crucial how to react when cyber attacks occur. The authors write about cyber warfare and its law based on International interest.

In [6] the authors state who an ethical hacker is, and why there's a need for the world to learn it. The authors also give us an idea of Ethical Hacking and its 5 steps/blocks, going in-depth into all the blocks and their definite purpose. The paper mentions the tool used for each block and a descriptive summary of it. Also, this paper gives a basic understanding of ethical hacking.

3. PROPOSED SOLUTION

Our proposed system involves the tools required/assisted for the initiation of the cyber kill chain - our software has a feature like a port scanner which is the initial phase of reconnaissance. The solution we propose here is to offer a handy toolbox that comprises tools of various phases such as reconnaissance, password cracking, encryption / decryption, and password manager. Dedicated and built solely for penetration testers to avoid wastage of time while navigating from one tool to another while they are in their hunting process. All this is wrapped in python GUI for ease of navigation.

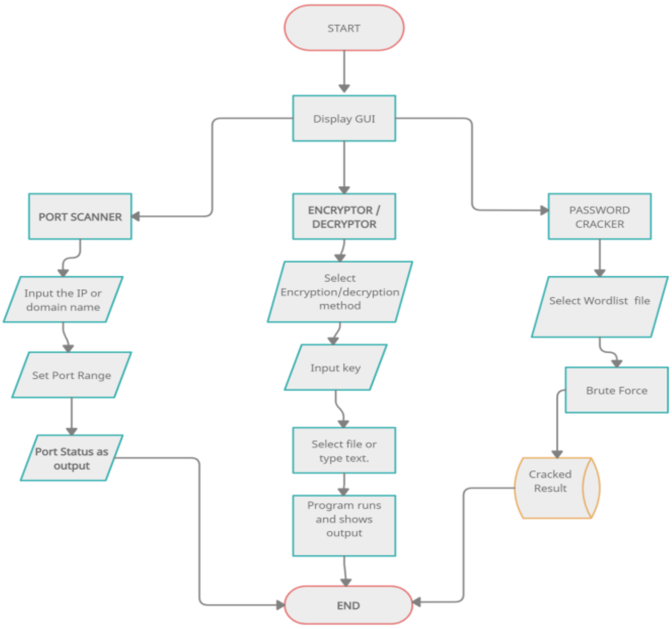


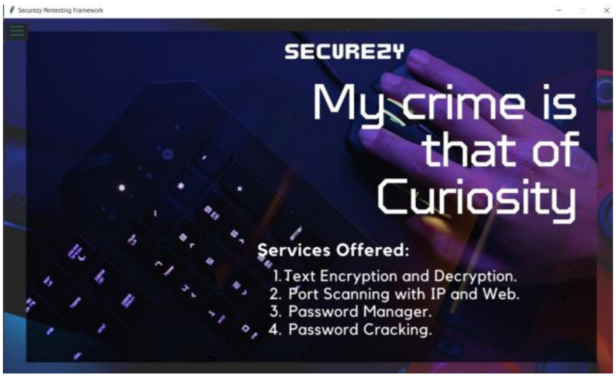
Fig -1: System Design

We have formulated the design with these methods:

1. **Reconnaissance Phase**: This is the first phase of the cyber kill chain to initiate a footprinting or information gathering process. To lookout for some loopholes on the network (open ports/closed ports).

2. **Gaining Access Phase:** Once a penetration tester or security researcher finds some credentials exposed over an internet application he/she can use the Encryptor/Decryptor tool to fulfil his purpose of gaining access to credentials.

3. **Password strengthening Phase**: Here this password manager tool allows the security researcher to generate a hashed password for social accounts or any other online accounts and keep that credentials in a password list which is protected by the master password set by the user.

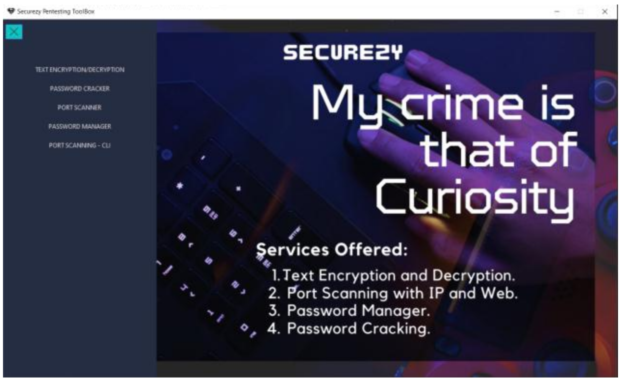

Securezy Pentesting Framework

SECUREZY

My crime is that of Curiosity

Services Offered:
1. Text Encryption and Decryption.
2. Port Scanning with IP and Web.
3. Password Manager.
4. Password Cracking.

Fig -2: Use Case illustration


Securezy Pentesting ToolBox

SECUREZY

My crime is that of Curiosity

Services Offered:
1. Text Encryption and Decryption.
2. Port Scanning with IP and Web.
3. Password Manager.
4. Password Cracking.

Fig -3: Tools

3. METHODOLOGY

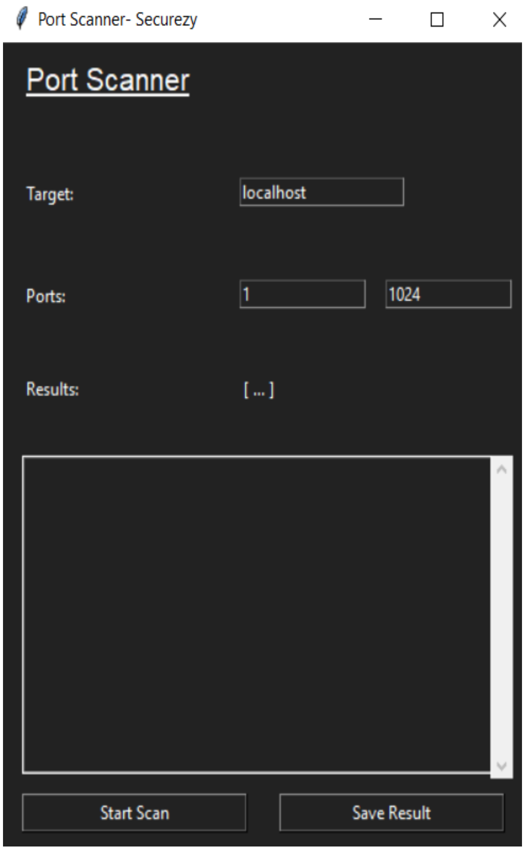
In our project, we used a methodology of PTES which stands for Penetration Testing Execution Standard. This method is globally recognized and covers the broad spectrum of the penetration test which starts from initial communication and the researcher's reasoning skill. Our software model follows the baseline of PTES via the Scan port feature and gaining access via the password cracking feature. Our software starts with a pre-engagement interaction via the web application our first feature checks for open or closed ports. Moving further to exploitation if we want to gain access or hunt for user credentials our second feature is inclined towards password cracking. Further, we found any data leaks or user credentials. We have our hasher which can crack hashed credentials of SHA256, SHA1, and MD5 encrypted texts. Further for the ease of the security researcher, we have also added a password manager feature.

3.1 SYSTEM MODULES

Our Software has a strong baseline and follows the PTES global standard. Our modules include Firstly the Port scanner feature followed by password cracking and hasher.

A. PORT SCANNER (GUI/CLI):

This feature is great for reconnaissance and initial footprinting for gathering information about the ports which are open/closed or filtered. This feature helps the penetration tester or security researcher to passively lookout for his initial approach to the hunting methodology. First input the target website into the given input and after that select the port range for running the scan on the target. The results will be displayed in the results section of the GUI.



Target: localhost

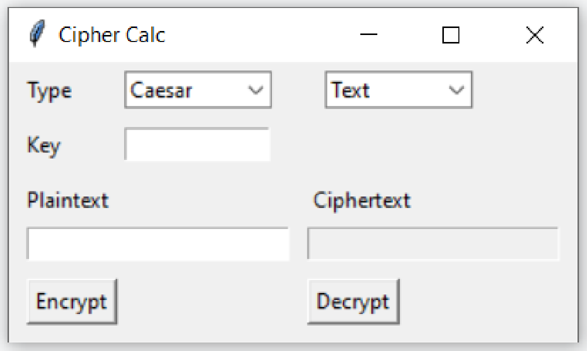
Ports: 1 1024

Results: [...]

Fig -4: Port Scanner GUI

B. TEXT ENCRYPTION / DECRYPTION

This tool helps users to encrypt and decrypt the secret messages/text using ciphers such as Caesar, Playfair, Columnar, and Vigenere by providing a key value. After selecting the operation that is encryption and decryption user can choose direct encryption or can select the file or folder to encrypt and vice versa.

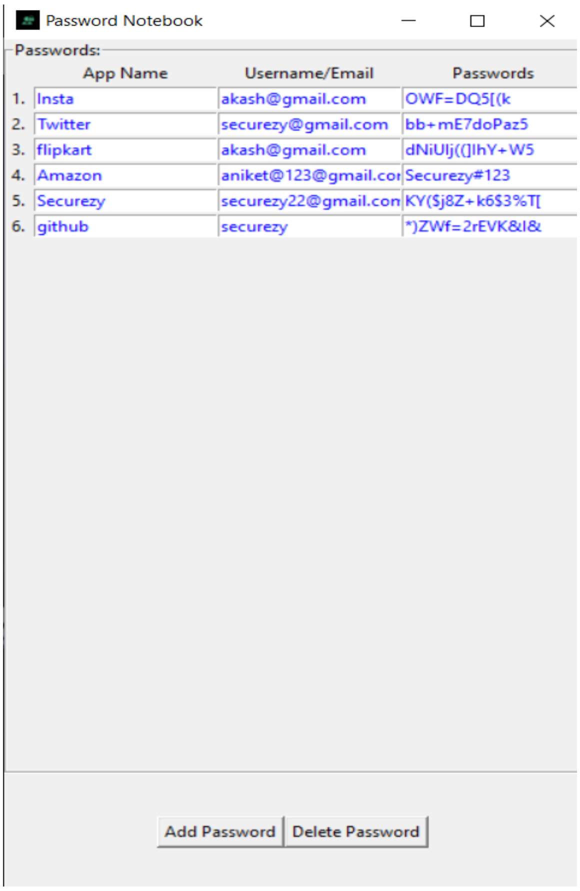


Type: Caesar, Text

Fig -5: Text Encryptor / Decryptor

C. PASSWORD MANAGER

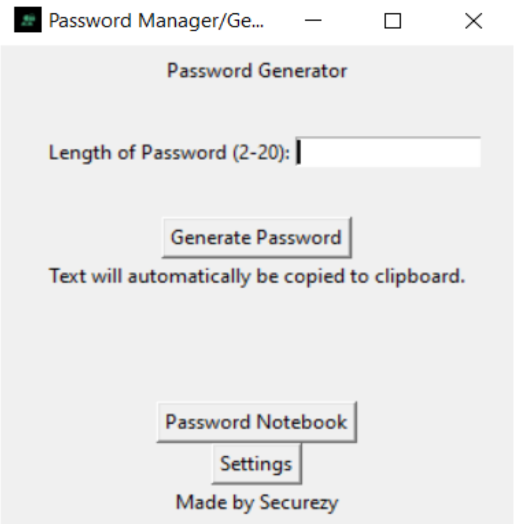
This feature helps the user to generate a hashed password for a social account or any other online account and save the credentials that are username/email and passwords in the password list which is protected by the master password set by the user. To access the password list the user needs to authenticate himself/herself by the master password.



Passwords:

	App Name	Username/Email	Passwords
1.	Insta	akash@gmail.com	OWF=DQ5[(k
2.	Twitter	securezy@gmail.com	bb+mE7doPaz5
3.	flipkart	akash@gmail.com	dNiUIj(()IhY+W5
4.	Amazon	aniket@123@gmail.cor	Securezy#123
5.	Securezy	securezy22@gmail.con	KY($j8Z+k6$3%T[
6.	github	securezy	*)ZWf=2rEVK&I&

Fig -6: Password Manager



Password Generator

Length of Password (2-20):

Text will automatically be copied to clipboard.

Made by Securezy

Fig -7: Password Generator GUI

D. PASSWORD CRACKER (CLI)

This feature is used to crack the inserted hashed password by matching it with the dictionary of passwords using a brute force attack. The tool can process hashed password which is hashed by MD5, and SHA hashing algorithms which can be further compared with the password list to check if it matches by using the brute force approach with the same if it does so it revert to the password that the user entered matches with the password list.

4. CONCLUSION

To make the Cyber Security domain accessible and interesting to young professionals, we have to lay out a roadmap for becoming a full-time professionals in this field. The first step of the roadmap is constructing an application encompassing multiple Ethical Hacking tools. In our software model, we have implemented our project keeping into consideration the PTES- Penetration Testing Execution Standard. Our software helps the researcher to have a toolbox handy while they start their Pen-Test or Penetration Testing and Vulnerability assessment. Our software saves time for the researcher to have a hassle-free and easy handiness of tools which helps for hunting. In conclusion, we can say that in the cyber world tools are necessary and saves a lot of time to automate a few steps thus our software can be a swiss army knife for Ethical Hackers. In the future, our software could have more features and tools necessary for Ethical Hacking.

REFERENCES

[1] Shah, M., Ahmed, S., Saeed, K., Junaid, M., & Khan, H. (2019, January). Penetration testing active reconnaissance phase–optimized port scanning with nmap tool. In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET) (pp. 1-6). IEEE.

[2] Lagraa, S., & François, J. (2017, May). Knowledge discovery of port scans from the darknet. In 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM) (pp. 935-940). IEEE.

[3] Rohrmann, R., Patton, M. W., & Chen, H. (2016, September). Anonymous port scanning: Performing network reconnaissance through Tor. In 2016 IEEE Conference on Intelligence and Security Informatics (ISI) (pp. 217-217). IEEE.

[4] Kakarla, T., Mairaj, A., & Javaid, A. Y. (2018, May). A Real-World Password Cracking Demonstration Using Open Source Tools for Instructional Use. In 2018 IEEE International Conference on Electro/Information Technology (EIT) (pp. 0387-0391). IEEE.

[5] Sevis, K. N., & Seker, E. (2016, June). Cyberwarfare: terms, issues, laws and controversies. In 2016 International Conference On Cyber Security And Protection Of Digital Services (Cyber Security) (pp. 1-9). IEEE.

[6] Patil, S., Jangra, A., Bhale, M., Raina, A., & Kulkarni, P. (2017, September). Ethical hacking: The need for cyber security. In 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI) (pp. 1602-1606). IEEE.

[7] https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm