A COMPREHENSION ON ETHICAL HACKING: TOOLS, BOOKS, AND WEBSITES

Anne Supriya[1], Gudem Shruthika[2], Ranga Rishitha[3], Thavidisetti A J Sri Sarayu[4],
Kiranmaie Puvulla[5], M Venu Gopalachari[6]
Department of Information Technology
Chaitanya Bharathi Institute of Technology
Hyderabad, Telangana, India – 500075

***Abstract*—In today's world of cyber security ethical hacking plays a prominent role and to master this landscape it is important to have access to the right tools, books, and learning resources. This document lists tools, books, and websites that are extremely helpful for the ones looking to probe into ethical hacking. From reconnaissance and penetration testing to crucial literature, this comprehension facilitates with required resources to enhance knowledge and skills in ethical hacking. With the growing number of cyber threats the requirement for skilled ethical hackers has also increased. This collection provides selected resources to help beginners or experienced professionals stay ahead in this dynamic and demanding field. This collection of resources, including tools, books by experts, and websites, offers a comprehensive learning experience for anyone interested in ethical hacking and cybersecurity. It covers both fundamental concepts and advanced techniques, equipping you with the necessary skills and knowledge to excel in this field.**

***Index Terms*—Cyber security, Ethical hacking, Reconnaissance, Penetration testing, Cyber threats, Advanced techniques.**

I. INTRODUCTION

Ethical hacking, also known as penetration testing, plays an important role in cybersecurity. It aims to identify and address issues within computer systems, networks and web applications. Ethical hackers are called white hat hackers, they use a variety of tools, techniques and methodologies to overcome real-world cyber attacks with the explicit permission of system owners. The main objective is to find and fix security flaws before malicious hackers make use of them for any evil purpose. In recent years, businesses in a variety of industries have realized how important it is to take preventative security measures and started work towards safeguarding their priceless information and assets from online attacks; hence, the demand for skilled and knowledgeable ethical hackers has increased dramatically. Through their systematic assessment of systems, ethical hackers play a crucial role in helping companies detect and mitigate potential security risks. By doing so, they aid in upholding the integrity of systems and safeguarding sensitive data. Many methods and resources used by malicious hackers are also used in ethical hacking. On the other hand, ethical hackers follow a rigid code of conduct and have explicit authorization from system owners, which is essential. They check a system's security posture and find flaws using methodical methodology. This includes phases such as reconnaissance, scanning, exploitation, post-exploitation, and covering tracks. Their role is to simulate the tactics, techniques, and procedures of cybercriminals. By doing so, they help organizations understand their security weaknesses and the potential impact of a breach. Ethical hacking involves a comprehensive process that includes planning, scanning, gaining access, maintaining access, and analyzing the findings. During the planning phase, ethical hackers work with the client to define the scope and goals of the testing. This ensures that the testing is conducted legally and within agreed boundaries.

After completing the tests, ethical hackers compile a detailed report of their findings, including the vulnerabilities discovered, the methods used to exploit them, and recommendations for remediation. This report is vital for organizations to understand their security posture and to implement necessary security measures to mitigate risks. Ethical hackers often work closely with IT and security teams to help them understand the findings and prioritize remediation efforts. Ethical hacking is governed by a strict code of conduct and professional standards. Ethical hackers must obtain explicit permission before conducting any tests, ensuring that their activities are legal and authorized. They are also expected to maintain confidentiality, protecting the sensitive information they may encounter during their testing. Certifications such as Certified Ethical Hacker (CEH) and Offensive Security Certified Professional (OSCP) are widely recognized in the industry, providing a benchmark for the skills and knowledge required to perform ethical hacking effectively. To find flaws and conduct penetration tests, ethical hackers use a variety of tools. A few of these technologies are Network scanners, vulnerability scanners, packet sniffers, password crackers and exploitation frameworks. Numerous books offer thorough instructions on ethical hacking, addressing different aspects of offensive security, penetration testing and cybersecurity. A variety of websites and online platforms provide a wealth of information and training possibilities for those interested in learning about ethical hacking. A vital part of contemporary cybersecurity procedures is ethical hacking, which enables businesses to proactively find and fix security flaws before malicious hackers may exploit them. The use of different tools and techniques, along with a systematic approach makes ethical hackers essential in protecting confidential data and guaranteeing system integrity. People interested in learning ethical hacking may find it beneficial to learn about cybersecurity and people with ethical hacking talent will find it useful to work in the cybersecurity sector since there is an increasing demand for qualified cybersecurity specialists. From this collected information, one can acquire the abilities and information required to become skilled ethical hackers and support the ongoing effort to prevent cyber risks through practice and constant learning.

II. Literature Review

Gaia, J., & Sanders, G. L. (2020). "Psychological Profiling of Hacking Potential." In this paper published in the Journal Name, Volume 3, pages 2230–2239, the authors delve into the psychological aspects of hacking potential. They likely explore various psychological profiling techniques to understand the characteristics and traits indicative of a propensity for engaging in hacking[**2**] activities. Understanding such factors could aid in identifying individuals who may pose a higher risk of engaging in malicious hacking, thereby contributing to cybersecurity efforts. Thomas, G., Burmeister, O., and Low, G. (2019) explore "The Importance of Ethical Conduct by Penetration Testers in the Age of Breach Disclosure Laws" in their paper published in the Australasian Journal of Information Systems. The authors likely delve into the ethical considerations surrounding the conduct of penetration testers, emphasizing the significance of ethical behavior, especially in light of breach disclosure laws. They may discuss the ethical dilemmas faced by penetration[**3**] testers and the potential consequences of unethical behavior in cybersecurity practices. The paper could offer insights into ethical guidelines and best practices for penetration testers to ensure responsible and lawful conduct in their activities, thereby contributing to the enhancement of cybersecurity frameworks.

Babbar, Jain, and Kang's work, available on Research Gate, likely contributes to the broader discourse surrounding ethical hacking[**4**]. Their research may explore various aspects of ethical hacking, such as methodologies, tools, ethical guidelines, and the role of ethical hacking in cybersecurity. By accessing their study, readers may gain insights into the technical and ethical considerations involved in this field. Munjal's paper likely delves into the societal implications of ethical hacking. By examining this work, readers may gain a deeper understanding of how ethical hacking practices influence various aspects of society, such as cybersecurity norms, privacy concerns[**5**], and legal frameworks. The paper may explore both the positive and negative impacts of ethical hacking on individuals, organizations, and communities.

This source from Cybrary likely provides an overview of the five phases involved in penetration testing. By summarizing these phases, the resource may offer insights into the systematic approach used by cybersecurity professionals to identify and address vulnerabilities in computer systems and networks. Readers can expect to learn about the different stages of penetration[**6**] testing, including reconnaissance, scanning, exploitation, post-exploitation, and reporting, along with the methodologies and tools commonly employed in each phase. The article titled "Is Ethical Hacking Ethical?" published in the International Journal of Engineering Science and Technology in 2011 likely explores the ethical implications of ethical hacking practices. It may delve into the debate surrounding the morality of hacking activities conducted for security testing[**7**] and defensive purposes. The paper could discuss various perspectives on whether ethical hacking aligns with ethical principles, considering factors such as legality, consent, privacy, and potential harm to individuals or organizations. Readers can anticipate an examination of the ethical frameworks and arguments surrounding the practice of ethical hacking within the broader context of cybersecurity and information technology.

In the chapter titled "Reconnaissance" from the book "The Basics of Hacking and Penetration Testing" by P. Engebretson, readers can expect an exploration of reconnaissance techniques used in penetration testing and ethical hacking. The chapter likely covers various methods employed to gather information about target systems, networks, and organizations before launching an attack. This could include passive and active reconnaissance techniques, such as footprinting[**8**], scanning, and enumeration. The author may also discuss the importance of reconnaissance in the overall penetration testing process and its role in identifying vulnerabilities and potential attack vectors. Additionally, readers may gain insights into the ethical considerations surrounding reconnaissance activities and how they contribute to improving cybersecurity defenses. The autotelic propensity of different hacker types, explored by Floyd, K., Harrington, S., Hivale, P. (2007) in their presentation at the 4th Annual Conference on Information Security Curriculum Development (InfoSecCD '07), likely investigates the inherent motivation and enjoyment hackers derive from their activities. This analysis could offer insights into how various hacker categories, such as black hat, white hat[**9**], and grey hat hackers, approach their tasks. Understanding these motivations may provide valuable perspectives on hacker behavior, target selection, and ethical considerations. Moreover, the study might discuss the implications of autotelism for cybersecurity education and training, highlighting the importance of fostering ethical hacking skills and promoting responsible conduct within the cybersecurity community.

Simpson, M. T., Backman, K., Corley, J. E. (2013) authored a comprehensive guide titled "Hands-on Ethical Hacking and Network Defense," published by Cengage Technology in Boston, MA. This resource likely provides practical insights and methodologies for conducting ethical hacking activities while emphasizing the importance of network defense strategies. It may cover topics such as penetration testing, vulnerability assessment, and incident response, equipping readers with the knowledge and skills needed to secure networks[**10**] effectively. The book likely combines theoretical concepts with hands-on exercises, enabling readers to gain practical experience in ethical hacking techniques and network protection strategies.

III. Tools

To assess the security of computer systems and networks ethical hackers rely on various tools. Here are some of the most popular and widely used ethical hacking tools:

1) **Nmap** - Nmap is a powerful open-source network scanner used for network discovery and security auditing
2) **Wireshark** - Wireshark is a popular network protocol analyzer for capturing and interacting with network traffic.
3) **Metasploit** - Metasploit is an advanced open-source penetration testing framework that facilitates the exploitation and testing of vulnerabilities.
4) **Burp Suite** - Burp Suite is a comprehensive web application security testing tool used to scan and exploit web applications.
5) **Hydra** - Hydra is a powerful online password-cracking tool that supports various protocols such as HTTP, HTTPS, FTP, etc.
6) **OWASP ZAP** - OWASP ZAP is an open-source web application security scanner for finding vulnerabilities in web applications.
7) **Aircrack-ng** - Aircrack-ng is a complete suite of tools to assess WiFi network security.
8) **Hashcat** - Hashcat is an advanced password recovery tool that supports various hashing algorithms.
9) **Zphisher** - Zphisher tool is used for phishing attacks, providing templates and methods to trick users into revealing sensitive information.
10) **SocialPhish** - SocialPhish is a social engineering toolkit designed for phishing attack, crafting convincing fake login pages for various platforms.
11) **TheFatRat** - TheFatRat is a tool used to generate undetectable payload and backdoor for penetration testing.
12) **Recon-ng** - Recon-ng is a reconnaissance framework that assists in information gathering and footprinting during penetration testing.
13) **John the Ripper** - John the Ripper is a powerful password-cracking tool, capable of dictionary and brute-force attacks against carious encrypted formats.
14) **SqlMap** - SqlMap is an open-source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws.
15) **Sora-OpenAI** - Sora-OpenAI is an AI-developed tool for creating videos from text input, leveraging natural language understanding and video generation technologies.
16) **WhoReadMe.com** - WhoReadMe.com is a service that allows users to track email opens and clicks, often used for email marketing and tracking purpose
17) **Spoofbox** - Spoofbox is a platform that offers tools and services for spoofing email addresses, phone numbers and other digital identities.
18) **BleachBit** - BleachBit is a disk cleaning utility designed to free up disk space and maintain privacy by securely deleting unnecessary files. It helps in covering tracks during penetration tests or security assessments.
19) **Shodan** - Shodan is a search engine for internet-connected devices, often used for security research and finding vulnerable systems.
20) **AirDroid** - AirDroid is a remote management tool for Android devices, which allows users to manage files, messages and more from the web browser.
21) **Ghidra** - Ghidra is a software reverse engineering framework developed by NSA for analysing malware and software vulnerabilities.
22) **BeEF (Browser Exploitation Framework)** - BeEF is a tool used for exploiting web browser vulnerabilities to perform various attacks such as XSS and CSRF.
23) **SEToolkit (Social Engineering Toolkit)** - SEToolkit is a tool kit used to perform social engineering attacks like phishing and credential harvesting.
24) **Hack The Box** - Hack The Box is an online platform that provides challenges and virtual environments for cybersecurity enthusiasts to enhance their skills in ethical hacking and penetration testing.
25) **Flipper Zero** - Flipper Zero is a multi-tool device for hackers and cyber security enthusiasts that offers capabilities such as RFID(Radio Frequency Identification) emulation, hardware hacking and more.
26) **Kali linux** - Kali Linux is a Debian-based Linux distribution designed for digital forensics and penetration testing.

IV. Architecture

A. *Nmap*

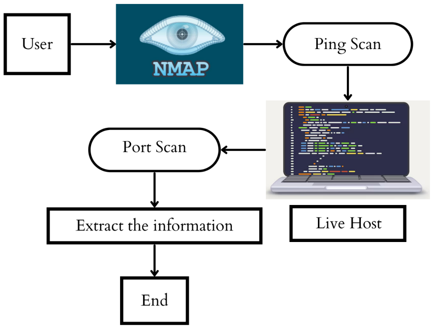


Fig. 1. Nmap Flowchart.

Nmap (Network mapper) is an open-source tool used for scanning networks and finding live hosts. It has flexible features which makes it a good choice for security professionals to use it for scanning. In Nmap first select the target system for scanning. Then execute a ping scan to check if the host is live. If any host is live, execute a port scan, choosing the appropriate options such as TCP or UDP scan. Analyze the results and extract all the information as in Figure 1., to generate a network map, then end the process. This is generally used for reconnaissance and scanning.

B. Metasploit

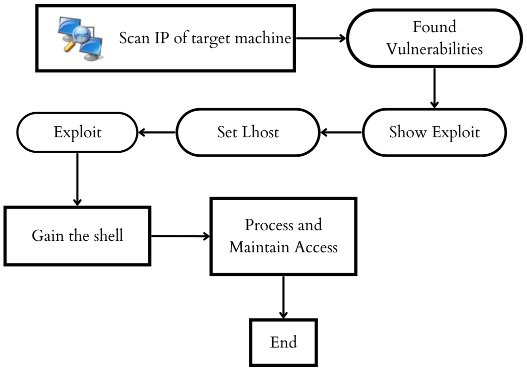


Fig. 2. Working of Metasploit.

The Metasploit tool for cybersecurity empowers ethical hackers with a robust framework for penetration testing and vulnerability assessment. It has an extensive database of exploits, payloads, and auxiliary modules. Thus Metasploit is an essential property in the cybersecurity collection. It is used by professionals to find, exploit and resolve vulnerabilities across various systems and applications. Once after finding the vulnerabilities using Nmap and after successfully exploiting the vulnerabilities identified in the vulnerability assessment step of Figure 2., initial access is gained. Following initial access, the attacker aims to maintain access to the system. If successful, The attacker can repeat the exploitation process or the attack ends. This tool is used in the gaining and maintaining access phase.

C. Zphisher

Phishing is a form of cyber attack where attackers disguise themselves as trustworthy entities to deceive individuals into providing sensitive information such as usernames, passwords, and credit card details. This is often done through deceptive emails, websites, or messages that appear legitimate. Zphisher tool helps the user to create various phishing pages and host them for example social media and other platforms. Hence, it is a popular choice for ethical hackers for phishing attacks. A user selects a template for a phishing page and then generates the phishing site shown in Figure 3., and then hosts it. Once hosted, they share the phishing link. If the victim interacts or enters credentials, the credentials are captured before the process ends, if not the project ends.

D. BleachBit

BleachBit is a prominent open-source tool that is used to clean the system's disk space and to find the tracks. It deletes unnecessary files and cookies to maintain privacy and to free up space. It ensures that the data in the system is secure and has no issue with leftover files. BleachBit provides options to select. After selecting cleaning options and files in the third-fourth steps of Figure 4., the cleaning process begins. Once started, the system checks if the cleaning is completed, if yes the process is completed. If not the cleaning continues until finished. This ensures a thorough cleaning according to the choice of user. This tool is mainly used in covering the tracks phase.

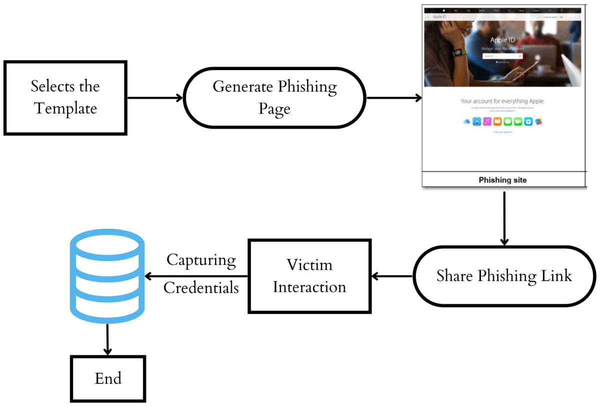


Fig. 3. Phishing using Zphisher.

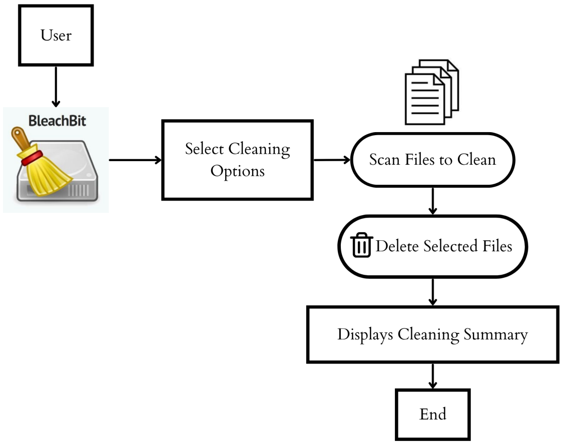


Fig. 4. Options in BleachBit.

V. Books

Besides practical knowledge gained by tools, one can be an expert by learning from books. These are a few key books help in lifting-up anyone in ethical hacking:

1) **"The Hacker Playbook 3: Practical Guide to Penetration Testing"** by Peter Kim.
2) **"Hacking: The Art of Exploitation"** by Jon Erickson.
3) **"Click Here to Kill Everybody"** by Bruce Schneier

4) **”Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World”** by cryptographer Bruce Schneier
5) **”The Web Application Hacker’s Handbook: Discovering and Exploiting Security Flaws”** by Dafydd Stuttard and Marcus Pinto
6) **”Mastering Hacking: The Art of Information Gathering and Scanning”** by HARSH. BOTHRA
7) **”Ethical Hacking: A Hands-on Introduction to Breaking In”** by Daniel G. Graham
8) **”Metasploit: The Penetration Tester’s Guide”** by David Kennedy, Jim O’Gorman, Devon Kearns, and Mati Aharoni.
9) **”Web Application Hacker’s Handbook”** by Dafydd Stuttard and Marcus Pinto.
10) **”The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy”** by Dafydd Stuttard and Marcus Pinto.
11) **”Violent Python: A Cookbook for Hackers, Forensic Analysts, Penetration Testers, and Security Engineers”** by TJ O’Connor.
12) **”Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software”** by Michael Sikorski and Andrew Honig.
13) **”Black Hat Python: Python Programming for Hackers and Pentesters”** by Justin Seitz.
14) **”The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy”** by Patrick Engebretson
15) **”Penetration Testing: A Hands-On Introduction to Hacking”** by Georgia Weidman.
16) **”The Web Application Hacker’s Handbook: Finding and Exploiting Security Flaws”** by Dafydd Stuttard and Marcus Pinto.
17) **”Gray Hat Hacking: The Ethical Hacker’s Handbook”** by Allen Harper, Daniel Regalado, Ryan Linn, Stephen Sims, Branko Spasojevic, Linda Martinez, and Michael Baucom.
18) **”Social Engineering: The Art of Human Hacking”** by Christopher Hadnagy.
19) **”Mastering Kali Linux for Advanced Penetration Testing”** by Vijay Kumar Velu.
20) **”CEH Certified Ethical Hacker All-in-One Exam Guide”** by Matt Walker.

VI. Websites

Ethical hacking can be learned from various websites, which offers wide range of courses from free to comprehensive level tutorials. Here are some of the websites helps to deepen in ethical hacking:

1) **Cybrary** - Offers free online cybersecurity training courses including ethical hacking.
2) **Udemy** - Provides a wide range of ethical hacking courses for both beginners and advanced learners.
3) **Coursera** - Offers online courses from universities and colleges covering various aspects of ethical hacking and cybersecurity.
4) **Pluralsight** - Provides a vast library of courses on ethical hacking, penetration testing, and cybersecurity.
5) **Hack The Box** - An online platform that allows you to test your penetration testing skills through various challenges.
6) **TryHackMe** - Offers interactive and gamified cybersecurity training, including ethical hacking.
7) **OverTheWire** - Provides various war games to learn and practice security concepts and techniques.
8) **SecurityTube** - Offers a wide range of video tutorials and courses on ethical hacking and cybersecurity.
9) **Cybersecurity Training from Offensive Security (OffSec)** - Offers online courses like ”Penetration Testing with Kali Linux” and ”Advanced Web Attacks and Exploitation.”
10) **Hacker101** - A free class for web security created by HackerOne.
11) **PortSwigger Web Security Academy** - Offers free online web security training, including tutorials and labs on web application security and penetration testing.
12) **Pentester Academy** - Offers online courses and virtual labs on ethical hacking, penetration testing, and cybersecurity, including network security, web application security, and wireless security.
13) **VulnHub** - Offers a hands-on learning experience in a safe and controlled environment.
14) **HackThisSite** - Offers a variety of challenges and tutorials to help users learn and practice hacking techniques.
15) **SANS Cyber Aces** - Offers free online cybersecurity courses and challenges for beginners.
16) **Open Security Training** - Offers free security training courses and materials, covers topics such as reverse engineering, malware analysis, and exploit development.

VII. Implementation and Results

A. UserRecon

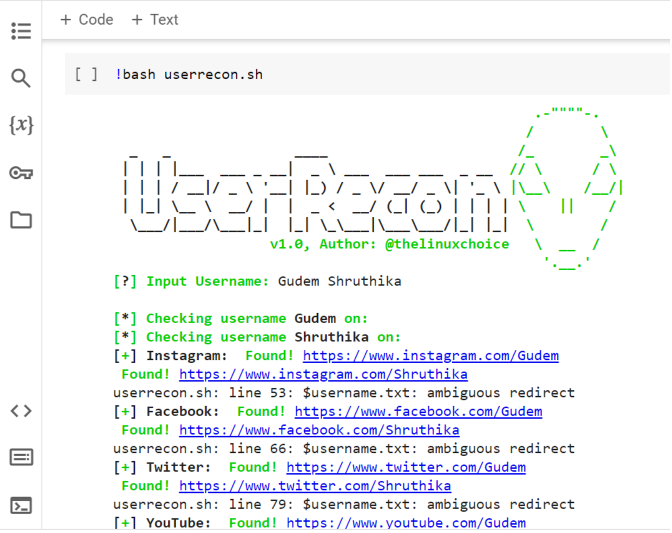
UserRecon is an open-source reconnaissance tool designed to help cybersecurity professionals gather information about user accounts across various online platforms. It works by sending requests to a wide array of popular platforms, including social media sites, forums, and other online services, and checking if the specified username exists. This can reveal if a username is linked to multiple accounts across different sites, potentially uncovering additional information about the target. The tool’s efficiency lies in its automation, which significantly speeds up the reconnaissance process compared to manual searching. The tool is implemented in Python, making it highly portable and easy to run on different operating systems. Its command-line interface allows users to execute scans quickly and integrate the tool into larger security workflows or scripts. The results provided by UserRecon can be used to identify potential vulnerabilities, such as reused usernames and the possibility of associated weak or reused passwords across sites, which are common security risks. Ethical use of UserRecon is paramount. It is designed for use in authorized security assessments, where penetration testers or security analysts have explicit permission to conduct reconnaissance. Unauthorized use of UserRecon to gather information without consent is illegal and unethical, violating privacy laws and the terms of service of many online platforms.

Implementation Steps:

1) **Clone the GitHub repository:**
   git clone https://github.com/wishihab/userrecon.git
2) **Navigate into the cloned directory:**
   cd userrecon
3) **Run the script:**
   bash userrecon.sh
4) **Enter the username** you want to recon(entered Gudem Shruthika)

Results Steps:

1) **View Found Profiles:**
   The script searches for the entered username across multiple online platforms, such as Instagram, Facebook, Twitter, etc.
   It displays found profiles on various platforms, including GitHub, Reddit, YouTube, etc., providing a comprehensive overview of the user's online presence.
2) **Review Not Found Profiles:**
   The script also indicates profiles not found on certain platforms like YouTube, Spotify, Blogger, etc.
3) **Purpose of "userrecon":**
   "userrecon" is designed for user reconnaissance in ethical hacking, automating the process of searching for a specific username across various online platforms to gather information about the user's online presence.
4) **Output Saving:**
   The script saves the results in a file for further analysis, providing valuable insights for security assessments, investigations, or other legitimate purposes within the scope of ethical hacking.
5) **Here are the results:**
   Found profiles as displayed in Figure 5., on various platforms including Instagram, Facebook, Twitter, YouTube, GooglePlus, Reddit, WordPress, GitHub, Tumblr, Flickr, Steam, Vimeo, SoundCloud, Disqus, Medium, DeviantART, VK, About.me, Imgur, Flipboard, SlideShare, MixCloud, Scribd, Patreon, BitBucket, DailyMotion, Etsy, CashMe, Behance, GoodReads, Instructables, Keybase, LiveJournal, AngelList, last.fm, Pastebin, Foursquare, Roblox, Gumroad, Newgrounds, Wattpad, Canva, CreativeMarket, Trakt, 500px, Buzzfeed, TripAdvisor, HubPages, Contently, Houzz, blip.fm, Wikipedia, HackerNews, CodeMentor, Designspiration, Bandcamp, ColourLovers, IFTTT, eBay, Slack, Ello, Tripit.
   Not found profiles on platforms like YouTube, Blogger, Fotolog, Spotify, Badoo, Kongregate, Dribbble, Codecademy, Gravatar, Foursquare, ReverbNation, OkCupid, Tracky, Basecamp.



```
[ ]  !bash userrecon.sh
```

```
                          v1.0, Author: @thelinuxchoice

[?] Input Username: Gudem Shruthika

[*] Checking username Gudem on:
[*] Checking username Shruthika on:
[+] Instagram:  Found! https://www.instagram.com/Gudem
 Found! https://www.instagram.com/Shruthika
userrecon.sh: line 53: $username.txt: ambiguous redirect
[+] Facebook:  Found! https://www.facebook.com/Gudem
 Found! https://www.facebook.com/Shruthika
userrecon.sh: line 66: $username.txt: ambiguous redirect
[+] Twitter:  Found! https://www.twitter.com/Gudem
 Found! https://www.twitter.com/Shruthika
userrecon.sh: line 79: $username.txt: ambiguous redirect
[+] YouTube:  Found! https://www.youtube.com/Gudem
```

Fig. 5. UserRecon

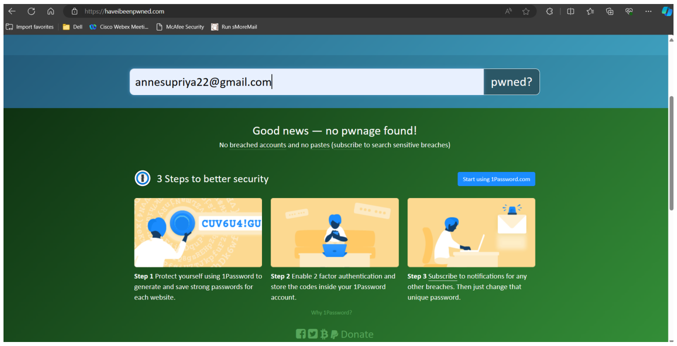
"userrecon" is designed for user reconnaissance in ethical hacking. It automates the process of searching for a specific username across various online platforms to gather information about the user's online presence as in Figure 5.

B. HaveIbeenPwned

"Have I Been Pwned?" (HIBP) is a widely used online service developed by security expert Troy Hunt. It allows users to check if their personal data is compromised in data breaches. Users can search for their email addresses or usernames on HIBP to check for data breaches. If a match is found, HIBP provides details about the breach, including the types of data compromised. One of the key features of HIBP is its vast database of breached data. Troy Hunt has collaborated with multiple organizations and security researchers to obtain and verify data from breaches, ensuring that the information provided by HIBP is accurate and up-to-date. The service includes data from both large-scale breaches involving millions of records and smaller, more targeted attacks. HIBP also offers a notification service, where users can subscribe to receive alerts if their email address appears in a future data breach. This proactive feature helps users stay vigilant and respond promptly to new threats. Additionally, HIBP provides a domain search feature, allowing domain owners to check if any email addresses associated with their domain have been compromised. This is particularly useful for organizations to monitor and protect their employees' data. The service also offers a monitoring feature that alerts users if their accounts appear in any future breaches. It also helps users take the necessary steps to secure their accounts and personal information in this increasing insecurity in the online environment.

Implementation Steps:

1) **Accessing the Website:**
   Users can visit the HIBP website at haveibeenpwned.com.



annesupriya22@gmail.com

pwned?

Good news — no pwnage found!

No breached accounts and no pastes (subscribe to search sensitive breaches)

3 Steps to better security

Start using 1Password.com

Step 1 Protect yourself using 1Password to generate and save strong passwords for each website.

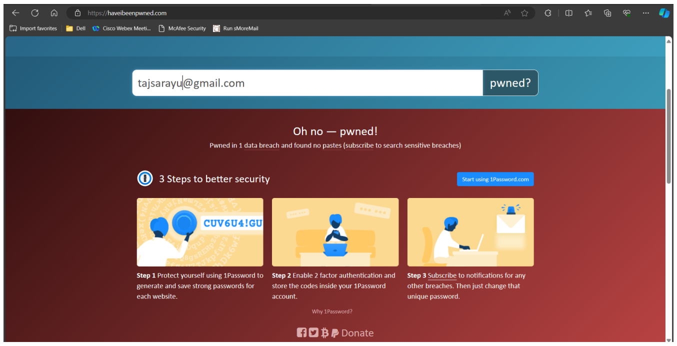
Step 2 Enable 2 factor authentication and store the codes inside your 1Password account.

Step 3 Subscribe to notifications for any other breaches. Then just change that unique password.

Why 1Password?

Donate

Fig. 6. No breaches found



tajsarayu@gmail.com

pwned?

Oh no — pwned!

Pwned in 1 data breach and found no pastes (subscribe to search sensitive breaches)

3 Steps to better security

Start using 1Password.com

Step 1 Protect yourself using 1Password to generate and save strong passwords for each website.

Step 2 Enable 2 factor authentication and store the codes inside your 1Password account.

Step 3 Subscribe to notifications for any other breaches. Then just change that unique password.

Why 1Password?

Donate

Fig. 7. Breaches found

2) **Check Email Addresses:**
   On the homepage, users can enter their email address in the search bar provided.
   After entering the email address, users click on the ”pwned?” button to initiate the search.
3) **Check Passwords:**
   HIBP also offers a feature called ”Pwned Passwords” where users can check if their passwords have been exposed in data breaches.
   Users can enter their password directly into the search bar to check if it has been compromised.

Results Steps:

1) **Email Address Search Results:**
   If no pwnage is found as shown in Figure 6., for the entered email address, HIBP indicates that there are no breaches.
   If the email address has been found in a breach as in Figure 7., HIBP provides information about the breach(es) it was involved in, along with the number of occurrences.
2) **Password Search Results:**
   When checking passwords, HIBP indicates if the password was exposed in a data breach.
   If the password has been previously exposed, users are advised to set a new strong and unique password instead.
3) **Security and Privacy:**
   HIBP prioritizes user privacy and does not store logs of any email addresses or passwords entered into the site.
   Users can check their credentials without fear of exploitation, as the website does not store sensitive information.
   HIBP operates transparently and is trusted within the cybersecurity community.

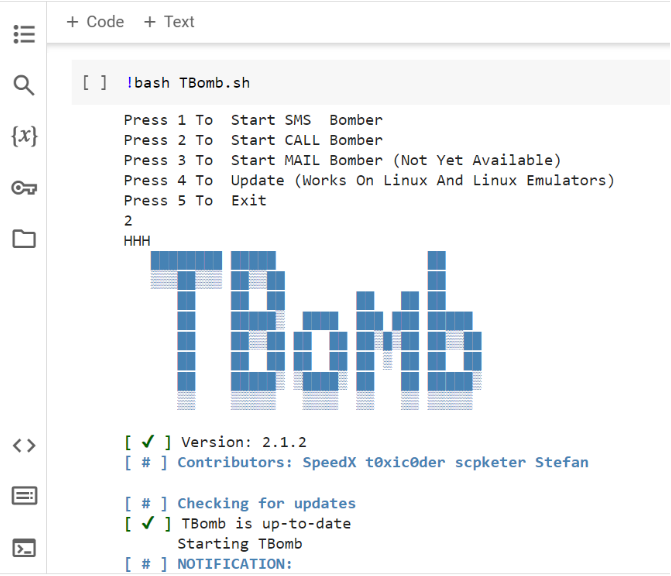
By utilizing HIBP, users can proactively monitor their online accounts for potential security risks and take necessary steps to safeguard their digital identities.

C. TBomb

TBomb is a Python-based SMS and Call bombing tool designed for educational and testing purposes, it was developed to assess the vulnerabilities of telecom services. It helps security enthusiasts with a powerful tool to understand the potential risks associated with SMS and call flooding. Using TBomb users can flood targets with a huge number of messages and phone calls. This tool supports multiple service providers and is capable of sending a high volume of messages or making repeated calls to a target phone number. During the bombing process, TBomb displays real-time updates in the terminal, showing the number of successful deliveries and failed attempts which allows the user to monitor the progress. However, it’s essential to use TBomb responsibly and ethically. These attacks can be used to overwhelm a user’s device, consume their message or call limits, and potentially lead to financial losses if the messages or calls incur charges. While TBomb demonstrates the ease with which these attacks can be carried out, its primary purpose is to educate users about the threats and encourage the development of better security measures. TBomb is equipped with several features that make it versatile and effective for testing purposes. It supports multiple APIs for sending messages and making calls, allowing users to simulate attacks from various sources. The tool also provides options for customizing the number of messages or calls and the interval between them, giving users control over the intensity of the simulation. Additionally, TBomb includes features to randomize the sender information, making the attack appear more realistic. Using TBomb, cybersecurity professionals can test the resilience of telecommunication systems and services against SMS and call bombing attacks. This can help identify weaknesses in these systems and provide insights into how they can be fortified. It serves as an educational tool that helps users understand the importance of security measures in telecommunication systems and encourages the development of better security to mitigate such attacks.

Implementation Steps:

1) **Clone the Repository:**
   Clone the TBomb repository from GitHub: git clone https://github.com/TheSpeedX/TBomb.git
2) **Install Git using the following command (if not already installed):**
   sudo apt install git
3) **Navigate to the TBomb Directory:**
   Change the directory to the TBomb folder: cd TBomb
4) **Run the Script:**



```
[ ]  !bash TBomb.sh

Press 1 To  Start SMS  Bomber
Press 2 To  Start CALL Bomber
Press 3 To  Start MAIL Bomber (Not Yet Available)
Press 4 To  Update (Works On Linux And Linux Emulators)
Press 5 To  Exit
2
HHH

[ ✓ ] Version: 2.1.2
[ # ] Contributors: SpeedX t0xic0der scpketer Stefan

[ # ] Checking for updates
[ ✓ ] TBomb is up-to-date
      Starting TBomb
[ # ] NOTIFICATION:
```

Fig. 8. TBomb

Execute the TBomb script using the bash command: bash TBomb.sh, shown in Figure 8.

Results Steps:

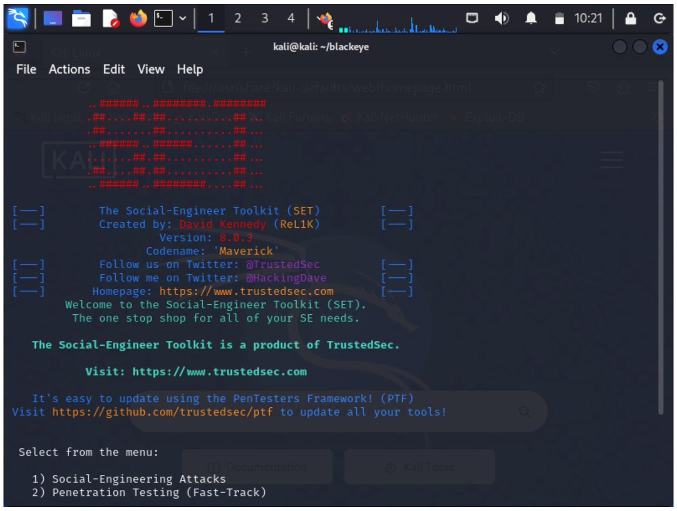
1) **Bombing Progress:**
   The script initiates the bombing process and displays the progress.

During the bombing process using TBomb, the script displays progress details in the terminal window. It shows the target phone number, the number of messages sent, the number of successful deliveries, and the number of failed attempts and the outcome of each attempt. For instance, it reveals the number of successful deliveries and the number of failed attempts. This real-time feedback allows users to monitor the progress of the bombing campaign effectively.

D. Setoolkit

The Social Engineer Toolkit (SET) is an open-source toolkit widely used for penetration testing and social engineering attacks. It provides a comprehensive suite of tools and modules that automate the process of crafting and executing social engineering attacks. One of the SET's standout features is its ability to create fake login web pages or phishing pages. They are designed to mimic legitimate login screens for popular services, tricking users into disclosing their credentials. SET simplifies the process of setting and deploying fake login pages, allowing professionals to assess the vulnerability of systems and educate users about the dangers of social engineering attacks. Beyond phishing, SET offers a range of other tools and techniques for testing and enhancing security measures, making it an invaluable resource for ethical hackers, security researchers, and penetration testers. Its user-friendly interface and its powerful functionality made it a popular choice for cybersecurity professionals

Implementation Steps:



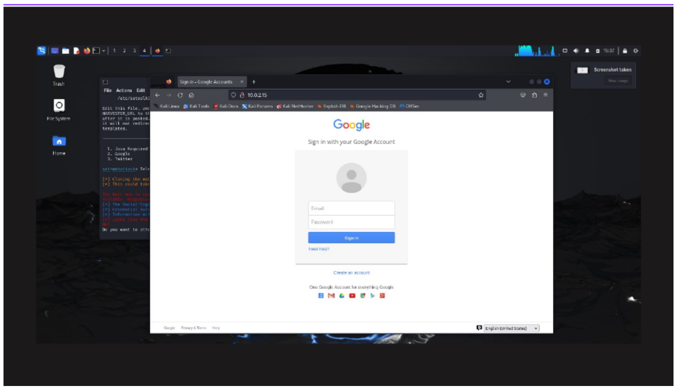
```
        ..######..########.########
        .##....##.##..........##...
        .##.......##..........##...
        ..######..######......##...
        .......##.##..........##...
        .##....##.##..........##...
        ..######..########....##...

[---]        The Social-Engineer Toolkit (SET)        [---]
[---]        Created by: David Kennedy (ReL1K)        [---]
                      Version: 8.0.3
                    Codename: 'Maverick'
[---]        Follow us on Twitter: @TrustedSec        [---]
[---]        Follow me on Twitter: @HackingDave       [---]
[---]       Homepage: https://www.trustedsec.com      [---]
        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
```

Fig. 9. Setoolkit

1) **Installation:**
   You can install SET on your system by cloning its GitHub repository or downloading it from the official website.
2) **Clone the GitHub repository:**
   git clone https://github.com/trustedsec/social-engineer-toolkit.git
   Follow the instructions provided in the README file for installation.
3) **Launch SET:**
   After installation, navigate to the SET directory and launch it using the command: cd social-engineer-toolkit sudo ./setoolkit
4) **Selecting Attack Vector:**
   Once SET is launched, you'll be presented with a menu of attack vectors as shown in Figure 9. Choose the appropriate option for creating a fake login page. This often involves selecting the ”Website Attack Vectors” option.
5) **Creating a Phishing Page:**
   Depending on the version of SET and its updates, you may find specific modules or options for creating fake login pages. Look for modules like ”Site Cloner” or ”Credential Harvester.”
6) **Configuring the Attack:**
   Follow the prompts to configure the attack, including selecting the website to clone, customizing the appearance of the phishing page, and setting up where the captured credentials will be stored.
7) **Deploying the Phishing Page:**
   After configuring the attack, SET will generate the phishing page. You can then deploy this page by hosting it on a web server or using other methods to make it accessible to your targets.

Results Steps:

1) **Captured Credentials:**



```
/etc/setoolki
Edit this file, and
HARVESTER_URL to th
after it is posted.
it will not redirec
templates.

  1. Java Required
  2. Google
  3. Twitter

set:webattack> Sele

[*] Cloning the web
[*] This could take

[*] The Social-Engi
[*] Credential Harv
[*] Information wil
[*] Looks like the
Do you want to atte
```

Fig. 10. Fake login web page

As users interact with the fake login page as in Figure 10., and submit their credentials, SET will capture this information and store it in the specified location. You can access the captured credentials for analysis and further exploitation.

VIII. Acknowledgment

Firstly, we would like to express our gratitude to Ms. Kiranmaie Puvulla, department of IT, our guide. She was a continual source of inspiration for us, and we were able to successfully complete this project thanks to her extensive knowledge, substantial experience, and skill with deep learning. We would especially want to express our gratitude to Dr. Rajanikanth Aluvalu, Head of the Department of Information Technology, whose guidance, constant support, and inspiration helped us turn our idea into a reality. We appreciate all of the comforts and help that our esteemed principal, Dr. C.V. Narasimhulu, has provided for us. We also wish to express our gratitude to the entire information technology department staff for their excellent help and sage advice. Lastly, we would like to express our gratitude to all of our friends and family for their unwavering support and enthusiastic encouragement.

IX. Conclusion

Ethical hacking is a dynamic and rapidly growing field, and staying updated about the latest tools, techniques, and best practices is essential to succeed in this field. By utilizing the tools, books and websites mentioned in the paper, one can improve their skills and knowledge in ethical hacking and can contribute to safeguarding the digital world. The demand for skilled ethical hackers is growing with growing cyber threats. Organizations around the world started recognizing the importance of cybersecurity and started investing in proactive measures to protect their confidential data and assets. Ethical hackers or white-hat hackers play a crucial role in this process by helping organizations identify and mitigate potential security risks before they can be exploited by malicious hackers. It is important for ethical hackers to possess strong problem-solving skills, pay attention to details and have a solid understanding of ethical principles and legal regulations along with technical skills. Ethical hackers must continuously learn and adapt to new challenges to stay ahead of emerging threats and effectively protect the integrity and security of digital systems and networks. In conclusion, ethical hacking offers a rewarding and challenging career path for individuals passionate about cybersecurity. By mastering the tools, techniques, and best practices outlined in this paper, ethical hackers, aspiring to develop their skills and knowledge will succeed in this exciting and rapidly growing field.

X. Future Scope

The future scope for ethical hacking tools is vast and continually evolving to address the complexities of modern cybersecurity threats. As cyber-attacks become more sophisticated, the need for advanced tools and methodologies grows. Future developments will likely focus on incorporating artificial intelligence and machine learning to automate and enhance the detection, analysis, and mitigation of security vulnerabilities. These advancements will enable tools like Nmap, Wireshark, and Metasploit to offer more precise and timely insights, making it easier for ethical hackers to identify potential threats in real-time. Additionally, there will be a concerted effort to expand the functionality and interoperability of these tools, ensuring seamless integration within various cybersecurity ecosystems and continuous integration/continuous deployment (CI/CD) pipelines. This integration will be crucial for maintaining robust security postures across diverse and distributed network environments.

Moreover, the scope of these tools will extend beyond traditional IT infrastructures to encompass emerging technologies such as IoT, cloud computing, and quantum computing. Tools like Aircrack-ng, Hashcat, and Shodan will be enhanced to address the unique security challenges posed by these technologies. There will also be significant advancements in social engineering tools, with platforms like SocialPhish and SEToolkit incorporating more sophisticated attack simulations and training modules to better prepare organizations against human-factor vulnerabilities. Furthermore, educational platforms like Hack The Box will evolve to provide more realistic and complex training environments, leveraging AI to tailor challenges to individual skill levels and fostering a more adaptive learning experience. Overall, the future of ethical hacking tools will be marked by greater automation, integration, and specialization, ensuring that ethical hackers are well-equipped to protect against the ever-changing landscape of cyber threats.

References

[1] Farsole, Ajinkya A., Amruta G. Kashikar, and Apurva Zunzunwala. ”Ethical Hacking.” *International Journal of Computer Applications*, 1(10): 14–20, February 25, 2010. http://dx.doi.org/10.5120/229-380.

[2] Gaia, J., Sanders, G. L. ”Psychological Profiling of Hacking Potential.” *Journal Name*, 3, 2230–2239, 2020.

[3] Thomas et al., 2019]thomas2019importance Thomas, G., Burmeister, O., Low, G. (2019). ”The Importance of Ethical Conduct by Penetration Testers in the Age of Breach Disclosure Laws.” *Australasian Journal of Information Systems*, 23, 1–14.

[4] Babbar, Sahil, Rachit Jain, and Jinkeon Kang. ”Ethical Hacking.” *Research Gate*, 2015. Accessed on 14 Dec. 2018. https://www.researchgate.net.

[5] Munjal, Meenaakshi N. ”Ethical Hacking: An Impact on Society.” 7.1 (2013): 922-931. Web. Accessed on 14 Dec. 2018.

[6] ”Summarizing The Five Phases Of Penetration Testing - Cybrary.” Cybrary. N.p., 2015. Web. Accessed on 14 Dec. 2018.

[7] “Is Ethical Hacking Ethical?,” Int. J. Eng. Sci. Technol., 2011.

[8] P. Engebretson, “Reconnaissance,” in *The Basics of Hacking and Penetration Testing*, 2011.

[9] Floyd, K., Harrington, S., & Hivale, P. (2007). The autotelic propensity of types of hackers. In *Proceedings of the 4th Annual Conference on Information Security Curriculum Development - InfoSecCD ’07*.

[10] Simpson, M. T., Backman, K., & Corley, J. E. (2013). *Hands-on Ethical Hacking and Network Defense*. Boston, MA: Cengage Technology.

[11] Palmer, Charles. Ethical Hacking. Published in IBM Systems Journal: End-to-End Security, Volume 40, Issue 3, 2001.

[12] Juneja, Gurpreet K. ”Ethical hacking: A technique to enhance information security.” International Journal of Computer Applications, vol. 2, Issue 12, December 2013.

[13] Lucas, G. R. ”Cyber warfare.” In *The Ashgate Research Companion to Military Ethics*, 2016.

[14] Thomas, G., Burmeister, O., Low, G. ”The Importance of Ethical Conduct by Penetration Testers in the Age of Breach Disclosure Laws.”

[15] Brenner, W. Susan. (2010). Cybercrime: Criminal Threats from Cyberspace. Westport: Greenwood Publishing Group.

[16] Gupta, Aman, and Anand Abhineet. ”Ethical Hacking and Hacking Attacks.” International Journal of Engineering And Computer Science 6.4 (2017).

[17] Chowdappa, Bala K., Lakshmi Subba S. P.N.V.S., and Kumar Pavan. ”Ethical Hacking Techniques with Penetration Testing.” International Journal of Computer Science and Information Technologies 5.3 (2014).

[18] Kumar, Sunil, and Dilip Agarwal. ”Hacking Attacks, Methods, Techniques And Their Protection Measures.” International Journal for Science and Advance Research in Technology 4.4 (2018): 2253–2257.

[19] Sinha, Shivanshi, and Dr. Yojna Arora. ”Ethical Hacking: The Story of a White Hat Hacker.” International Journal of Innovative Research in Computer Science Technology 8.3 (2020): 131-136.

[20] Iyer, Shweta. ”Learning Ethical Hacking Can Be A Disaster If You Neglect These 7 Rules.” Knowledge Hut, 19 Apr. 2021, https://www.knowledgehut.com/blog/security/learning-ethical-hacking-can-be-a-disaster-if-you-neglect-these-7-rules.