CyberPeace editor@cyberpeace.net

THE CYBERPEACE JOURNAL

Supported by United Service Institution of India

Academic Partner Shah & Anchor Kutchhi Engineering College

CYBERNEX: Offensive Security Multi-Tool

Shubham Kolaskar
Cybersecurity
Shah and Anchor Kutchhi Engineering College
Mumbai, India
shubham.17280@sakec.ac.in

Karan Parelkar
Cybersecurity
Shah and Anchor Kutchhi Engineering College
Mumbai, India
karan.17323@sakec.ac.in

Dr. Shwetambari Borade
Cybersecurity
Shah and Anchor Kutchhi Engineering College
Mumbai, India
shwetambari.borade@sakec.ac.in

Abhimod Bhatkar
Cybersecurity
Shah and Anchor Kutchhi Engineering College
Mumbai, India
abhimod.17395@sakec.ac.in

Devansh Sanghvi
Cybersecurity
Shah and Anchor Kutchhi Engineering College
Mumbai, India
devansh.17398@sakec.ac.in

***Abstract*— Cybersecurity professionals are bifurcated into two significant teams i.e., the RED TEAM & BLUE TEAM. . In the context of Blue Team, the focus shifts to filtering alerts from SIEM software and to configure firewalls, EDR solutions & conducting forensic examinations etc. Red team professionals must deal with a lot of data and raw information while conducting operations. In such a scenario one must deal with multiple tools and terminal windows. This process is quite cumbersome and has avenues ripe for operator error and hence can prove to be major roadblocks during a pen-test operation. To cater to this issue and automate tasks for a red team operator, this research proposes CYBERNEX: Offensive Security Multitool to mitigate the issues encountered by Red Team Operators.**

Keywords — Cyber Security, Hacking, Red Team, Automation, Ease of Access, Penetration Testing, Mitigation, Offensive Security

I. INTRODUCTION

R. Chivukula, T. Jaya Lakshmi, L. Ranganadha Reddy, Kandula and K. Alla [1] suggest that Cybersecurity red team operations are a critical component of assessing and enhancing an organization's security posture. Red teams are groups of skilled professionals who simulate cyberattacks and other security threats to help organizations identify vulnerabilities and weaknesses in their defenses. Red team operations can be thought of as the "offensive" side of cybersecurity. Red Team operations are very long and intensive. They include various information gathering and analysis aspects. The part of implementing attack vectors, determination of attack surfaces also comes into play. During such operations the time factor of the attacks is also very crucial. The attacks and objectives are very dynamic and ever-changing. This research that we have conducted will aid red team operators to effectively focus on their crucial objectives and help them with timeline and automation tasks. The process of an External Pen-Test can last up to 32 Hours depending upon the size and scope of the ROE (Rules of Engagement) given by the client organization.

II. OBJECTIVES

The objectives of the research on effectiveness of offensive security multi-tools are as follows:

A. *Testing and Demonstrating Security Weaknesses*: Security flaws are tested and illustrated using offensive security techniques. They assist in locating weak points and openings in your system, which raises the possibility of ransomware, data breaches, and other harmful assaults.

B. *Knowing Capabilities*: It will be helpful for systems administrators and other IT specialists to know what these technologies are capable of. This entails knowing how to prevent these kinds of assaults as well as how attackers might use system flaws.

C. *Sustaining a Robust Security Posture*: To safeguard your company against dangers, preserve a robust security stance, and reduce risk, it is essential to test your setup using the appropriate offensive security tools.

D. *Evaluating Security Protocols, Guidelines, and Measures*: Penetration testing is a component of offensive security that teaches IT and cybersecurity personnel how to handle potential breaches before they happen and evaluates the efficacy of the organization's security policies, processes, and controls. Automating Security

Operations: These tools also save precious time by automating various security operations. For instance, they can detect vulnerable endpoints in the network, review source code, web applications, network security architecture, and find solutions to mitigate potential cybersecurity threats.

III. LITERATURE SURVEY

S. Kraemer, P. Carayon, and R. Duggan [2] discusses the need of firm frameworks in place for red team audits. Security audits' primary goals are to inspect and evaluate computer systems, the overall system of its component pieces as well as a company's operating practices. With it, one needs to identify gaps and develop proposals on how to organize for the implementation of remedy strategies. In the detection stage, the identified team will look for gaps in the existing protective mechanisms, opportunities for the development of new or alteration of existing policies and see whether staff ought to be trained on new tactics. Identifying primary and secondary objectives is one of the many operational procedures that make up the security audit process because the results must be known. The organization's purpose then synchronizes the evaluation framework; this includes the people involved in the review and the timing of the review; this comprises the personal systems included in the audit and the duration of the audit. From there, we come to learn that knowledge acquired by red teams is particularly useful in cases where the target system is relatively young, and designers can make changes easily. The abovementioned red team strategy is based on the belief that an analyst can find inherent vulnerabilities in a computer and information system that he or she would not see if attempts to directly imitate an adversary. Thus, for conducting a successful assault, they seek ways and means to compound the system, organizational, and architectural weaknesses. An important point that a red team makes is the vulnerabilities and gaps in the systems of computer and information protection. The concept of red teams and the practice often referred to as 'ethical hacking' are the crucial preventive measures in revealing system flaws and thus improving security since it gives the side of defenders an insight into the perception of an attacker.

C. Peake [3] highlights that, we are aware that the Infosec process's assessment step includes Red Teaming. Before putting in place the necessary security controls, security experts must assess the system's or network's risk. Threats and vulnerabilities must be to calculate risk. Depending on the extent of the assessment that the customer has requested, the Red Team can project potential threats and use technologies to look for vulnerabilities. Red Teaming, on the other hand, takes a more thorough approach than most would-be attackers do because, to evaluate the risk involved, security experts must identify every potential vulnerability for a given system, whereas would-be attackers only need to locate one. To increase the probability of undetected exploitation, the attacker targets a single vulnerability to a specific attack and with increased attempts on probing for vulnerabilities more chances are that the attacker's activities will be noted. Because the red teaming should assess against all types of threats, the following should be discovered: denial of service, access, modification, and repudiation. Conclusively, a clear understanding of the status of a concrete system or network's security should be gained through the assessment given by the Red Team. However, risk identification by means of Red Teaming and other methods cannot by itself deliver information security; the company/organization must go on through the Infosec process to be able to adequately manage risk and deliver security protection.

H. Taherdoost [4] highlights that, cybersecurity standards are primarily intended to avoid or lessen cyberattacks and lower the likelihood of cyberthreats. Time will be saved, expenses will drop, earnings will rise, user awareness will increase, risks will be reduced, and business continuity will be provided by the adoption of standards. Using standards also makes it easier for a company to adhere to industry best practices and processes and gives international comparison of security systems possible. In order to safeguard assets against cyber threats, some organizations and enterprises have adopted cyber security standards. Because of this, some corporations have created distinct cyber security standards to guarantee that businesses of all sizes and types take the necessary precautions to avoid and lessen cyber risks. However, as various standards have been developed across organizations to cover various aspects of cybersecurity, it can be difficult for business owners to choose the standards that are right for their business.

K. Pelechrinis, M. Iliofotou and S. V. Krishnamurthy [5] states that, wireless networks are becoming increasingly prevalent, and with this growth comes a rise in security concerns. One threat is denial-of-service (DoS) attacks, which aim to disrupt or disable legitimate network communication. In the context of wireless networks, these attacks are often referred to as Wireless DoS (WDoS) attacks. Jamming is a common technique used in WDoS attacks. Jammers are malicious devices that transmit radio signals that interfere with legitimate communication, effectively preventing devices from connecting or exchanging data. The shared nature of the wireless medium makes it easier to launch jamming attacks compared to wired networks. Attackers can exploit this by flooding the channel with interference, making it impossible for legitimate devices to communicate. Jamming techniques can range from simple continuous transmissions to more sophisticated methods that target specific protocols or exploit vulnerabilities in communication channels.

L. Cheng, F. Liu, and D. D. Yao [6] infers that identity theft is a major concern for most businesses mainly because of the massive amount of data that most enterprises store and the enhanced and frequent attempts by hackers. Based on this article, the following are the examined reasons, problems, prevention approaches, and vision of the further development in the sphere of the enterprise DLPD. Outdated systems, inadequate access controls, vulnerabilities in software, and lack of network segmentation can create entry points for attackers. Unskilled or negligent employees can

accidentally expose data through phishing attacks, weak passwords, or improper data handling procedures. Disgruntled employees or malicious actors with authorized access can intentionally steal or leak sensitive data. Attackers constantly develop new techniques, making it difficult to stay ahead of the curve. The vast amount and diverse nature of enterprise data make it challenging to identify and protect all sensitive information. Implementing stringent security measures can hinder employee productivity and user experience.

IV. METHODOLOGY

The implementation of the multitool is done in the bash shell. This tool is designed to run within a CLI environment. The ideal Operating System is Kali Linux which is a Debian-64 based Linux Distribution. Also, we need a NIC (Network Interface Card) with wireless capabilities to access the wireless exploitation tools. Also, python needs to be installed on the system because many of the tools aggregated in the multitool are designed on python-based scripts. The Bash environment, A strong and popular command-line interface (CLI) for Unix and Unix-like operating systems is called "Bourne Again Shell." As a text-based interface, it provides an opportunity to interact with the operating system which can be used for execution of different commands and scripts. Here's a closer look at the Bash environment and its key features. Command Execution: Bash provides a means to execute commands by typing them into the terminal. Users can launch system utilities, run scripts, and control various aspects of the operating system using simple commands. It acts as a bridge between the user and the underlying system. Scripting: One of the most significant strengths of Bash is its scripting. Bash is highly customizable. Users can define aliases, functions, and configure environment variables to personalize their command-line experience. This flexibility makes it a favorite among power users and system administrators. Bash keeps a command history, enabling users to recall and reuse previously executed commands. This feature is useful for both repetitive tasks and troubleshooting.

After getting into the command line interface of our distro we can start setting up the tool and importing the core python files and the Python3 Env package. The CLI then is converted into a Root terminal as we need administrative privileges to execute the commands and install packages, clone repositories.

Once the script is installed the following requirements are installed into the system: flask, boxes, lolcat, requests etc. The tools directory houses the different assortment of penetration testing tools available into the framework. If a user wants to install a tool, the python functions into the core script get activated and pull an image of the tool from their source. So instead of manual installation we can have all the required tools in the playbook at our fingertips.

In the Menu we have a variety of suggested options along with their descriptions and repositories attached to them.

1. Information Gathering
2. Wordlist Generators
3. Phishing Tools
4. Web Exploitation
5. Forensics
6. SQL Injection Tools
7. XSS Attack Tools
8. Wireless Attack Utilities
9. Social Media Reconnaissance Tools

All the options are easily accessible, and they are programmed to have their own separate menus. It is very simple and intuitive to use and maintain over time.

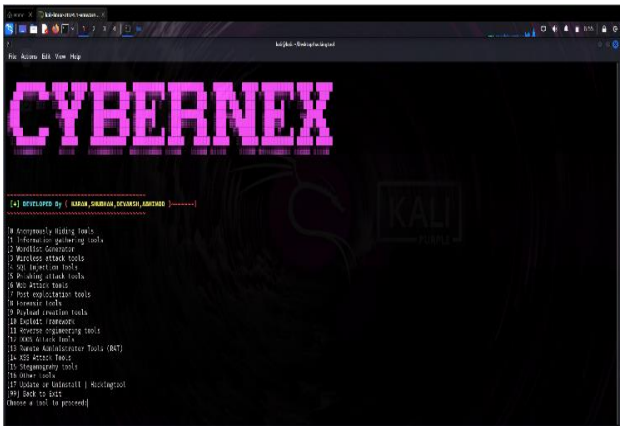

Fig. 5.1 Homepage

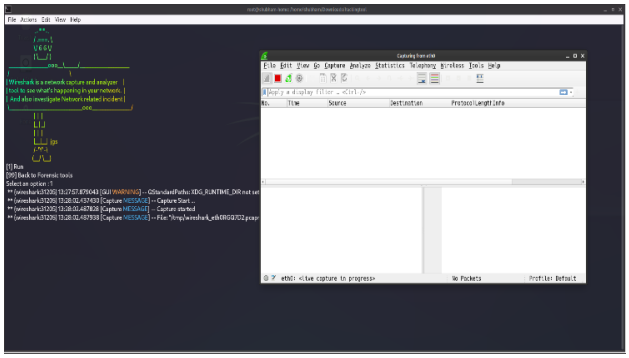

Fig 5.2 Embedded Wireshark Utility

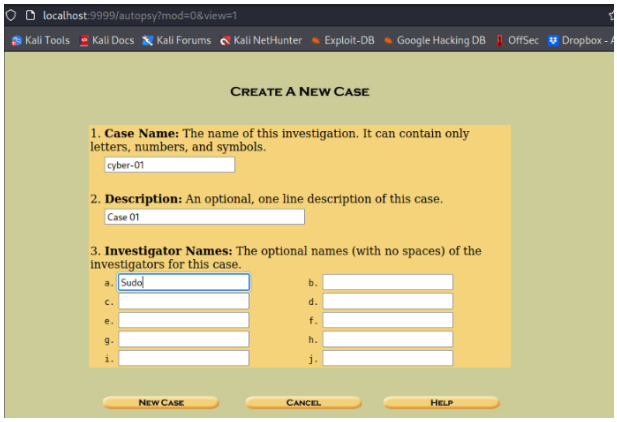

Fig. 5.3 Autopsy Forensics Platform

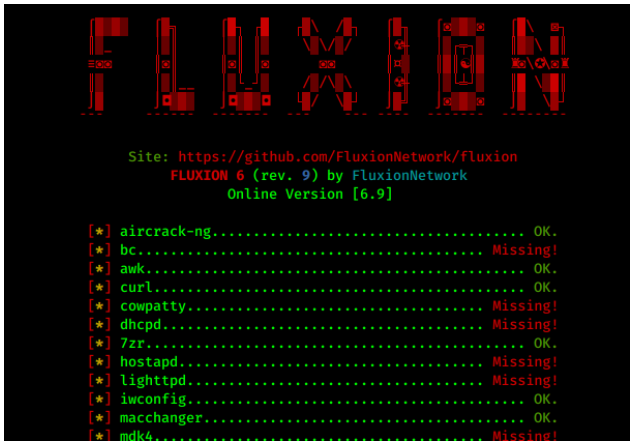

Fig. 5.4 Fluxion Wireless Exploitation Suite

AKNOWLEDGEMENT

The Completion of this research would not have been possible without the mentorship and guidance of several individuals. We would like to express my sincere gratitude to our mentor, Dr. Shwetambari Borade and Dr. Nilakshi Jain, Head of Cybersecurity Department for their constant support and insightful feedback thought this research. Also, we are grateful to Dr. Bhavesh Patel, Shah and Anchor Kutchhi Engineering College for his unwavering support and for providing the resources necessary to conduct this research.

REFERENCES

[1] S. Kraemer, P. Carayon, and R. Duggan, "Red Team Performance for Improved Computer Security," *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 48, no. 14, pp.1605–1609, Sep. 2004, doi: https://doi.org/10.1177/154193120404801410.

[2] A.-D. Tudosi, A. Graur, D. G. Balan, and A. D. Potorac, "Research on Security Weakness Using Penetration Testing in a Distributed Firewall," *Sensors*, vol. 23, no. 5, p. 2683, Mar. 2023, doi: https://doi.org/10.3390/s23052683.

[3] C. Peake, "'Red Teaming: the Art of Ethical Hacking,'" *https://www.sans.org/white-papers/*, 2003. https://www.sans.org/white-papers/1272/

[4] H. Taherdoost, "Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview," *Electronics*, vol. 11, no. 14, p. 2181, 2022, doi: https://doi.org/10.3390/electronics11142181.

[5] K. Pelechrinis, M. Iliofotou and S. V. Krishnamurthy, "Denial of Service Attacks in Wireless Networks: The Case of Jammers," in IEEE Communications Surveys & Tutorials, vol. 13, no. 2, pp. 245-257, Second Quarter 2011, doi: 10.1109/SURV.2011.041110.00022.

[6] L. Cheng, F. Liu, and D. D. Yao, "Enterprise data breach: causes, challenges, prevention, and future directions," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 7, no. 5, p. e1211, 2017, doi: https://doi.org/10.1002/widm.1211