INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact Factor: 6.078
(Volume 7, Issue 4 - V7I4-1227)
Available online at: https://www.ijariit.com

Menu-based Penetration Testing and Vulnerability Assessment

A. N. Anshuman
anshumanan.17cs@saividya.ac.in
Sai Vidya Institute of Technology, Rajanukunte, Karnataka

Abhinandan C.
abhinandanc.17cs@saividya.ac.in
Sai Vidya Institute of Technology, Rajanukunte, Karnataka

Suraj Upadhya G.
surajupadhyag.17cs@saividya.ac.in
Sai Vidya Institute of Technology, Rajanukunte, Karnataka

Thanushree C.
thanushreec.17cs@saividya.ac.in
Sai Vidya Institute of Technology, Rajanukunte, Karnataka

Kishore S. Verma
kishoreverma.s@saividya.ac.in
Sai Vidya Institute of Technology, Rajanukunte, Karnataka

ABSTRACT

The systems and networks run by an individual or an organization are prone to get exploited by hackers for personal gains or any other motive. The flaws or loopholes in the operating systems or operating procedures and practices may lead to a stage where once they are compromised; there is no going back beyond that point. This is a serious issue that must be rectified and safety measures must be inculcated in the operations. The systems and networks in use must be thoroughly checked for vulnerabilities to ensure protection. This is a required objective in every system and every organization. The project that we are working on is a menu based vulnerability assessment and penetration testing tool that checks the selected system or network and tries to find the most common and most complex risks associated in the system or network. The tool is called EDITH, which stands for "Executable and Distinguished Interface to Hack". This tool simplifies the process by allowing the authorized user to choose from the options provided. The simplicity of the tool is what makes it idiosyncratic in the field of penetration testing and risk analysis. The tool is built using advanced python modules that support kernel and terminal level of access and operation rights. The tool provides a wide range of options to check vulnerabilities and perform penetration testing on the selected system or networks. The options are categorised into network related tests and system related tests. The tool is capable of performing penetration tests from a low security system to a highly secured firewall-built system. The tests performed by the tool are completely ethical and do not void any laws unless they are used for illegal purposes. This is a brief description of our project.

Keywords: *Vulnerability, Penetration Testing, Analysis, Menu-Based Vulnerability Assessment.*

1. INTRODUCTION

The systems and networks run by an individual or an organization are prone to get exploited by hackers for personal gains or any other motive. The flaws or loopholes in the operating systems or operating procedures and practices may lead to a stage where once they are compromised; there is no going back beyond that point. This is a serious issue that must be rectified and safety measures must be inculcated in the operations. The systems and networks in use must be thoroughly checked for vulnerabilities to ensure protection. This is a required objective in every system and every organization.

The proposed system is a menu-based vulnerability assessment and penetration testing tool that checks the selected system or network and tries to find the most common and most complex risks associated in the system or network. The tool is called EDITH, which stands for "Executable and Distinguished Interface To Hack". Most vulnerability checks and analysis are performed by cyber security experts. This tool simplifies the process by allowing the authorized user to choose from the options provided.

The simplicity of the tool is what makes it idiosyncratic in the field of penetration testing and risk analysis. he tool is built using advanced python modules that support kernel and terminal level of access and operation rights.

The tool provides a wide range of options to check vulnerabilities and perform penetration testing on the selected system or networks. The options are categorised into network related tests and system related tests. The tool is capable of performing penetration tests from a low security system to a highly secured firewall-built system. The tests performed by the tool are completely ethical and do not void any laws unless

they are used for illegal purposes. This is a brief description of our proposed system.

2. LITERATURE SURVEY

[1] Ravindranath Kongara, "vSTAAS - an Integrated Pen-Testing Tool", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-9 Issue-2, December, 2019: this paper offers Strong, actionable intelligence with RPA, Machine Learning, and AI Automation concerning security requirements across the SDLC.

[2] Zoran ĐURIĆ, "WAPTT - Web Application Penetration Testing Tool", Advances in Electrical and Computer Engineering 14(1):93-102: this paper proposed a modular, easily extended by end-user efficient algorithm for page similarity detection with promising results.

[3] Christian Mainka, Juraj Somorovsky, J¨org Schwenk, "Penetration Testing Tool for Web Services Security", June 2012: this paper proposes an overview of their design decisions and provides evaluation of four Web Service frameworks and their resistance against WS-Addressing spoofing and SOAPAction spoofing attacks.

[4] Aruna Pavate, Pranav Nerurkar, "Performance Analysis of Cloud Based Penetration Testing Tools", International Journal of Engineering Research & Technology (IJERT) Vol. 3 Issue 2, February: this paper provides detailed information and analysis of tools and their performance and accuracy , the result can be used to understand the best tool for penetration testing.

[5] Monika Pangaria, Vivek Shrivastava, Archita Bhatnagar, "Comparative Study of Web Application Penetration Testing Tools ", International Conference on Electrical, Electronics and Computer Science (ICEECS): this paper mainly focuses on Accunetix and w3af and comparing them against few vulnerabilities and distinguishing the features of the two and choosing the tools based on users need.

[6] Aparicio Carranza, Daniel Mayorga, Casimer DeCusatis, Hossein Rahemi, "Comparison of Wireless Network Penetration Testing Tools on Desktops and Raspberry Pi Platforms", this paper investigates three popular open source wireless penetration testing tools (Aircrack –ng, Reaver, and Kismet) and compare their behavior on a traditional desktop computer and a Raspberry Pi model 3.

[7] Palak Aar, Aman Kumar Sharma, "Analysis of Penetration Testing Tools", International Journals of Advanced Research in Computer Science and Software Engineering(Volume 7,Issue-9): this paper provides an overview and comparisons on various penetration testing tools providing the result in terms of graphs and tables.

[8] Mubarak Albarka Umar, Chen Zhanfang, "A Study of Automated Software Testing: Automation Tools and Frameworks", this paper presents a comprehensive study of test automation tools and frameworks.

3. SYSTEM DESIGN

Some of the tools used to test the platform are N-map, BeEF, etc. Once we acquire the report from different tools, we choose the tool which is much more appropriate. We can find the efficiency of the tool by using different attack vectors to evaluate the platform's security level. We use distinguished tools for each application or category to evaluate the risk factors involved with it. Once we choose the appropriate tool, we can carry out the test using that tool to avoid the risk of system or network from getting compromised.

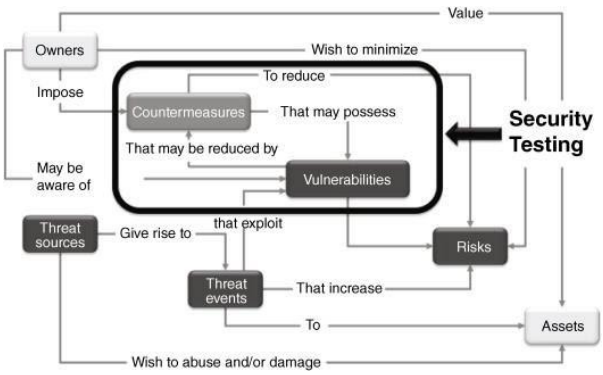


Fig 3.1: System Design

4. PROPOSED SYSTEM

The modules in the project have been implemented based on various cyber security categories and sub-modules with extended functionalities. The various modules are System modifications, Website testing, Network testing, Network testing, Sniffing and Spoofing, Information Gathering, Database Attacks, Password Cracking Attacks and Reverse Engineering tools.

The System modification is used to modify the system settings in order to maintain anonymity over the internet and stay secure. Modification or alteration, an unauthorized change of information, covers three classes of threats. The goal may be deception, in which some entity relies on the modified data to determine which action to take, or in which incorrect information is accepted as correct and is released. The options available are MAC Change to Random Address and MAC Change to Permanent Address.

The Website Testing may be a sub-type of computer code testing that involves characteristic risks, threats, and vulnerabilities in an application. The aim of this testing is to stop cybercriminals from infiltrating websites and launching malicious attacks. The options available are Website Information Gathering; Website Vulnerability Assessment and DDoS. We use Nmap, Dirb and Zenmap for the above options.

Network Testing is an associate degree investigation conducted to produce stakeholders with knowledge regarding the quality of the merchandise or service at a lower place they take a look at. Network testing can also supply academic degree objectives, freelance reading of the network to allow the business and perceive the risks of network implementation. The options available are Wi-Fi hacking which uses Wifite; Nmap for Network Monitoring and Aircrack-ng for Network De-authentication.

Sniffing is employed by hackers either to induce info directly or to map the technical details of the network so as to form an extra attack. The options available are Man-in-the-Middle attack which uses mitmf tool that intercepts the users and acts as the mediator to modify or steal the information; Browser exploitation framework using BeEF that remotely exploits a user's browser just by making them to click a link. Information Gathering is the act of gathering different kinds of information against the targeted victim or system. The more the information gathered about the target, the more the probability

to obtain relevant results. Information can be gathered from search engines, social networks, Domain names and Web servers. The options available are Username Database Collection using Sherlock which searches for specified username in a huge number of websites and collects the URL if it finds a hit in the database; Instagram Information gathering using osintgram used to gather user data specifically from Instagram.

Database Attack is a technique by which the attacker injects the input code in queries which change order in the query structure intend by administrator and gains the access to database which may lead to deletion of data or user data in database. In case the injection happens it will exploit vulnerabilities in database layer. The SQL Injection is performed using SQL map which performs an injection on the selected database and gathers data and records stored on it.

Password cracking is the method of getting the right watchword to an account in an unauthorized approach. Nearly each watchword has vulnerabilities, and it makes it less complicated to hack. Password attackers use varied techniques to crack passwords, together with the employment of records obtained from information breaches. The options available are Cracking Hashes using JTR tool that can specifically crack encrypted files or texts in many formats; Bypassing passwords on websites using hydra which requires just a URL to start the cracking and bypassing methods which can be used to login to websites with weak security or vulnerabilities.

Reverse engineering is a method of studying a finished project using special methods. Reverse engineering covers a wide range of areas, which includes decompiling and disassembling of executable files and libraries, and analysis of system information. It is accustomed establish the main points of a breach that however the aggressor entered the system, and what steps were taken to breach the system. Reverse APK tool extracts all the files and folders from an APK file and we can later modify it according to our needs. The tool has the capability to even crack APK files that are highly secure.

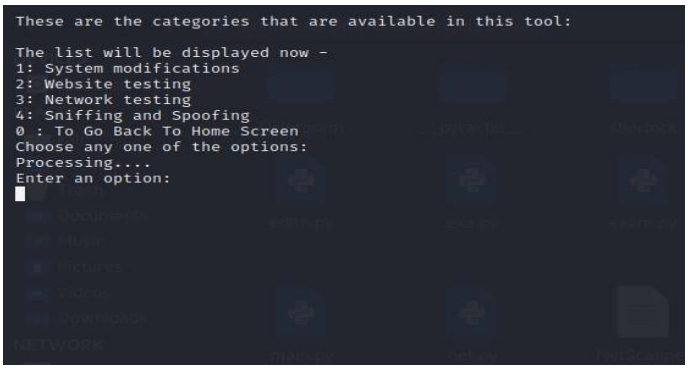
The modules implemented in the proposed tool are advanced and provide precise and accurate results. All the modules have universal use cases and can be used for variety of purposes from individual to organisational and military grade levels.

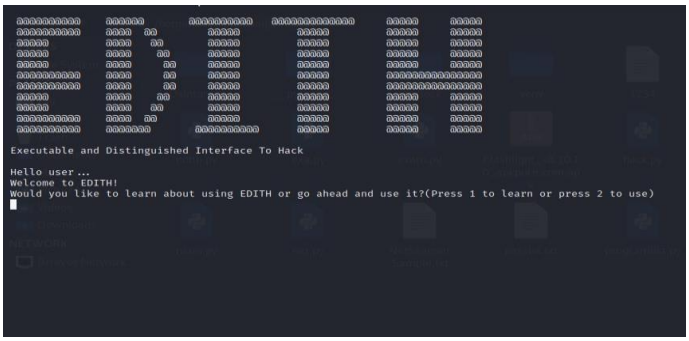
5. RESULTS

After a thorough understanding and working with a lot of tools, we have selected and implemented the best tools for the users to work with and ease the process for them. We have had immense success in the implemented tools with accuracy at its best.

- The macchanger provides an array of options that are available for the user to modify their system configurations in such a way that it is less complex and it is easier to revert back changes to the permanent device configurations.
- Zenmap could be a free and ASCII text file application that aims to form Nmap straightforward for initial learners to use whereas providing advanced options for skilled Nmap users often used scans are saved as profiles to form them straightforward to run recursively.
- Wifite is an automated wireless attack tool and it is used mainly for penetration testing and it is very reliable when it comes to wireless injections and checking the total packets a network can handle at a time making it reliable for checking the capacity of the network, So as it fully automated up to the date tool it is highly reliable for our main tool to work efficiently.
- Aircrack-ng is a complete suite of tools to assess WiFi network security. As this single tool does these functions all at once it becomes very efficient and speeds up the process of checking the network security.
- MITMf supports active packet filtering and manipulation, permitting users to switch any style of traffic or protocol. The configuration file could also be altered whereas MITMf is running, the changes are passed down through the framework.
- Using BeEF, Create a command to line a crop up alert at the Target's browser, wherever malicious uniform resource locators are often another at the Plugin URL.
- Sherlock is used to find usernames on social media on many sites and it reveals many user accounts created by the same person in the multiple social media platforms with their screenname or username.
- Osintgram is an Associate in Nursing OSINT tool on Instagram to gather, analyze, and run reconnaissance missions.
- SQL injection, conjointly referred to as SQLI, could be a common attack vector that uses malicious SQL code for backend info manipulation to access info that wasn't meant to be displayed. This info includes any variety of things, as well as sensitive company knowledge, user lists or non-public client details.
- Using John the Ripper has helped heaps in cracking passwords of various levels. JTR has 3 modes namely: Single crack, Word list, progressive. The one crack mode is the quickest and best mode for a full countersign file to crack.
- APK tool will decrypt resources to original sort and recreate them when creating some modifications. It additionally makes operating with an associate in supporting app easier attributable to the project like file structure and automation.

The above-mentioned tools use the technology that is advanced and has best in class protective and penetration testing measures. The implementation is not limited to a certain range and can be used across any number or systems and networks for enhanced security testing.





6. CONCLUSION

In order to reduce the number of cyber-crimes and threats which are increasing at an alarming rate every day, we must stop this at any cost as there is no effective solution discovered. This project provides a vulnerability scanner that can find the perfect protection required for an individual or an organization.

The implementation of a menu-based penetration testing tool combined with the vulnerability assessment procedure helps to find flaws in a system or network so that it can be fixed before it is exploited. The tool comprises of modules that are exceptionally well suited for different kind of testing and assessment. It can identify the potential threats and attack vectors that pave way for unauthorised individuals or organisations to try to gain access of the system or network.

The tool is suitable for individual and organisation level of implementation and provides a better detail in terms of risks involved in the system environment. It uses the technology that is advanced and has best in class protective and penetration testing measures. The implementation is not limited to a certain range and can be used across any number or systems and networks for enhanced security testing.

7. ACKNOWLDGEMENT

We are grateful for our Guide and Associate Professor Dr. S Kishore Verma's immense support, advice and encouragement.

8. REFERENCES

[1] Ravindranath Kongara, "vSTAAS - an Integrated Pen-Testing Tool", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-9 Issue-2, December, 2019.

[2] Zoran ĐURIĆ, "WAPTT - Web Application Penetration Testing Tool", Advances in Electrical and Computer Engineering 14(1):93-102.

[3] Christian Mainka, Juraj Somorovsky, J¨org Schwenk, "Penetration Testing Tool for Web Services Security", June 2012.

[4] Aruna Pavate, Pranav Nerurkar, "Performance Analysis of Cloud Based Penetration Testing Tools", International Journal of Engineering Research & Technology (IJERT) Vol. 3 Issue 2.

[5] Monika Pangaria, Vivek Shrivastava, Archita Bhatnagar, "Comparative Study of Web Application Penetration Testing Tools ", International Conference on Electrical, Electronics and Computer Science (ICEECS).

[6] Aparicio Carranza, Daniel Mayorga, Casimer DeCusatis, Hossein Rahemi, "Comparison of Wireless Network Penetration Testing Tools on Desktops and Raspberry Pi Platforms".

[7] Palak Aar, Aman Kumar Sharma, "Analysis of Penetration Testing Tools", International Journals of Advanced Research in Computer Science and Software Engineering (Volume 7,Issue-9).

[8] Mubarak Albarka Umar, Chen Zhanfang, "A Study of Automated Software Testing: Automation Tools and Frameworks".

BIOGRAPHIES

A N Anshuman
Bachelor of Engineering, Computer Science and Engineering Department,
Sai Vidya Institute of Technology, Bengaluru, Karnataka, India

Abhinandan C
Bachelor of Engineering, Computer Science and Engineering Department,
Sai Vidya Institute of Technology, Bengaluru, Karnataka, India

Suraj Upadhya G
Bachelor of Engineering, Computer Science and Engineering Department,
Sai Vidya Institute of Technology, Bengaluru, Karnataka, India

Thanushree C
Bachelor of Engineering, Computer Science and Engineering Department,
Sai Vidya Institute of Technology, Bengaluru, Karnataka, India

