2023 World Conference on Communication & Computing (WCONF)
Raipur, India. July 14-16, 2023

Kali Linux based Empirical Investigation on Vulnerability Evaluation using Pen-Testing tools

1st Biresh Kumar
Amity Inst. of Information Technology
Amity University
Jharkhand, Ranchi, INDIA
bkumar@rnc.amity.edu

2nd Sahil Prasad Bejo
Amity Inst. of Information Technology
Amity University
Jharkhand, Ranchi, INDIA
sahil.bejo@s.amity.edu

3rd Riya Kedia
Amity Inst. of Information Technology
Amity University
Jharkhand, Ranchi, INDIA
riya.kedia@s.amity.edu

4th Pallab Banerjee
Amity School of Engg. and Technology
Amity University
Jharkhand, Ranchi, INDIA
pbanerjee@rnc.amity.edu

5th Pooja Jha
Amity Inst. of Information Technology
Amity University
Jharkhand, Ranchi, INDIA
pjha@rnc.amity.edu

6th Mohan Kumar Dehury
Amity Inst. of Information Technology
Amity University
Jharkhand, Ranchi, INDIA
mohankdehury@gmail.com

2023 World Conference on Communication & Computing (WCONF) | 979-8-3503-1120-4/23/$31.00 ©2023 IEEE | DOI: 10.1109/WCONF58270.2023.10235163

***Abstract*— Currently, because almost all interactions occur online, internet security is a critical concern. Penetration testing evaluates network and system security while also revealing security weaknesses. Piercing testing is carry out to ensure that there are no security flaws in the system or network that would permit unauthorised access. Penetration testing, often known as Pen Testing, is a collection of processes designed to track down vulnerabilities in a network or system, or online application that an attacker may exploit. It assists to confirm the effectiveness and efficiency of the different security measures put in place. This document concisely describes the foundations of penetration testing as well as illustrates how and where to deploy and utilise several tools and methodologies for penetration testing using Kali Linux for detecting system vulnerabilities: and provide a review of firewalls, networking protocols, as well as basic security problems that must be addressed in the goal of better protection of the system, ending after analysing the results.**

Keywords*— Cyber Security, Penetration Testing, Hacking, Vulnerability Assessment.

I. Introduction

Cybersecurity, or defending computer systems from intrusion or attack, has grown in significance and attention on a global scale. Many countries have official cyber security policies in place, and some are making considerable investments in the field. The Australian government had just announced that it will spend $50 million over the next seven years on cyber security research [15]. The substantial threat that cybercrimes pose to corporations, governments, and individuals is highlighted by the rising attention and investment from huge organisations and governments. Effective techniques and technologies must be created in order to protect computer systems from these dangers [20].

A. Penetration Testing:

Penetration testing, also known as" pentesting or short P"T, is an authorised, active simulation of a “cyber-attack” with the goal of evaluating cybersecurity and identifying concealed weaknesses. Pentesting is now more important than ever in bolstering computer systems' defence against cyber-attacks as digital assets are vulnerable to relentless intruders, diversified, and complex threats more frequently than ever. This test can be performed manually through the use of hardware as well as socially designed approaches [3].

In the past few years, the IT sector has added more functions and Companies use a test called pen-testing, which is covered in the following section, to cease intruder activities [12].

B. Methodologies used in penetration testing:

The approach used for penetration testing might vary based on the testing engagement's unique requirements.

Generally, penetration testing technique should be adjusted to the individual demands of the testing engagement, considering the target system or network, the customer's needs, and the testing team's resource.

C. Specialized OS for Penetration Testing:

There are Specialized OS(Operating System) are built specially for Penetration testing [19].

Some of notable pen-testing operating systems include:

- Kali Linux.
- BlackArch.
- BackBox
- Parrot Security OS.
- Pentoo i
- WHAX is a Slackware-based operating system.

D. Kali Linux:

Offensive Security created it, and it is based on Debian Linux.

Kali Linux comes with a plethora of tools and utilities pre-installed for doing different cybersecurity activities such as vulnerability assessment, penetration testing, digital forensics, and network analysis. Kali Linux's tools are divided into several areas, including Information Collecting, Password Attacks, Web Applications, Wireless Attacks, and Exploitation Tools.

Because of its robust capabilities and flexible design, Kali Linux is frequently utilised by cybersecurity experts and researchers. It is also used by ethical hackers including penetration testers to mimic real-world attacks on networks and IT systems.

979-8-3503-1120-4/23/$31.00 ©2023 IEEE

E. Web Penetration Testing Tools:

1) Wapiti:

Using Wapiti, web-app security can be evaluated. It performs black box based scans, which implies that the source code of the programme is not looked at [11]. Wapiti becomes a fuzzer after acquiring this list, adding payloads to look for script flaws.

2) Skipfish:

Skipfish is a current web application security reconnaissance tool [11].

3) Arachni:

Arachni can handle attack/input vectors that non-humans would not normally be able to detect. Finally, Arachni's asynchronous HTTP technique contributes to its exceptional performance (courtesy of Typhoeus). As a result, the audited server's responsiveness and your bandwidth will be your only limitations.

4) Nessus:

Nessus provides network security scanner tool.. Plug-in installation is made simple, as is checking which ones are installed to determine if you're up to date [11]. Vulnerability inspections are handled through plug-ins. Another feature of Nessus is its ability to scan Windows and Unix systems for security flaws. As a result, you may scan a variety of areas in a single session, making it a great all-purpose tool.

5) w3af (Web Application Attack and Audit Framework):

It is used for finding and using web application vulnerabilities.

6) Acunetix:

It looks for several vulnerabilities, including weak passwords, XSS, along with SQL injection.

7) Web security:

It incorporates a powerful platform for online application security testing. It can be accessed from mobile and web-based devices as well as from all common desktop platforms. Table 1 compares the various Web penetration tools on the market based on a variety of characteristics.

8) Nmap

Nmap is well known for being an incredibly quick port scanner.

F. Penetration Testing Phases:

1) Pre-engagement Interactions:

This refers to a stage in which preparations are done for the pen test.

2) Information Gathering:

In this stage information is gathered [13].

3) Vulnerabilities analysis:

Following information collecting, the network or machines is inspected for vulnerabilities. During this scanning step, the tester evaluates the vulnerabilities, judge factors such as OS, the version of a particular service, the firewall service, or port number [13].

4) Vulnerability exploitation:

Basic goal of a pen tester is to see how deeply within the systems it can go while still discovering viable targets..

5) Post exploitation:

When the intrusion is complete, the intruder or attempts to remain in the machine for an extended period of time without being detected [13].

6) Report Generation:

A document in the manner of a status report is created. This paper describes the complete penetration testing methodology in detail.

G. Vulnerability Assessment:

Vulnerability assessment is a kind of penetration testing which focuses upon detecting flaws in a network or a system that attackers may exploit. A vulnerability assessment's purpose is to discover and evaluate vulnerabilities while also prioritising them according to their potential effect and risk of exploitation.

Automated technologies, like as vulnerability scanners, and are used during a vulnerability assessment to uncover known vulnerabilities including such unsecured software, weak passwords, and open ports. These programmes may search for and verify known vulnerabilities to a list of known vulnerabilities with common attack signatures.

H. Types of Attacks:

1) Password Attacks:

Password assaults are attempts to guess or crack passwords used to safeguard user accounts. To get user passwords, hackers could employ tactics like brute-force assaults, phishing attacks, along with dictionary attacks.

2) Malware Attacks:

Malware attacks occur when malicious software is utilized to obtain unauthorised entrance to a machine or network. Virus, worms, ransomware, and Trojan horses are examples of malware.

3) SQL Injection:

SQL injection attacks include loading malicious code into a website's or app's SQL database, allowing attackers to access sensitive information in the database system.

4) XSS:

Cross-site scripting (XSS) attacks include inserting malicious code into the web pages of a website or app, allowing hackers to execute arbitrary code in the view of the victim's internet browser [19].

5) MITM:

MITM attacks entail eavesdropping network communications between two individuals and intercepting, altering, or inserting malicious material into the connection.

These are just a handful of the numerous forms of penetration assaults that might be used by intruders to obtain unauthorised access to machine or computer networks. Organizations must aware of various attack types and take appropriate countermeasures, such as following security best practises, conducting frequent vulnerability assessments, and deploying security systems like firewalls, access restrictions, and IDS (Intrusion Detection System) /IPS (Intrusion Prevention System) [10].

II. Problem Statement

A. The Problem

Cyber threats are growing more complex in today's environment, and attackers are continually devising new ways to exploit weaknesses in computer systems, networks, and applications thus a successful data breach can have dire effects for a business, including data loss, financial loss, and reputational damage. To enforce consistency with security standards and regulations, many industries and regulatory authorities require constant security audits, including vulnerability assessments as well as penetration testing.

B. Solution

Vulnerability assessment and penetration testing assist companies in identifying possible vulnerabilities prior to an attack, allowing them to take proactive actions to safeguard their systems and maintain business continuity. Vulnerability assessment and penetration testing are critical for detecting possible security threats and mitigating assaults.

III. Objective And Goal

The main objective is to gather data about vulnerability assessment and penetrations testing, analyze, as well as illustrate how they are to be utilised lawfully for greater aims such as security breaches as well as thorough protection techniques.

A. Goal

The primary objective was to give a detailed analysis of vulnerability evaluation as well as penetration testing.

B. Specific Objectives

The objectives are:

- To show what is vulnerability assessment along with penetration testing.
- To show what are the tools and OS used for penetration testing.
- To demonstrate a practical vulnerability assessment.
- Analyze and evaluate the results.

IV. Review of Literature

The analysis and review of prior work was done based on use and study on vulnerability assessment along with penetration testing. The preceding works chosen selected from OffSec (offensive security) dominion with circumstances to VAPT (vulnerability assessment and penetration testing), several types of them and novel ideas.

1. According to the authors in [15], this work is the first to use reinforcement learning for automated penetration testing. Before RL may be utilized in commercial settings, more effort must be done to build scalable RL algorithms and test these algorithms in better realistic simulators.

2. Authors in [5] conducted a firewall assault and were able to record the target Wi-Fi network's handshakes, which then exploited to set up a rogue AP and crack the password. The constructed phoney login page provided the password. The master key, which had been retrieved from the earlier-captured handshakes, was then matched with the password. Their findings indicated that the assaults made against the firewall and the web were successful.

3. In [9] Wi-Fi network pen-testing with Kali Linux is carried out by authors in the simulation environment and analysed.

4. To increase the effectiveness of exploration, authors in [18] rationally incorporate five improvements to DQN. To bring down the action domain, authors disintegrate the action along with divide the neural network's estimators to compute two action items individually. Ultimately, a variety of cases are studied to determine how well algorithm's function.

5. The authors in [4] introduce mining techniques like taint analysis, symbol execution, and fuzzy assessment. To judge the security aspect of the satellite communication network, they employed Trojan horse infiltration, cross-site scripting, buffer overflow, and SQL injection. It was found that it is advantageous to increase the satellite communication network's capacity for proactive defence and security assurance.

6. In the paper [8], certain fundamentals of penetration testing are briefly discussed. Using the pre-existing modules, exploits, and tools of the Metasploit framework, authors discuss penetration testing procedures.

7. Authors in [13] assess security convention for Wi-Fi Protected Access (WPA), 802.11i (WPA2), along with Wireless Equivalent Privacy (WEP) by pen-testing and found that it can be effectively cracked if only the passphrase is present in the dictionary or wordlist of the attacker.

8. Authors in [3] carried out a variety of attacks, such as smartphone penetration testing, Bluetooth phone hacking, traffic sniffing and covered potential defences.

9. Authors in [12] highlight security flaws and identify risks that hackers can use to gain access to systems and carry out various actions, particularly on Android smart phones.

10. After doing an assessment of some of the available web penetration tools, authors in [11] developed architecture for scanning a website's vulnerabilities utilising the nesus and Metasploit tools.

11. In [16] authors have carried out server-side long with client-side based exploitations. Finally, in order to fend against hacking attacks, suggested mitigation strategies and security upgrades.

12. Authors in [17] suggested a framework that is capable of precisely resolving computers with common vulnerabilities and publicly available exploits, according to experimental results.

13. Several penetration tests were carried out in [14] by employing tools, virtualized systems, and private networks and. conclude that there isn't perfect protection by downloading and installing antivirus applications based on the incidents that are happening globally.

14. The technical method for manual web-app penetration testing is discussed in the paper [2] with a view to maintaining the security of the online applications. Authors carefully scan for and exploit the top 10 vulnerabilities listed by OWASP. Finally presented several courses on penetration testing and vulnerability assessment those are open to everyone.

15. In [7] authors examine penetration testing from a variety of angles and describe its main subtypes also show

between hacking and penetration testing, there is a clear line of distinction.

V. Methodological Approach

While implementing the concept, experimental and agile framework was utilized as methodology for the proposed study. For conducting experiments in this study, I All the data has been collected from relevant sources. All the data is studied in detail. For evaluating the penetration testing software and framework a simulation of pen-testing is discharged, and result data is gathered. The results as well as findings are evaluated.

A. Softwares specification:

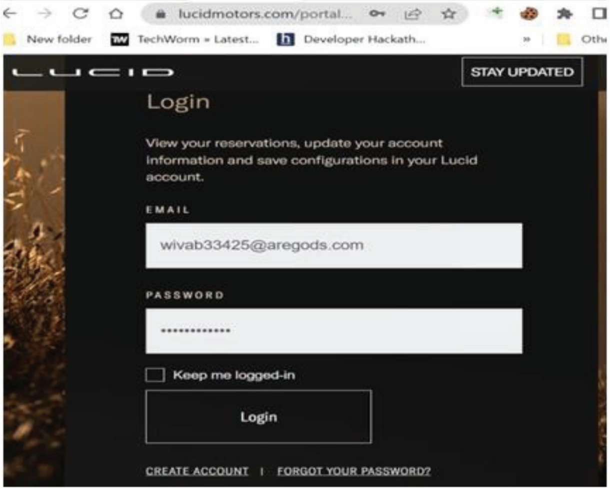
VMware: For creating sandbox environment
Operating System: Kali Linux (inside Vmware)
ZAP Proxy
Kali Linux
CookieEditor
Google Chrome Browser
Firefox Browser

B. Implementation

For demonstrating how a penetration testing works we have done a real site “lucidmotors.com” open for bug bounty in bug bounty platform Bug crowd. After scanning the site vulnerabilities found are Authentication as well as session Management:

Penetration testing for this includes detecting and abusing vulnerabilities inside an application's and system's authentication and session management processes. Broken authentication as well as session management refers to the circumstances where a penetration tester or hacker may circumvent the authentication and session management processes and obtain unauthorized access to the application or system.

WORKING:
For testing the site, we used the following steps:
Step 1: Boot Kali Linux.
Step 2: Open ZAP Proxy for scanning the url.
Step 3: Scanned the site using ZAP Proxy for scanning vulnerabilities.
Step 4: Open Google Chrome browser to login into account shown in fig 1.



Login

View your reservations, update your account information and save configurations in your Lucid account.

EMAIL
wivab33425@aregods.com

PASSWORD
••••••••••••

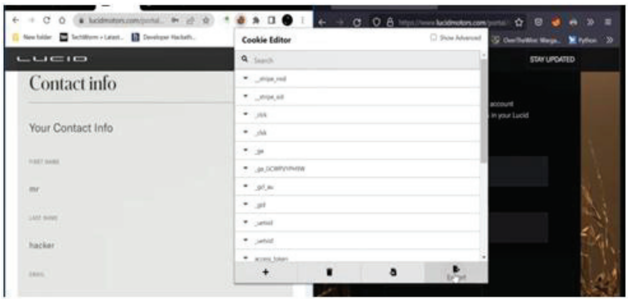
□ Keep me logged-in

Login

CREATE ACCOUNT | FORGOT YOUR PASSWORD?

Fig. 1. Logging in Google Chrome browser

Step 5: Export the cookies session from add on cookies editor fig 2.



Contact info

Your Contact Info

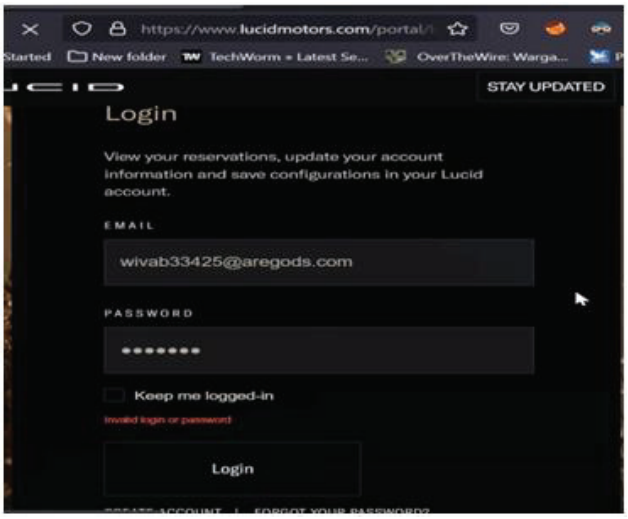
FIRST NAME
mr

LAST NAME
hacker

EMAIL

Fig. 2. Exporting Cookies Using CookieEditor

Step 6: Again, open the login page in another browser fig 3.



Login

View your reservations, update your account information and save configurations in your Lucid account.

EMAIL
wivab33425@aregods.com

PASSWORD
•••••••

□ Keep me logged-in

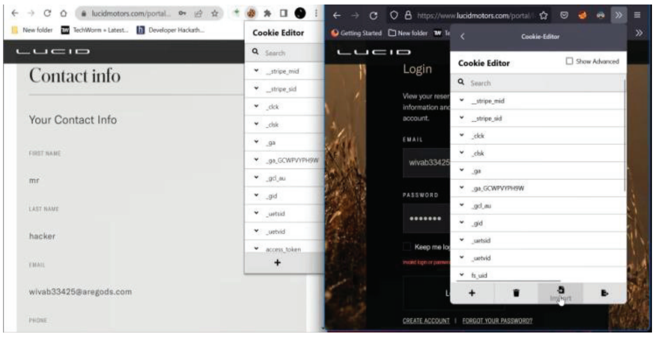
Invalid login or password

Login

CREATE ACCOUNT | FORGOT YOUR PASSWORD?

Fig. 3. Opening Login Page in Firefox Browser

Step 7: Import cookies in the by Pasting the cookies in Cookie Editor like Fig 4 and 5.



Contact info

Your Contact Info

FIRST NAME
mr

LAST NAME
hacker

EMAIL
wivab33425@aregods.com

PHONE

Login

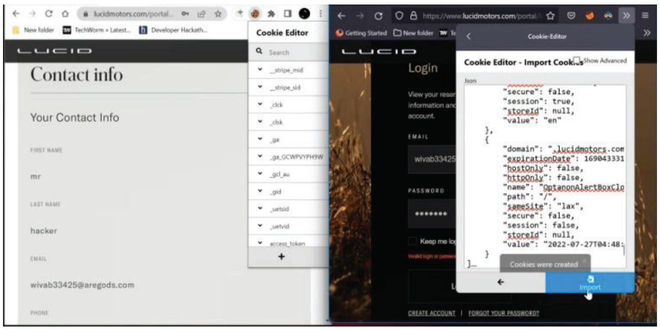
EMAIL
wivab33425

PASSWORD
•••••••

Keep me lo

CREATE ACCOUNT | FORGOT YOUR PASSWORD?

Fig. 4. Importing Cookies Using CookieEditor



Cookie Editor - Import Cookies

Json

```
        "secure": false,
        "session": true,
        "storeId": null,
        "value": "en"
    },
    {
        "domain": ".lucidmotors.com
        "expirationDate": 169043331
        "hostOnly": false,
        "httpOnly": false,
        "name": "OptanonAlertBoxClo
        "path": "/",
        "sameSite": "lax",
        "secure": false,
        "session": false,
        "storeId": null,
        "value": "2022-07-27T04:48:
    }
]
```

Cookies were created

Contact info

Your Contact Info

FIRST NAME
mr

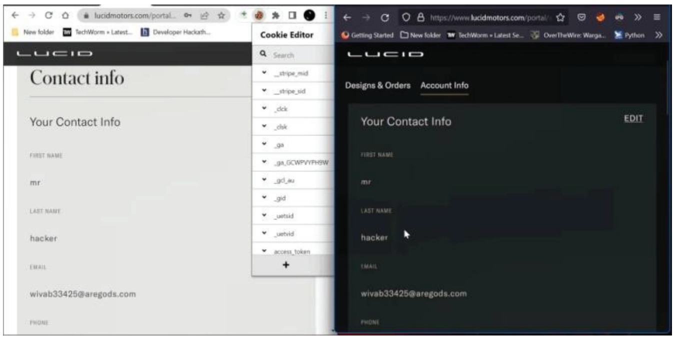
LAST NAME
hacker

EMAIL
wivab33425@aregods.com

PHONE

Fig. 5. Pasting Cookies in CookieEditor

Step 8: Refresh the page and it will Successfully login; shown in Fig 6.



Contact info

Your Contact Info

FIRST NAME
mr

LAST NAME
hacker

EMAIL
wivab33425@aregods.com

PHONE

Fig. 6. Successful Login after refreshing the Page.

To reproduce the steps are:

1. Login to account in Google Chrome browser.

2. Export the cookies session from Cookie Editor in Chrome Browser.

3. Again, open the login page in another browser (we used Firefox).

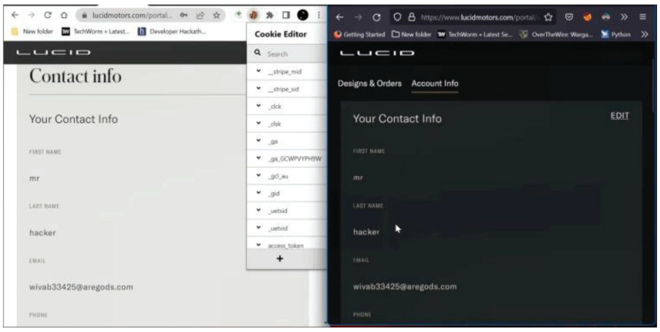
4. Import cookies in the Firefox browser.

5. Paste the cookies in cookie editor and refresh the page.

6. Logged in.

VI. RESULT AND ANALYSIS

After analysis of previous work based on penetration testing, we have tried to demonstrate penetration testing. While scanning for vulnerability using ZAP Proxy it produced a lot of false positives. But after scanning for all the possibilities we got a positive result with a successful broken authentication and session management vulnerability exploit as shown in figure 7. But it was already produced before thus we got a duplicate reporting.



Contact info

Your Contact Info

FIRST NAME
mr

LAST NAME
hacker

EMAIL
wivab33425@aregods.com

PHONE

Fig. 7. Proof of Exploit

VII. LIMITATIONS AND FUTURE WORK

Vulnerability evaluation is a vital component of penetration testing given that it assists in identifying potential security issues in a system or application. However, there are several limits and opportunities for further study in Kali Linux vulnerability evaluation, which include false positive as Vulnerability assessment techniques frequently produce a high number of false positives, which might take time to analyze and evaluate. This can result in time and resources being wasted on issues that are not genuine vulnerabilities. The vulnerability scanning tool does not have the capability to scan 0-day vulnerability which is a constraint for scanners.

To alleviate these constraints, in future Kali Linux based vulnerability assessment and penetration testing can work on creating new vulnerability assessment tools to decrease false positives and increase vulnerability detection accuracy. The range of vulnerability assessment tools is being expanded to include new types of vulnerabilities and testing methodologies. Creating new testing methodologies and tools to discover emerging risks like zero-day vulnerabilities or new attack strategies.

VIII. CONCLUSION

It thoroughly described what vulnerability and penetration testing are, how they function, and why they are important for businesses. Following an analysis and evaluation of previous work and experiment results, it is stated that vulnerability assessment is a vital aspect of Kali Linux penetration testing since it identifies possible security issues in a system or application. Vulnerability assessment tools can aid in the systematic discovery of vulnerabilities, saving time and money throughout the testing process. Nevertheless, keep in mind that vulnerability assessment tools have downsides such as false positives, limited scope, and limited reporting options. To go around these limitations, penetration testers must apply a variety of testing approaches, such as manual testing including code review, as well as stay up to date on emerging threats and attack strategies.

REFERENCES

[1] Arote, A., & Mandawkar, U. (2021). Android Hacking in Kali Linux Using Metasploit Framework. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 497–504. https://doi.org/10.32628/cseit2173111

[2] Bhatia, G., Bhatia, O., Bhandare, A., Bagde, V., & Prayagkar, A. (2021). Vulnerability Assessment and Penetration Testing. International Journal of Engineering Research & Technology (IJERT), 10(05). www.ijert.org

[3] Denis, M., Zena, C., & Hayajneh, T. (n.d.). Penetration Testing: Concepts, Attack Methods, and Defense Strategies. www.kali.org

[4] Dong, K., Zhang, H., Liu, Y., Li, Y., & Peng, Y. (2021). Research on technologies of vulnerability mining and penetration testing for satellite communication network. IOP Conference Series: Earth and Environmental Science, 693(1). https://doi.org/10.1088/1755-1315/693/1/012112

[5] Gunawan, T. S., Lim, M. K., Kartiwi, M., Malik, N. A., & Ismail, N. (2018). Penetration testing using Kali linux: SQL injection, XSS, wordpres, and WPA2 attacks. Indonesian Journal of Electrical Engineering and Computer Science, 12(2), 729–737. https://doi.org/10.11591/ijeecs.v12.i2.pp729-737

[6] Holik, F., Neradova, S., Horalek, J., Zitta, S. & Marik, O., (2014). Effective penetration testing with Metasploit framework and Methodologies. CINTI 2014 : 15th IEEE International Symposium on Computational Intelligence and Informatics, 237–242.

[7] Kaur, G., & Kaur, G. (2016). Penetration Testing: Attacking Oneself to Enhance Security. International Journal of Advanced Research in Computer and Communication Engineering, 5(4). https://doi.org/10.17148/IJARCCE.2016.54141

[8] Rani, S., & Nagpal, R. (2019). PENETRATION TESTING USING METASPLOIT FRAMEWORK: AN ETHICAL APPROACH. International Research Journal of Engineering and Technology. www.irjet.net

[9] Lu, H. J., & Yu, Y. (2021). Research on WiFi Penetration Testing with Kali Linux. Complexity, 2021. https://doi.org/10.1155/2021/5570001

[10] Kumar, B.; Sinha, A.; Roy, S.; Iwendi, C.; Strážovská, Ľ. E-Commerce Website Usability Analysis Using the Association Rule

Mining and Machine Learning Algorithm. Mathematics 2023, 11, 25. https://doi.org/10.3390/math11010025

[11] Mukhopadhyay, I., Goswami, S., & Mandal, E. (2014). Web Penetration Testing using Nessus and Metasploit Tool. IOSR Journal of Computer Engineering (IOSR-JCE), 16(3), 126–129. www.iosrjournals.org

[12] Raj, S., & Walia, N. (2020). A Study on Metasploit Framework: A Pen-Testing Tool. International Conference on Computational Performance Evaluation : ComPE 2020.

[13] Kissi, M. K., & Asante, M. (2020). Penetration Testing of IEEE 802.11 Encryption Protocols using Kali Linux Hacking Tools. International Journal of Computer Applications, 176(32), 26–33.

[14] Santhi, V., Kumar, K. R., & Vinay, B. L. v. (2016). Penetration Testing using Linux Tools: Attacks and Defense Strategies. www.ijert.org

[15] B. Kumar et al., "A Static Machine Learning Based Evaluation Method for Usability and Security Analysis in E-Commerce website," in IEEE Access, doi: 10.1109/ACCESS.2023.3247003.

[16] Tabassum, M., Mohanan, S., & Sharma, T. (2021). Ethical Hacking and Penetrate Testing using Kali and Metasploit Framework. Nternational Journal of Innovation in Computational Science and Engineering, 2(4), 9–22.

[17] Valea, O., & Oprisa, C. (2020). Towards Pentesting Automation Using the Metasploit Framework. Proceedings - 2020 IEEE 16th International Conference on Intelligent Computer Communication and Processing, ICCP 2020, 171–178. https://doi.org/10.1109/ICCP51029.2020.9266234

[18] Zhou, S., Liu, J., Hou, D., Zhong, X., & Zhang, Y. (2021). Autonomous penetration testing based on improved deep q-network. Applied Sciences (Switzerland), 11(19). https://doi.org/10.3390/app11198823

[19] Kayani, A. K., & Saeed, M. Q. (2021). Comparative Analysis of Anti-Virus Evasion Malware Creator Tools of Kali Linux, with Proposed Model for Obfuscation. 2021 International Conference on Cyber Warfare and Security, ICCWS 2021 - Proceedings, 24–29. https://doi.org/10.1109/ICCWS53234.2021.9702944

[20] S. P. Bejo, B. Kumar, P. Banerjee, P. Jha, A. N. Singh and M. K. Dehury, "Design, Analysis and Implementation of an Advanced Keylogger to Defend Cyber Threats," 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, (2023), pp. 2269-2274, doi: 10.1109/ICACCS57279.2023.10112977