Cyber Threat Prevention: Enhancing Resilience with VAPT Solutions

G Swaroop[1], Harish Budarpu[2], Manasa B N[3], Prof. Meghashree N[4]

[1 2 3]Student Scholar, Dept. of Computer Science and Engineering, Atria Institute of Technology, Karnataka, India
[4]Asst.Professor, Dept. of Computer Science and Engineering, Atria Institute of Technology, Karnataka, India

---***---

Abstract - *Computers, mobile devices, and other networks and systems are not sufficiently secure and are open to various cyberthreats. Every year, there are more and more cyberthreats. Vulnerability assessment is the process of locating the weaknesses in networks and systems. Vulnerability assessment aids in offering the required countermeasures to online threats. It entails identifying vulnerabilities, such as those in networks, physical systems, and applications, and evaluating the risks that come with them. This paper presents a new method for performing cyberattack analysis by utilizing penetration testing and vulnerability assessment techniques. The suggested approach makes use of a variety of Kali Linux tools, combined with an intuitive menu system and Python modules. A comparative study is conducted between the results of a major proposed approach and Kali Linux's built-in tools. Notably, the results show significant advancements in a number of critical domains, such as information gathering, network and website testing, system modifications, sniffing, and spoofing. These enhancements make cyber-attack analysis more effective and efficient overall and provide valuable data for more effective security measures.*

***Key Words*: cyber security, cyber-attack prevention, vulnerability assessment, penetration testing.**

1. INTRODUCTION

Cyber-attacks and threats are defined as a broad range of actions conducted by individuals who typically use malicious software to gain access to a person's or an organization's network or systems. They may even result in data loss, system crashes, and poor performance when computer systems malfunction. Cyberattacks can be carried out from any location by an individual or a group. Hackers and cybercriminals are the ones who carry out these types of cyberattacks. We can use the tools that Kali Linux provides to address these vulnerabilities. We have presented a menu-based interface for vulnerability assessment and penetration testing using Python modules in this paper.

2. Literature Review

[1] A comparison of web application automation testing tools is presented in this paper. The popular automation testing tools were chosen for this study their features, usability, performance, ease of use, and compatibility with web applications were assessed. The study's limitations include its narrow focus on web applications and the small number of tools it examined. Future studies can investigate a wider variety of instruments and expand the assessment to different kinds of applications in order to get around these limitations. [2] A paper's main focus is on penetration testing and vulnerability assessment. For these tasks, the authors suggest an implementation of a solution. As part of the methodology, a portable testing platform for penetration testing and vulnerability analysis is designed and developed. The paper's limitations include its particular focus on a portable solution and its requirement for additional testing and validation of the recommended solution. provides a thorough examination of numerous cyberattacks. [3] The research methodology employed in this study entails a review and analysis of various cyber-attack types, covering their attributes, methods, and possible consequences. [4] The reporting and analysis of wireless network security test results using Kali Linux is the main goal of this study. Utilising Raspberry-Pi and Kali devices, experiments are conducted as part of the methodology to assess wireless network security. The study has several limitations, such as its narrow focus on Raspberry Pi devices and the need for more extensive validation of the results. To overcome these limitations, even more research can compare evaluations with other security assessment methods using different hardware platforms. [5] A comparative analysis of web application security aspects is presented in this paper. Key security parameters were identified and current trends in web application security were reviewed as part of the research techniques. The study's shortcomings include its emphasis on particular security criteria and the absence of a thorough assessment of the state-of-the-art methods for web application security. Future researchers can include a wider range of security parameters and compare the effectiveness of various security techniques in order to overcome these limitations. [6] This paper primarily focuses on information gathering and pen testing tools. Analyzing current information-gathering methods and penetration testing tools is part of the methodology. The primary limitations of the paper are the narrow range of information collection methods discussed and the need for further empirical validation of the instruments. To overcome these constraints, future investigators can investigate supplementary data collection methods and carry out empirical investigations to verify and contrast various instruments. [7] The implementation and comparison of various password cracking tools is the main topic of this paper. The process entails choosing well-known password-cracking software and assessing how well it performs and cracks passwords. The small number of tools examined and

the lack of a specific thorough assessment of every password cracking method are two of the research's limitations.

Overall, by offering insights into automated testing tools, vulnerability assessment and penetration testing, cyberattacks, web application security, information gathering, wireless network security, and password cracking tools, these papers contribute to the field of cybersecurity. Every paper does, however, have certain shortcomings that should be addressed by more research in order to advance understanding and provide robust security solutions.

3. Contribution

In this specific work, we perform vulnerability research, which helps to find both new and old vulnerabilities in software and systems. This is a significant contribution to a vulnerability assessment and penetration testing tool project. Vulnerabilities can be found and exploited by developing vulnerability assessment and penetration testing tools, which aids in improving system security for organisations. In addition to having a thorough understanding of software and systems architecture, vulnerability researchers usually need to be familiar with common attack vectors and techniques. This paper makes three significant contributions: (i) it implements a menu driven approach; (ii) it provides accurate reports on risk assessment using custom tools; and (iii) it reduces the likelihood that the systems may be compromised. The second section explains the anticipated work on vulnerability assessment and penetration testing tools. Section III presents the findings, while Section IV closes the study.

4. Proposed Work

This section emphasizes on system architecture, vulnerability scanner and utilization of vulnerability assessment and penetration testing tools.

4.1. System Architecture

Multiple levels of protection are used for different system components in this vulnerability assessment and penetration testing system architecture. Figure 1 displays the components of the system.

Threat sources: These are the entities that pose a potential threat for the security issues of an organization. Threat sources can be internal or external. Identifying potential threat sources is a major part of VAPT, as that helps organizations to understand where their security risks lie.

Events or situations that pose a threat to an organization's resources or interfere with its regular business operations are known as threat events. Data breaches, denial-of-service attacks, and malware infections are a few examples of threat events. VAPT helps organizations identify potential threat events and develop strategies to prevent them.

Countermeasures: These are defences against possible threats that are put in place to safeguard an organization's assets. Firewalls, intrusion detection systems, access controls, and security policies are a few examples of countermeasures. Organisations can use VAPT to determine which countermeasures will work best for their specific security requirements.

Security testing is the process of evaluating an organization's security posture in order to spot potential threats and weak points in an attack. A variety of methods, including vulnerability scanning, penetration testing, and social engineering, can be used in security testing.

Vulnerabilities: An organization's security flaws that could be used by adversaries to gain access; Vulnerability Assessment and Penetration Testing (VAPT) assists organisations in proactively locating and resolving these issues to stop potential exploitation.

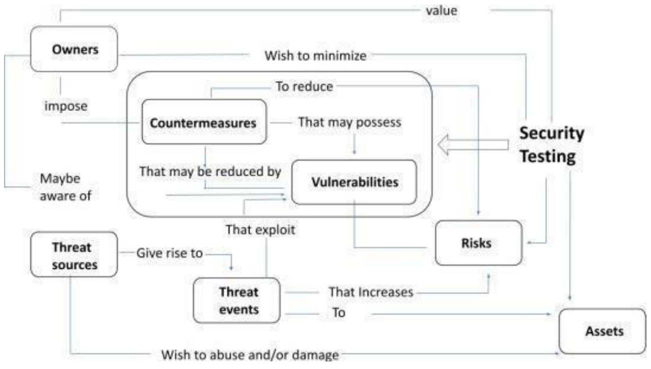


Fig 1. System Architecture

4.2. Vulnerability Scanner

A tool named a vulnerability scanner is made to automatically find security flaws in specific networks, applications, and systems. By scanning the target system for known vulnerabilities, the tool detects any flaws that an attacker could exploit. Vulnerability scanners use a specific database of known vulnerabilities in addition to a variety of other techniques to locate and exploit vulnerabilities. Typically, the scanner has two modes of operation: passive and active. In order to find and fix vulnerabilities, the scanner sends packets to the target system while it is in active mode. When in passive mode, the scanner scans a network for traffic and, mainly, uses the traffic it sees to identify vulnerabilities.

Following the identification of every vulnerability, the scanner will produce an extensive report that clearly explains each vulnerability's characteristics, including its severity. Security experts would primarily use the report to schedule and prioritise remediation actions, as indicated in Fig 2.

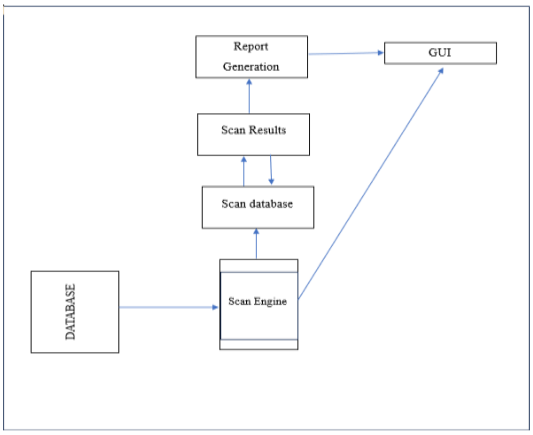


Fig 2. Vulnerability Scanner

4.3. Utilization of vulnerable assessment and penetration testing.

Security experts use penetration testing and vulnerability assessment tools to identify and test vulnerabilities in computer systems, networks, and applications. Security experts use these tools to proactively find and fix security risks and vulnerabilities as well as to make sure the systems are safe from possible attacks. The main purpose of vulnerable assessment tools is to search computer networks and systems for known vulnerabilities. Automated system and application scans will be carried out by these tools to find vulnerabilities. Reports detailing the specifics of each vulnerability, such as its severity and suggested remediation actions, will be generated. Tools for vulnerability assessments are often used to find holes in systems before attackers take advantage of them. Tools for penetration testing are used to mimic actual attacks on networks and systems. Penetration testing tools are capable of detecting vulnerabilities in systems that vulnerability assessment tools are unable to detect. They can also assist organizations in evaluating the effectiveness of their security controls in thwarting attacks. Figure 3 illustrates the steps involved in vulnerability assessment and penetration testing. Tools for vulnerability assessment and penetration testing are essential for spotting possible security threats and weaknesses that an attacker might have used against you. Through proactive identification and mitigation of these risks, organisations can decrease the probability of successful attacks and mitigate the potential consequences of diverse security incidents. All things considered, penetration testing and vulnerability assessment tools are crucial parts of any successful security testing programme. Organisations could strengthen their security posture, lower the chance of successful attacks, and adhere to industry best practices and legal requirements by utilising these tools to find and fix vulnerabilities.

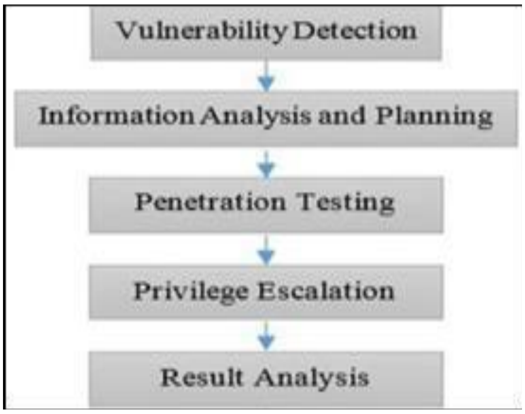


Fig 3. Stages of Penetration testing and Vulnerability assessment

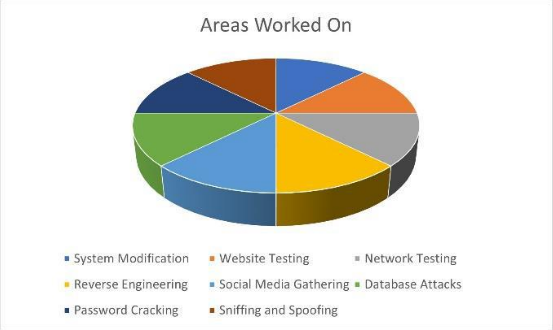
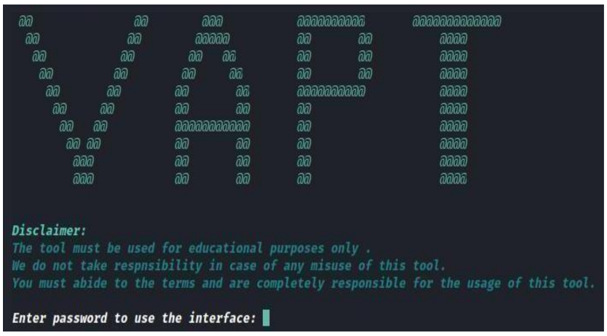


Fig. 4. Graph indicating areas worked on

Figure 4 illustrates that, in contrast to [8], which has implemented only three areas of concern, we have implemented eight areas or modules. The modules we've put in place include information gathering, database attacks, sniffing and spoofing, website testing gathering, system alterations, password cracking attacks, and reverse engineering tools are all examples of network testing.

5. Results

After comparing the results with [8], improvements were observed in multiple areas including system modifications, network and website testing, sniffing and spoofing, and information gathering.



```
@@               @@         @@@             @@@@@@@@@@       @@@@@@@@@@@@@
 @@             @@         @@@@@            @@       @@          @@@@
  @@           @@         @@   @@           @@       @@          @@@@
   @@         @@         @@     @@          @@       @@          @@@@
    @@       @@         @@       @@         @@@@@@@@@@           @@@@
     @@     @@          @@       @@         @@                   @@@@
      @@   @@           @@@@@@@@@@@         @@                   @@@@
       @@ @@            @@       @@         @@                   @@@@
        @@@             @@       @@         @@                   @@@@
        @@@             @@       @@         @@                   @@@@

Disclaimer:
The tool must be used for educational purposes only .
We do not take respnsibility in case of any misuse of this tool.
You must abide to the terms and are completely responsible for the usage of this tool.

Enter password to use the interface: 
```

Fig 5. Home Screen

Our application provides a wide range of categories for performing penetration on the chosen system or networks identifying vulnerabilities as shown below in Figure 6. Our meticulous selection and application of a range of effective and user-friendly tools has produced remarkable accuracy when compared to [8].

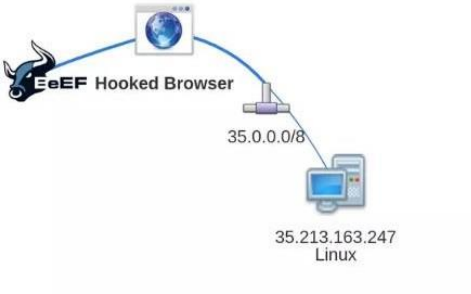


Fig 7. BeEF tool

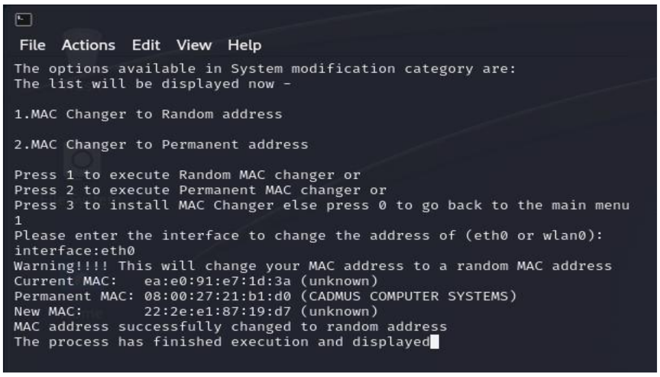
Malicious URLs can be added to the Plugin URL and a command can be written to cause an alert to appear on the target's browser by utilising BeEF, as shown in Fig 7.

Zenmap is a free ASCII text file programme that offers advanced options to users with experience while streamlining Nmap for novice users. To enable basic recursive runs, scans are maintained as profiles.

A wireless assault tool called Wifite is primarily utilized for penetration testing. It is reliable when it comes to testing a network's ability to handle packets and performing wireless injections. It is the perfect tool for the effective operation of this primary tool because of its automation.

One of the most important tools selected is the MAC changer, which is depicted in Fig. 8. It provides a number of options for changing system configurations, facilitating a return to the factory default device setups.

By offering active packet filtering and manipulation, MITMf enables users to seamlessly transition between any kind of protocol or traffic. While the tool is operating, users can make changes to the configuration file, and the changes will be implemented throughout the framework.



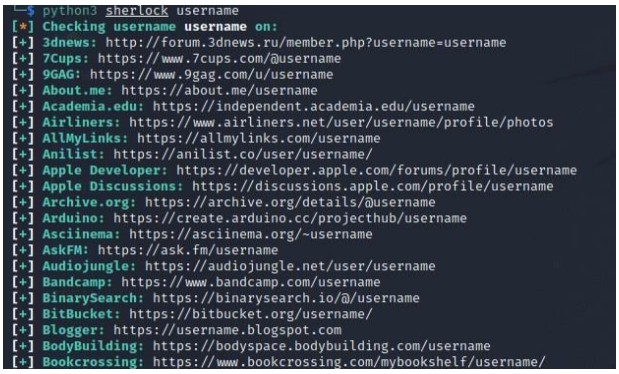
```
The options available in System modification category are:
The list will be displayed now -

1.MAC Changer to Random address

2.MAC Changer to Permanent address

Press 1 to execute Random MAC changer or
Press 2 to execute Permanent MAC changer or
Press 3 to install MAC Changer else press 0 to go back to the main menu
1
Please enter the interface to change the address of (eth0 or wlan0):
interface:eth0
Warning!!!! This will change your MAC address to a random MAC address
Current MAC:   ea:e0:91:e7:1d:3a (unknown)
Permanent MAC: 08:00:27:21:b1:d0 (CADMUS COMPUTER SYSTEMS)
New MAC:       22:2e:e1:87:19:d7 (unknown)
MAC address successfully changed to random address
The process has finished execution and displayed
```

Fig 8. Mac Changer



```
└─$ python3 sherlock username
[*] Checking username username on:
[+] 3dnews: http://forum.3dnews.ru/member.php?username=username
[+] 7Cups: https://www.7cups.com/@username
[+] 9GAG: https://www.9gag.com/u/username
[+] About.me: https://about.me/username
[+] Academia.edu: https://independent.academia.edu/username
[+] Airliners: https://www.airliners.net/user/username/profile/photos
[+] AllMyLinks: https://allmylinks.com/username
[+] Anilist: https://anilist.co/user/username/
[+] Apple Developer: https://developer.apple.com/forums/profile/username
[+] Apple Discussions: https://discussions.apple.com/profile/username
[+] Archive.org: https://archive.org/details/@username
[+] Arduino: https://create.arduino.cc/projecthub/username
[+] Asciinema: https://asciinema.org/~username
[+] AskFM: https://ask.fm/username
[+] Audiojungle: https://audiojungle.net/user/username
[+] Bandcamp: https://www.bandcamp.com/username
[+] BinarySearch: https://binarysearch.io/@/username
[+] BitBucket: https://bitbucket.org/username/
[+] Blogger: https://username.blogspot.com
[+] BodyBuilding: https://bodyspace.bodybuilding.com/username
[+] Bookcrossing: https://www.bookcrossing.com/mybookshelf/username/
```

Fig 9. Sherlock tool

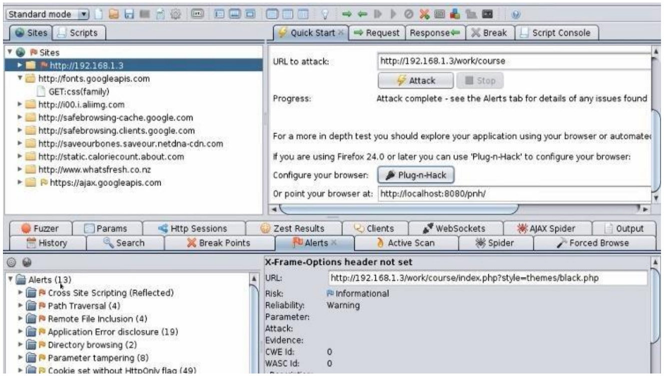
As seen in Fig. 9, Sherlock is a tool for locating usernames on social media that can identify multiple accounts made by the same person using the same screen name or username.

Osintgram is an OSINT tool primarily used for conducting reconnaissance missions and gathering, analysing, and analysing information about Instagram.

SQL injection, or SQLI, is a method that accesses data not meant for display by manipulating backend data with SQLcode.

This information includes sensitive company data, user lists, and private client details.

It has been helpful to crack passwords of various levels of complexity with John the Ripper. There are three modes for JTR: progressive, word list, and single crack. The most practical and efficient way to crack an entire password file is to use the single crack mode.



Sites
http://192.168.1.3
http://fonts.googleapis.com
GET:css(family)
http://i00.i.aliimg.com
http://safebrowsing-cache.google.com
http://safebrowsing.clients.google.com
http://saveourbones.saveour.netdna-cdn.com
http://static.caloriecount.about.com
http://www.whatsfresh.co.nz
https://ajax.googleapis.com

URL to attack: http://192.168.1.3/work/course
Progress: Attack complete - see the Alerts tab for details of any issues found
For a more in depth test you should explore your application using your browser or automatec
If you are using Firefox 24.0 or later you can use 'Plug-n-Hack' to configure your browser:
Configure your browser:
Or point your browser at: http://localhost:8080/pnh/

Alerts (13)
Cross Site Scripting (Reflected)
Path Traversal (4)
Remote File Inclusion (4)
Application Error disclosure (19)
Directory browsing (2)
Parameter tampering (8)
Cookie set without HttpOnly flag (49)

X-Frame-Options header not set
URL: http://192.168.1.3/work/course/index.php?style=themes/black.php
Risk: Informational
Reliability: Warning
Parameter:
Attack:
Evidence:
CWE Id: 0
WASC Id: 0

Fig 10. ZAP Tool

Resources can be recreated after modifications and decrypted back to their original form using APK tools. Its automation and project-like file structure make working with supporting apps easier.

The ZAP tool features an intuitive interface and offers a range of functionalities, including advanced interception tools, active and passive scanning, and spidering, as illustrated in Figure 10. It has a vibrant user community that supports and updates the tool frequently, along with an extensive amount of documentation.

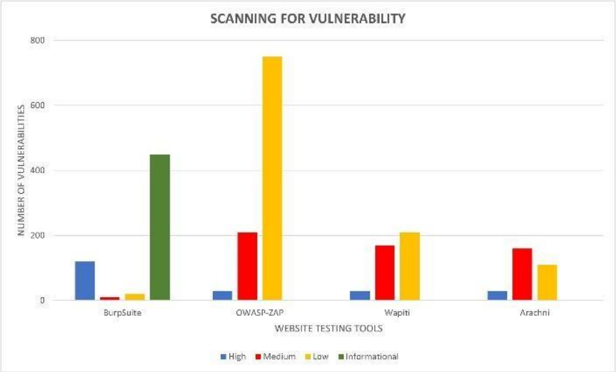


Fig 11. Graph indicating number of vulnerabilities scanned by various website testing tools

Since it can effectively scan for high and medium risks, as shown in Fig. 11, our suggested work incorporating the OWASP-ZAP can be regarded as the best tool for website testing. According to [5], it also scans for a sizable number of low vulnerabilities, which helps mitigate low risks in comparison to other tools.

This paper discusses the critical role that vulnerability assessment and penetration testing tools play in preventing cyberattacks. Organisations must take proactive steps to detect and fix vulnerabilities in their systems and applications due to the rising frequency and sophistication of cyberattacks. Organisations can improve their cybersecurity posture by identifying potential weaknesses and implementing the appropriate corrective measures with the help of a penetration testing and vulnerability assessment system architecture. In order to ensure thorough coverage of potential security risks, this system architecture uses a wide range of different tools and techniques to cover various system components, such as file systems, applications, system services, device drivers, libraries, system calls, and networking. In the face of increasing cyber threats, companies can protect their data, uphold their reputation, and guarantee the continuous integrity of their operations by putting penetration testing and vulnerability assessment tools into place. Therefore, maintaining a high level of security and stability for the systems and data of organisations depends on the use of vulnerability assessment and penetration testing tools in cyber-attack prevention.

Future research and development will focus on creating penetration testing and vulnerability assessment tools that are even more sophisticated and advanced, Future research and development will focus on creating penetration testing and vulnerability assessment tools that are even more sophisticated and advanced, and that have improved features like network mapping scanning and reporting to help find and fix complex security vulnerabilities like fileless malware, supply chain attacks, and advanced malware. In order to offer more thorough and proactive defence against cyber threats, there is also a great deal of room for additional research into the integration of vulnerability assessment and penetration testing tools with other cybersecurity technologies, such as artificial intelligence and machine learning.

REFERENCES

[1] E. Pelivani and B. Cico, "A comparative study of automation testing tools for web applications," 2021 Embedded Computing (MECO), Budva, Montenegro, 2021.

[2] R. Pandey, V. Jyothindar and U. K. Chopra, "Vulnerability Assessment and Penetration Testing: Aportable solution Implementation," 2020 12th Global Conference on Computational Intelligence and Communication Networks (CICN),

[3] Kavya Rani S R,Soundarya B C, "Comprehensive Analysis of Various Cyber Attacks", IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE), 2022

[4] D. Delija, Ž. Petrović, G. Sirovatka and M. Žagar, "An Analysis of Wireless Network Security Test Results provided by Raspberry Pi Devices on Kali Linux," 2021 44th International Convention on Information, Communication and Electronic Technology (MIPRO), Opatija, Croatia, 2021

[5] Shahid, J.; Hameed, M.K.; Javed, I.T.; Qureshi, K.N.; Ali, M.; Crespi, N. Comparative Study of Web Application Security Parameters: Current Trends and Future Directions. Appl. Sci. 2022

[6] A. S. Laxmi Kowta, K. Bhowmick, J. R. Kaur andN. Jeyanthi, "Analysis and Overview of Information Gathering & Tools for Pentesting,"International Conference on a Computer Communication andInformatics (ICCCI),pp no. 1-13 Coimbatore, India,

[7] Disha Pahuja, Prerna Sidana,"Implementing and Comparing Different Password Cracking Tools," International Research Journal of Engineering andTechnology (IRJET) Volume: 08 Issue: 05 | May2021

[8] S.R. Kavya Rani, B. C. Soundarya, H. L. Gururaj and V. Janhavi, "Comprehensive Analysis of Various Cyber Attacks," 2021 IEEE Mysore Sub Section International Conference (MysuruCon), Hassan, India, 2021

BIOGRAPHIES:

G Swaroop
Department of Computer Science and Engineering,
Atria Institute of Technology.

Harish Budarpu
Department of Computer Science and Engineering,
Atria Institute of Technology.

Manasa B N
Department of Computer Science and Engineering,
Atria Institute of Technology.

Asst. Professor Meghashree N
Department of Computer Science and Engineering,
Atria Institute of Technology.