*2020 International Conference on Computational Performance Evaluation (ComPE),*
*North-Eastern Hill University, Shillong, Meghalaya, India. July 2–4, 2020*

# A Study on Metasploit Framework: A Pen-Testing Tool

Sudhanshu Raj
*Deptt. of Computer Science and Engineering,*
*Chandigarh University,*
Mohali, Punjab, India
cu.18bcs6576@gmail.com

Navpreet Kaur Walia
*Deptt. of Computer Science and Engineering,*
*Chandigarh University,*
Mohali, Punjab, India
navpreet.walia12@gmail.com

***Abstract*—In today's world, the usage of internet is everywhere. It plays an important part in the life of humans. As we all know that the Internet has made the life of humans much easier not only in personal but also in professional aspect. This ease in life has given birth to so many threats and flaws that are further giving access to the intruders known as 'Hackers' to enter in a user's private space and perform some activities which can be very harmful for that particular user. In this paper, we will discuss about the Metasploit Framework tool which is always used by the Hackers & Pen-testers to perform activities i.e. from Scanning to exploiting the systems.**

***Index Terms*—Internet, Threats and Flaws, Hackers, Pen-testers.**

## I. Introduction

Over the past few years, IT industries are adding more features and accessibility in the existing applications and producing new applications for the benefit of the customers as well as employees. These additional functionalities boost up the Hackers for always seeking for the vulnerability by which they can exploit and can perform some activities like stealing private and confidential data, getting access to user bank accounts and so on. The engineers are giving their best to cover all the vulnerabilities by which they can stop the Hackers. However, vulnerabilities are not limited and can be accidentally elicited in systems or resources that are operative for an extended period. To stop the intruder activities, the companies are using a testing named as Pen- testing which is discussed in the next section.

## II. Pen-Testing

Pen-testing is the short form of Penetration Testing and is also known as Ethical hacking. Pen-testing is method of tracking the security vulnerabilities in a computer system, network or net application that a hacker may exploit [1]. penetration testing is often machine drive with package applications or performed manually. The method involves gathering of the data regarding the target before the check, characterizing the potential entry points, trying to interrupt in either nearly or for real and coverage back the findings.

### A. Early History of Pen-Testing

Computer protection professionals as early as 1965 warned authorities and commercial enterprise that the growing capacity of computers to alternate information across communication lines would inevitably lead to attempts to penetrate those strains and attain get right of entry to the information being exchanged [2]. At the 1967 annual Joint Computer Conference that added together greater than 15,000 laptop security experts, government and business analysts mentioned issues that PC verbal exchange lines may want to be penetrated, coining the time period and figuring out what has emerge as possibly the essential task in PC communications today. The idea of definitely testing systems to make sure their integrity arose with the main security networks such as the [3] RAND Corporation that first recognized this now major threat to internet communication. The RAND Corporation, in cooperation with the Advanced Research Projects Agency (ARPA) in the USA [4], produced a seminal report, typically called The Willis Report after its lead author. The record discussed the security problem and proposed policy and technical considerations that even these days lay the groundwork for security measures. From this report, government and enterprise commenced to put together teams that would strive to discover vulnerabilities in laptop networks and structures to defend the laptop structures from unethical hacking or penetration. So-called tiger teams, named after specialized army teams, have been fashioned in the late 1960s to check the ability of pc networks to resist attack. Most systems failed shortly and abysmally. The penetration testing [3], generally carried out via the RAND Corporation and government, confirmed two things: first, systems may want to be penetrated and second, the usage of penetration checking out strategies to perceive vulnerabilities in systems, networks, hardware, and software program was a beneficial exercising that wanted to be further studied and developed. Now a days the most useful tool used in the pen-testing as well as in hacking are as follows [5]:

- Metasploit Framework: Scanning to extracting.
- SQL Map: Database extraction
- OWASP Zed: Web application security scanner
- Wireshark: Profiling network traffic and analyzing packets.
- Nmap :Network Discovery
- Aircrack-NG

978-1-7281-6644-5/20/$31.00 © 2020 IEEE

Table I: Comparison between NMap, Sql Map, Metasploit

| NMAP | SQL MAP | METASPLOIT |
|---|---|---|
| Perform tasks like network inventory, managing service upgrade schedules, and monitoring host or service uptime. This tool is used in hacking and the main work of this tool is to scan the networks and hosts. | The tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. This tool is generally used for exploit the SQL Injection vulnerability in website. | Metasploit permits its customers to access its source code and add their custom modules. Various other exceedingly paid tools exist for carrying out penetration testing. Performs tasks from scanning to exploiting on Web, Software, O.S, and so many platforms. |

### B. Comparison between the Tools

*1) Metasploit Framework:* It has so many different module for different platforms and devices. It has 4 main modules [6].

- Exploit: A way to attack compromised system threat.
- Payload: The hacker is able to get data by interacting with target.
- Auxiliary: Used to test, scan or recon the target.
- Encoders: Used for evading Firewall & Anti-virus.

*2) SQL Map:* Used to detect and exploit SQL injection vulnerability automatically(for rest please see Appendix A). Options available are as follows:

- Acquire Database list
- Acquire Table list
- Acquire Column list
- Dump everything acquired

*3) OWASP ZAP:* All in one web application security auditing tool. It has so many features, such proxy server, AJAX web crawler, web scanner, and fuzzer. When used as proxy it let hacker to manipulate the data from the traffic(for rest see Appendix B) [6].

*4) Wireshark:* It let the hacker to sniff and capturing the network traffic which is very helpful for network analysis, troubleshooting, vulnerable assessment(for rest see Appendix C).

*5) Nmap:* The best network auditing tool used for network discovery i.e. host, port, service, OS and vulnerability detection(for rest see Appendix D) [7].

### C. Aircrack-NG

A complete network auditing tool to assess wireless network connection(for rest see Appendix E). It has 4 categories [8]:

- Capturing
- Attacking
- Testing
- Cracking

Yet, Metasploit is the most powerful tool among others because it provides its service from Scanning to exploiting and extracting. Also the most usable and popular tool used by the Pen-testers as well as by the hackers is the Metasploit Framework which is explained in the next section.

## III. Metasploit Framework

The Metasploit, Framework is a project that has the information regarding security vulnerabilities and aids in penetration testing and IDS development. It's closely held by Boston, Massachusetts based security company RAPID7 and its known sub-project is the Metasploit Framework. It is especially designed for anti-forensics and evasions [9]. This tool comes pre-installed in the pen-testing operating systems like Kali Linux, Parrot O.S, etc. It can also run on termux in android system. This is the tool that is always used while hacking in some one's system by the hackers [2]. This tool has various types of payloads for various platforms like Windows, Linux/Unix, Android, CCTV, etc. and is also used for the Scanning purpose like open port scanning, etc. This tool may be a standard penetration testing platform that permits hackers to write down and execute exploit code. It contains a collection of tools that a hacker will use to check security vulnerabilities, enumerate networks, execute attacks, and evade detections.

### A. Early History of Metasploit Framework

Metasploit used to be created by way of H. D. Moore in 2003 as a portable network device using Perl. By 2007, the Metasploit Framework had been definitely rewritten in Ruby [10]. On October 21, 2009, the Metasploit Project announced that it had been obtained by way of Rapid7, a safety enterprise that offers unified vulnerability management solutions. Like related business products such as Immunity's Canvas or Core Security Technologies' Core Impact, Metasploit can be used to test the vulnerability of laptop structures or to smash into far off systems. Like many data safety tools, Metasploit can be used for both reputable and unauthorized activities. Since the acquisition of the Metasploit Framework, Rapid7 has added two open core proprietary versions called Metasploit Express and Metasploit Pro. Metasploit's emerging role as the de facto exploits development framework led to the release of software vulnerability advisories regularly accompanied by way by a third party. Metasploit take advantage of module that highlights the exploit-ability, risk, and remediation of that particular bug. Metasploit 3 commenced to encompass fuzzing tools, used to discover software vulnerabilities, rather than simply exploits for recognized bugs. This avenue can be considered with the integration of the lorcon wireless (802.11) tool-set into Metasploit 3 in November 2006. Metasploit 4 was launched in August 2011 and currently it is having following interfaces.

- Metasploit Framework Edition
- Metasploit community Edition
- Metasploit express
- Metasploit pro
- Armitage

## IV. Metasploit Framework in Kali Linux

This tool comes pre-installed in this operating system and plays a major role in performing the exploiting task. The steps for starting this framework is as follows:

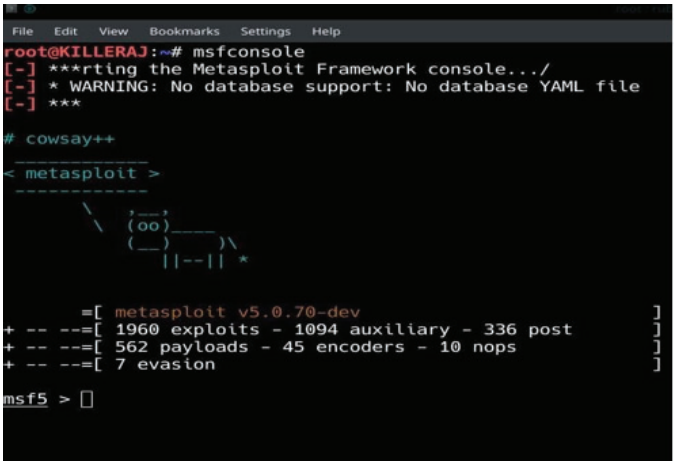


Figure 1: Metasploit Terminal Console

Step 1 : Tap CTRL+ALT+T or click on terminal icon to directly open the terminal on screen.

Step 2 : Type msfconsole in the terminal and the non-graphical console of the Metasploit framework will run on the terminal as shown in Figure 1.

.

### A. *Different Keywords in Metasploit Framework*

*1) Search:* The search keyword is the command which is used in the Metasploit Framework to search any type of module i.e. payloads, exploits, host, port scanning, etc. for every platform. For the search keyword, all the payloads currently present in the Metasploit Framework directory is searched by typing search payloads after the opening of the Metasploit framework console in the terminal, as shown in Figure 2.

**Syntax:** Search Payloads

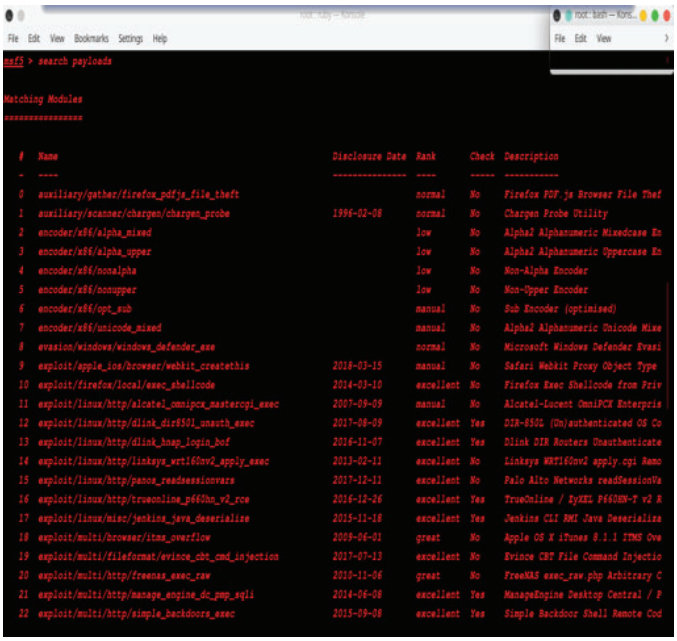


Figure 2: List of Payload

### B. *Use*

The use keyword in the Metsploit framework is used to use the particular module present in the Metasploit framework.Syntax: use module name

For example: If user want to use SHODAN which stands for Sentiment Hyper-Optimised Data Access Network [11].

The steps needed to be followed after opening theMetasploit console are:

- Search shodan
- Use auxiliary/gather/shodan$_s erach$

and it will lead to starting the shodan as shown in Figure 3.

### C. *Exploit and Run*

This keyword is used to exploit the vulnerability which is currently present in the target system after providing the right set of payloads and the platforms in the Metasploit Framework console. After the run, the Metasploit Framework will connect with the target system and will give access to the Hacker to see, steal and change the data present inside the target

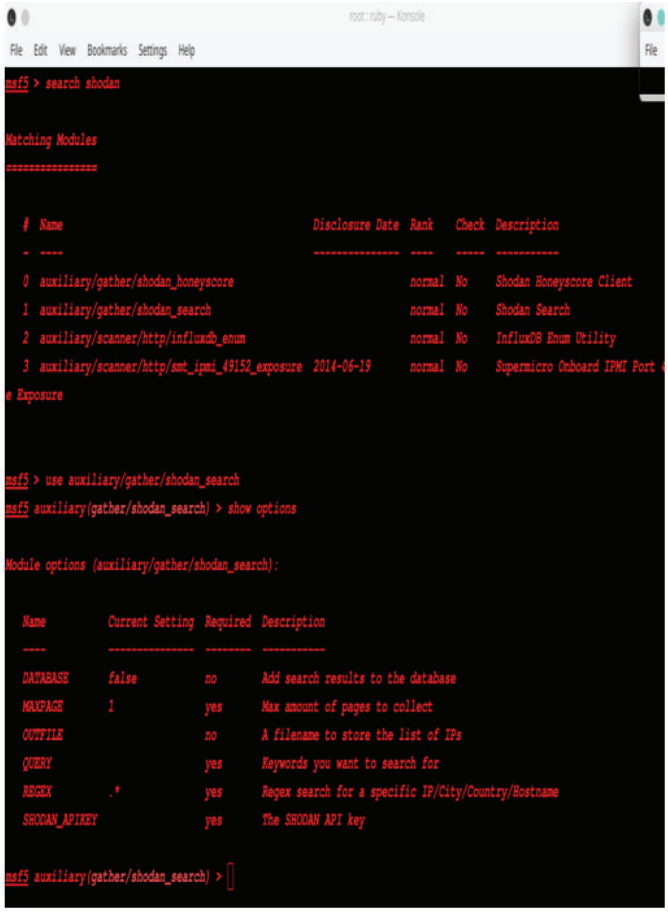


Figure 3: Shodan module of Metasploit

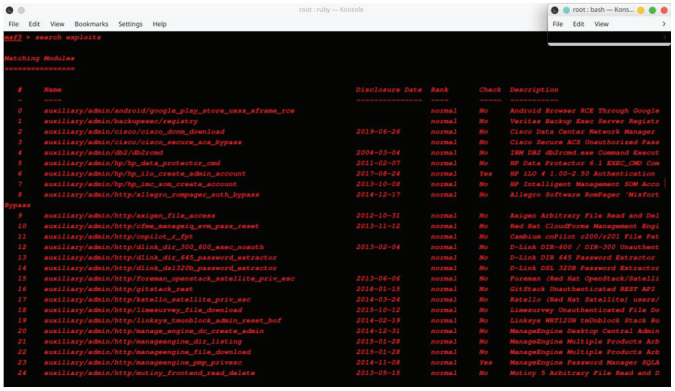

Figure 4: Exploits List Beginning

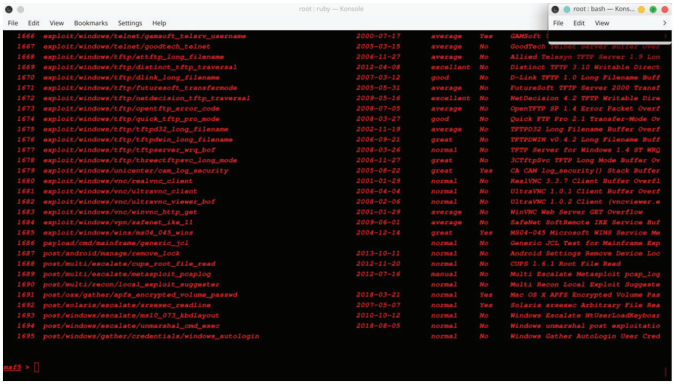

Figure 5: Exploit List Ending

system. There is a total of 1695 exploits currently present in the Metasploit as shown in Figure 4 and Figure 5.

The process goes like this: search → use → exploit.

### D. Servers used in Metasploit framework

There are some servers that comes pre-installed in kali Linux that a hacker needed to start before running the tool Metasploit framework, with its help hacker can get connected with the target after exploiting the target system as shown in Figure 6 and Figure 7. The list of servers which comes pre-installed in kali Linx are as follows:

- apache2
- postgresql
- simplehttpserver

**Syntax:**

1. For starting : service server-name start
2. For Status : service server-name status
3. For stoping : service server-name stop

## V. Implementation of Metasploit Framework on Android Operating System

Android operating system version 9.0.0_r52 PIE is used for testing in Metasploit framework tool. The modules used in this testing are the handler, reverse connection, meterpreter and the payload for the android platform is generated with the help of Msf-venom.

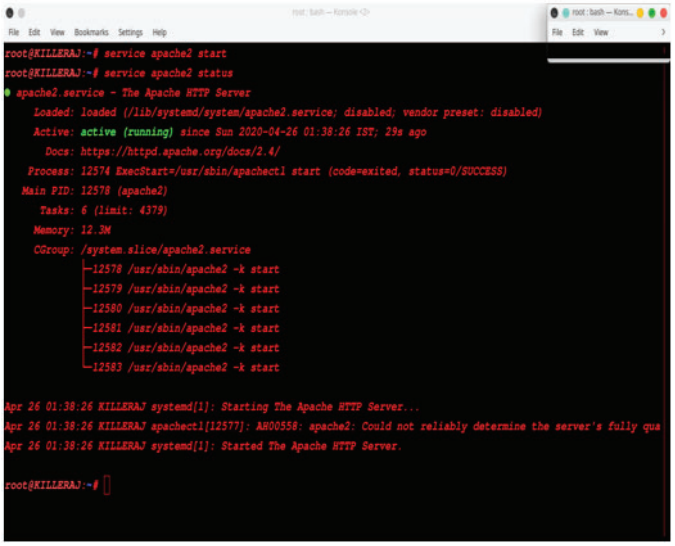

Figure 6: Server startup and status

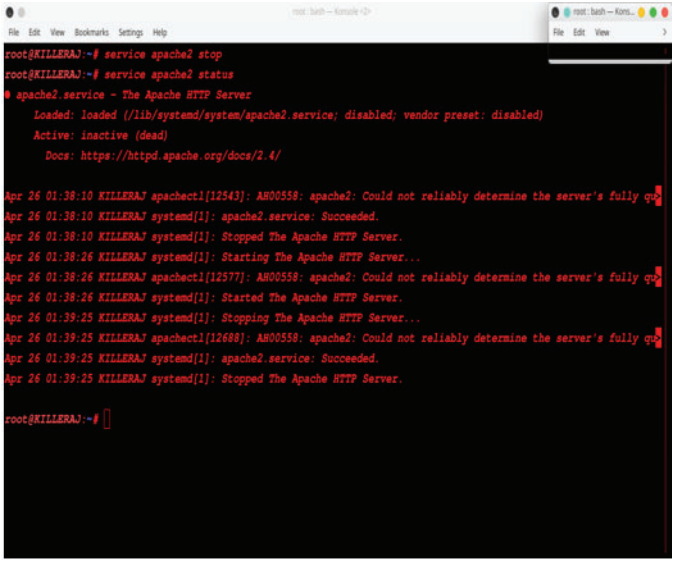

Figure 7: Server Stoping & Status

### A. Handler

The handler can be started at any time with Metasploit, this is used to handle the requests of the target's machine and makes a reverse connection to take back the control. Now let's discuss the steps needed to start handler at the same port of the backdoor.

The steps to run the handler in Metasploit with the command are as follows:

1. msfconsole
2. msf¿ use exploit/multi/handler

### B. Reverse Connection

A reverse connection is typically used for bypassing fire wall restrictions on open ports. A fire wall typically blocks incoming connections on open ports however doesn't block


Figure 8: Msf-venom bug generation

outgoing traffic. In an exceedingly traditional forward affiliation, a consumer connects to a server through the server's open port. However within the case of a reverse connection, the consumer opens the port that the server connects, and the foremost common means a reverse connection is employed to bypass firewall and router security restrictions.

### C. Msf-Venom

Msfvenom is a Metasploit Standalone Payload generator which is a replacement of msfpayload and msfencode [12]. Through msfvenom module, the user will be able to generate any reasonably shellcod/payload relying upon the platform in which the user would like to hack.

**Syntax:**

msfvenom -h (for helping)

msfvenom –platform (for checking platforms) msfvenom -p [payload] LHOST=[listeninghost]

LPORT=[listeningport]¿R .apk (payload generation)

## VI. Testing Case

Here a bug is created (Figure 8) for the android platform with the help of msfvenom, a file with .apk extension is generated which can be installed in the target android system and the name of that application after installation will be Main Activity. Hacker need to paste that payload to the HTTP local server folder located in the OPT directory for injecting the bug in target's android system by accessing the that address where app is copied.

### A. Starting the local server

Now starting one local server from the three discussed above i.e.

- Apache2
- postgresql
- simplehttpserver

After starting the server a web address of the IP same used at the time of creating the payload is created, then accessing that specific IP and putting a slash (/) and the payload name after the IP address to download bug, then install it in the target android system.


Figure 9: Starting of Listener

### B. Starting msfconsole

The last exploiting process is done by the Msfconsole [6]. The steps to follow are:

Step1: Open the terminal and type msfconsole

Step2: use multi/handler

Step3: set payload android/meterpreter/reverse_tcp Step4: set LHOST IP & LPORT numbersame as the payload

Step5: exploit/run for exploiting the target system. Step6: Finally a listener will start on the terminal screen as shown in Figure 9.

A meterpreter session will get open which provides a backdoor access to the target's system. The tasks which can be performing in this session are as follows.

- Can execute shell code as shown in Figure 10.
- Check call logs, Contacts, Messages as shown in Figure 11.
- Can install any application as well as can access the list of applications installed.
- Can access the Cameras (Front & Rear), etc.

## VII. Conclusion

We all are in an era in which no physical weapon is required for war instead of that if a country wants to start a war then a bunch of hackers from that country can start a cyber-war against any country. They can get access to the restricted and confidential resources of the target country by doing some intrusions to the database of banks customers, Military, E-commerce websites. They get the credentials of the user and sell them for a good amount of money. The term hacking which is repeatedly used in this paper is elaborated in this


Figure 10: Meterpreter command list 1st

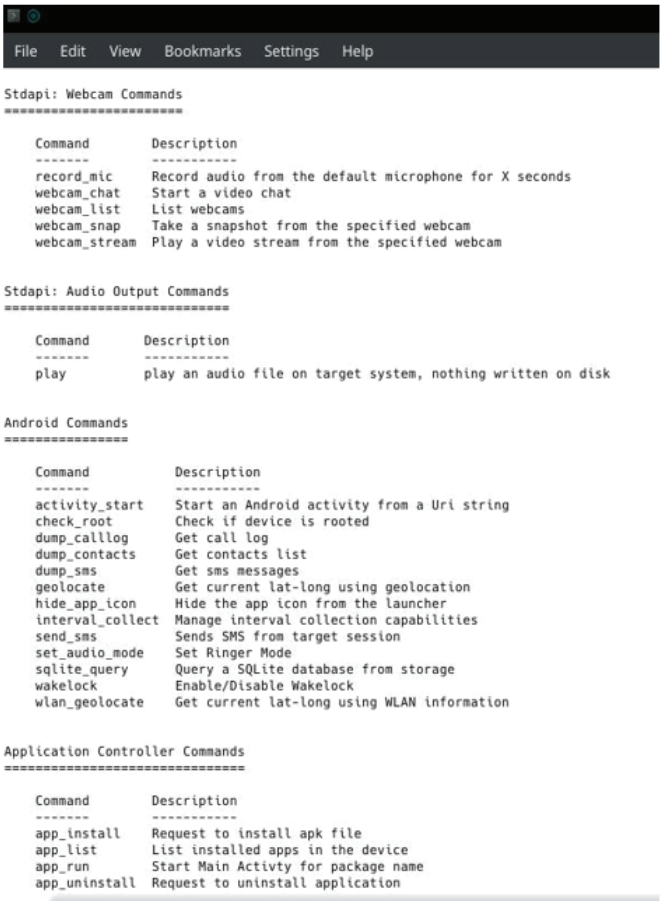


Figure 11: Meterpreter command list 2

paper. Also, the most popular tool used by the hackers to attack and exploit any system i.e. Metasploit Framework as well as all the options that a hacker can opt i.e. Servers, Payloads, Virus/bug, Exploits, etc. are discussed in this paper. By the paper, the basics of the Metasploit Framework i.e. how a hacker can get access to anyone's system and after getting access what commands a hacker can execute remotely in target's system is discussed. All the test process discussed in paper of Android version 9.0.0_r52 PIE are practically implemented with the help of Kali Linux 2019 O/S and are found that Metasploit Framework is a very effective tool for hacking purpose. In future there will be a lot of scope of Penetration Testing and security. We are observing that world is digitizing day by day, now it will be convenient to hack Peoples now not their machines or system however Hacking Peoples, creativeness is becoming reality. So to prevent these, we need loads and lots of Security and Pen-testers, because who will save them. By upgrading the system doesn't imply that hackers doesn't evolve and adopt the Environment. The goals of the paper is to show the gaps in security and discover the threats by which a hacker can get access to system and what activities it can perform specially in Android smart phones.

## REFERENCES


[1] D. Maynor, *Metasploit toolkit for penetration testing, exploit development, and vulnerability research*. Elsevier, 2011.

[2] M. Moore, "Penetration testing and metasploit," 2017.

[3] A. Fiat and M. Naor, "Broadcast encryption," in *Annual International Cryptology Conference*. Springer, 1993, pp. 480–491.

[4] M. E. Gallo, "Defense advanced research projects agency: Overview and issues for congress," *Congressional Research Service*, 2018.

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

[6] "Owasp zed attack proxy project - owasp," https://www.linuxsecrets.com/owasp-wiki/index.php/ZAP.html, (Accessed on 08/11/2020).

[7] J. Messer, *Secrets of Network Cartography: A comprehensive guide to nmap*. Professor Messer, 2007.

[8] B. F. Murphy, "Network penetration testing and research," 2013.

[9] C. B. E. C. A. G. L. L. J.-P. M. R. N. H. G. P. S. P. P.-F. R. W. R. M. S. B. S. D. B. L. v. d. V. F. H. S. v. Ludolph, Albert C; Bendotti, "Guidelines for preclinical animal research in als/mnd: A consensus meeting," *Amyotroph Lateral Scler*, vol. 11 (1-2), pp. 38–45, 2010.

[10] W. Chen, "Encapsulating antivirus (av) evasion techniques in metasploit framework," *Rapid*, vol. 7, p. 2018, 2018.

[11] S. Verma, "Searching shodan for fun and profit," *Research paper.[Internet]. Available: http://www. exploit-db. com/docs/33859. pdf*, 2014.

[12] "Metasploit cheat sheet - sans institute download printable pdf — templateroller," https://www.templateroller.com/template/262828/metasploit-cheat-sheet-sans-institute.html, (Accessed on 08/10/2020).


## APPENDIX A

SQL map is an open source pen-testing tool that automates to detect and exploit SQL injection flaws and takeover the database servers. It comes with an effective detection engine, It provides a variety of options such as database extraction and dumping all the data wherever the hacker wants. It supports MySQL, Oracle, PostgreSQL, Microsoft SQL Server,

Microsoft Access and so many different types of database management system.

## APPENDIX B

OWASP ZAP (short for Zed Attack Proxy) is an open-source internet software security scanner. It is intended to be used by using both these new to application safety as well as expert penetration testers. It is one of the most energetic Open Web Application Security Project (OWASP) initiatives and has been given Flagship status. When used as a proxy server it allows the consumer to manipulate all of the site visitors that passes thru it, inclusive of traffic the usage of https.

## APPENDIX C

The world's foremost and widely-used network protocol analyzer. It is rich in features like:

- Live data can be read from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI, and others (depending on your platform)
- Decryption support for many protocols, including IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, and WPA/WPA2

## APPENDIX D

Nmap stands for Network Mapper is a free and open source utility for network discovery and security auditing. Many structures and network administrators additionally discover it beneficial for duties such as network inventory, managing service improvement, and monitoring host or service. It uses raw IP packets in novel approaches to determine what hosts are handy on the network, what application name and version these hosts are offering, what's the OS versions they are running, what kind of packet filters/firewalls are in use, and dozens of different characteristics.

## APPENDIX E

It's a complete suite of tools to assess Wi-Fi network security. It focuses on different areas of Wi-Fi security like packet capture and export of data to text files for further processing by third party tools. It also Replay attacks, do deauthentication, and make fake access points and others via packet injection. It also checks Wi-Fi cards and driver capabilities.