Design and Development of Rapid Penetration Testing Framework

Harmandeep Singh
Research Scholar, Department. of Computer Science & Engineering,
NIILM University Kaithal, Haryana,

Pankaj Kumar Verma
Associate Professor, Department. of Computer Science & Engineering,
NIILM University Kaithal, Haryana,

Surender Jangra
Assistant Professor, Department. of Computer Applications,
GTB College, Bhawanigarh, Sangrur, Punjab.

Abstract- In today's world, more and more people are using the internet. With this, the number of cyber attacks is also increasing on government and private entities. The damage caused by sabotage and the intellectual property theft amounts to several billions of crores every year. Also the cyber attacks are dynamic and asymmetric in nature. The network security is one of the biggest challenges to us. The penetration testing provides the solution for this problem. Penetration testing is used to find the vulnerabilities in the system or network before they can be exploited by hacker. Penetration testing helps in evaluating the security posture of any organization or network. In this paper the process of performing the penetration testing is explained. This paper proposes a rapid penetration testing model for performing the penetration testing. We also discuss the design and development of this new platform and the results are taken on the local area network. The results show that framework provides an automatic, rapid and easy to deploy methodology for performing the test and overcomes the drawbacks of existing frameworks.

Keywords – VAPT, Kali Linux, DMZ, DDOS, SSH, XSS (Cross- site scripting), TCP/IP, PGP.

I. INTRODUCTION

Millions and millions of people across the world today share the similar habit, that is of using the internet. It is not surprising that this number is still increasing. People are using the internet for accessing the government services, financial transactions, academics, entertainment and lots of more things. But the alarming fact which worries the world is that the number of cyber crimes is also increasing with the internet usage. It has become quite difficult for companies to keep their confidential information secret with their presence on the internet. Though many security techniques like firewall, cryptography, demilitarized zone (DMZ) are already in use to tackle this problem. But they are found to be in sufficient. So it is better to check the security by thinking and acting like a hacker.

Penetration testing [1] is a process to search out the loop holes or gaps existing in the network or system. It is a technique which act and work like a hacker. By analyzing all the security measures, the tester tries to illegally break these to enter the network. The aim is to identify the vulnerabilities and report it to programmer so as to fill them before they can be exploited by malicious user.

Penetration testing is of three types. Black box, gray box and white box penetration testing. When there is no information available for performing the test about target, it is black box penetration testing [2]. When limited information is available, it is grey box. If complete information is available, it is known as white box penetration testing. Mostly black box penetration testing is performed on systems or network.

II. RELATED WORK

This section discusses the findings of some important papers.

William G. J. et al [2011] [11] uses the two new techniques for improvement of input vector identification and attack detection against the existing techniques. The proposed approach provides the better results than existing one. More number of vulnerabilities are found with this new approach. A.Bechtsoudis et al [2012] [10] performed the penetration testing at the network layer to find the exploitable vulnerabilities. To achieve the goal, the author set up the lab network and performed the test for exposing the loopholes. Brandon F. Murphy [2013] [9] performed yet another attack on window 7 operating system from Linux system with the help of Backtrack 5 and BlackBuntu operating system. They not only performed the attack but also tried to retrieve the host's information. Sugandh Shah and B. M. Mehtre [2014] has also explained the techniques of penetration testing using their own methods and guidelines. Some of the tools that were used for performing the testing and assessment are discussed in this paper.

According to Jai Narayan Goel et al [2015] [5], VAPT can be used as an important tool against cyber crime.. He has further described about some open source tools and techniques that can be used for testing. Suraj S. Mudalik [2015] [4] explained that it is better to make our system flawless before deploying them. According to him system can be simulated with number of attacks with the help of kali Linux and backtrack using open source tools. For the penetration testing, Munir A. Ghanem [2015] [3] suggests the use of various tools which are present in Backtrack Linux operating system. To name a few, there are nmap, wireshark, ettercap, and metasploit and browser exploitation framework. Deris Stiawan et al [2016] [2] in his research performed the penetration test and identified the vulnerabilities in the window server. The author performed the denial of service and brute force attack thus finding some loop holes or vulnerabilities in the system.

III METHODOLOGY

The methodology tells the step by step process to perform the penetration test. The whole process of penetration testing is divided into four parts.

- Reconnaissance about target.
- Identify vulnerabilities.
- Scanning and attack
- Result Analysis and Report generation.

In information gathering or reconnaissance [6] stage, our aim is to gain maximum information about our target using the commands like ping, ipconfig or many more. Internet is also helpful to collect the public information about the operating system of the target. Vulnerability Identification [12] targets at extensive search of the various loop holes present in the target system or network which some hacker could exploit negatively. It can then audit the system for vulnerabilities in the software.

At the third stage, penetration tester [13], attempts to exploit the loopholes that were recognized in previous stage. Sometimes tester use existing exploits and payloads for this purpose. If none is suitable, then it writes its own exploits for penetration test. This step has to be performed with extra care because it can lead to destruction of sensitive data. In the last stage, report is prepared for the management showing the result of the test. The test should also give the recommendation about how to increase the security of systems or network.

IV. IMPLEMENTATION

In this Virtual local area network is established using the VMware workstation 12. The machines are made of windows Xp, windows 7 and Debian7. In the framework the major focus is on reconnaissance, bruteforcer and scanning programs. In reconnaissance part, we are using the reconng and the harvester. In brute forcing part, ncrack and medusa will be considered. In scanning part, we will be considering the scapy and hping3. In this framework we are checking the strength of some tools. Our objective is to find at what time and in which condition in the process of penetration testing, which program is the best.

Reconnaissance

In the information gathering or reconnaissance the penetration tester wants to gather information about the network or system on which attack has to be performed. It has to be done before attack has to be performed.

The theharvester program is used to gather information about emails, sub domains, hosts, open ports and banners from different sources like search engine, PGP key servers and SHODAN computer database. It helps the penetration tester to understand the customer footprints on the network. The recon-ng program of the penetration testing is developed in python. It provides modules like hosts, netcraft, auxiliary, pwnedlist, contacts and many more. In the netcraft module, it displays all domains associated with provided domain in set source value. The different commands used for information gathering are:

1. Apply the commands as: Use netcraft→ show info→Show options.
2. Set source sans.org and run. It will start gathering information.
3. Apply the show hosts command. It will display all the hosts of sans.org.
4. First apply the recon/hosts-hosts/resolve module and show options and then run. This module will automatically pick value from hosts list and will perform IP resolution. Then perform the command show options, it will display all hosts and their ip address.
5. Then Use the command use geoip. Then perform the run command to find the geographical location. And then apply the show hosts command , that will display all hosts, their ip and their country, lattitude and longitude position.
6. Use the Pgp_search module: to check emails on PGP. For this use the command use pgp. Then show options and apply the run command. Then s apply the show contacts command. It will display all the email contact list on the server.
7.Recon- ng provides the reporting feature. For this apply the command use report. Then use reporting/html→ show options→ set creator test →set customer test→run. It will generate the report.

Based on the working of the harvester and recon-ng tool, a comparative approach is designed based on the following metrics.

	The Harvester	*Reconng*
Ease of Usage	Easy to use Self-explanatory program One just need to check help	Tough to use as prior reconng module knowledge required. As well as, framework knowledge required to work with recon-ng.
Time Factor	Takes a time to display output	Quickie
Information Digging Parameter	Dig information only about sub domains and emails.	Wide information will be fetched due to the different available modules. Such as ip resolve, geo location, ip neighbors and so on.
Additional Cost and Efforts	Not as such	Cost will be charged for bringing up an api from particular domain such as LinkedIn, twitter,shodan.
Add-ons Feature	DNS brute forcing	Can check for some vulnerabilities as well. Like: *econ/hosts/enum/http/xssed* *Module for checking XSS vulnerability.*
Reporting	Very Good Report-making feature	Report quality is not as good, although automatically add host and contact list based on modules search.

Brute forcing

Brute forcing is a technique to find the passwords without the authorization. By this, we check that how secure is our password. The attacker or hacker systematically checks all possible combinations of passwords and passphrases until the correct one is found. The success is depend mostly on password length and combinations of alphabets. Many tools are used to perform brute force attack such as burp suite intruder, hydra, ncrack, medusa etc. Our focus is on ncrack and medusa. Using these tools, user can check for bad passwords.

Ncrack is a program used by the organizations to check the strength of their passwords. It provides a command line interface for launching the attack. The command of ncrack for SSH brute forcing is:

SSH bruteforcing: *ncrack -p 22 --user overflow -P password.txt 192.168.1.3*

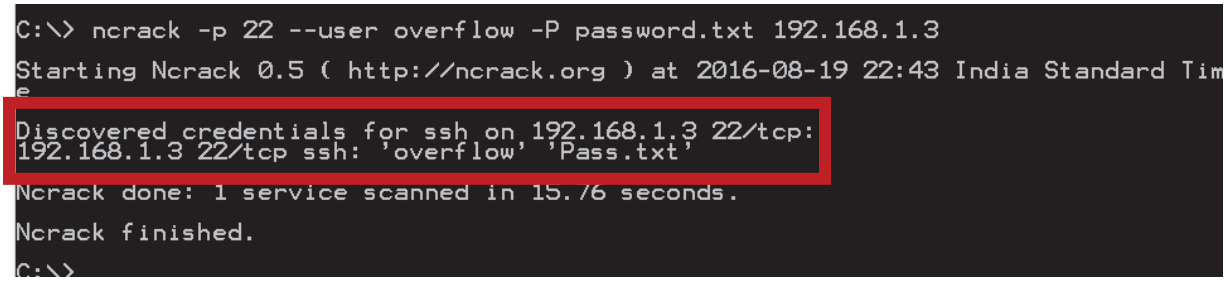


Fig1: Ncrack SSH brute attack

Medusa is intended to be a speedy, massively parallel, modular, login brute-forcer. It supports many protocols: AFP, CVS, FTP, HTTP, IMAP, rlogin, SSH, Subversion, and VNC to name a few. It is an open source software password auditing tool for Linux that will put all of your organization's passwords to the test. The command for medusa usage is:

SSH Brute-force attack: *medusa -u overflow -P password -M ssh -h 192.168.1.3*

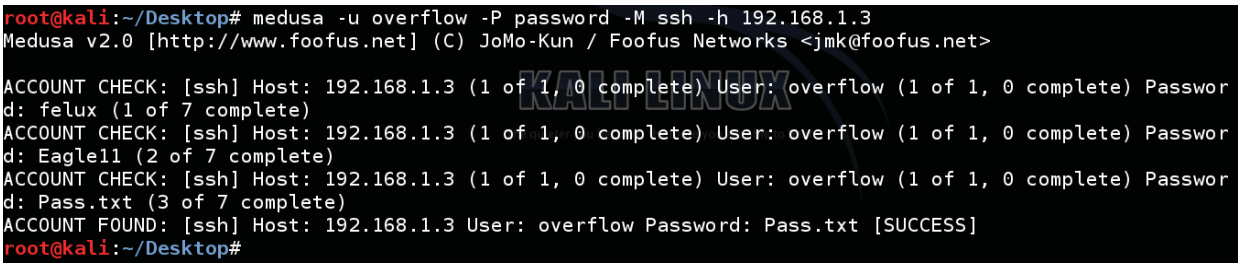


Fig2: Medusa SSH Brute Force Attack

A comparative approach is designed based on the following parameters.

	ncrack	*medusa*
Ease of usage	Easy to use	Module knowledge required
Speed Factor	Quick	Slow
Advancement	Can take an input parameter from nmap outputs/reports.	Everything needs to provide manually.
Other Tool Compatibility	Works great with nmap.	No tool compatibility.

Scanning:

In this part of the penetration testing, various attacks are found based on the vulnerabilities. Hping3 is program which sends the TCP/IP packets. It is used for checking the whether the ports are filtered or not. It is also used to find which ports are open and close. It also perform port scanning using different packet size and different protocols. It is used to implement the DDOS attack using the following command.

hping3 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.1.1 –V.

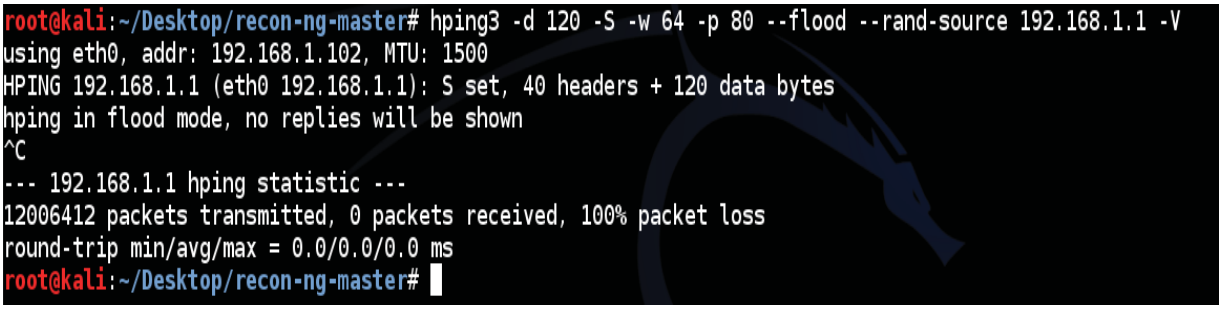


Fig3: DDOS hping3

Scapy is a program used for packet generation, sniffing and port scanning. It is developed in python language. Denial of Service is implemented using Scapy and Hping3 and response is measured in wireshark. Based upon it a comparative approach is designed

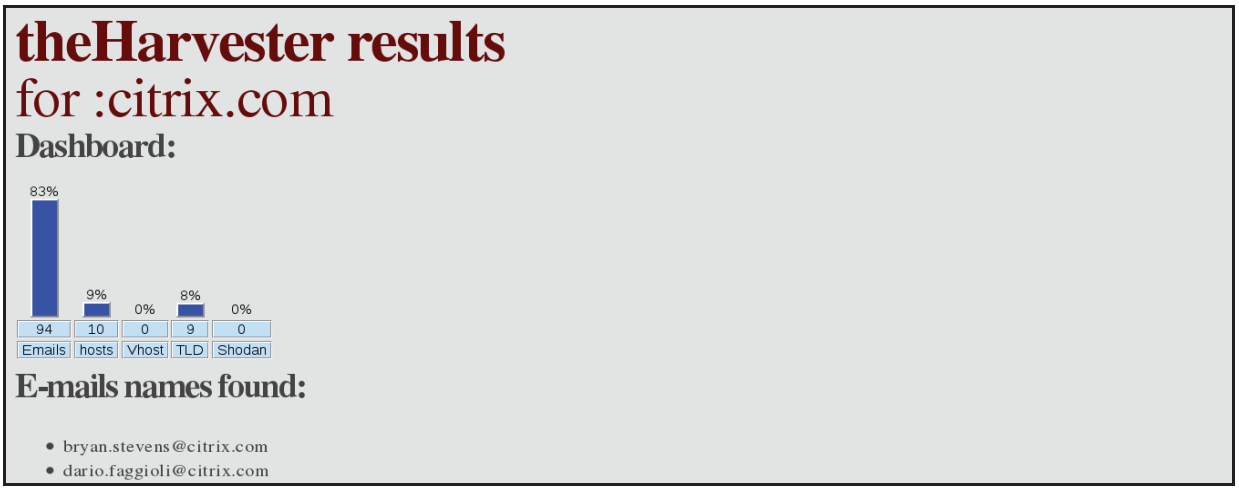
	Hping3	*scapy*
Ease of usage	Moderate to use. Help menu helps a lot.	Scapy commands, packet crafting in scapy and syntax need to check or learn before starting.
Advancement (Future Aspects)	Less scope as limited headers scanning available.	Scapy is independent packet crafting tool with many more features like inbuilt tshark like feature, compatibility with python language. Can be used in future for more advanced scanning tools.
Attack Performance	Ease of exploiting attack such as DOS.DDOS using hping3 is easy. -a: spoof --random-source: for random source addresses	Tough to perform attacks as full scapy framework, commands knowledge required.
Firewall Evasion	Useful in evading firewall.	Can help in evading firewall very wisely but skilled user can do this that has full knowledge about packet crafting and packet headers.
Packet Crafting	Not from Scratch packet crafting	User can build packets from scratch.

IV. RESULTS

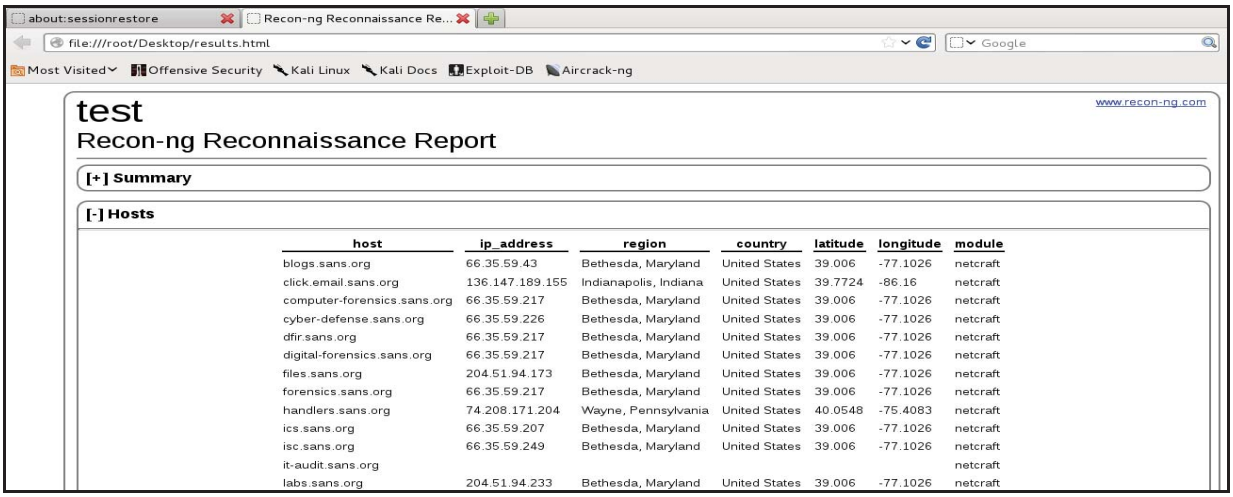
In the reconnaissance with the harvester tool, the report is generated with the following command on citrix.com.

theharvester –d citrix.com –t –l 500 –b pgp –f test

It will list all the citrix.com emails on PGP (Pretty Good Privacy). Which is an email security standard. It also finds its sub domains and also perform host name resolution.



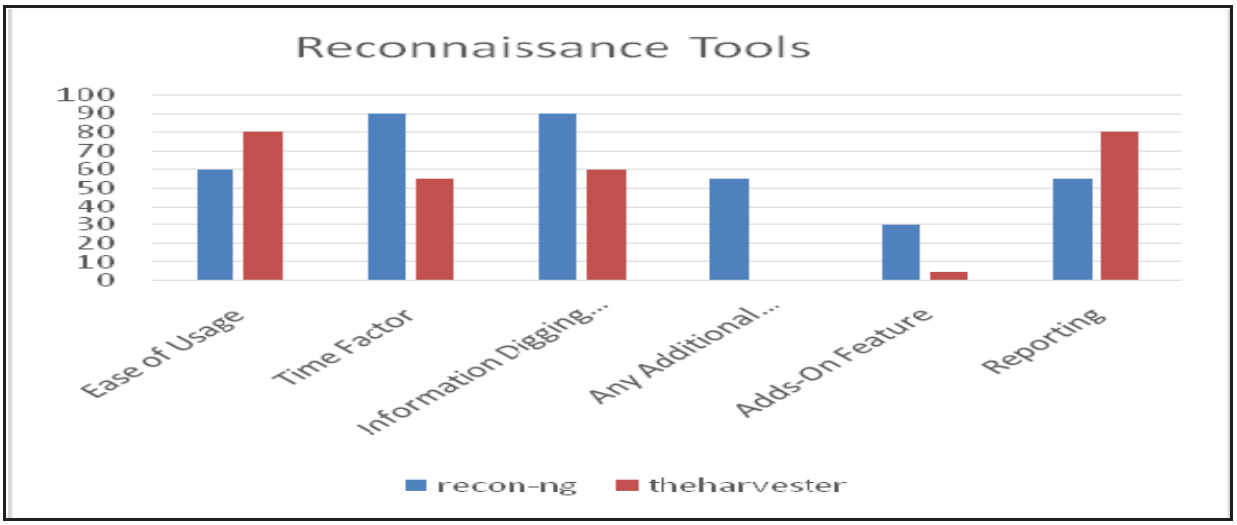
Similarly, the following report comes with the recon-ng.



Based upon the results, a comparative analysis of the information gathering tools are given in the table.

	Ease of Usage	Time Factor	Information Digging Parameters	Any Additional Cost/Efforts	Adds-On Feature	Reporting
recon-ng	60	90	90	55	30	55
theharvester	80	55	60	0	5	80

The graph is generated based upon the values get from the seccessful run of reconnaissance programs.

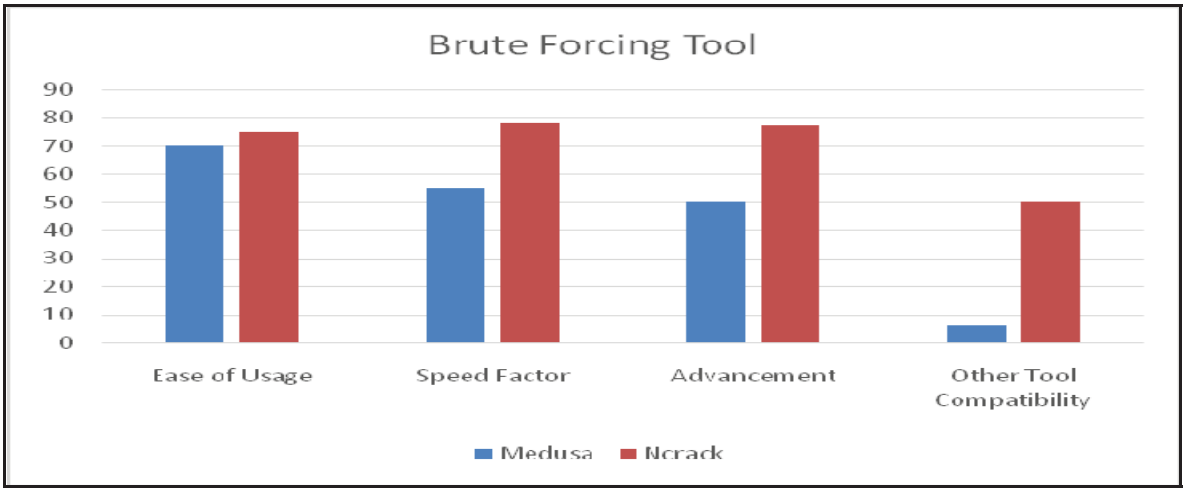


Graph1: Comparison of Reconnaissance programs

For the bruteforcing attack of penetration testing, comparative analysis of the Medusa and Ncrack programs is done based on the following parameters.

	Ease of Usage	Speed Factor	Advancement	Other Tool Compatibility
Medusa	70	55	50	6
Ncrack	75	78	77	50

Graphs is generated from the values as shown below.

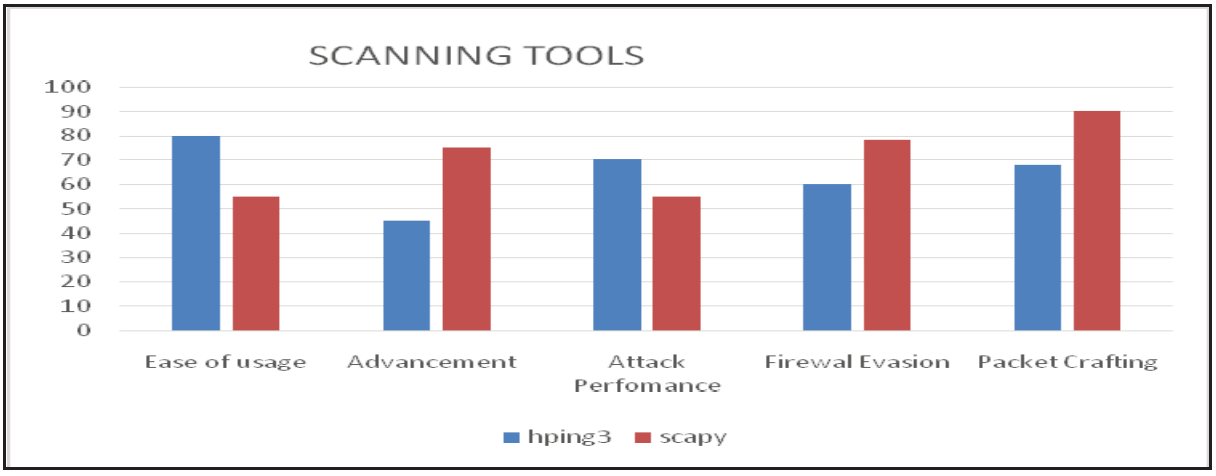


Graph2: Comparison of Brute force programs

Similarily a comparative analysis of following scanning programs are performed based on metrices given in the table.

	Ease of usage	Advancement	Attack Performance	Firewall Evasion	Packet Crafting
hping3	80	45	70	60	68
scapy	55	75	55	78	90

Based upon the values from the table, graph is generated below.



Graph3: Comparison of scanning programs

V. CONCLUSION

Penetration testing is used for checking the security measures that are implemented in the organization. It finds whether the security is penetrable or not by hackers. In this paper, a framework is developed for performing the penetration test. In this framework comparison is performed on the information gathering or reconnaissance programs like theharvester and reconng. The results are compared based upon ease of usage, time factor, information digging and reporting features. In the reporting and ease of usage theharvester has an edge upon the recon-ng. While in other parameters, the recon-ng is the winner. In the brute forcing attack of the penetration testing, ncrack and medusa programs are compared in terms of different parameters. Ncrack is found to be better in terms of speed, ease of usage, advancement and other tools compatibility. In scanning part of penetration testing, in terms of ease of usage and attack performance, hping3 is better while scapy in better in terms of firewall invasion and packet crafting. Denial of service attack is performed by both the tools. The Hping3 provides more elaborate denial of service attack than scapy. Thus it is concluded that in terms of reconnaissance theharvester is better than recon-ng. While in brute force attack ncrack is better than medusa. In terms of scanning part Hping3 is more suitable for performing the penetration testing. Thus the penetration testing can be successfully employed to increase the security of the organizations.

REFERENCES

[1] K. Avinash, "TCP/IP Vulnerabilities: IP Spoofing, SYN Flooding, and the Shrew DoS Attacks" in Lecture Notes on "Computer and Network Security" March 7, 2016.
[2] Deris Stiawan1, Mohd Yazid etc," Penetration Testing and Mitigation of Vulnerabilities Windows Server", International Journal of Network Security, Vol.18, No.3, PP.501-513, 2016.
[3] Munir A. Ghanem,"BackTrack System: Security against Hacking", International Journal of Scientific and Research Publications, ISSN 2250-3153, Volume 5, Issue 2, February 2015.
[4] Suraj S. Mudalik," Penetration testing: An Art of Securing the System (using Kali Linux)", International Journal of advanced research in Computer Science and Software Engineering, ISSN: 2277 128X ,Volume 5, Issue 10, October-2015.
[5] Jai Narayan Goel, BM Mehtre," Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology", 3rd International Conference on Recent Trends in Computing 2015 (Elsevier), Procedia Computer Science 57,pp 710-715, 2015.

[6] B. M. Mehtre, Sugandh Shah,"An overview of vulnerability assessment and penetration testing techniques", Springer Journal of Computer, pp 27-49, 2014.
[7] E. Martins, M.I.P. Salas," Security Testing Methodology for Vulnerabilities Detection of XSS in Web Services and WS-Security", Elsevier, pp.133–154, 2014.
[8] NunoAntunes and Marco Vieira," Penetration Testing for Web Services",IEEE,ISSN: 0018-9162/14, 2014.
[9] Brandon F. Murphy," Network Penetration Testing and Research", NASA. John F. Kennedy Space Center, USRP Summer ,July 30 2013
[10] N. Sklavos, A. Bechtsoudis," Aiming at Higher Network Security through Extensive Penetration Tests", Revista IEEE , Vol. 10, Issue 3, 2012.
[11] Shauvik Roy Choudhary, William G. J. Halfond, etc ," Improving penetration testing through static and dynamic analysis", Wiley Online Library, DOI: 10.1002/stvr.450, 2011.
[12] ElieBursztein, Jason Bau etc," State of the Art: Automated Black-Box Web Application Vulnerability Testing", IEEE Symposium on Security and Privacy (SP), 2010
[13] Lloyd Greenwald and Robert Shanley,"Automated Planning for Remote penetration testing", IEEE,ISSN: 978-1-4244-5239-2, PID: 901436, 2009
[14] Forouzan, B. A, "Data Communications and Networking", New York: Tata McGraw-Hill,2006.
[15] James S. Tiller," The Ethical Hack, A Framework for business value Penetration Testing", Auerbach publications, ISBN: 0-8493-1609-X, 2005.