International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 07, July 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

Analysis of Various tools of Penetration Testing

Harshdeep Singh[1], Jaswinder Singh[2]

[1,2]*Department of Computer Engg.,Punjabi University Patiala, Punjab(India)*

ABSTRACT

Wireless technology has brought many changes in the way of communication in modern days. With the increased worldwide employment of wireless technology, there is raising concern about the security standards of the technology. Many encryptions and decryption techniques have been implemented today to transmit data over the networks. [*1*] *Penetration testing is the one which can be used to identify the unknown traffic in the network. This makes pen test crucial to validate the security mechanisms of the system and outcomes of penetration testing could be used to secure the network. This research will contain an overview of the network penetration testing. It is a technique which is used for keeping the high-security levels in the system by the effective study of loopholes present in the security system. The contents include penetration tests which are used for the purpose of network penetration. The types of penetration testing are further included in this research. The study also includes a detailed information of penetration or pen tests. The research will further discuss the methods of penetration testing and the various phases of the penetration as we proceed in the research. The study will be focused on the effectiveness of the technique that how it can be used in preventing the hacking and providing recommendations to resolve the threats. A framework is created to test the tools and to provide a mechanism to secure the system from being hacked*

Keywords- Network Penetration Testing, Pen Test, Pen Tester, Wireless Networks.

I. INTRODUCTION

Water, Network penetration testing is a technique of finding out vulnerabilities related to security threats for organizations and companies in their network security before any hacker can break into their system [9]. A number of different penetration tests are performed on the security network to ensure the safety of the system to the hacking of any confidential and important data such as funds, consignment details, etc. The aim of network penetration is to simulate the hacking attack or cyber-attack and thus to discover the areas of weakness in the security network system. The results enable the user to work on security problems to set the network security levels which cannot get hacked by understanding and overcome the vulnerabilities to the system. The technique provides the user with the vulnerabilities which can be found by the hacker and helps in counterattacking the chances of being hacked. [14]

Network Penetration

Network Penetration Testing can also be called as Pen Test. Penetration testing provides a way to institutions and businesses to validate the security of the system by checking any potential vulnerabilities in the system. The Pen Test access the computer devices to check for entry flaws. It identifies the security flaws in the system, an infrastructure, web applications, or a network. Security flaws might present in an operating system, mal-configuration, application

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

or endpoints. A system may have various kinds of vulnerabilities related to its security such as access vulnerability, configuration vulnerability, boundary condition vulnerability, exception handling vulnerabilities, authentication vulnerabilities, etc. There may be various other loopholes in the security network. The penetration testing technique provides a window by giving access to exploiting the system with the authority of doing penetration to find out the possible number of exploits present in a security system [2].

Penetration testing

The penetration testing is a next step to the vulnerability assessment process of network penetration under which the vulnerabilities are located and assessed before doing the penetration into the system. The penetration tests are carried out intentionally to have a potential knowledge of the threats in the system composition of security that can be used by a hacker or cyber professional for hacking the system [2]. The aim of authorized exploitation of the system is the safe keeping of the personal information of an organization or company so that it cannot fall into the wrong hands. The penetration testing introduces with the weak links that are present in the programming and designing of the security. It helps in ensuring the strong defense of the system against any kind of flaws related to the security of the system by suggesting measures or solutions to the problems related to the network security. Ettercap, Driftnet, Nmap, Wireshark, Metasploit are certain tools which are used in the process of penetration testing [3]

Pen Tester

A pen-test or penetration test is an attempt to assess the safe keeping of an IT groundwork by safely trying to exploit susceptibilities. The vulnerabilities may exist in the application flaws and services, improper configuration and risky end-user behavior and may be in the operating system. Such type of assessment can help in identifying the possible risks and the effectiveness of the security system in use. [12]

Pen tests are typically achieved using manual or automated skills to methodically compromise endpoints, servers, web applications, network devices, wireless networks, mobile phones and other possible points of the disclosure. Benefits of Pen Testing are that it logically manages weaknesses, it can help in avoiding the charge of system downtime, it helps in meeting regulatory necessities and avoid penalties, it also helps in preserving the corporate image and maintaining the customer loyalty. Pen tests are performed to reduce or stop security breaks and any related disruptions in the routine of working on applications and services that could result in immediate financial losses which can threaten organization's statutes by eroding customer reliabilities and attracting negative media which can generate major penalties and fines. [8]

Methods of Pen Test

Considering needs, there are two types of pen tests.

- **External Penetration Test**:

  This test shows what a hacker would see into the network systems and use the vulnerabilities seen over the net. Here the threat is from the associated external network from the web. This check is performed over the web, overriding them firewall/IDS. [11]

- **Internal Penetration Test:**

  This check shows risks from inside the network. As an example, what threat a disappointed inside worker will cause to the network. This check is performed by connecting to the internal local area network. [15]

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

Types of Penetration testing

The penetration specialists or the security consultants hired by the company follow a well-defined methodology in which they have to find the maximum number of present vulnerabilities and pursue the potential loopholes in the system in the given period of time sometimes with the prior information of system or sometimes without any knowledge of the system. There are basically two types of penetration testing which are used in network penetration:

The announced penetration is a technique of getting access and retrieval of the flag files which are pre-identified and compromising the exploitation of the system with the help of information and cooperation from the information technology staff of a company. Such type of penetration arrangement is used for understanding the individual systems and present security infrastructure with a number of presents and possible vulnerabilities related to its security [9].

The unannounced penetration test is a penetration technique attempt in which the flag files which are a pre-identified and compromising system with the information only related to the upper levels of the management related to the client network. These type of penetration tests are conducted for the understanding of company's security-related infrastructure, the present security procedures which are followed by the company and to see the responsiveness of the staff related to the issues of networks of security system [9].

The penetration tests are further classified into the black box tests and the white box or crystal box tests.

- **Black box:**

In the case of the black box penetration test, the authorized hacker or consultant of security matters has no knowledge of any information related to the system he is hacking which makes it a real time taking and cumbersome job to penetrate into the security system. [2]

- **White Box**:

In crystal box or white box type of penetration, the team of security consultant works with the inside information or the people who have the access and prior knowledge of the privileged information related to the security for example, the information related to the software and hardware in use or the configuration of the network [9].

- **Grey Box/Crystal Box:**

There is also an another type of penetration called Gray penetration in which only the partial information is provided to the security agencies such as company name. The type of the penetration test which is to be used for security network penetration is decided according to the demand and choice of the organization rendering to the utility evaluation of the system. [2]

Process of Penetration testing

The penetration testing involves following steps in its process of improving the security by recognizing the possible number of threats in a network.

Planning and preparation start with defining the objectives and goals of the penetration testing. The client and the tester outline the goals together so that both sides have the same objective and understanding. The common goals of penetration testing are to recognize the susceptibility and improve the safety of the technical systems. [12]

Reconnaissance includes an analysis of the primary information. The tester starts by examining the presented information and, if required, desires for more information such as system descriptions, network plans, etc. related to the system from the client. The only objective is to attain ample and detailed information. [12]

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

Discovery refers to the knowledge and discovery of vulnerabilities by scanning the network for detection of additional servers, systems and other devices, host scanning to locate the open ports on the devices and the service interrogation to discover actual running services.

The analyzing of information includes the fulfillment of goal defined by the test and finding the potential threats to the system. It is a really time-consuming and complex process. [12]

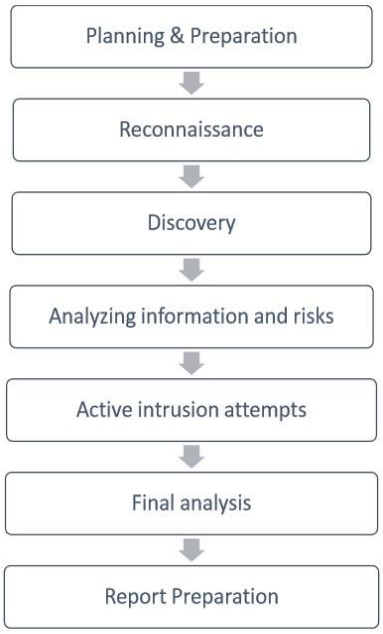

Figure 1: Process of Penetration testing

Active Intrusion Attempts must be performed with due care when an authentication of possible vulnerabilities is needed. This step involves the calculation of degree to which the probable exposures that were identified in the discovery step hold the actual risks.

The final analysis takes into consideration of all the information gathered from above steps and tried to maintain the transparency towards the possible vulnerabilities to the client. And finally, the tester gives his recommendations regarding the removal of expected problems. [12]

The report presentation contains all the necessary details related to the vulnerabilities and threats in the system and the possible countermeasures that can be taken for improving the security. [12]

II. RELATED WORK

Wang, S., Wang, J., Feng, C., & Pan, Z. (2016), analyzed the vulnerabilities and types of attacks on WLAN which is specified as IEEE 802.11 standard. The IEEE 802.11 WAN is a wireless network which uses radio waves to transfer the data. So, it is most susceptible to the security issues like WPE/WPA/WPA2 cracking, Denial of Service (DoS), and rogue access points. By siht, a ylisae rekcatta eht csecse eht srefsnart ,atad evitisnes eht s . sllawerif eht ssapyb dna ,stekcap eht tpecretni ,stekcap suoicilamThe penetrating testing ensures the security of the wireless networks. F ot ,oslA . loot gnitidua eht sa desu si SPDIAW ,skcatta sseleriw eht gnitceted ro ,NALW eht gnitcetorp rof dna sksir eht etagitim the desu si noisurtni sseleriw. WAIDPS is an open-source wireless Swiss-Knife which works on Linux and is written in Python. This tool is designed to audit the networks and

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

detect wireless intrusion. The results of this research indicated that WAIDPS could efficiently detect the attacks in order to protect WLAN. [1]

Goel, J. N., & Mehtre, B. (2015) used Vulnerability Assessment and Penetration Testing (VAPT) for cyber defense. eser siht nlar,hc the nefed rebyc eht rof dezylana si TPAV eht fo ecnamrofrepse ygolonhcet to provide the proactive cyber defense. It helps in founding the vulnerabilities in advance for preventing the attacker from compromising a system. eser sihT ar eht debircsed hcPrevalent Vulnerability assessment techniques and VAPT tools. The VAPT process is step by step process that consists of 9 phases in its life cycle. The results of the research shown that VAPT is a useful technique for Cyber defense technology. The proposed method oslaallows an administrator to save the sensitive information and resources. It also helps in achieving the cybersecurity [2].

B L V Vinay Kumar, K Raja Kumar, & V. Santhi (2016) investigated different Penetration testing tools using Kali Linux. This research helped to understand how to perform the different penetration tests using private networks, virtualized tools, and systems. t lla tceted ot desu saw gnitset noitartenep ehThe skcatta l gniffins ciffart eki . kcatta elddiM-eht-ni- naM dnaF ces dna sisylana krowten retupmoc eht rou dna pacrettE ,gnitidua ytir desu si euqinhcet tentfirD. The implementation also used the Wireshark for traffic sniffing. The results demonstrated that the proposed technique for penetration testing could be used successfully in real time environment. [3]

Fiocca, M. (2009) presented an introduction of Penetration testing to address the vulnerability of computer systems. This paper included a literature survey of Penetration testing which is performed by security experts to find the vulnerabilities of the system. This study mainly presented the two main types of penetration testing. These testing are black box testing and white box testing. The study also analyzed various tools of penetration testing specifically vulnerability scanners that included a more explained review of tools such as Nessus. [4]

Salas, M., & Martins, E. (2014) proposed a technique for security testing which used the two techniques in order to detect the XSS attacks against the web services. The two techniques are Fault Injection and Penetrating Testing. XSS is cross-site scripting attack on Web services which raises new security challenges. This type of testing technique is used to identify the sender by combining the security tokens and WSS (WS- Security). It also ensures the authorized access to SOAP messages communication. Another injection tool that was used is WSInject which introduce the faults or error on Web Services for checking the environment behavior. The results indicated that the WSInject tool is better and improves the detection of vulnerability to compete with XSS attacks than soapUI. [5]

T. Refaat, T. Abdelhamid and A. Mahmoud Mohamed (2016) presented a security solution for WLANs in order to achieve the standard network security requirements having low cost and stability. The proposed security solution works on two levels. These levels are Radio Frequency (RF) and the frame security. This solution is unique from the other as it works in the two WLAN security levels. The proposed solution provides the required frame security by incorporating AES encryption, and conjunction with 802.1x authentication Free RADIUS server for WLANs. This solution achieves the standard security requirements as AES offers the access control, free RADIUS server offers which is required for authentication, non-repudiation, standard confidentiality and integrity[12].

M. Denis, C. Zena and T. Hayajneh (2017) investigated various aspects of the penetrating testing which includes the attack methodologies, tools, and defense strategies. Penetrating testing used to secure the networks and for highlighting the various issues of security. In this research, various penetrating tests are performed with the help of the virtualized systems and tools, private networks and devices. The tools are used within the Kali Linux suit. The

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

attacks which are performed in the research are open ports using the advanced port scanner, hacking remote PC via IP, hacking phones Bluetooth, spying **(**accessing a PC microphone**)**, Man**-**in**-**the**-**Middle attack, hacking WPA**-**Protected Wi**-**Fi, traffic sniffing, smartphone penetration testing [13].

D. Bertoglio and A. Zorzo (2017) demonstrated the overview and open issues on the penetration test. This research also described various methodologies, tools, models, challenges, and application scenarios which are used for the security testing. This research helps in understanding the various aspects and the solutions which are related to the Pentest. In this research, a mapping study was conducted with 1145 papers. Out of which 1090 distinct papers are evaluated. At last, 54 primary studies were selected which were analyzed qualitatively and quantitatively. The author classified the models and tools which were used on Pentest. The results of the research help to define the testing scope and in evaluating the various tools and methodologies which were depending on the context. [14].

K. Skracic, et al. (2014) described the virtual wireless penetration testing with the help of the laboratory model. Penetrating testing is used to ensure the information system security and for avoiding the security incidents like unauthorized access or eavesdropping to the internal systems. A virtual wireless penetrating testing laboratory was designed for the educational purposes which eliminated the problems like the need for the equipment, expert, and presence of students in the lab. The proposed solution helps in eliminating the need for the real hardware by enabling the automatic assessment. The result indicated that the proposed model could be used in order to simulate the wireless network penetration laboratory without the help of the real hardware [15].

S. Shah and B. Mehtre (2014) described the four phases of the vulnerability assessment and penetrating testing. The security professionals across the globe addressed the security risks by the Vulnerability Assessment and Penetrating Testing (VAPT). It helps in defending the cyber assets of an organization. It has the two major parts such as Vulnerability Assessment (VA) and Penetrating Testing (PT). In penetrating testing, This research also demonstrated the various phases and methodologies of VAPT. For VAPT, various commercial and open source tools are available. From which the author selected the Open Source/Free Tools for each of the category of testing in VAPT. This research also presented the comparative analysis of all the methodologies and techniques which are used in VAPT with precautions and standards [16].

I. Mukhopadhyay, S. Goswami and E. Mandal (2014) presented about web penetration testing with the help of Nessus and Metasploit Tool. Web penetration testing is a type of tool which tells about the reaction of the website when a vulnerability attack is made. Today many of the hackers use the web penetration tool in order to determine the vulnerability of the website. In this research, a survey is presented of some of the available web penetrating tools. The author also proposed the architecture for a scan the vulnerabilities of the website with the help of the Metasploit and Nessus tool [17].

D. Rushing, J. Guidry and I. Alkadi (2015) demonstrated the collaboration penetration testing and analysis toolkit. Penetration testing is also known as the pen testing which is very critical in increasing and maintaining the reliability of computer networks while lessening their vulnerability. The value and importance of these networks have been grown from the earlier time. This research also described the software project surrounding network penetration testing from the collaboration standpoint. All the problems and solutions are presented in this which are associated with the team-based efforts that are utilized by the network analysis tools and technologies [18].

Y. Stenfinko, A. Piskozub and R. Banakh (2016) described the automated and the manual penetrating testing which is a methodology for the security of the information. The author also described various benefits and drawbacks of the

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

penetrating testing. In this research, penetrating Testing was used for determining the potential of systems which are subverted by malware and hacking schemes using the same manner as the attacker's employ. Due to many different vulnerabilities in the security sections, manual penetrating tests are more useful and popular. [19].

M. Reddy and P. Yalla (2016) presented a mathematical analysis of penetration testing such as physical penetrating testing, social engineering, and application security and vulnerability countermeasures. Penetration testing is the research for the security of information and measure to protect the web applications from various attackers and hackers. At last, the author also described various strategies for the development of data security and different tools which support penetration testing and the main role of the advanced penetration testing [20]

III. TOOLS & TECHNIQUES USED IN RESEARCH

The We have implemented and used the tools of Kali Linux Operating System in our research. These tools are used for different purposes for testing and checking the system against vulnerabilities. Some of the tools which are used are given below:-

hping3

This tool is used to check the firewall status, port scanning, and path discovery. This tool is used by running certain commands which start from hping3 and use the link as input to determine the details of that link.

We are using this now to check the –port of the following website-:

hping3 -S http//:www.facebook.com -p 80 -c 2)SYN Req, -c =count(

When we enter the above commands, it will result in the following output which is shown in the figure.

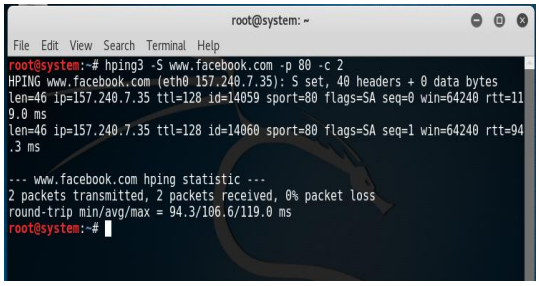

Figure 2 :hping3

sqlmap

This tool is used to get the database details like database names, tables, recognizing passwords, downloading and uploading database files. This tool affects all the private information if the link is not secured.

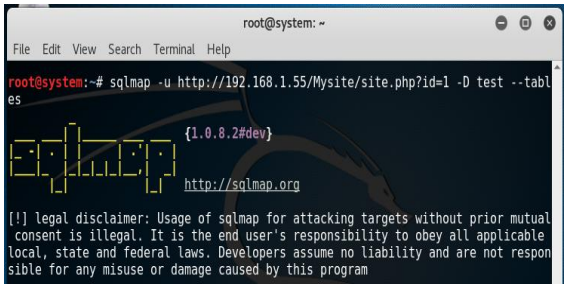

Figure 3:sqlmap1

International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 07, July 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

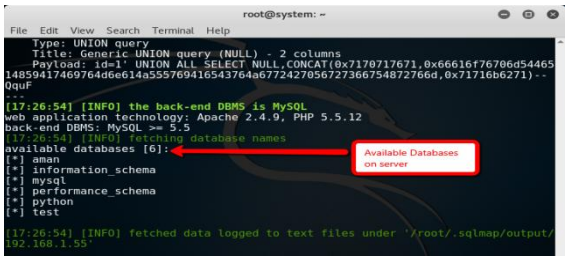

Figure 4:sqlmap2

Nmap

It is a tool used for testing the firewall, routing, mapping network filter, get information on the operating system, software, and services. It also checks all the details of the operating system and details related to network, application, and system.

It is KaliLinux tool which is used for mapping a network filter, firewalls, and routers, etc .

It determines the following:

- Host available on the network.
- Services (Application name and Version).
- The operating system, firewall, etc.

The following command is used to determine the detail of a specific IP:

nmap– v –A –sV 192.168.1.55

Now, this tool will start scanning all the port on IP we used in the commands and start scanning all the details related to IP.

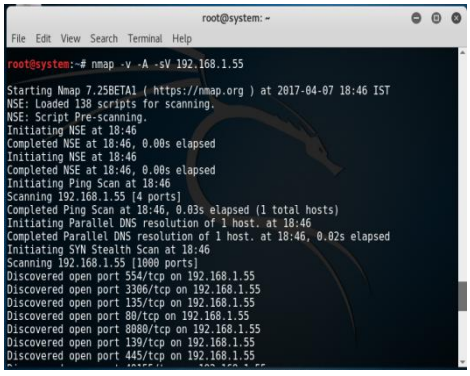

Figure 5:nmap1

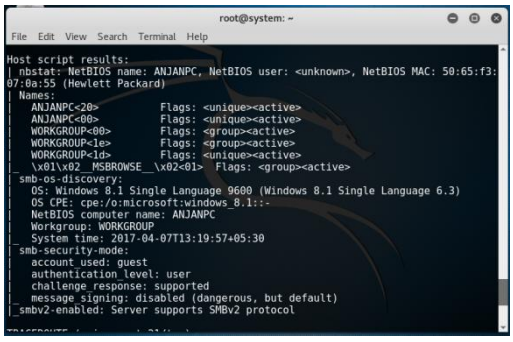

Figure 6:nmap2

International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 07, July 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

The Harvester

It is used for penetrating testing to get the email, subdomains, host, employee name, banner, and ports. It used the domain name as input and a data source to get the information about the domain, and this provides all the discovered information related to a domain. It is used to determine the following:

- Emails
- Subdomains
- Hosts
- Employee name, banner, and ports, etc.

We used the following commands to detect the emails on a particular domain

the harvester- d facebook.com -l 10 -b google

where d → domain name

l → limit

b →data source

By this, we can find out emails and hosts and their port no.

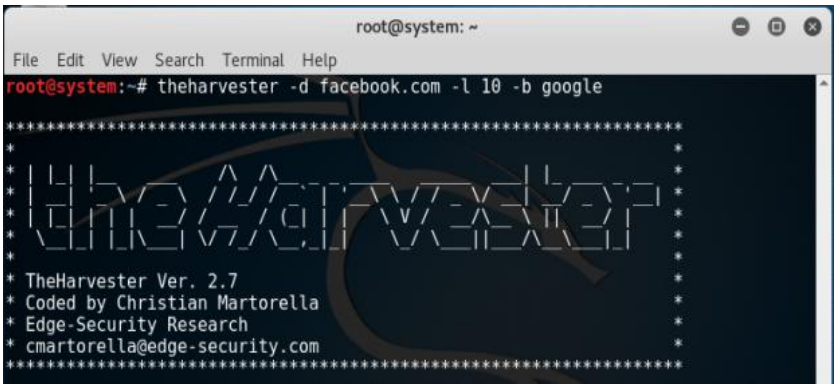

Figure 7:harvester1

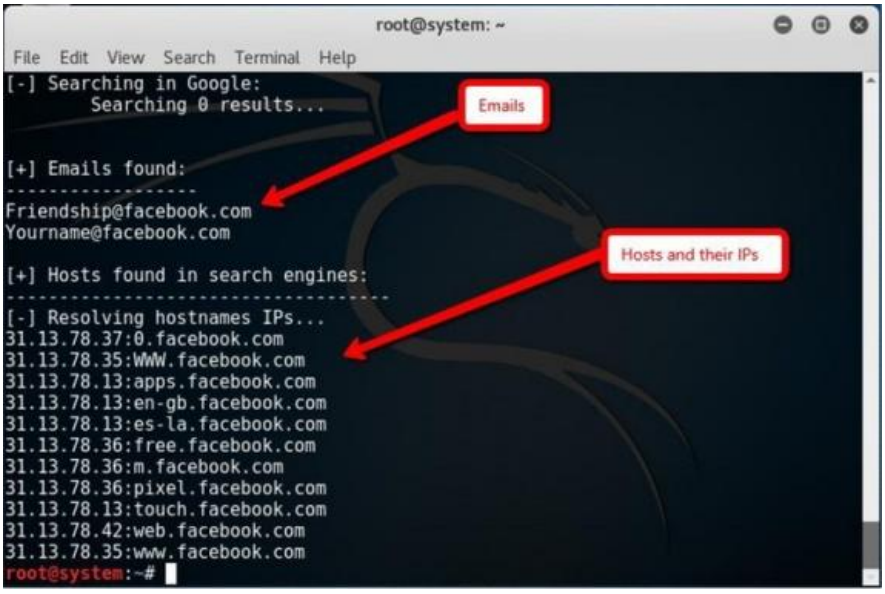

Figure 8:harvester2

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

TABLE1 COMPARISION

Tools	Port and IP	Database	Application and System details	Emails	Sub-domains	Success Rate
hping3	✓					High
sqlmap		✓				Low
Nmap	✓		✓			Medium
theharvester	✓			✓	✓	Medium

IV. CONCLUSION

The study has given the conclusion about the usability of the network penetration techniques that how effectively they can help in identifying the possible number of threats to the security system of the company and the possible ways in which they can be removed or eliminated. It is a significant method that can help in stopping any kind of hacking related to the theft of important data, information of the organization, or any other theft related to funds or money. The possible ways and methods which are used in this technique take out a keen observation on all the aspects of collecting previously recorded data to threat verification and proving the solution to the vulnerabilities and increasing the efficiency of the system. In this research, we used Kali Linux Operating System as it provides many security based tools that can help in performing penetration testing. Also, it provides various other tools that can be used in protecting the system from vulnerabilities. This research used tools from Kali Linus OS and then applied on a created framework to provide a proper technique(s) to protect the systems. The results from the various tools concluded that if the system is insecure, then there is a chance of hacking. The system needs to be secured by using firewall protection, the server should also be secured with encryptions security, and much other security need to be followed for a complete secured system. The individual result of tools helps in determining the things which are required to protect the system from unauthenticated access. The research has also explained the point of time when there is a requirement of the penetration tests to the security system of an organization.

REFERENCES

[1] Wang, S., Wang, J., Feng, C., & Pan, Z. (2016). Wireless Network Penetration Testing and Security Auditing. *ITM Web of Conferences*, *7*, 03001.

[2] Goel, J. N., & Mehtre, B. (2015). Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology. *Procedia Computer Science*, *57*, 710-715.

[3] B L V Vinay Kumar, K Raja Kumar, & V Santhi. (2016). Penetration Testing using Linux Tools: Attacks and Defense Strategies. *International Journal of Engineering Research andTechnology*, *V5*(12), 153-158.

[4] Fiocca, M. (2009). Literature Study ofPenetration Testing. Retrieved from https://www.researchgate.net/publication/254054590_Literature_Study_of_Penetration_Testing

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

[5] Salas, M., & Martins, E. (2014). Security Testing Methodology for Vulnerabilities Detection of XSS in Web Services and WS-Security. *Electronic Notes in Theoretical Computer Science*, *302*, 133-154.

[6] Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & Security*, *56*, 1-27.

[7] Srivastava, A., Morris, T., Ernster, T., Vellaithurai, C., Pan, S., & Adhikari, U. (2013). Modeling Cyber-Physical Vulnerability of the Smart Grid With Incomplete Information.*IEEE Transactions on Smart Grid*, *4*(1), 235-244.

[8] Reaves, B., & Morris, T. (2012). Analysis and mitigation of vulnerabilities in short-range wireless communications for industrial control systems. *International Journal of Critical Infrastructure Protection*, *5*(3-4), 154-174.

[9] He, L., & Bode, N. (n.d.). Network Penetration Testing. *EC2ND 2005*, 3-12.

[10] Friedberg, I., McLaughlin, K., Smith, P., Laverty, D., & Sezer, S. (2016). STPA-SafeSec: Safety and security analysis for cyber-physical systems. *Journal of Information Security and Applications*.

[11] Ten, C., Liu, C., & Manimaran, G. (2008). Vulnerability Assessment of Cybersecurity for SCADA Systems. *IEEE Transactions on Power Systems*, *23*(4), 1836-1846.

[12] T. Refaat, T. Abdelhamid, and A. Mahmoud Mohamed, "Wireless Local Area Network Security Enhancement through Penetration Testing," *International Journal of Computer Networks and Communications Security*, vol. 4, no. 4, pp. 114-129, 2016.

[13] M. Denis, C. Zena and T. Hayajneh, "Penetration Testing: Concepts, Attack Methods, and Defense Strategies," *New York Institute of Technology*, pp. 1-6, 2017.

[14] D. Bertoglio and A. Zorzo, "Overview and open issues on a penetration test," *Dala Lana Bertoglio and Zorzo Journal of the Brazilian Computer*, pp. 1-16, 2017.

[15] K. Skracic, J. Petrovic, P. Pale, and D. Tralic, "Virtual wireless penetration testing laboratory model," *International Symposium ELMAR*, pp. 281-284, 2014.

[16] S. Shah and B. Mehtre, "An overview of vulnerability assessment and penetration testing techniques," *J Comput Virol Hack Tech*, pp. 1-23, 2014.

[17] I. Mukhopadhyay, S. Goswami and E. Mandal, "Web Penetration Testing using Nessus and Metasploit Tool," *IOSR Journal of Computer Engineering (IOSR-JCE)*, vol. 16, no. 3, pp. 12-129, 2014.

[18] D. Rushing, J. Guidry and I. Alkadi, "Collaborative Penetration-testing and Analysis Toolkit," *IEEE*, pp. 1-9, 2015.

[19] Y. Stenfinko, A. Piskozub, and R. Banakh, "Manual and Automated Penetrating Testing. Benefits and Drawbacks. Modern Tendency", *TCSET*, pp. 488-491, 2016.

[20] M. Reddy and P. Yalla, "Mathematical Analysis of Penetration Testing and Vulnerability Countermeasures," *IEEE International Conference on Engineering and Technology (ICETECH)*, pp. 1-5, 2016.

[21] A. Bacudio, X. Yuan, B. Bill Chu and M. Jones, "An Overview of Penetrating Testing," *International Journal of Network Security & Its Applications (IJNSA*, vol. 3, no. 6, pp. 19-38, 2011.

[22] C. Shivayogimath, "An Overview of Network Penetration Testing," *International Journal of Research in Engineering and Technology*, vol. 3, no. 7, pp. 408-413, 2014.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

[23] S. Pavithran and S. Pavithran, "Advanced Attack Against Wireless Networks Wep, Wpa/Wpa2-Personal, And Wpa/Wpa2-Enterprise", *Internation Journal of Scientific & Technology Research*, vol. 4, no. 8, pp. 147-152, 2015.

[24] W. Hasan, S. Chakraborty and S. Reza, "A Comparative Overview of Penetration Testing," *Conference Paper*, pp. 25-28, 2015.

[25] S. Kadam, B. Mahajan, M. Patanwala, P. Sanas and S. Vidyarthi, "Automated Wi-Fi Penetration Testing," *International Conference on Electrical, Electronics, and Optimization Techniques*, pp. 1092-1096, 2016.

[26] R. Rosa, D. Rodríguezy, G. Pívaroz, and J. Sousa, "Analysis of Security and Penetration Tests for Wireless Networks with Backtrack Linux," pp. 1-5, 2017.

[27] Antunes, N., & Vieira, M. Defending against Web ApplicationVulnerabilities. Retrieved 09 Oct 2013, fromhttp://www.infoq.com/articles/defending-againstweb-application vulnerabilities