Volume 5, Issue 10, October-2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Penetration Testing: An Art of Securing the System (Using Kali Linux)

Suraj S. Mundalik
Scholar of Bachelor of Engg., Department of Information Technology,
Pune Institute of Computer Technology, Pune University, Pune, Maharashtra, India

Abstract— In Recent years, many stories come in the rumours about companies being hit by cyber-attacks. The attackers habitually, 'Hackers' try to spoil up the tasks of applications by hacking or attacking on it. They mainly employ SQL Injection while attacking on a web application where web portal mostly goes down due to deficient scripts like login script or database handling scripts. The precaution must be taken for preventing such attacks on system. As consequently, security of web applications is key anxiety. So, prior to actually deploying system, simulate the attacks on the system for testing efficiency of attacks. Here, simulation of "Penetration Testing" comes in to play. The foremost aspire is engineering of web or standalone application flaw-free. The simulation is accomplished using assortment of tools like, tools in Kali Linux (The Harvester, Whois, Webshag, etc.) or tools in Backtrack etc. The tools are open source and are mainly developed on the Linux environment. The crucial point of exertion is uncover vulnerabilities in web applications and investigate diverse stages of penetration testing for simulating attacks which make web application flaw-free. In Presented work, information gathering and attack simulation implementation done particularly with Kali Linux by using various penetration testing tools. Kali Linux makes it easier to simulate the penetration testing on the target with the help of its massive tool set which free of cost and is open source.

Keywords— Penetration Testing, Pen-Test, Kali Linux, BackTrack, The Harvester, Whois, Webshag, SQL Injection, Hackers. Open Source

I. INTRODUCTION

Lots of organizations provide security services around the world. But in most of the case they incorrectly use the terms associated with the security systems. '*Vulnerability Assessment*' is the step by step process of examining the potential risks and issues (backdoors) associated with any system. Whereas, '*Penetration Testing'* is the process of actually performing the potentially harmful attacks on the system that reveals the issues or risk (backdoors) associated with the system. On the whole, this process helps to make a system secure from such kind of attacks by the hackers or any other attackers willing to grant himself/herself an unauthorized access in the system. So now it is clear that Penetration Testing takes over a client's system (authorized) and find the backdoors and gets them fixed to make it more secure.

II. RELATED WORK

Before Kali Linux, Backtrack was the successful Operating System to be used by penetration testing teams. Kali Linux is the successor of Backtrack which was also maintained and copyrighted by Offensive Security Ltd. Backtrack allows to use more than 300+ tools for penetration testing and forensics. Backtrack was used mostly on the virtual environments like VMware and Virtual Boxes. Reference [6] shows penetration testing using Backtrack 4 and covers different penetration testing activities like Target Discovery, DNS information extraction, OS fingerprinting, Vulnerability mapping and many more.

Backtrack was used to provide only some of the tools to simulate the forensics on the target and is now outdated and is no longer supported by the Offensive Security Ltd. Whereas, Kali Linux is now released by Offensive Security with double the tools that were available in Backtrack. Kali Linux is available in different languages. Backtrack faced some wireless card issues that are now fixed in Kali Linux by providing support for wide range of wireless devices.

III. BASIC PENETRATION TESTING TERMINOLOGY

Penetration Testing is the massive field in security systems. It deals with most of common things that usually a developer forgets to cover during the development process. But, by the magic of Penetration Testing it is possible to remove such kind of holes in the application or in any system. This is as crucial as development process since a single hole can spoil the whole system without even knowing that this is actually being happened. So, in this research in order to understand the concept of Penetration Testing some terms related to it must be understood, the terms like:

A. What is Penetration Testing?

Penetration Testing is the process of simulating attacks (on purpose) on the system that needs to be flawed-free (i.e., there should not be any holes) in order to stop a hacker or attacker to follow out an attack along the organization.

The person performing penetration testing also known as Pen-Test, is called as a Penetration Tester or a Pen-Tester. Of course, you are doing this without harming the system or an application. Now, you must be confused between the terms Hacker and Penetration Tester (Pen-Tester)?

So, there is a major difference between a hacker and pen-tester, a hacker implements an attack on a system without having rights to do this that is, in simple words hacker is doing these activities in an unauthorized manner. But, a Pen-Tester is having all the rights to simulate such attacks in order to make the system secure from hackers. A pen-tester may be having a full access or a partial access to the system. Penetration Testing is also known as:

- Pen-Test
- PT
- Ethical Hacking
- White Hat Hacking
- Offensive Security
- Red Teaming [3]

Penetration Testing is basically done to make sure that the attacker(mainly a Hacker) should not enter into the network, system or an application from any other way i.e., without being authorized.

B. How legal is it?

Let's make it pretty clear: Penetration testing requires that you get permissions from the person who owns the system. Otherwise, as mentioned above you are doing the hacking. And you may be charged under the I.T. Act 2000 Section (66) for performing illegal activities or hacking acts.

C. What is Vulnerability?

A vulnerability is a security hole in a Software, Operating System, and Web Application or in any Network that allows an attacker to enter into it without having the permissions of the owner.

D. What is an Exploit?

Ok, now you have vulnerability in the target (system, network, application, etc.). So, to take the advantage of a vulnerability, you often need an Exploit. An exploit is a highly specialized piece of code (program) or software that's intentionally designed solely for the purpose of taking advantage of the vulnerabilities & providing access into the system or network. Exploit often deliver a massive Payload to the target in order to forcefully grant the access permission to the attacker. The Metasploit Project has the world's largest public database of quality-assured exploits.

E. What is a Payload?

A payload is a piece of software that lets you manipulate a system after it's been exploited. Generally, a payload is attached to and delivered with the exploit. Metasploilt's popular and best payload is the Meterpreter, which enables you to do all kind of groovy stuff on the target application or system. Payload is basically written as a script or program that gets executed in background after the exploitation is done on the target [11].

IV. AN INTRODUCTION TO KALI LINUX

Kali Linux is an open source Debian-derived Linux distribution specially designed for digital forensics and penetration testing. Kali Linux is developed and maintained by Offensive Security Ltd. It is available in different architecture: x86, x86-64. It also provides its live cd that allows to use it without actually installing on the system (through thumb drive or a DVD).

Along it provides the virtual images that can be used in virtual environments like VMWare or Virtual Box. Kali Linux gained fame mostly for its huge set of built-in tools for digital forensics and penetration testing. It has almost 600 pre-installed tools. Kali Linux can be downloaded from its official website: http://www.kali.org/downloads

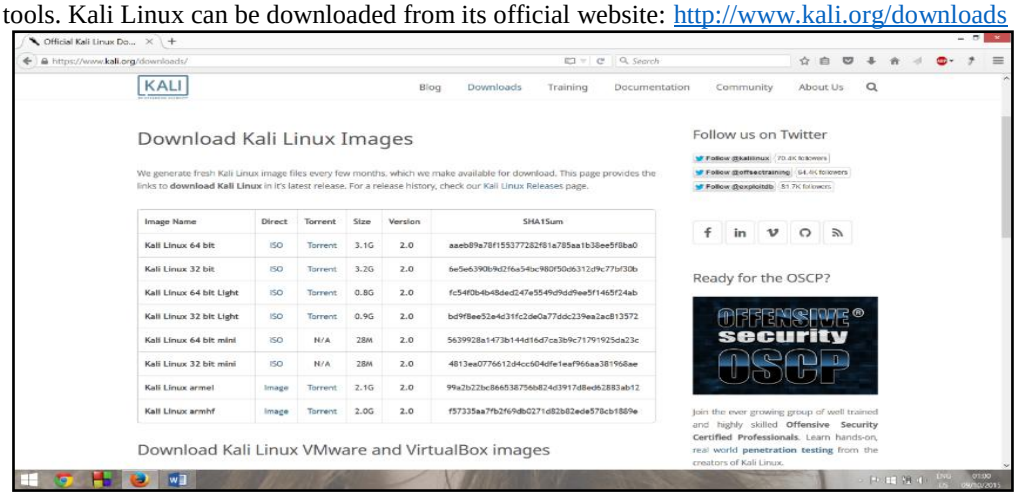

Fig.1 Available Kali Linux Downloads

V. PHASES OF PENETRATION TESTING

Basically, the overall process of penetration testing can be carved up into a no. of steps that make an inclusive methodology of penetration testing. The main purpose behind using methodology is that it allows you to divide a complex process into a series of simple, more manageable tasks or modules. Different methodologies use different names for the steps, although the purpose or tasks are similar. For example, some methodologies use the term "Information Gathering", whereas others use the term "Reconnaissance" or "Recon"[3]. The phases of penetration testing are as follows:

- Information Gathering
- Scanning
- Exploitation
- Post Exploitation & Maintaining Access

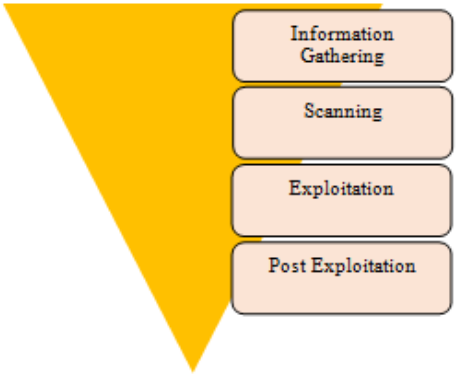

Fig.2 Zero Entry Pen-Testing Methodology [3]

Fig-2 shows the *"Zero Entry Penetration Testing Methodology"*. The purpose of using the inverted triangle is that it allows to describe the steps from broader to more specific manner. For example, the information gathering stage produces a massive information regarding the target, so the triangle shows the broad step, indicating that the data produced by this step or phase is big or large.

The first phase involves gathering or exploring all the necessary details of the target such as the target IP (Internet Protocol) address or in case of physical devices the MAC address is also required. The second phase includes a deep scanning of the target (obviously, not the antivirus scanning). So that the tracks (holes or backdoors) can be found to get the access into the system or application. In simple words, the second phase is about exploring the vulnerabilities in the target using variety of tools. In the third phase we use the results of previous phases (like, target and its vulnerabilities) in order to exploit the system or application. The final phase include maintaining access over the target after the exploitation, which is quite tricky. Oftentimes, the payloads delivered by the exploits give temporary access over the target.

A. Information Gathering (Reconnaissance)

This phase needs patience and lots of time, since this phase generates a massive amount of information about the target. The deeper you go, the more information you explore about the target that helps in the further activities like finding vulnerabilities of the target. In this research Kali Linux tools are being used to simulate the testing on the target. So, Kali Linux provides a variety of tools for gathering information about the target. To be successful at reconnaissance, there must be a proper strategy. The most essential thing is the power of internet. There are two types of reconnaissance:

- **Active Reconnaissance:** Where the pen-tester directly interacts with the target. During this type of process the target may record the pen-testers IP address and other activity log [3].
- **Passive Reconnaissance:** In this type of reconnaissance, the use of enormous amount of information available on the web come into the picture. The benefit is that the target cannot track the pen-tester at all (i.e., pen-tester's IP address or activity logs) [3].

The main motto of Information Gathering is to collect as much information as possible on the target. The information that has been explored in this phase must be centrally organized and that too in electronic format. The reason behind storing the information in electronic format is that it allows easier data processing such as, data editing, sorting, searching and data retrieval later on whenever required.

Most of the times, if you are going for the web application penetration testing then the very first thing required is the website of that web-application. Which is not a harder part of the phase as we can make use of any search engine to locate the website (if the website is optimized well for search engines the website will come on the very first page of the search engine results).

1)HTTrack-Website Copier:

Typically, the pen-testing begins with locating the target's website. But in some case it is good to copy the target website completely i.e., page-by-page. HTTrack is a free utility that allows to copy the whole website data easily. It will allow the pen-tester to have a copy of the target website on the local machine [3]. The utility copies all the pages, links,

pictures and the original code from the target website's server. HTTrack can be downloaded from: http://www.httrack.com/

Before proceeding further, note that cloning (copying the contents) the website is easy to trace by the target and is considered to be as highly offensive activity. So, before going to do the pen-tester needs to have the authorized permissions to do so otherwise he/she may get in trouble.

2)Google Directives-GOOGLE FU:

Another handy tool (without actually going for Kali Linux) is the Google search engine. It allows its users to easily find the information about a website through "directives". These directives are nothing but the keywords associated with every website indexed by the Google Bot. So, by making use Google directives the penetration tester can find more information regarding a single thing. To make proper use of these directives we need the following 3 things:

- The name of the directive you want to use
- A colon
- The term you want to use in the directive[8]

TABLE-IGOOGLE-FU SEARCH OPERATORS/DIRECTIVES [9]

Search Service	**Directive/Search Operator**
Web Search	allinanchor:, allintext:, allintitle:, allinurl:, cache:, define:, filetype:, id:, inanchor:, info:, intext:, intitle:, inurl:, link:, related:, site:
Image Search	allintitle:, allinurl:, filetype:, inurl:, intitle:, site:
Groups	allintext:, allintitle:, author:, group:, insubject:, intext:, intitle:
Directory	allintext:, allintitle:, allinurl:, ext:, filetype:, intext:, intitle:, inurl:
News	allintext:, allintitle:, allinurl:, intext:, intitle:, inurl:, location:, source:
Product Search	allintext:, allintitle:

For example: let's take an example of "site:" directive. To make use of this directive we need to type following in Google search box:

site: domain term(s) search

For example: *site: pict.edu IT* will display following results:

Fig.3 Search results using "site" directive

B. Scanning

This stage is the most important phase where the pen-tester needs to identify the exposures of the target. This can be also referred to as "Vulnerability Assessment".The pen-tester uses different tools and utilities to reveal the holes in the services, ports and applications running on the host. The typical path is to skim for the ports on the web server and find the open port for granting the access into it.Webservers use different TCP ports, and luckily you may encounter any one of them opened. Many protocols on the servers are handled through readable non-encrypted text. Table-II gives a list of common port numbers and their corresponding service.

TABLE-II COMMON PORT NUMBERS AND THEIR SERVICES

Port Number	**Service**
21	FTP Control
22	SSH
25	SMTP (Email)
53	DNS
80	HTTP

So, let's take a look at some of the tools available in Kali Linux for finding the vulnerabilities of the target.

1)Webshag:

Webshag is a multi-threaded multi-platform tool used to audit the web servers. The tool gathers some common functionalities of a web server such as port scanning, URL scanning and file fuzzing (security loophole). It can be used to scan a web server in HTTP or HTTPS, using a proxy or HTTPS authentication. This tool can also perform fingerprinting of the web pages [3]. The below example scans the website: http:// www.itstudentsarena.co.in for open ports and vulnerabilities. As shown in the Fig-4 there are 3 open ports of the target: 443, 80 and 8080 which are of HTTPS, HTTP and Web Proxy respectively. So the pen-tester can easily get into the access to the target through these ports. So, the vulnerability assessment completed successfully.

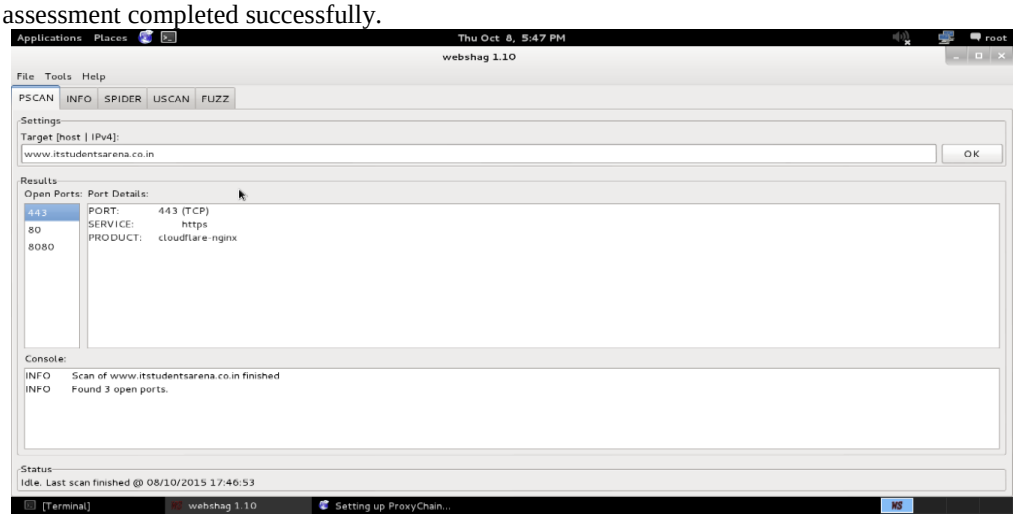

Fig.4 Webshag GUI

2)Vega:

Vega is a security testing tool used to crawl a website and analyse page content to find links as well as form parameters. To launch Vega in Kali Linux, go to **Web Applications > Web Vulnerability Scanners** and select **Vega.** The tool can work as a proxy as well as a scanner so in this research scanner is required to scan the target [3].

For example, in this research the target is www.itstudentsarena.co.in is scanned using Vega. So after completion of the scanning it'll generate an audit of the scan. Fig.5 shows scanning report of the target (www.itstudentsarena.co.in). The report shows the possible vulnerability of Cross-site Scripting and Shell Injection.

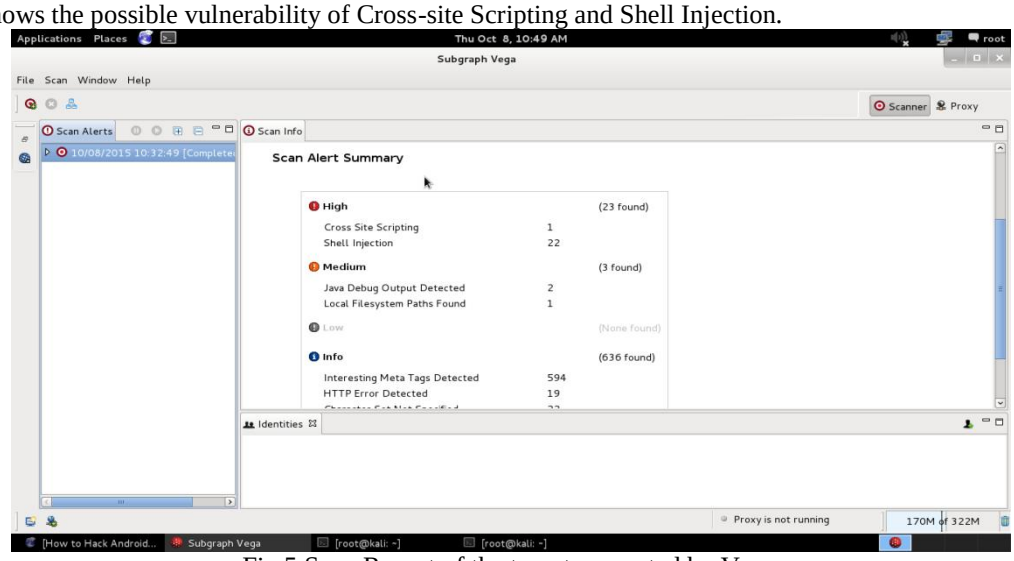

Fig.5 Scan Report of the target generated by Vega

C. Exploitation

Now, the environment is set up and the vulnerabilities of the target are also discovered. Now it's time to take over the target through the holes (vulnerabilities) of the target. This process is nothing but the Exploitation process. In simple words gaining access to the target using its vulnerabilities is known as Exploitation. Exploitation delivers the payloads on the target in order to forcefully grant the access into the target. Some vulnerabilities such as default password are easy to exploit, it hardly feels like exploitation is being done. There are different types of exploits available over the Internet, but the widely used is the "*Metasploit Project"*.

1)Metasploit Project:

The Metasploit is a computer security project that provides information about security vulnerabilities and aids in penetration testing. It's the open source project developed by Rapid7.Metasploit allows the pen-testers to select the target and deliver a variety of payloads. The payloads are compatible and are not knotted to a specific payload. A payload is

nothing but the answer to the question: *"I have access to the target. What to do next?* Metasploit project provide payloads like Creating New Users, Installing Malicious Scripts, Opening Backdoors, etc.

The main difference between a Vulnerability Scanner and a Metasploit is that, a vulnerability scanner scans the target and just verifies whether the target is vulnerable or not. But, in case of a Metasploit actually exploits the target it is scanning& then reports whether it is vulnerable or not. Metasploit can be downloaded from: http://www.metasploit.com

Metasploit is pre-loaded in Kali Linux and can be used in either GUI environment or through the command line interface. In this research, the Metasploit usage is focused on the command line based known as *"msfconsole"*. The *msfconsole* is fast, user friendly and easy to use. To launch msfconsole, open a terminal and execute the following command:

msfconsole

Starting the msfconsole takes between 10-30 seconds (don't worry if the terminal freezes). After that the msfconsole will be in action and will have default shell prompt like: ***msf >***. Fig.6 shows the Metasploit environment in Kali Linux.

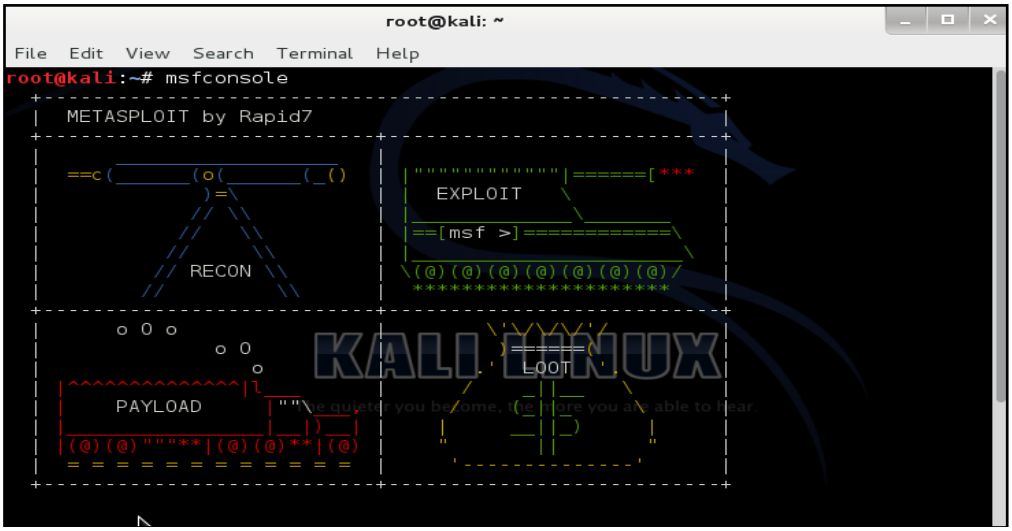

Fig.6 Metasploit Initial Window

As mentioned earlier, an exploit is a pre-packaged code that gets sent to the target. This code causes the target to behave in some atypical way and allowing the pen-tester to execute s payload. Note that, instead of blindly delivering the exploit on the target, try to know the vulnerabilities and then proceed with it. Mainly there are two concepts associated when dealing with delivering the exploits on the target:

- **Bind Payloads:** As shown in Fig.7, in bind payloads the attacker machine is sending exploits as well as connecting to the target. The target machine passively waits for the connection to come in [3].
- **Reverse Payloads:** As shown in Fig.8, in reverse payloads the attacker machine only sends the exploit and forces the target to actively make a connection back to the attacker machine [3].

Basic steps to run the Metasploit against the target are as follow:

- Start Metasploit
- Search which payload to use on the target
- Select the payload
- Set the payload on the target
- Finally, Exploit!

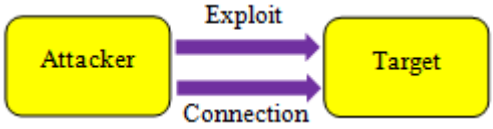

Fig.7 Bind Payload [3]

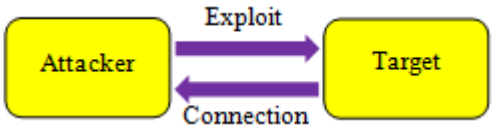

Fig.8 Reverse Payload [3]

D. Post Exploitation and Marinating Access using Backdoors, Rootkits and Meterpreter

This phase plays a crucial role in the penetration testing process. Maintaining access to the target after the exploitation is a very serious activity and needs to done carefully. Several years ago, hackers were used to exploit the target, steal the data or manipulate the data or crash the files and leave. But now a day's many modern attackers (hackers) are interested in long-term or even permanent access to the target.

Thus, in order to achieve this *"backdoors"* are required to be created and needs to be loaded on the target. Backdoors are nothing but a piece of software that allows the unauthorized user to get into the target at any time. Basically, backdoors are the background process that is hidden from the normal user. Some exploits are fleeting (short-lived). In simple words, some exploits allow access as only as the exploited target is running. If the target reboots or the

exploit stops then the connection is lost to the target. There are different backdoor tools in Kali Linux like: *Netcat, Cryptcat, WeBaCoo (Web Backdoor Cookie), etc…*

1)Rootkits:

Rootkits are very simple to install and produce amazing results. Running a rootkit allows the attacker to hide the messy stuff done by him such as manipulation of files, creation of new processes and installation of any new programs on the system. Rootkits can be used to hide the files and processes from the users as well as from the operating system also. Rootkit are very good at hiding the stuff and since they can easily evade most of the antivirus software's and operating system as well [3].

The word rootkit is derived from "root" (having administrative permissions or root privileges) and "kit" (referring to the collection of tools implementing the tool). In Penetration testing make sure you have the rights to implement a rootkit. Otherwise your career will come to an end even if you are authorized for the penetration testing.

Rootkits are extremely stealthy (cautious), they can be utilized for a mixture of purposes, including escalating privileges, recording key strokes (just like a key-logger), installing backdoors and other evil tasks. Many rootkits are able to avoid detection because they work at very low level of the operating system itself, inside the kernel. It is important to note that a rootkit is not an exploit [3].

2)The Meterpreter:

The Metasploit Project provides its own tool for post-exploitation or to maintain a proper access after the exploitation, known as the Meterpreter. Meterpreter can be used to make the target compromise against the exploit allowing the attacker to gain access over the target. The payloads are basically used to achieve specific tasks on the target (like create new user, install a script, etc.) but they have a major disadvantage. Payloads work by creating new processes on the compromised target. This can trigger alarms of the antivirus software and can be caught easily. Also, a payload can perform specific operations that the command set of the console support. To overcome these difficulties Meterpreter came into the picture [3].

Meterpreter is simply a command interpreter like any other command interpreter such as BASH in Linux or CMD in Windows, but for Metasploit that works as payload. It works in context with the exploited process, so it does not creates a new process. This makes it more stealthy and powerful.

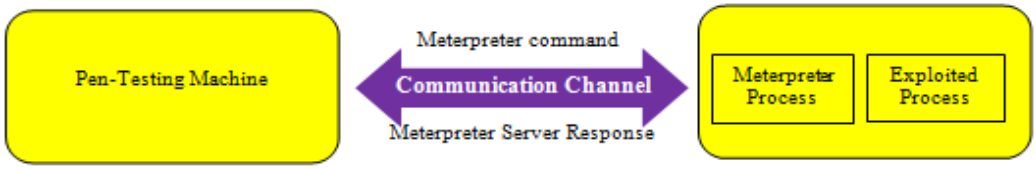

Fig.9 Meterpreter Working [3]

Fig.9 shows the working of the Meterpreter. There exists a two way communication between the pen-testers machine and the target. The commands entered by the pen-tester are interpreted and executed on the target by the Meterpreter through the Communication Channel. On the other hand, if everything goes well the response from the target is sent back to the pen-testers machine via the same communication channel.

VI. CONCLUSION

Penetration Testing or Pen-Testing is the most essential focus of any system, it may be a web application or a standalone machine. Penetration testing allows the developer to ascertain and define the security issues associated with the system that he/she has acquired.As determined in the research, minor things like open ports can cause you a massive loss in terms of data, or may be confidential files and text files. The attacker can totally control the system while you are doing the work as well the attacker can even spy on you using the exploits. As mentioned earlier in the presented work, the rootkits can make the ways to enter into the target again and whenever the attacker wishes to. The penetration testing methodology seen in this research i.e., "Zero Entry Pen-Testing Methodology" helps the pen-tester to take effective steps against a system or an application to uncover and prevent any flaws of the target system or application.

Different phases use different tools in order to explore massive amount of information that helps the pen-tester to make the target flaw-free. One of the most important thing to be noted is that the pen-tester when implementing the pen-testing on a target he/she needs to think almost like a hacker does. But, there exists a major difference between a penetration tester and a hacker that is, a hacker is applying his whole focus in order to break into the target without having prior authorities or rights to do that. As in case of a pen-tester, he/she is having the prior permissions and authorities to simulate such deadly attacks on the target to find its security issues and get them fixed. Prevention needs to be taken by the developer while developing the application or any system so that the attacker, mainly a hacker cannot find a single entry into the developed system.

Hence, it is very much important to perform penetration testing on the system you are going to be used. There are many professional companies that offer the best security services. If don't want to spend the bucks on the organizations, Kali Linux is proved to be very useful and completely free Operating System that can be used for the penetration testing. Penetration testing requires lots of time and patience to get the results and to get them repaired.

Penetration Testing can be implemented using Kali Linux for future security regarding the applications that require high level of security. Security for such applications or systems can be tested for any risks that may or may not be associated with it with the help of Zero Entry Methodology of penetration testing. This will lead to cover all the vulnerabilities (if any) of the developed system or an application.

ACKNOWLEDGEMENT

First Of all I am grateful to my motherSmt.Vaishali S. Mundalik and my sister Ms.Deepali S. Mundalik for theirblessingthroughout the journey. I am tremendously grateful to Prof.RohitKautkar, for their continuous support and motivation for me during the research and the proper guidance towards the present work.I am sincerely thankful to Dr. Vilas Bhadane for his blessings and support to me. I would also like to thank my fellow friends for cheering and helping during the preparation of the presented work.

REFERENCES

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

[2] Weidman, G. &Eeckhoutte, P. (2014). Penetration testing: a hands-on introduction to hacking. San Francisco, California: No Starch Press.

[3] Engebretson, P. (2013). The basics of hacking and penetration testing ethical hacking and penetration testing made easy. Amsterdam: Syngress, an imprint of Elsevier.

[4] Broad, J. &Bindner, A. (2014). Hacking with Kali practical penetration testing techniques. Amsterdam Boston: Syngress.

[5] Wilhelm, T. (2013). Professional penetration testing: Creating and learning in a hacking lab (Vol. 1). Newnes.

[6] Ali, S., &Heriyanto, T. (2011). BackTrack 4: Assuring Security by Penetration Testing: Master the Art of Penetration Testing with BackTrack. Packt Publishing Ltd.

[7] 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.

[8] http://grayhathacking.blogspot.in/2012/10/google-fu-using-directives.html

[9] http://www.googleguide.com/advanced_operators_reference.html

[10] https://www.kali.org/

[11] http://www.kalitutorials.net/

