Modern Day Penetration Testing Distribution Open Source Platform - Kali Linux - Study Paper

Devanshu Bhatt

Abstract: Penetration testing is extremely crucial method to discover weaknesses in systems and networks. There are numerous methods available for ethical hacking via penetration testing. This paper describes a white hat hacker techniques of penetration testing. I have conducted this test on personal system where five operating systems are configured and connected through Oracle Virtual-Box technologies. These systems were connected through NAT Network protocol, which was not connected to real internet . One virtual machine was configured with Debian Linux and two target virtual machines were configured with Windows 7 and 10 respectively, as well one target was configured with the Metasploitable Linux distribution, this distribution is intentionally insecure and developed to be used for security testing, Another virtual machine was configured with Kali Linux, which is specially modern day open source platform to help Penetration testing used by security professionals to make system and network safe while identifying vulnerabilities in number of ways, specializations, including penetration testing, forensics, reverse engineering and vulnerability assessment.

Index Terms: Cyber Security, Dmitry, Ethical Hacking , Exploits, Kali Linux, Metasploit, Penetration Testing

1 INTRODUCTION

The penetration tests are procedures of attempt to examining your data security methods. There are actually plethora of possibilities these could be performed, but the most typical method could be that the security measures are actively examines for pattern flaws, technical defects and vulnerabilities; Penetration tests are a manipulated attack simulation that assists determine vulnerability to software, system, and operating-system breaches. Penetration testing enables you to actively determine vulnerabilities, verify present controls and develop recommendations for removal the outcomes will be presented thoroughly in the document, to organization's chief managements, Administrations and Specialized members. There are number of tools and techniques available to perform the penetration tests; This report will explain few of the capabilities of Kali Linux - which is open source distributed modern day platform to perform penetration testing with already defined applications and frameworks within it. This paper describes a white hat hacker techniques of penetration testing. I have conducted this test on personal system where four operating systems are loaded and connected through Oracle VMware virtual machines. These systems were connected through NAT Network protocol, which was not connected to real internet. One virtual machine was configured with Debian Linux and two other virtual machines were configured with Windows 7 and 10 respectively. Another virtual machine was configured with Kali Linux, which is specially modern day open source platform to help Penetration testing used by security professionals to make system and network safe while identifying vulnerabilities in number of ways, specializations, including penetration testing, forensics, reverse engineering and vulnerability assessment.

- *Devanshu Bhatt is currently working as Consultant, IT App Development at Nationwide General Insurance, Columbus, OH, U.S.A. PH-6784683152.*
EMAIL - devanshu20@gmail.com

2 OVERVIEW OF VIRTUAL LAB

2.1 Concepts of Virtualization

In this section, I will focus on how to established up and do security assessment in a virtual lab. To build the lab, we will use a virtualization technique, known as Virtual-Box, which operates on a Windows host computer system. To do the assessment, we will use a Linux system distribution, which is intended particularly for security function, referred to as Kali Linux system. We will also have in the virtual lab, a variety of targeted systems that we can analyze. There are a variety of benefits of utilizing a virtual test lab.

2.2 Benefits of Virtualization

Virtualization is a incredibly simple way of establishing up a assessment environment, and eliminates the need to have to acquire shelves of computer systems and networking devices. I am utilizing my ProBook 4540s with i5 to manage a virtual test lab, but with the performance of modern-day virtual environments, nearly any computer system is effective enough to do this. Utilizing a virtual lab for testing guarantees that all assessment is included inside of a recommended environment, and test scans and probes do not outflow out upon the internet. This is an crucial thing to consider in ethical penetration testing. And it is also advisable to make certain that testing actions do not unintentionally turn out to be unlawful actions. Virtualization is not only a easy way to develop a lab, but also provides additional benefits when interacting with possibly risky tools. Utilizing a virtual environment, a specialist can acquire a replicate of a known good condition and conserve it as a snapshot. Following operating a assessment session, the snapshot can be utilized to recover the lab and eliminate any footprints of malicious activity. Two well-known software-assisted virtualization programs for Windows are VMware, and Oracle's Virtual-Box.Virtual-Box is cost-free to use, it is readily available for the x86 kind of operations, and operates on a variety of operating systems, such as Windows, Linux system, Macintosh, and Solaris. Virtual-Box is parallel licensed, the starting bundle comes as a cost-free download, and includes almost everything necessary to manage a virtual environment. An expansion package is also obtainable, which consists of additional capabilities, and this is totally free of cost for individual use. Business clients are motivated to acquire a professional license in order to obtain extra capabilities and

help for mission-critical use.

Fig. 1. *Penetration Testing Virtual Lab environment setup*

3 Steps To Install & Configure Virtual Machines And Kali Linux

In general penetration below steps can be performed to install and configure Virtual Machines and Kali Linux

3.1 Virtual Box

Download virtual box from virtualbox.org and install with most of default setup, update network settings with the NAT Network and make sure to provide all settings as mentioned in Fig. 2

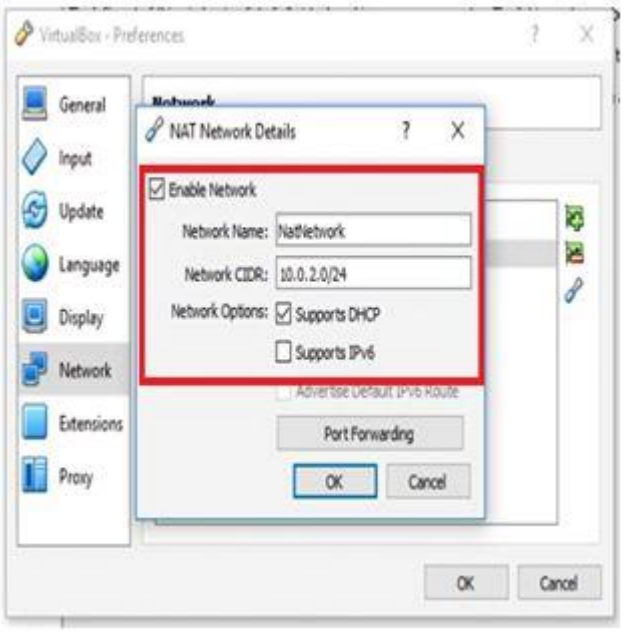

Fig. 2. *Virtual Box Network Settings*

3.2 Debian Linux

Now install and configure Debian Linux Virtual machine by downloading it form Debian Linux site and download first of the i386 ISO CDs. and install it with default settings, change domain name as local.net and create password for root user.

3.3 Kali Linux - Install and Update

Kali Linux system is a distinctive make of the Debian operating system, which is pre-configured with a substantial variety of assessment tools, addressing internet, infrastructure, and wireless assessment specifications. It truly is the platform of preference for numerous penetration testers. Kali can be mounted as the only system on a hardware platform, and this is acknowledged as a bare metal installation. It can be loaded as a 2nd bootable image on a system with an pre-existing operating system, acknowledged as a dual boot set up. It can also be operate as a virtual machine, as explained in paper previously. There is already pre-packaged 64 bit version of three gigabyte 7Z compressed file image available which uncompressed image named as kali-linux-2018.1-vbox-amd64.ova identified as Kali rolling releases. The easiest way is to import .ova image into virtual box as import appliance. Once it is configured then update it while giving below shell commands - **apt update** followed by either **apt upgrade, apt-get upgrade, or aptitude safe-upgrade**

Fig. 3*. Kali rolling Linux update and upgrade*

3.4 Metasploit - exploit development framework

Metasploit, was developed by H.D. Moore in 2003 utilizing Perl. And in 2007, was entirely re-written in Ruby. It was acquired in 2009 by Rapid7 and it is been improved with Express and Pro editions. It is now develop into the standard exploit development framework and, with its addition as part of Kali Linux system, is the most well-known pen assessment tool. The Metasploit programmers have also introduced an deliberately vulnerable setup of the Ubuntu Linux system technique known as Metasploitable 2, which is developed to be a risk-free target for educating and studying pen testing utilizing Metasploit. This can be download from internet as an archive that contains it in virtual disk form, even though it is not

offered as an OVA. Metasploit can be configured as a Virtual machine as OS Linux system and Ubuntu 32 bit type. After installing Metasploit successfully, change the networking protocol to NAT network, like other Virtual Machines.

3.5 Virtual Machines with Window7 and Windows 10

Download Windows 7 and Windows 10 OVA files from official Microsoft developer portal, those are available for free to use for limited period of time to use as a individual purposes, create Windows 7 and Windows 10 virtual machines respectively with help of OVA images. and set networking protocol to NAT network. Make sure to disable automatic updates for both Windows 7 and Windows 10 ; these two targeted systems are indented to use for penetration testing with Kali Linux distribution platform.

4 OVERVIEW - KALI LINUX OPEN SOURCE DISTRIBUTION PLATFORM

Kali Linux is the outcome of several years of improvement and the outcome of a constant progression of the platform, from WHoppiX to WHAX, to BackTrack, and now to a comprehensive penetration testing framework utilizing numerous capabilities of Debian GNU/Linux and the energetic open source community world-wide. Kali Linux has not been developed to be a easy range of tools, but instead a adaptable framework that specialized penetration testers, security enthusiasts, students, and newbie can personalize to match their particular needs. Although Kali's emphasis can be easily described as "penetration testing and security auditing", there are numerous various responsibilities included guiding these actions. Kali Linux is developed as a framework, due to the fact it consists of several applications addressing extremely distinct use cases. For instance, Kali Linux can be utilized on a variety of kinds of computer systems: certainly on the systems of penetration testers, but also on servers of system administrators wanting to keep an eye on their network, on the work stations of forensic experts, and much more unexpectedly, on stealthy embedded devices, usually with ARM CPUs, that can be slipped in the selection of a wireless network or connected in the computer of targeted users. Several ARM systems are also ideal attack devices because of to their tiny form components and very low energy needs. Kali Linux can also be implemented in the cloud to rapidly develop a farm of password-cracking devices and on cell phones and tablets to enable for genuinely portable penetration testing. Kali Linux distribution has over six hundred security testing tools and graphical interfaces to make those tools to use very easy for newbie as well. As per below Fig. 4. it has tools ranging from Information Gathering category up to System Services.

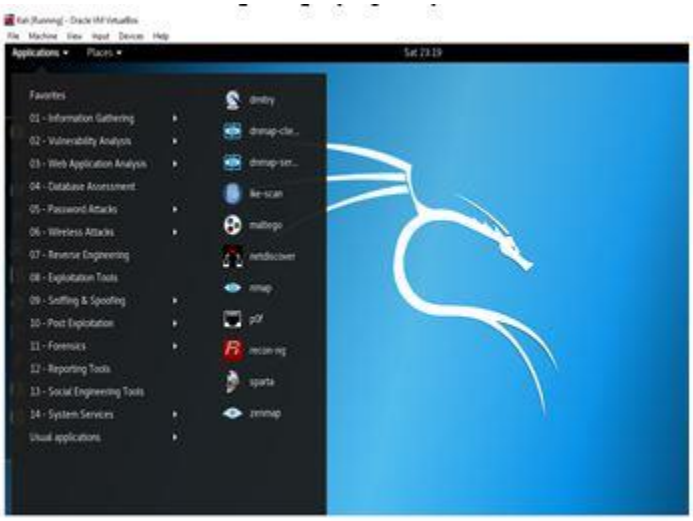

Fig. 4. *Kali rolling Linux Application tools Menu*

4.1 Kali Linux Applications Menu - Overview

- **Information Gathering**: Accumulating information about the targeted system and its framework, determining computer systems, their operating systems, and the services that they operate. Determining possibly vulnerable components of the information program. Removing all varieties of entries from operating index services.
- **Vulnerability Analysis:** Rapidly assessment whether or not a local or remote system is impacted by a range of identified vulnerabilities or unconfident configurations. Vulnerability scanners use databases that contain 1000's of signatures to recognize possible vulnerabilities.
- **Web Application Analysis:** Determining mis-configurations and protection flaws in web applications. It is critical to determine and reduce these problems provided that the general public accessibility of these programs tends to make them perfect targets for attackers.
- **Database Assessment:** From SQL injection to targeting credentials, databases attacks are a extremely frequent vector for attackers. Methods that examination for attack vectors varying from SQL injection to information extraction and evaluation can be discovered.
- **Password Attacks:** Authentication programs are constantly a go-to attack vector. Numerous helpful resources can be identified here, from online password attack resources to offline attacks towards the encryption or hashing programs.
- **Wireless Attacks:** The persistent characteristics of wireless networks indicates that they will constantly be a frequently attacked vector. With its extensive variety of assistance for numerous wireless cards, Kali is an apparent option for attacks towards numerous varieties of wireless networks.
- **Reverse Engineering:** Reverse engineering is an exercise with numerous reasons. In assistance of attacking actions, it is one of the major techniques for vulnerability identification and exploit advancement. On the preventive aspect, it is utilized to evaluate malware utilized in focused attacks. In this capability, the objective is to determine the abilities of a provided portion of

actions.

- **Exploitation Tools:** Exploiting, or consuming benefit of a vulnerability, enables you to acquire control of a remote machine. This accessibility can then be utilized for additional opportunity escalation attacks, possibly locally on the jeopardized machine, or on other machines obtainable on its local network. This category includes a variety of tools and resources that streamline the procedure of composing personal exploits. As well there are number of other applications and tools available in Kali Linux like Post Exploitation, Sniffing and Spoofing, Forensics, Reporting Tools, Social Engineering Tools and System Services.

5 Penetration Testing Techniques With Kali Linux Tools

5.1 Understanding The Target - Info Gathering

The very first activity for performing this task is to profile target, so it can be exploited in sequence fashioned which designed by attacker. Gathering Information can possible with number of ways, with help of these tools it is possible to get DNS information as well to identify IDS which is utilized to filter traffic. There is possibility to get data from SMTP, SNMP and SSL services which might be not secure and open. **Dmitry** is a deep magic information gathering tool, which used to identify hosts, domains, and sub domains, and looks for open ports by performing scans on targets.

Fig. 5. *Port Scanning with Dmitry*

Dmitry will check the ports on one of the machines in the testing system lab by utilizing the -p switch. I'll also use the b switch to get the banner from the ports so that I can see the version of software providing the port service. by executing below command

5.2 Debian Linux System Exploitation with Metasploit

Let us take a rapid glimpse at Metasploit. After I start out the application, Below dark screen window begins. The very first time on kicking off it develops database, Or else, it'll by pass this set up phase. Once it is started, the msf prompt shows up. Metasploit has become completely ready to be used. Metasploit contains a repository of testing modules, assembly, and encoding functionality to control manipulate and payload code, as well as an interpreter, a payload which supplies a strong remote shell.

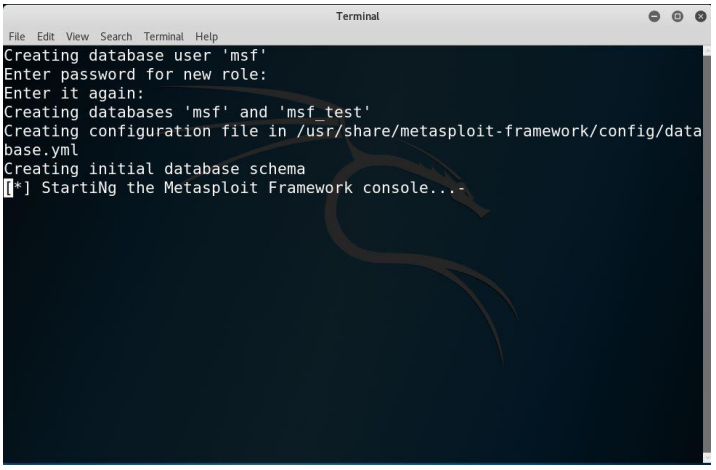

Fig. 6. *Metasploit Framework startup screen*

Once it is loaded properly there are 1,722 exploits and 507 payloads in its databases, as well as a variety of other segments. Exploit segments are operate towards the target system to verify whether or not it is insecure. Payloads are routed into a target system to illustrate that the exploit was effective by carrying out on the target.

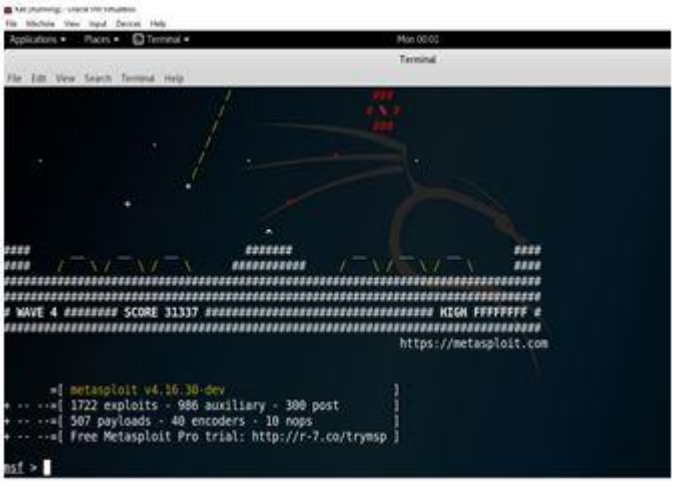

Fig. 7. *Total Exploits and payload details*

The very first Metasploit command I will key in is help. This displays all the commands that we can provide in Kali. Metasploit help command will demonstrate complete collection of various commands, which may be employed on target systems.

1. Core Commands, **2**. Module Commands. **3**. Job Commands. **4**. Resource Scripts command 5. Database Backend Commands, and **6**. Credentials Backend

Commands. And below command will show all the exploits which are available in Metasploit repository database. Left side it will show exploit name and right side it shows disclosure dates, the impact of exploit and the description of about it.

msf > show exploits

Now command Metasploit to examine if system is vulnerable, to the system defined for exploitation in Virtual Test Netowork, this can be executed by command **msf > search irc.** Now to use Unix exploit, command **msf > use unix/irc/unreal_ircd_3281_backdoor** Once it is successful, now it is ready to use for target. command **msf > show targets** displays available targets which can be possible to exploit. command **msf > set target 0** will set the exploit on target for payloads.

Fig. 8. *Set Target for exploit command*

Once target is set, find payload while performing command **msf > info cmd/unix/reverse** to get information about reverse shell, which will shows the port numbers on shell created.

Now command **msf > set payload cmd/unix/reverse** after type command **msf > show options** to get options.

Aftre set remote host address by command **msf > set rhost 10.0.2.13** and local host address by command **msf > set lhost 10.0.2.10** and now pass **msf > exploit**

Fig. 9. *Remote system is acquired*

Above Fig. 9 shows that remote system is acquired now and shell command is established successfully with admin user "root" as well we can review and configured all processes on remote system as well. Likewise there can be other payloads also can perform now on vulnarable system using above same techniques.

6 CONCLUSION

By utilizing Kali Linux - Open source Distribution Framework and number of applications it supports like Dmitry and Metasploit, I been able to get access on the target Debian Linux machine. Kali Linux's Dmitry and Metasploit Framework offers significant variety of exploits with the collection of all operating system with available versions and service packs. Specifically in actual world situation; it is essential to include complete variety of threats and available most critical categories applications from Kali Linux. The assessment need to be carried out on systems with anti-virus and firewalls to get the precise final result. And all those resources need to be utilized which have most recent vulnerability exploits.

REFERENCES

[1] https://www.kali.org/releases/kali-linux-2017-3-release/ https://docs.kali.org/category/installation

[2] http://forums.kali.org/

[3] http://www.metasploit.com/projects/Framework/

[4] https://www.virtualbox.org/

[5] http://git.kali.org/gitweb/

[6] https://en.wikipedia.org/wiki/Kali_Linux

[7] https://en.wikipedia.org/wiki/Debian

[8] https://en.wikipedia.org/wiki/Metasploit_Project