REVIEW

|  |  |
| --- | --- |
| Title | Modern Day Penetration Testing Distribution Open Source Platform – Kali Linux – Study Paper |
| Type | Int. Journal of Scientific & Technology Research |
| Volume & Page | Vol 07, No 04 |
| Year | 2018 |
| Author | Devanshu Bhatt |
| Reviewer | Diba Madya Margerefti, Rahmaulia, Rosita, Seli Puri Andani |
| Date | 07 Desember 2019 |
| Objective(s) | This research describes a white hat hacker techniques of penetration testing with Kali Linux |
| Subject | 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 |

In this research show the 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. 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. this distribution is intentionally insecure and developed to be used for security testing.

The author focus on how to established up and do security assessment in a virtual lab. To build the lab, the author 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.

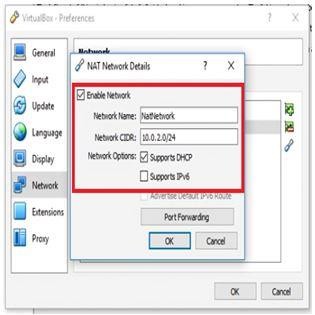
The benefits of virtualization is a incredibly simple way of establishing up a assessment environment, and eliminates the need to have to acquire shelves of computer systems and networking devices. The author utilizing my ProBook 4540s with i5 to manage a virtual test lab, but with the performance of 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. 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.

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.

Steps to Install & Configure Virtual Machines and Kali Linux :

1. 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 below.



# Next step are 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.

# Kali linux install 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.

# Metasploit – exploit development framework 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.

# 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.

Author tells about 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.

Kali Linux Applications Menu – Overview :

* Information Gathering
* Vulnerability Analysis
* Web Application Analysis
* Database Assessment
* Password Attacks
* Wireless Attacks
* Reverse Engineering
* Exploitation Tools

PENETRATION TESTING TECHNIQUES WITH KALI LINUX TOOLS :

## Understanding The Target - Info Gathering

## Debian Linux System Exploitation with Metasploit

So the conclusion of this research are by utilizing Kali Linux - Open source Distribution Framework and number of applications it supports like Dmitry and Metasploit, author 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