**REVIEW**

|  |  |
| --- | --- |
| **Title** | Basics of Ethical Hacking |
| **Type** | International Journal of Engineering Science & Emerrging Technologies |
| **Volume & Page** | Volume 7 Issue 4 pp: 715-720 |
| **Year** | 2015 |
| **Author** | Chenchu Laksmi S, P I Basarkod |
| **Reviewer** | Rosita |
| **Date** | 05 Desember 2019 |
| **Introduction** | The vast growth of Internet has brought many good things like electronic commerce, email, easy access to vast stores of reference material etc. The more developing an internet technology the more people who are not responsible for hacking the system. Therefore One of the more effective ways of testing network security is penetration testing or ethical hacking. ethical hacking is hacking to find weaknesses in a computer or network system for security testing. Ethical hacking can be categorized as a security assessment, a kind of training, a test for the security of an information technology environment. |
| **Difference between Hacking and Ethical Hacking** | Hacking is the act of finding an entry point that might exist in a computer or network system until it is successfully taken over, while Ethical Hacking is hacking to find weaknesses in a computer or network system for security testing |
| **Categories of Hackers** | * White Hats : They use Skills to determine the vulnerabilities in computer systems * Black Hats : They use Skills to vulnerabilities for mischief, personal gain or other purposes * Grey Hats : can become White Hats and Black Hats |
| **Penetration Testing** | is the method of examining the weakness and vulnerabilities of Computer and network security. Why need of **Penetration Testing ? because to eliminate the weaknesses and vulnerabilities of the system security before being hacked. Types of penetration Testing :**   * Black Box Test : testing is closely stimulated to that of an external attacker * White Box Test : testing the tester generally provided with detailed information about the network to be tested include the IP address. |
| **Working Of an Ethical Hacker** | Working with attention principles of Ethical Hacker, high professional, Respecting Privacy and Not crashing your systems |
| **Ethical Hacking Methodology** | An **ethical hacker** doesn’t need to take that much care in hiding his traces and tracks. |
| **Ethical Hacking Process** | Ethical Hacking Process consists of several processes including starting from Specific systems to be tested, risk, schedule test, knowledge of the systems, What is done when a major vulnerability is discovered and finally make the report of testing. |
| **Hacking Tools** | characteristics for the use of tools : Adequate documentation, Detailed reports on the discovered vulnerabilities, Updates and support when needed and reports that can be presented to managers. Such as : Port Scanners (Nmap. etc) and etc |
| **Conclusion** | **Ethical Hacking is the most effective way to find security weaknesses and the vulnerability of the system or network so that it can find ways to work around the solution to fix it before irresponsible people try to crashing the system** |

**REVIEW**

|  |  |
| --- | --- |
| **Title** | Indonesia Cyber Security Development: The Analysis Of Infrastructure, Regulation And Institutional Building |
| **Type** | INFORMATION SYSTEM APPLICATION |
| **Volume & Page** | Vol. 02, No. 01 |
| **Year** | 2007-2015 |
| **Author** | Elsa Faradilla, Anak Agung Banyu Perwita |
| **Reviewer** | SELI PURI ANDANI |
| **Date** | 06 Desember 2019 |

In this research centered upon the effort of Indonesia in resolving current global cyber threats and attacks by analyzing the cyber security infrastructure development, implementation of the regulation or policy, and role of the institutional building that handling cyber security. The time frame taken is from 2007-2015. Qualitative method will be used by this research in order to examine and explain the analysis in narrative order supported by some pictures and tables. The research seeks to conclude that how far the development of Indonesia cyber security in resolving current global cyber threats and attacks.

This paper aims at explaining the cyber threats as part of non-traditional threats in Indonesia and looks at the efforts of Indonesia’s government in dealing with this issue. More specifically, this paper focuses on the development of infrastructure, regulation and institutional building in countering the cyber security threats in Indonesia.

The strong and effective institutions are needed in carrying out the tasks and cyber security activities by referring to the specified policy. This includes the structure of the organization, the duties and responsibilities, working mechanism and monitoring. These institutions need to be realized through the study of the institutional development which followed by the steps of preparation and the formation, adjustments and/or institutional strengthening, so it provided effective institutions in support of cyber security.

The institutions also must be adjusted with the needs of the implementation of cyber security, in order to make sure that the purpose of the cyber security can be achieved optimally.

- Government institutions

- Educational institution/Community

- Business entity

**CONCLUSIONS**

Indonesia is currently in the urgent circumstances cyber security, because of the fact that the level of threats and attacks in the cyber space or cyber crime in Indonesia has reached the stage of concern. Indonesia establishes the first Cyber Security Center for Indonesia and establishes Disaster Recovery Center in every company, even though the implementation is still sectorial. The data network traffic in Indonesia is continuing to grow, even though not all Indonesia citizens can enjoy the high speed of internet access. Indonesian government has embracing international standard on security administration. Indonesia also has been installing of various internet security products to prevent possible, exploitation of various weakness which is owned by a system. Unfortunately, the development of technology in Indonesia can be categorized as quite slow compared to other countries in Southeast Asia; it is because of the political instability and the slow economic growth and the limited use of English in Indonesia, as well as lack of access to telecommunication infrastructure in rural areas. Currently, Indonesia also does not have the system Internet infrastructures that centralized and have many connections to the international network. So, the development of cyber security infrastructure in Indonesia is already good enough, but still need the improvement and serious action from government.

**REVIEW**

|  |  |
| --- | --- |
| Title | Backtrack System: Security against Hacking |
| Year | 2015 |
| Author | Munir A. Ghanem |
| Reviewer | Rahmaulia |
| Date | 7 Desember 2019 |

|  |  |
| --- | --- |
| Objective | In this journal discuss about research, Iam going to focus on the security tools of BackTrack system, which are really efficient and capable to analyze and protect from any hacking attack. This operating system “BackTrack” can launch a counter destructive attack. |
| Subject | In this research, I am focusing on “BackTrack System” and highlight more on its security and protection capabilities that can be used to rise security precautions levels and analyze system network in order to determine weakness points and identify points that attack our system.  My research subject is very important, especially in these days, where we heard in almost every week, about an e-attack that hits major sites in my country; Saudi Arabia, while the majority of people frightened, doesn’t know how to stop such attack. |
| Definition BackTrack System | It is an operating system based on Ubuntu GNU/Linux distribution aimed at digital forensics and penetration testing use. The most updated version of this operating system is “BackTrack 5”, which called “Revolution”. |
| Tools BackTrack System | * Metasploit integration: One of the major contents of Measploit integration is the Metasploit project, which is used to analyze & test computer network by giving information in regard to security vulnerabilities, penetration testing and IDS signature development. * Aircrack-ng: It is a network software suite consisiting of a detector, packet sibffer, WEP and WPA/WPA 2-PSK cracker and analysis tool for wireless LANs. * Kismet : It is a network detector, packet sniffer, and intrusion detection system for wireless LANs. * Nmap : It’s a network map-per that used as a security scanner to discover hosts and services on the computer network by creating a “map” of the network. * Ophcrack : It’s a free open source program that cracks windows passwirds by using LM hashes through rainbow tables. * Ettercap : It’s a free and open source network security tool for man-in-the-middle attacks on LAN. * Wireshark (formerly known as Ethereal) : It is a free and open-source packet analyzer that is used for network troubleshooting, analysis, software anf communications protocol development.      * BeEF (Browser Exploitatation Framework) : It is an open-source penetration testing tool used to test and exploit web application and browser-based vulnerabilities. * Hydra : This tool is the best, fastest and most powerful tool to guess passwords that relies on any protocol. * Owasp Open Web Application Security Project : Owasp is an online community dedicated to web application security. * Cisco OCS Mass Scanner : It is a very reliable and fast scanner for routers with telnet/enable default password. * Ouypt (Terminal Emulator) : It is a private software made by Crimson Hacking group. |
| Downloading & Using the System BackTrack System | The system is available to be downloaded from the manufactured company official web site: <http://www.backtrack-linux.org/>. The user is recommended not to download the system directly to PC unless he is aware of thissystem properties, as his PC maybe exposed to risks of damaging all of his files, due to this system privacy. Therefore, it’s recommended first to download a virtual program; Vmware Workstation program and thereafter to download BackTrack.  Support for Live CD and Live USB functionality allows users to boot BackTrack directly from portable media without requiring installation, though permanent installation to hard disk.  Generally, there are several tools in BackTrack, some of them to examine network by using network sniffers and file integrity checkers. Other tools are used to analyze and identify, targets by using application security testing, vulnerability scanning, wireless scanning and network port/service identifiers. Some tools in BackTrack are used to find vulnerable targets with tools that crack passwords, test remote access and use penetration testing. |
| Conclusion | This research raise an alert to the increase number of e-security breaches in my country: Saudi Arabia.  This research presents a system that is capable to permanently defend and stop e-security breaches.  Through this research, I want to extend a recommendation to Saudi universities council to teach active information security courses during the bachelor’s degree study plan, which synchronizes the modern developments that occurs in the hacking field.  Through this research, I want to extend a recommendation to Saudi universities to send excel students to participate in specialized information security training courses. |

**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 |
| 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.

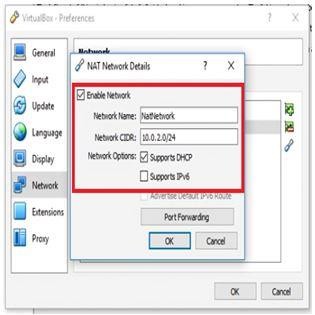
The benefits of virtualization is a incredibly simple way of establishing up a assessment environment, and eliminates the need to have to acquire shelves of computer systems and networking devices. The author utilizing my ProBook 4540s with i5 to manage a virtual test lab, but with the performance of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