**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. |