BackTrack System: Security against Hacking

Munir A. Ghanem

Information Technology Department, Northern Border University

Abstract- Hacking became one of the world's most famous information technology problem. It's the work of whom doesn't has a work, a work to gain more money, a work to harm others, and a work for many other purposes. Almost every week, if it is not every day, we hear about hacking attacks that hits many significant sites in the country, such as: Ministries, Banks, Uniform sites and many other important persons accounts on the social network sites. Fortunately, not all the hackers are professional in hacking, but they trained them self on one or more of such programs for one of the previous purposes. On the other side, the secret of success in such hacking attacks is that the intended attacked targets did not take the proper precautionary measures to protect themselves from such attacks.

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.

Index Terms- BackTrack, Hacking, Security, tools.

I. Introduction

Due to great developments that occurred in different technology fields and covers most of life aspects, depending on computer applications becomes an issue that no one can evade using it.

Computer applications exist in many important sites that can pose a threat to anyone, such as banks, passports general directorate, universities, ministries, emails web hosts, social media sites and many other sensitive country sites.

Depending on his interest, the hacker will be having so many options in which site to attack.

In the past few months, we heard about many e-attacks that hits many important electronic sites in Saudi Arabia. Unfortunately, these attacks happened without any reaction on how to stop such attacks, nor how to defend against it. The assumed hacker repeated his attack so many times, as he was confident that no one can stop him.

In this research, I am 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.

Lastly, our research presentation in front of the discussion committee, will be followed by a practical application to show the security tools of BackTrack.

II. Problem Definition

Problem that imposes to write this research can be summarized as follows:

1. Clear increase of hacking attacks without any deterrent or knowing how to stop it.
2. Unawareness of many individuals on how to secure their computers.
3. Raise people knowledge on e-piracy culture, and consequently raising knowledge of information security.
4. Active participating in national efforts against hackers attack.

III. BackTrack System

3.1. Definition:

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"[1].

It is intended for all audiences from the most savvy security professionals to early newcomers in the information security field. It consists of many different programs and tools specialized in security, protection and hacking. BackTrack is famous with "Penetration test" that can identify network security weakness.

3.2. History:

BackTrack distribution originated from merging of two formerly competing distributions which focused on penetration testing[2]:

- *WHAX*: a Slax based Linux distribution that was developed by a security consultant, MatiAharoni; Earlier versions of WHAX were called *Whoppix* and based on Knoppix.
- *Auditor Security Collection*: a Live CD based on Knoppix that was developed by Max Moser, which includes over 300 tools organized in a user-friendly hierarchy.

3.3. Tools:

BackTrack system provide users with easy access to a comprehensive and large collection of security-related tools, ranging from port scanners to password crackers. BackTrack includes many well known security tools that can be summarized as follows:

- Metasploit integration: One of the major contents of Metasploit 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. Another one main content of Metasploit integration is the Metasploit Framework, which is used for developing and executing exploit code against a remote target machine. The Metasploit integration is well known for its anti-forensic and evasion tools, where some of it are built into the tool.

- Aircrack-ng: It is a network software suite consisting of a detector, packet sniffer, WEP and WPA/WPA2-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 is used as a security scanner to discover hosts and services on the computer network by creating a "map" of the network. To achieve its goal, Nmap sends special crafted packets to the target host and analyzes the response.
- Ophcrack: It's a free open source program that cracks windows passwords 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. It can be used for computer network protocol analysis and security auditing.
- Wireshark (formerly known as Ethereal) : It is a free and open-source packet analyzer that is used for network troubleshooting, analysis, software and communications protocol development.
- BeEF (Browser Exploitation Framework) : It is an open-source penetration testing tool used to test and exploit web application and browser-based vulnerabilities. BeEF provides the penetration tester with practical client side attack vectors. It leverages web application and browser vulnerabilities to assess the security of a target and carry out further intrusions. This project is developed for lawful research and penetration testing.
- 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 Cisco routers with telnet/enable default password.
- Quypt (Terminal Emulator): It is a private software made by Crimson Hacking group. It is leaked to the Mainstream which is called Blackhat.

3.4: BackTrack System Releases [3]:

Date	Release
February 5, 2006	BackTrack v.1.0 Beta
May 26, 2006	The BackTrack project released its first non-beta version (1.0).
March 6, 2007	BackTrack 2 final released.
June 19, 2008	BackTrack 3 final released.
January 9, 2010	BackTrack 4 final release. (Now based on Debian)
May 8, 2010	BackTrack 4 R1 release
August 18, 2011	BackTrack5 R1 release based on Ubuntu

3.5 Downloading & Using the 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 this system 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.

Basically, for anyone who wants to download & use BackTrack, that the user has first to read intensively about the system to be familiar with its commands & tools.

3.5 Overview on BackTrack System:

This system has the same contents like any other windows operating system; e.g.: word editor, internet browser, control panel and many other user requirements & applications, in addition to the security tools which are the core of interest in this research.

BackTrack security tools can be arranged into twelve categories:

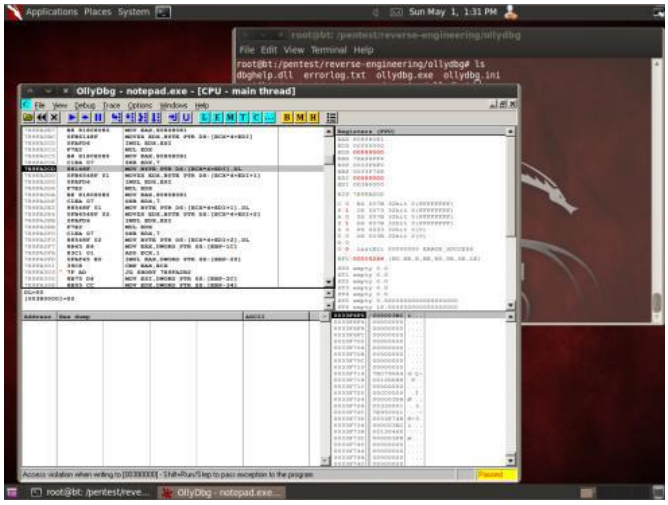
- Information Gathering.
- Vulnerability Assessment.
- Exploitation Tools.
- Privilege Escalation.
- Maintaining Access.
- Reverse Engineering.
- RFID Tools.
- Stress testing.

- Forensics.
- Reporting Tools.
- Services.
- Miscellaneous.

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.

Additional tools that do not pertain to penetration testing that Backtrack also offers covers privilege escalation, maintaining access, reverse engineering, radio frequency identification (RFID) tools, stress testing, forensics, reporting tools, network services, and other miscellaneous tools. After all, Backtrack can standout where it really can make a difference.

3.6 Photos of the program [1]:



IV. Conclusion and Further Work

1. This research raise an alert to the increase number of e-security breaches in my country; Saudi Arabia.
2. This research presents a system that is capable to permanently defend and stop e-security breaches
3. 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.
4. Through this research, I want to extend a recommendation to Saudi universities to send excel students to participate in specialized information security training courses .

References

[1] Retrieved from http://realitynerd.wordpress.com/tutorials/operating-system-guide/linux/backtrack-5-cracking/
[2] Retrieved from http://www.backtrack-linux.org/
[3] Retrieved from http://www.cc.boun.edu.tr/network_security.html
[4] Retrieved from http://www.greyfriars.net/gcg/greyweb.nsf/miam/article01
[5] W. Stallings, "Cryptography and Network Security-Principles and Practice", Fifth Edition, Pearson Education, 2010.
[6] Retrieved from http://forum.electroon.com/f39/
[7] Cardwell, Kevin. " BackTrack : Testing Wireless Network Security". Birmingham : Packt Publishing". 2013
[8] Pritchett, Willie. "BackTrack 5 Cookbook". Birmingham, Packt Pub"2012
[9] Ramachandran, Vivek. "BackTrack5 wireless penetration testing : beginner's guide". Birmingham

Authors

First Author – Munir A. Ghanem, Information Technology Department, Northern Border University, Email: munir.ghanem@nbu.edu.sa.