(BackTrack, 2012)

BackTrack Linux: The 21st Century Network Hacker's Dream Toolkit

William F. Slater, III, MBA, M.S., PMP, CISSP, CISA, ITIL v3, CDCP

February 10, 2013

Chicago, IL

United States of America

Introduction

This article is a brief introduction to Backtrack Linux. This distribution has quickly risen to the position of becoming the de facto hacker's tool for network infrastructures. This article is not a BackTrack user guide, nor is it a User Guide for any or all the tools that are available in BackTrack Linux. Rather, I am going to explain in general terms why BackTrack has become a best of breed hacker tool and some useful ways that you can use it to help make your organization more secure.

First a Quick Disclaimer

Though I consider myself a hacker like many of you, I think of myself as more of a very well-rounded cybersecurity professional who is out to educate and do good in the Internet and cybersecurity universe. In fact, due to my affiliation with several professional IT and IT security organizations, I am bound by several codes of conduct and/or codes of ethics to conduct myself ethically at all times. Therefore, though I can tell you about the uses of Backtrack, I have to be extremely careful to admonish you that 1) I am not doing blackhat hacking with the tools included with BackTrack; and 2) you can get yourself into real trouble (legally and criminally) using the tools that are included with Backtrack.

Strong Advice

Also, as a cybersecurity professional who has several certifications related to security and will complete an M.S. in Cybersecurity in March 2013, I am also obliged to explain to you that you should NEVER engage in any activities related to hacking on a network (reconnaissance or penetration or otherwise) without the explicit written permission of the owner of the network. Without this critical step, if you are in the U.S. and several other countries with well-defined computer laws, you are subjecting yourself to a world of troubles involving civil penalties, criminal penalties, or both.

What Is BackTrack?

BackTrack is a Linux distribution that is packaged with several standard network security hacker and exploitation tools.

Who Makes BackTrack?

BackTrack is assembled and packaged under the GNU Public Software License by Mati Aharoni, Emanuele Gentili, and others.

Where Do You Get BackTrack?

The easiest place to obtain BackTrack is to download it from the website at http://www.backtrack-linux.org. But you can also purchase it from places like Amazon, eBay, etc. Make sure when you obtain BackTrack from a place that is different from the original BackTrack website that you pay close attention to the version number that they are selling you. Otherwise, you may end up receiving an older version.

Backtrack is also included in this text: Hands-On Ethical Hacking and Network Defense, second edition, by Michael T. Simpson, et al, but since this book was published in 2011, it includes an older version of BackTrack.

What's In BackTrack?

BackTrack includes a great array of tools that can be used to assess the vulnerabilities that are present in an organization's network. The current edition of BackTrack, version 5 release 3, dated August 13, 2012.

Tool	Use
Metasploit for integration	Integration of attack scenarios
RFMON	Injection capable wireless drivers
Aircrack-ng	Cracking user passwords on wireless networks
Gerix Wifi Cracker	Cracking user passwords on wireless networks
Kismet	Wardriving and wireless network vulnerability identification
Nmap	Port scanning and stealth port scanning
Ophcrack	Cracking user passwords on wireless networks
Ettercap	Setting up man-in-the-middle attacks for network eavesdropping
Wireshark (formerly known as Ethereal)	Packet capture, inspection and advanced analysis.
BeEF	(Browser Exploitation Framework) Tool to identify browser vulnerabilities to assess the security posture of a target.
Hydra	Password cracker for browsers
OWASP Mantra Security Framework	A collection of hacking tools, add-ons and scripts based on the Firefox browser
Cisco OCS Mass Scanner	This is a very reliable, high performance scanner for Cisco routers that includes telnet

BackTrack Platforms – Where does it run?

Presently, BackTrack is confined to these CPU platforms: x86, x64, and ARM.

Using Backtrack

When you obtain BackTrack, if you have you the resources, you can install it to a virtual machine.

Other run options include:

1. Execution from a Live (Bootable) DVD (Configure your CMOS to go to the DVD Drive First)

2. Execution from a Live (Bootable) USB Configure your CMOS to go to the USB Drive First)

3. Installation in a dual-boot configuration on an existing laptop or PC

4. Installation on a Spare Laptop or PC Workstation

Why BackTrack?

What Are the Advantages of Using BackTrack?

The really nice think about BackTrack is that it includes some of the most commonly used tools for identification of vulnerabilities and hacking. It's also free if you download it, and easy to obtain, and relatively easy to use, once you master the basic uses of the tools that it includes.

What Are the Disadvantages of Using BackTrack?

There are a few disadvantages to using BackTrack and you should be aware of these:

1) Because each of the tools that are included with Backtrack are constantly being examined and improved by their respective publishers, then a BackTrack version can easily become outdated when a tool is revised.

2) Using BackTrack may provide you and/or organization with a false sense of security because BackTrack is not the ultimate set of hacker tools. There are many more tool suites with far more powerful capabilities. Nevertheless it is extremely powerful for something that is free or almost free, depending on where you get it.

3) Like any group of free tools, each of these tools has its limitations. If you want a better class of tools for vulnerability analysis and/or forensic analysis, you will ultimately pay for it or have to request that your organization does the analysis and pays for it.

4) If you are caught sneaking around and using BackTrack without authorization, don't be surprised if your management and/or your organization's Security Team think the worst about your activities and the nature of your intentions. Once upon a time, back in the 1970s, there were people whose homes might be searched on suspicion of crimes such as illegal drug possession. If during a court-ordered search, a copy of the Anarchist's Cookbook was identified, in a person's home, the law enforcement authorities would treat the person and the situation in a much more hostile manner, assuming the worst. Those sneaking an unauthorized copy of BackTrack into an organization on a DVD or a USB, or secretly installing it on a laptop or virtual machine may experience similar treatment.

What Are the Best BackTrack Resources?

I have included an extensive list of resources at the back of this article, and while many of these are related to hacking and penetration testing, to save you time, I will share the very best BackTrack in the list below:

Allen, L. (2012). Advanced Penetration Testing for Highly-Secured Environments: The Ultimate Security Guide. Birmingham, UK: Packt Publishing.

Faircloth, J. (2011). Penetration Tester's Open Source Toolkit, third edition. Waltham, MA: Syngress.

Harper, A., et al. (2011). Gray Hat Hacking: The Ethical Hacker's Handbook third edition. New York, NY: McGrawHill.

Prichett, W. and Smet, D. D. (2012). Backtrack 5 Cookbook: Over 80 recipes to execute many of the best known and little known penetration testing aspects of BackTrack 5. Birmingham, UK: Packt Publishing.

Ramachandran, V. (2011). BackTrack Wireless Penetration Texting: Mastering bleeding edge wireless testing techniques with BackTrack 5. Birmingham, UK: Packt Publishing.

Simpson, M. T., et al. (2011). Hands-On Ethical Hacking and Network Defense. Boston, MA: Course Technology.

Singh, A. (2012). Metasploit Penetration Testing Cookbook: Over 70 Recipes to master the most widely used penetration testing framework. Birmingham, UK: Packt Publishing.

Are Penetration Tests a Good Thing?

Yes. Absolutely penetration tests are a good thing because they will help you identify network and software vulnerabilities that must be remediated using security controls, so that you can resolve the problems before the bad guys get into to your company's IT infrastructure.

Penetration tests are valuable for several reasons:

1. Determining the feasibility of a particular set of attack vectors (Wikipedia, 2013).
2. Identifying higher-risk vulnerabilities that result from a combination of lower-risk vulnerabilities exploited in a particular sequence (Wikipedia, 2013).
3. Identifying vulnerabilities that may be difficult or impossible to detect with automated network or application vulnerability scanning software (Wikipedia, 2013).
4. Assessing the magnitude of potential business and operational impacts of successful attacks (Wikipedia, 2013).
5. Testing the ability of network defenders to successfully detect and respond to the attacks (Wikipedia, 2013).
6. Providing evidence to support increased investments in security personnel and technology (Wikipedia, 2013).
7. Penetration tests are a component of a full security audit. For example, the Payment Card Industry Data Security Standard (PCI DSS), and security and auditing standard, requires both annual and ongoing penetration testing after system changes to identify potential vulnerabilities and/or configuration anomalies (Wikipedia, 2013).

Adopting a framework

Penetration tests are best planning and performed as projects. If you plan to use BackTrack as your toolkit of choice for whitehat or grayhat penetration testing on your company's infrastructure, besides obtaining permission for the actual hacking process, you will probably want to study, adopt and use one of a couple of well-defined open frameworks for penetration testing. In this way, your organization's leadership will recognize that you are taking a professional approach to your penetration testing to uncover one or more vulnerabilities that may exist in your infrastructure and/or in the users that access and user the infrastructure to use your organization's networked resources.

Conclusions

BackTrack Linux and its associated tool suite is a valuable tool that can help you make your company's IT infrastructure more secure if you will carefully and systematically address the vulnerabilities identified by tools like NMAP and Kismet. In the hands of bad guys (you know that bad guys have BackTrack and use it also) you can be sure that it is a formidable tool for reconnaissance and actual penetration testing. It is best to find and fix your own vulnerabilities before the bad guys find and exploit your vulnerabilities and commit acts like data theft, sabotage, and/or espionage on your network. Again, my advice is to get BackTrack, research, learn and adopt a formal penetration testing methodology, and ALWAYS get written permission to conduct the operations that BackTrack and its tools will easily allow you to do. In fact, because the mere existence of BackTrack on your network can represent a threat to your IT Security Department, you should also obtain written permission to bring it into the company and install it.

Finally, if you do get BackTrack, take the time to learn how use the tools that are packaged with Backtrack and keep them updated, because as everyone knows, tools that are current perform better and constitute less of a security threat to the person using the tool.

Resources and References:

Allen, L. (2012). Advanced Penetration Testing for Highly-Secured Environments: The Ultimate Security Guide. Birmingham, UK: Packt Publishing.

Allsopp, W. (2009). Unauthorized Access: Physical Penetration Testing for IT Security Test Teams. West Sussex, U.K.: Wiley Publishing.

Altheide, C. and Carvey, H. (2011). Digital Forensics with Open Source Tools. Waltham, MA: Syngress.

Andress, J., and Linn, R. (2012). Coding for Penetration Testers: Building Better Tools. Waltham, MA: Syngress.

Armistead, L. (2004). Information Operations: Warfare and the Hard Reality of Soft Power. Washington, DC: Brassey's Inc.

Backtrack. (2012). BackTrack Linux. Retrieved from http://www.backtrack-linux.org on September 30, 2012.

Basta, A. and Halton, W. (2008). Computer Security and Penetration Testing. Boston, MA: Thomson Course Technology.

Brancik, K. (2008). Insider Computer Fraud: An In-Depth Framework for Detecting and Defending Against Insider IT Attacks. Boca Raton, FL: Auerbach Publications.

Brenner, J. (2011). America the Vulnerable: Inside the New Treat Matrix of Digital Espionage, Crime, and Warfare. New York, NY: Penguin Press.

Chririllo, J. (2003). Hack Attacks Testing: How to Conduct Your Own Security Audit. Indianapolis, IN: Wiley Publishing, Inc.

Cialdini, R. B. (2009). Influence: Science and Practice, fifth edition. Boston, MA: Pearson Education.

Cole, E. and Ring, S. (2006). Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Present Employees and Contractors from Stealing Corporate Data. Rockland, MA: Syngress Publishing, Inc.

Cunningham, B., et al. (2005). Network Security Evaluation Using the NSA IAM. Burlington, MA: Syngress.

Dhanjani, N., et al. (2009). Hacking: The Next Generation. Sebastopol, CA: OReilly.

Engebretson, P. (2011). The Basics of of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy. Waltham, MA: Syngress.

Erikson, J. (2008). Hacking: the Art of Exploitation, second edition. San Francisco, CA: No Starch Press.

Faircloth, J. (2011). Penetration Tester's Open Source Toolkit, third edition. Waltham, MA: Syngress.

Fennelly, L. J. (2004). Effective Physical Security, third edition. Burlington, MA: Elsevier.

Hadnagy, C. (2011). Social Engineering: The Art of Human Hacking. Indianapolis, IN: Wiley Publishing, Inc.

Harper, A., et al. (2011). Gray Hat Hacking: The Ethical Hacker's Handbook third edition. New York, NY: McGrawHill.

Jackson, G. M. (2012). Predicting Malious Behavior: Tools and Techniques for Ensuring Global Security. Indianapolis, IN: Wiley Publishing, Inc.

Long, J., et al. (2008). Google Hacking for Penetration testers, Volume 2. Burlington, MA: Syngress Publishing, Inc.

Long, J., et al. (2008). No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing. Burlington, MA: Syngress Publishing, Inc.

McNab, C. (2008). Network Security Assessment. Sebastapol, CA: OReilly.

Middleton, B. (2005). Cyber Crime Investigator's Field Guide, second edition. Boca Raton, FL: Auerbach Publications.

Mitnick, K. and Simon, W. (2002). The Art of Deception: Controlling the Human Element Security. Indianapolis, IN: Wiley Publishing, Inc.

Mitnick, K. and Simon, W. (2006). The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers. Indianapolis, IN: Wiley Publishing, Inc.

Mutch, J. and Anderson, B. (2011). Preventing Good People from Doing Bad Things: Implementing Least Privilege. New York, NY: Apress.

Northcutt, S., et al. (2006). Penetration Testing: Assessing your Overall Network Security Before Attackers Do. A SANS Technical Whitepaper Published in June 2006. Retrieved from http://www.sans.org/reading_room/analysts_program/PenetrationTesting_June06.pdf on June 6, 2012.

Parker, T., et al. (2004). Cyber Adversary Characterization: Auditing the Hacker Mind. Rockland, MA: Syngress Publishing, Inc.

Peikari, C. and Chuvakin, A. (2004). Security Warrior. Sebastapol, CA: OReilly.

Pfleeger, C. P. and Pfleeger, S. L. (2003). Security in Computing, third edition. Upper Saddle River, NJ: Prentice Hall.

Prichett, W. and Smet, D. D. (2012). Backtrack 5 Cookbook: Over 80 recipes to execute many of the best known and little known penetration testing aspects of BackTrack 5. Birmingham, UK: Packt Publishing.

Raghavan, S. V. and Dawson, E. (editors). (2011). An Investigation in the Detection and Mitigation of Denial of Service (DoS) Attacks: Critical Information Infrastructure Protection. Chennai, India: Springer.

Ramachandran, V. (2011). BackTrack Wireless Penetration Texting: Mastering bleeding edge wireless testing techniques with BackTrack 5. Birmingham, UK: Packt Publishing.

Rogers, R., et al. (2008). Nessus Network Auditing, second edition. Waltham, MA: Syngress.

Sammons, J. (2012). The Basics of Digital Forensics: the Primer for Getting Started in Digital Forensics. Waltham, MA: Syngress.

Schneier, B. (2008). Psychology of Security. An article published at Schneier.com on January 18, 2008. Retrieved from the web at http://www.schneier.com/essay-155.html on March 13, 2012.

Shema, M. (2011). Hacking Web Apps: Detecting and Preventing Web Application Security Problems. Waltham, MA: Syngress.

Simpson, M. T., et al. (2011). Hands-On Ethical Hacking and Network Defense. Boston, MA: Course Technology.

Singh, A. (2012). Metasploit Penetration Testing Cookbook: Over 70 Recipes to master the most widely used penetration testing framework. Birmingham, UK: Packt Publishing.

Street, J., et al. (2010). Dissecting the Hack: the Forbidden Network, revised edition. Burlington, MA: Syngress.

Wikipedia. (2013). Penetration test. An article retrieved from http://en.wikipedia.org/wiki/Penetration_test on February 1, 2013.

Wiles, J., et al. (2007). Low Techno Security's Guide to Managing Risks: For IT Managers, Auditors, and Investigators. Burlington, MA: Syngress Publishing, Inc.

Wiles, J., et al. (2012). Low Tech Hacking: Street Smarts for Security Professionals. Waltham, MA: Syngress Publishing, Inc.

Wilhelm, T. and Andress, J. (2011). Ninja Hacking: Unconventional Penetration Testing Tactics and Techniques. Burlington, MA: Syngress.

Wilhelm, T. (2010). Professional Penetration Testing: Creating a Formal Hacking Lab. Burlington, MA: Syngress.

Bio:

William F. Slater, III is an IT security professional who lives and works in Chicago, IL. He has over 20-security related certifications, including a CISSP, SSCP, and a CISA certification. In March 2013 he completes his M.S. in Cybersecurity Program at Bellevue University in Bellevue, Nebraska. He has written numerous articles on IT Security and Cyberwarfare. Mr. Slater is also an adjunct professor at the Illinois Institute of Technology and the devoted husband of Ms. Joanna Roguska, who is a web developer and a native of Warsaw, Poland. You can read more about Mr. Slater at http://billslater.com/interview.