Security Assessment with Kali Linux

Petar Čisar*, Sanja Maravić Čisar**, Igor Fürstner***

*Academy of Criminalistic and Police Studies, Belgrade, Serbia,
**Subotica Tech, Subotica, Serbia,
***ÓBUDA UNIVERSITY, Donát Bánki Faculty of Mechanical and Safety Engineering, Budapest, Hungary,
petar.cisar@kpa.edu.rs, sanjam@vts.su.ac.rs, furstner.igor@bgk.uni-obuda.hu

***Abstract* — This paper discusses the assessment of information system security. When referring to the security of an information system, the authors focus on three major features of the system: confidentiality, integrity and availability. Diverse methods are used to identify existing security weaknesses and security assessment, including the Kali Linux operating system. This work offers a wide-ranging overview of possible uses, benefits and drawbacks. The greatest advantage of implementing this operating system is the considerable collection of various tools for vulnerability assessment and penetration testing, mainly intended for ethical hacking. Further, the paper outlines which present forms of vulnerabilities are best identified by Kali.**

***Keywords*:** Kali Linux; information security assessment; vulnerability; penetration test, ethical hacking

1 INTRODUCTION

The roles that various organizations in information security (vendors, coordinators, researchers, users) play are numerous, including motivations, priorities, resources etc. When referring to the security of an information system, the authors focus on the three main features of the system: confidentiality, integrity and availability. These days it is the task of IT experts to identify and evaluate vulnerabilities across the range through a great number of specific hardware and software configurations. Further, they ought to regulate these vulnerabilities and repair the ones that pose the most serious danger. The most important challenge is to generate applicable, actionable information in a given case of enormous vulnerability data. In this setting, vulnerability refers to a weakness in the design, implementation, use and management of an information system.

In an attempt to assess the security needs of a given organization, so as to efficiently counter cybercrime and select different security products, policies, procedures and decisions, it is necessary to define requirements and categorization of approaches that satisfy these criteria in a systematic way. Three aspects of information security need to be examined:

- Attack – Any action risking the security of information. Attack is the basic form of cybercrime.
- Security mechanism – The mechanism devised to identify, prevent or recover from a security attack.
- Security service – Service that improves the security system for the processing and transfer of data. Security service implies using one or more security mechanisms.

Identification of existing security weaknesses and security assessment may happen in various ways, including the use of the Kali Linux operating system. This paper outlines its capabilities, its benefits and drawbacks.

2 INFORMATION SECURITY ASSESSMENTS

Commonly, there are four main categories (or phases) of information security assessment [1]: a vulnerability assessment, a compliance (audit) test, a traditional internal/external penetration test, and an application assessment.

Vulnerability assessment: A vulnerability assessment (scan) is a technical assessment designed to yield as many vulnerabilities as possible in an environment, along with severity and remediation priority information.

Penetration test: A penetration test is an attack on a computer system, network or Web application to find vulnerabilities that an attacker could exploit with the intention of finding security weaknesses, potentially gaining access to it, its functionality and sensitive data. The output is a report which states the goals as either achieved or not, it also includes other observations made in the process. These penetration tests fail to offer a full list of vulnerabilities and they do not prioritize what was detected. They can be automated with software applications or can be performed manually. Penetration tests are sometimes termed “white hat” attacks due to the fact that in a pen test, the break-in is performed by the ‘good guys’. In slang, the term “white hat” identifies an ethical hacker, or a computer security expert, whose field of specialty is penetration testing and various testing methodologies so as to safeguard the security of an organization's information systems.

Application assessment: An application assessment (usually white- or black-box testing) is used to assess the functionality and resilience of an application to determine security threats including (but not limited to) buffer overflows, cross site scripting (XSS), cross site request forgery, unsuitable data sanitization, injection attacks (for instance, SQL Injection) and weak authentication. This assessment evaluates all components of an application infrastructure, including the form of each component’s deployment and form of communication with both the client and server environments. Experts use a group of commercial and open-source tools to perform this assessment as well as run manual testing. Application credentials may be required for a more encompassing review of a particular application to be conducted. Normally, the review of some host and network security practices is part of an application vulnerability assessment. Among the applications that may be assessed in this

manner are the following: Web applications, compiled desktop applications and mobile applications.

Compliance (audit) test: The task of audits is to determine how a given organization measures against a particular standard. As a general rule, audits do not test security directly, but rather test compliance with a standard. It is possible for the standard, which is tested against, to have a strong or weak link to actual security, while this should not be confused with a vulnerability assessment or penetration test. The output of an audit is a list of areas, which, if compliance is to be achieved, need to be fixed.

The figure below summarizes all the phases described previously, as well as their corresponding activities.

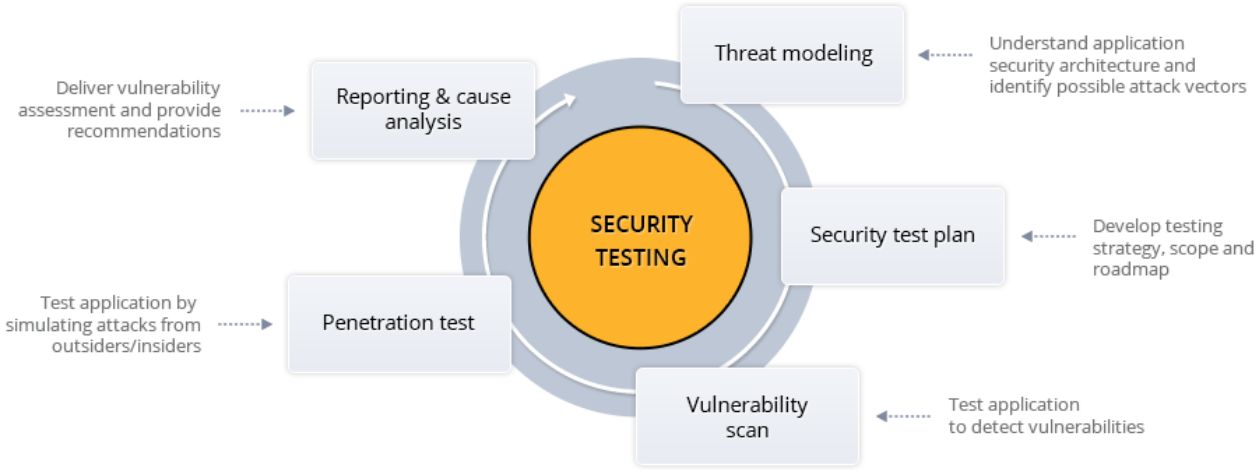

Fig. 1. Phases of security testing

The main difference between vulnerability assessment and penetration testing lies in the fact that the flaws that exist in the system are indentified by the vulnerability assessments without their impact measured. Conversely, the penetration testing makes headway and exploits these vulnerabilities in order to evaluate their consequences.

Among the most widespread vulnerability classes (attacks) are [1]: denial-of-service (DoS; breaks the behavior of an application rendering it inaccessible), memory corruption (e.g. buffer overflow; leading to manipulation of process memory, thereby frequently enabling an attacker code execution), Web vulnerabilities (which attack web services using techniques like SQL injection and XSS), password attacks (attacks against the authentication system; often leverage password lists to attack service credentials) and client-side attacks.

3 Penetration Testing Methodology

Penetration testing methodology and standards are vital for the success of this ethical hacking technique, helping security professionals asses information security measures.

The penetration testing process involves the following:

- planning and preparation
- collecting information about the target prior to the test (reconnaissance)
- vulnerability detection - possible entry points identification (port scanning)
- penetration attempt - trying for a break-in (either virtually or for real)
- analysis and reporting

Formulating these differently (in fact, more informally), the steps of the penetration test are as follows:

- Establish the goal
- Information gathering
  - Reconnaissance
  - Discovery (port scanning, vulnerability scanning)
- Vulnerability analysis
  - Taking control (exploitation, brute forcing, social engineering)
  - Pivoting
- Reporting
  - Evidence collection
  - Risk analysis
  - Remediation

While one can find many security testing methodologies, there are few that provide stepwise, consistent instructions on measuring the security of a system or application. Five of the most famous open source security assessment methodologies are [2]:

- Open Source Security Testing Methodology Manual (OSSTMM),
- Information Systems Security Assessment Framework (ISSAF),
- Open Web Application Security Project (OWASP),
- Penetration Testing Execution Standard (PTES),
- Web Application Security Consortium Threat Classification (WASC-TC).

For instance, the Web Application Penetration Testing Methodology based on OWASP consists of 12 subcategories [3]:

1. Introduction and Objectives
2. Information Gathering

3. Configuration and Deploy Management Testing
4. Identity Management Testing
5. Authentication Testing
6. Authorization Testing
7. Session Management Testing
8. Data Validation Testing
9. Error Handling
10. Cryptography
11. Business Logic Testing
12. Client Side Testing.

The figure below graphically presents the general testing methodology.

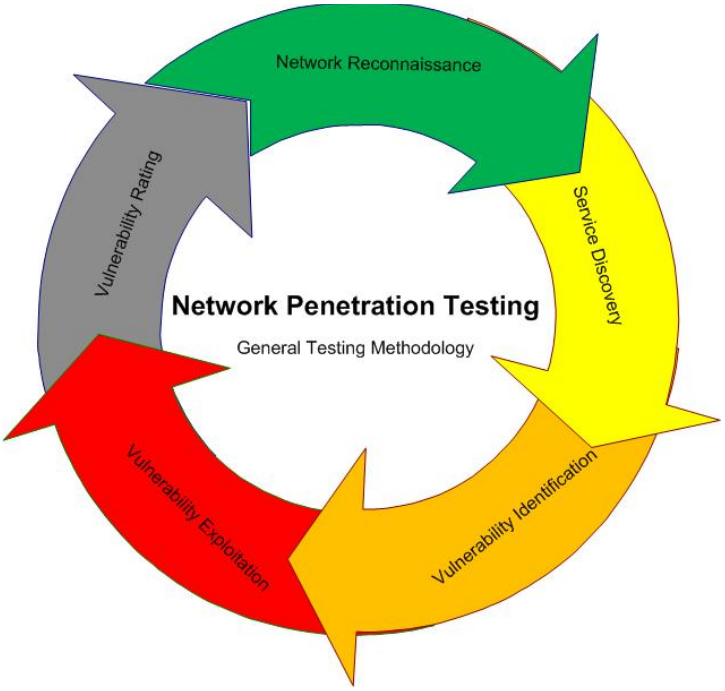

Fig. 2. General testing methodology

4 Penetration Testing Tools Available in Kali Linux

Kali Linux is a Debian-based Linux distribution aimed at advanced penetration testing and security auditing. Kali includes hundreds of tools tailored to perform a number of information security tasks, including penetration testing, security research, computer forensics and reverse engineering.

There are several ways to run Kali Linux, either from a hard disk, live CD, or live USB. It is a supported platform of the Metasploit Project's Metasploit Framework, a tool for developing and executing security exploits. Kali Linux was released in 2013 as a complete rebuild of BackTrack Linux, completely keeping to Debian development standards.

Tools integrated in Kali can be classed as follows [4]: Information gathering,

- Vulnerability analysis,
- Wireless attacks,
- Web applications,
- Exploitation tools,
- Forensics tools,
- Stress testing,
- Sniffing and spoofing,
- Password attacks,
- Maintaining attacks,
- Reverse engineering,
- Hardware hacking and Reporting tools (Fig. 3).

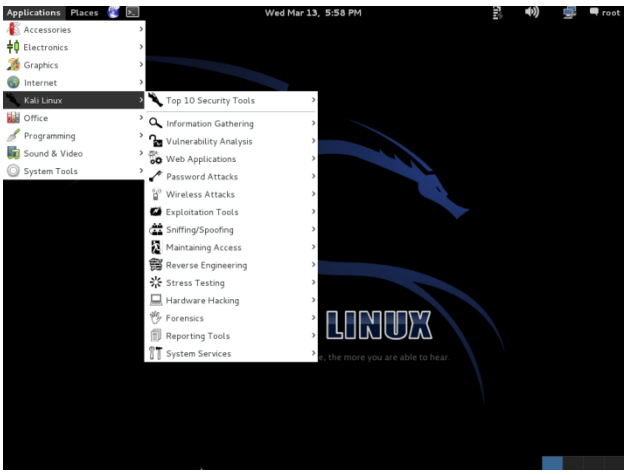

Fig. 3. Kali Linux integrated tools

Kali Linux is preinstalled with a great many popular penetration testing tools, including: Nmap (port scanner),

Wireshark (packet analyzer), John The Ripper (password cracker), Aircrack-ng (software suite for penetration testing wireless LANs), Nikto (web server scanner), Sqlmap (tool for identifying and exploiting SQL injection flaws and taking over of database servers), Owasp-zap (discovering vulnerabilities in web applications), Metasploit Framework (exploitation), among others.

5 Benefits and Drawbacks of Kali Linux

Kali Linux has benefits and drawbacks, like any other Linux distribution. The user profile will determine the choice (pen-tester/simple user/developer). Kali is a Linux distribution specifically aimed at professional penetration testers and security specialists, and considering its unique nature, this distribution is not recommended for users who are not familiar with Linux or those searching for a general-purpose Linux desktop distribution for development, web design, gaming, etc.

The advantages of implementing Kali Linux [5]:

Advanced penetration testing tools - Kali Linux has upward of 600 advanced penetration testing tools incorporated. The tools of BackTrack Linux, which fall short of the mark or repeated countlessly, have been replaced in the Kali Linux system with the advanced penetration testing tools.

Ultimate free Linux tool - The Kali Linux system is completely free like the BackTrack Linux and offers their users the free life time services. This is a significant plus factor encouraging people to opt for this system.

Open sourced Git tree - This Kali Linux is open source system and is readily accessible to the users. All the codes in the Kali Linux are easily visible for any users and the open development tree also enables users to check the development of coding at every step.

FHS support - Kali observes the FHS (File-system Hierarchy Standard), offering Linux users easy access to binaries, support files, libraries, etc. This key feature distinguishes Kali Linux from other Linux systems.

However, Kali Linux also has drawbacks that must be mentioned [5]:

1. There are countless users still not familiar with Linux, but 'Windows minded' instead. One way of surmounting this disadvantage is by offering trainings or education so that users become familiar with Linux.

2. Support hardware from certain vendors that do not perform well on Linux.

3. The installation software/applications are more complicated than in Windows. Installing software on Linux will become easier when connected to the internet or if have a CD / DVD.

4. System administrators new to Unix-like systems (such as Linux) will predictably have to familiarize themselves with these.

6 Conclusions

Kali Linux is a significant step of progress, the output of ceaseless upgrading of distribution. Also, it has a novel appearance, new features, tools, and workflow. In comparison with BackTrack, its predecessor, Kali feels somewhat more comprehensive, more stout, despite the fact that both distributions have the same focus and balance on normal, every-day usability, and forensics. Moreover, it ensures hacking and analysis tools that may not only enable users to audit and save their environment but, apart from that, also learn a considerable amount about the network stack and command line utilization.

References

[1] Hertzog, R., O'Gorman, J., & Aharoni, M. (2017). Kali Linux Revealed, Offsec Press, 283-284.

[2] Allen, L., Heriyanto, T., & Ali, S. (2014). Kali Linux - Assuring Security by Penetration Testing, Packt Publishing, 54-64.

[3] Meucci, M., & Muller, A. (2014). Testing Guide 4.0. OWASP, Web Application Penetration Testing, https://www.owasp.org/images/1/19/OTGv4.pdf

[4] Kali Linux Tools Listing, https://tools.kali.org/tools-listing

[5] Quora, https://www.quora.com

[6] Official Kali Linux Documentation. (2014)., https://docs.kali.org/pdf/kali-book-en.pdf

[7] Offensive Security: Penetration Testing With Kali Linux, https://www.offensive-security.com/documentation/penetration-testing-with-kali.pdf

[8] Pritchett, W., & De Smet, D (2013). Kali Linux Cookbook. Packt Publishing.