Web penetration testing with kali linux research paper

Law, Security

ASSIGN BUSTER

\n[toc title="Table of Contents"]\n

\n \t

\n[/toc]\n \n

Testing web penetration aspect with Kali Linux

Introduction

With security issues of the internet becoming a major point of concern for many organizations, there is a need to have testing of the internet to check if there is sufficient security. This is equivalent to auditing the penetration of the organization. Penetration testing is a process where the vulnerabilities that have been identified are real threats or false. One of the methods that an assessment can make use is that of scanning tools which can show the vulnerabilities that exist in a given system. The penetration test would be conducted by trying to hack the given vulnerabilities just the way a hacker does and see the result. This would show if the attack would be successful. By this process, there would be the distinction of genuine and false threats and the administrators would concentrate on the ones that seem to be genuine in the system. The penetration tests that are found to be successful are those that target specific systems with goals that are specific goal and target. One of the main features of a penetration test would be quality and not quantity. By testing about a specific system in the process of penetration testing, there will be detailed information that will be gathered regarding the system in this process. Penetration testing does not make systems to be more secure but only evaluates the security that is available in the network (Rubens, 2010).

Research question/problem

This paper will be guided by the following research question:

How exhaustive is Kali Linux in undertaking web penetration testing?

This is an important concept that should be undertaken in any network security assessment as this will show the areas that need to be checked in the security assessment process. It is important to understand the methodology that is used web penetration testing and see if they are as effective. In this process of web penetration testing, there is a need to be effective and exhaustive in undertaking the process.

Features of Kali Linux

Kali Linux is an advanced development of Back Track Linux. The new distribution has advanced and more developed features of web penetration. One of the motivations for the development of Kali Linux was the need to have more advanced and enhanced features of web penetration testing. This would combat the threats that were brought about by cyber attacks. For improved internet security, there is a need to undertake penetration testing. One of the advantages of Kali Linux over Back Track is that it has more updated tools. The tools have been streamlined with the repositories of Debian and the synchronization takes place four times a day. This translates to having more updated security fixes in the system. The new Kali Linux filesystem that is compliant means that the tools can be run from any location in the system. It makes security processes easier. Other security features that have been enhanced with Kali Linux are the customization, installation which is unattended and desktop environments which are flexible. These are the strongest features that come with Kali Linux (Rubens, 2010).

Analysis

Reconnaissance

One aspect of assessing the exhaustibility of a security tool is that of reconnaissance. This is the process of scanning and exploring the environment that is the used by the attacker. This is learning more information regarding the environment of the attacker. This is the process that an attacker or penetration tester will do. This is referred to as footprint establishing for a target. This process is not undertaken actively but passively. It is also a legal process.

Kali Linux has tools that are used to undertake reconnaissance. The set of tools is referred to as Information Gathering tools. These tools are specified for gathering information regarding the target. There are extensive tools that are used for information gathering regarding the target. Kali Linux has an efficient information gathering mechanism that is well developed than the rest of the distributions (Okolie et al., 2013).

When undertaking reconnaissance, there is great emphasis on knowing as much information about the target. There are many tools that are found on the internet that are used to undertake reconnaissance. There are ICMP reconnaissance tools that are available and are used for undertaking reconnaissance procedures. One of the basic information that is used to find the basic information about the target is ping and traceroute commands. As the commands traverse the different devices like routers, firewalls and other devices that are used by computer systems.

There are other tools that are installed in high-target reconnaissance. These are the DNS names that are associated with DNS. Domain information gropper is one of the most widely used information gathering tools that are available (Okolie et al., 2013).

One of the security features that have been installed on Kali Linux for information gathering procedures is Fierce. This is a tool that comes with Kali Linux and is used for gathering the information about the target that is being investigated. This tool works with DNS mechanism and will check the DNS server if it allows zone transfers. If this is enabled in the server, then Fierce will then undertake a zone transfer and will then inform the user of the entries that are involved. If the host DNS server does not allow zone transfer, then Fierce can be configured to brute force host names on the DNS server. The creation of Fierce was to enable reconnaissance to take place (Offensive Security, 2013).

Maltego

This is a tool that is built into Kali Linux. It is a graph that is used to gather information. This is a tool that is used to gather information by employing the open and public information that is found on the internet. It has reconnaissance tools that have been built into the system. The tool has more functionalities as there is some information that has been enabled. It has more intelligence on the process (Offensive Security, 2013).

Conclusion

Kali Linux has built in tools that enable it to undertake web penetration testing. The developments of Kali Linux distribution has been emphasized on security issues. There have been the developments and enhancements of the distribution to gather information regarding the target. In penetration testing, the knowledge about the target should be understood well. This is an important process that has been integrated in the development of Kali Linux. There are many security features that have been developed in this distribution. Penetration testing is exhaustive and the research question can be said to have been answered.

References

Offensive Security (2013). Kali Linux Tools Policy. Retrieved on 20 Nov 2013 from http://docs. kali. org/kali-policy/penetration-testing-tools-policy

Okolie C. C., Oladeji F. A, Benjamin B. C., Alakiri H. A, Olisa O. (2013). Penetration Testing for Android Smartphones. Retrieved on 20 Nov 2013 from http://iosrjournals. org/iosr-jce/papers/Vol14-issue3/P0143104109. pdf

Rubens, P. (2010). Automate penetration testing with Linux and Fast-track.

Retrieved on 20 Nov 2013 from http://www. wi-fiplanet. com/tutorials/article.

php/3856916/Automate-Penetration-Testing-with-Linux-and-Fast-Track. htm