International Journal of Computer & Information Technologies (IJOCIT)
www.ijocit.ir & www.ijocit.org
ISSN = 2345-3877

Full Summary of the Activities of the Penetration Testing in Electronic Payment

Mehdi mehdizadeh [1], Dr.Nasser modiri [2]
[1]MSc, Department of Electrical, Computer & IT, Zanjan Branch, Islamic Azad University,
[2] Associate Professor in Department of Electrical , Computer & IT, Zanjan Branch,
Islamic Azad University, Zanjan, Iran
post_mehdizade@yahoo.com[1]

Abstract: Organizations to assess their influence, the influence of expensive, hackers and stay safe for the equipment and sites and their access information such as the influence of their expensive test , are testing and assessment themselves, this test method is called penetration testing. In fact penetration testing test and network security assessment and the services, programs, applications, data and all the information is in an organization that in which the behavior of the invaders and influence of expensive are evaluated by the evaluator team and the influence of the ways of penetrate is done. In this article we will explores and introduces network penetration testing and web pages that electronic payments through them is done , as well we will review the most important methods and tools for penetration testing

Keywords: Security Holes, Electronic Payment, Penetration Testing, Manual Penetration Testing, Automated Penetration Testing, Web Scanners.

1. Introduction

Web-based applications to provide their services to users use network infrastructure and it is necessary to learn how to get users to these types of programs, and according to the existing policy, provide access .With the increasing growth of the Web-based application and interaction with different people a security requirement, is a necessity. Yet, we witness various attacks to Web-based applications with the goal of financial abuse or theft of sensitive information.

Many attacks result in defects and security holes in the authentication section. Only one vulnerability on the authentication mechanism,

would be able the attacker to access unlimited to the functions and the application data. Without Strong authentication mechanisms none of the other security mechanisms like access control and session management can be useful.

So far, there are several methods for authentication is done on the Web. Reducing vulnerability in the Web through the Security requirements, which is to develop a bio-secure Web applications are associated with the authentication process for the abatement of these attacks.

One of the best methods to pull out security bugs is using penetration testing at a specified time period and continuous.

Take advantage of the e-payment requires high security payment system at different levels.

An electronic payment system is a mechanism of payment or the transaction pricing on a public network for obtaining commodities (electronic or physical) to provide the service.

Payment via networks, especially Internet requires a high security because sending the data and financial information such as credit card numbers, account numbers, confidential financial information, send the password and password code and thousands of other confidential information concerns for both parties to the transaction and this is the good reason for the importance of the methods for creating secure and a variety of secure payment systems, this is an issue that requires penetration testing should be carried out in this type of network at the time specified.

The following flow chart shows the overall penetration testing.

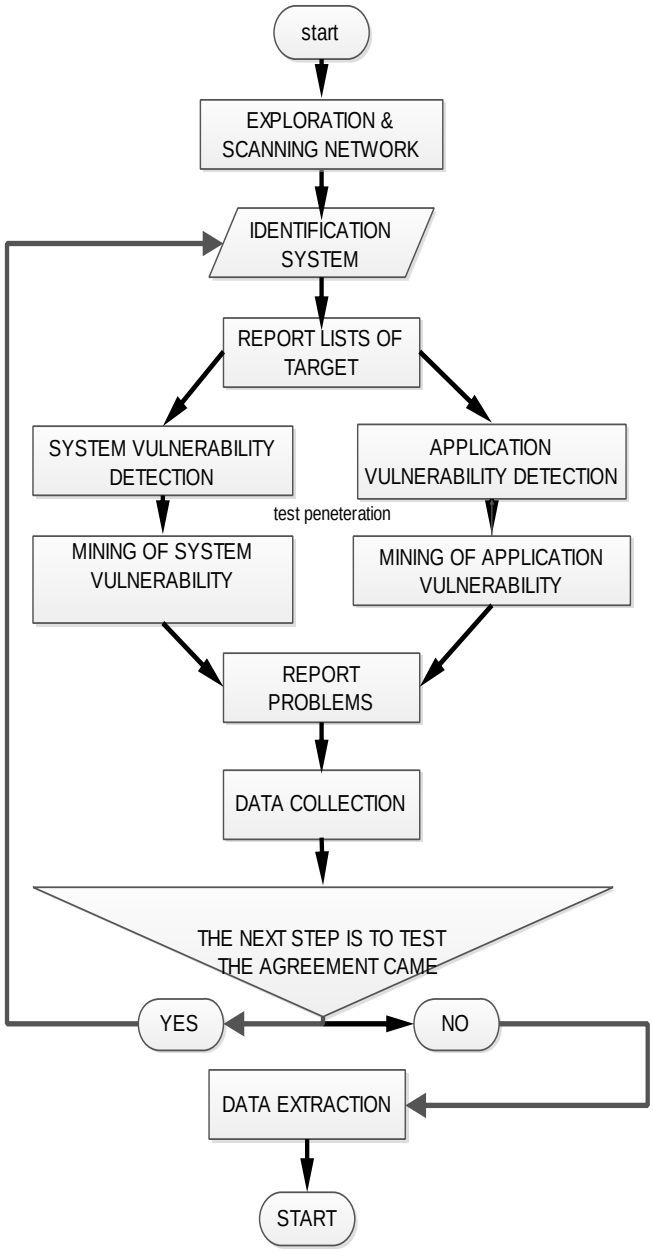

Figure 1: Flowchart of Penetration Testing

This paper is organized as follows. First, in section 2 we introduce penetration testing. penetration testing web applications results are presented, in the section 3. Finally, we conclude our paper in section 4

2. Penetration Testing

Network penetration testing, security assessment process, is a services and applications in an organization, in which the actual behavior of a team or group of assailants can be simulated by the appraiser. In fact, penetration testing is a comprehensive activity of using of technical and non technical invasive methods that it is needed so efficient and experienced team. Whatever the level of knowledge and expertise of the evaluation team which run the penetration testing preceded and they take advantage of the more specialized tools, they will get more accurate and deeper results.

In this security assessment, while attempting to collect the maximum of information and knowledge of network, information systems and programs and software used in the target organization the evaluator team tries to find a bunch of security weakness for bypass and disable the security protection and control, and obtain or upgrade accessibility.

In implementing penetration testing a variety of security weaknesses and vulnerabilities are to be considered during the implementation of the attacks and instead of having an independent look to each vulnerability assessment it is applied to combine them by team to simulate a real scenario.

This is caused a more accurate view of the damages that the assailants were able to enter to the information into the system and network organization and this is also considered an advantage compared to the assessment technical vulnerability independently for the organization. The objective of penetration testing is increasing the coefficient of data and network security. Information and security weaknesses that can be specified in the penetration testing are confidential and should not be up to the full disclosure on the side.

2.1. Kinds of Penetration Testing:

Penetration testing a variety of ways for the most major difference is that the Fed is in a test system about the amount of information is desired

Penetration is in two ways (Black Box and White Box. In Black Box from the perspective of a hacker who is located outside of the network and does not have any information about the network configuration and the server, the network and server can be attacked. In White Box from the perspective of a hacker who is located inside of the network and have information about the network structure and server, the network and the server has to be attacked and tried to increase access. In the meantime, there are some other methods that they provide only part of the information on a tester that is known as (Gray-box). Penetration testing is typically done periodically to new security problems are resolved. With white box testing performed, the system can be accurate and to be more testing, meanwhile with black box testing, all the holes in the system may not get the test. So in the event that security plays a key role and is sensitive, it is necessary that the white-box testing is done.

2.2. Steps of Penetration Testing

Percolation test process can be divided into four stages.

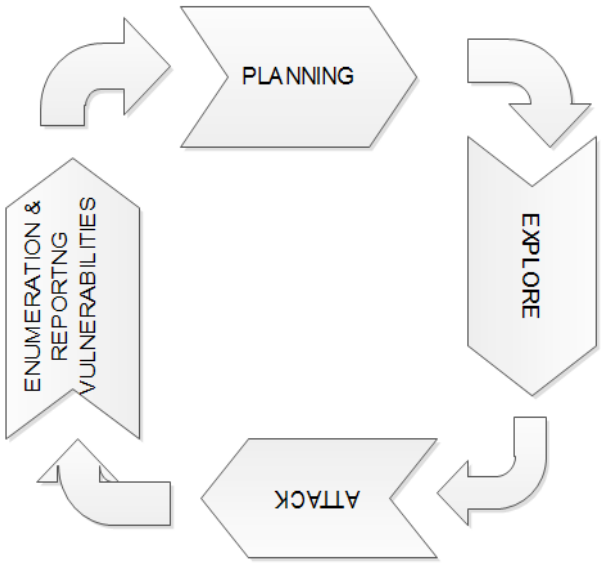

Figure 2: Deming Cycle Implementation in Penetration Testing

The first phase is the planning phase that usually involves specifying the steps to reach the goal the test starts with the discovery process. The purpose of this stage is comparison of the program on a attack with a standard database that is known as the vulnerable database and have specific information about the different types of attack. At the end of this phase, the log files are produce and are kept in the system.

The third step of the process is the attack with the responsibility of the attack on the system.

The attacks are done on vulnerability has been found in the discovery stage.

The results obtained from the attack phase, in the fourth stage meaning the stage of collecting and reporting is offered in the fourth stage.

The final report must contain the found vulnerabilities, attack and analyzing the log files.

2.3. The Advantages of Penetration Testing

The following list shows the main benefits of penetration testing

- The appropriate risk management
- Increased business continuity
- To minimize attacks
- Protection of customers, commercial partners and third parties
- Having the security of being in accordance with the regulations or certification
- Supply investment evaluation
- Protection of public relations and brand issues
- Other benefits of penetration testing performed on the tools or organizations can be pointed to the following as well.
  - ✓ Find security holes in the used systems: before others will discover this holes.
  - ✓ Analyze network security from the perspective of expensive access: apparent weakness in penetration testing, are covered to avoid expensive access and influence by it.
  - ✓ Report to the managers of the Organization: Group IT security in your organization has enough familiarity to the weaknesses of the system and penetration testing can announce the weaknesses in the form of reports to the senior management of the organization to speed security organization decisions.
  - ✓ Employees ' cultural vulnerability assessment with techniques of social engineering
  - ✓ Reducing the cost of the restoration, by reducing the risk of penetration of the invaders.

2.4. Automated Penetration Testing – Automatic

In fact, penetration testing is to test security and reliability of a system; it can be done manually or automatically.

Manual penetration testing is a test of the system that is done manually and stages by stages and requires an experienced and skilled group that knowing attacks of influence of expensive and organizations' systems.that by relying on skill and experience must be able to penetrate the system problems during the test and identified the holes and deal to offer solution and strategy.this means that manual penetration testing requires much time and a group of experienced and skilled team, and these reasons are a lot of costs.

In contrary mechanized testing can be automated and the system automatically scanning and routing problem, identify attacks and ways to cope and provide secure system.

Due to the lack of need for additional and skilled and experienced manpower, has low cost and less time than manual penetration testing also penetration testing can be used in multiple agencies and continuous in terms of performance and accuracy improve and this will often identify holes and attacks and ways to cope and security solutions to provide automatically and accurately. And as a ready package it can be used in different organization that this will reduce the cost and time of this test impressively. Nowadays most of the automated penetration testing packages are used because of low-cost and time consuming.

2.5. Penetration Testing In Operating System Layer

Penetration testing in operating system includes a complete test of the operating system used in the structure of the Organization, including the setup network on the operating system. At the beginning various security settings of the service will be evaluated, and then the various vulnerability scanning on this stage can be tested exactly.

In the next step the focus is on the operating system and its core.

A study of the patch will be installed on the systems security and efficient are done to prevent the operating system with some vulnerability that is available in the operating system.

2.6. Penetration Testing in User Layer

In the penetration testing of the user area security testing the most new vulnerability area of users and the Website operators will be tested to test that to what extent is the amount of managers' vulnerability and attacks against the user support team. As we know many attacks to great links to Web and even data centers by some method that it can be called social engineering, but this method is beyond words.

Many of the Influence of the operator by sending a letter of support to the management team or the contaminated sites action has to infect users ' systems and it's through attempting to install all kinds of Trojans and Klagers and then easily extract passwords and enter site.

This vulnerability can be found on the office software or IE Internet monitor and etc and they need to be in the exact control of security.

2.7. Network Penetration Testing

Network penetration testing is a simulated attack to review all systems and existing viruses on the network and server security in terms of

penetration test and review. Due to the direct relation of network security with other securities, including electronic payment is required to being test at the time of the successive network security because today the networks are faced with an influence of expensive that cause network security threats arise.

And in the event of a lack of security in networks security in electronic banking and electronic payments and databases, etc. security threat arise.

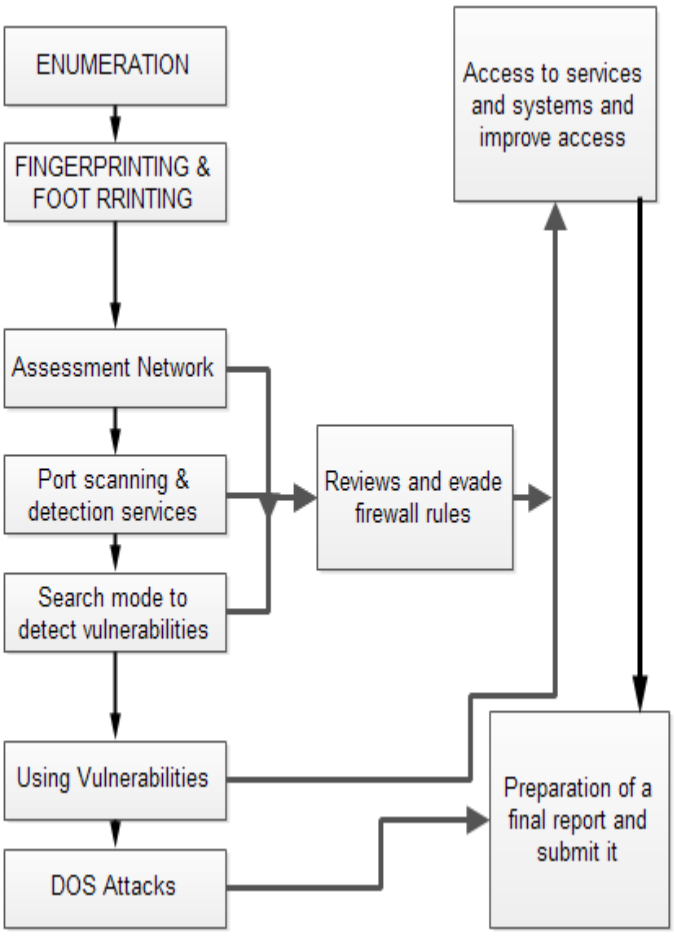

Figure 3: Network Penetration Testing Flowchart

3. Penetration Testing Web Applications

Many of the electronic services such as e-payments on the Internet using Web-based software and the security of this software have much importance.

Web application penetration testing is a collection of procedures that are related to security bugs related to Web programs .Since the vulnerability in Web-based software is different with the vulnerability of other soft wares, there are particular of procedures for penetration testing security testing Web based software and Web Service. To perform penetration testing on Web, it is necessary to use scanners to scan the target and identify gaps and vulnerabilities. *There are drawbacks associated with web* scanner are incorrectly stated that a code has a bug that needs to be tested and it took a lot of testing to find vulnerabilities that actually affected the header that does not exist.

Another problem is that due to used poor scanners crawling algorithm, we can have access to all parts of the target and therefore may not be able to detect all the vulnerabilities of the target Some of these tools has been scanned and are available as open source Such as IBM and AUNETIX WVS and WEBINSPECT APPSCAN and POWERFUZZER and ZAP AND IRON WASP and W3AF and the tools to identify and fix these bugs are helpful. Our attempt is to introduce these tools.

3.1. Web Application Security Scanner

Is a program that through a final software in order to identify potential Web application vulnerabilities and weaknesses of the software architecture to communicate with it. This is a black-box test runs. Unlike source code scanners, web applications scanners don't have access to the source code and therefore detect vulnerability are identified by attacks. Web applications since 2000 has been very popular because they allow users to experience the Internet's interactive

Only instead of static web pages, allows users to create individual accounts, add content, query the database and provides complete transactions. In the process of providing an interactive experience of Web applications, often the collection, storage and use of sensitive personal data take place for delivery to the service. Users can benefit from the ease of use of the software, while personal information stored in web applications are at the risk of falls through hacker attacks, insider leaks and etc. compromised.According to the Privacy Rights, more than 18 million customer records in 2012 have been compromised due to insufficient security controls in the data big companies and web applications.

3.2. Applied Scanners OWASP Zed Attack Proxy –ZAP

OWASP's program or "Freedom Project Web application security" is a global nonprofit organization that focuses on security in web applications. Zed Attack Proxy is an open source tool for integration and test in order to find vulnerable spots.

The program includes an automated monitor with the tools to find vulnerabilities manually The zap has an automatic scanner that uses a set of tools possible to find out possible security vulnerabilities manually. This tool is easy to install and supports more than 20 languages.

3.3. Web Application Attack and Audit

3.3.1. Framework (W3AF)

W3af is a framework for testing web applications.The project aims to build a framework for finding and removing the vulnerable web applications that are easy to use and extend.

w3af is working to make the best of open source software in their work.

W3AF is an open source tool and by modify the code and identifying new vulnerabilities can be the upgrade the tool.

3.3.2. Skipfish Web Vulnerability Scanner: Tool

Skipfish is an automated tool for security in web applications, to find vulnerabilities in web sites before a hacker find it. The way it works is that by moving back and enjoy PROB map find the target site and by obtained map by using the corresponding output is interpreted and vulnerabilities are reported.

3.3.3. Nikto-Vulnerability Scanner : Nikto

It is one of the best open source tools to monitor vulnerabilities which are available in the most popular Linux distributions such as Bktrk, Gnacktrack, Backbox and etc.

Further it can be used in other distributions such as Linux and Windows because It only needs perl script.

3.3.4. Netsparker Web: Application Security Scanner

Netsparke is a commercial tool for finding vulnerabilities in web applications design. Netparker free version is also available that can be used for rapid penetration testing.

3.3.5. Websecurify- Website Security Testing Tool

Websecurify tool can run on Linux OS, Windows and Mac. Websecurify is the best tool for finding popular vulnerabilities in web that may cause serious harm to the programs.

4. Conclusions

In this article we explored and introduced network penetration testing and web pages that electronic payment through them is done.

As a human immune system, prevention is better than cure and electronic payment systems are based on the same thing the difference is that prevention in an electronic payment system is penetration testing and finding holes and vulnerabilities before malicious hackers could achieve.

Penetration testing includes tools and methodologies which stated in brief and for thorough penetration test we require the right tools, and it would be dealt with at successive time.

References

[1] G.A. Di lucca and a.r. fasolino, "Testing Web-Based Applications: The State of the Art and Future Trends" , (2006), Elsevier information and Software technology, vol 48, pp. 1172-1186.

[2] Kumar , R, "Mitigating the Authentication Vulnerabilities in Web Applications Through Security Requirements ", (2011), information and communication technologies (WICT) , 1294 – 1298 .

[3] www.wikipedia/org, [Accessed on December, 2012]

[4] http://www.c2networksecurity.com/pentesting.htmll, [Accessed on June 2014].

[5] http://www.secforce.com/blog/2011/02/benefits-of-penetration-testing, [Accessed on January, 2011]

[6] Samant, n.(2011), "Automated Penetration Testing" (doctoral dissertation, San jose state university)

[7] Doupe , A.,Cova , M.,&Vigna, G. (2012). " Whe Johnny Can' T Penest: An Analysis Of Black-Box Web Vulnerability Scanners.In Detection Assessment", pp.111-131, Springer Berlin Heidelberg

Larry Suto. Analyzing the Accuracy and Time Costs of Web Application Security Scanners Available: http://ha.ckers.org/files/Accuracy-and- Time-Costs-of-Web-App-Scanners.pdf [Accessed Jun 2014]

[8] Www.Owasp.Org/Index.Php/Owasp_Zed_Attack_Proxy_Project, [Accessed on Jul 17, 2014].

