Web Security Vulnerability Analysis of Ethiopian Government Offices

Tliahun Ejigu Belay

M.Sc, Admas University (Department of Computer Science), Addis Ababa, Ethiopia

Abstract

This research focused on detailed analysis of Ethiopian governmental office server side and client side "Web Security Vulnerability Analysis of Ethiopian Government Offices". The purpose of this assessment is to discover weak links (vulnerabilities) and provide recommendations and guidelines to vulnerable entities found in its web application. however, choose to qualitatively assess impact and probability explicitly. For each term has been assign high, medium, or low vulnerability. A simple matrix is developed to estimate overall exposure. Vulnerability analysis is a series of activities undertaken to identify the weaknesses and holes to exploit security vulnerabilities. It helps to confirm the effectiveness of the security measures that have been analyzed. The methodology of vulnerability analysis includes three phases: test preparation, conducting test and test result analysis. Each of them involves a series of further steps and tasks. This report further illustrates how to apply this methodology to conduct vulnerability analysis on ten (10) sample governmental office web applications, finally the result of the research shows all the possible number of Vulnerabilities rate and system weakness perspective attack of governmental office network asset vulnerability analysis finding results of both approaches based on Vulnerability impact rate or risk level and system technology weakness or attack perspective by using black box testing.

Keywords: Vulnerability Analysis; Security Testing, Vulnerability Assessment; Penetration Testing, Web Application Penetration Testing.

1. Introduction

Network security is a growing field of concern for Ethiopian governmental offices and agencies. Information technology Security can protect a network by testing the network for potential threats, and continuous defense against malicious attacks. Network threats in today's age, are forever changing. Hackers with malicious intent are continually attempting to infiltrate networks to steal information cyber security now in the world dynamic change.

The significant of security analysis today's connected device pose challenge for cyber security professional uses computer network to access and store information its needs understand more security challenges and security analysis.in Ethiopian most governmental office From the security point of view a hardware system like PC, software and network infrastructure Weakness in the design or implementation of an information system (including the security procedures and security controls associated with the system) because the researcher have been observed from INSA'S annual auditing and evaluation report from 20

governmental office auditing serve 15 of governmental office vulnerable in case of weak information system.so they should be implementing effective cyber security measurement particularity challenge today because there are more device than people and attackers are becoming more innovation and connected internet that is the era of internet of things, so after vulnerability analysis the research has been done to understand and recommended the best practices, standard and bench marks of vulnerability tools.

In Vulnerability Assessment and Penetration Testing Methodology Overview including the main steps of vulnerability analysis those are. Discovery: The penetrator performs information discovery via a wide range of techniques, Enumeration: the specific networks and systems are identified through discovery, Vulnerability Identification: The vulnerability identification step is a very important phase in penetration testing. This allows the user to determine the weaknesses of the target system and where to launch the attacks. And Exploitation and launching of attacks: After the vulnerabilities are identified on the target system [1].Vulnerability assessment tools generally work by attempting to automate scan a "footprint" analysis to determine what network services and software programs. In Information System Security Framework and Vulnerability Assessment for Ethiopian governmental office using Kali Linux has been used for penetration testing tools like OWASP Zed Attack Proxy (ZAP) for vulnerability scanning in security weaknesses [2]; however after evaluating this research has been recommend the best counter measure to the existing vulnerability considering internal and external system.

2. Related Work

Detecting Security Vulnerabilities in Web Applications Using Dynamic Analysis with Penetration Testing

Authors: Andrey Petukhov

The number of reported web application vulnerabilities is increasing dramatically. The most of vulnerabilities result from improper input validation. This paper presents extensions to the Tainted Mode model which allows intermodule vulnerabilities detection. Besides, this paper presents a new approach to vulnerability analysis which incorporates advantages of penetration testing and dynamic analysis. This approach effectively utilizes the extended Tainted Mode model.

Web Applications Security and Vulnerability Analysis Financial Web Applications Security Audit – A Case Study

Authors: Tiago Vieira

Information security can no longer be neglected in any area. It is a concern to everyone and every organization. This is particularly important in the finance sector, not only because the financial amounts involved but also clients and organization's private and sensitive information. As a way to test security in infrastructures, networks, deployed web applications and many other assets, organizations have been performing penetration testing which simulates an attacker's behavior in a controlled environment in order to identify its vulnerabilities. This article focus on the analysis of the results of security audits conducted on several financial web applications from one institution with aid of automatic tools in order

to assess their web applications security level. To help in security matters, many organizations build security frameworks for vulnerability assessment, security assessment, threat modeling, penetration testing, risk management and many more. As for penetration testing, organizations such as OWASP provide vulnerability and security information, a testing methodology, risk analysis and penetration testing tools.

Web vulnerability analysis and implementation

Authors: E B Setiawan

Data security on the internet is synonymous with a website and a computer network that connects to one another. In the context of computer networks, any existing data on a computer that is connected to another computer, is unsafe, so need to do some way to secure the data so that cannot be accessed by another computer. Each website is created using a series of codes to be able to display data that is public and accessible or accessible to everyone. However, usually on the server computer where the website is stored, there are also data that are confidential or private, so it is not allowed to be accessed by the public. This research is conducted to analyze various techniques and ways of attack that usually done on the internet website, in order to implement various ways of handling so that the existing website can be more secure against the attack so that the data contained in the server. The results have been obtained that is known some weaknesses and attacks that occur on a website. This research used htaccess technique and website script for security improvement. But, the improvements that have been done still cannot guarantee the website 100% safe, it is because that in the world of data security in addition to the web and server side is fixed, must also be viewed from the network security.

3. Existing System

The EU Cyber Security Strategy provides a policy framework for EU initiatives. But in Ethiopia government's doesn't exit nether policy or auditing service .In addition Vulnerability analysis use to computers, networks or applications for known weaknesses. In plain words, these scanners are used to discover the weaknesses of a given system. They are utilized in the identification and detection of vulnerabilities arising from within a network-based asset such as a firewall, router, web server, application server. Because security vulnerability analysis use are numerous, industry frameworks and best practice guidance typically include vulnerability assessments in their list of suggested measures Simply, a governmental organization cannot fully understand the security flaws, overall risk, and assets that are vulnerable to cyber security breaches. To stay understand and to counter surprise attacks, a thorough vulnerability analysis help to fix the unattended security issues.

Disadvantages of existing system:

- Security flaws
- Unattended security issues.

4. Proposed System

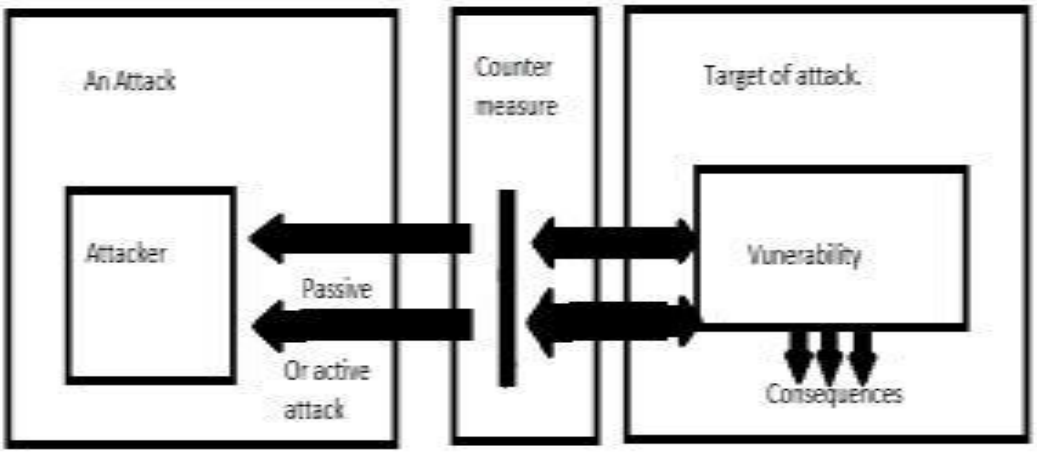
In this research has been used dynamic technique of vulnerability analysis strategy because there differ standard in differ serve now mainly the research has been selected Information Systems Security Assessment Framework (ISAAF), The Open Source Security and Testing Methodology Manual (OSSTMM). And Application Penetration Testing and Ethical Hacking (APTEH) published by (System Admin, Audit, Network and Security) SANS Security company is the another methodology that we used. The main objective of this thesis to understand the governmental office web security analysis used different vulnerability scanner tools discover the security weakness within impact rate and put possible recommendation and countermeasures.

Advantages of proposed system:

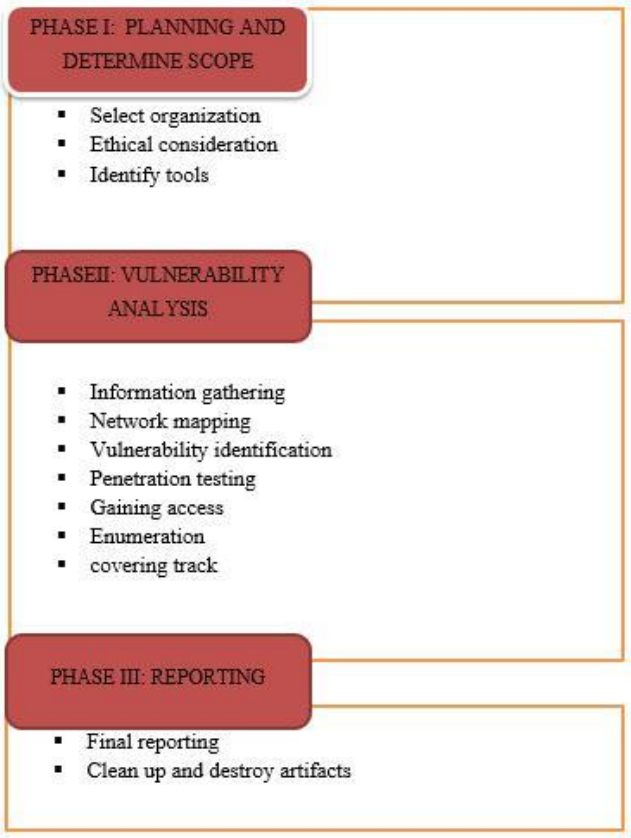
- Confirm the effectiveness of the security measures.
- Identify the weaknesses and holes to exploit security vulnerabilities.

5. System Architecture

Fig.1: System Architecture



Phases:



6. Risk Calculation

The discovered of vulnerabilities analysis had been classified in two based on vulnerability impact rate or risk level and system technology weakness or attack vulnerable that covers compromise Confidentiality, Integrity and Availability (CIA) on services and applications over the website. The following chart shows the number of Vulnerabilities rate and system weakness.

Fig.2: Impact rate or risk level

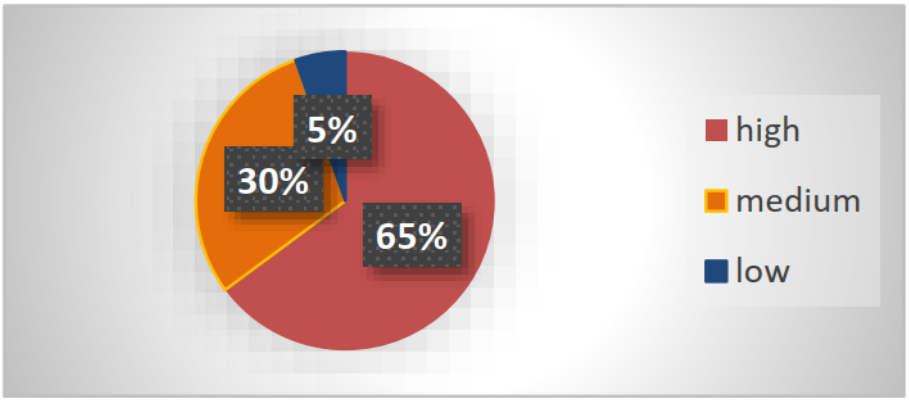
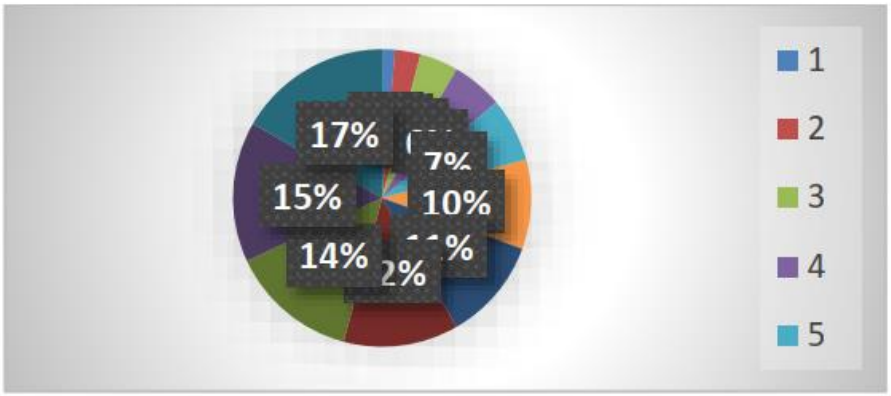


Fig.3: Website vulnerability based on system technology weakness



7. Conclusion

In this Chapter, the conclusion and the recommendations for future works of this research is given The Chapter is organized in two sections. The conclusion of the research and the recommendations for future works are presented. Vulnerability analysis is a comprehensive method to identify the Penetration testing in a system. It offers benefits such as prevention of financial loss; compliance to industry regulators, customers and shareholders; preserving corporate image; proactive elimination of identified risks before damage. The research has been chosen black box penetration testing, depending on the specific objectives to be achieved. The security of a website vulnerability analysis adapting any pen-test methodology does not necessarily provide a complete picture of the vulnerability analysis process, which execute pen-test methodology.

8. Future Work

As summary of recommendation the vulnerability should be fixed as soon as possible especially the high vulnerability. And the application uses third party frameworks and libraries that should have to be updated and patched on the regular basis, but currently, the websites which has multiple types of vulnerabilities. In this research has been done only focused on the some governmental office website target network asset, the other office network infrastructure is needs to be vulnerability analysis for the future work.

References

[1] Ankita Gupta Anamika Saini, "Blue Eyes Technology," International Journal of Engineering Research and General Science, vol. 4, no. Issue 1, January-February, 2016 , p. 549, , 2016.

[2] Haftom Gebreziagbher, "Information System Security Framework and Vulnerability Assessment for Ethiopian Higher Educational," International Journal of Information Technology, vol. Volume 2, Issue 12, no. ISSN (2413-2950) –, pp. 16-17, December 31, 2018.

[3] Sanjay Goel1, "Managing Information Security: Demystifying the Audit Process for Security Officers," in Managing Information Security: Demystifying the Audit Process for Security Officers, Washington University at Albany, SUNY, 2002, p. 3.

[4] SURESH KUMAR, "Ethical Hacking and Penetration Testing Strategies," International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE), vol. Volume 11 Issue 2 , no. ISSN: 0976-1353, p. 22, NOVEMBER 2014.

[5] By S. Anantha Sayana, "Approach to Auditing Network Security," Information Systems Audit and Control Association, vol. V OLUME 5, p. 2, 2003.

[6] b,*, BM Mehtre Jai Narayan Goela, "Vulnerability Assessment & Penetration Testing as a Cyber Defence," in 3rd International Conference on Recent Trends in Computing 2015 (ICRTC-2015) , School of Computer and Information Sciences, University of Hyderabad, Hyderabad 500046, India, Procedia Computer Science 57 (2015).

[7] Kirandeep Kaur Kavita, "ulnerability Assessment and Penetration Testing," nternational Journal of Engineering Trends and Technology, vol. Volume4, no. Issue3, 2013.

[8] Chandresh Parekh Nidhi Vora*1, "Vulnerability Assessment and Penetration Testing in Web," International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. Volume 2, no. Issue 6 | , pp. 731-735, 2017 IJSRCSEIT.

[9] SensePost (Pty), "Security Assessment Methodologies," South, 1999/004700/07.

[10] Jai Narayan, "Vulnerability Assessment and Penetration Testing in Web," International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 2, no. 6, p. 734, 2017.