Volume 2, Issue 5, May 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Comprehensive Study on Risk, Threat & vulnerability in an Operating System and Online Application Software

Afreen Chowdhury
Department Of CSE
Stamford University, Bangladesh

Nilufa Yesmin
Department Of CSE
Stamford University, Bangladesh

Mr. Taslim Taher
Department of CSE
Stamford University, Bangladesh

Abstract----- This research paper is particularly developed for knowing about the security risk of the system or application software. The main purpose is to find out how risky an operating system or software of the users to be used. There are two software named risky Project Professional and winvulscan used to do these works. As a result one can know details about the risk of a program. For this way a user can understand about the insecurity to use an operating system or software.

Keywords ----- Operating system/online application software, vulnerability, threat, risk, probability.

I. INTRODUCTION

A security system is one of the master interests to the every software developers but not to the customers. Clients whose always expect to have good software so it is very important to know that the software or operating system is safe or not. For this issue the security terms such as software risk, OS or operating system risk, their vulnerability, threats, probability, impact has been discussed. These all are related concepts and need to be clarified first. Thereafter utilize their availability in various kinds of operating system and online software. At the end, display the results at percentage for security in the system by which users find out the risk of the system approximately.

II. IDENTIFICATION AND ANALYZATION

To discover the vulnerability of the system refers to find out the security risk of those systems because vulnerability is also known as a security risk. For detecting vulnerability we used software named "winvulscan". It has checked the system and find out the vulnerabilities. This software also discovers the security bulletin and rated them in various impacts. Threat detection depends on the security risk. A vulnerability in an operating system or an application software for an attack on what step to take action, it has been understood by the threat of. Spoofing is one of t he serious attack by which an attacker gains access to the certificate used by the end user for authentication. On the other hand, risk is identified by detecting the threat and vulnerability [2]. Probability and impact help to identify the level of risk in the system [5]. There are different levels of probability. Such as, very low, low, medium, high and very high [1] where the impact level refers negligible, minor, moderate, serious or important and critical. The probability of it occurring can range anywhere from just above 0% to just below 100%. Color combinations also indicate the level of risk [6].

Risk score is a calculated parameter that equals probability multiplied by impact where impact also indicates the percentage of loss [3]. In an operating system or application software, it is the total dominance of a successful attack. These score refers the total risk factor that also presents as a percentage of exposure [3].

TABLE I. Stratum of Risk Rating

Probability rating	Probability labels	Impact rating	Impact labels
0% to 20%	Very low	< 1 month delay	Negligible
20% to 40%	Low	1 to 3 months delay	Minor
40% to 60%	Medium	3 to 6 months delay	Moderate
60% to 80%	High	6 to 12 months delay	Serious or Important
80% to 100%	Very high	> 1 year delay	Critical

Risk score is a calculated parameter that equals probability multiplied by impact where impact also indicates the percentage of loss [3]. In an operating system or application software, it is the total dominance of a successful attack. These score refers the total risk factor that also presents as a percentage of exposure [3].

TABLE II. Total Risk Factor

Very Low	Low	Medium	High	Very High
1 to 30	31 to 60	61 to 57	57 to 175	≥ 175

After considering everything, come to the main point which is called finalization. In a system, after finding the risk impact, probability and score, a basic understanding of the system can found in. If the risks score of 1 to 30, then the system regarded as very low risk, if the risks score of 31 to 60 then the system regards as low risk, if the risks score of 61 to 57, then the system regarded as medium risk, if the risks score of 57 to 175 then the system regards as high risk and if

the risks score more than 175, then the system regarded as high risk [3]. Now take a final decision to finalize that how much risky an operating system and an application software.

III. APPLYING THE ABOVE METHODS ON WINDOWS 7 AND MARKET ANALYSIS SYSTEM SOFTWARE

TABLE III. Windows 7 [7]

Vulnerability	Threat	Risk	Probability	Impact	Score
Specially crafted office file or web page can be viewed	Attacker could take complete control of an affected system	Loss of availability; Malfunctioning	13.0%	90.0%	11.7%
Host application opens in an application run time	When a user is logged on with administrative user rights, an Attacker could take complete control of an affected system	Information disclosure; Desktop Malfunctioning	25.0%	90.0%	22.5%
User opens a specially crafted excel file	Attacker could take complete control of an affected system	Loss of availability; Malfunctioning	9.5%	70.0%	6.6%
User opens a specially crafted excel file	Attacker could gain the same user rights as the local user	Malfunctioning	30.0%	90%	27.0%
User opens a specially crafted publisher file	Attacker could gain the same user rights as the local user	Malfunctioning	91.0%	90.0%	81.9%
Opened an attachment in an e-mail crafted message	Attacker could gain the same user rights as the local user	Malfunctioning	35.0%	70.0%	24.5%
A user opens a specially crafted power point file	Attacker could take complete control of an affected system	Loss of availability; Malfunctioning	35.5%	90.0%	31.5%
Windows Messenger active on the desktop	Most anti–virus software don't scan the Windows messenger messages or files thus can be exploited by hackers to launch DOS or malware infection attacks	Loss of availability ; Information disclosure	10.0%	70.0%	7.0%

A. Results

In the above table, the summation of overall risk is 212.7. So the total risk score will be 26.5875. That means there is very low risk specified in this operating system. Countermeasure implementation will enhance security, but is of less urgency to repair.

TABLE IV. Market Analysis System Software [4]

Vulnerability	Threat	Risk	Probability	Impact	Score
Buffer overrun	Attackers takes advantage of a program that is waiting on a user's input	Malfunctioning	25.0%	30.0 %	7.5 %
Cash overflow	Remote attacker will repeatedly crash servers until the victim deposits funds to an international bank account	Unauthorized access; Malfunctioning	65.0%	70.0 %	45.5 %
Cross site scripting	Attacker steal authentication information	Malfunctioning; Information leak	12.0%	10.0 %	1.2 %
Elevated privileges	An attacker may able to exploit this assumption so that unauthorized code is run	Information leakage	2.0%	90.0 %	1.8 %
Weak Authentication	An attacker can sniff the traffic to discover user's authentication and authorization credentials	Unauthorized access; Loss or disclosure of information.	80.0%	90.0 %	72.0 %
Information leakage	Unauthorized parties gain access to sensitive data	Unauthorized access; Loss or disclosure of information; Malfunctioning	90.0%	70.0 %	63.0 %
Password hacking	Attacker could take complete control of an entire system	Unauthorized access; Information leakage; Malware/worm infection	10.0%	90.0 %	9.0 %
Internal fraud	Attacker may take advantage to access the system	Information loss	12.4%	70.0 %	8.7 %

B. Results

In the above table, the summation of overall risk is 208.7. So the total risk score will be 26.0875. That means there is very low risk specified in this application software. Countermeasure implementation will enhance security, but is of less urgency to repair.

IV. CONCLUSIONS

Users of different types of operating systems and application software are used. When using these types of systems or programs may face some problem called vulnerability. Through this vulnerability, it is possible that an attacker very easily to do on the computer system can handle called Threat. These types of threats attack damage to the computer of a program or system called risk. These three elements mainly create computer risk. By this process user can approximately find out the computer risk and take necessary steps against these risks.

REFERENCES

[1] *Basic Risk Management Guide, [Online]. Available.*

[2] Steve Elky. *An Introduction to Information System Risk Management.* SANS Institute InfoSec Reading Room. May 31, 2006.

[3] *FEMA. Risk Assessment / Risk Management Guide.* 22 February 2012.

[4] Lawrence Allhands. *Network Security Threat Matrix.* May 2004.

[5] Dr. James McCaffrey. *MSDN Magazine. Analyzing Project Exposure And Risk Using PERI,* January 2009.

[6] Nancy A. Renfroe PSP and Joseph L. Smith, PSP. *Threat / Vulnerability Assessments and Risk Analysis.* Last updated: 19

[7] COTS Security Guidance (CSG—10/ S) – *Summary Of Overview* Of Operating System Security Features. Published date: August 2009.

