Vulnerability Evaluation Based on CVSS and Environmental Information Statistics

Shuguang Wang, Chunhe Xia, Jinghua Gao, Qiong Jia
Beijing Key Laboratory of Network Technology
School of Computer Science, Beihang University
Beijing, China
shuguang.wang1990@gmail.com, xch@buaa.edu.cn, jhgao09@gmail.com, jq_buaa@163.com

***Abstract*— In the field of network security, vulnerability evaluation is a very important method to assess the attack and defense means in many practical use, such as penetration testing and safety pre-warning. Up to now, there are a lot of vulnerability evaluate methods, such as CWE, CVSS, and there are a lot of basic evaluate methods for further improvement and optimization. This paper analyzes the existing vulnerability evaluate method and has found some insufficient changes in real-time environmental. This paper adds some new elements including topology environment factors, as well as log system information statistics, to make sure vulnerability evaluation can be used in a more flexible network security.**

Keywords—vulnerability evaluation; network security; CVSS; Environment statistics

I. INTRODUCTION

Vulnerability evaluation is an important method to assess the damage of different vulnerability to the network security. In the case of certain statistical indicators of vulnerability analysis, to make a quantitative or qualitative judgment to the threat of vulnerabilities, finally it's applied to some aspects of network security. [1, 2]There are some common vulnerability evaluation methods.

Common Vulnerability Scoring System (CVSS) [3] is the most common vulnerability evaluation. The threat score generated by CVSS is mainly divided into three aspects, basic score, temporal score and environment score. The base score mainly evaluates the inherent characteristic of the vulnerability itself, as well as its impact, temporal score makes quantitative analysis of factors which lead the threat level to change by time, and environmental score mainly evaluates the factors that users change the environment. The granularity of environmental factors may be rough.[4]

Vulnerability Evaluation can be based on Analytic Hierarchy Process(AHP), three layers evaluation structures consist of attribute layer, affect layer and asset layer. Use AHP to solve indicators quantify problem. Weight calculation is mainly achieved by judgment matrix, the result of vulnerability assessment is achieved by experts.[5]

Currently the method of vulnerability evaluation has a wide variety. Most of the evaluation methods put their focus on basic indicators of the processing vulnerabilities instead of specific use of environmental factors, although there is a considerable number of vulnerability evaluation methods, they are not very good at directing different networks. Our method extends the information from the host and some log system, so the vulnerability evaluation can give often more fixed, sensitive result to the actual risk evaluation which can avoid inconvenience.

On the other hand, the judgment in penetration testing work is often associate with the working environment. By improving CVSS environmental attributes, and combined its basic score with the actual topology of the environment elements information, finally we can be able to give a dynamic quantitative evaluation of the vulnerability topologies environment correspondingly. We use the current topology information environment, NVD's Common Weakness Enumeration to give the threat of each vulnerability Category classification for the current environment.

The rest of the structure of the paper is organized as follows: The second part introduces the related work and the method description, the third part and the fourth part presents the experiment with analysis and conclusion.

II. METHOD DESCRIPTION

This paper uses the NVD vulnerability classification and collects the log in the network environment. By the known cases, gather the vulnerability of the host and its mark in it, then form it to be atomic information, and through a careful evaluation of atomic information on vulnerabilities also some other component, the model is divided into three parts: the first one is the basic CVSS score (data from NVD) and the CWE; the second parts is Environmental factors which is gathered from the host network and process by some pattern match algorithm; the last part of it is impact matrix which means the contribution degree of each atomic information.

A. Processing the CVSS Basic Score

CVSS score consists of the base score, temporal score and the environment score. We select CVSS inherent parameters affecting as our base for vulnerability evaluation. The inherent attribute will not change with the time and environment. This paper can use it to ensure the accuracy of experimental result.

The formula of the basic score

$$V_{basic} = RoundUp(Min[(V_{impact} + V_{explit}),10]) \quad (1)$$

The V_{impact} and $V_{exploit}$ is the impact and exploitability sub score of CVSS.

This paper calculates the severity score of each category S_{ci} .

$$S_{ci} = w_1 S_{PU(Ci)} + w_2 S_{PA(Ci)} \quad (2)$$

The w_1 and w_2 is the weight of the risk level, the $S_{PU(Ci)}$ is the severity metric for patches not available, and the $S_{PA(Ci)}$ can show the severity matric which is available. The formula of the two parameters is summarized below[5]

$$S_{PU(Ci)} = \frac{\sum_{j=1}^{n} V_{basic}}{\sum_{i=1}^{n} V_{PU(Ci)}} \quad (3)$$

$$S_{PA(Ci)} = \frac{\sum_{i=1}^{n} V_{basic} * e^{-\beta Age(vk)}}{\sum_{i=1}^{n} V_{PA(Ci)}} \quad (4)$$

The parameter n is the number of vulnerabilities, e improves it with CVSS basic score so we could process with more parameters below, and the $V_{PU(Ci)}$ is the score that means the patches which is not available. $V_{PA(Ci)}$ is the available vulnerabilities scores.

B. Environmental Factors

In order to get better environment network topology description, we use a 7-tuple to store useful information. The 7-tuple is $t = \{A, S, M, U, C, T, H\}$

A is the authorization information, its description is below

$$AuthInfo ::= \{ipaddress, subnet, number, errornum\} \quad (5)$$

The authentication information has 5 elements, the IP address, the subnet of it, the total authentication number, and the suspicious login behavior.

S, the SQL information which is separated out as a factor, because SQL is a main target of vulnerabilities attack, the impact on the database is often a tendency to represent the attack suffered by the current topology. The SQL info is

$$SOLInfo ::= \{Database, time, InjectionAction\} \quad (6)$$

Database is the mark of it, and the Injection Action is a storage which stores the Suspicious injection behavior.[6]

M is Memory Information of the server.

$$MemoryInfo ::= \{Memory, overflow\_time\} \quad (7)$$

Overflow time can be the information of the memory exception state.

$$urlInfo ::= \{ipaddress, url, distribute\} \quad (8)$$

The URL information represents the content of U. It describes the distribute situation[7].

C is represent by

$$CronInfo ::= \{id, account, err\_name\} \quad (9)$$

The system finds hidden danger by timed task state, the account can be used when the system describes the active time of the account.

Network traffic(T) is an import basis to determine whether the system is under attack. It is constructed by three element and can represent traffic information.

$$TraficInfo ::= \{Sick\_traific, mount, time\} \quad (10)$$

The Paper uses the detecting system to get the traffic information when the host encounter attack such as DDOS.

H is the data of the host include port, segment and other Necessary data.[8, 9]

C. Impact Matrix

The existing environment may cause harm and the use of traces of several factors, based on the statistics. We refer to these elements and vulnerabilities, establishing correspondence Influence Matrix. For a certain class of vulnerabilities such as buffer error, the statistics under the category of vulnerability can affect more than seven tuples statistics which are obtained. It is necessary to calculate the impact matrix.

To calculate the weight of each element in the tuple with each Vulnerability category, the formula is

$$W_{element} = \frac{\sum_{i=1}^{n} H_i N_{element}}{w_1 S_{PA(Ci)} + w_2 S_{PU(Ci)}} \quad (11)$$

H_i is the harmful data about each message which the information contains. Then the weight of each element of the 7-tuple can be used for the Impact Matrix.[8]

D. Get Threaten List

Here the paper uses statistical methods for vulnerability category which differentiate vulnerabilities. Evaluation of the severity of a single vulnerability is often not representative of the overall situation. And we need to establish a more comprehensive environmental factors. On the other hand, the

statistical category of vulnerability can make prevention become more feasible. According to vulnerability classification study on NVD, it can be summarized as total 34 different categories.

The result of the threaten list is shown below

$$V_h = M_{basic} * M_{mapping} * M_{impact} \quad (12)$$

The M_{basic} is the matrix which contains the processed score of each vulnerability category. The $M_{mapping}$ means that the certain category can influence the element of the 7-tuple.

III. EXPERMENT AND ANALYSIS

A. Topology Information

This part introduces topology environment and the topology of the environment to do some information gathering persistence.

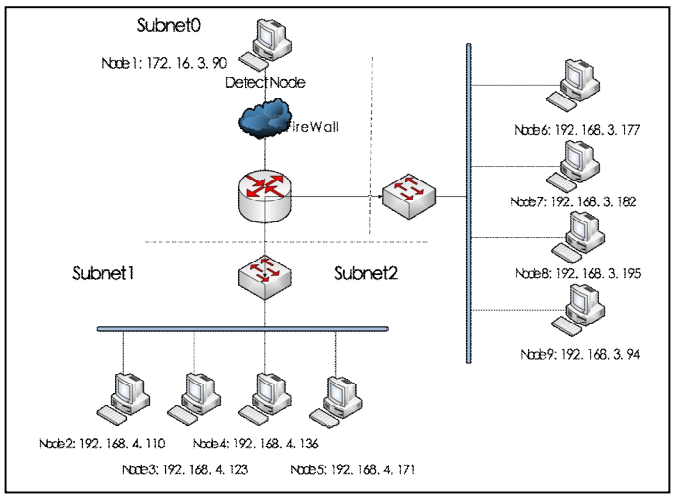

Fig. 1. Experiment environment.

To be tested in the target network, node network penetration testing is implemented. The host name and IP ground table are shown in Table 9 (Based on VSphere).

TABLE I. MESSAGE OF THE SUBNET

Node of Experiment	*Subnet*	*IP*
1	0	172.16.3.90
2	1	192.168.4.110
3	1	192.168.4.123
4	1	192.168.4.136
5	1	192.168.4.171
6	2	192.168.3.177
7	2	192.168.3.182
8	2	192.168.3.195
9	2	192.168.3.94

There are 3 Subnet and 9 terminal in this topological network. We install different services in the computers to make the environment more complex. The services are mainly divided into three kinds: the web server, the SQL server, the self-service server.

B. Analysis the Basic Score of the Weak

To use the formula in Part II, we can get an basic score table.

TABLE II. VALUE OF S(CI)

No.	*Category*	*Weighted Severity Score %Score*
1	Authentication	0.79
2	Buffer Error	13.30
3	Code Injection	0.60
4	Configuration	1.10
5	Credentials Management	0.50
6	CSRF	1.63
7	XSS	6.00
8	Cryptographic Issues	1.20
9	Design Error	1.00
10	Format String	0.33
11	Information Leak/Disclosure	2.95
12	Input Validation	16.50
13	Insufficient Information	21.22
14	Link Following	0.30
15	Numeric Errors	4.00
16	OS Command Injection	0.53
17	Path Traversal	4.12
18	Race Condition	0.55
19	Resource	10.37
20	SQL Injection	6.51

High Score represents the vulnerability that is more High-risk and needs more attention. The information means authentication vulnerability is the most dangerous vulnerabilities based on the CVSS base score.

C. Get the Impact Matrix and Result

The impact is a matrix which calculate by (11), for example the SQL Injection [6]

$$V_{20} = \{0.23, 0.85, 0.12, 0.03, 0.19, 0.57\}$$

Its mapping matrix is

$$M_{mapping\_20}{}^{T} = \{1,1,0,1,0,0,1\}$$

The sorted result is (with top 10 Category)

TABLE III. THE REUSLT

No.	*Category*	*V*
1	Buffer Error	12.17
2	SQL Injection	10.52
3	Authentication	8.63
4	CSRF	7.10
5	XSS	7.03
6	Input Validation	2.32
7	Configuration	0.75
8	OS Command Injection	0.56
9	Information Leak/ Disclosure	0.53

The Buffer Error is now the most threatening vulnerability, and the second is the SQL Injection, it is caused by the host which opens too much port and the SQL database using the old version software. The result is relatively reliable.

IV. CONCLUSION

By improving the CVSS and using the Environmental Information Statics, the paper proposes an improved vulnerability evaluate method which can give dynamic result with different network environment. The result gives threat reference to the penetration testers and has received a very good response. It is the method which can help tester to filter redundant security information.

REFERENCES

[1] Bishop, M., About Penetration Testing. Security & Privacy, IEEE, 2007. 5(6): p. 84-87.J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[2] Duan, B., Y. Zhang and D. Gu, An Easy-to-Deploy Penetration Testing Platform, in Young Computer Scientists, 2008. ICYCS 2008. The 9th International Conference for. 2008, IEEE: Hunan. p. 2314-2318.K. Elissa.

[3] Houmb, S.H. and V.N.L. Franqueira. Estimating ToE Risk Level Using CVSS. in Availability, Reliability and Security, 2009. ARES '09. International Conference on. 2009. Fukuoka.

[4] Mell, P., K. Scarfone and S. Romanosky, Common Vulnerability Scoring System. Security & Privacy, IEEE, 2006. 4(6): p. 85-89.

[5] Fruhwirth, C. and T. Mannisto. Improving CVSS-based vulnerability prioritization and response with context information. in Empirical Software Engineering and Measurement, 2009. ESEM 2009. 3rd International Symposium on. 2009. Lake Buena Vista, FL.

[6] Fonseca, J., M. Vieira and H. Madeira, Testing and Comparing Web Vulnerability Scanning Tools for SQL Injection and XSS Attacks, in Dependable Computing, 2007. PRDC 2007. 13th Pacific Rim International Symposium on. 2007, IEEE: Melbourne, Qld. p. 365-372.

[7] Gallon, L. and J.J. Bascou. Using CVSS in Attack Graphs. in Availability, Reliability and Security (ARES), 2011 Sixth International Conference on. 2011. Vienna.

[8] Fonseca, J., M. Vieira and H. Madeira, Evaluation of Web Security Mechanisms Using Vulnerability & Attack Injection. Dependable and Secure Computing, IEEE Transactions on, 2013. 11(5): p. 440-453.

[9] Antunes, N. and M. Vieira, Evaluating and Improving Penetration Testing in Web Services, in Software Reliability Engineering (ISSRE), 2012 IEEE 23rd International Symposium on. 2012, IEEE: Dallas, TX. p. 201-210.

[10] Tripathi, A.A.S.U., On prioritization of vulnerability categories based on CVSS scores, in Computer Sciences and Convergence Information Technology (ICCIT), 2011 6th International Conference on. 2011. p. 692-69.