ATLANTIS PRESS

Advances in Computer Science Research, volume 80

International Conference on Computer Science, Electronics and Communication Engineering (CSECE 2018)

A Network System Security Assessment Method Based on Penetration Testing

Yue Li[1], Xiaolin Zhao[1,*], Chonghan Zeng[1], Yu Fu[1] and Ning Wang[2]

[1]School of Software, Beijing Institute of Technology, Beijing 100081, China

[2]Academy of Intelligent Collaborative Cloud System, China Aerospace Science and Industry Corporation Limited, Beijing 100081, China

[*]Corresponding author

***Abstract*—As the development of the information technology, people show strong interest to the emergence of all sorts of convenient and new technologies. However, there will be vulnerability in these technologies and bad attackers may be attack it to break it down. So, if we want to protect a system in detail, we must build a network system security assessment standard or method that can evaluate the security of network systems precisely. In recently years we are paying attention to problems of cyberspace security developing badly. Therefore, we attempt to establish the method of network system security evaluation based on penetration test to safeguard the improve of new technologies, the network system can defense the penetration and work well after the bad attacks.**

Keywords—*assessment; network system security; penetration test*

I. INTRODUCTION

This paper standing on the penetration testing will research and analyze the key technologies in network system security evaluation, and design a network system security assessment method based on penetration test. We hope to make some improvements to our current security environment and get an effective system safety assessment method.

The main contents of this paper include:(1)Analyzing the current network system assessment methods.(2)Building a model of network system security assessment based on AHP, and confirm the weight of indication in the evaluation.(3)Designing a network system security assessment method based on penetration test and the coordinate of functions, architecture and models in detail.(4)Proving the effectiveness of this method by evaluate a entity system. From the above, we can weigh the pros and cons to choose the most effective and appropriate evaluation method. After penetration testing, the effectiveness of the evaluation method can be determined.

II. CURRENT SITUATION OF NETWORK SYSTEM SECURITY ASSESSMENT AND TECHNICAL ANALYSIS

A. Current Situation of Network System Security Assessment

Network security assessment is the basic premise and foundation for ensuring information security. Network security assessment is of great significance to information security. But there are less research achievements in our daily research life, and many in foreign have not been open because of the security and privacy. Since the 1990s,the researchers raised the demand of implementing the security classified protection to the information system of computer, and then came up with a series of standard and management specification of it. After that, the awareness of network security began to form and increased it gradually. Nowadays, the main work pay attention to the building of the business architecture, and the standard and technology architecture are still in a researching stage.

B. The Current System Security Assessment Method and Its Shortcomings

As the development of information network systems, there have been raised a series methods of system security assessment. The building of indications, confirm of the weight of indications, the methods of evaluating the results are all the heart technologies. Every methods all have its advantages to address issues, but on the whole, there are all sorts of flows in the table 1 that need to fix. Some methods and some disadvantages of these includes:

TABLE I. COMPARISON

method	defects
a Requirement Engineering-based Evaluation Approach[2]	***It is to note that this article mainly focuses on the derivation of evaluation criteria and not to perform a comparative study. [2].***
An Information Security Evaluation Method Based on Entropy Theory and Improved TOPSIS[3]	***Because the calculated amount of the maximum entropy model is huge, the use of models depend on the quality of the method in a project.***
Information security evaluation of system based on Bayesian network[1]	***Bayesian model needs to refer to available information when assessing a result of test,but these information may be not authoritative and queried by some exerts.So we can not prove the accuracy of result.***

III. THE ADVANTAGE OF PENETRATION TESTING MODEL

If we want to improve the method of network system security assessment, these aspects must be carried out:(1)Improve the technology when assessing a system. For example, some of the methods mentioned above, we must exploit the new technologies for these methods.(2)If we have chose a technology, we need to choose a method of result evaluation what is the most suitable for this technology to increase the effectiveness and

accuracy. According to the contrast described in above section, we have summarized the flows of each method. So, we decide to choose the penetration testing model to test the security of system and improve the security assessment methods to increase the accuracy.

A. The Choose of Assessment Technology

At first, Penetration testing is a simulation of an attack to verify the security of a system or environment to be analyzed. The objective of this test is to examine, under extreme circumstances the behavior of systems, networks, or personnel devices, in order to identify their weaknesses and vulnerabilities[4].

The reason why most network system being attacked is the vulnerability of it. For addressing the problem, we must find bugs by test. But if we want to seek out these bugs, penetration test can perfectly meet the demand. In recently years, the research on penetration test is deepening. In terms of building the standard of penetration test, NIST had raised the process of penetration test in Technical Guide to Information Security Testing and Assessment(NIST SP 800-115) including stages of planning, exploiting, attacking and reporting, and raises a dynamic feedback attack mining process through excavating .Contacting the excavating with attacking through this process adopt perfectly to the penetration test, and finally, through these four stages, we hope to achieve the test results.

PTES (The Penetration Testing Execution Standard)is a new standard that developing in area of penetration technology in security. This standard divides the penetration test process into seven stages: interaction, collecting intelligence, modeling threat, vulnerability analysis, penetration attack, After penetration attack, report. Penetration testing can help security assessment to repair some uncertain weights and parameter very good[10].

All in all, a network system security assessment based on penetration test is critical to protect the network security. From the characteristics of penetration testing, this paper also believes that the system security evaluation should be carried out from within the system. Analyzing the vulnerability of system by penetration test can improve the veracity and security of assessment of system safety.

B. The Choose of Result of Penetration Testing Assessment Method

Evaluation method for an object or event, said in general can be divided into two categories, one is individual evaluation, namely the application of certain criteria for evaluation of some aspect of the object to make quantitative evaluation, its purpose is to reveal the merits of the individual performance index of the evaluation objects. Another kind is a comprehensive evaluation, that is, according to different evaluation purposes, choose corresponding evaluation form, build a mathematical model of converting multiple evaluation factors or indicators to reflect the process of overall quality evaluation objects. Comprehensive evaluation from several aspects to meet the demand of evaluation subject degree of evaluation object quantitative test method, is to be objective, fair and reasonable evaluation object. The comprehensive evaluation method, therefore, the comprehensive evaluation method is also called multiple attribute or multi-attribute evaluation method, which is one of the most effective evaluation method for complex systems.

Now, the common evaluation method includes fuzz comprehensive method, analysis hierarchy process, data envelopment analysis, grey relational analysis and so on. However, every methods all have its advantages and disadvantages. For example: Fuzzy comprehensive evaluation method is applicable to uncertain parameter values ,because network penetration testing results will be affected by the various factors. Otherwise, test results need to review with experts to be more objectively reflect the performance of these indicators. Therefore, the attack test results are uncertain. The fuzzy evaluation can be combined with other evaluation methods, and the fuzzy evaluation method is applicable to the evaluation of network penetration test results. Principal Component Analysis is a classic method of statistics analysis. This method adopt to issue that exist large sample of quantitative indexes. Although it can be used to assess a result of network penetration test, gaining a sample is so hard. So, this method can be used for evaluation under conditions of permit.

Data envelopment analysis needs a large of data when assessing a system. That applies only to quantitative discussion between each unit with the same industry background with the evaluation index, so this method is not adopt to the assessment. Grey relational analysis demands effective information from large data, and this method applies not to the evaluation of results of attack test.

Through the above comparative analysis, the paper choose AHP and fuzz comprehensive analysis to assess the result of network penetration test. Evaluate all levels by fuzz comprehensive analysis.

C. The Choose of Method of Determination of Weight

The methods of determining weights are usually determined by experts grading method, factor analysis weight method, information degree, dependence weight, RSR and AHP.

According to the analysis of 2.2,this paper determines the weight of test indicators by using hierarchical analytic hierarchy process. The reasons are as follows:

The analytic hierarchy process (AHP) was proposed by the famous American operations research scholar Sadie in the 1970s, which is a multi-objective decision analysis method combining qualitative and quantitative analysis. The analytic hierarchy process can be applied to the combination of quantitative and qualitative indicators, and can be used to reduce the complexity of evaluation by its layers' recursion. Therefore, the evaluation of the attack test results is more applicable, but the evaluation itself has greater subjectivity, so it should be corrected when used. The core of this method is to make quantitative analysis of the decision-maker's experience judgment, and provide decision basis in way of quantity for decision makers. As a result, in this paper, the analytic hierarchy process is used to determine the weight of test index system, and the weight of each layer is determined by the method.

IV. COMPUTATIONAL MODEL DESIGN

This section will conduct experimental design based on the improved methods and techniques mentioned in section 2.

A. Confirming the Weight

Weight is the relative importance of indicators relative to the previous level, and the determination of weight is based on the importance of each test index to the test target. Determining the weight of the index to make the importance of each index to form a rational and scientific proportion is an important link in the final scientific evaluation of test results.

The Delphi method is usually used to determine the judgment matrix of each evaluation expert and then synthesize it when we calculate the weight of each layer because experts from different professional backgrounds have different relative importance to different levels of elements.

The procedures of weight determination are as follows:

In the hierarchical substructure of the index system, We set the upper indicators of criterion A to be the criterion of its lower indicators. Weight is the importance of relative to the criterion A, b1, b2, …, bn. For these indicators, We can't directly quantify comparisons in normal condition, and the importance of each other can only be determined by qualitative evaluation. Its specific judgment comparison rule is: for criterion A, What is the importance of the indicator of the subordinate index, we usually ensure it in 1~9 scale. he specific meaning of the scale of 1 ~ 9 scale is shown in the table2 below:

TABLE II. SCALE OF IMPORTANCE SCALE

Scales	Meaning of scale
1	***It is of equal importance to represent two elements.***
3	***The former is slightly more important than the latter.***
5	***The former is obviously more important than the latter.***
7	***The former is more important than the latter.***
9	***The former is very more important than the latter.***
2,4,6,8	***Represents the intermediate value of the above adjacent judgment***
reciprocal	***If the ratio of the importance of element i to j is C_{ij},the ratio of element j to element i is $C_{ij}=1/C_{ij}$.***

Therefore, according to the scale method of the above table,any expert can obtain a comparison judgment matrix C after comparing the underlying indicators of criterion A based on his own views:

$$C = (c_{ij})_{n\times n} \quad (1)$$

Among them, C_{ij} represents proportional scale of importance of bi index relative to bj index.

Step 2: Integrated the judgment matrix

Since each of the experts gives a relative weight ratio matrix of multiple indicators under the same criterion, and in order to get a reasonable weight, the opinions of various experts should be integrated and the judgment matrix given by them should be integrated treatment. In this paper, we adopt the integrative approach to the eigenvector and then the consistency test method to determine the weight. The specific implementation steps are as follows:

a: Establishment of judgment matrix: Assuming that there are n indicators under the same criterion A, there are m experts, and the judgment matrix given by the 9th expert is $C_k = (c_{ij})_{n\ x\ n}$, k=1,2,…,m, At the same time, the judgment matrix given by any expert can satisfy the consistency test.

b: Calculate the average value of the matrix: There are many ways to calculate the mean of the matrix, and we use the geometric mean. Let $C = (c_{ij})_{n\ x\ n}$, .Because there are m experts, there are m judgment matrices. The of the corresponding elements in these matrices defined the value of Cij. According to previous proof, matrix C meets the consistency check.

c: The round numbers of geometric mean: In the last step, the geometric average method was used to find the value of each element of the matrix, but the number of results was more than one, so the results should be rounded.

Step 3: Consistency check of matrix

The consistency test here is mainly to overcome the complexity of things and the differences of people's understanding. When the expert constructs the judgment matrix, the matrix is only constructed from a mathematical point of view, but the non-transitive paradox of the importance of relative weights between indicators is not strictly required. It may appear that "a is more important than b, and b is more important than c, which is more important than a". Therefore, the consistency of the matrix should be tested again. The method is as follows: First, calculate the largest characteristic root λ_{max} of matrix; The matrix consistency index C.I. is also calculated. The formula(2) using is:

$$C.I. = (\lambda_{max} - n)/(n-1) \quad (2)$$

Checked the average random consistency index R.I.of the matrix ,specific reference values are as follows:

TABLE III. THE VALUES OF AVERAGE RANDOM CONSISTENCY INDEX

Order	1	2	3	4	5	6	7	8	9	10	11	12
R.I.	*0.00*	*0.00*	*0.52*	*0.89*	*1.12*	*1.25*	*1.35*	*1.42*	*1.46*	*1.49*	*1.52*	*1.54*

Finally, calculating the consistency ratio C.R.,The formula that it uses is: C.R. = C.I./R.I. ,After calculate the value of C.R.,For more than three orders of judgment matrix,If the value is less than or equal to 0.1,and it is considered that the consistency test is passed, otherwise the judgment matrix needs to be modified and adjusted.We refer to methods proved feasible in the past in the research and application of several problems in analytic hierarchy process,Its core idea is to get new matrix after judgment matrix normalized. Use "sum-product method" for the new ordering vector matrix, at the same time, based on the original judgment matrix and the new matrix sequencing vector to construct the original matrix of the induced matrix. By using the induced matrix of the various elements of the original matrix adjustment, in order to make the new matrix to achieve

consistency.The aim is to obtain a judgment matrix that is not reconfirmed by experts, while maintaining the views of multiple experts at the same time.

Step 4: Calculating the relative weight vector between the indices under the same criterion ω

In the first three steps, the judgment matrix of each expert is combined and the consistency test is carried out, and the relative weight of each index is calculated by using the comprehensive judgment matrix C.There are many ways to calculate weight.For example:geometric mean;method of characteristic roots and so on.For simplicity and convenience,the geometric mean is used here.The method is as follows: Multiply the elements of the matrix C by column,then get a new vector by square-root.Then the vector of weight $\omega = (\omega_1, \omega_2, \cdots, \omega_n)$ is obtained by the following formula(3):

$$\omega_i = \frac{(\prod_{j=1}^{n} c_{ij})^{\frac{1}{n}}}{\sum_{h=1}^{n} (\prod_{j=1}^{n} c_{hi})^{\frac{1}{n}}} \tag{3}$$

i=1,2,…,n.After ensure the relative weight,it needs to be tested for consistency,the exact method is the same as the third step,this paper is not going to describe it anymore.

Each indicator of the same criterion can be used to assign value to the weights.

B. Establishing a Multilevel Fuzzy Comprehensive Evaluation Model

The specific steps of multi-level fuzzy comprehensive evaluation are mainly divided into the following two steps:

Step 1: Determine the minimum limitation of system security.Its specific calculation method is: Suppose there are n experts, and statistics for each minimum value of experts, noted S_{imin},i=1,2,…,n.The values of S_{imin} are integers between 0 and 10.Set a Comment set D ={Excellent, good, general, unqualified}, and then take statistics for each minimum value of experts,Count the frequency: m_{it},t=1,2,3,4 of S_{imin} of each class belong to comment set.

Using the formula(4):

$$e_{min}^{t} = \frac{m_{it}}{n} \tag{4}$$

Calculated the minimum limitation of fuzzy evaluation value of S_{min},and the fuzzy evaluation value of the minimum limitation of system security $E_{S_{min}} = (e^1_{min}, e^2_{min}, e^3_{min}, e^4_{min})$.

According to the principle of maximum membership and entropy property,we use formula(5):

$$S_{\min} = \left(1 + \sum_{i=1}^{4} (\alpha_i e_{\min}^i) \ln e_{\min}^i\right) \times 100\% \tag{5}$$

The value of Smin is calculated, which is the minimum value to measure the system's security.It is considered that the system is safe if the result is greater than that value, whereas it is considered unsafe.The ai represents the relative weight of each security class importance(a_i = 0.25).

Step 2:Implementing multilevel fuzzy comprehensive evaluation

Because of the hierarchy of the index system, the fuzzy comprehensive evaluation should be carried out from the lowest level index to the fuzzy comprehensive evaluation, until the comprehensive evaluation results of the highest level are obtained.First to network penetration testing various test data can be obtained by using normalized processing, obtains a bottom index fuzzy evaluation value relative to the evaluation set, second, we should calculate the index fuzzy evaluation value of calculation between the layers.Assuming that the system safety index system is divided into m layers, the lower indices of each index reflect the security features of the upper index relative to the whole system.The ith index xi in the upper index is assumed to have n,and set jth index of the lower class xij.Its fuzzy evaluation value is $E_{xij} = (e^1_{ij}, e^2_{ij}, e^3_{ij}, e^4_{ij})$, (i,j=1,2,3, …, n).

The weight vector of the lower index of the index X_{ij} is $\varpi_i = (\omega_{i1}, \omega_{i2}, \cdots, \omega_{in})$ .Then,representation of Matrix Mi of fuzzy evaluation values of the upper index X_i relative to the lower index is :

$$M_i = \begin{vmatrix} e_{i1}^1 & e_{i1}^2 & e_{i1}^3 & e_{i1}^4 \\ \cdots & \cdots & \cdots & \cdots \\ e_{in}^1 & e_{in}^2 & e_{in}^3 & e_{in}^4 \end{vmatrix}$$

The fuzzy evaluation value of upper index Xi can be calculated by formula(6):

$$E_{xi} = \bar{\omega} \bullet M_i \tag{6}$$

L is the ordinal number of upper index; $\bullet$is fuzzy operator. The current fuzzy operator usually adopts the Chad operator. The test indicator system is divided into four layers. The fuzzy evaluation value E of each criterion is calculated by using this method from the bottom level to the top level, until we have calculated the fuzzy evaluation value corresponding to the target $E_s=(e^1_s, e^2_s, e^3_s, e^4_s)$.Finally, the overall objective evaluation of system security is calculated. Using this formula(7) to calculate the result by the principle of maximum membership and the properties of entropy:

$$S = (1 + \sum_{i=1}^{4} \alpha_i e_S^i \ln e_S^i) \tag{7}$$

We should get the system security values. The a_i expresses the importance of the relative weight of each grade in the comments set, e_i is the fuzzy evaluation result of the judgement layer relative to target layer. The calculated results are compared with the minimum system security value S_{min} calculated in the first step.If S>=S_{min},in the background of network penetration testing, the system is safe and can be used in practice. Otherwise, it is deemed that the system is unsafe and the system security personnel need to be reformed.

C. The Acquisition and Processing of Data of Penetration Test

Step 1: Acquisition of network penetration test results data. Using the network penetration test to test the system security, the result is to obtain the test result values of the underlying indexes in the test index system, which we call the raw data. Not only determine the relative scientific test results, but also will attack test data acquisition form submitted review committee of experts, based on the set of test scenarios and test data to obtain a list of comprehensive analysis, combined with own work experience, making evaluation and score to each kind of ability. The score is within 0-10 range.

Step 2: Processing of network penetration test results data. The result of data processing is the evaluation of single performance index, and the process of data processing is as follows:

Experts discuss the selection of evaluation methods->Experts discuss the determining of the evaluation criteria->Experts rate the raw data based on criteria->Score statistics->The evaluation of raw data of test results.

In order to make fuzzy evaluation, we need to set up a set of comments. This paper divided evaluation into collection of comments from high to low d_i(i=1,2,3,4)is: D ={Excellent, good, general, unqualified}={d_1,d_2,d_3,d_4}.After consulting relevant experts, experts believe that if the score is within 9-10 range, the ability is excellent; In a 7-8 range, the ability is good; In the 4-6 range, the ability is general; Below 3 points, this ability is not qualified.

Suppose the experts in the evaluation group of network infiltration test results have n bits. And the fuzzy statistic is to let these experts classify the results according to the above comments. Calculate the results of each test index gradually, which is the frequency of each grade mijt(t=1,2,3,4),Then the calculation formula(8) for the fuzzy evaluation value E_{zzij}=(e_{ij1} e_{ij2} e_{ij3} e_{ij4}) of the capability is as follows:

$$e_{ijt} = \frac{m_{ijt}}{n} \tag{8}$$

The e_{ij1} in the fuzzy evaluation E_{zzij} expression indicates the degree of excellence;e_{ij2} indicates the degree of good;e_{ij3} indicates general degree;e_{ij4} indicates disqualification.

V. EXPERIMENT

A. Overview of the System to be Tested

To verify the usability of the network system security assessment method based on penetration testing, this paper selects a system that is validated as security by other security assessment methods for penetration testing. This object system had established a set of security system index based on AHP, which is divided into target layer, criterion layer, sub-criterion layer and indicative layer according to the analytic hierarchy process.

The target layer S is the information system security based on osmotic testing. The criterion was named Z_1,Z_2,Z_3,Z_4.Where Z_1 is divided into ZZ_1 and ZZ_2.The rest of the sub-criteria layer will not described in this articles in detail, and there are nine criterion sub-criterion layers and 29 indicators in indicative layer .In this safety indicator system, there are only 3 indicators in the sub-criteria except ZZ 1and ZZ_2.The index layer is named ZZ_{ij},(i=1,2,...,9.j=1,2,3,4).

B. The Acquisition of Fuzzy Comprehensive Evaluation Values

According to the method in above, we set up 20 experts to make fuzzy evaluation of 29 indicators to get the fuzzy assessment value : E_{ZZij} of each indicator.

The method of acquiring fuzzy evaluation value is taken as an example of ZZ11.After giving results of test values to the experts, the grade giving by them are(9,9,8,9,10,7,6,5,6,9,7,7,8,9,10,10,8,9,6,5).According to the standard of the evaluation set in the preceding article, there are nine best evaluations, six good evaluations, five normal evaluations. Therefore, we can calculate the degree of excellence is 0.45,good is 0.3,normal is 0.25,disqualification is 0 by the formula (8).After the same calculation, the fuzzy evaluation value of 29 indexes is shown below:

E_{zz11}=(0.45,0.3,0.25,0)E_{zz12}=(0.65,0.3,0.15,0)

E_{zz13}=(0.7,0.15,0.15,0)E_{zz14}=(0.6,0.3, 0.05,0.05)

E_{zz21}=(0.5,0.3,0.2,0)E_{zz22}=(0.55,0.45,0,0)

E_{zz23}=(0.75,0.25,0,0)E_{zz24}=(0.9,0.05,0.05,0)

E_{zz31}=(0.05,0.95,0,0)E_{zz32}=(0,0.7,0.25,0.05)

E_{zz33}=(0,0.25,0.75,0)E_{zz41}=(0,0,0,0)

E_{zz42}=(0.25,0.75,0,0)E_{zz43}=(0.35,0.6,0.05,0)

E_{zz51}=(0,0.7,0.25,0.05)E_{zz52}=(0.8,0.2,0,0)

E_{zz53}=(0.05,0.75,0.15,0.05)

E_{zz61}=(0.35,0.5,0.1,0.05)E_{zz62}=(0.55,0.4,0.05,0)

E_{zz63}=(0,0.5,0.45,0.05)

E_{zz71}=(1,0,0,0)E_{zz72}=(0,0.05,0.9,0.05)

E_{zz73}=(0,0.05,0.75,0.2)

E_{zz81}=(0,0.05,0.45,0.5)E_{zz82}=(0,0.05,0.65,0.3)

E_{zz83}=(0,0.4,0.5,0.1)

E_{zz91}=(0.85,0.15,0,0)E_{zz92}=(0.75,0,1,0.15,0)

E_{zz93}=(0.05,0.65,0.15,0.15)

C. Confirming the Critical Point of This System Security

According to the qualitative description and the system security level of the system security, and the organization of the network penetration test, the experts of the group of security evaluation ensure the critical point of this system security S_{min}. During an attack test, the score of 20 experts was (9,8,6,7,5,10,9,7,8,6,8,8,7,9,10,6,9,10,8,7).In summary, the time of excellence is 7,good is 9,normal is 4,disqualification is 0.So E_{smin} equals to (0.35,0.45,0.2,0).Using formula(5),we can calculate the S_{min} is 72.7%.As a result, the critical point of this system security is 72.7%.

D. Giving Values to the Weight

According to the method of calculation of index weight, the relative importance of each indicator relative to the superior indicator is evaluated by experts. This paper set six experts to evaluate the weight of indicators. After we get the six judgment matrices, we set geometric mean on scale values. Then we can get the initial comprehensive judgment matrix, and examine its conformity. If the result is not met the conformity, the adjustment method of the judgment matrix will be adjusted until the matrix meets the consistency check.

Step 1: Calculate the weight of the sub-criterion layer relative of the index layer. Because of the large amount of calculation, we take ZZ_1 as an example to calculate the weight. The specific methods are follows:

There are four indicators:ZZ_{11},ZZ_{12},ZZ_{13},ZZ_{14} below ZZ_1.According to the assessment of experts, the judgment matrix are follows:

$$C_{ZZ_1}^{(1)} = \begin{vmatrix} 1 & 1 & 1 & 1 \\ & 1 & 1 & 1 \\ & & 1 & 1 \\ & & & 1 \end{vmatrix} \quad C_{ZZ_1}^{(2)} = \begin{vmatrix} 1 & 1/2 & 1/2 & 1/2 \\ & 1 & 2 & 2 \\ & & 1 & 2 \\ & & & 1 \end{vmatrix}$$

$$C_{ZZ_1}^{(3)} = \begin{vmatrix} 1 & 1/3 & 1/3 & 1/2 \\ & 1 & 1 & 3/2 \\ & & 1 & 3/2 \\ & & & 1 \end{vmatrix} \quad C_{ZZ_1}^{(4)} = \begin{vmatrix} 1 & 1/2 & 1 & 1 \\ & 1 & 2 & 2 \\ & & 1 & 1 \\ & & & 1 \end{vmatrix}$$

$$C_{ZZ_1}^{(5)} = \begin{vmatrix} 1 & 1 & 1 & 1 \\ & 1 & 1 & 1 \\ & & 1 & 1 \\ & & & 1 \end{vmatrix} \quad C_{ZZ_1}^{(6)} = \begin{vmatrix} 1 & 1 & 1 & 1 \\ & 1 & 1 & 1 \\ & & 1 & 1 \\ & & & 1 \end{vmatrix}$$

After using the consistency test method, we affirm the matrices are consistent. Skip the process of calculation. After the roundness of geometric equalization of these matrices , the initial comprehensive judgment matrix is obtained:

$$C_{ZZ_1} = \begin{vmatrix} 1 & 1/2 & 1 & 1 \\ 2 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{vmatrix}$$

The ω^k_{zz1} (k=1, 2, 3, 4)of the matrix C_{zz1} is obtained through the root method:ω^1_{zz1} = 0.841;ω^2_{zz1} = 1.189;ω^3_{zz1} = 1;ω^4_{zz1} = 1;After normalization, the relative weight value of the four underlying indexes relative to the sub-criterion layer index ZZ_1 is obtained:ω_{zz1} = (0.2087,0.2951,0.2481,0.2481);

Performing a consistency check, According to the formula(9):

$$\lambda_i = \left. \sum_{j=1}^{4} C_{zz_{1j}} \cdot \omega_{zz_1}^{j} \right/ \omega_{zz_1}^{j} \tag{9}$$

we can calculate the λ1=4.085, λ2=4.096,λ3=4.031,λ4=4.031.

Using formula(10) :

$$\lambda_{\max} = \frac{1}{4}\sum_{i=1}^{4} \lambda_i \tag{10}$$

to determine the λ_{max} = 4.061. According to the formula(2),

$$C.I. = \frac{\lambda_{\max} - n}{n-4} = 0.0203 \quad C.R. = \frac{C.I.}{R.I.} = 0.023 < 0.1$$

The above calculation indicates that the judgment matrix can be accepted and the relative weight can be applied.

Therefore,ω_{zz1} = (0.2087,0.2951,0.2481,0.2481).

According to the method above, the judgment matrix and weight of other underlying indexes relative to sub-standard layer indexes can also be obtained.

Step2: Calculate the judgment matrix and weight value of the relative criterion layer of sub-criterion.The exact step is the same as the first step, and this is just the result:

$$C_{Z_1} = \begin{vmatrix} 1 & 4/3 \\ 3/4 & 1 \end{vmatrix} \quad \omega_{Z_1} = (0.57, 0.43) \quad C.R. = 0$$

$$C_{Z_2} = \begin{vmatrix} 1 & 9/8 \\ 8/9 & 1 \end{vmatrix} \quad \omega_{Z_2} = (0.5294, 0.4706) \quad C.R. = 0$$

$$C_{Z_3} = \begin{vmatrix} 1 & 6/5 \\ 5/6 & 1 \end{vmatrix} \quad \omega_{Z_3} = (0.5455, 0.4545)$$

$$C_{Z_4} = \begin{vmatrix} 1 & 1/2 & 1/3 \\ 2 & 1 & 2/3 \\ 3 & 3/2 & 1 \end{vmatrix} \quad \omega_{Z_4} = (0.1667, 0.3333, 0.5)$$

Step3: Calculate the judgment matrix and weight value of the relative target layer of the criterion layer. The exact step is the same as the first step, and this is just the result:

$$C_S = \begin{vmatrix} 1 & 2 & 1 & 10/9 \\ 1/2 & 1 & 1/2 & 5/9 \\ 1 & 2 & 1 & 10/9 \\ 9/10 & 5/9 & 9/10 & 1 \end{vmatrix}$$

$$\omega_S = (0.3154, 0.1577, 0.3154, 0.2115) \quad C.R. = -0.0555 \approx 0$$

E. Fuzzy Comprehensive Evaluation

After calculation of the weight of various indicators, can make a comprehensive fuzzy evaluation, the purpose is the values of fuzzy evaluation of target layer, to ensure the degree of excellence, good, the proportion of qualified and unqualified degree. The specific calculation steps are as follows:

Step 1: to evaluate fuzzily the sub-criteria. Take ZZ_1 as an example to make a simple evaluation. The fuzzy evaluation value (the performance evaluation value of the single index) test results of the four indexes of ZZ_1, ZZ_{11}, ZZ_{12}, ZZ_{13} and ZZ_{14} are represented by matrix representation as follows:

$$M_{ZZ_1} = \begin{vmatrix} 0.45 & 0.3 & 0.25 & 0 \\ 0.65 & 0.3 & 0.15 & 0 \\ 0.7 & 0.15 & 0.15 & 0 \\ 0.6 & 0.3 & 0.05 & 0.05 \end{vmatrix}$$

The result of evaluation of ZZ_1 is follow:

$$E_{ZZ_1} = \omega_{ZZ_1} \bullet R_{ZZ_1}$$

$$= (0.2087 \quad 0.2951 \quad 0.2481 \quad 0.2481) \bullet \begin{vmatrix} 0.45 & 0.3 & 0.25 & 0 \\ 0.65 & 0.3 & 0.15 & 0 \\ 0.7 & 0.15 & 0.15 & 0 \\ 0.6 & 0.3 & 0.05 & 0.05 \end{vmatrix}$$

$$= (0.609, 0.263, 0.166, 0.013)$$

The result after normalization is :

E_{zz1}=(0.579,0.25,0.158,0.013).

In the same way, the fuzzy evaluation value of indexes of other sub-criterion layer are:

E_{zz2}=(0.605,0.223,0.172,0);E_{zz3}=(0.02,0.62,0.35,0.01);

E_{zz4}=(0.3,0.675,0.025,0);E_{zz5}=(0.219,0.593,0.15,0.038);

E_{ZZ6}=(0.28,0.467,0.216,0.037);

E_{zz7}=(0.415,0.029,0.478,0.078);

E_{zz8}=(0,0.1375,0.5625,0.3);

E_{zz9}=(0.389,0.455,0.089,0.067).

Step 2: set a fuzzy evaluation of each index of criterion layer. The results are as follows:

E_{z1}=(0.59,0.238,0.164,0.008);

E_{z2}=(0.137,0.584,0.274,0.005);

E_{z3}=(0.248,0.535,0.179,0.038);

E_{z4}=(0.263,0.278,0.312,0.147);

Step 3: fuzzy evaluation of target layer can obtain the fuzzy evaluation value of this system security relative to the evaluation set:

E_s=(e^1_s,e^2_s,e^3_s,e^4_s)=(0.279,0.507,0.176,0.038);

The formula(7) is used to calculate S= 74.5%.

Comparing S with S_{min}, we get the result S> S_{min}, which can be determined that the system is in line with security objectives under the network penetration test, so the system is safe.

VI. CONCLUSION

This paper introduced a network system security assessment method based on penetration test by analyzing the current assessment methods and the flaws of these methods.

The main tasks includes: Introduction and analysis to the current system safety assessment method, building and using of penetration test model. The penetration test is designed to test the security of the information system and evaluate the system after expert evaluation and fuzzy evaluation. By using analytic hierarchy process and multilevel fuzzy evaluation method, carries out a relatively scientific and safe result of evaluation of test .Given the previous security assessment of the object system, the evaluation of the system was basically consistent with the evaluation of the system using a security assessment based on penetration testing. Therefore, it is reasonable and feasible to evaluate the security evaluation of network system based on osmotic testing, and also greatly improve the accuracy of the system security assessment from the aspect of simulated attack.

ACKNOWLEDGMENT

This work was supported the National Key R&D Program of China (No. 2016YFB0800700)

REFERENCES

[1] Z. Q. Cai; J. B. Zhao; Y. Li; S. B. Si; M. N. Ni,Information security evaluation of system based on Bayesian network,2015 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM),Pages: 315 - 319,2015.

[2] Sravani Teja Bulusu, Romain Laborde, Ahmad Samer Wazan, François Barrère, Abdelmalek Benzekri; Which Security Requirements Engineering Methodology Should I Choose?: Towards a Requirement Engineering-based Evaluation Approach,ARES 2017: 29:1-29:6,2017.

[3] Dongqing Wang,Yueming Lu,Jiefu Gan.An Information Security Evaluation Method Based on Entropy Theory and Improved TOPSIS,2017 IEEE Second International Conference on Data Science in Cyberspace (DSC),Pages:595-600,2017.

[4] Arianit Maraj, Genc Jakupi, Ermir Rogova, Xheladin Grajqevci, "Testing of network security systems through DoS attacks", Embedded Computing (MECO) 2017 6th Mediterranean Conference on, pp. 1-6, 2017.

[5] US Department of Commerce, NIST. Guide to Information Security Testing and Assessment[J]. Itlb.

[6] Marri Rami Reddy, Prashanth Yalla, "Mathematical analysis of Penetration Testing and vulnerability countermeasures", Engineering and Technology (ICETECH) 2016 IEEE International Conference on, pp. 26-30, 2016.

[7] Jinsoo Shin,Hanseong Son,Gyunyoung Heo. Cyber Security Risk Evaluation of a Nuclear Instrumentation and Control System Using Bayesian Networks and Event Trees[J]. Nuclear Engineering and Technology,2016.

[8] William G J Halfond, Shauvik Roy Choudhary, Alessandro Orso, "Improving penetration testing througll static and dynamic analysis[J]", Software Testing Verification & Reliability, vol. 21, no. 3, pp. 195-214, 2011.

[9] Microsoft (2016) Common types of network attacks, [online] Available: https://technet.microsoft.com/en-us/library/cc959354.aspx.

[10] M. Saindane, "Penetration Testing-A systematic Approach", 2012.

[11] Gary McGraw, Software Security. Datenschutz und Datensicherheit - DuD, vol. 9, no. 36, pp. 662-665, 2012.

[12] P. K. Manadhata, J. M. Wing, "An Attack Surface Metric", Software Engineering IEEE Transactions on, pp. 371-386, 2011.

[13] Xue Qiu. An automated method of penetration testing[A]. IEEE Beijing Section.Proceedings of 2014 IEEE Computers, Communications and IT Applications Conference (ComComAp)[C].IEEE Beijing Section:,2014:6.

[14] Patrick Engebretson. What Is Penetration Testing?[M].Elsevier Inc.:2011.

[15] Sanjay Bavisi. Penetration Testing[M].Elsevier Inc.:2013.

[16] Yu Jiao Wang,Hai Yun Lin. A Kind of Network Security Evaluation Method Based on Local Variable Weight[J]. Key Engineering Materials,2011,1244(474):.