Journal of Computers Vol. 28, No. 2, 2017, pp. 105-118
doi:10.3966/199115592017042802008

A Network Risk Assessment Method Based on Attack-Defense Graph Model

Wei Zhou, Hong Zhang, and Qian-mu Li

College of Computer science and engineering, Nanjing University of S&T, 210007, China
Kingmorusun@sina.com

Received 28 December 2015; Revised 28 March 2016; 28 March 2016

Abstract. The attack-defense graph is a model-based network vulnerability analysis technique. Based on the situation of electric power information network, a hierarchical network security risk assessment framework is proposed using bottom-up analysis method. The framework divided the network security risks into two parts: vulnerability security risks and attack security risks, then assessed network security risk layer by layer in accordance with the network's hierarchy. Firstly, using vulnerability scanning tool to detect the vulnerability information in the network nodes, as well as associating the vulnerability information which attacks relying on with vulnerability information of the node itself to build the state attack-defense graph, further calculating the vulnerability reliability vector and attack reliability vector of the node. Combined with each vulnerability's hazard index and the attack hazard index, we calculate the vulnerability security risk and the attack security risk of the node, then assess the security risk value of a single node; Secondly, we quantify the security risk from the single node to the whole network combined with the weight of each node in the network itself. In order to exclude the own uncertainties of vulnerability scanning tools and the unity of the data source, this assessment method fuses several test results of scan tool, and constitutes the data source when calculating the vulnerability reliability. Eventually, based on the Dempster-shafer theory and the European Space Vector Projection, an attack-defense graph algorithm is proposed, which makes the evaluation results more objective and credible.

Keywords: digital signal processing, e-commerce, operating systems, RFID

1 Introduction

Recent years, many researchers develop a large number of researches on network security risk, the main methods can be divide into two classes, static assessment and dynamic assessment. Static assessment methods use some evaluation criteria such as TCSEC、ITSEC、CC、IOS/IEC 17799、BS 7799、ISO 13335, etc. [1, 5, 7]. Since lacking of real-time performance, static assessment methods can only estimate the security risk level of the network accurately, and lack real-time risk detection for the network suffered from attacks, dynamic security risk assessment research has become a hotspot in the field [2, 6, 8].

Philip et al. proposed an alarm processing model named M-Correlator [9]. This model builds an important connect between alarm, target and target resource based on a tree structured Bayes propagation method, and deals with security incidents to get the threat levels of the attack to the target, then divide them into high, medium and low three levels. But the objects involved in this method are all isolated alarms, which means it cannot make a complete evaluation to the attack process. Stephen Boyer et al. proposed a Stellar evaluation model [2], this model is composed of attack process reconstruction and security risk assessment, and the risk assessment of the model is accomplished by a series of rules which are well prepared by the experts. The shortage is that the formulation of these rules is completely dependent on the expert experience, and the preparation of rules is time-consuming, laborious and subjective. Based on the real-time risk assessment of the automatic intrusion model, Gehani [3] proposed RheoStat real-time risk management model. This model calculates the risk by multiplying threat probability, the vulnerability point of exposure rate and the impact of the assets, then assess the attack threat,

the target assets, the target vulnerable point. But the model can only be used to evaluate the risk of a single host, and cannot be used in network layer. Hariri et al. evaluate and analyze the impact of network attacks on system security based on network performance metrics [4]. But this method can only be applied to the analysis of denial of service attacks, and cannot be used in other types of attacks on system security.

Aiming at the problem of network security risk assessment in two aspects of risks, and based on the attack state graph model from the point of view of the network node and the node may suffer from the attack, we design a hierarchical risk assessment model by using the method of hierarchical analysis. The model can decompose the whole risk of the network into the weighted sum of the nodes in the network, the risks of a single node are also decomposed into the vulnerable point risks and the attack risks. Then we calculate the risk of a single host's vulnerability and attack risk, evaluate the security risk of the entire network combined with the weight of each node in the network.

2 Risk Assessment Model

In the risk theory, assets represent a kind of resources, procedures, products, computers and all enterprises which will be protected, it is a valuable subject and also can be logical, such as information or data. It can also be physical, such as computer systems. Assets in this paper refers to all network devices in the network system and business data or softwares related to the network system. The value of assets can be expressed by five factors including their own value, support and maintenance of the value and the size of the loss after the loss of confidentiality, integrity and availability.

Threats mean the abnormal of the system traffic or the system's attack, they can cause security risks to the network or assets, and they are a part of the risk model.

Vulnerability is a weakness that can be exploited by an asset or asset group, also known as a hole which includes threats to the network or a weak point of the system, such as access to enhance the denial of service, buffer overflow, etc. The vulnerabilities make a system more vulnerable to be used by the attacker, and damage to the assets.

Influence means the loss of the network system after the occurrence of threats. The loss can be described by the integrity, confidentiality and availability.

Network attack is the behavior that damage the integrity, confidentiality and availability of the network system. These behaviors can be classified into three basic cases: integrity damage attack, information disclosure attack and denial of service attack.

Security risk is a potential, negative damage in the state where nothing has happened. Security risk is composed of five aspects which includes the origin, the way, the channel, the receptor and the consequences. Among them, the origin is a threat to the initiator, known as the source of danger. The way threat source implements threat is called the threat of behavior. Channel is the weak link in the use of dangerous sources, known as vulnerabilities. Receptor is the recipient of a threat, which is the asset. The result is the loss caused by the dangerous source, called the impact. That is to say, one or more sources of the security risks, through one or more channels, against one or more receptors based on one or more ways, and have a bad consequence in the environmental assets. The model is shown in Fi. 1.

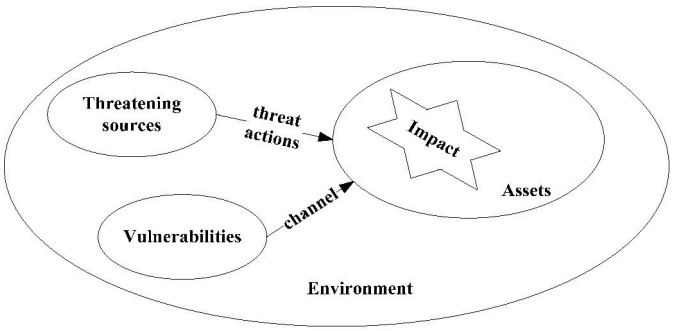

Fig. 1. The environmental assets model

Safety control is the prevention of the threat, the reduction of vulnerability and the protection of assets. And it limits the impact of unexpected events, becomes a practice, procedure or mechanism to reduce

security risks. Fig. 2 shows the relationship between the above basic concepts in network security risk assessment.

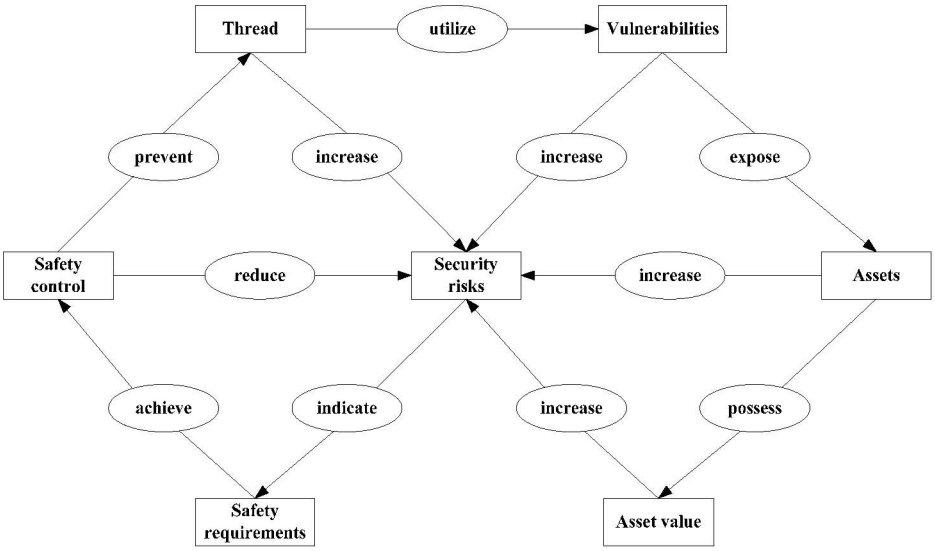

Fig. 2. Basic concepts of security risk assessment

Network security risk assessment is to identify the risks that exist in the network environment, and make a comprehensive analysis. The principle is shown in Fig. 3, which is mainly related to assets, threats and other basic elements of vulnerability.

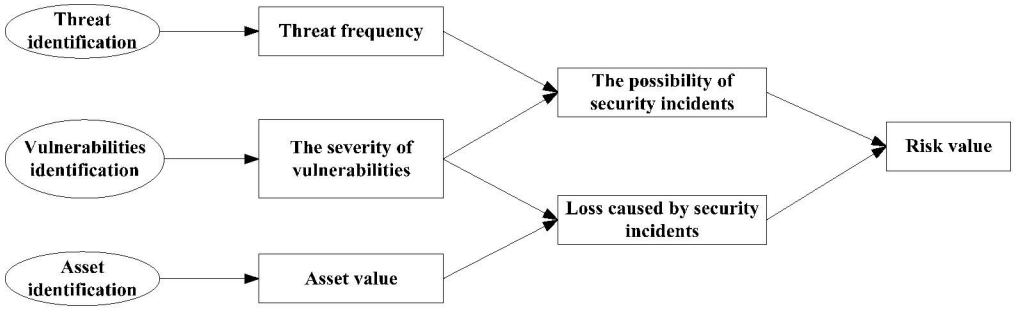

Fig. 3. Schematic diagram of network security risk assessment

Network security risk assessment is a process of analyzing and determining the risk. This paper mainly includes the following steps:

(1) The preparation of the risk assessment is mainly to clarify the system, determine the evaluation of the object, and provide assessment of the data object for the data analysis phase.

(2) To find out the weakness of the system, and use the vulnerable point scanner to find out the vulnerable points of the network nodes.

(3) To find out the threat of system and the attack of the system based on the state attack graph generated by relationship of the network nodes can reach and their own vulnerability and the attack on the use the vulnerable point.

(4) Calculating the probability of a successful attack, which is based on the reliability and ease of use of the vulnerable points.

(5) Calculating the loss of security. Calculating the damage to the network assets according to the extent of damage of vulnerable point potential to assets and the assets loss after the attack.

(6) Quantifying security risks. We calculate the impact of the attack on the evaluation object according to the existence of weak points, the degree of vulnerability, the probability of the occurrence of security incidents and the loss of network assets. Then we use the impact to quantify the risk value of the node. The risk value of the entire network is evaluated combined with the weight of each node in the network.

Fig. 4 shows the flow chart of the network security risk assessment based on the attack and defense

state graph model.

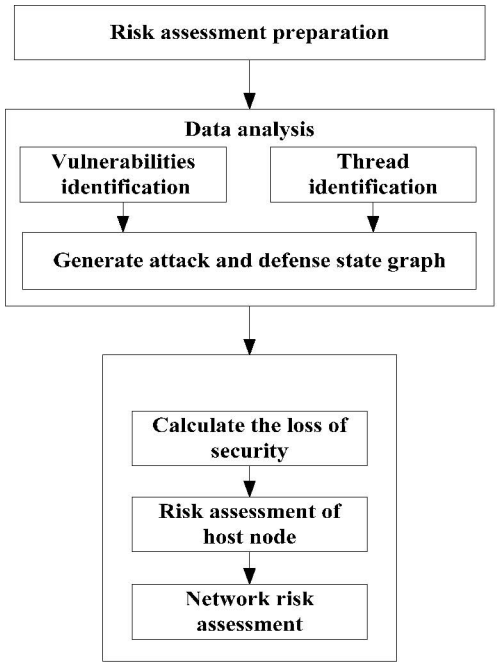

Fig. 4. Network security risk assessment process

In this paper, the network security risk assessment framework is designed based on the hierarchical structure of attack and defense and the logical relationship between attack and vulnerable points.

The framework is bottom-up. Firstly, we determine the vulnerable point set by a variety of vulnerable point scanners according to the status of attack and defense. Furthermore, we calculate the confidence of all vulnerable points in the node and the probability of the success of atomic attacks for each node combined with the hazard index of each vulnerable point and the atomic attack frequency and its risk index, then calculate the security risk of the vulnerable points of the node and the risk of attack security. After that, we evaluate the security risk value of a single node. At last, we quantify the security risk value of the whole network system based on the weight of each node in the network.

The definitions are given below for the risk involved in the evaluation framework.

Due to the uncertainty of the attack and defense, this paper introduces concept of the reliability of attack and defense (denoted as f) to express the degree of support or credibility of the individual vulnerable points. The damage degree of single vulnerable points in a node denoted as E. Since the vulnerability index is a direct expression of the severity of vulnerability, it can be used to measure the severity of the vulnerability index. National Vulnerability Database is one of the most authoritative information database of vulnerable points. The database gives a measure of the severity of the vulnerability which is between 0 and 10. The measure comes from several aspects, including the use of vulnerable points, the use of complexity, the number of target authentication and the impact of information confidentiality, integrity and availability. With the identification of the Common Vulnerabilities and Exposures, we query the corresponding degree of severity from the National Vulnerability Database as a vulnerable point of the hazard index.

The risk of a single vulnerable spot in a node is represented by the product of the weak point of attack and defense and the vulnerability index.

$$R_v = f \times E \tag{1}$$

where f is the confidence level of a single point of vulnerability, the E is a single point of vulnerability to the node's hazard index.

At present, most of the attacks on the network are multistep combination attack, which is accomplished through the implementation of multiple atomic attacks. An atomic attack is carried out by an attacker using a single point of vulnerability. Thus, an attack is made up of a series of atomic attacks.

Definition 1: atomic attack frequency. The number of individual atomic attacks in a node for a time,

denoted as C. It can be obtained by attacking the log database.

Definition 2: the success probability of atomic attack. The possibility of a successful attack on a single atom in a node, denoted as P. From the network system as a whole, the successful implementation of atomic attacks with randomness. It is affected by the factors like the reliability of the results of vulnerability scanning and the ease of use of vulnerable points. In previous studies, the success probability of atomic attack is strong subjectivity, because it is obtained by expert scoring. In order to avoid this shortcoming, this paper employs the confidence of the vulnerable points used in the attack graph of atomic attack. Then it quantifies the value of the individual vulnerability point combined with the Common Vulnerability Scoring System. Finally, the probability of an attack is defined as the product of the degree of difficulty of attack and defense, which is

$$p = f \times exp \tag{2}$$

Among them, f is the reliability of the vulnerable points of attack and defense. Calculation method in the next section will be given in detail. exp is the ease of use of vulnerable points. In order to satisfy the probability of the calculation result is less than 1, the calculation formula of the vulnerable points in CVSS is modified as:

$$\exp = 2 \times \text{AccessVector} \times \text{AccessComplexity} \times \text{Authentication} \tag{3}$$

In CVSS, the AccessVector reflects the way the vulnerable points are utilized, and the possible values are Local (L), Adjacent (A) and Network (N). AccessComplexity reflects the complexity of the attack, which may be used for High (H), Medium (M) and Low (L). Authentication reflects the times of attacks targeted identity the attacker's when using the vulnerable point, which may be the value of Multiple (M), Single (S) and None (N), the corresponding quantization value is shown as follows.

$$AccessVector = \begin{cases} 0.395 & L \\ 0.646 & A \\ 1 & N \end{cases}$$

$$AccessComplexity = \begin{cases} 0.35 & H \\ 0.61 & M \\ 0.71 & L \end{cases}$$

$$Authentication = \begin{cases} 0.45 & M \\ 0.56 & S \\ 0.704 & N \end{cases}$$

Definition 3: atomic attack hazard index. The degree of damage caused by a single atomic attack in a node after a successful attack is recorded as r. In this paper, we describe the damage to the network system security properties by using the vulnerable points of the network system security. Referring to the information security property of [98], the security of vulnerable points can be classified into ConfImpact damage, IntegImpact damage and AvailImpact damage by the calculation method of brittle weakness in CVSS, the damage index of atomic attack is defined as:

$$r = p \times [10.41 \times (1-(1-ConfImpact) \times (1-IntegImpact) \times (1-AvailImpact))] \tag{4}$$

where the success probability of the atomic attack p is calculated by the formula (2). ConfImpact, IntegImpact and AvailImpact reflect the confidentiality, integrity and availability of the vulnerable points, which may be used as None (N), Partial (P) and Complete (C) in CVSS, and the corresponding quantization values are shown as follows.

$$IntegImpact = \begin{cases} 0 & N \\ 0.275 & P \\ 0.660 & C \end{cases}$$

$$ConfImpact = \begin{cases} 0 & N \\ 0.275 & P \\ 0.660 & C \end{cases}$$

$$AvailImpact = \begin{cases} 0 & N \\ 0.275 & P \\ 0.660 & C \end{cases}$$

Definition 4: atomic attack security risk Ra. The risk is caused by the success of external attacks using the vulnerable points in the network nodes. Due to the fact that the risk of a high damage index attack has Greater risk than Low hazard index attack, we represent the security risk of an atomic attack by the product of the atomic attack frequency and 10 atomic attack damage index Times Square in calculating the security risk of atomic attack.

$$R_a = c \times 10^r \tag{5}$$

Where c is a single atomic attack frequency, r is a hazard index for the nodes of a single atomic attack.

Definition 5: node security risk Rh. The security risk of a single node is composed of two parts. It is the security risk of all the vulnerable points and the safety risk of atomic attack. That is:

$$R_h = \sum_{i=1}^{m} R_{v_i} + \sum_{j=1}^{n} R_{a_j} \tag{6}$$

Where M is the number of vulnerable points in a single node H. N is the total number of atomic attacks in a single node H. R_{v_i} is a security risk for a single point of vulnerability in formula (1). R_{a_j} is the security risk of a single atom attack calculated from the formula (5).

Definition 6: network security risk R_{N}. The impact of external attacks through the network of all nodes, expressed by all the weights of the nodes and the security risk weighted.

$$R_{\mathrm{N}} = \sum_{k=1}^{p} \omega_k R_{h_k} \tag{7}$$

Among them, p is the total number of nodes in the network. ω_k is the weight of a single node HK in the network, it is the based on the importance of the nodes, the node's topological connection and the number of access times. As shown in Table 1, we get it by means of domestication. In the actual operation, the system can be adjusted according to different systems. R_{h_k} is the security risk of a single node calculated from the formula (6).

Table 1. Importance of node

Level	Classes	Equipment importance
*L*1	Router or gateway	5
*L*2	FTP、Database server	4
*L*3	Web server	3
*L*4	Host workstation	2
*L*5	Intelligent terminal	1

According to the network security risk assessment framework in Fig. 5, if we want to evaluate the security risk value of the entire network system, we must calculate the security risk values of all vulnerable points on a single node and the security risk value of atomic attacks firstly. However, if you want to calculate the risk of a single point of vulnerability Rv and a single atomic attack security risk Ra, you must determine the degree of confidence of the fragile F, the vulnerability index e, the success probability of atomic attack P and atomic attack hazard index R. Among them, it is the key to calculate the reliability of F.

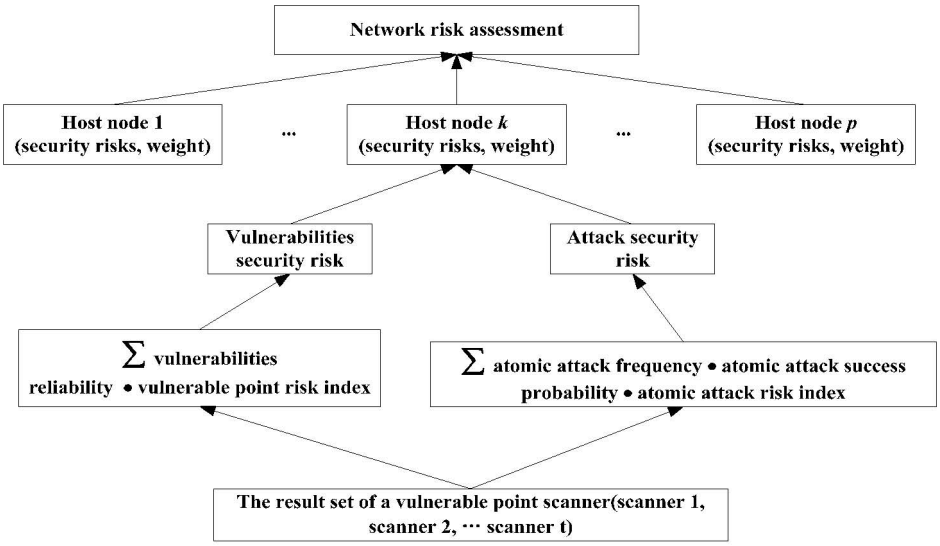

Fig. 5. Network security risk assessment framework

3 The Network Risk Assessment Method Based on the Offensive and Defensive State Graph Model

In the process of network security risk assessment, the vulnerability scanner is needed to find out the weak points of the nodes. And due to the technical defects of vulnerability scanner implementation, it has a different degree of fault rate and false alarm rate, which brings uncertainty for the results and affects the results of network security risk assessment. In order to make the evaluation result more accurate and reliable, this paper introduces the confidence level of the vulnerability point in the presence of attack and defense. Based on the evidence theory and comprehensive consideration of the scanning results of multiple vulnerable point scanners, a network risk assessment method is proposed to calculate the confidence of a single weak point based on the model of attack and defense.

Evidence refers to the property and objective environment (real evidence) of the things that people have to analyze the proposition, and to seek the basis of its basic confidence. Through the analysis of the evidence, we get the basic m (A) of the proposition, the basic m (A) here is the true confidence in the front that people believe that proposition A is true, as shown in Fig. 6.

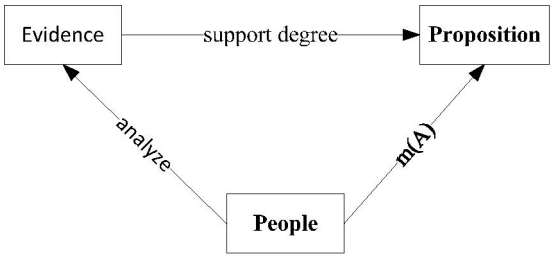

Fig. 6. Evidence and confidence credible

For a decision problem, assuming that people can know possible results set and show as the collection Θ, people care about any proposition corresponds to a certain subset in the collection Θ. Θ is called frame of discernment based on the offensive and defensive state graph model.

Definition 7: Assuming that set Θ is defensive state graph model based on the frame of discernment ,if the Set function m:2Θ → [0,1] (the 2Θ is the Density function of Θ) meets:

$$(1)\ m(\varnothing) = 0 \qquad (2)\ \sum_{A \subset \Theta} m(A) = 1$$

Then we call M as basic probability assignment of frame of discernment based on offensive and defensive state graph model Θ; ∀A⊂Θ, m(A) is called the basic number of credible of A. The function M is called basic probability distribution function or become mass functions. If A is the subset of Θ, and m(A)>0, then A is called the focal element. If the number of elements in A is 1, which means that A atoms focal elements of evidence.

The basic number of trusted m (A) reflects the size of the confidence level of proposition A. But it cannot give any further and proper subset of a trust because of insufficient evidence. In the angle of the subject, M (A) seems to be evidence to support A, but not a proper subset. In order to calculate the atomic focal elements basic trusted number by adopting the idea of Euclidean space vector projection, this paper puts forward a kind of network risk assessment method based on the offensive and defensive state graph model.

In the evidence theory, recognition framework is defined as the set of all possible conclusions based on the offensive and defensive state diagram model, and all kinds of conclusions are mutually exclusive and complementary, therefore they can be explained by the ideas of the European space and defines some concepts of the theory of evidence.

Definition 8: Assuming that set Θ is containing N different proposition for a recognition framework based on the offensive and defensive state diagram model, then put N different proposition as two mutually perpendicular axes as containing N coordinate axis coordinate system, namely ,the N dimensional vector space.

Definition 9: Assuming that set Θ is containing N different proposition for a recognition framework based on the offensive and defensive state graph model. M is a basic confidence distribution based on the offensive and defensive state graph model identification. Then defining M·cosαij for M to the projection of each coordinate axis, and αij representing focal element I and the angle between the axis j. The size of α_{ij} is associated with the number of elements in focal element and its elements. The angle α_{ij} meet focal element *i* included in the s element j1, j2,... , js, focal element *I* and the angle between the *s* different axes are equal, that is $\alpha_{ij_1} = \alpha_{ij_2} = \cdots = \alpha_{ij_s}$, an angle of 90 degrees between the rest of the coordinate axes, namely cosαij = 0, j ≠ j1, j2, …, js.

Definition 10: Assuming that set Θ is containing N different proposition for a recognition framework based on the offensive and defensive state graph model. M is a basic confidence distribution based on the offensive and defensive state graph model identification, mark m′ as each coordinate axis projection for m to get an approximation of probability distribution function, m′ is the result of all focal element on different axes of projection and normalized then.

Because the method is get evidence after projection decomposition which can be expressed in a *Nd* vector through constant to each coordinate axis of focal element projection, so the above process is called confidence defensive state vector diagram analysis. In the function *m′*, which is an approximate probability distribution function after the definition 13 normalized, all focal element is focal element only contains an element of atoms.

In order to reduce the uncertainty of vulnerabilities scanner when calculating a single weak point of confidence in the compute nodes, we use a variety of vulnerabilities scanner to scan in the network node based on the above method. Scanning result set as proposition *A*, the accuracy of vulnerabilities scanner is set as credible number of A, that is *m (A)*. A variety of scanner results are set as recognition framework *Θ* based on offensive and defensive state graph model. The scanning results are confidence defensive state vector graph analysis, and then a single weak point of confidence is get.

In the case of a single node H_k scanning with *T* kinds of vulnerability scanner, based on the confidence level vector analysis method of attack and attack state graph analysis, the confidence level of a single point of vulnerability is shown as follows:

Input: each set of vulnerabilities scanner scans

Output: each vulnerabilities in the node degree of confidence.

In the first step, using the kind of t vulnerabilities scanner to vulnerabilities scanning of nodes H_k, each of the tools for node vulnerabilities scans results collection, where $V_s, s = 1, 2, \cdots, t$ .The set of all vulnerabilities scanner H_k scan results, and as a node H_k of reliability vector space, and defense figure vulnerable to remember $\Theta = \bigcup_{s=1}^{t} V_s = \{x_1, x_2, \cdots, x_m\}$. Due to the elements in Θ are not mutually included, so

make one of the elements as two mutually perpendicular axes, namely, Θ contains a coordinate axis coordinate system.

In the second step, regarding the results of each scanning tools set V_s as a confidence level of the vector $\mathbf{v}_s$ of Θ, and regarding the accuracy of each scanner as confidence after normalized vector $\mathbf{v}_s$ mode, and set $\|\mathbf{v}_s\| = r_s$.

In the third step, establishing $\alpha_{\mathbf{v}_s x_i}$ as the direction of confidence vector $\mathbf{v}_s$ and the axis angle x_i, $i = 1, 2, \cdots, m$, calculating the confidence of each coordinate axis in the direction cosine vector and space. $\forall x_i \in \Theta$, so $\cos \mathbf{v}_s x_i = 0$, if $x_i \in V_s$ $\mathbf{v}_s$ equals to axis direction cosine. Setting Confidence vector $\mathbf{v}_s = \{x_1, x_2, \cdots, x_u\}, s = 1, 2, \cdots, t$, Confidence vector space.

$$\Theta = \{x_1, x_2, \cdots x_u, x_{u+1}, \cdots, x_m\} \ \cos \alpha_{\mathbf{v}_s x_i} = 1/\sqrt{u}$$

In the fourth step, calculating the confidence vector $\mathbf{v}_s$, $x_i, i = 1, 2, \cdots, m$ on the axis of offensive and defensive state diagram analysis value, namely

$$r_s \cdot \cos \alpha_{\mathbf{v}_s x_i} \tag{8}$$

In the fifth step, summing the chart analysis values of each confidence vector $\mathbf{v}_s$ in the same axis on the offensive and defensive state accumulative.

$$f_{x_i} = \sum_{s=1}^{t} r_s \cdot \cos \alpha_{\mathbf{v}_s x_i} \tag{9}$$

Normalizing all $f_{x_i}, i = 1, 2, \cdots, m,$ so

$$\overline{f}_{x_i} = \frac{f_{x_i}}{\sum_{i=1}^{m} f_{x_i}} \tag{10}$$

Where $\overline{f}_{x_i}$ is a single weak point of the node H_k confidence. The set of $\overline{f}_{x_i}$ is the offensive and defensive graph vulnerabilities reliability vector of the node H_k .

But because the value of t is so big and will lead to assess cost, so the computation time is too long.While when the value of t is too small , it will make non-response rates and misstatement rate too high. Therefore, its values generally 3 to 4 relatively appropriate based on experience.

4 Experimental Verification and Analysis

In order to verify the feasibility and effectiveness of the risk assessment model and the network risk assessment method based on the model of attack and defense, this paper designs the network experiments, and the network topology is shown in Fig. 7. In the network system, there are three servers, a Web server, a FTP server which is used for important documents and data backup, and an Oracle database server which is used to provide service for Web server database. Attackers can access to the three servers in the network system directly with access permissions for user's permissions. Three servers can also be accessed by each other with user's permissions.

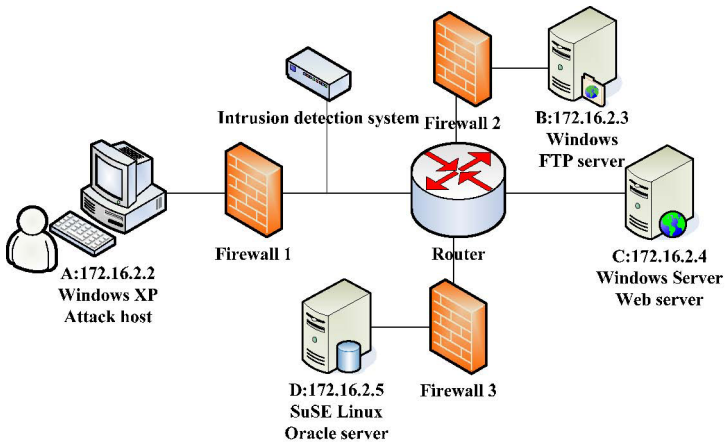

Fig. 7. Network topology graph

The reachability relationships among the nodes are shown in Table 2.

Table 2. Reachable relation table of state attack graph

Accessible relation	Source node	Target node	Protocol	Open port
A→B	172.16.2.2	172.16.2.3	FTP	21
A→C	172.16.2.2	172.16.2.4	HTTP	80
A→D	172.16.2.2	172.16.2.5	TNS	1521
B→C	172.16.2.3	172.16.2.4	HTTP	80
B→D	172.16.2.3	172.16.2.5	TNS	1521
C→B	172.16.2.4	172.16.2.3	FTP	21
C→D	172.16.2.4	172.16.2.5	TNS	1521
D→B	172.16.2.5	172.16.2.3	FTP	21
D→C	172.16.2.5	172.16.2.4	HTTP	80

This paper takes three kinds of vulnerable point scanners- Nessus, X-Scan and ISS to scan the three server nodes in the network, the scan results are shown in Table 3, the accuracy of the 3 kinds of vulnerable point scanners are 0.98, 0.90 and 0.94.

Table 3. Scan results for vulnerable points

Scanner	Node		
	Web server	FTP server	Oracle server
Nessus	CVE-2010-4562 CVE-2011-1871 CVE-2007-0066	CVE-2004-2111 CVE-2011-4800	CVE-2002-0060 CVE-2000-0800
X-Scan	CVE-2011-1871	CVE-2004-2111	CVE-2002-0060 CVE-2000-0800
ISS	CVE-2010-4562 CVE-2011-1871	CVE-2009-1439 CVE-2012-0450	CVE-2002-0060 CVE-2000-0800

Taking Web server node as an example, we calculate the confidence of the existence of the vulnerabilities of the node. According to the method of network risk assessment based on the model of attack and defense state graph, reliability vector space of attack and defense map of Web server Θ={CVE-2010-4562,CVE-2011-1871,CVE-2007-0066}∩{CVE-2011-1871}∩{CVE-2010-4562,CVE-2011-1871}={CVE-2010-4562,CVE-2011-1871,CVE-2007-0066}.X1, X2, and X3 representing CVE-2010-4562, CVE-2011-1871, CVE-2007-0066 as confidence degree vector space ourselves in the three coordinate axes. Nessus scan results of {CVE-2010-4562, CVE-2011-1871, CVE-2007-0066}, get confidence degree vector v1= (x1, X3, x2), ISS scan results of {CVE-2011-1871}, get confidence degree vector v2=(x2), SARA scan results of {CVE-2010-4562,CVE-2011-1871} get confidence degree vector v3=(x1, x2), then ||v1||=0.348，||v2||=0.319，||v3||=0.333. The direction cosines of confidence vector v1 and x1,

x2, x3 are $\cos\alpha_{v_1x_1}=\cos\alpha_{v_1x_2}=\cos\alpha_{v_1x_3}=1/\sqrt{3}$; The direction cosines of confidence vector v2 and x1, x2, x3 are $\cos\alpha_{v_2x_1}=0$, $\cos\alpha_{v_2x_2}=1$, $\cos\alpha_{v_2x_3}=0$; The direction cosines of confidence vector v3 and x1, x2, x3 are $\cos\alpha_{v_3x_1}=\cos\alpha_{v_3x_2}=1/\sqrt{2}$, $\cos\alpha_{v_3x_3}=0$ .The analysis values of attack and defense status chart of confidence vector v1 in x1, x2, x3 are all $0.348\times1/\sqrt{3}$ =0.200; The analysis values of attack and defense status chart of confidence vector v2 in x1, x2, x3 are 0 , 0.319×1=0.319, 0, respectively; The analysis values of attack and defense status chart of confidence vector v2 in x1, x2, x3 are $0.33\times1/\sqrt{2}$ =0.235, $0.33\times1/\sqrt{2}$ =0.235, 0, respectively. The sum analysis values of attack and defense status chart of confidence vectors v1, v2, v3 in x1 is f_{x_1} =0.200+0+0.235=0.435; The sum analysis values of attack and defense status chart of confidence vectors v1, v2, v3 in x2 is f_{x_2} =0.200+0.319+0.235= 0.754; The sum analysis values of attack and defense status chart of confidence vectors v1, v2, v3 in x2 is f_{x_3} =0.200+0+0=0.200. f_{x_1} , f_{x_2} and f_{x_3} normalized, get $\overline{f}_{x_1}=0.313$, $\overline{f}_{x_2}=0.543$, $\overline{f}_{x_3}=0.144$. That is, the brittle vulnerable point of the Web server CVE-2010-4562,CVE-2011-1871,CVE-2007-0066 existing in the confidence level of 0.313, 0.543 and 0.144 respectively.

From table 3, three kinds of scanners are all detected CVE-2011-1871, so it has the highest degree of confidence. The vulnerable point CVE-2010-4562 is detected by two kinds of scanners. And the vulnerable point CVE-2007-0066 is detected by Nessus scanner only. Although the accuracy of Nessus is the highest in the three scanners. Because the quantity of evidence is at least, and sufficient is lacked, so its degree of confidence is the lowest, the above calculation results are also consistent with the real situation.

In the same way, the confidence level of the vulnerable point on FTP server node CVE-2004-2111, CVE-2011-4800, CVE-2009-1439, CVE-2012-0450 can be calculated, and they are 0.441, 0.192, 0.1835, 0.1835 respectively. The confidence level of Oracle of CVE-2002-0060 , CVE-2000-0800 are 0.5 and 0.5 respectively.

According to the formula of the security risk of vulnerable point 1) and (3.6), the security risk of the vulnerable points of each server node is shown in Table 4. Numerical values in parentheses indicate the hazard index of the vulnerable point.

Table 4. Security risks for vulnerabilities

Server node	Vulnerability number	Affect and defense graph vulnerabilities reliability	A single vulnerability value at risk	Vulnerabilities total risk
FTP server	CVE-2004-2111 (8.5)	0.441	3.7485	7.29315
	CVE-2011-4800 (9.0)	0.192	1.728	
	CVE-2009-1439 (7.8)	0.1835	1.4313	
	CVE-2012-0450 (2.1)	0.1835	0.38535	
Web server	CVE-2010-4562 (4.3)	0.313	1.3459	6.6037
	CVE-2011-1871 (7.8)	0.543	4.2354	
	CVE-2007-0066 (7.1)	0.144	1.0224	
Oracle server	CVE-2002-0060 (7.5)	0.5	3.75	8.75
	CVE-2000-0800 (10.0)	0.5	5	

With three time periods-8:00 to 9:00, 9:00 to 10:00, 11:00 to 10:00, we simulated hackers on the Web server, FTP server and Oracle database server to launch denial of service attacks (Denial of Service, DoS), FTP buffer overflow attacks and Root privilege escalation attack. The vulnerable points of the attack are shown in Table 5.

Table 5. The use rule of vulnerable points

Atomic Attack	Pre-Condition				Post-Condition
	src_priv	dst_priv	vul_id	connection	
Denial of service	Root	User	CVE-2011-1871	A→C	User
ftp buffer overflow	Root	User	CVE-2004-2111	A→B	User
Root authority promoting	Root	User	CVE-2000-0800	A→D	Root

The first time interval: 8:00-9:00, Web server C launched DoS attacks, the status of attack and defense, as shown in Fig. 8.

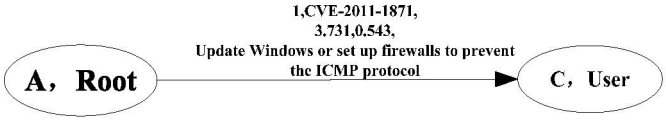

Fig. 8. The first time interval of state offensive and defensive diagram

The attack frequency of each server node is shown in Table 6.

Table 6. The first time interval attack detection results

attack \ node	Web server	FTP server	Oracle server
ftp buffer overflow	0	0	0
Root authority promoting	0	0	0
DoS	5	0	0

Table 6 shows that the time DoS attack happened in only a Web server, DoS attacks by using the weak point of CVE - 2011-2011. According to the formula 2 and 3, we can calculate the probability of the atoms successful attack is 0.543. According to the formula 4, we can calculate the atomic attack damage index is 3.731. By the formula 5 and Table 6 attack frequency, we can calculate the atomic attack safety risk is 26913.48913. Combining with the Web server vulnerabilities risk, by formula 6, the Web server security risk value is 26920.09283.

However, the FTP server and Oracle database server did not take any attack, their safety risk security risks for its vulnerable points only 7.29315 and 8.75 respectively. According to table 1, the Web server, FTP server, and Oracle database server weight are 0.19, 0.25 and 0.25 respectively. And the whole network safety risk of the first time interval is 5189.

The second time interval: 9:00-10:00, we continue to strengthen the Web server C to DoS attack, at the same time to the FTP server B FTP buffer overflow attack, attack and defense figure as shown in Fig. 9.

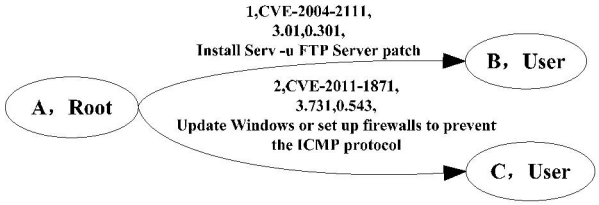

Fig. 9. The second time interval of state offensive and defensive diagram

The attack frequency of each server node is shown in Table 7.

Table 7. The second time interval attack detection results

attack \ node	Web server	FTP server	Oracle server
ftp buffer overflow	0	1	0
Root authority promoting	0	0	0
DoS	10	0	0

DoS attacks happened to the Web server, FTP buffer overflow attacks have taken place in FTP server at this time interval. According to the above same calculation method, the vulnerabilities used by the DoS attacks is CVE - 2011-2011. According to the formula 2 and 3, we calculated that the probability of the atoms successful attack is 0.543. According to the formula 4, the atomic attack damage index is 3.731. By the formula 5 and Table 7 attack frequency, the atomic attack safety risk is 53826.97825. Combining with the web server vulnerabilities risk, the web server security risk value is 53833.58195 by formula 6.

FTP buffer overflow vulnerabilities are used by the attack of CVE - 2004-2004. According to the formula 2 and 3, the probability of the atoms successful attack is 0.301. According to the formula 4, the atomic attack damage index is 3.01. By the formula 5 and Table 7 attack frequency, the atomic attack safety risk is 1023.29299. Combining with the FTP server vulnerabilities risk, by formula 6, the web server security risk value is 1030.58614.

However, the Oracle database server does not take any attack, their safety risk security risks for its vulnerable points is 8.75. According to table 1, the Web server, FTP server, and Oracle database server weight are 0.19, 0.25 and 0.25 respectively. And the whole network safety risk of the second time interval is 10488.

The third time interval: 10:00-11:00. We continue to do FTP buffer overflow attack by FTP server B, at the same time to the Oracle database server D take elevated privileges Root attack, Stop the DoS attack on the Web server B, and the status of the attack and attack graph is shown in Fig. 10.

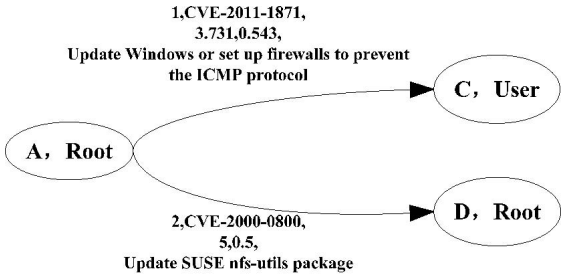

Fig. 10. The third time interval of state offensive and defensive diagram

The attack frequency of each server node is shown in Table 8.

Table 8. The second time interval attack detection results

attack \ node	Web server	FTP server	Oracle server
ftp buffer overflow	0	1	0
Root authority promoting	0	0	1
DoS	0	0	0

FTP buffer overflow attacks took place in FTP server, Oracle server had a root privilege escalation attack at this time interval. According to the above same calculation method, the vulnerabilities used by the FTP buffer overflow attacks is CVE-2004-2111. According to the formula 2 and 3, the probability of the atoms successful attack is 0.301. According to the formula 4, the atomic attack damage index is 3.01. By the formula 5 and Table 8 attack frequency, the atomic attack safety risk is 1023.29299. Combining with the Web server vulnerabilities risk, by formula 6, the web server security risk value is 1030.58614.

Root permissions to enhance the vulnerability of the attack is CVE-2000-0800. According to the formula 2 and 3, the probability of the atoms successful attack is 0.5. According to the formula 4, calculate the atomic attack damage index is 5. By the formula 5 and Table 8 attack frequency, the atomic attack safety risk is 100000. Combining with the Oracle server vulnerabilities risk, the web server security risk value is 100008.75 by formula 6,.

However, the web server did not take any attack, their safety risk security risks for its vulnerable points is 6.6037. According to table 1, the web server, FTP server and Oracle database server weight are 0.19, 0.25 and 0.25 respectively. And the whole network safety risk of the third time interval is 25261.

The experimental results show that the network security risk mainly comes from the attack security risks, vulnerabilities have not been successfully used by an attacker, the potential safety risk is relatively small. We can see clearly from Figure 8, the network security risk is minimum in the first time interval, in the middle for the second time interval and the third time interval has the highest security risks. Compared with the first time interval, why the second time interval is less is due to the fact that web server has an increase of number of DoS attacks and FTP buffer overflow attacks is added on the FTP server, so the network security risk has been a significant increase compared with the first time interval. In the third time interval, while we stopped the Web server's DoS attack, only launched FTP server buffer overflow attacks on an FTP and open a Root access to the Oracle server attack, the total number of attacks has an

obvious drop comparing with the two time intervals before, but as a result of attack damage index is larger, so instead of a further increase in the risk of the third time interval, a high hazard index further verified against the security risk than many middle and low hazard index against risk. At the same time, the experiment is also presented to verify the validity and rationality of network security risk assessment method which is put forward in this paper.

5 Conclusion

This paper proposes a network risk assessment method based on the offensive and defensive state graph model. This method makes the results of multiple vulnerabilities scanner as data source, the individual vulnerabilities scanner accuracy as confidence, scanning result set as a confidence vectors, then analyzes the offensive and defensive state graph on every confidence level vector and calculate the single offensive and defensive figure vulnerable points. In three different times of the attack scenarios, the proposed method is employed in a small local area network risk assessment. Experiments show that this risk assessment method can correct the evaluating of the network security risks, and the evaluation results are more in line with the actual situation and can give quantitative risk values directly.

Reference

[1] P. A. Porras, M. W. Fong, A. Valdes, A mission-impact-based approach to INFOSEC alarm correlation, in: D. Balzarotti, S. Stolfo, M. Cova (Eds.), Recent Advances in Intrusion Detection- 15th International Symposium, RAID 2012, Amsterdam, The Netherlands, September 12-14, 2012, 95-114.

[2] S. Boyer, O. Dain, R. Cunningham, Stellar: a fusion system for scenario construction and security risk assessment, in: Proc. 13th IEEE International Workshop on Information Assurance, 2015.

[3] A. Gehani, Support for Automated Passive Host-based Intrusion Response, Duke University Department of Computer Science, Durham, 2013.

[4] S. Hariri, G. Qu, T. Dharmagadda, M. Ramkishore, C.S. Raghavendra, Impact analysis of faults and attacks in large-scale networks, IEEE Security & Privacy 11(5)(2013) 49-54.

[5] Q.M. Li, J. Li, Rough outlier detection based security risk analysis methodology, China Communications 9(7)(2012) 14-21.

[6] W.-H. Ma, Y.-C. Guo, H.-B. Zhang, Research on the security of multiple execution mechanisms, Software 36(6)(2015) 83-87.

[7] P.-R. Fang, G. Tang, X.-N. Cheng, Security analysis of WPA/WPA2 protocol, Software 36(1)(2015) 22-25.

[8] Q.-Y. Wu, Q.-H. Zheng, P. Wang, A scalable network user behavior log acquisition method, Software, 35(10)(2014) 21-25.

[9] C. Philips, L.P. Swiler, A graph-based system for network-vulnerability analysis. in: Proc. 1998 Workshop on New Security Paradigms, 1998.