Forest Chemicals Review
www.forestchemicalsreview.com
ISSN: 1520-0191
January-February 2022 Page No.324-331
Article History: Received: 28 October 2021 Revised: 05 December 2021 Accepted: 10 January 2022 Publication: 28 February 2022

Research on Network Security Defense Model Based on Combination Strategy of Firewall and IPS

Dafei Wu[1*]

[1]College of Information Engineering, Hunan University of Science and Engineering, Yongzhou, Hunan, China

*Corresponding Author.

Abstract:

Firewall and intrusion detection system are widely used network security protection equipment, which plays a vital role in preventing network attack and intrusion. However, they have inevitable defects, which reduces the protection function provided in actual use. Therefore, in order to further improve network security, this paper designs a new network security protection technology which can integrate the advantages of multiple security technologies and make up for their shortcomings. This paper proposes a network security defense model based on the combination strategy of firewall and IPS. The purpose of policy based intrusion prevention system (pb-ips) is to realize the real combination of security management and network management system. This can take the network management system as the intermediary, integrate the firewall technology and intrusion detection technology, and realize a new network security protection measures.

***Keywords**: Firewall, intrusion detection system, network security, IPS combination strategy.*

I. INTRODUCTION

With the vigorous development of the network, the global network security problem is becoming more and more serious. CERT/CC pointed out in the attack trend report in 2002 that the trend of network attacks is evolving towards the direction of increasing the update speed of attack tools, increasing the complexity of attack tools, increasing the vulnerability detection speed, enhancing the penetration ability of firewalls, increasing asymmetric threats and increasing attacks on network infrastructure [1-2]. In the deteriorating network security environment, aiming at different types of security problems, network security managers usually use different security devices to defend and build a hierarchical defense system [3]. This makes related security products such as firewall, VPN, IDS, anti-virus, identity authentication, data encryption, security audit and other security protection and management products widely used in the network. Although the existing network security devices (such as IDS, firewall, anti-virus software, etc.) can play a role in a specific direction and level. However, these devices are often limited to dealing with single point and single security problems, can not support and cooperate with each other, and there is no effective unified management and scheduling mechanism between them, so they can not meet the monitoring and control requirements of global network, especially large-scale network security [4-5]. Therefore, it is necessary to study related technologies to solve these problems.

II. RESEARCH ON NETWORK SECURITY SITUATION ASSESSMENT METHOD BASED ON INFORMATION ENTROPY

1.Situation assessment

In fact, the occurrence of security problems with real threat often requires diverse conditions, which are reflected in the log information of each security device. Security situation value provides a macro alarm method, and security situation assessment combines the internal relationship of security information data with the internal characteristics of some security events. When the outbreak of certain events meets certain characteristics and laws, the security situation assessment can draw corresponding judgments according to these phenomena, and inform the administrator of what security threats may occur and what the future development trend will be [6]. Because the security situation information source contains a lot of noise, even if the system has vulnerabilities, it may not affect the system security because its utilization conditions are not met. In this way, the number of security events or vulnerabilities cannot directly represent the security status of the system [7-8]. Therefore, how to reasonably calculate the security situation value is a difficult problem in the field of security situation assessment.

One of the important characteristics of entropy law is its equivalence. One irreversible process can deduce another irreversible process. Different processes are interrelated, which is the essence of the universality of entropy law. The opening and dissipation effect of the system is inevitable, and it is also a process of increasing entropy. With the increase of various risk factors, the overall influence and harm will be great. From the perspective of network security situation assessment, when the IDS alarm records, firewall logs, viruses, vulnerability reports and other information in the network system increase, the greater the corresponding entropy, the more critical the network security situation is, and vice versa. Therefore, combined with the uncertainty in the process of network security situation assessment and the characteristics that some indicators are difficult to accurately evaluate quantitatively and qualitatively, the following main contents of this paper will discuss the relevant principles and concepts of information entropy and apply it to network security situation assessment.

2.Information entropy

In thermodynamics and statistical mechanics, entropy is a physical quantity that reflects the irreversibility of macro spontaneous process, and its size reflects the stability of the state of the system. According to Boltzmann relation, such as formula (1), entropy S is a physical quantity reflecting the disorder degree of micro particles in the system; In addition, entropy is also a measure of uncertainty of random variables. From the historical evolution and application of the concept of entropy, entropy has become a method to describe the micro state of the system in the theory of system science, and the general theory of system evolution also believes that "once the cognitive object is treated as a system, in order to obtain knowledge about the system, we can only focus on understanding the state of the system".

$$S = kInW \quad (1)$$

Where: K - Boltzmann constant

W - the number of states contained in the macro state of the system.

Entropy increasing principle: for reversible processes in an isolated system, the entropy of the system always remains unchanged; For irreversible processes, the entropy of the system always increases. The increase of entropy indicates that the system evolves from a state with low probability to a state with high probability. In a general sense, entropy increase means that the system evolves from a more regular and orderly state to a more irregular and disorderly state.

$$I(xi) = -logp(xi) \quad (2)$$

The amount of information contained in the source is defined as the average uncertainty of all possible messages sent by the source. Shannon calls the amount of information contained in the source information entropy,

$$H(x) = -\sum_{i=1}^{q} p(xi)logp(xi) \quad (3)$$

Where: q-number of source messages.

Nowadays, the concept and theory of information entropy have been applied in many fields, such as pattern recognition, machine translation, psychology, genetics, neurophysiology, linguistics, semantics and so on.

3.Network security situation assessment method based on information entropy

From the perspective of the organizational structure of the network, the network is composed of network equipment, security equipment, servers, user PCs and other hosts. Different hosts play different roles in the network and have different degrees of importance. Therefore, their influence on network security is also high or low. For ease of description, we can define some variables and functions involved in situation assessment calculation.

Define 3-1 the information entropy of IDS alarm record reflecting the security of a host as E_{ids}; The vulnerability scanning result reflects that the information entropy of a host security is E_{scaner}; The information entropy recorded by the firewall reflecting the security of a host is $E_{firewall}$; The sniffing result reflects that the security information entropy of a host is E_{snifer} (if there is information provided by other security devices, it can be analogized in turn).

Define 3-2 the information entropy of each host reflecting network security as E_{host}, and the calculation function is:

$$E_{host}\left(k\right)=f\left(E_{ids}\left(k\right),E_{scanner}(k),E_{firewall}(k),E_{sniffer}(k),...\right)\ (4)$$

Where: k - the number of the host in the network, 1 ≤ k ≤ N

N - number of hosts in the entire network

Definition 3-3 network security situation value SituationTrend is determined by the information entropy of network security reflected by all hosts in the network, and the calculation function is:

$$SituationTrend=f\left(E_{host}\left(1\right),E_{host}(2),E_{host}(i),...,E_{host}(N)\right)\ (5)$$

Where: i - the number of the host in the network, 1 ≤ i ≤ N

N - is the number of hosts in the entire network

III. RESEARCH ON A COMBINED NETWORK SECURITY SITUATION PREDICTION METHOD

1.Two prediction models

ARMA (auto regressive and moving average) is a model family, which is composed of three basic types: autoregressive (AR) model, moving average (MA) model and autoregressive moving average model. The autoregressive model AR (P) expresses the observed value at the current time by the observed value at the past several historical times and a random interference term at the current time; The moving average model MA (q) is a linear combination of white noise sequences called random interference to express the observed values at the current time; The combination of AR model and MA model is ARMA model. If the time series yt is a linear function of its current and previous random error terms and previous values, it can be expressed as:

$$y_t=\phi_1 y_{t-1}+\phi_2 y_{t-2}+...+\phi_p y_{t-p}+\theta_1 u_{t-1}-\theta_2 u_{t-2}-...-\theta_q u_{t-q}\ \ (6)$$

Formula (6) is the autoregressive moving average model of order (p, q), which is recorded as ARMA (p, q).

Where: $\phi_1,\phi_2,\ldots,\phi_p$ - autoregressive coefficient, the parameter to be estimated of the model

$\theta_1,\theta_2,\ldots,$ θq - moving average coefficient, the parameter to be estimated of the model

ut- random term, a mutually independent white noise sequence, obeys a mean of 0 and a variance of δu Normal distribution of.

Obviously, AR model and MA model are special cases of ARMA model, that is, for ARMA (p, q), if order q = 0, it is autoregressive model AR (p); If the order p = 0, it becomes the moving average model MA (q).

If we calculate the autocorrelation function and partial autocorrelation function of the sequence, we can identify its tailing and truncation characteristics according to the drawing method, and then judge the values of p and q of the model according to table 1.

TABLE I. ARMA model identification principle table

MODEL	AUTOCORRELATION FUNCTION	PARTIAL AUTOCORRELATION FUNCTION
AR(p)	Trailing	P-order truncation
MA(q)	Q-order truncation	Trailing
ARMA(p, q)	Trailing	Trailing

Because the network security situation value is a column of dependent random variables, and each order autocorrelation coefficient describes the strength of the relationship between the situation values with time delay. Therefore, according to the basic idea of exponential weight Markov chain prediction, it can be considered to predict the situation value at that time according to the situation value at several previous times. Then, according to the weighted sum of the dependence between the previous time and the time, the purpose of making full and rational use of information for prediction can be realized.

When forecasting the network security situation, we can first divide the change interval reflecting the strength of the network security situation; Then, the weighted Markov chain is used to predict the future strength change of the situation with the weight of each order autocorrelation coefficient normalized by the network security situation value sequence. The weight calculation steps are as follows:

(1) sCalculate the autocorrelation coefficients rk, k ∈ E of each order

$$r_k = \frac{\sum_{l=1}^{n-k}\left(x_l - \overline{x}\right)\left(x_{l+k} - \overline{x}\right)}{\sum_{l=1}^{n}\left(x_l - \overline{x}\right)^2} \quad (7)$$

Where, rk represents the k-th order autocorrelation coefficient; xl represents the security situation value at time l, and x represents the average value of historical security situation value; n represents the length of the security situation value sequence.

(2) Normalize the autocorrelation coefficients of each order, i.e

$$w_k = \frac{\left|r_k\right|}{\sum_{k-1}^{m}\left|r_k\right|} \quad (8)$$

(3) It is taken as the weight of Markov of each lag time (step) (M is the maximum order calculated according to the prediction demand).

Markov model is based on the probability of state transition, so it is necessary to determine the state of network situation, that is, to group the evaluation values of network security situation by some grouping method; After grouping, the frequency matrix is counted, and then the state transition probability matrix is determined; Then see whether it satisfies the Markov property, that is, test the "Markov property"; If the Markov property is satisfied, the state transition probability matrix and the corresponding autocorrelation coefficients of each order are weighted, and the state with the largest probability after weighting is taken as the prediction state.

2.Combined prediction model of network security situation

Combined forecasting is an effective comprehensive forecasting method developed in recent years. It has been well applied in other fields, but this kind of model has not been applied in the prediction of network security situation. Combined forecasting method is to establish a combined forecasting model, combine several forecasting methods according to their respective weights, and finally get a combined forecasting result for analysis and decision-making. The advantage of combined forecasting method is that it can absorb the information of various forecasting methods to a great extent, which is more systematic and comprehensive than a single forecasting model. The main purpose of combined prediction is to reasonably combine several different prediction methods, make full use of the information provided by each prediction method, and improve the prediction accuracy as much as possible. In combination forecasting, an important content is the selection of the weight of each forecasting model. This paper uses the error of the previous forecasting result to determine the weight of the next forecasting.

The purpose of using the combined forecasting method is to improve the forecasting accuracy, and the key to improve the accuracy lies in how to determine the weight WJ. Common weight calculation methods include average method, reciprocal of variance method, reciprocal of mean square method, simple weighting method and binomial coefficient method. In this paper, ARMA prediction model and Markov prediction model are combined, and the weight of the next prediction is determined based on the error of the previous prediction result. The combined prediction model is shown in equation (9).

$$\hat{y}_t = \frac{\left|e_{a(t-1)}\right|}{\left|e_{a(t-1)}\right| + \left|e_{m(t-1)}\right|} \cdot y_{mt} + \frac{\left|e_{m(t-1)}\right|}{\left|e_{a(t-1)}\right| + \left|e_{m(t-1)}\right|} \cdot y_{at} \quad (9)$$

Where: yt - combined predicted value at time t

yat, $e_{a\ (t-1)}$ - prediction value of ARMA model and its prediction error at the previous time

The prediction value of ymt, $e_{m(t-1)}$ - Markov model and its prediction error at the previous time

IV. RESEARCH ON INTRUSION INTENTION RECOGNITION METHOD BASED ON

HMM

Hidden Markov model (HMM) is a statistical model. It is mainly used to describe a Markov process with unknown parameters. It can be regarded as the simplest dynamic Bayesian network. HMM was first proposed in a series of statistical papers by Leonard Baum in the late 1960s, and began to be applied to the field of speech recognition in the 1970s. It was applied to DNA sequence analysis in the late 1980s.

In the Markov model, the state is directly visible to the observer, so the transition probability of the state is all the parameters of the whole model. In HMM, the state is not directly visible, but some variables affected by the state are visible, and each state has a probability distribution on the possible output symbols, so that the sequence of output symbols can characterize some information of the state sequence.

A system described by HMM can be used to solve three basic problems, namely evaluation, decoding and learning.

(1) Evaluation. The evaluation problem is to find the probability of an observation sequence through a given HMM. Suppose we have some HMM describing different systems and an observation sequence, we want to know which HMM is most likely to produce this given observation sequence. To solve this problem, the forward algorithm is usually used to calculate the probability of an observation sequence after a given HMM, so the most appropriate HMM is selected.

(2) Decoding. The decoding problem is to search for the most likely hidden state sequence given the observation sequence. To solve this problem, Viterbi algorithm can be used.

(3) Learning. The learning problem is to generate an HMM for a given observation sequence, that is, estimate the most appropriate HMM according to an observation sequence and a hidden state set related to it, that is, determine the most appropriate (π, A, B) triplet described by the known sequence. To solve this problem, when matrices A and B cannot be estimated or measured directly, forward backward algorithm can be used for learning.

In addition, when the output sequence is known to find the most possible state transition and output probability, Baum Welch algorithm and reversed Viterbi algorithm are usually used. Some recent methods use junction tree algorithm to solve these problems.

V. CONCLUSION

Based on the analysis of the related research of network security situation, this paper discusses and puts forward the research methods of related directions for the evaluation and prediction technology of network security situation. A network security situation evaluation method based on information entropy is proposed. The experimental results show that this method can effectively evaluate the network security situation, assist the network security managers to identify the security problems in the network and find the development trend of the network security situation. Combined with the concepts, principles and specific prediction methods of ARMA model and Markov model, a combined prediction method is proposed. The experimental results show that compared with a single prediction method, the combined prediction can predict the network security situation more accurately. The research on network security situation is a comprehensive subject with great breadth and depth. From the perspective of theoretical research, the existing research has not established a unified theoretical basis; From the perspective of application research, there is no perfect system product in the industry. Therefore, there are still many directions worthy of in-depth research.

ACKNOWLEDGEMENTS

This research was supported by the Hunan University of Science and Technology Application Characteristic Discipline Construction Project, Thirteenth Five-Year Plan Specialty Comprehensive Reform Pilot Project of General Colleges and Universities in Hunan Province ([2016] No. 276).

REFERENCES

[1] Bai Dongming, Zeng Lihua.Thoughts on the construction of enterprise network security defense system based on the integration of offense and defense. Information System Engineering, 2021(8): 68-70.

[2] Liu Gang, Li Qianmu, Zhang Hong. Network security defense strategy generation method based on state attack and defense graph model. Computer Applications, 2013, 33(S1): 121-125.

[3] Wang Chencan, Xu Yangbin, Fan Yige. Implementation of Computer Network Security Defense System and Analysis of Key Technologies.Network Security Technology and Application, 2021(5): 20-22.

[4] Huo Chengyi ,Zhen-qiang wu. Research on Network Security Dynamic Defense Model. Information Security and Communication Secrecy ,2006 (12): 105-107.

[5] Li Yan, Ma Xudong. Implementation of Computer Network Security Defense System and Key Technology Analysis. Electronic Technology and Software Engineering, 2021(10): 249-250.

[6] Li Shuhua, Chen Chengxin, Zhang Xuanyi. The key points of network security defense strategy: inspiration and thinking of a model. Information Magazine, 2019, 038(010):90-95,126.

[7] Liu Yun. SYN Flood defense method based on lightweight detection and hybrid connection strategy. Computer Applications and Software, 2016, 33(11):310-313.

[8] Zhang Feng.Research on network security active defense model based on strategy tree. Doctoral dissertation of University of Electronic Science and Technology of China., 2005.