Application of attack tree theory in network information security penetration testing

Mingfeng Li[1], Deyu Yuan[1*], Mianning Hu[1]
1. School of Information and Network Security, People's Public Security University of China, Beijing, 100038, China
lmf_ppsuc@sina.com

Abstract: This paper firstly discusses the strategies and processes under network information security penetration testing techniques, and extends the attack countermeasure tree using attack tree theory. Secondly, the probability of the attack countermeasure tree model is calculated and the model is generated, and the network information security penetration testing model is constructed based on the attack countermeasure tree. Finally, the real attack machine and target machine are built on the virtual platform with the engineer station network as an example to simulate the penetration testing process. The results show that: in network information security, the probability of occurrence of attacks through network switch reserved interface access, obtaining system driver and USB interface access in three ways are 0.548, 0.492 and 0.475 respectively. The way with the greatest attack effect is to execute SQL injection attack through windows vulnerability, and its evaluation result is 0.9834. Thus it shows that using attack tree theory can be effective penetration testing of network information security, and in this way to help network information security to provide targeted protection recommendations.

Keywords: network information security; attack tree theory; attack

countermeasure tree; penetration testing; attack effectiveness

1. Introduction

The rapid development of the network era has brought convenience to people while network information security threats come along with it. The development trend of the whole network information security industry at the technical level also makes the attackers' methods more and more sophisticated [1-4]. With the increase in cyber threats, more and more companies are making network information security a top priority. Network information security professionals actively install patches and configuration management, continuously monitor system defenses and ensure that they securely configure systems and all applications [5-8]. However, no matter how diligent they are, attackers may still find security vulnerabilities to breach the network's defenses and steal data.

Network attacks have always been a thorny issue in network information security, and the U.S. Information Assurance Forum also pointed out that with the continuous development of network communication technology, the means of network attacks have become gradually more complex [9-10]. Network penetration testing is to simulate the whole process of network attacks from the attacker's point of view, and the process of penetration testing will reveal the weaknesses in the network system and the effects caused by various types of network attacks [11-13].

In order to set and fix the network defense strategy, so penetration testing and network attacks are inseparable. Penetration testing is essentially the same process as implementing a network attack, which requires discovering and exploiting security flaws in the target network system, except that the entire process is secure and controlled [14-16].

This paper takes network information security penetration testing technology as an entry point, discusses the strategy and process of penetration testing respectively, and gives the basic structure of the attack tree model. Based on the attack tree model, the attack countermeasure tree model is extended, and then the probability calculation method and model generation method of the model are given. A network information security penetration test model is constructed based on the attack countermeasure tree, and in order to verify the effectiveness of the model, a simulation penetration test analysis is conducted. The results show that effective penetration tests can be conducted for network information security using the attack tree theory, and then provide data support for network information security protection.

2. Literature review

Penetration testing is an effective means to test and evaluate network information security by simulating real malicious attacks and checking the fault tolerance and security metrics of the target system.Guangxu Y

constructed a contextual feature extraction method based on machine learning in order to be able to better target network information security detection. And it is shown that the method can perform network information security detection in massive network data with good generalization ability and robustness [17]. Lu H J et al. constructed a WiFi penetration testing method based on Kali Linux for vulnerabilities in wireless network information security. The simulation of monitoring, scanning, data capture, and data analysis of wireless networks by this method showed that it can effectively improve the information security assessment of wireless networks [18]. Chen Z et al. discussed the impact of network penetration attacks on network security issues and detected network penetration attacks using an ant colony classification rule mining algorithm. The results show that the method can effectively target the detection of security vulnerabilities in power IoT and improve the effectiveness of the attack detection method [19].

In addition, Rak M et al. analyzed the effectiveness of the application of the security assessment expert system in identifying threats, vulnerabilities, and attacks in the IoT ecosystem and showed that the system can effectively help testers to perform network information security penetration testing and provide effective treatment solutions for IoT ecosystem security [20]. Nuno Antunes et al. analyzed SQL injection vulnerabilities by example in network information security testing work

under the detectability and using three innovative testing tools for network penetration testing. The results show that the three tools can be adapted to network information security penetration testing in different scenarios and have a wider coverage and higher identification rate [21]. Lee Y et al. analyzed for the association between node attributes in the network structure and showed that the network topology makes a certain network dependency between node attributes. And the analysis was carried out using adjacency matrix, which showed a nonlinear and high-dimensional network dependence between the network structure and node attributes [22].

3. Penetration testing model construction based on attack tree theory

The purpose of penetration testing is to invade the target system, obtain valuable information of the target system and implement non-destructive attacks by means of security technology, and finally compile the invasion path and the impact on the system after implementing the attacks into a penetration test report, and put forward reasonable defense suggestions for the system vulnerability found during the penetration test to enhance system security. This chapter is based on the attack tree theory for the construction of penetration testing models, as a way to illustrate the effectiveness of the application of attack tree theory in network information

security penetration testing.

3.1 Network information security penetration testing techniques

3.1.1 Penetration testing strategy

To complete a penetration test, it is necessary to meet both the software aspects and the hardware requirements at the same time. For hardware, the main elements are basic network equipment, vulnerability port scanners, key servers dedicated to penetration testing, etc. For the software, operations and maintenance engineers and network security engineers are the core, simulating the non-destructive attack behavior of hackers under the guidance of the engineers' implementation. In the process of implementing the combination of hardware and software together, the penetration testers record the specific test operations and the related data generated, and finally form a documented statement of results to be presented to the client.

Depending on the specific objectives to be achieved and the amount of information available to the tester, the existing penetration testing strategies are classified as shown in Figure 1.

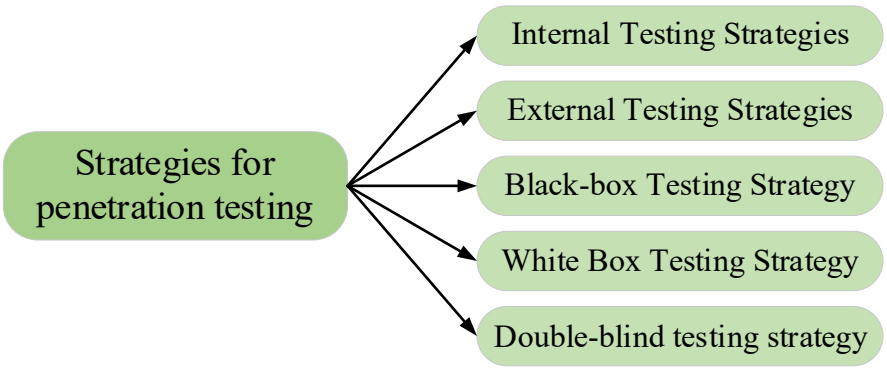

Figure 1 Penetration testing strategy classification

3.1.2 Penetration testing process

Penetration testing is carried out by testers who simulate the behavior of hackers to perform attacks on the network to detect the vulnerability of the system. The process can be divided into three phases, i.e., information gathering phase, attack phase, and security analysis phase.

(1) Information collection phase

The information gathering phase is mainly to collect information related to the target system to prepare for the next phase of the attack. Figure 2 shows the techniques used in this phase, specifically address scanning, operating system scanning, port scanning, and vulnerability scanning.

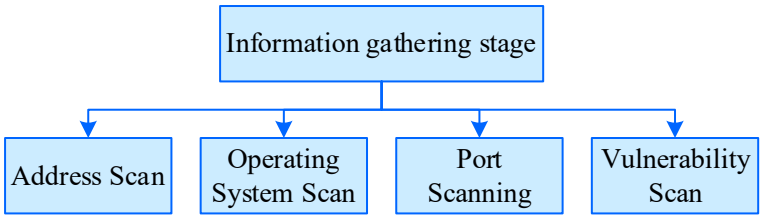

Figure 2 Scanning technology at the information collection stage

To collect information about the system, we first discover the surviving hosts in the target network, then scan the information of each host in the network to understand the operating system, ports, protocols and vulnerability status of the hosts, and finally capture packets to understand the port communication between hosts.

(2) Attack Phase

The attack phase is the most critical and challenging step in the penetration testing process. Testers should make full use of the target system information collected in the previous phase to plan the penetration path that has the greatest impact on how to obtain higher privileges on the target system and attack the target system with the thinking of an intruder, and then implement the attack on the target system according to the attack path.

(3) Security analysis stage

In the information collection phase and the attack phase, the tester is standing in the intruder's point of view for attack testing, but in the security analysis of the system, the tester needs to stand in the user's point of view, analyze the vulnerabilities in the target system and the impact on the system operation after the application of vulnerabilities, and propose corresponding defense measures for the target system vulnerabilities to improve the overall security defense level of the system.

3.2 Attack tree theory and attack countermeasure tree model

3.2.1 The basic structure of the attack tree model

An attack tree is a multi-layered tree structure that includes a root node, a non-leaf node, and a leaf node. In an attack tree, the root node of the tree represents the attacker's final attack goal to be achieved, the non-leaf nodes represent the intermediate steps to be completed to achieve the final goal, and the leaf nodes represent the specific attack behaviors and methods. Each branch of the attack tree represents a path that may be taken to reach the final goal.

The nodes of the attack tree have the following three relationships, namely, the “or (OR)” relationship, the “with (AND)” relationship, and the “sequential with (SAND)” relationship. The “OR” relationship means that if the attack target of any child node is achieved, the target of its parent node will also be achieved. The “with (AND)” relationship means that the attack goals of all child nodes are realized before the goals of their parents are realized. The “sequential with (SAND)” relationship indicates that the attack goals of all child nodes are realized in order for the goals of their parents to be realized. Figure 3 shows the node relationships in the attack tree model.

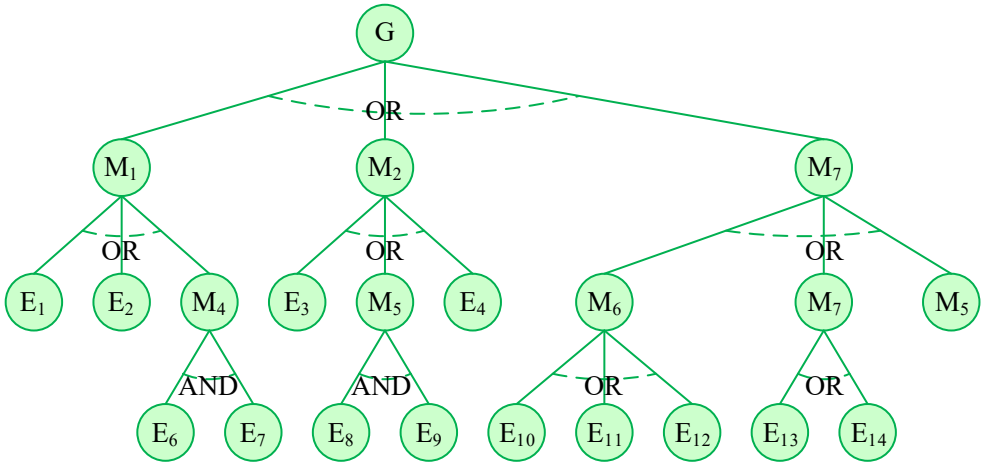

Figure 3 Node relationships in the attack tree model

In the figure, the root node G represents the attacker's final attack target, i.e., the server's firmware, the leaf nodes represent the various attacks taken, i.e., specific attack events, and the intermediate nodes represent the intermediate steps of the attack.

Let P_m be the probability of realization of the parent node and $P_{m1}, P_{m2}, ..., P_{mn}$ be the probability of realization of each child node under it. For nodes with AND relationship, the realization probability of the parent node is the product of the realization probabilities of each child node under it, i.e:

$$P_m = P_{m1} \times P_{m2} \times ... \times P_{mn} \tag{1}$$

For a node with OR relationship, the realization probability of its parent node is the maximum of the realization probability of each child node under it, i.e:

$$P_m = \max\{P_{m1}, P_{m2}, ..., P_{mn}\} \tag{2}$$

3.2.2 Attack countermeasure tree model probability calculation and generation

The Attack Countermeasure Tree (ACT) was proposed by Roy, Kim, and Trivedi at Duke University in 2010 for attack and defense modeling, and the method unifies the respective analysis methods of the attack and defense trees. The attack countermeasure book allows defenses to be added at any node of the tree and the quantitative analysis is extended with a probabilistic component. The theoretical definition of ACT is as follows:

$$ACT = \{V, \psi, E\} \tag{3}$$

Among them,

$$V = \{\forall k, v_k : v_k \in \{A_j\} \| v_k \in \{D_j\} \| v_k \in \{M_j\}\} \tag{4}$$

$$\psi = \{\psi_k : \psi_k \in \{AND, OR, k-of-n\ gate\}\} \tag{5}$$

$$E = \{\forall k, e_k : e_k \in (v_i, \psi_j) \| e_k \in (\psi_i, \psi_j)\} \tag{6}$$

and $X = (x_{A_1} x_{A_2}, ..., x_{D_1} x_{D_2}, ..., x_{M_1} x_{M_2})$ is the state vector of the attack countermeasure tree, where $x_{A_k}, x_{D_k}, x_{M_k}$ is a Boolean variable and is associated with the corresponding event A_k, D_k, M_k.

There are three types of events in the attack countermeasure tree, i.e., attack events, detection events, and mitigation events. The relationship between events belonging to the same parent node has three types of gates including AND, OR, and $k-of-n$. Notice that the last type of gate is not present in the original attack tree, indicating that k events are selected among the n attack events for AND operation, and there is no priority requirement for the selection of these k events.

(1) Probability calculation of attack countermeasure tree model

It should be noted that in this paper, we use the “and not” connector above the nodes of detection and defense events, and define “and not” as a new connector, and the detection and mitigation events below it are calculated according to the actual situation, i.e. “no attack detected” and “attack detected but no mitigation”, then it should be:

$$P_G = \overline{P}_D + P_D \times \overline{P}_M \tag{7}$$

a) If an attack countermeasure tree instance analysis is performed, the probability of a successful direct attack on its corresponding target node is expressed as

$$P_{goal} = P_A \tag{8}$$

b) If an attack event and a detection event are used, the corresponding probability expression for the success of an undetected attack is

$$P_{goal} = P_A(1 - p_D) \tag{9}$$

c) If the detection events are extended to n to detect one attack event, the corresponding attack success probability is expressed as

$$P_{goal} = P_A(1 - p_{D1})(1 - p_{D2})...(1 - p_{D3}) \tag{10}$$

In the attack countermeasure tree, if only detection events are available, then it is considered that the mitigation event is perfect, i.e., mitigation event probability $P_M = 1$. However, if the mitigation event is not perfect $0 < P_M < 1$, it means that the attack countermeasure tree needs to use detection mechanisms in addition to mitigation techniques.

d) When ACT has an attack event and corresponds to a detection event and a mitigation event, the probability of success of its corresponding attack is expressed as

$$P_{goal} = P_A(1 - p_D + p_D(1 - p_M)) = P_A(1 - p_D \times p_M) \tag{11}$$

e) When there is an attack event in ACT corresponding to multiple detection events and a mitigation event, the probability expression for the success of the matching attack is

$$P_{goal} = P_A(1 - (1 - \prod_{i=1}^{n}(1 - p_{D_i})) \times p_M) \tag{12}$$

f) When there is an attack event in ACT corresponding to a detection event and multiple mitigation events, the probability of success of the attack is

$$P_{goal} = P_A(1 - p_D \times (1 - \prod_{i=1}^{n}(1 - p_{M_i}))) \tag{13}$$

g) When the ACT contains an attack event with multiple pairs of detection events and mitigation events, the properties of the triggered mitigation events depend on the properties of the intrusion detection. The probability of its attack success is:

$$P_{goal} = P_A \prod_{i=1}^{n}(1 - p_{D_i} \times p_{M_i}) \tag{14}$$

(2) Generation of the attack countermeasure tree

Like the attack tree, the attack countermeasure tree can also be abstracted as a directed acyclic graph with a root node, and the construction process is a backward reasoning process.

First determine the attack target as the root node of the tree, first construct the attack tree, obtain the preconditions or event combinations required for the occurrence of the root node event through backward analysis, and express the event relationships "with" and "or" and "$k-of-n$". Then continue to expand and extend the sub-targets downward until the nodes in the tree can no longer continue to refine, or have become a specific realization of an atomic attack event, i.e., the leaf node of the attack tree.

In the attack countermeasure tree, two cases are considered to achieve a successful attack, "no attack detected" and "attack detected but no mitigation achieved". The probability calculation is done as described above, and the "detection event" and "mitigation event" are uniformly represented by an "and not" connector. The process of expanding the attack tree into the corresponding attack countermeasure tree is shown in Figure 4.

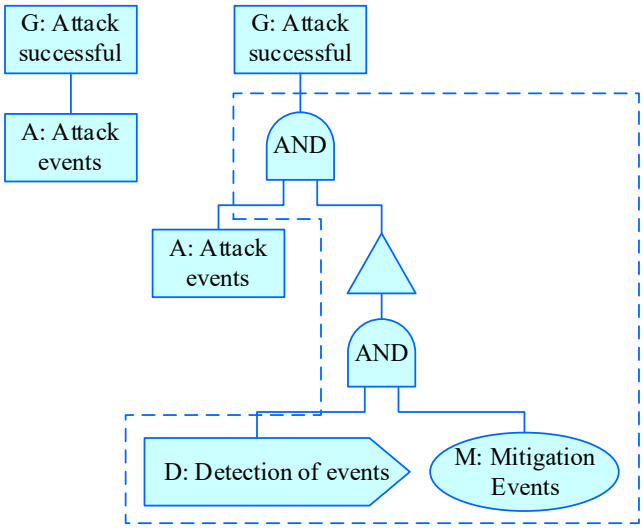

Figure 4 Attack tree extended to attack countermeasure tree

In the actual network information security penetration test modeling, the most critical or interested nodes in the attack countermeasure tree can be selectively refined in depth for different analysis requirements. Through gradual refinement and refinement from the root node to the leaf nodes, a model of all possible attack defense scenarios and related paths against the system target can be built. The attack countermeasure tree construction process is shown in Figure 5.

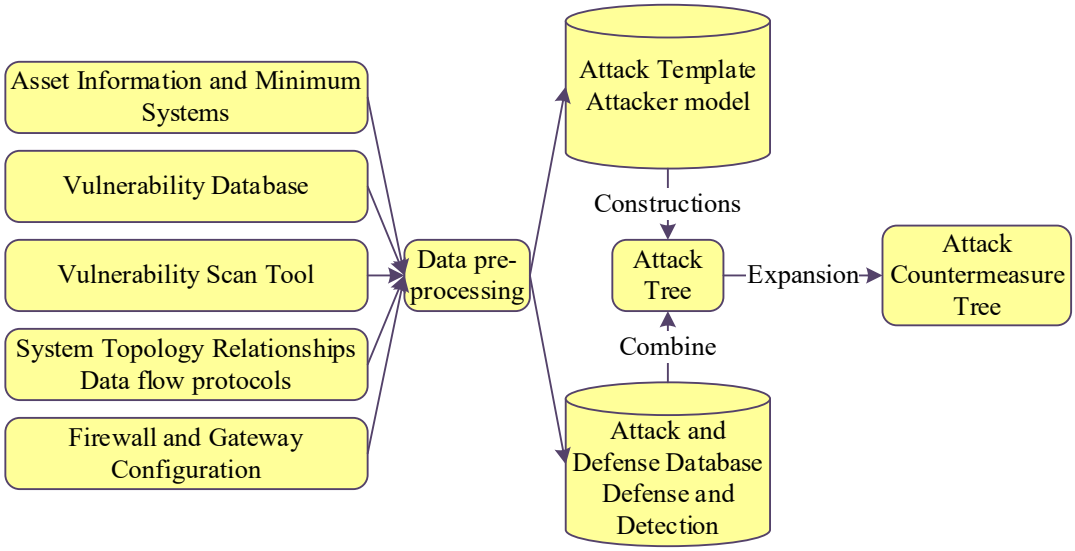

Figure 5 ACT generation process diagram

3.3 Penetration testing model structure based on attack countermeasure tree

Based on the previous paper on the attack tree model and the basic structure of the attack countermeasure tree, this paper gives the penetration test model structure based on the attack countermeasure tree in order to realize the penetration test of network information security. The model

mainly includes four modules, i.e., building attack countermeasure tree, generating attack path, information collection and data pre-processing, and executing network information security penetration test. The structure of the penetration test model based on the attack countermeasure tree is shown in Figure 6.

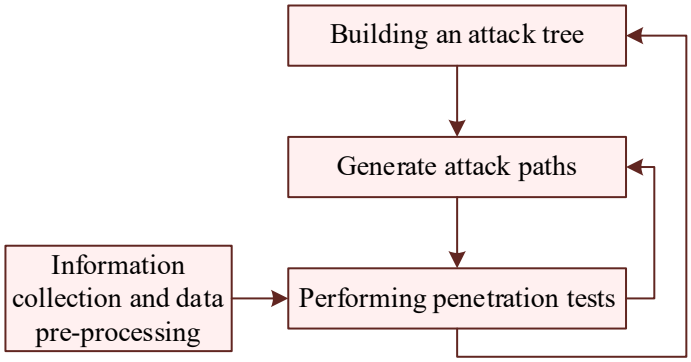

Figure 6 ACT-based penetration testing model

The process of network information security penetration testing model based on the attack countermeasure tree is as follows:

(1) The final target is used as the root node to construct the attack countermeasure tree.

(2) Generate the best attack path based on or node and with node policy.

(3) Collect the target network information and perform data pre-processing, and then execute the penetration test according to the generated optimal path. If the execution is successful, the attack is reported as successful and exits. If the execution is unsuccessful, the next best attack path is found from the attack tree and the penetration test is continued. If

all the paths in the attack tree are traversed without success, the attack tree is reconstructed based on the information obtained from the penetration test and the above process is repeated.

4. Analysis of the application of penetration testing models based on attack countermeasure trees

In this paper, we design the experimental network topology environment, build real attack machines and target machines on the virtual platform, simulate the penetration testing process, and analyze the current network security state of the experimental environment as a whole using the penetration testing model based on the attack countermeasure tree constructed in the previous chapter to verify that the gain-based probabilistic attack graph model has a better global and analytical guidance in the implementation of the penetration testing process. Of course, this experiment ensures that the penetration testing process is controlled and does not involve irregularities.

4.1 Building a countermeasure tree model for engineer station attacks

The Engineer Station is used for configuration and management of the safety level DCS system's own parameters and engineering application data to meet the functional requirements of all phases of engineering design, system commissioning, and operation and maintenance. Its core is the

Engineer Station software, which runs offline on a PC and is capable of generating logic configuration and image configuration program codes, generating engineering configuration information, monitoring variables and status, etc. By studying the relevant configuration information of the engineer station, analyzing its vulnerability, and taking “engineer station under attack” as the root node, an attack tree model is established for the engineer station, the specific structure of which is shown in Figure 7.

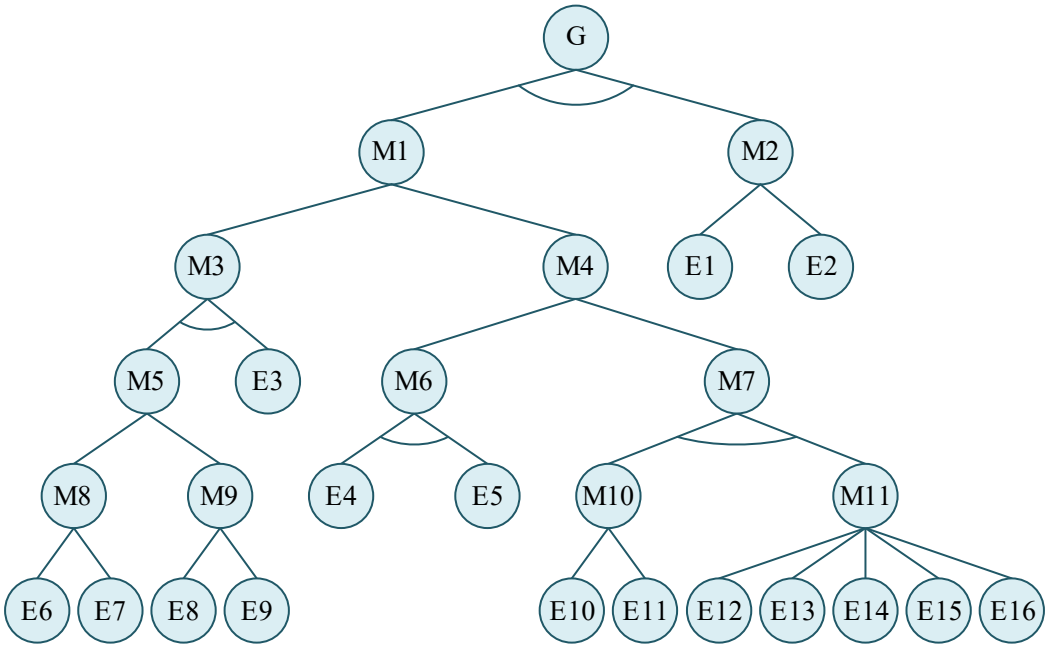

Figure 7 Engineer Station Attack Countermeasure Tree Model

The meanings of the root, middle and leaf nodes of this attack countermeasure tree are shown in Table 1.

Table 1 Meaning of each node in the attack countermeasure tree

Symbols	Meaning	Symbols	Meaning
G	Engineer station under attack	E3	Malicious download of applications
M1	Attack behavior	E4	Obtain system drivers
M2	Access to the site to start and	E5	Connecting to black box attack

	connect to the MTS		tools
M3	Physical attack	E6	Decrypting user logs
M4	Logical attack	E7	Installing special cameras to monitor
M5	Obtain high privilege accounts	E8	Unintentional disclosure
M6	Using black box attacks	E9	Intentional leakage
M7	Malware attacks	E10	USB port access
M8	Use of special hardware	E11	Network switch reserved interface access
M9	Person of interest compromise	E12	windows vulnerability
M10	Reserved interfaces to load malware	E13	SQL injection attack
M11	Writing and running malware	E14	Configuration Software Vulnerability
E1	Person of interest on site	E15	Communication Protocol Vulnerability
E2	Other means of access	E16	Engineer Station Software Vulnerability

4.2 Analysis of the probability of attack occurrence for each leaf node of the attack countermeasure tree

Based on the calculation of the probability of successful attack occurrence for the leaf nodes in the attack countermeasure tree in Section 3.2, this section first scores the attribute values of each leaf node using the expert evaluation method and finds the probability of occurrence of the attack event for each leaf node, and the results are shown in Figure 8.

From the probability of attack of each leaf node, the highest probability of occurrence is 0.548 for E11 node, followed by 0.492 for E4 node, 0.475 for E10 node, and 0.467 for E13 node, which indicates that the highest threat of attack for the engineer station network security system is through the network switch reserved interface access local interface. And

use the database vulnerability of the malicious code into the engineer station, and then execute SQL injection attack to steal data and damage the system. This shows that in the network information security to focus on the switch interface security, and developers need to upgrade the network system access channel and database to ensure its information security protection capabilities.

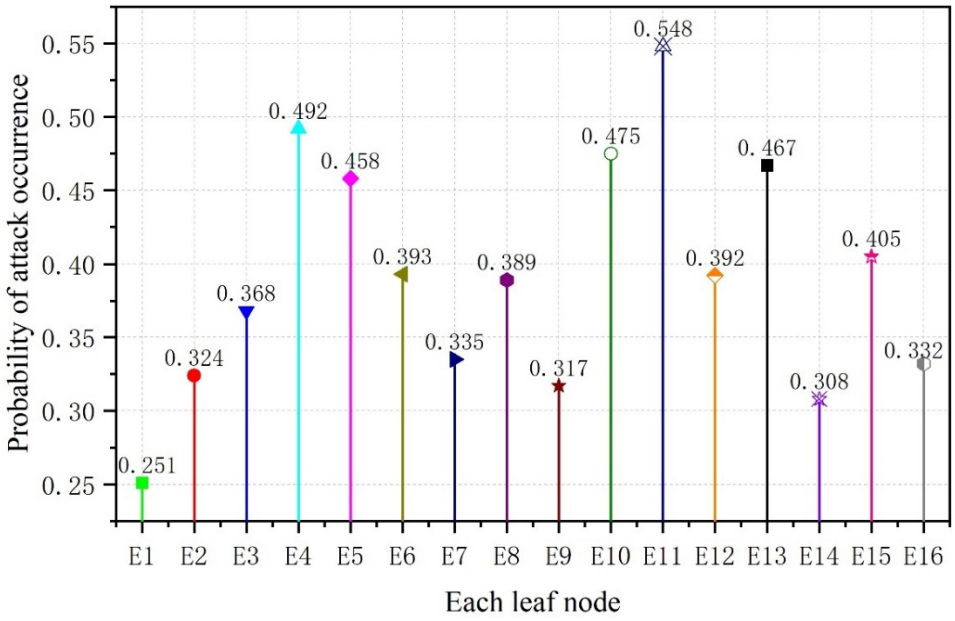

Figure 8 Probability of attack occurrence for each leaf node

4.3 Analysis of the impact coefficients of each leaf node of the attack countermeasure tree

In order to further understand the effect of penetration testing of network information security, this section analyzes the impact coefficients of confidentiality, integrity and availability for each leaf node of the attack countermeasure tree corresponding to vulnerabilities, and the analysis results are obtained as shown in Figure 9.

From the impact coefficient of each leaf node of the attack countermeasure book corresponding to vulnerabilities, the E2 node represented by other ways to approach the impact coefficient is larger, and its confidentiality, integrity and availability impact coefficients are 0.58, 0.45, 0.54. This also indicates that in the process of conducting the analysis of network information security at the engineer's station, there are other ways to approach to make the vulnerability attack more likely to succeed. In the follow-up process, we need to further improve the overall network protection capability of the engineer station to make the protection network of the engineer station cover a wider area and reduce the impact of other ways of approaching. In addition, the availability impact factor of E11 node is 0.55, which indicates that the network switch reserved interface is used to access the engineer station network, which can promote the sharing of network resources in the engineer station. However, as the success probability of attack given in the previous section, this node will also have some impact on network information security, so it needs to be used carefully and enabled under the condition of ensuring network information security to prevent information leakage.

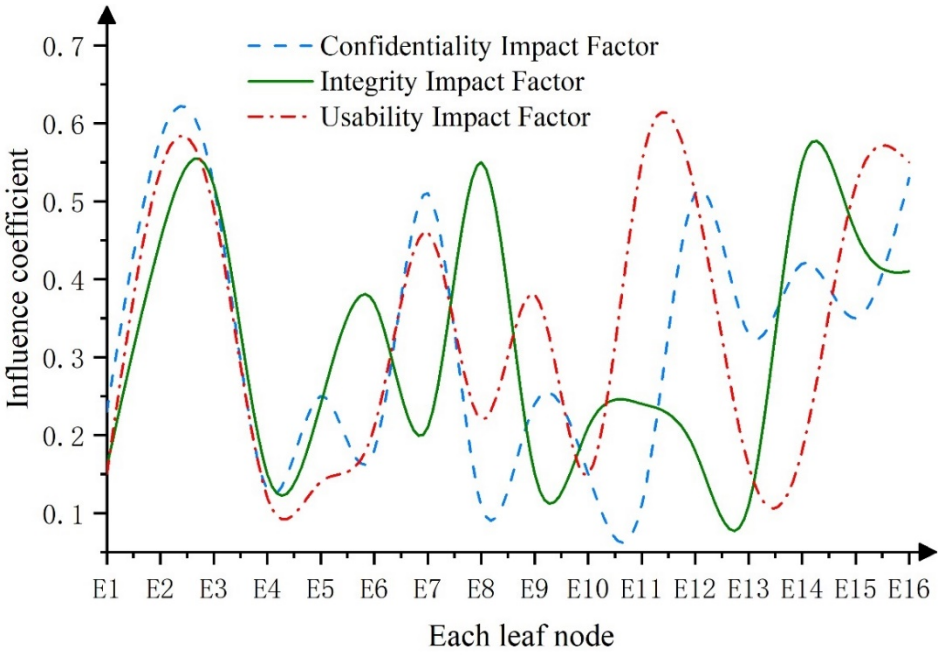

Figure 9 Analysis of the influence coefficient of each leaf node

4.4 Analysis of the evaluation of the attack effect of each attack sequence

In order to further analyze the effect of the attack on the information security of the engineer's station network, the quantitative analysis of the data is carried out using the quantitative assessment algorithm of the attack effect, which is expressed as follows

If multiple vulnerabilities of the same device $l = \in \{1,2,...,L\}$ are used to carry out the attack, the loss generated by the node of the device is expressed as

$$Lost\_H_i = imp_i \cdot \prod_{l=1}^{L} P_{i,l} \cdot (\vec{A}_{i,l} \cdot \vec{w}_{i,l}) \tag{15}$$

Where, imp_i denotes the importance of the device node, $\vec{A}_{i,l}$ denotes the demand weight on the confidentiality, integrity and availability

of the device, and $\vec{w}_{i,l}$ denotes the coefficient of impact of the l th weakness of the i th device on the confidentiality, integrity and availability of the device node.

Without loss of generality, the attack sequence is assumed to be

$$S_j = \{E_{1,l}, ..., E_{i,l}, ..., E_{m,l}\} \tag{16}$$

$$\begin{cases} j = \{1, 2, ..., J\}; i \in \{1, 2, ..., m\} \\ m \in \{1, 2, ..., n\}; l = \in \{1, 2, ..., L\} \end{cases} \tag{17}$$

Then the attack effect is quantified and expressed as

$$AssResult\_S_j = \prod_{i \in \{1,2,...,m\}} Lost\_H_i \tag{18}$$

According to the impact coefficients of confidentiality, integrity and availability of each leaf node given in Section 4.3, the security loss of the device node is obtained using Eq. (15), and the quantitative evaluation results of the attack effect corresponding to each attack sequence are obtained using Eq. (18), and the specific results are shown in Table 2.

Table 2 Evaluation results of attack effect of each attack sequence

Attack Sequence $S_j \in S$	Number of steps	Attack effect
$S_1 = \{E4, E10, E11\}$	3	0.6342
$S_2 = \{E12, E13\}$	2	0.9834
$S_3 = \{E15, E16\}$	2	0.7396
$S_4 = \{E1, E2, E5, E13\}$	4	0.1457
$S_5 = \{E3, E6, E7, E8, E9\}$	5	0.1628

From the quantitative evaluation results of the attack effect of each

attack sequence, we can get the size relationship of each attack sequence as $S_2 > S_3 > S_1 > S_5 > S_4$. The attack method with the largest attack effect is SQL injection attack executed through windows vulnerability, and its evaluation result is 0.9834. This indicates that in order to ensure network information security, we need to upgrade Windows system as soon as possible, update the system virus database, find the vulnerability and timely repair, and thus ensure network information security.

5. Conclusion

In this paper, we analyze the attack tree theory and extend it to the attack countermeasure tree model construction starting from network information security penetration testing technology. A network information security penetration model is constructed based on the attack countermeasure tree, and an empirical analysis is conducted to verify the effectiveness of the application of the model. The following conclusions are drawn:

(1) From the attack probability of each leaf node of the attack countermeasure tree, the top three nodes are network switch reserved interface access, obtaining system driver and USB interface access, and their attack probabilities are 0.548, 0.492 and 0.475, respectively. this indicates that when building a network information security system, it is necessary to do a good job of security detection of the network switch

interface, ensuring that the system driver and reduce the use of USB memory, so as to ensure the security of network information security system.

(2) From the impact coefficient of each leaf node of the attack countermeasure tree, the impact coefficient of other approaching methods represented by E2 node is larger, and the impact coefficients of confidentiality, integrity and availability are 0.58, 0.45 and 0.54 respectively. This indicates that the other approaching methods will make the network information security have a certain degree of attack probability, and it is necessary to focus on various types of system access methods to ensure system security.

(3) From the evaluation results of the attack effect of each attack sequence, the most effective way to attack network information security is to execute SQL injection attack through windows vulnerability, and its evaluation result is 0.9834. This indicates that it is necessary to repair system vulnerabilities from time to time and improve the system security protection network to avoid external vulnerability attacks.

References

[1] Sun, T. (2018). A risk assessment standard and application method of computer network information security. Basic & clinical pharmacology & toxicology.(S7), 123.
[2] Feng, L., Han, R., Wang, H., Zhao, Q., Fu, C., & Han, Q. (2021). A virus propagation model and optimal control strategy in the point-to-group network to information security investment. Complexity, 2021.
[3] Hongfeng, C. (2020). Information network security construction based on depth

learning and modulus algorithm. Journal of Intelligent and Fuzzy Systems, 38(4), 1-12.
[4] He, D., Zhang, Y., Li, T., Chan, S., & Guizani, N. (2020). Vulnerability analysis and security compliance testing for networked surveillance cameras. IEEE Network, PP(99), 1-7.
[5] Sun, L., & Gao, D. (2022). Security attitude prediction model of secret-related computer information system based on distributed parallel computing programming. Mathematical Problems in Engineering, 2022.
[6] Liu, Lin, Xinbao, Pei, Jun, & Pardalos, et al. (2017). A game-theoretic analysis of information security investment for multiple firms in a network. Journal of the Operational Research Society.
[7] Wang, Y. Z., Gao, B., & Lu, W. C. (2018). Application of bp neural network based on pca in information security. Basic & clinical pharmacology & toxicology.(Suppl.3), 123.
[8] Dang-Pham, D., Pittayachawan, S., & Bruno, V. (2017). Investigation into the formation of information security influence: network analysis of an emerging organisation. Computers & Security, 70(sep.), 111–123.
[9] Zhang, R., & Hu, Z. (2021). Access control method of network security authentication information based on fuzzy reasoning algorithm. Measurement, 185, 110103-.
[10] Garg, ShreePeddoju, Sateesh K.Sarje, Anil K. (2017). Network-based detection of android malicious apps. International Journal of Information Security, 16(4).
[11] Ji, B. K. D. H. (2021). Evaluating visualization approaches to detect abnormal activities in network traffic data. International Journal of Information Security, 20(3).
[12] Ficco, M., Choras, M., & Kozik, R. (2017). Simulation platform for cyber-security and vulnerability analysis of critical infrastructures. Journal of Computational Science, 22(sep.), 179-186.
[13] Shitharth, S., Shaik, M., Sirajudeen, A. J., & Sangeetha, K. (2019). Mining of intrusion attack in scada network using clustering and genetically seeded flora based optimal classification algorithm. IET Information Security, 14(6).
[14] Dang-Pham, D., Pittayachawan, S., & Bruno, V. (2017). Applying network analysis to investigate interpersonal influence of information security behaviours in the workplace. Information & Management.
[15] Du, M. (2020). Application of information communication network security management and control based on big data technology. International Journal of Communication Systems.
[16] Erdodi, L., & Zennaro, F. M. (2022). The agent web model: modeling web hacking for reinforcement learning. International Journal of Information Security(2), 21.
[17] Guangxu, Y. (2020). Research on computer network information security based on improved machine learning. Journal of Intelligent and Fuzzy Systems, 40(3), 1-12.
[18] Lu, H. J., & Yu, Y. (2021). Research on wifi penetration testing with kali linux. Complexity, 2021.
[19] Chen, Z., Zuo, X., Dong, N., & Hou, B. (2019). Application of network security penetration technology in power internet of things security vulnerability detection. Transactions on Emerging Telecommunications Technologies(2).

[20] Rak, M., Salzillo, G., & Granata, D. (2022). Esseca: an automated expert system for threat modelling and penetration testing for iot ecosystems. Computers & Electrical Engineering, 99, 107721-.
[21] Nuno Antunes, & Marco Vieira. (2017). Designing vulnerability testing tools for web services: approach, components, and tools. International Journal of Information Security.
[22] Lee, Y., Shen, C., & Vogelstein, J. T. (2017). Network dependence testing via diffusion maps and distance-based correlations. Biometrika.