Artificial intelligence design research on the cyber security penetration testing of power grid enterprises

X D Sun¹, Z Ren¹, P W Yang¹, J Li², H Y Chen¹ and T Q Liu¹

¹State Grid Inner Mongolia East Power Company Electric Power Research Institute, The 17th Floor in Block B of Green Land Tengfei Building, Tengfei South Street, Saihan District, Hohhot City, China
²State Grid Shandong Electric Power Research Institute, No.2000, Wangyue Road, Shizhong District, Jinan City, China

E-mail: suenxiaoda@126.com

Abstract. This paper introduces the key components of Artificial Intelligence (AI) expert system. It studies the main application of AI technology in network security. It deeply analyzes the network security situation of power grid enterprises, as well as the main problems in the troubleshooting and verification of vulnerability. The AI penetration test expert system is designed, and the implementation of the system is elaborated.

1. Introduction
Penetration testing is an evaluation method that tests the security of a computer network system by simulating a malicious hacker attack by a technician with knowledge and experience in network security. The penetration testing can be divided into two forms: white box test and black box test. A white-box test is a test conducted by a penetration tester with all the knowledge of the customer organization; a black-box test means that the penetration tester simulates an attack by an attacker who knows nothing about the client organization [1]. Power companies are huge in size and have a large number of information and communication equipment. Vulnerability scanning equipment have high error rate and miss rate, which is difficult to meet current needs. For example, when troubleshooting system vulnerabilities, the vulnerability scanning equipment only determines whether the vulnerability exists by identifying the system version. This method does not perform further verification, resulting in high error rate and miss rate. The network security vulnerabilities existing in power companies are still being checked and verified by manual penetration testing in most cases, relying heavily on the number and experience of technicians, and it is difficult to effectively control enterprise network security risks. With the continuous advancement of information technology, cyber attacks such as ransomware attacks, industrial control systems cyber attacks and APT attacks are emerging. In 2018, the International Information System Security Certification Alliance stated that the global network security talent gap has expanded to 3 million. The manual penetration testing accounts for nearly 70% of the work of the grid company network security personnel. The manual penetration testing consumes a lot of manpower and financial resources and has been unable to meet the current requirements.

In recent years, the development of science and technology has been changing with each passing day. AI has received considerable attention both at home and abroad, and has played a pivotal role in more and more fields. With the ubiquitous construction of the power Internet of Things and the continuous updating and development of network security attack and defense technology, the network
security of power grid enterprises faces enormous challenges [2]. In order to solve the limitations of traditional manual penetration testing, this paper combines AI and penetration testing technology. An AI-based penetration testing expert system was built.

2. AI technology

2.1. The concept of AI technology
AI is a branch of computer science, a technology that presents human intelligence through ordinary computer programs. AI, as a developing comprehensive marginal discipline, together with atomic energy technology and space technology, is called the three major scientific and technological achievements of this century. At present, AI is gradually developing into a huge technical system. In the field of AI, it includes technologies in many fields such as machine learning, deep learning, human-computer interaction, natural language, and machine vision.

2.2. Expert system
Expert system is an important branch of artificial intelligence. It is a kind of computer intelligent program system with expertise and experience. It simulate the complexity that can be solved by domain experts using the knowledge representation and knowledge reasoning technology of the artificial intelligence. The expert system is an intelligent computer program system, which contains a large number of experts and knowledge in a certain field, and can use the knowledge and problem solving methods of human experts to deal with the problems in the field [3]. Figure 1 is its basic composition structure. The knowledge base and inference engine are the core components. The expert system applies artificial intelligence technology and computer technology to make inferences and judgments based on the knowledge and experience provided by one or more experts in a certain field, simulate the decision process of human experts, and solve complex problems that require human experts to deal with.

![Figure 1. Basic structure of the expert system.](image)

2.3. Application of AI technology in network security
At present, artificial intelligence technology has great technical advantages in the field of network security. First, big data analysis identifies threats and can make big security based on big data. The second is the analysis of related security postures, comprehensively aware of internal and external security threats. The third is self-learning emergency response defence, which can build an active security defence system. In recent years, multi-agent systems, neural networks, expert systems, machine learning and other artificial intelligence technologies have emerged in the network security defence. However, the authors have found that artificial intelligence lacks relevant research on penetration testing.

3. Network security situation of grid enterprises

3.1. Cyber security situation
The power grid is an attractive target for hackers. The security risks of power system cyber security may cause risks such as large-scale power outages, power generation set shutdown, and customer
information leakage. Unlike natural disasters such as typhoons, hackers are becoming smarter all the time. On March 7, 2019, Venezuela suffered the largest blackout in the world, and the government claimed to have been attacked by cyber attacks. In 2015 and 2016, the Ukrainian power grid also suffered a massive power outage due to cyber attacks.

![Network security vulnerability of a provincial power company in 2017-2018.](image)

Figure 2. Network security vulnerability of a provincial power company in 2017-2018.

Figure 2 shows the number of network security vulnerabilities discovered by a provincial power company in 2017-2018. According to OWASP (Open Web Application Security Project) Top 10-2017, the authors have classified the number of vulnerabilities. Amazing 2,438 cases, mainly focused on security misconfiguration, using components with known vulnerabilities and other issues. It can be seen that there are a large number of network security risks in power grid enterprises, and the investigation and management of hidden dangers are under tremendous pressure. It is reported that the number of terminals of the State Grid Corporation that only access smart meters, protection equipment, measurement and control equipment, etc. has reached 540 million. In the future, the construction of ubiquitous power Internet of Things will be vigorously promoted, with the high interconnection of enterprise equipment. The number of connected devices in the future will be in a blowout state. It is expected that the Internet of Things terminal equipment will reach 2 billion in 2030. By then, the entire ubiquitous power Internet of Things will be the largest IoT ecosystem for access devices, which will bring the network security work of power grid enterprises a huge challenge.

3.2. Advantages of AI penetration testing system

At present, power grid enterprise vulnerability investigation and verification work relies heavily on manual penetration testing. In recent years, network security attack technologies have emerged in an endless stream. In order to avoid grid security attacks and ensure safe and stable operation of power grids, power grid enterprises consume huge manpower in the training of penetration testers. Financial resources, but still cannot meet the needs of enterprises for network security talents, the development and utilization of AI penetration testing system can help solve these problems:

- Make up for the shortage of personnel. The degree of automation of artificial penetration testing is low, and the demand for personnel is large. As the number of cyber attacks increases, the degree of harm increases, and the demand for corporate network security
professionals soars, but the relevant talent pool is still insufficient. The artificial penetration-based automated penetration testing system can make up for the shortage of personnel.

- Improve work efficiency. Artificial penetration testing is inefficient and time consuming. The current network environment is more complex, attack methods are emerging, and penetration testing methods are increasing. In the era of big data, the scale of data to be processed by network security penetration testers is seriously mismatched with its processing capacity. There are many assets of power grid enterprises. At present, the statistical management methods of assets are still not perfect, and there are still many (and will continue to exist in many professional and fringe places). Produce a large number of vulnerabilities. Through AI technology, simulating penetration testing thinking, and building an intelligent model for vulnerability verification and utilization, the efficiency of network security risks will be greatly improved.

- Eliminate subjective bias. At present, the subjective awareness of the penetration tester has a great impact on the test results. The troubleshooting and verification of the vulnerability relies heavily on the personal ability of the technician, and the vulnerability investigation and verification process cannot be traced. The AI automatic penetration testing technology analyzes and judges the target objects with different information elements through the training model, and adopts appropriate detection means to solve the problem that the traditional vulnerability scanning equipment cannot verify the vulnerability and the subjective deviation of the personnel.

4. Implementation of AI penetration test expert system

4.1. Basic frame composition

Figure 3 shows the system framework diagram. In this paper, AI technology is used to model the penetration method of penetration testing experts, and an artificial penetration testing expert system is built to make the system have the same level of problem solving ability as domain experts. The core components of the system are the knowledge base and the inference engine. The knowledge base is the
set of domain knowledge required for problem solving. The knowledge base can obtain various penetration test data information through the existing basic knowledge, the knowledge of domain experts and the channels of independent learning. Such as exploit libraries, attack event libraries, vulnerability information bases, etc. Users can continuously optimize the performance of expert systems by adapting and refining the knowledge content in the knowledge base. Based on the knowledge semantics, the inference engine finds the required penetration testing methods and performs the penetration testing process according to certain strategies.

The tester inputs the IP/URL of the target object, obtains the target information element, selects a specific vulnerability attack verification means according to the rules derived by the inference engine in the expert system, implements an automatic iterative test, and outputs a test report.

4.2. Principle of implementation

As shown in figure 4, the implementation of the AI penetration test expert system is divided into two stages: modeling phase and application phase.

![Figure 4. System flow chart.](image)

4.2.1. Modeling phase. Based on the existing vulnerability verification method, collect the test experience and means related to the penetration test experts, form the vulnerability verification library set required for the penetration test, and filter the penetration methods related to the specific information elements from the collection through a large number of information detection and cycle tests analysis. The test methods are executed one by one, the vulnerability verification process is completed, and the successful verification method is used to record and form a model.

- **Detect.** Enter the test object IP/URL, and obtain the basic information of the target host through various detection methods (crawler, sniffing, scanning, etc.): port number, protocol type, service name and version, operating system type and version information, etc., which constitute information elements. Such as: port number - 21, protocol type - tcp, service name - vsftpd, service version - 2.3.4, operating system type - linux, operating system version - 2.6.X, etc.
- **Analyse.** Information detection obtains basic information elements. Each information element is compared with the vulnerability verification method in the vulnerability verification library set by the feature code. The relevant vulnerability verification script or attack payload is analyzed, filtered, recorded, and then, form the knowledge base.
- **Train.** Exploit the records in the knowledge base one by one, and retain all the records that
have been successfully used. Vulnerabilities in each information element, if successful, record the intersection and form an automatic penetration test sample record. n times trainings form the sample record and take the union to form an automatic penetration test record as a rule of the expert system.

4.2.2. Application phase. Based on the expert system model, the penetration tester can achieve automated penetration testing to the target object.

- **Detect.** When the penetration tester applies the expert system, the target object IP/URL is input, and the system acquire the information element of the target object by the detection means. The expert system allows the manual addition of the information element.
- **Penetration test.** After the information is detected, the expert system will match the rules in the system according to the information elements automatically. If it is successful, the vulnerability verification and utilization are directly performed, and the penetration test is automatically completed.
- **Improve the model.** For the infiltration attack with unsuccessful rule matching, the expert system enters the analysis and training phase automatically, and regards this penetration test as a training to form a new automatic penetration test sample record. The system allows manual intervention and corrects the infiltration method continuously based on the acquired new knowledge to optimize the expert system model.
- **Generate report.** The test report will be generated automatically, and it contains the penetration test process and results.

5. Conclusion and outlook
This paper mainly analyzes the main problems in the network security vulnerabilities troubleshooting and verification of the power grid enterprises, studies the application prospects of AI in penetration testing, and builds an AI penetration testing expert system model, and elaborates on the implementation of the system. The system is still in the development stage. It is believed that AI will make great progress in penetration testing technology in the future, and at the same time, the threat it poses and the uncertainty caused by the system during testing should be further studied.

References
[1] Michalski R S, Carbonell J G and Mitchell T M 2013 Machine Learning: An AI Approach (Berlin: Springer Science & Business Media)
[2] Senkal S and Ozgonenel O 2014 Performance analysis of artificial and wavelet neural networks for short term wind speed prediction International Conference on Electrical and Electronics Engineering (Kuala Lumpur, Malaysia)
[3] Vapnik V N 1995 The Nature of Statistical Learning Theory (Berlin: Springer)