Research on Network Attack and Defense Based on Artificial Intelligence Technology

Mingxuan Li[1] ,Zhushi Yang[2],Jinsong Zhong[1] ,Ling He[1],Yangxin Teng[1]
1. State Grid Xinjiang Electric Power Research Institute, Urumqi, China
2. State Grid Xinjiang Electric Power Limited Company，Urumqi, China
517134857@qq.com,393792160@qq.com

***Abstract*—This paper combines the common ideas and methods in offensive and defensive confrontation in recent years, and uses artificial intelligence technology-based network asset automatic mining technology and artificial intelligence technology-based vulnerability automatic exploitation technology, carries out research and specific practices in discovering and using system vulnerability based on artificial intelligence technology, designs and implemented automatic binary vulnerability discovering and exploitation system, which improves improves the efficiency and success rate of vulnerability discovering and exploitation.**

Keywords—artificial intelligence; automatic binary vulnerability discovering and exploitation system; network attack and defense

I. INTRODUCTION

At present, major countries in the world have invested research and development forces in artificial intelligence-based automation network offense and defense. In the 2016 DEFCON final, the automated attack team Mayhem (the champion of the CGC in 2014) participated in the competition with 14 human teams and once defeated two human teams, indicating that the automatic attack methods generated by artificial intelligence systems can already be faster than humans. Continuously scan system defects and discover vulnerabilities more effectively. The Ministry of Defense of Japan also announced recently that in order to strengthen its ability to respond to Cyber attacks, artificial intelligence technology will be introduced into the information defense network defense system of the Japan Self-Defense Force.

It is foreseeable that the deep application of artificial intelligence in the field of Cyber offense and defense may bring revolutionary changes and increase the imbalance in the strategic power of cyberspace in various countries. Therefore, systematically investigating the development status of artificial intelligence-based network offense and defense at home and abroad, comprehensively analyzing the development trends of domestic and international related technologies, analyzing the development outlines and specifications of artificial intelligence offense and defense in various countries in the world, and studying the application status and future of artificial intelligence offense and defense are of great significance for promoting the development of China's artificial intelligence offensive and defensive technologies and ensuring the core interests of cyberspace..

II. SITUATION ANALYSIS

This paper found the following problems during the research of network attack and defense:

(1) The method of manually vulnerability discovering manually is time-consuming and costly, and it may cause omissions. At the same time, the code path coverage of existing vulnerability discovering methods is low and inefficient.

(2) The existing vulnerability exploitation methods are mainly based on dynamic or static memory analysis methods. Through analysis of the memory, the crash points and runtime states are found. However, many vulnerabilities cannot be proven to be exploitable.

Based on the above problems, this paper combines the common ideas and methods in offensive and defensive confrontation in recent years, and uses artificial intelligence technology-based network asset automatic mining technology and artificial intelligence technology-based vulnerability automatic exploitation technology, carries out research and specific practices in discovering and using system vulnerability based on artificial intelligence technology, and enhance the system's vulnerability discovery and utilization capabilities.

III. RESEARCH ON NETWORK ATTACK AND DEFENSE BASED ON ARTIFICIAL INTELLIGENCE TECHNOLOGY

A. Automated Binary Vulnerability Discovering and Exploitation System

This paper closely combines artificial intelligence technology and cyber security attack technology, and conducts cross-cutting research from two levels of theoretical research and system construction to achieve the promotion of the defense system with the improvement of attack capabilities, and the strengthening of the defense system counteracting the ultimate improvement of attack capabilities.

This paper designs and implements an automated binary vulnerability mining and exploitation system. The system can automatically obtain the binary program under test, mine vulnerabilities, utilize vulnerabilities and finally feedback to the user. It has the characteristics of stable and efficient, simple to use, low learning cost, and loose coupling, which greatly reduces the technical capability requirements of researchers in exploiting and exploiting vulnerabilities.

978-1-7281-4390-3/20/$31.00 ©2020 IEEE

Authorized licensed use limited to: University of Edinburgh. Downloaded on June 14,2020 at 19:47:22 UTC from IEEE Xplore. Restrictions apply.

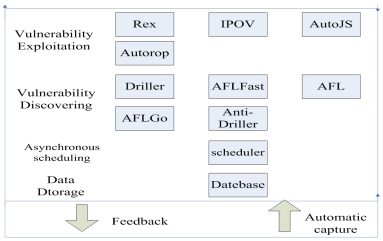

Fig 1. Structure of the automated binary vulnerability discovering and exploitation system

The structure of the automated binary vulnerability discovering and exploitation system is shown in Fig 1. It includes data storage, asynchronous scheduling, vulnerability discovering, and vulnerability exploitation. The database provides data storage services such as binary programs, crash fragments, and utilization code; the scheduler provides task scheduling services for different tasks, such as discovering modules, exploitation modules, etc .Vulnerability discovering modules and exploitation modules separately provide Vulnerability discovering and exploitation services. Compared with the previous method, the system achieves the following improvements.

(1) In terms of data storage, a lightweight database design is used, which reduces the amount of data storage by about 70% compared to other systems.

(2) In task scheduling, the scheduler can automatically collect the binary files to be tested. Each vulnerability discovering and exploitation service will be abstracted into "tasks", and the scheduler will allocate computing resources for each "task" according to a preset resource allocation scheme of CPU, memory, hard disk, etc., to realize automatic scheduling and management.

(3) In terms of vulnerability discovering, the system integrates the more popular and efficient discovering methods AFL, Driller, AFLGo, and AFLFast. In addition, the system has built-in innovative design methods to improve the efficiency of vulnerability discovering.

(4) In terms of vulnerability exploitation, the system integrates a popular vulnerability exploitation method, Rex, and three newly developed vulnerability exploitation methods, IPOV, AutoROP, and AutoJS, a total of four methods, improving the success rate of vulnerability exploitation.

B. The Process of Automated Binary Vulnerability Discovering and Exploitation System

This system was developed based on python2.7, using Kubernetes as the underlying management platform, and using Docker technology to achieve independent operation of each module and avoid interference from other modules. It can discovery and exploit stack overflow, integer overflow, and format string vulnerabilities.

The detailed process of the automated binary vulnerability discovering and exploitation system is shown in Fig 2. The system runs on the local side, and the binary files under test are stored on the remote side. When the system detects that there is a binary file under test at the remote end, it will proactively issue a request and obtain the binary file, and then the binary file will be stored in the local database; when the system detects a new file in the database, it will actively schedule a vulnerability discovering module, which can use a single Fuzzy testing, single dynamic symbol execution, or a combination of the two methods; when a crash is successfully generated, the exploit code will be used to construct the exploit code and verify whether the system permissions can be obtained; if the permissions can be successfully acquired, the exploit code will be passed to verify remotely whether you can obtain the permissions of the remote server, otherwise it cannot be used. The system's analysis of binary files is shown in Fig 3.

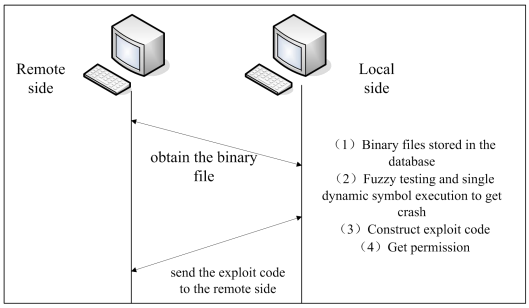

Fig 2. Automated binary vulnerability discovering and exploitation system work flow

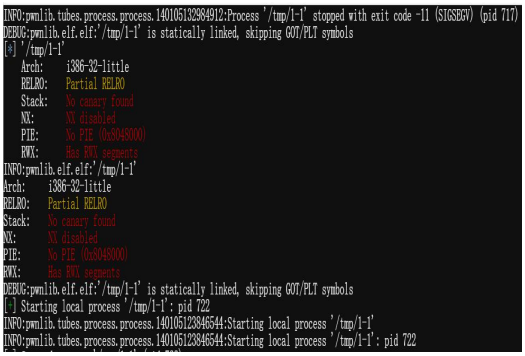

Fig 3. System analysis process of binary files

C. Typical Case Analysis

This chapter explains the usability and effectiveness of the system through typical use case analysis. The target object of a typical case is: an unprotected binary program with a stack overflow vulnerability. The vulnerability of this program is shown in Fig 4. The cause of the vulnerability is that the input variable v1 is not checked, and it is allowed to input arbitrary char type data, which causes a stack overflow.

```
1 int sub_80488D6()
2 {
3   int result; // eax
4   char v1; // [esp+Ch] [ebp-1Ch]
5   int v2; // [esp+1Ch] [ebp-Ch]
6
7   v2 = dword_80EB068;
8   sub_8048938((int)&v1, 256);
9   result = dword_80EB068;
10  if ( v2 != dword_80EB068 )
11    exit(0);
12  return result;
13 }
```

Fig 4.Vulnerability point location

Authorized licensed use limited to: University of Edinburgh. Downloaded on June 14,2020 at 19:47:22 UTC from IEEE Xplore. Restrictions apply.

During the vulnerability discovering phase, multiple crashes were discovered using multiple vulnerability discovering tools, as shown in Fig 5. Among them, the blue crash is available, and the specific crash is shown in Fig 6.

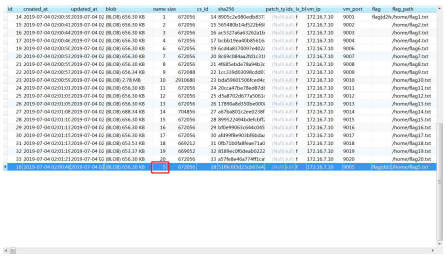

Fig 5.Vulnerability crashes

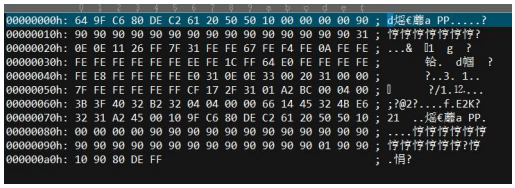

Fig 6.Available crash details

In the exploit phase, use the program shown in Fig 7 to generate exploit code.



Fig 7.Utilize code generator

The system's automatic execution process is shown in Fig 8.



Fig 8.The system's automatic execution process case

The utilization effect shown in Fig 9.

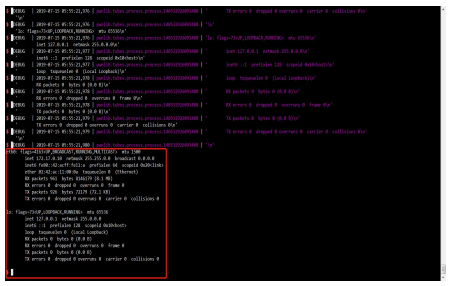

Fig 9. System utilization effect

IV. CONCLUSIONS

With the development of business, various components such as terminals, information systems, software, and programs that support the operation of various types of power grids continue to increase. However, the traditional security protection methods, such as vulnerability discovering of various components that use manual attacks as the main means, have problems such as incomplete security discovery, poor timeliness, and low accuracy. The existing methods based on fuzzy testing have low coverage. The symbolic execution method has problems such as path explosion. Therefore, discovering potential security risks through artificial intelligence technology is of great significance for improving the network security confrontation ability of the State Grid Corporation and strengthening the construction of the information security system.

This paper combines the common ideas and methods in offensive and defensive confrontation in recent years, and uses artificial intelligence technology-based network asset automatic mining technology and artificial intelligence technology-based vulnerability automatic exploitation technology, carries out research and specific practices in discovering and using system vulnerability based on artificial intelligence technology, which improves the system's vulnerability discovery and utilization capabilities, reduces the work of security personnel to a certain extent, and improves the efficiency and success rate of vulnerability mining and utilization. It provides an idea for other types of repetitive work in the future.

REFERENCES

[1]Xie Wenguang. Research on Application of Computer Network Technology Based on Artificial Intelligence.Computer Products and Distribution,2017(09),279。

[2]Kong Xiangjing, Ma Lixin, Chen Ming et al. Application of artificial intelligence technology in cyberspace security defense.The Third Smart Grid Conference 2018.

[3]Xiao Zhouxuan. Talking about the Application of Artificial Intelligence Technology in Cyberspace Security Defense.China New Communications,2018.20(04):95.

[4]Wu Yanbo.Application of artificial intelligence technology in cyberspace security defense.Chinese and foreign entrepreneurs,2018(05):124.

Authorized licensed use limited to: University of Edinburgh. Downloaded on June 14,2020 at 19:47:22 UTC from IEEE Xplore. Restrictions apply.