Table of contents

1 Introduction

There are various ways of network penetration. According to different needs and usage habits, various network penetration tools have appeared on the Internet.

These tools are classified into many categories. For the same needs, there are many ways to achieve them based on different application environments. At

the same time, the compatibility of these tools results in their effectiveness in different application environments. Different tools can be used together in corresponding

application environments to reflect their functionality.

Small tool, big effect. Efficient, fast, and stable network tools can make users' businesses run more smoothly. However, the current special investigation laboratory

tools are temporarily unable to meet the growing needs of special investigation work, and various network special investigation tools find It is not easy to use

unfamiliar network special investigation tools, which will result in low efficiency of special investigation work, and existing network special investigation tools may not be able to

meet the current application environment, and lack standardized management and use, and suitable network special investigation tools After standardized management

and use, it will help improve the efficiency and stability of special investigation work. Therefore, how to cluster these different network special investigation tools is an

urgent problem that needs to be solved.

2 Requirements analysis

There are many types of network special investigation tools, huge in number, and powerful in function. However, various network tools lack unified management and specifications.

use, resulting in users being unable to distinguish the application scenarios and applicable environments of various network special investigation tools, and being unable to use various network special investigation tools.

Maximize effectiveness when carrying out special investigation work. On the one hand, various network special investigation tools are sensitive and need to be disguised and applied.

On the other hand, due to the large variety of special investigation tools, users cannot quickly find tools that suit their own usage habits, so they need to base their efforts on

Quickly search and sort commonly used tools based on frequency of use, making it easier for users to query and use.

> Enables quick navigation

The higher the proficiency in using tools, the more conducive it is to the development of special investigation business. In order to ensure the smooth development of special investigation business

with high quality and quantity, the "Individual Soldier Toolbox" needs to have a fast search function to quickly find tools that fit the actual use environment. At the same time, in order to make

various tools fit the usage habits, it needs to be organized according to the frequency of use. Rank the top 10 commonly used tools according to their level, so as to speed up business development

and quickly engage in special investigation work.

> Tools can be classified

There are many types of special investigation tools, which can easily lead to a mismatch between functions and needs. Therefore, it is necessary to conduct unified management of various network special investigation tools and annotate the functions of all tools in order to standardize the use of various network special investigation tools and make full use of them. Its functional characteristics can be used in different special investigation business scenarios to further improve the stability and ease of use of the tool and ensure the stable and effective conduct of special investigation business.

> Conducive to concealment and camouflage

The network special investigation business is sensitive and must be carried out in a hidden environment to avoid alerting the target and causing the failure of the special investigation mission. However, the daily use rate of laptops is high, so high-performance laptops can be used to reproduce special investigations. On the one hand, the reconnaissance tool facilitates the covert execution of special reconnaissance operations, and on the other hand, it can improve the portability of the "individual soldier toolbox" so that special reconnaissance operations can be carried out in a variety of environments.

3 Product Introduction

3.1 Product introduction

"Individual Toolbox" is a cluster management platform for penetration testing tools of various network sites. It has a large number of built-in network special investigation tools, which can be used as special investigation means to conduct LD discovery, LD utilization and remote control management of targets, and then Get data intelligence resources. The platform performs cluster management of various network special reconnaissance tools through high-performance notebooks. Users only need to open the "Individual Soldier Toolbox" and connect to the network to carry out special reconnaissance work on targets.

3.2 Product composition

"Individual Soldier Toolbox" is a professional network special investigation tool set. The system is equipped with high-performance laptops to provide users with a good software running environment and penetration environment.

The product composition list of the "Individual Soldier Toolbox" is mainly as follows:

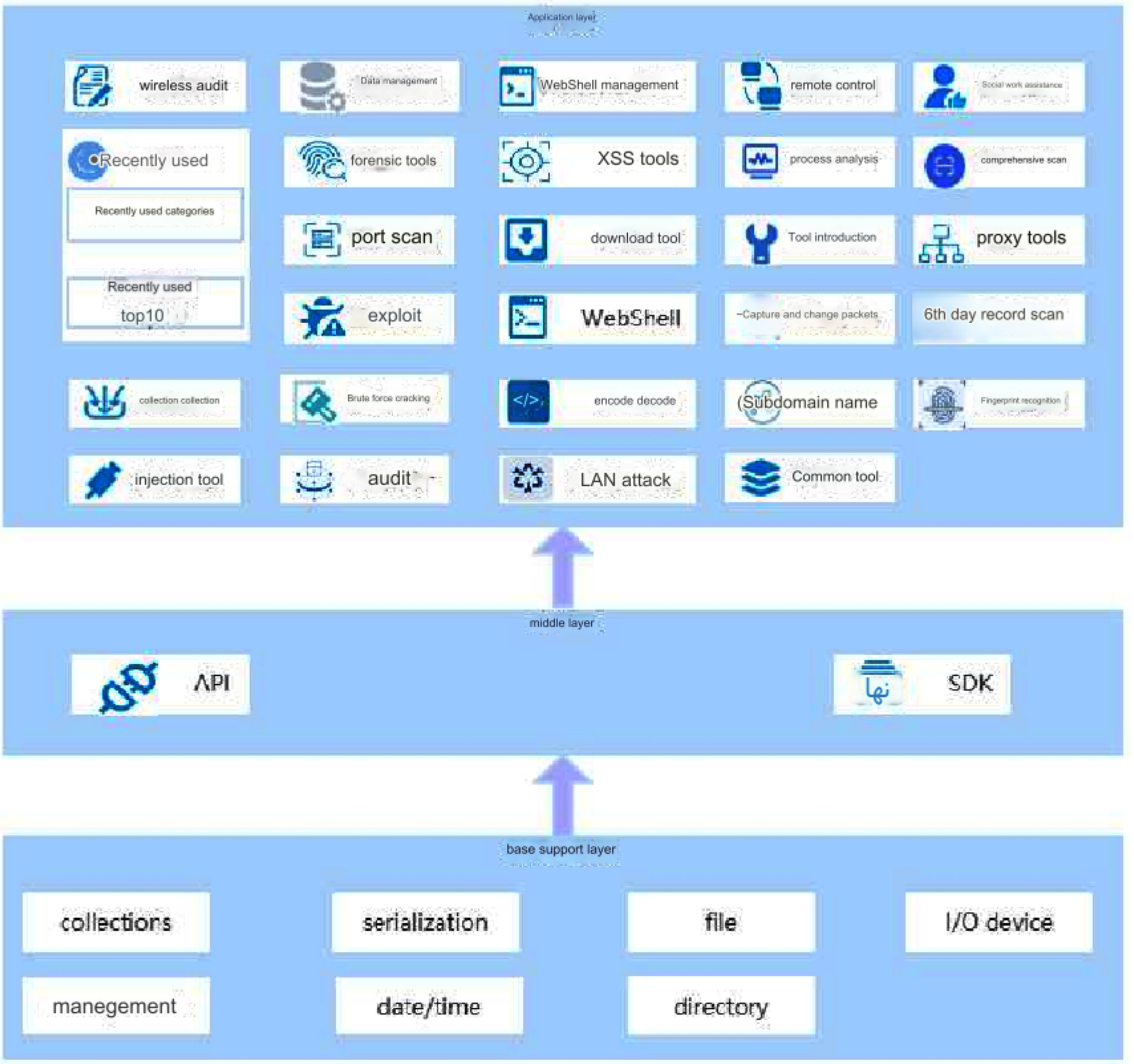
1. "Individual Soldier Tool Box": 1 unit

2. Platform user manual: 1 copy

3.3 System architecture

The "Individual Soldier Toolbox" is mainly composed of a basic support layer, an intermediate layer and an application layer. The basic support layer is the underlying architecture of the system and provides

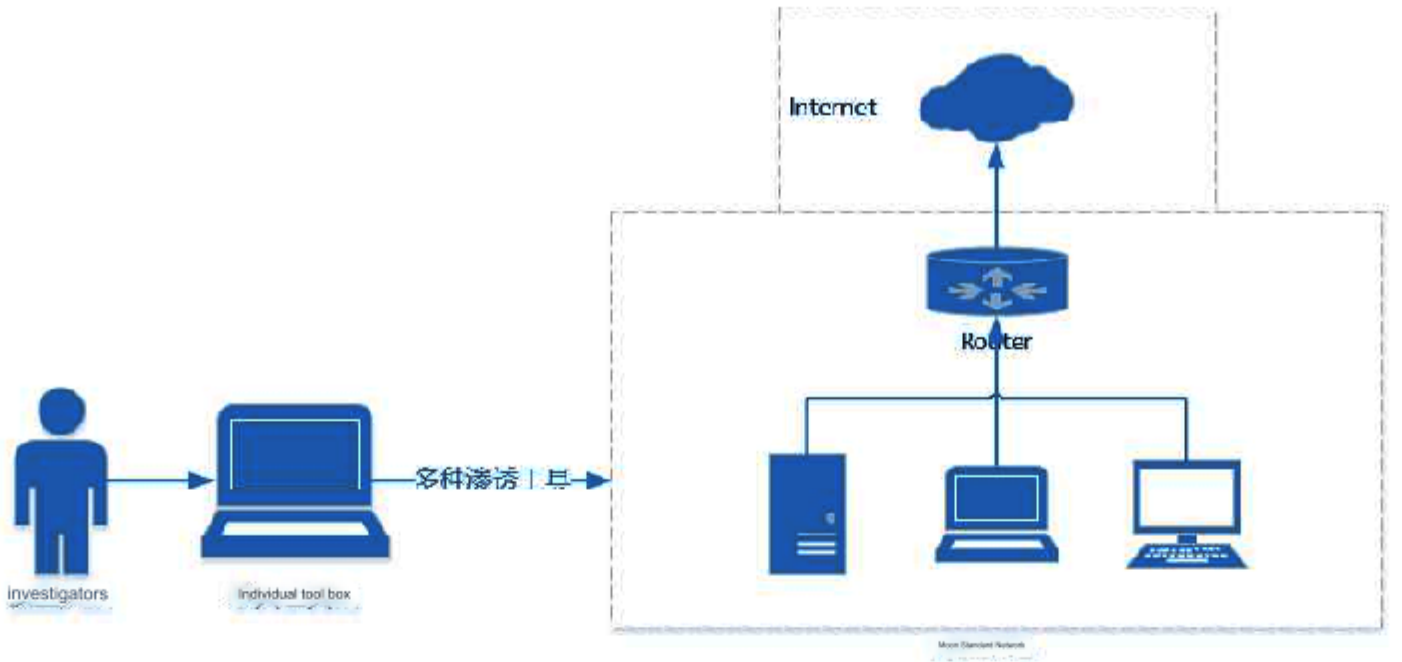
It provides functions of classification, interface beautification, function sorting, tool introduction and cluster management. The middle layer improves the coupling between each component unit through the API structure and SDK interface. The API interface is used to provide various package interfaces for To provide powerful functional guarantee for the system, the application layer is the specific implementation layer of various tools and realizes the cluster management functions of various tools.



(system architecture diagram)

3.4 Network architecture

The "Individual Soldier Toolbox" is an integrated combat equipment that uses a high-performance notebook as a carrier and integrates a large number of network special reconnaissance tools. Reconnaissance personnel can use the "Individual Soldier Toolbox" to conduct LD discovery and analysis of target application sites through the "Individual Soldier Toolbox" LD utilization, discover the LD existing in the target application site, launch the LD utilization tool, control and collect evidence on the target application site, and achieve the purpose of obtaining intelligence information of the target application site.



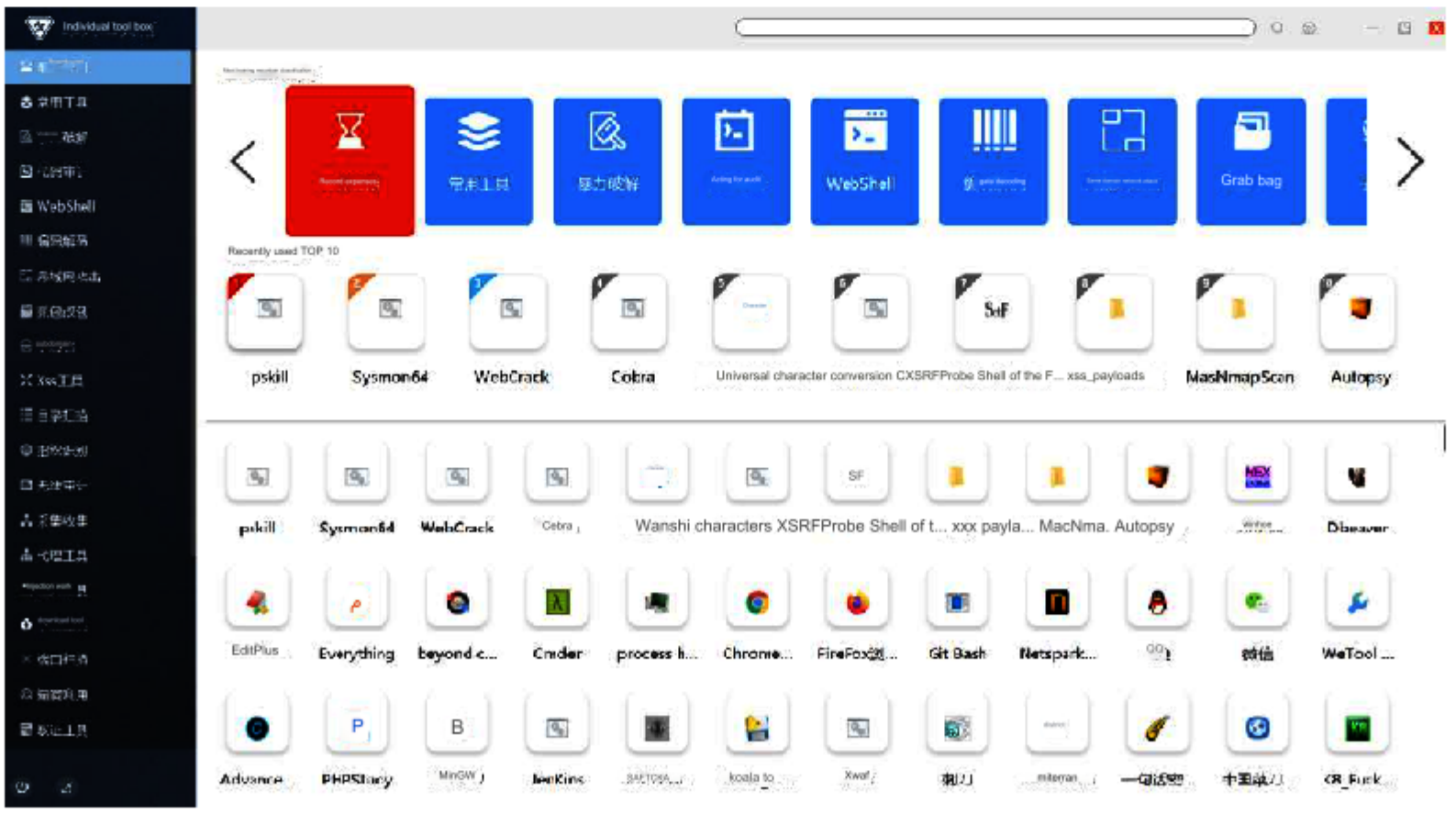
("Individual Soldier Toolbox" network architecture diagram)

4 product features

The "Individual Soldier Toolbox" is a special product for the network reconnaissance work of the special reconnaissance department. The "Individual Soldier Toolbox" is built-in with a large number of commonly used tools, brute force cracking, code auditing, encoding and decoding, LAN attacks, XSS tools, comprehensive scanning, data management, remote control and other professional software tool sets, which can quickly conduct network reconnaissance on targets.

4.1 Recently used

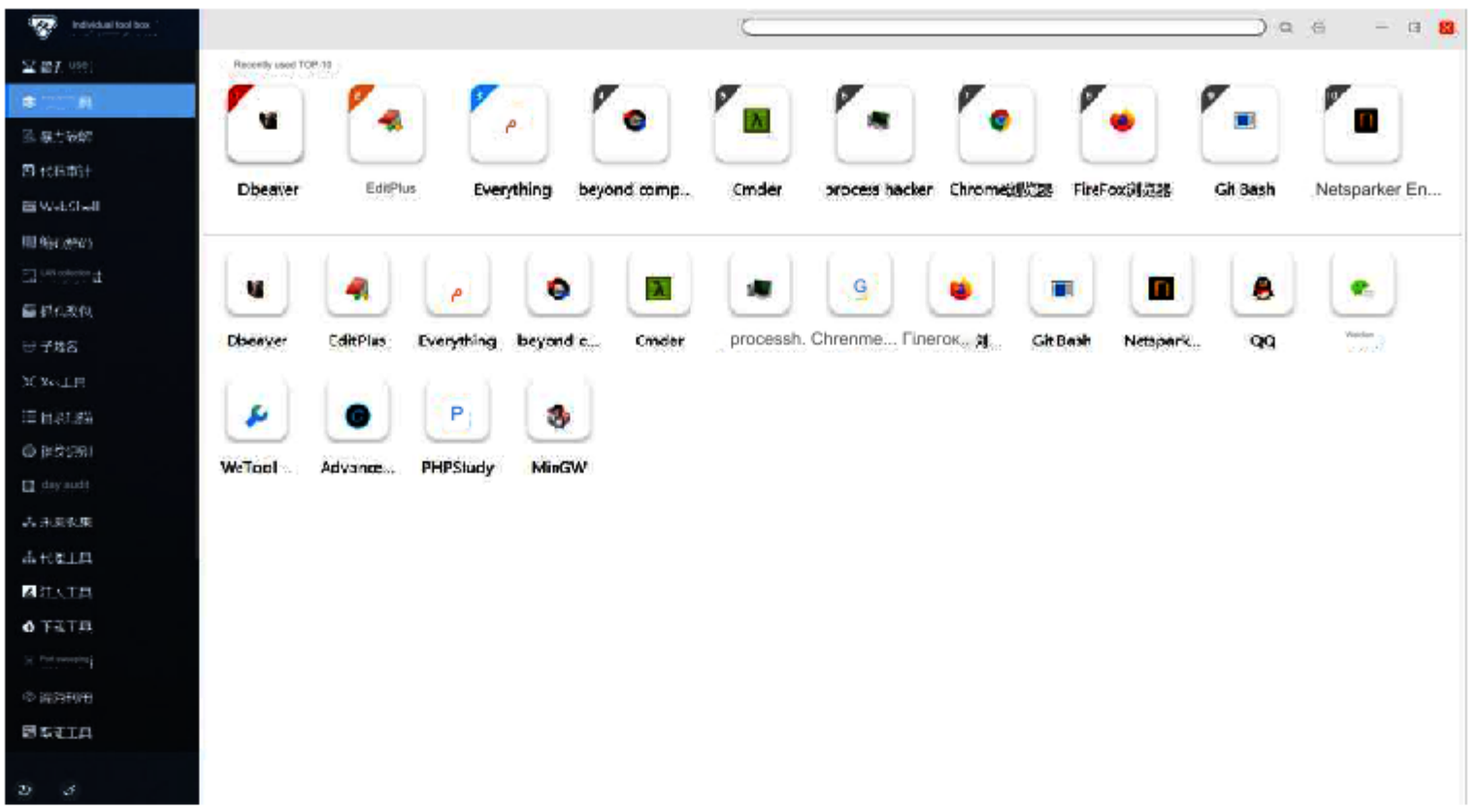
The recently used function mainly provides a search function for existing tools. According to the frequency of use, it provides a sorting function of the Top 10 commonly used tools and sorts different tool categories according to the frequency of use, making it easier for users to quickly find commonly used tools, closer to user usage habits, and improving Special investigation efficiency.



(Recently Used)

4.2 Commonly used tools

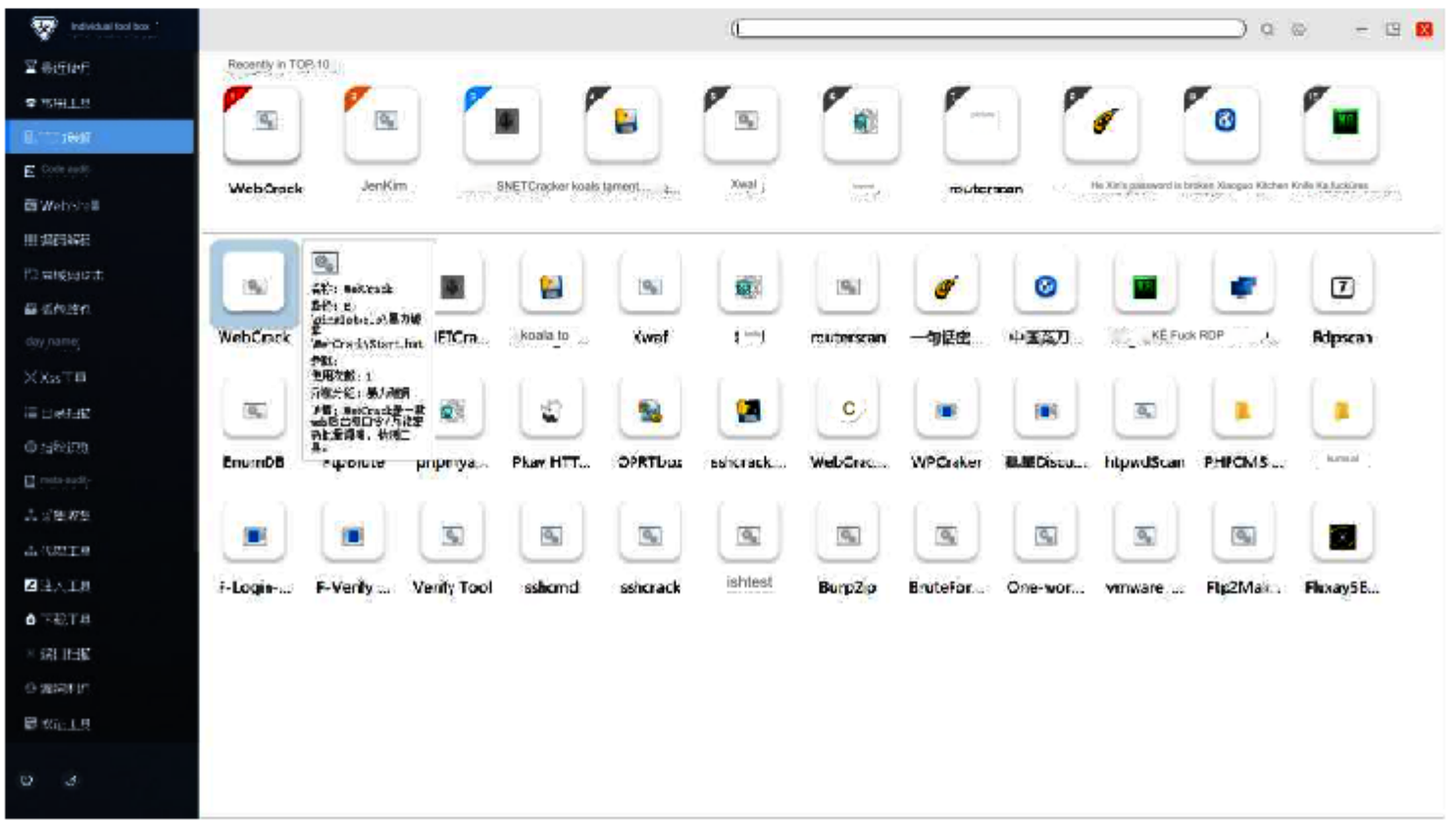
It has built-in a large number of commonly used network tools, such as WeChat, QQ, Google Chrome, Dbeaver and Cmder, which fully meet the needs of special investigation work and improve the convenience of special investigation work.



(Common tool)

4.3 Brute force cracking

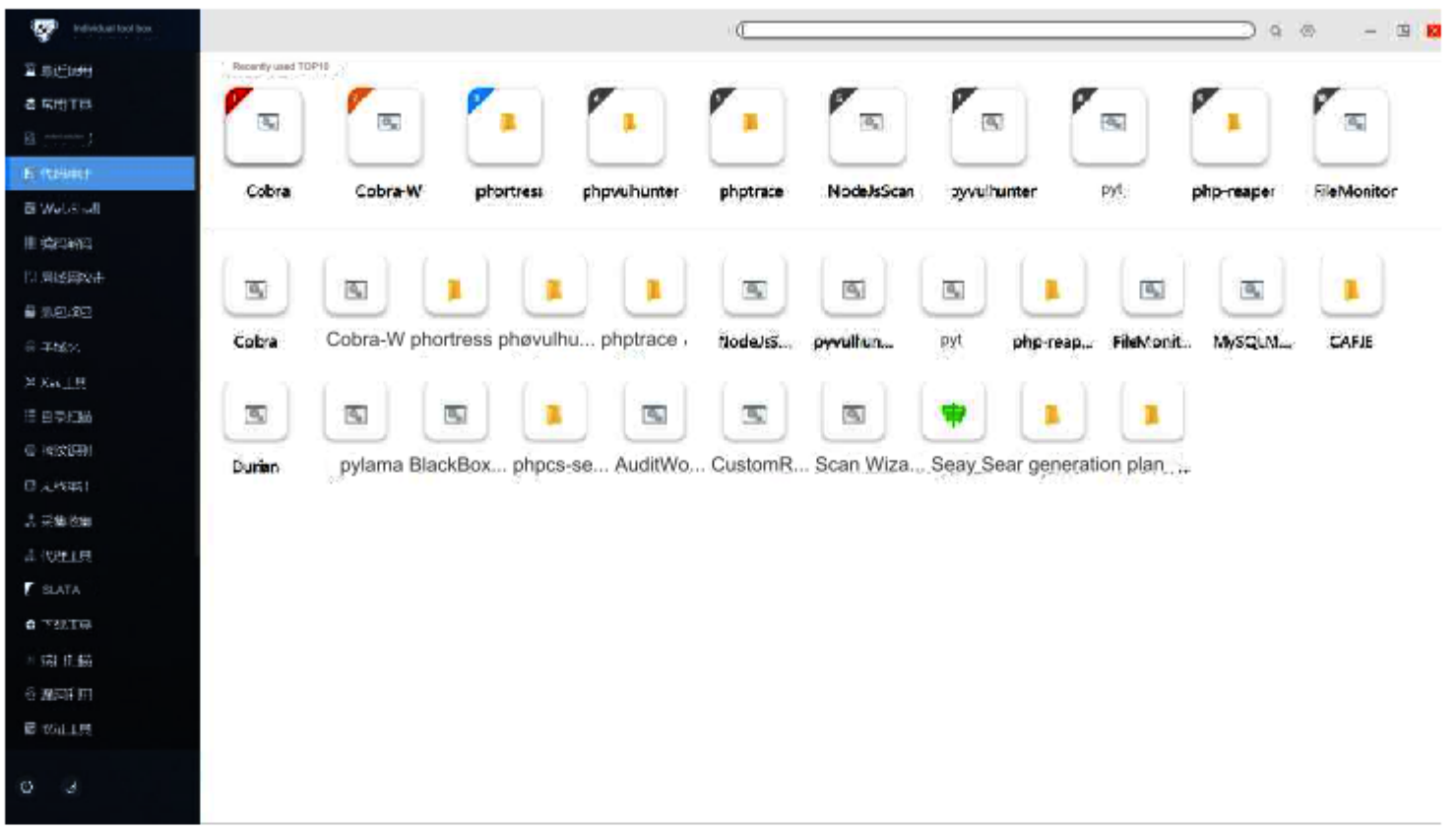
Built-in homemade brute force cracking scripts and established password cracking tools. It can perform unlimited exhaustive searches on the account and password of MSSQL database, MYSQL database and SSH, and crack the account password; it can also crack the administrator account and password of Windows and Linux and the encrypted ciphertext containing the protocol.



(brute force cracking)

4.4 Code audit

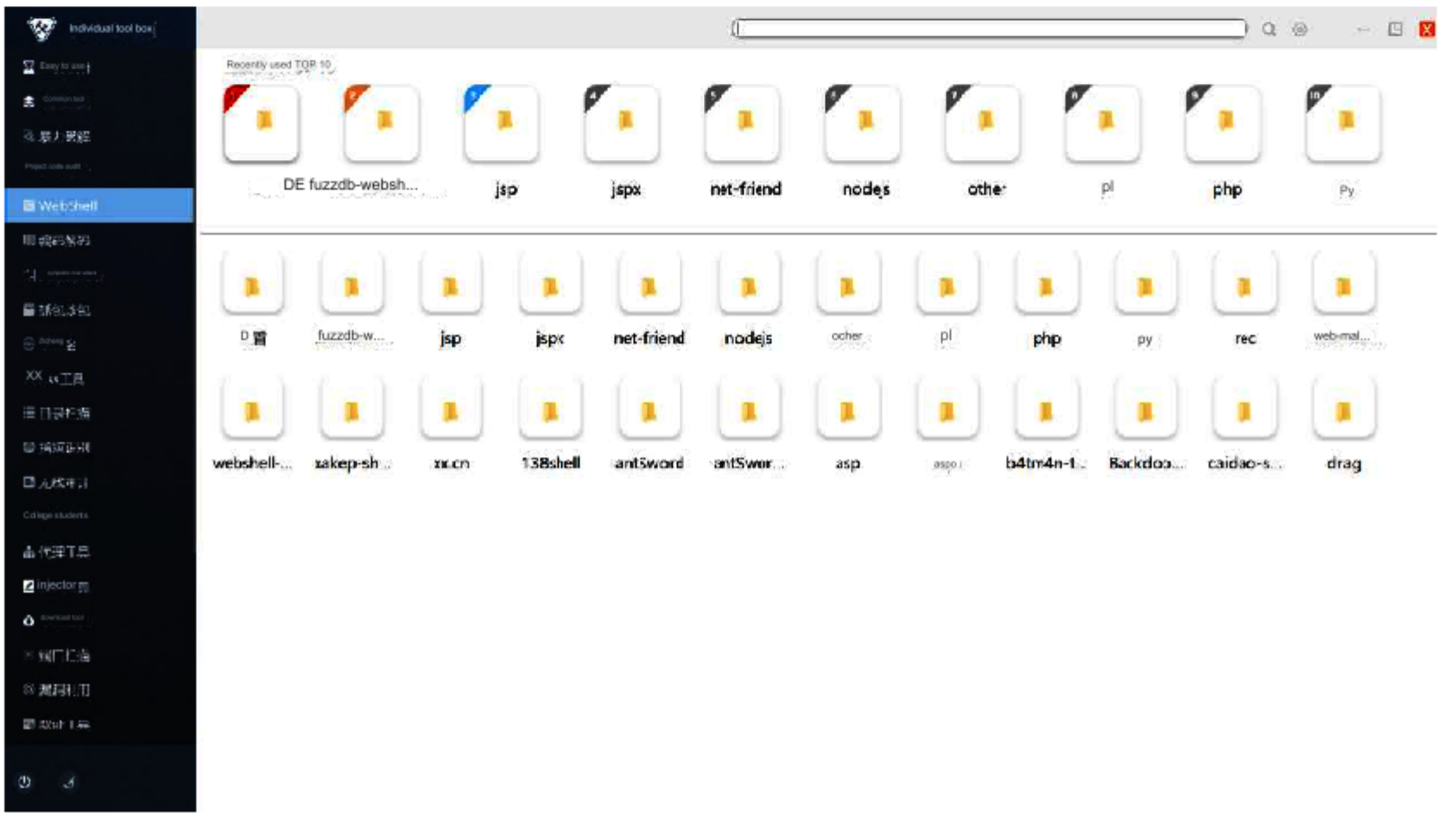
Integrate commonly used code audit tools to check the security flaws of the source code in the project and discover code LD, which facilitates penetration personnel to further exploit the LD.



(code audit)

4.5 WebShell Tools

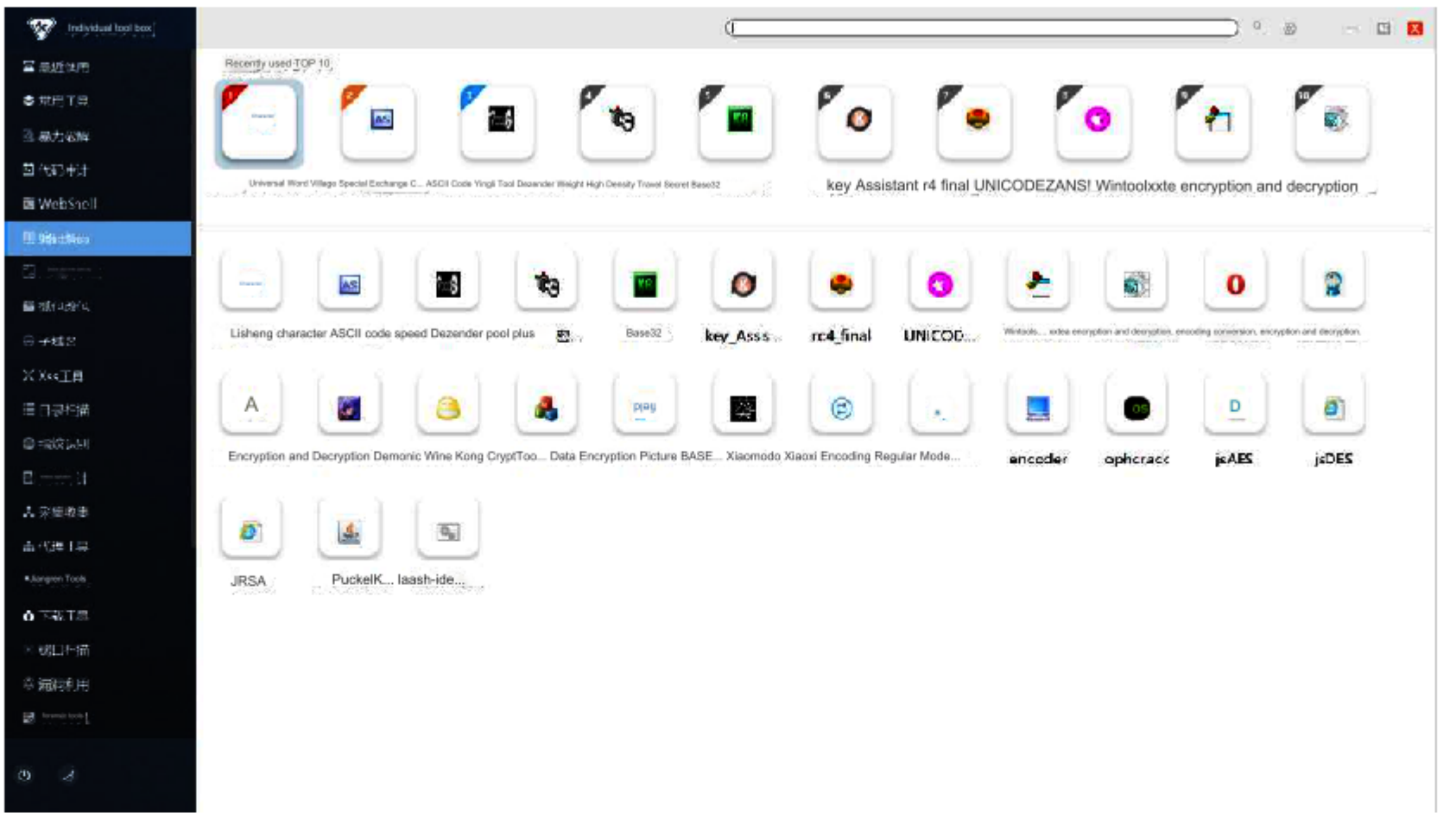
Integrate multiple command execution environments in the form of web files such as asp, php, jsp or cgi, that is, web backdoors. When performing penetration work on the target website, such tools can be mixed with normal web files in the WEB directory of the website server. Together, using a browser to access the asp or php backdoor, you can get a command execution environment to control the target website server.



(WebShell)

4.6 Encoding and decoding

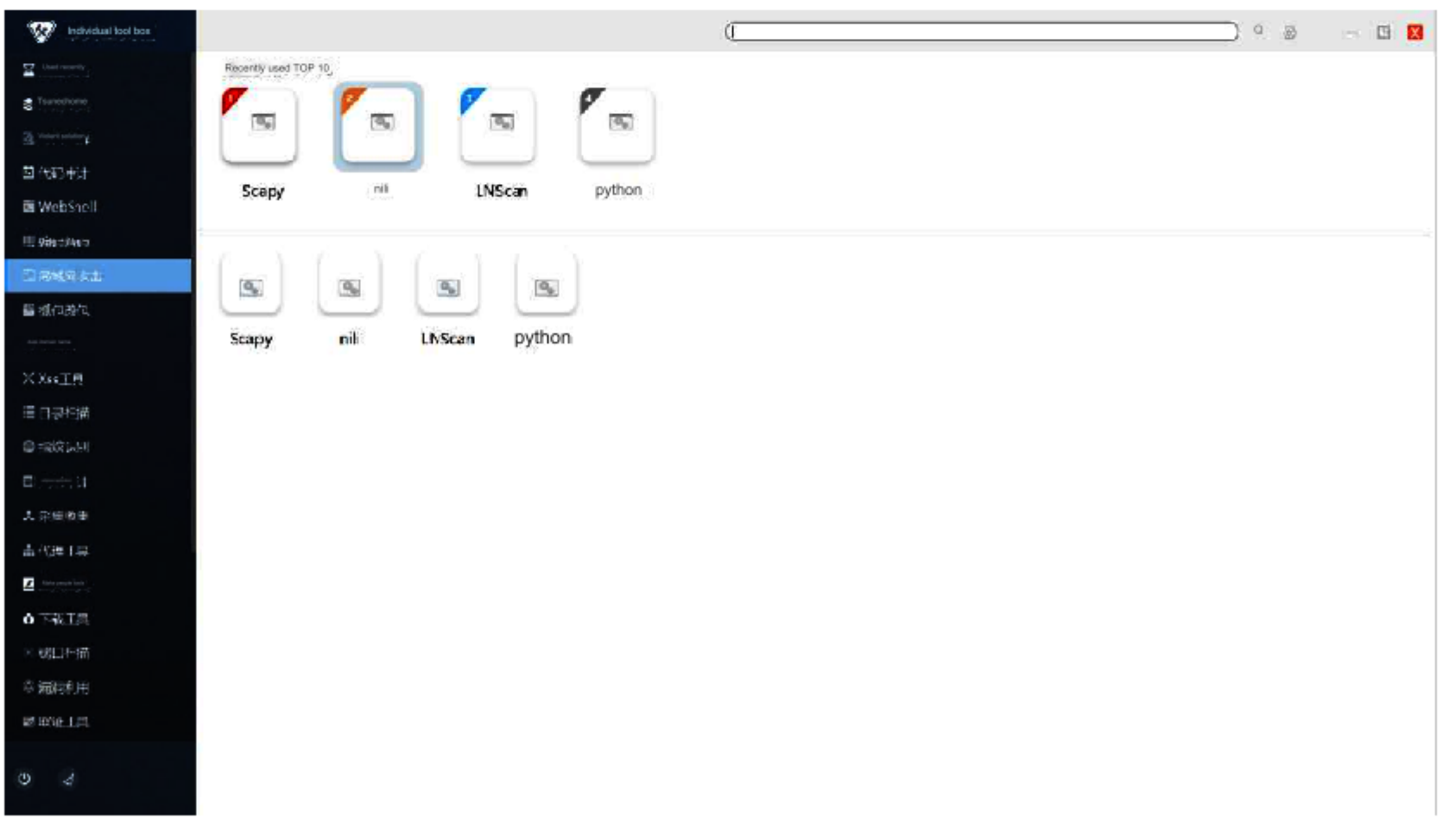
Integrate a large number of commonly used encryption and decryption, code conversion, and hexadecimal conversion tools to facilitate users to quickly encrypt and decrypt, code conversion, and hexadecimal conversion of targets.



(encode decode)

4.7 LAN attack

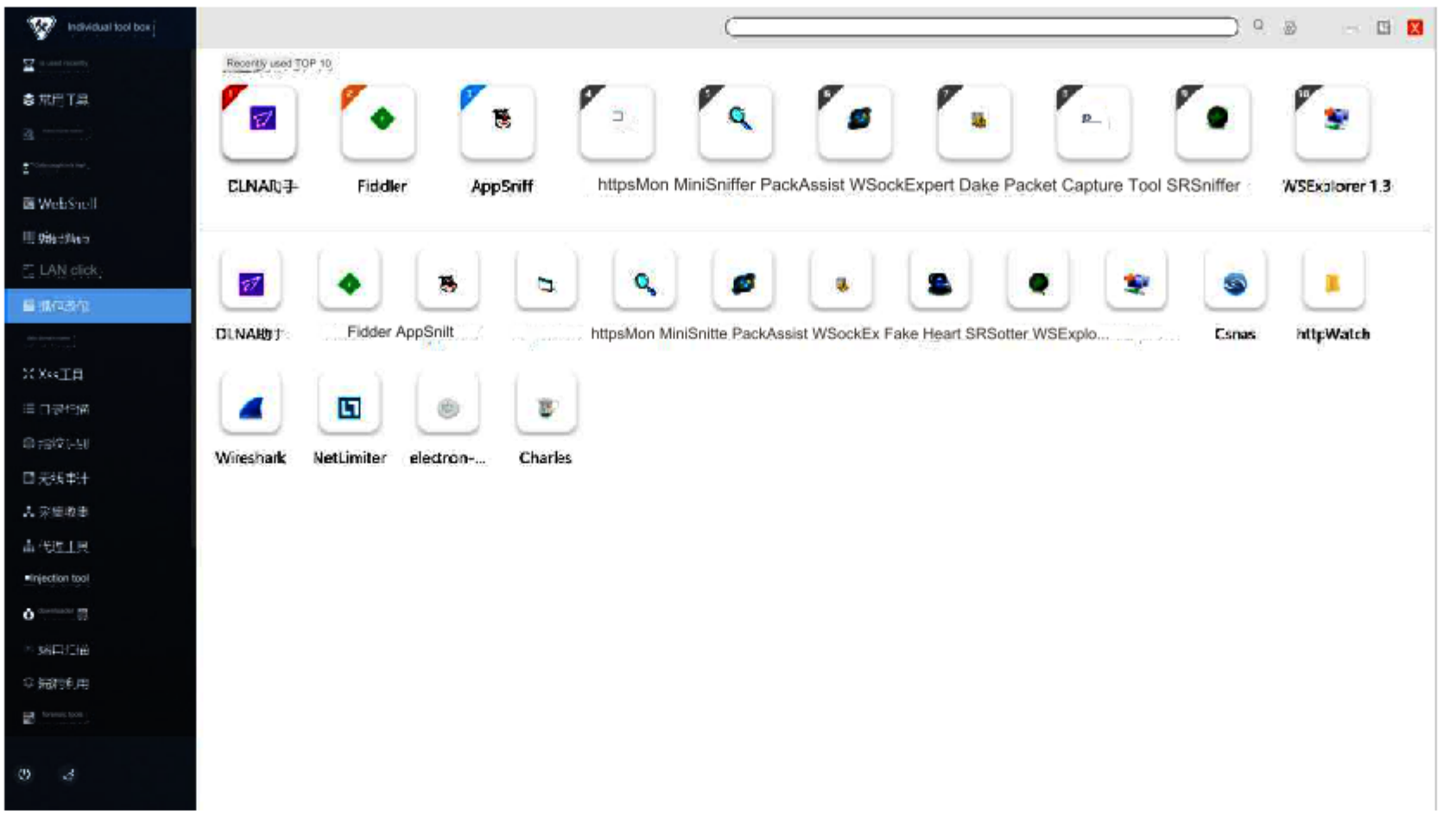
It has a large number of built-in tools and script files for LAN attacks, which can effectively carry out penetration attacks against the target LAN.



(LAN attack)

4.8 Capture and modify packets

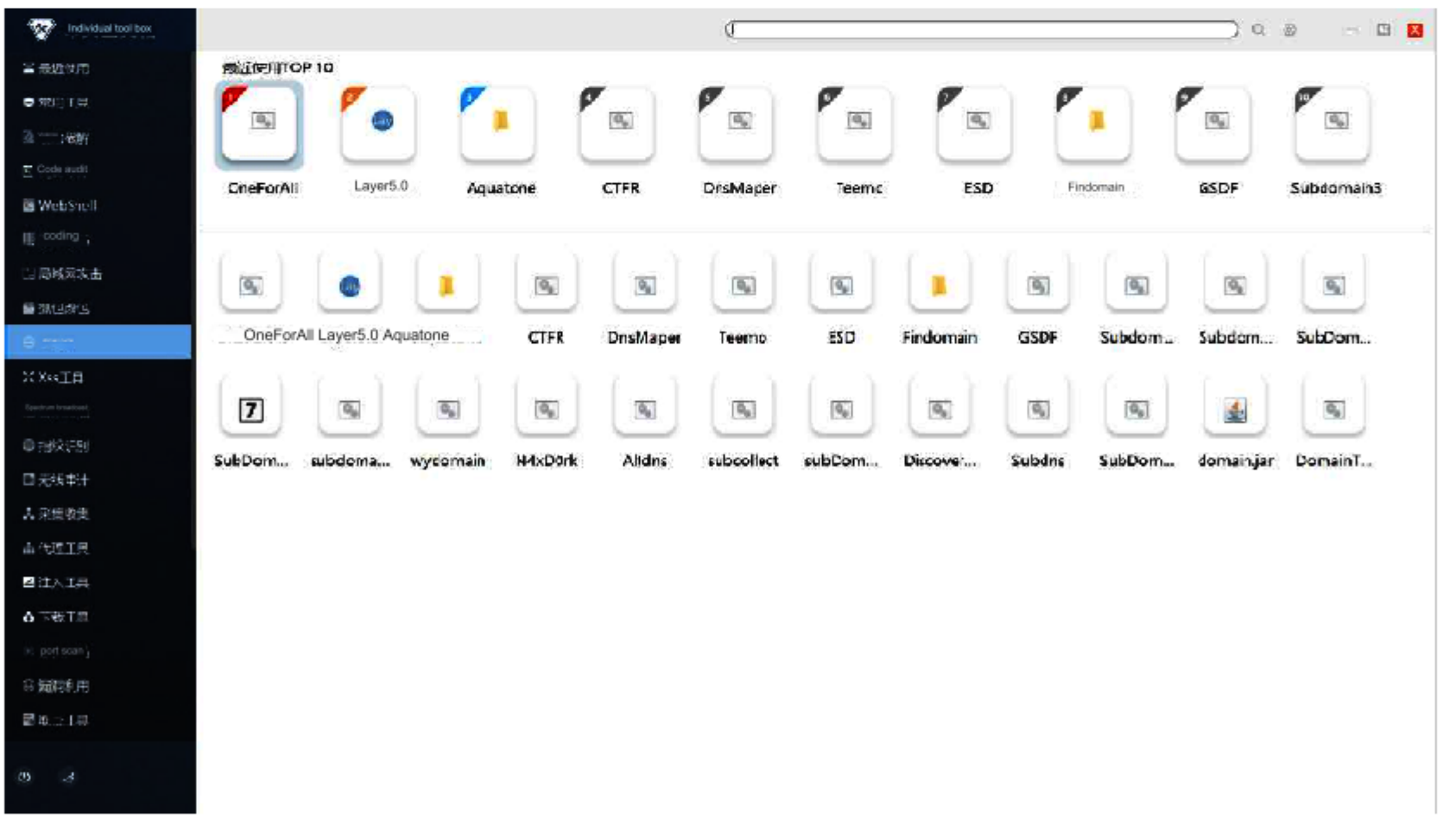
Integrate a large number of commonly used packet capture and modification tools to capture and modify packets for target traffic.



(Capture and change packets)

4.9 Subdomain name

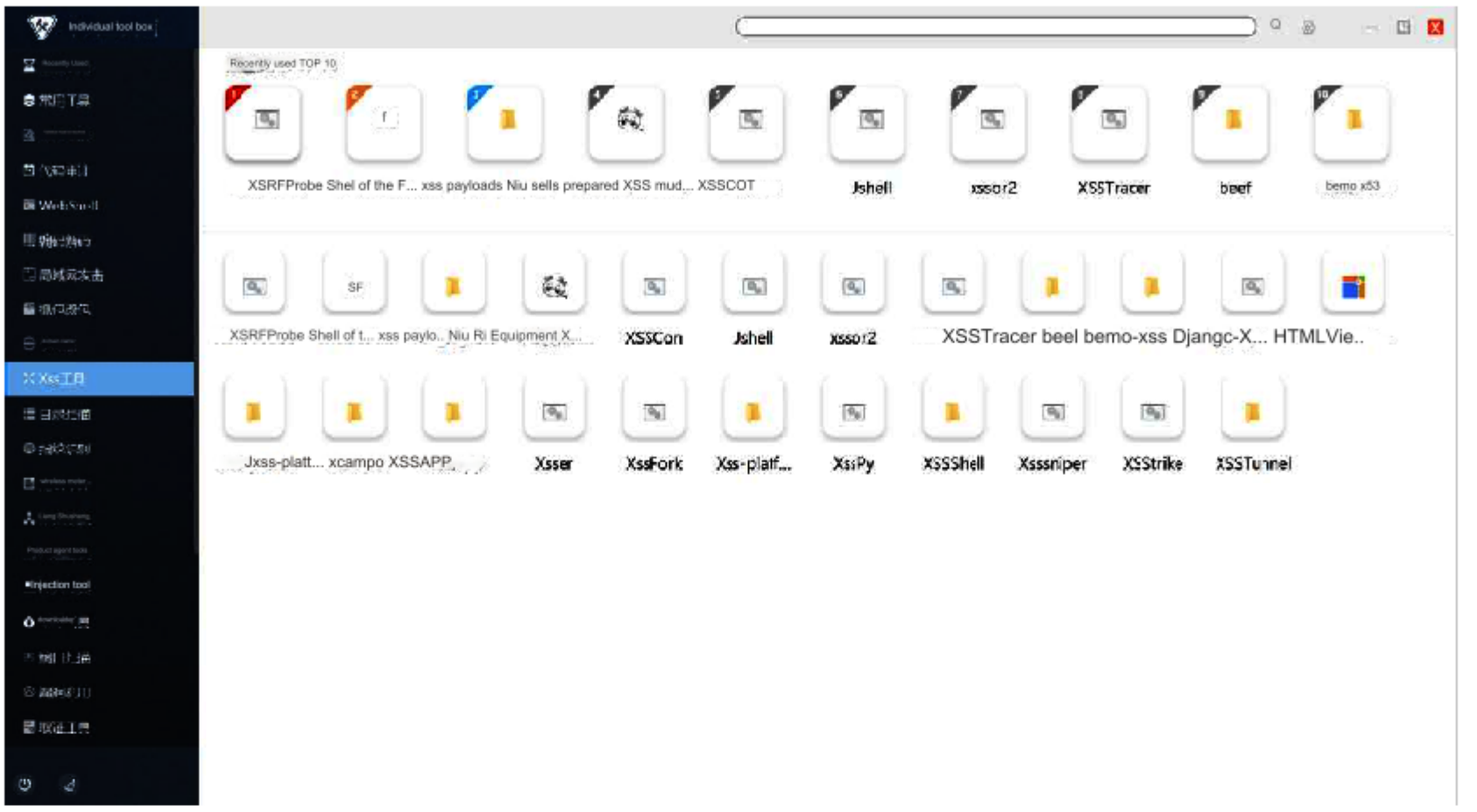
Built-in common domain name collection tools support information collection for subdomain names related to the target domain name.



(subdomain name)

4.10 XSS Tools

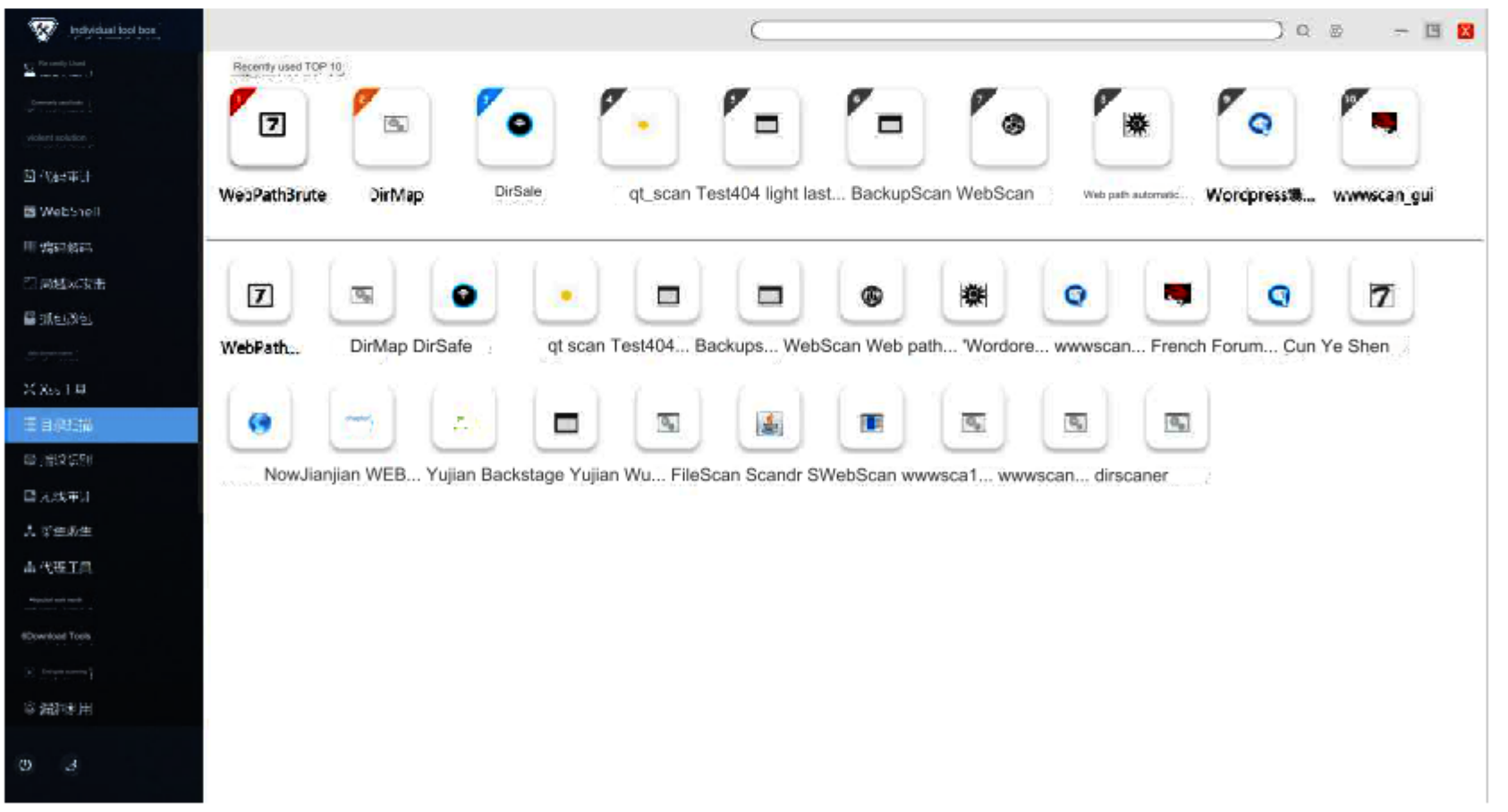
Built-in a large number of XSS attack tools, it supports delivering malicious script code to the client through the web site LD to achieve the purpose of attacking the client.



(XSS tool)

4.11 Directory Scan

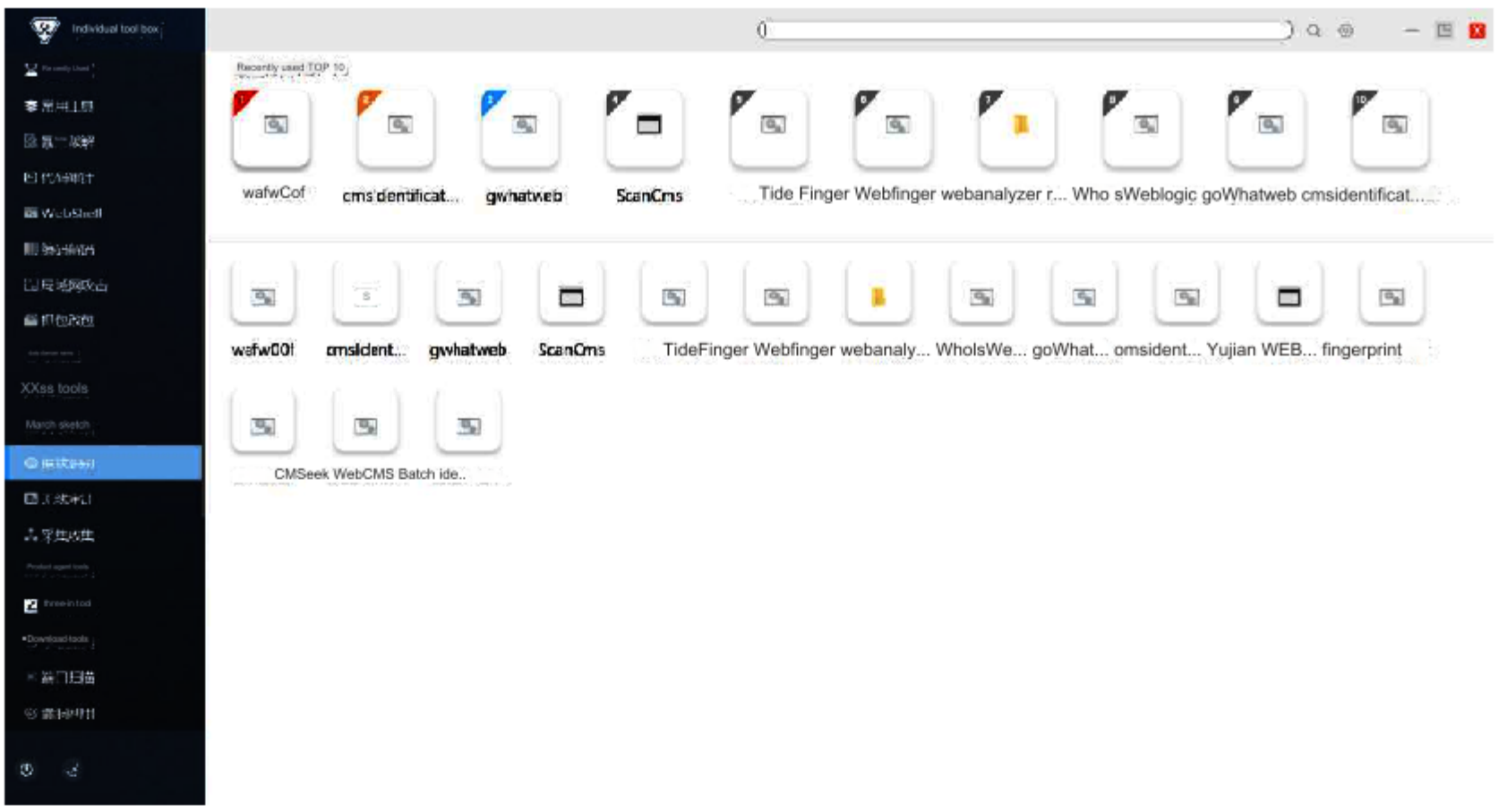
Built-in common directory scanning tools support scanning and information collection of directories existing under the target website.



(directory scan)

4.12 Fingerprint identification

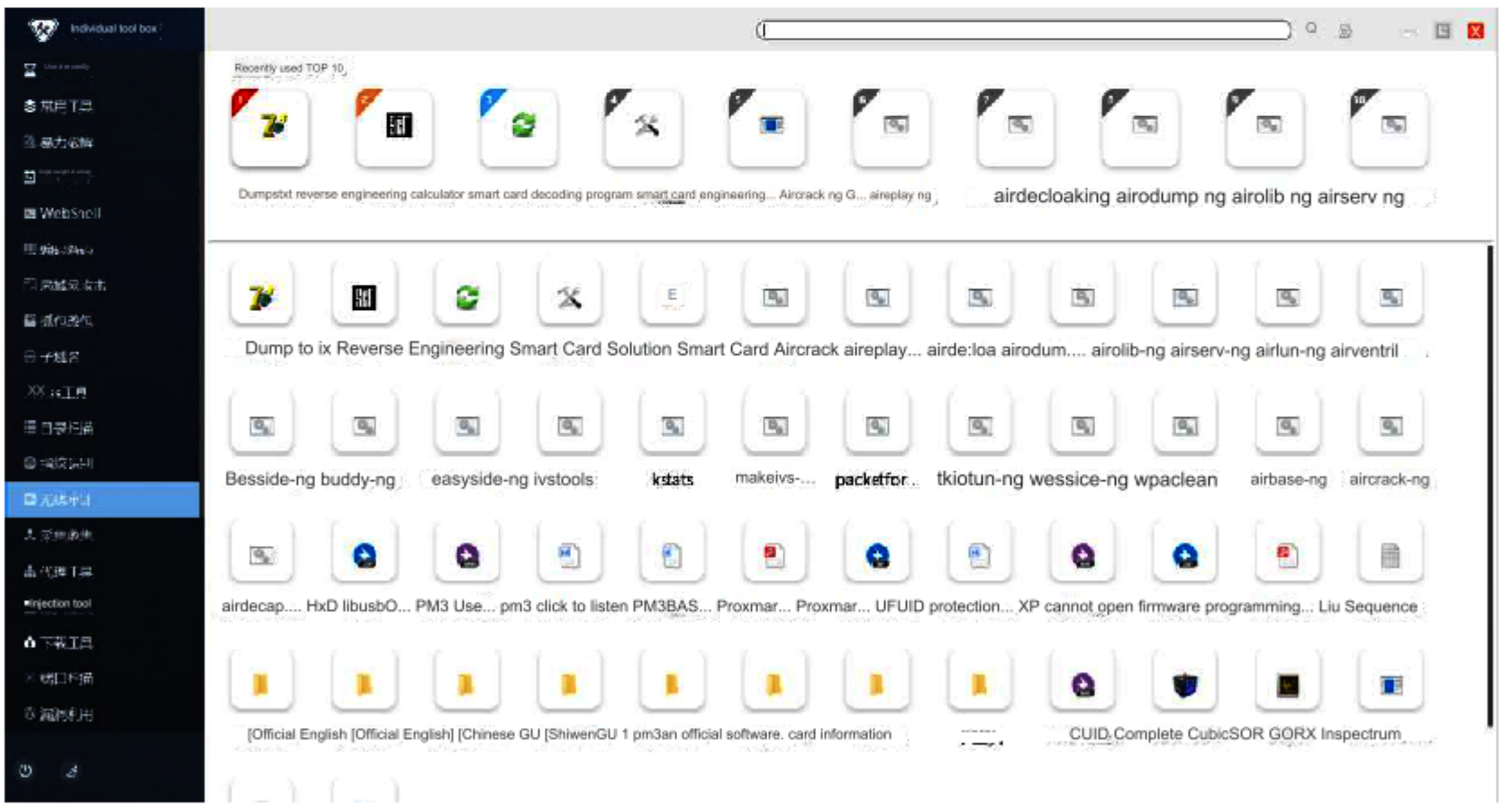
Built-in commonly used fingerprint identification tools support cracking target website fingerprint identification and are used to identify the basic information of the target website.



(Fingerprint recognition)

4.13 Wireless Audit

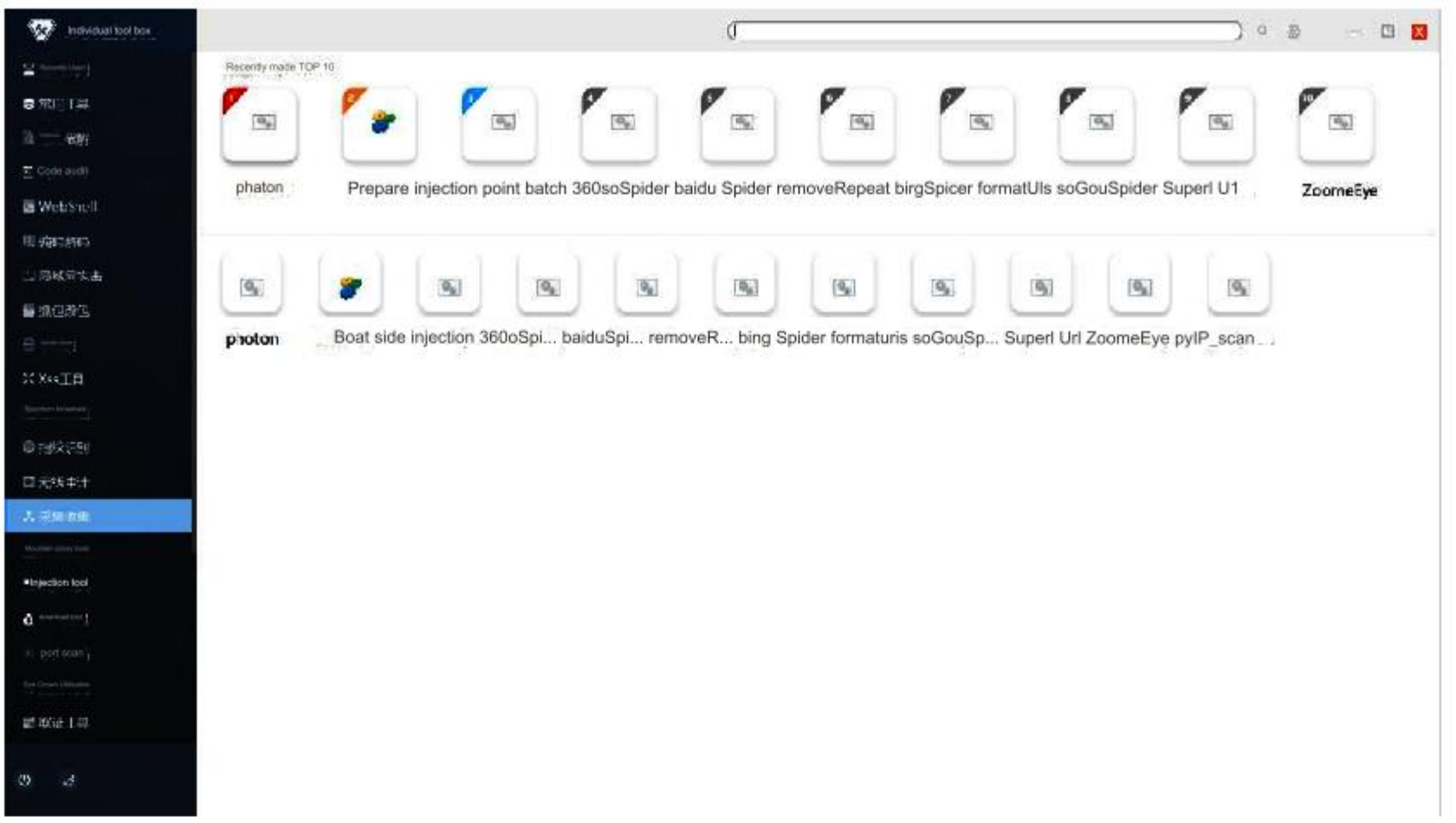
A large number of built-in wireless audit tools support capturing network data packets through wireless WIFI for compilation, classification, retention, and statistical analysis, including web pages, emails, instant messaging, downloads and uploads, online games, network traffic audits, etc.



(wireless audit)

4.14 Collection

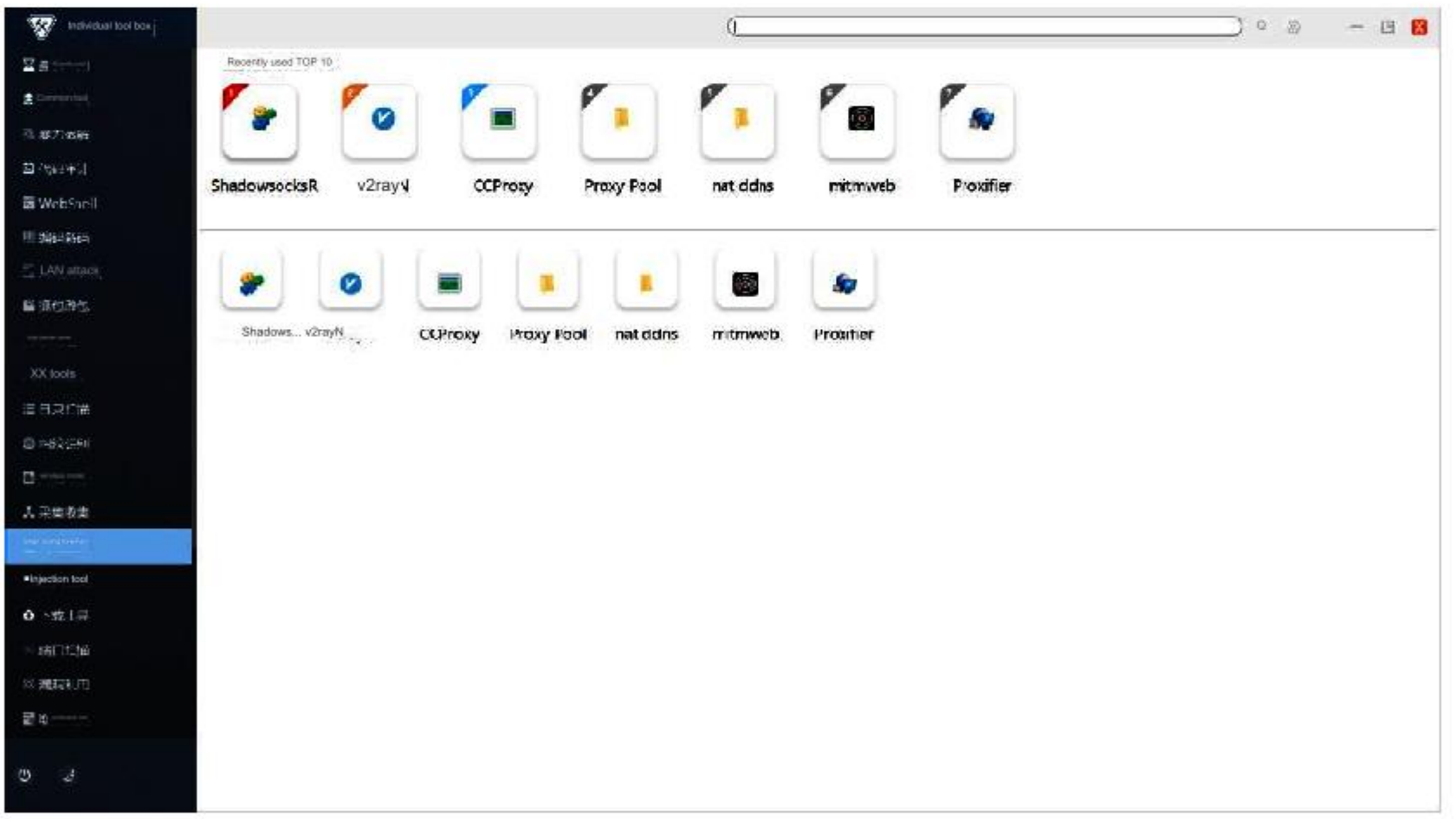
Built-in common information collection tools can search for target information through various browser search engines.



(collect collection)

4.15 Agent Tools

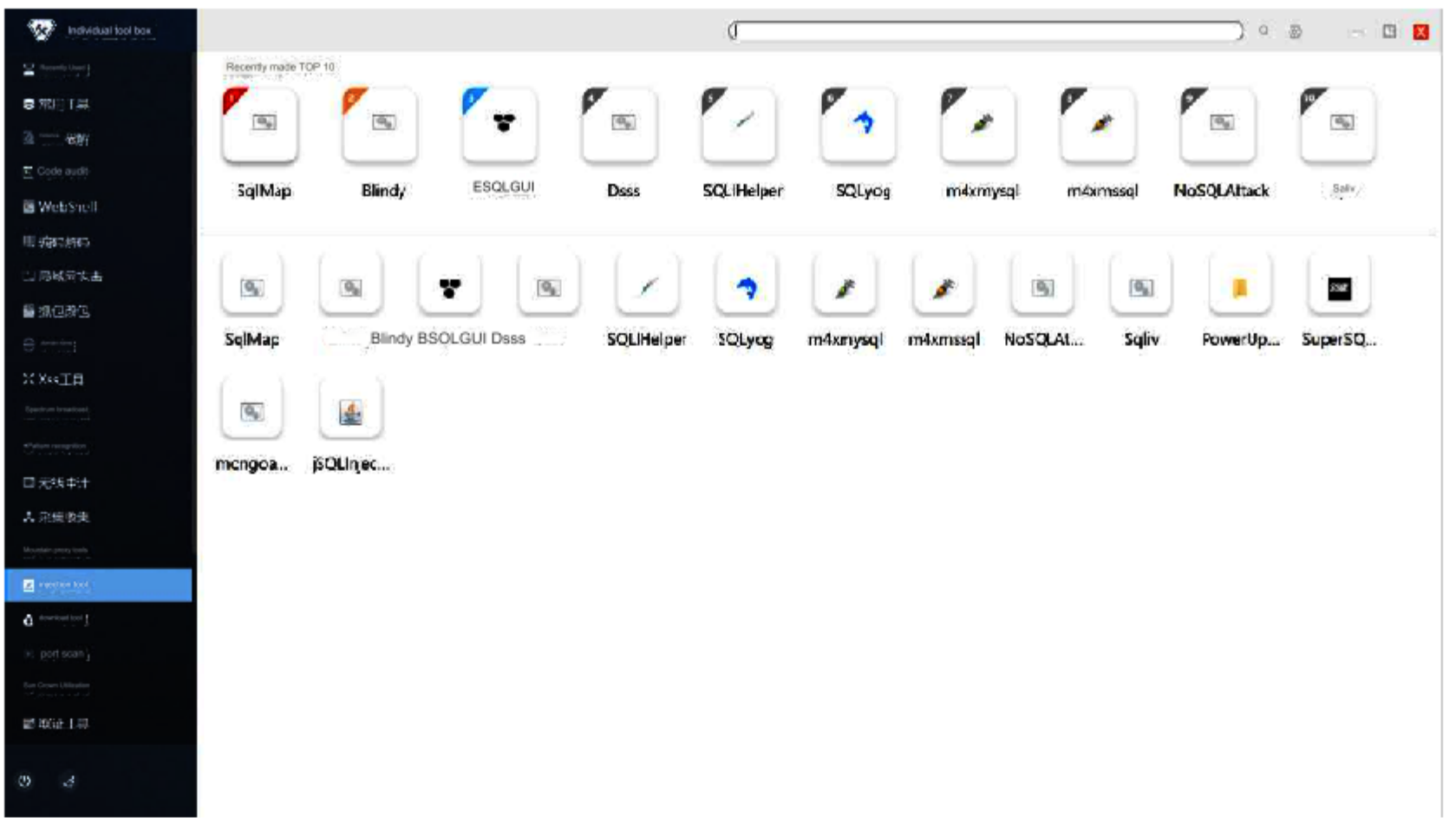
Integrated executable network agent task tools to facilitate users to perform network agent tasks.



(agent tool)

4.16 Injection tools

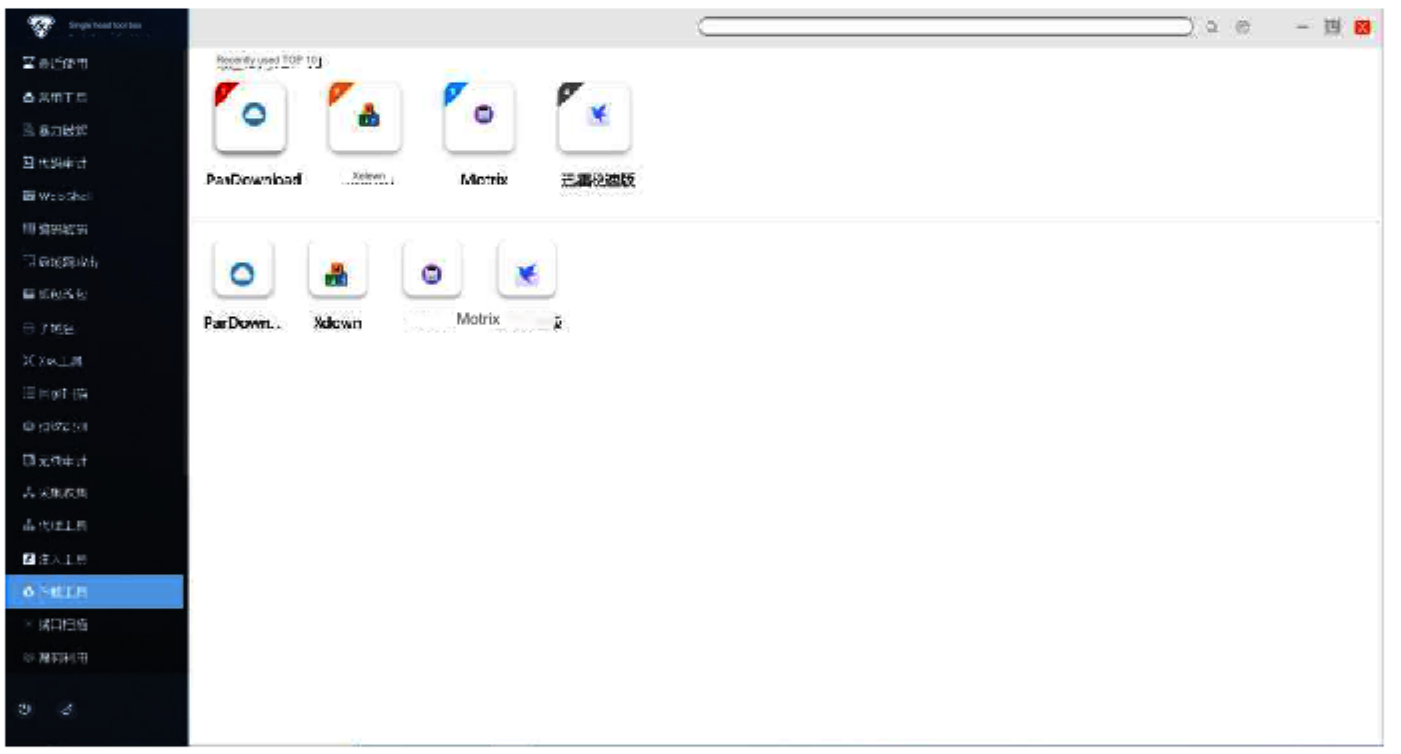
A large number of built-in SQL injection tools can be used for LD detection and utilization of SQL injection.



(injection tool)

4.17 Download tools

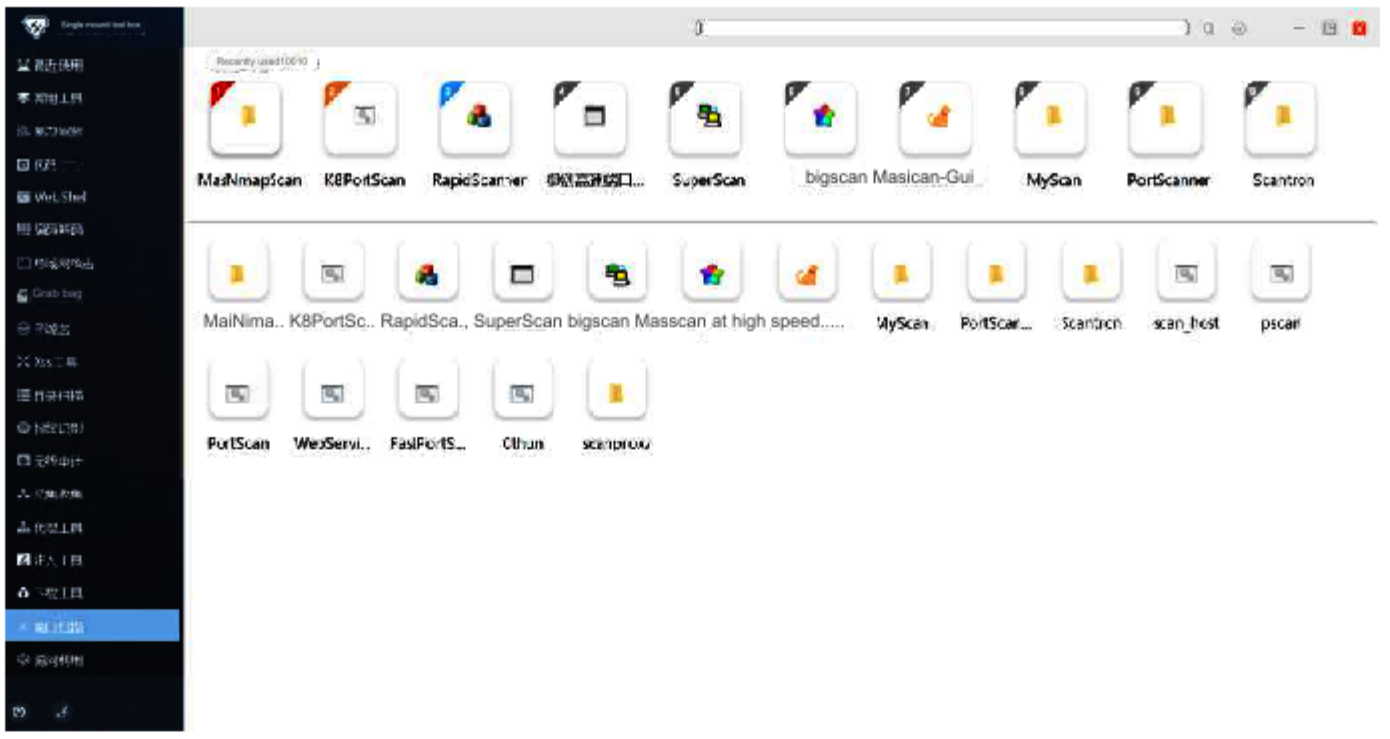
A large number of built-in network resource download tools, such as Thunder, PanDownload and Xdown, etc.



(download tool)

4.18 Port scanning

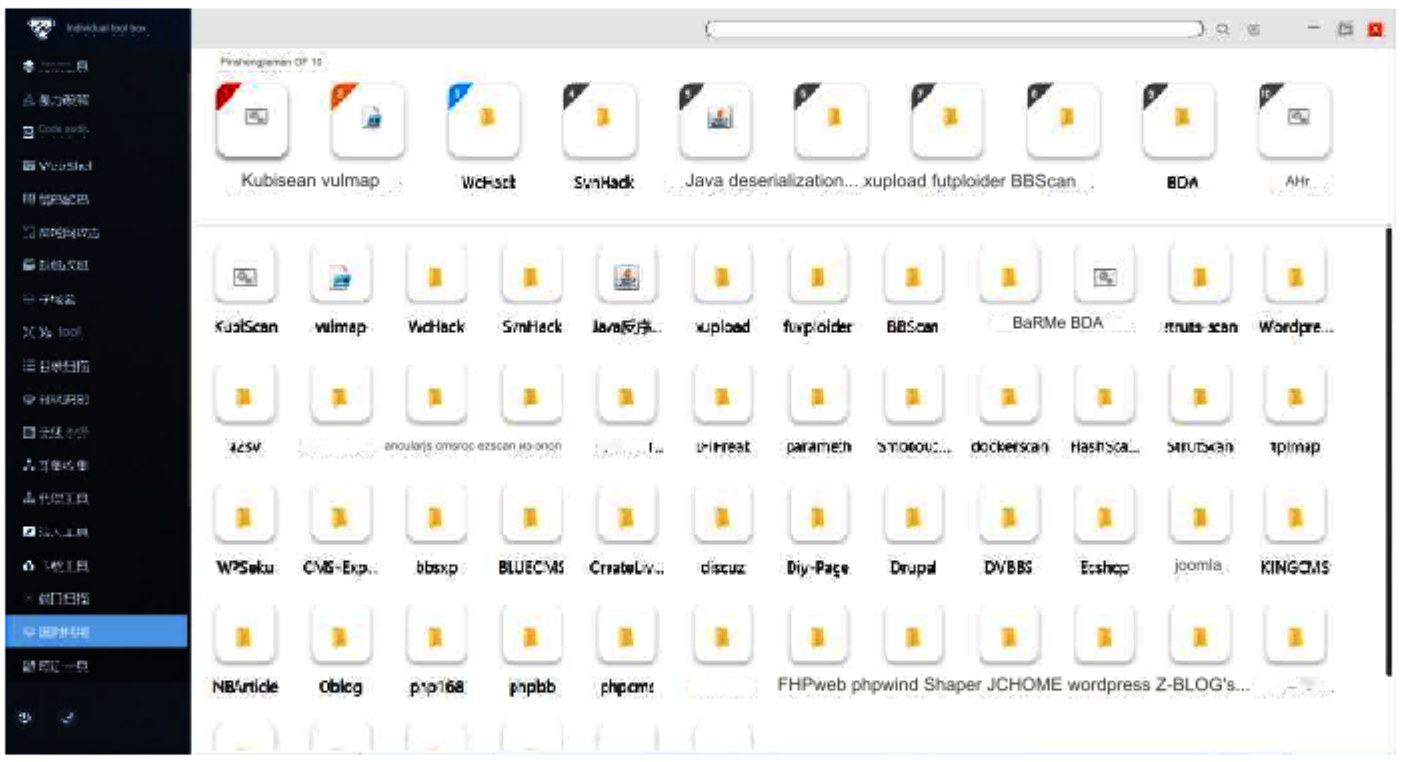
Integrated with a large number of port scanning tools, it can conduct online real-time detection of target port openings.



(port scan)

4.19 LD Utilization

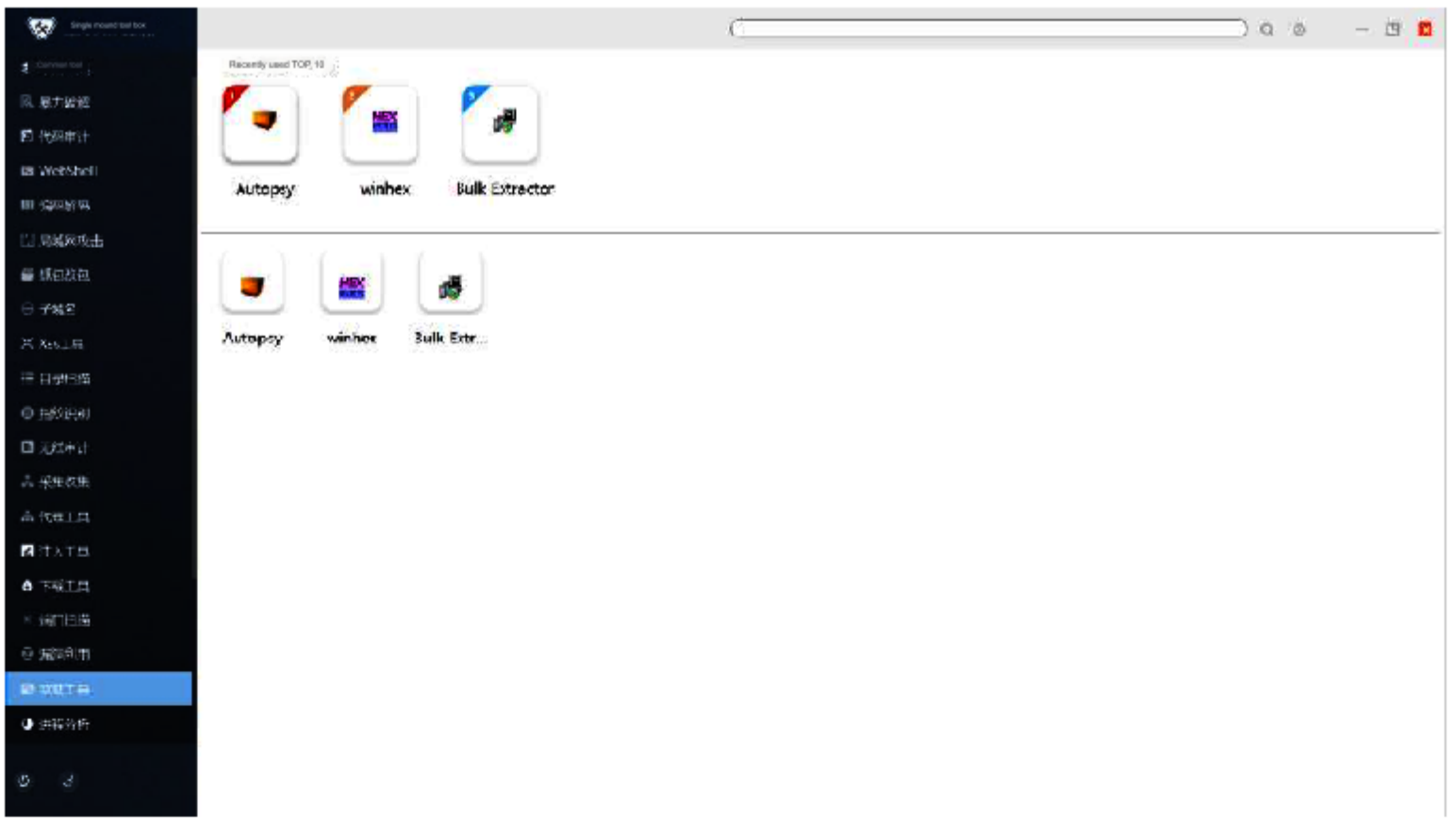
A large number of built-in LD utilization tools support the reuse of discovered LDs.



(LD use)

4.20 Forensic Tools

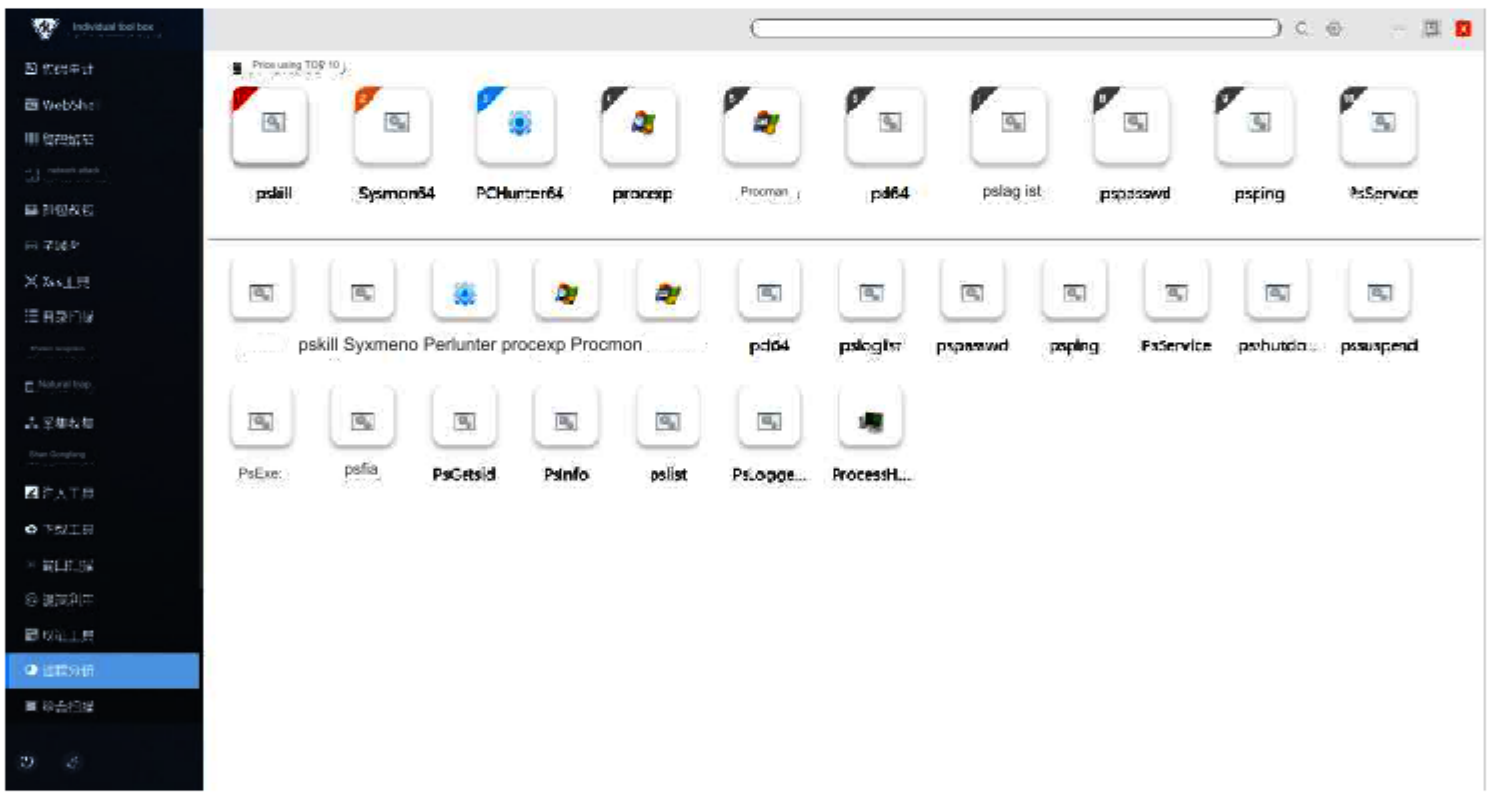
A large number of built-in forensic tools support efficient forensics and information collection on target computers, hard drives and files.



(forensic tools)

4.21 Process Analysis

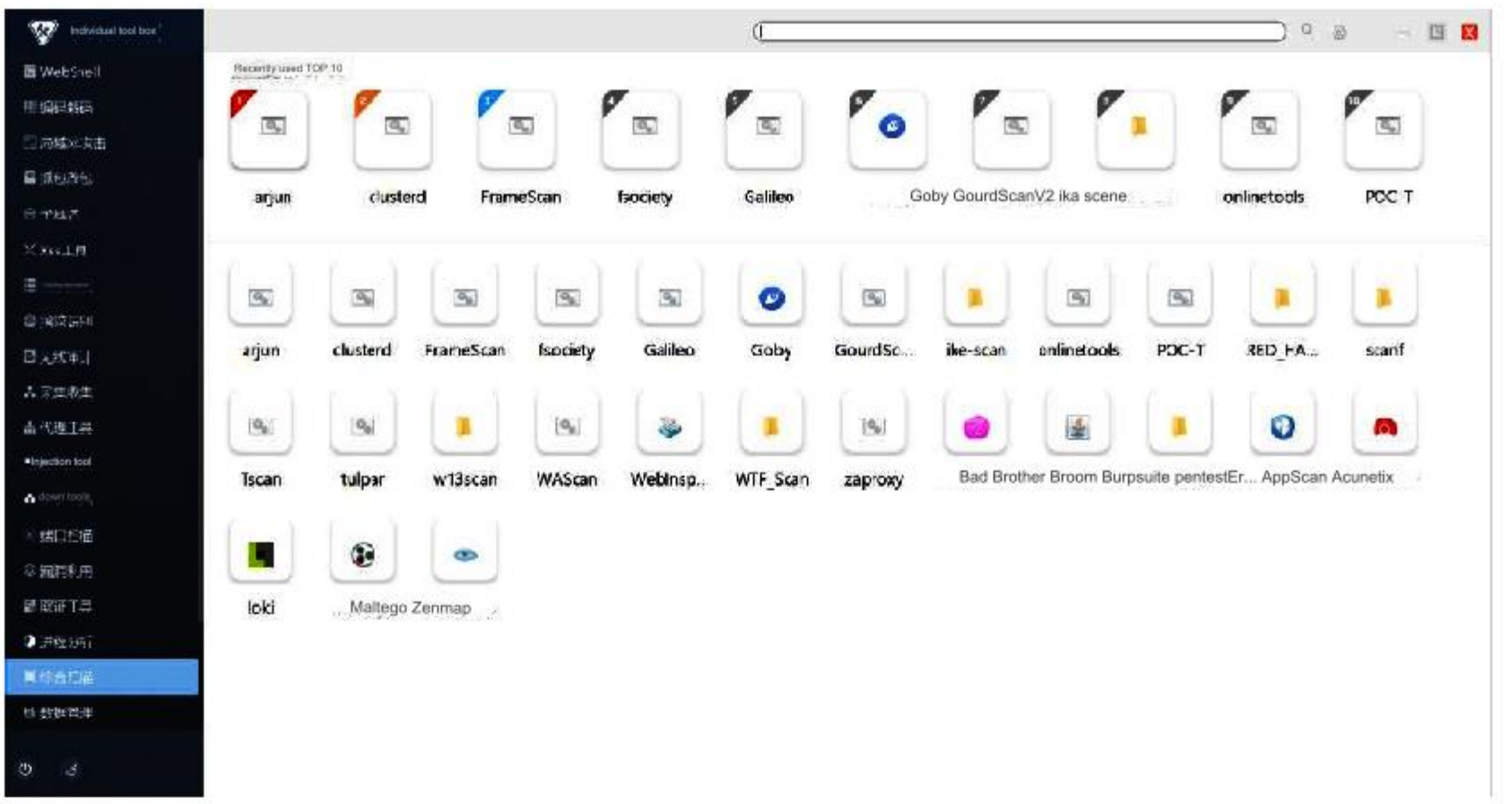
Supports process monitoring for targets and obtains information related to process running.



(process analysis)

4.22 Comprehensive scan

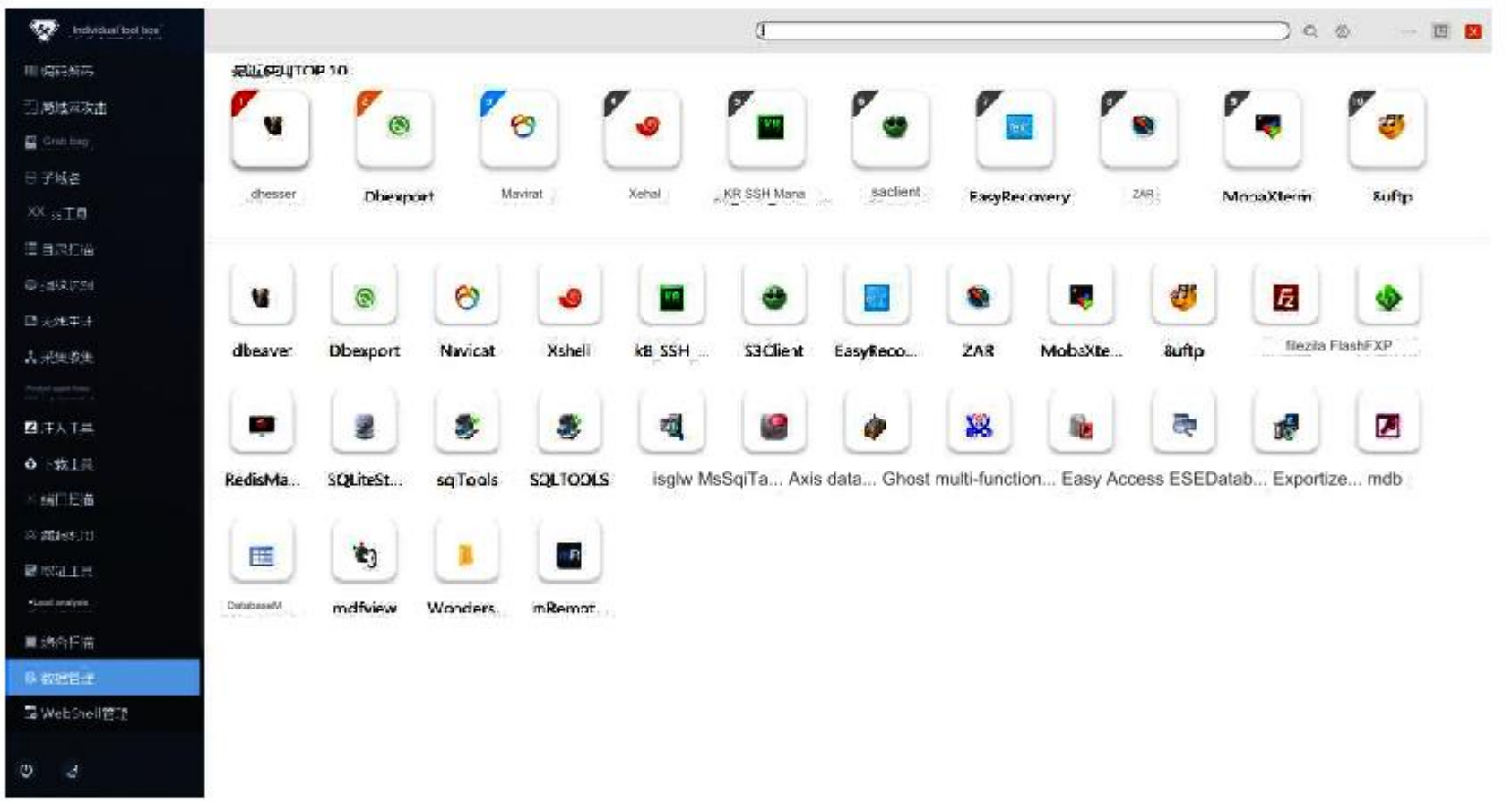
Integrate a large number of comprehensive scanning tools to support port scanning and website LD scanning of target hosts.



(comprehensive scan)

4.23 Data management

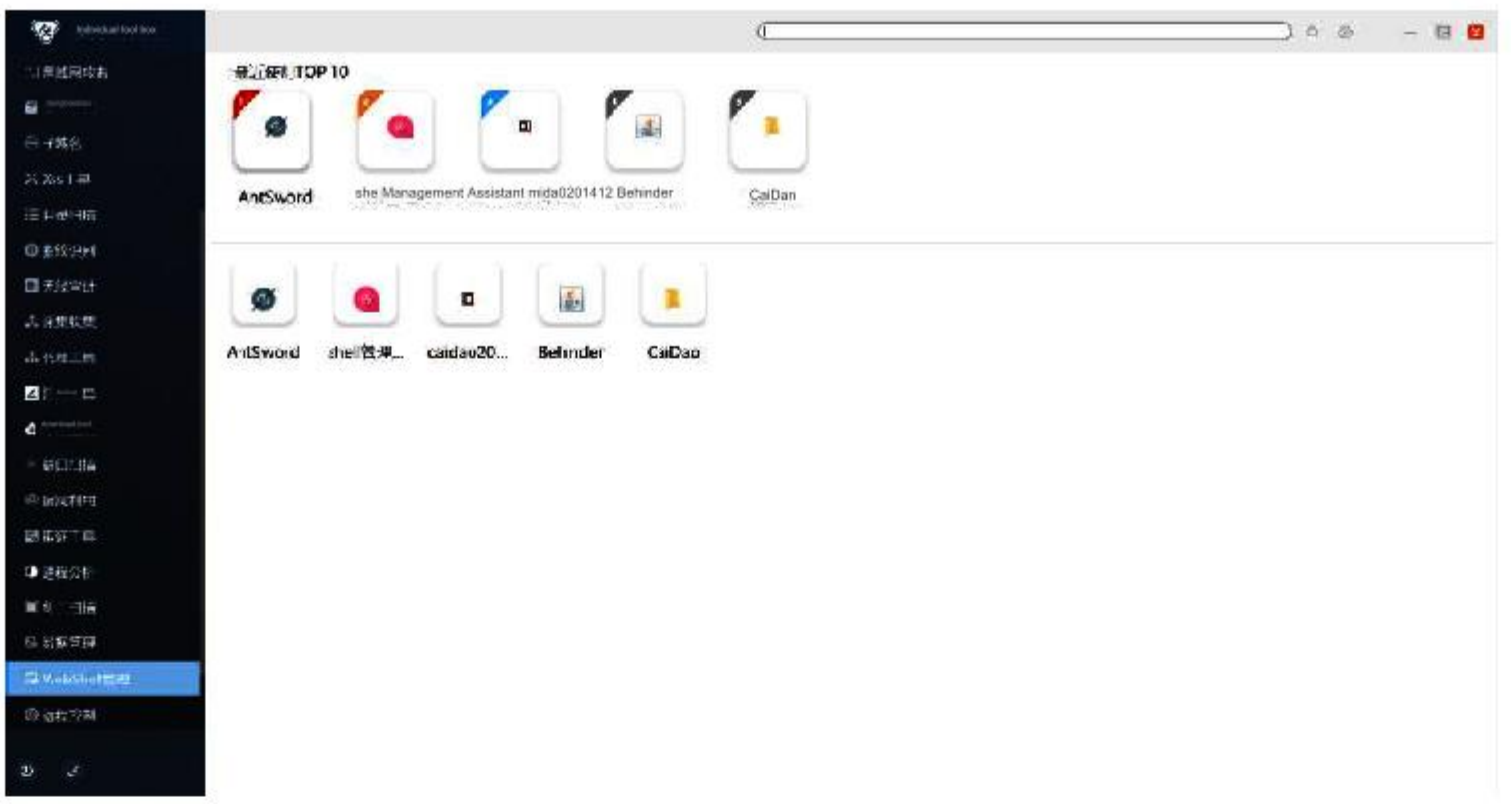
Provides data management and operation tools for visual operations on the database.



(data management)

4.24 WebShell Management

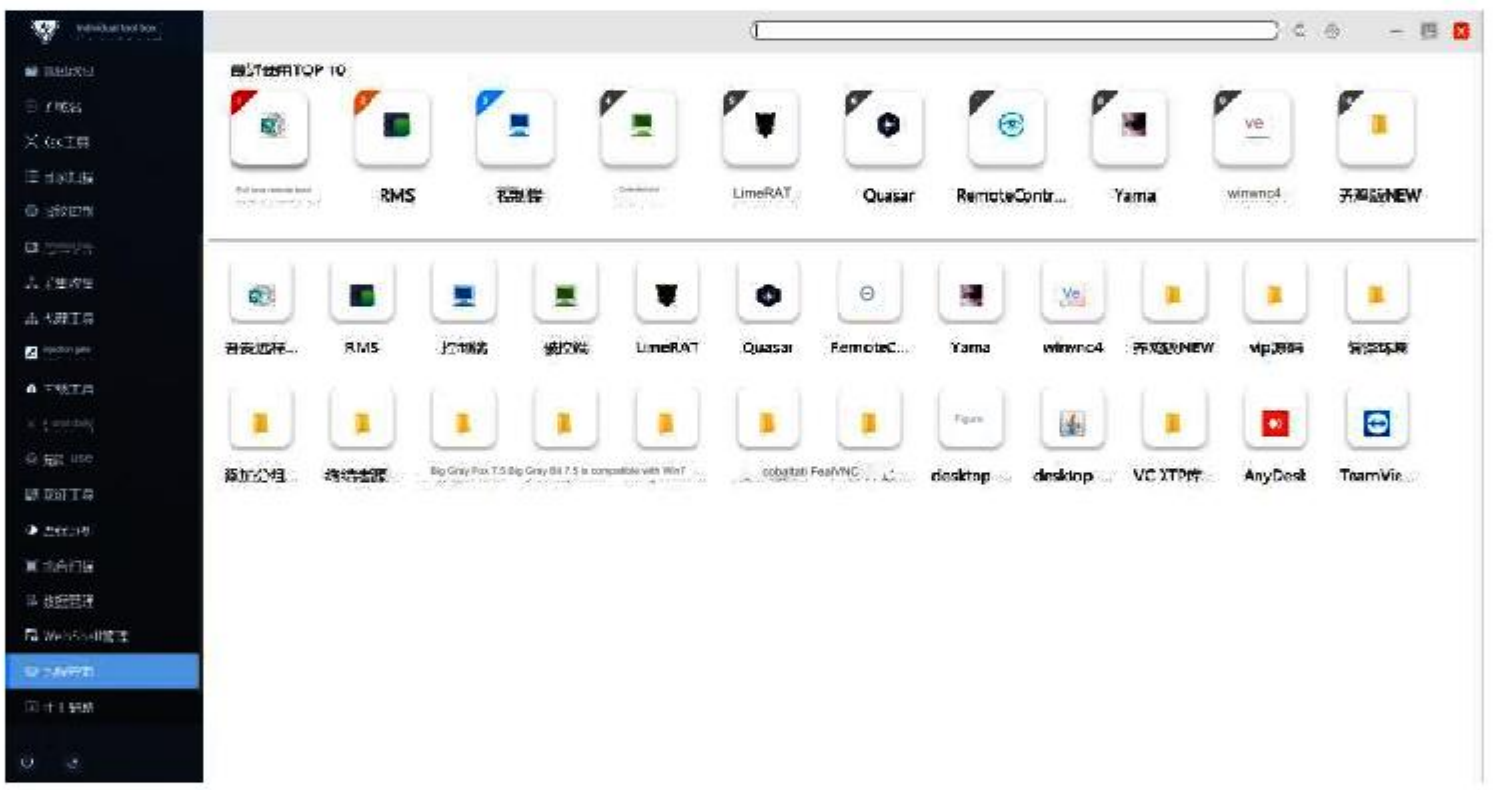
Provides WebShell management tools, which can be used for target site penetration testing and scientific management of target sites.



(WebShell Management)

4.25 Remote control

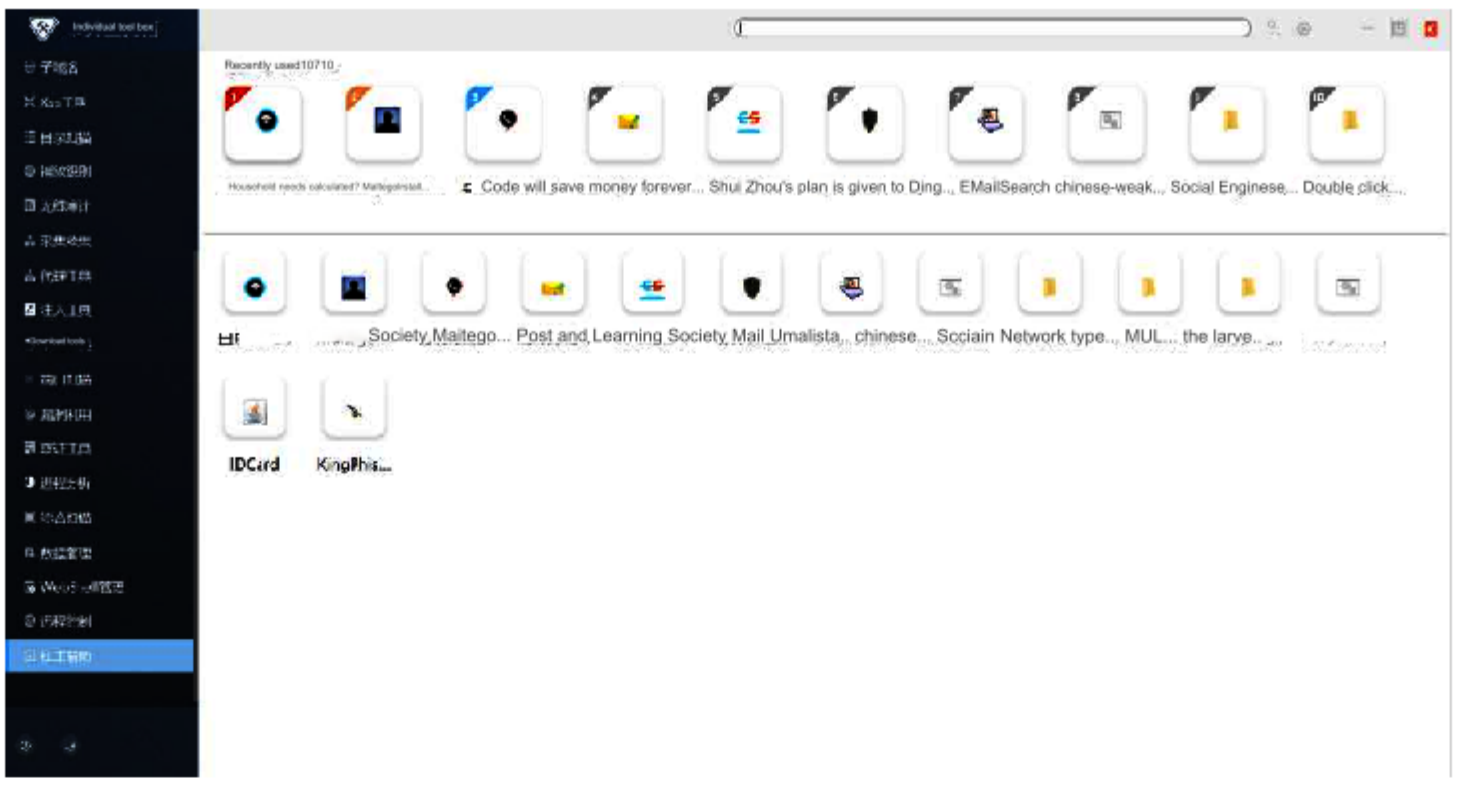
A large number of built-in remote control tools can be used for remote control connections to target hosts and sites.



(remote control)

4.26 Social work assistance

Integrate commonly used social engineering auxiliary tools, which can assist in generating and forging relevant information through partial information.



(Social Work Assistant)

5 Product parameters

category	parameter
processor	Intel Core i7-7700HQ，2.8Ghz
motherboard	Intel CM238 chipset
Memory	16384MB (2x8GB) DDR4-2666 SO-DIMM dual channel Memory
Hard drive capacity	1T+256GSSD
Screen specifications	15.6 inches
physical resolution	1920×1080
size	25x389x305(mm)
weight	3.548 kg + 810 g (notebook + 240W power supply)
Number of toolsets	Can be added according to actual situation

6 Product Deployment

6.1 Applicable environment

The "Individual Soldier Toolbox" is suitable for penetration testing of various network sites. It can be used as a special investigation method to remotely control and manage targets and obtain data and intelligence resources. The platform performs cluster management of various network special reconnaissance tools through high-performance notebooks. Users only need to open the "Individual Soldier Toolbox" and connect to the network to carry out special reconnaissance work on targets.

6.2 Deployment method

"Individual Soldier Toolbox" is a comprehensive management platform for professional special investigation software toolsets. It uses high-performance notebooks as carriers and professional special investigation software as technical means to carry out special investigation work on targets. Specific computer configuration requirements are as follows:

project	parameter
processor	Intel Core i7-7700HQ，2.8Ghz
motherboard	Intel CM238 chipset
Memory	16384MB (2x8GB) DDR4-2666 SO-DIMM dual channel memory
Hard drive capacity	1T+256GSSD
Screen specifications	15.6 inches

physical resolution	1920×1080
size	25x389x305(mm)
weight	3.548kg+810g (notebook+240W power supply)
Number of toolsets	Can be added according to actual situation

7 product advantages

> Strong camouflage

The professional penetration tool set is loaded on a high-performance laptop, which not only ensures the stability of the tool, but also ensures that it can be effectively disguised and not discovered when used.

> Powerful

It has a large collection of built-in professional penetration software tools to meet various network reconnaissance needs. All tools are accompanied by notes detailing the applicable environments of the tools.

> Quick navigation

For tools that are used more frequently, they are sorted according to the frequency of use. The top ten most frequently used tools can be displayed in the frequently used toolbar, which is consistent with usage habits and allows you to quickly locate commonly used tools.

> Good ease of use

The system is based on the Windows system environment and adopts a graphical operation interface, which is more in line with users' daily usage habits and enables quick search and use of various tools.

Bayingol Mongolian Autonomous Prefecture Project

Feasibility Cooperation Agreement

my country's Xinjiang Uyghur Autonomous Region, as a northwest border region with a relatively large area, a sparse population, and abundant resources, has seen the emergence of some terrorist organizations since the 1930s that have attempted to "separate Xinjiang from northwest my country"-as-their political agenda. Since our government has always promoted the economic and social development of Xinjiang's remote areas through scientific ethnic policies and social governance methods, and has used military force to crack down heavily on terrorist forces, the forces have gradually begun to carry out terrorist activities on the basis that they have no hope of splitting the country. Among them, the most famous terrorist organization of this type is the "East Turkistan" terrorist organization. While fleeing overseas to avoid attacks, it has developed close ties with religious extremism in Central Asia and the Middle East, sending terrorists back to the country to cause terrorist incidents and disrupt the law and order and attempt to cause social unrest.

Nowadays, various terrorist organizations make extensive use of modern communication technology for communication, command and dissemination; the methods and means of illegal and criminal activities have become more covert and diversified. Due to the convenience and uncontrollability of overseas communications, it has become a hotbed for the spread of laws and disciplines. In order to strengthen the effective monitoring of these terrorist organizations and combat terrorist activities, it is necessary to further-strengthen the investigation of relevant terrorist organizations and lawless elements. Based on this background, our company proposed to cooperate with the Bazhou Public Security Bureau to implement military-civilian joint, domestic and overseas cooperation and other strike methods to achieve in-depth counter-terrorism in Xinjiang and gradually build a comprehensive network-side defense force in the northwest region.

The first is anti-terrorism data support. Based on our company's APT work for more than ten years, we have controlled various types of server permissions and intranet permissions in multiple countries. (The specific data are in the following categories: anti-terrorism, political and economic, travel, military-related, and communications. The anti-terrorism data includes the postal service data of the Pakistan Punjab Anti-Terrorism Center, the Pakistani government postal service, and the Pakistani Punjab Police Postal Service. ,Pakistan Perouz Police Station Post Service,

Afghan National Security Council intranet + postal service, Southeast Asia Anti-Terrorism Center postal service, etc. Political and economic data include Malaysian Ministry of Foreign Affairs and Interior, Thailand Ministry of Finance and Commerce, Mongolian Ministry of Foreign Affairs and Police, etc. Travel data include AirAstanna Airlines Company, Air Macau, etc.; military-related data includes Malaysian Military Network, etc.; communications data includes Zong operator of Pakistan, Kcell and Beeling Communications Company of Kazakhstan, Mongolian Telecom and skytel operators, etc.) At the same time, our company has set up specific project teams for Afghanistan, Syria, Uzbekistan and Iran to collect network information on specific target organizations and prepare for infiltration implementation work. Based on the data support provided by our company, the Bazhou Public Security Bureau can reach a strategic cooperation agreement with our company and become a strategic partner in the anti-terrorism operation in the Xinjiang Uygur Autonomous Region. Provide effective technical support for Uyghurs' anti-terrorism activities in Xinjiang. It can achieve effective monitoring of anti-terrorism organizations in Xinjiang and combat terrorist activities, and further strengthen the monitoring and management of terrorist activities against Uyghurs in Xinjiang.

The second is technical services. Provide comprehensive technical services based on A-level assessment support, personnel training, specific target information acquisition and other aspects. In this cooperation, our company, as the first batch of companies shortlisted by the Ministry of Public Security, will provide customized support services to the Bazhou Public Security Bureau for the A-level proficiency verification assessment, including practice of corresponding types of examination questions and assault technology improvement training, and then Effectively and quickly improve the technical capabilities of the Bazhou Public Security Bureau and improve the assessment pass rate; based on the real business situation of the Bazhou Public Security Bureau and the actual training needs, our company will conduct customized network attack and defense practical training for the Bazhou Public Security Bureau. The training courses are all conducted by our company's professional network attack and defense technical talents. Through preliminary theoretical knowledge training, trainees can understand attack and defense principles, techniques, and basic operations. After the trainees have accumulated a certain amount of theoretical knowledge and understanding, our company will provide the Bazhou Public Security Bureau with practical training operations based on its own research and development and design of a practical training platform to improve the trainees' actual network attack and defense capabilities; and obtain information for specific targets. Services, covering personal terminal remote control and targets

Network penetration attack: Provide network penetration and remote control services for users' key personal target terminals. right

Provide network penetration attack services for users' key target network environments. This will effectively improve the efficiency and convenience of the Bazhou Public Security Bureau in obtaining target information.

The third is to launch a talent training plan. In order to better respond to anti-terrorism activities in Xinjiang, as well as the Bazhou Public Security Bureau's employment strategies and goals for network security, information security and other related positions, our company proposes to give full play to the three-party in-depth cooperation between the Bazhou Public Security Bureau, enterprises and schools. With the resource advantages of all parties, we can continue to effectively promote the establishment and improvement of a full-chain talent supply and demand mechanism such as talent training, introduction, and transportation; on the one hand, we can quickly cultivate and output information security technical talents with high matching and strong professional practical ability for the Bazhou Public Security Bureau. , On the other hand, it effectively promotes the targeted and effective goals of the talent training output of cooperative colleges and universities, comprehensively improves the employment level and quality of students, and truly realizes the common development and win-win cooperation of "units, enterprises, and schools". The training adopts a school + enterprise joint approach to carry out targeted class training and targeted class teaching management, thereby effectively cultivating multi-directional technical talents.

The fourth is comprehensive laboratory construction. According to the latest requirements of my country's national policies: In order to promote the hierarchical construction of my country's network special investigation teams and laboratories, and enhance the online proactive offensive capabilities of my country's network security departments. In accordance with the requirements of documents such as the "Opinions on the Implementation of the Construction of Cyber Special Investigation Teams" (Gongban [2010] No. 128), the "Specifications for the Cybersecurity Investigation of Public Security Bureau Cybersecurity Departments"-(Gongban [2010] No. 2159) and other documents, cyber security departments across my country will Carry out the construction of a network special investigation laboratory based on its own actual situation. Comprehensive laboratory equipment is-different from traditional network investigation and control equipment. It mainly provides operational support and technical support for attack penetration, target control, attack process security protection and other aspects of the network special investigation work of the public security agency's network security department. Based on the actual situation of hierarchical construction of characteristic laboratories of law enforcement departments and the latest standards of hierarchical construction of laboratories in my country, law enforcement departments still need to continue to improve the construction of relevant special investigation equipment.

> Attack equipment: With the purpose of "attacking forward", actively develop active offensive weapons and equipment in cyberspace. It can simultaneously carry out intrusion, penetration, interference and destruction of traditional network applications and new network applications.

work such as destroying, cracking down and suppressing.

> Protective equipment: With the goal of "preventing" and based on the need for active attacks in cyberspace, we build-a-security protection system that covers the entire workflow of attack terminals, resource links, monitoring and auditing, and security detection.

> Reconnaissance equipment: With the goal of "deep reconnaissance", based on the needs of network TZ means intelligence reconnaissance under informationization conditions, we build TZ intelligence reconnaissance equipment oriented to the Internet, WiFi hotspots, communication networks, and user basic information networks to realize the realization of cyberspace Precision operations provide all types of intelligence.

> Control equipment: With the goal of "long-term control and defense", based on the secret control and defense of key people, key objects, and important network nodes in special investigations; the development is oriented to different network applications, different terminal firmware, different network environments, and different application scenarios. long-term control equipment.

> Linkage equipment: With the goal of "integrated linkage", it is based on the overall coordination and mobilization of various business links such as active attack, active defense, intelligence reconnaissance, target control and defense, and data concealment and encrypted transmission to form a TZ linkage data center to ensure TZ operations Synchronized and integrated development in cyberspace. Combined with the needs of comprehensive laboratory construction, our company can currently provide special equipment mainly including:

1. Attack equipment: network attack and defense training platform, network attack and defense combat platform, WiFi proximity attack system, automated penetration testing platform, and Shen Shuanzi password cracking platform.

2. Protective equipment: anonymous anti-tracing wall, scientific Internet equipment.

3. Reconnaissance equipment: network terminal fingerprint probe system, individual soldier toolbox, R&D test toolbox, reverse analysis toolbox, security attack toolbox, and remote detection toolbox.

4. Control equipment: email encryption platform, Twitter control evidence collection platform, Android remote control management system, Windows remote control management system, Mac remote control management system, Linux remote control management system.

5. Linked equipment: Anxun cloud intelligence data query platform, email analysis intelligence decision-making system, and single data query platform.

Matters not covered in this agreement can be improved in a timely manner according to actual needs after friendly negotiation between both parties.

This Agreement shall come into effect from the date of signing.

There are two copies of this Agreement, each party holds one copy.

Xinjiang Bazhou Public Security Bureau

signature:

year month day

Sichuan Anxun Information Technology Co., Ltd.

signature:

year month day

Individual tool box

Product white paper

(V1.0 version in 2022)