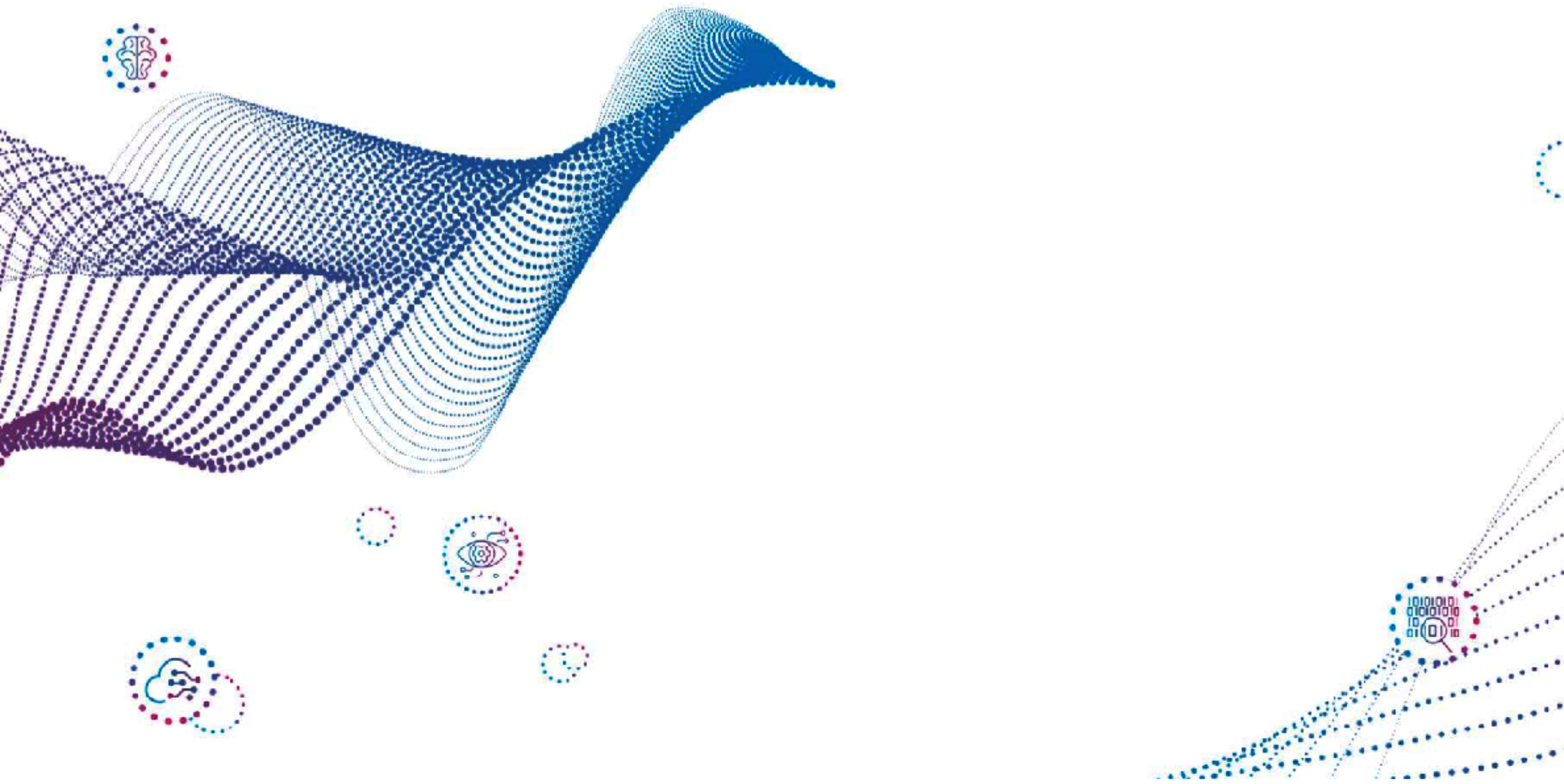


Automated penetration testing platform

Product white paper

(V1.0 version in 2022)

Table of contents

1 Introduction

Catalyzed by frequent security incidents, network information security has risen to a national strategic level. Security testing and evaluation are an essential part of information security assurance measures. Article 38 of the National Cyber Security Law stipulates that “Operators of critical information infrastructure shall conduct inspections and assessments of the security and possible risks of their networks at least once a year on their own or by entrusting a network security service agency to do so.” From the frequent exposure of important security vulnerabilities and related events every year, we can know that only continuous security testing and evaluation can achieve effective security defense results.

As network security receives more and more attention from people, penetration testing, as a means of most realistically reflecting the security risks existing in information systems, has attracted more and more attention. Among security detection and evaluation technologies, penetration testing is widely considered to be the best test of system security because it is closest to real-world attacks. Performing these tests typically requires a significant amount of time from highly skilled personnel to perform, and ideally the engineers performing these tests need to meet or exceed the skill level of potential attackers.

Therefore, it is necessary to develop such-a-penetration testing platform that can carry out active attacks on the system, provide basic functions such as detecting security vulnerabilities in the system, and test the impact of new attack technologies, and simulate attacks through the penetration testing services provided by the penetration testing platform.

Evaluate the security of application systems and equipment.

2 Requirements analysis

Since the existing network penetration testing theory is still in the process of rapid development and change, the corresponding practical technology also relies heavily on the personal technical level of network security experts. Through the construction of "automated penetration testing platform", on the one hand, it solves the problem that security managers have limited technical level and cannot master effective penetration testing knowledge in a short time. On the other hand, due to the expensive and high cost of the tools on the market, it is impossible to truly To meet practical purposes such as simplicity and ease of use for users, the construction of this platform can provide some simple and easy-to-use tools for those with a certain-professional foundation. The construction of the entire platform needs to meet the following requirements:

(1) Detect the security of the target network

Penetration testing, as the main means of network system security testing, can effectively evaluate the target network security problems and possible risks of. The "automated penetration testing platform" supports penetration testing of the target network according to the actual needs of the user, and obtains the target

Network data information. At the same time, the platform has a large number of built-in attack templates and tools. Through simple configuration, users can conduct penetration attacks on the target network, detect vulnerabilities and risks in the target, and determine the security of the target network.

(2) Automated vulnerability verification

Vulnerability exploitation is an extremely important part of penetration testing. Accurately determining the exploitability of selected vulnerabilities is the most critical step before vulnerability exploitation. Single analysis is extremely prone to risky errors. The "automated penetration testing platform" supports the import of missed scan reports from other manufacturers to verify whether key high-risk vulnerabilities can be exploited, providing convenience for penetration testing and prompting users to discover and repair key critical vulnerabilities as soon as possible. Security Risk.

(3) Professional penetration testing report

As a summary of the penetration test, the penetration test report determines the final result of the penetration test. The traditional manual penetration test report depends on the professionalism of the penetration tester, which can easily lead to a situation where the test report is not professional enough. The "automated penetration testing platform" supports the generation of professional test reports, supports multiple file formats and multiple report templates for use in different scenarios, ensuring that users can resolve the vulnerabilities of their networks or devices based on the reports.

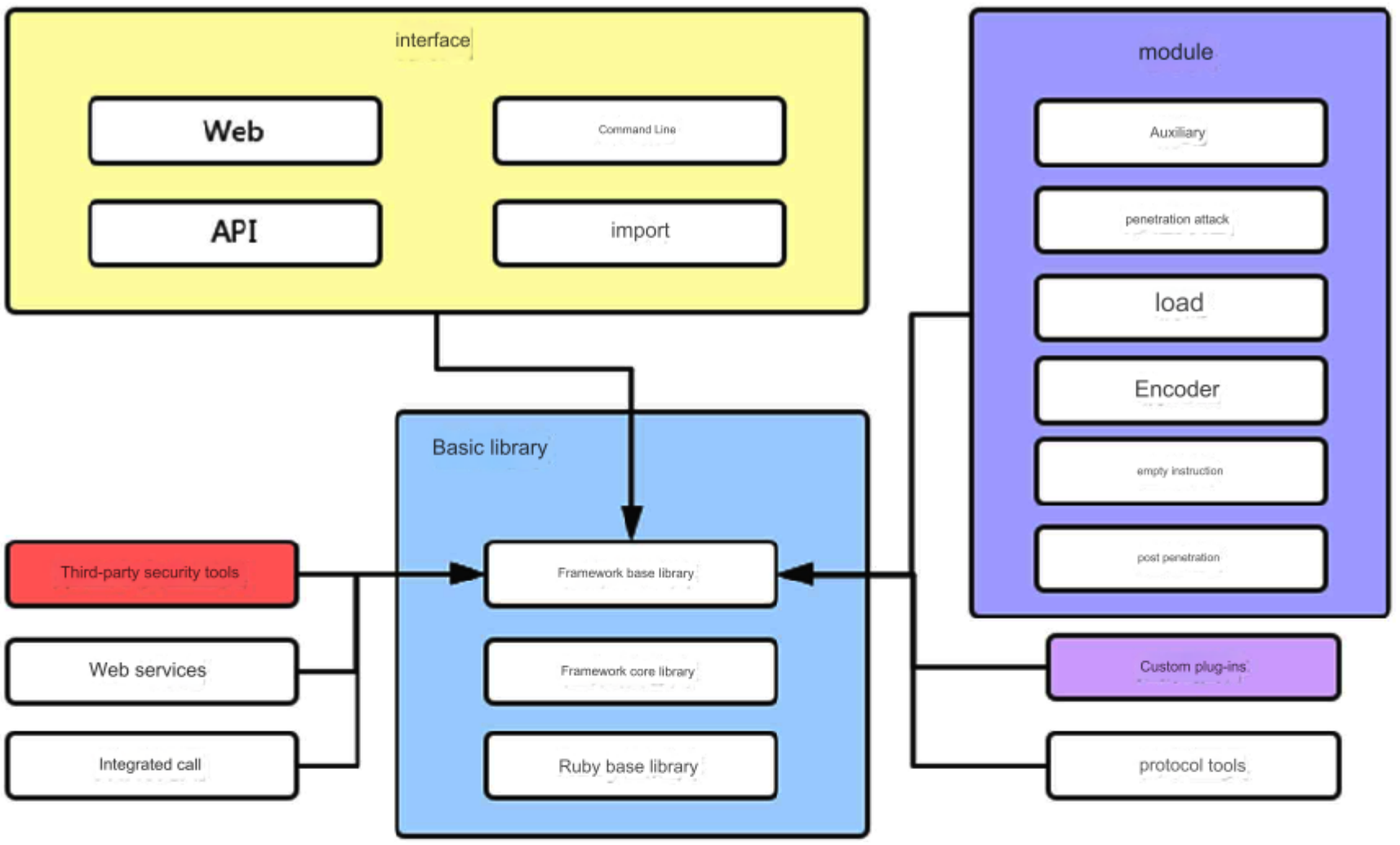
3 Product Introduction

3.1 Product introduction

"Automated Penetration Testing Platform" is a platform that integrates hundreds of vulnerability templates and penetration testing methods to support automated penetration testing of various network devices and hosts. Attack the real production environment through a variety of testing methods built into the platform to realize the test platform. Through information detection, vulnerability verification, vulnerability exploitation, penetration attacks and report generation of Platform F network and equipment, the efficiency, convenience, completeness and accuracy of penetration testing are improved.

3.2 System architecture

The construction of the "automated penetration testing platform" is based on the Ruby language and adopts a highly modular design. Generally speaking, it is divided into 4 parts: basic libraries, modules, interfaces and other third-party integration tools or plug-ins.



(system architecture diagram)

> Basic library

The basic library is the core part, and other functional modules are coupled together through it. It not only provides interaction with various functional parts, but is also responsible for project management, session management, log management, etc.

1) Framework base library

The framework base library is responsible for implementing all interactive interfaces with various types of upper-layer modules and plug-ins.

2) Framework core library

The framework core library extends the framework basic library, provides simpler packaging routines, and provides some functional classes that do not handle various aspects of the framework to support user interfaces and functional programs that call the framework's own functions and framework integration modules.

3) Ruby basic library

The Ruby base library is the most basic components on which the entire framework depends, such as wrapped network sockets, network application protocol client and server implementation, logging subsystem, penetration attack support routines, Po penetration greSQL and MySQL database support wait.

> Module

The module part is the part closely related to vulnerabilities and vulnerabilities in security detection, and is loaded and used by the framework. According to the penetration testing process

The different uses in each link are divided into auxiliary modules, penetration attack modules, post-penetration attack modules, payload modules, null command modules, encoder modules, etc. These modules have a very clear structure and a predefined interface, can be loaded into the detection system framework, and can be combined to support penetration testing tasks such as information collection, penetration attacks, and post-penetration attack expansion.

1) Auxiliary module

It provides a large number of auxiliary module support in the penetration information collection process, including scanning and enumeration of various network services, building fake services to collect login passwords, password guessing and other modules. In addition, the auxiliary module also includes some penetration attacks that do not require loading of attack loads and are often not intended to obtain remote control of the target system. The entire information collection is mainly divided into the following three steps:

(1) Verify whether the system is running: Determine whether the target system has been turned on and whether it can communicate with our computer. communicate or interact with each other. Log all active computers that responded.

(2) Scan system ports: Used to identify which ports are opened and which services are running on a specific host. When scanning a single port of the system, keep records and save the output results of all tools.

(3) Scan the system for vulnerabilities: Vulnerability scanning is a process of identifying known vulnerabilities in services and software running on the target computer.

Commonly used tools and methods are as follows:

Ping: Ping is a specific-type of network packet, called an ICMP packet. In addition to telling us that a certain host is active and receiving traffic, the ping packet also provides other valuable information, including the round-trip time of the packet. .

Port scanning: The purpose of port scanning is to identify which ports are open on our target system and determine which services are started.

ACK scanning: The scanning host sends ACK packets to the target host. Obtain the port information based on the returned RST packet. If the TTL value of the returned RST packet is less than or equal to 64, the port is open, otherwise the port is closed.

FIN scan: In FIN scan, after a data packet with the FIN bit set is sent, if the target host responds with an RST packet, it means the port is closed, and if there is no response, it means it is open.

Connect() scan: This scan attempts to perform "three-way handshake" communication with each TCP port. If it can be successfully established

If connected, it proves that the port is open, otherwise it is closed.

SYN scanning: The scanner sends a SYN packet requesting a connection to a port of the target host. After receiving the SYN/ACK, the scanner does not send an ACK response but sends an RST packet requesting a disconnection. In this way, the three-way handshake is not completed and a normal TCP connection cannot be established. SYN only needs to send the initial SYN packet to the target host. If the port is open, it will respond with a SYN-ACK packet; if it is closed, it will respond with an RST packet;

NULL scan: The principle is to send a data packet without any flag bit set to the TCP port. In normal communication, at least one flag bit must be set. According to the requirements of FRC793, when the port is closed, if a packet is received without any flag bit set, flag bit in the data field, then the host should discard this segment and send a RST packet, otherwise it will not respond to the client computer that initiated the scan. That is to say, if the TCP port is closed, it will respond with an RST packet, if it is open, there will be no response.

Dump Scan: Also known as Idle Scan or Reverse Scan, a third-party zombie computer scan is applied when scanning a host. The zombie host sends a SYN packet to the target host. The target host port responds to SYN|ACK when it is developed, and returns to RST when it is closed. The zombie host responds to RST to SYN|ACK, but does not respond to RST. When scanning from a zombie host, a local Continuous pings from the computer to the zombie host. Check the ID field of the Echo response returned by the zombie host to determine the target Which ports on the host are open or closed.

The data that can be detected includes: IP, network segment, domain name, port, operating system version, application of each port, web application, mail application, version information, service information, domain name registrant information, website poster ID in web application, Administrator name, protection information, etc.

2) Penetration attack module

Code components that use discovered security vulnerabilities or configuration weaknesses to attack remote target systems to implant and run attack payloads to gain access control to the target system. The penetration attack module in the platform framework can be based on the location of the exploited security vulnerability.

Locations are divided into two categories: active penetration attacks and passive penetration attacks.

Active penetration attack: The security vulnerability exploited is located between the network server software and the upper-layer applications carried by the server software.

, because these services usually open some listening ports on the host and wait for client connections, by connecting to the target system network service

Services, inject-some specially constructed network request content containing "evil" attack data, trigger security vulnerabilities, and cause the remote service to execute the attack payload contained in the "evil" data, thereby obtaining the control session of the target system. Active penetration attacks against network servers are traditional penetration attacks.

Passive penetration attack: The exploit vulnerability is located in client software, such as browsers, browsing plug-ins, email clients, office and Adobe and other document and editing software. For this type of security vulnerability that exists in client software, we cannot actively input data into the client software remotely, so we can only use passive penetration attacks. That is, constructing "evil" web pages, emails or document files, and setting up servers containing such malicious content, sending email attachments, combining social engineering attacks to distribute and trick target users into opening them, and combining network deception and hijacking techniques. Waiting for users on the target system to access these contents, thereby triggering security vulnerabilities in the client software and giving a shell session that controls the target system. Passive penetration attacks on client software can bypass network boundary protection measures such as firewalls. The two most common types of passive penetration attacks are browser software vulnerability attacks and file format vulnerability attacks.

hole attack.

3) Post-penetration attack module

The post-penetration attack module mainly supports after the penetration attack obtains remote control of the target system, with the help of the powerful control function of the payload platform, various post-penetration attack actions can be carried out in the controlled system, such as obtaining sensitive information and further developing-the system. , implement springboard attacks, clean up traces and other activities.

4) Attack payload module

The attack payload is a piece of implanted code that prompts the target system to run after a successful penetration attack. It is usually used to open a control session connection on the target system for the penetration attacker. In traditional penetration code development, the attack payload is just a ShellCode code with a simple function, compiled in assembly language and converted into machine code supported by the CPU architecture of the target system. After the penetration attack triggers the vulnerability, the program execution process is hijacked and jumped. Enter this machine code and execute it to complete the single function implemented in ShellCode.

5) Empty command module

No-op instructions (NOP) are some no-operation or irrelevant operation instructions that do not have any substantial impact on the running status of the program. The most typical are

A type of empty instruction is a no-op, and the opcode on the X86CPU architecture platform is ox90. When a penetration attack constructs an "evil" data buffer, it is often necessary to add an empty command area before the Shellcode that is actually to be executed. This way, when the penetration attack is triggered and the ShellCode is executed, there is a larger safe landing zone, thereby avoiding ShellCode execution failure caused by memory address randomization, return address calculation deviation, etc. improves the reliability of penetration attacks.

6) Encoder module

After the attack payload and the empty command module assemble a command sequence, before this command is added to the "evil" data buffer by the penetration attack module and handed over to the target system for running, the platform framework still needs to complete a very important process - encoding. . The first mission of the encoding module is to ensure that the attack payload does not contain "bad characters" that should be avoided during the penetration attack. The second mission of the encoder is to "avoid killing" the attack load, that is, to avoid detection and blocking by anti-virus software, IDS intrusion detection system and IPS intrusion prevention system.

> Interface

The interface part provides a variety of user interfaces, such as Web interface, API interface, command line interface, and import interface.

Web interface: Provides an application interface for Web-related automated penetration, which can quickly call web-based vulnerabilities, XSS, SQL injection and other tools and application technologies;

API interface: API interface that provides system-related data permissions to facilitate customized development and special scenario applications according to user needs;

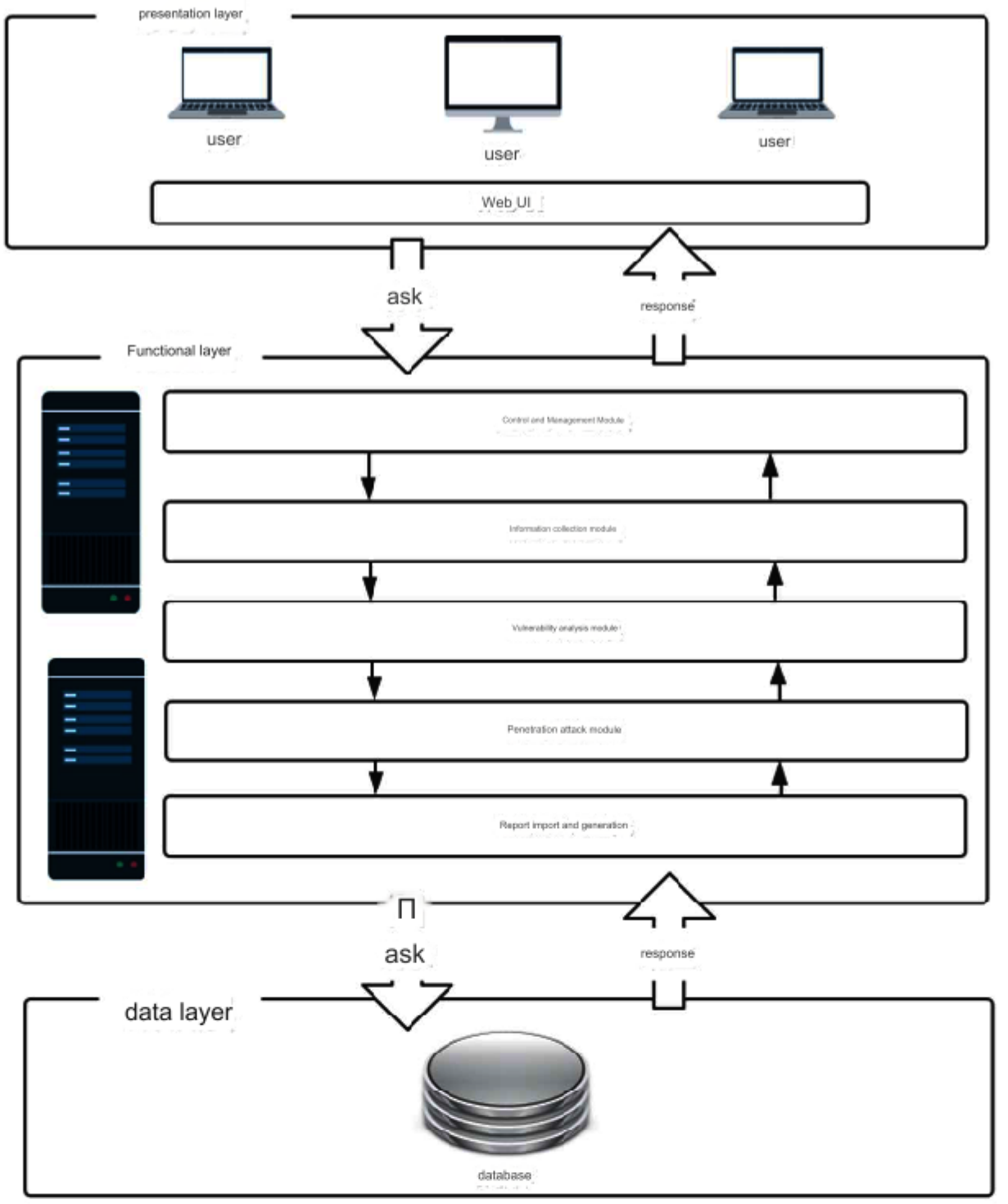
Command line interface: Provides a command line interface, which can facilitate penetration personnel with strong professional and technical skills and solid technical foundation to directly call platform-related functions and perform related tasks through the command line interface;

Import interface: supports the import of relevant tools and materials such as scripts, tools and data to further expand and improve the functions of the platform.

> Other parts

The use of third-party security tools such as Nmap expands the basic capabilities of the framework, and can quickly develop and integrate additional functions, such as Nessus, OpenVAS vulnerability scanners, etc., further improving the platform's automated penetration capabilities and penetration success rate.

3.3 Network architecture



(Network architecture diagram)

In order to meet the needs of users for remote use, the "automated penetration testing platform" adopts the currently popular three-layer B/S mode architecture.

The presentation layer runs on the client and consists of dynamic Web pages and Web browsers, which is the interface of the system. The human-machine interface part handles the interaction with the user, including user login, setting policies, and executing penetration. Operations such as testing and querying reports. In order to improve the security of the system, the HTTPS protocol is used to communicate with the server.

The functional layer runs on the server. It encapsulates the business logic module of the network security assessment system, including the control and management module, information collection module, vulnerability analysis module, penetration attack module, and report generation module. It is the main body of the assessment system and is responsible for responding. Web client requests.

The data layer is located at the bottom of the system framework, including database platform, database software and system data. It is responsible for storing and managing data, processing and realizing data requests from the functional layer. The three-tier system structure of B/S can easily manage and maintain data, and separate data and applications, which not only achieves system stability, but also improves system scalability, thereby improving system integrity.

able.

4 product features

Build an "automated penetration testing platform" based on professional penetration processes to implement active attacks on networks or devices, provide basic functions such as detecting security vulnerabilities in the system, and test the impact of new attack technologies, fully satisfying users' needs for security detection and evaluation work. need.

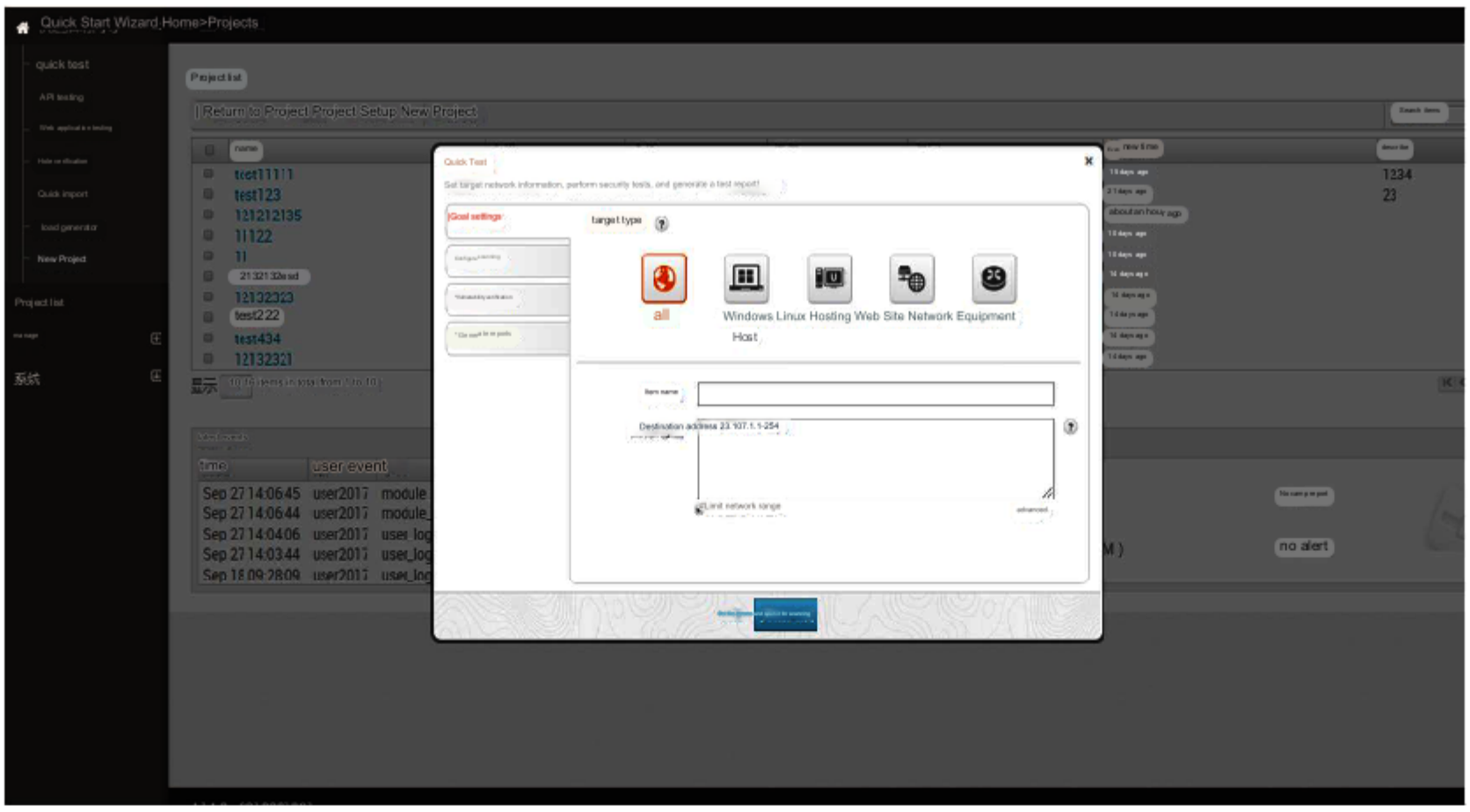
4.1 Automated penetration testing

The construction of the automated penetration function mainly involves discovering the target's open ports and services through a series of processes such as vulnerability scanning, vulnerability exploitation, and permission acquisition. Based on the detected information, the system exploits vulnerabilities to further obtain target permissions. The specific content is as follows:

> Vulnerability Scan

The vulnerability scanning module includes two different modes: quick scanning of vulnerabilities and detailed scanning of vulnerabilities. Quick scanning of vulnerabilities mainly targets various targets such as Windows hosts, Linux hosts, Web sites, network devices, etc., to conduct quick scan tests to determine the host online status and port openings. , operating system version and other information, and generate a report based on the results.

Detailed vulnerability scanning is based on tens of thousands of built-in detection templates and vulnerabilities, and uses functions such as Web vulnerability scanning, operating system vulnerability scanning, weak password detection, etc. to proactively analyze all weaknesses, technical flaws or vulnerabilities of the system under test, and generate a report on the results. Including: host information, vulnerability assessment, vulnerability details, vulnerability exploitation, service list, port information, database information, file directory information, scanning history, etc. As shown below:



(Vulnerability scanning interface)

> Exploit

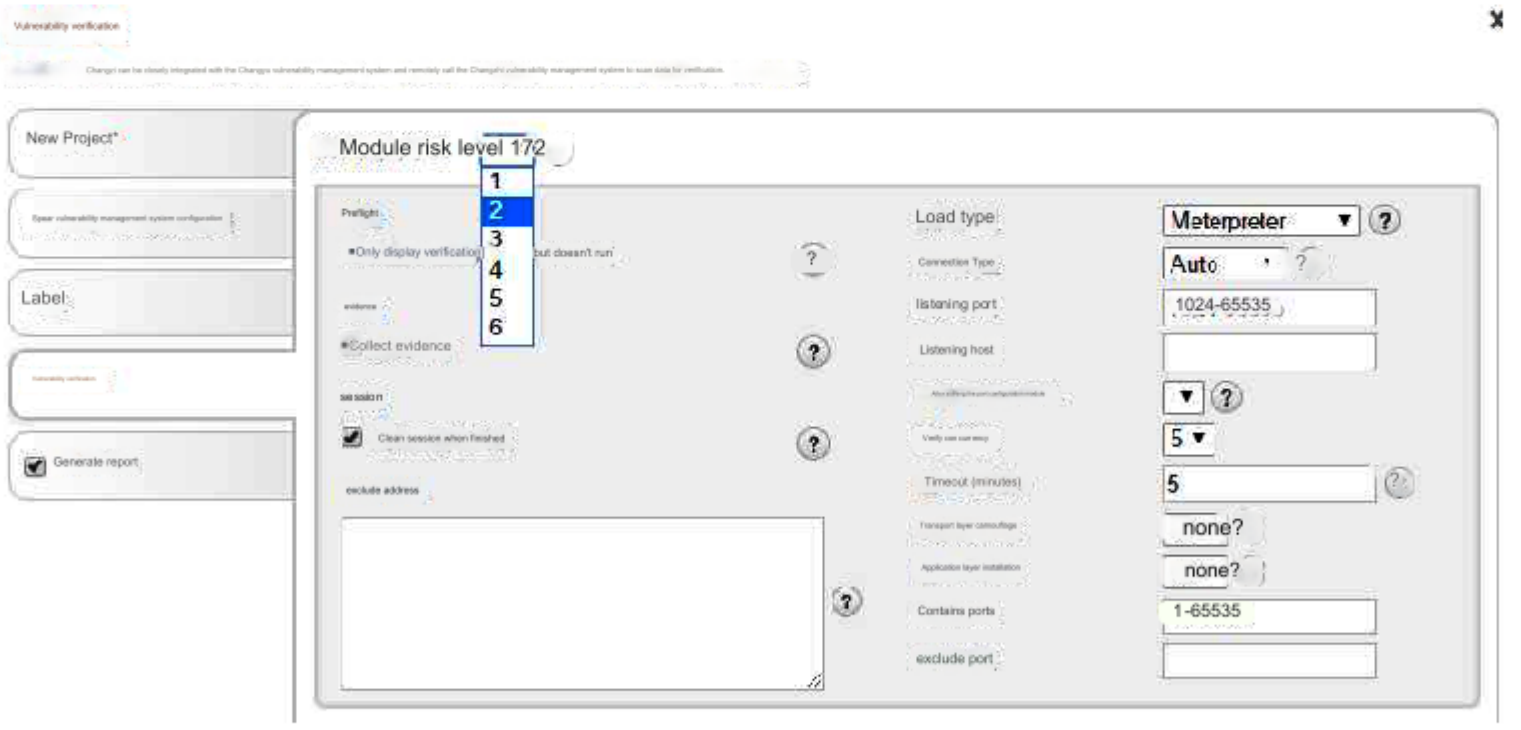
Vulnerability exploitation is based on the vulnerability scanning results, custom-selecting vulnerability exploitation modules with different risks, and executing penetration of the target vulnerability.

attack. At the same time, the platform supports the import of scanning results and vulnerability verification from a variety of third-party security scanning tools, automatically identifying and importing reports.

In the system, choose to conduct penetration verification on the imported host and corresponding vulnerabilities. After confirming that the vulnerabilities are real, you can attack. Support includes: Green Alliance Extreme

Light, Venus Sky Mirror, AppScan, NeXpose, Acunetix, Core Impact, Nessus, NetSparker,

Nmap et al. As shown below:



(Exploit interface)

> Permission acquisition

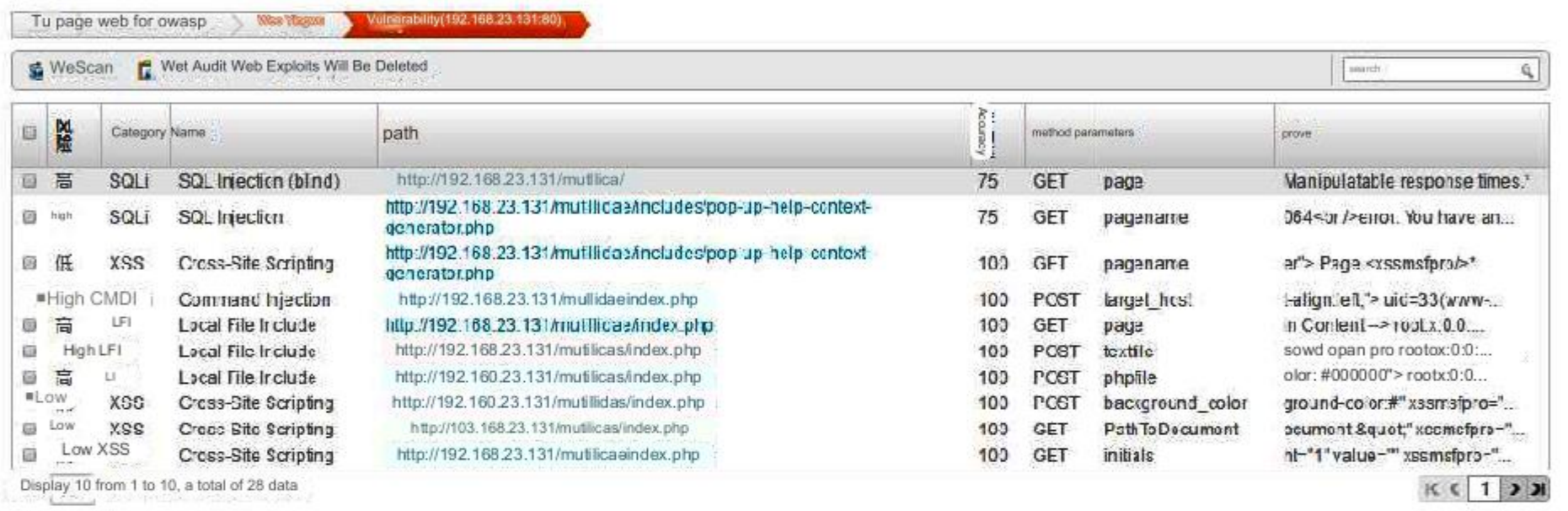
After the vulnerability is successfully exploited, the system supports selecting a series of execution codes and execution codes written according to the vulnerability exploitation method based on the penetration results.

Script program to achieve the acquisition of target permissions.

4.2 WEB application testing

Integrated web scanning, testing, and auditing functions can easily scan and audit web applications, and support the detection and verification of vulnerabilities such as SQL injection, XSS, upload vulnerabilities, and command execution.

The platform supports crawling the specified range of web pages for the input URL, and using the Web testing module to test the pages, including: automatic testing of the latest top ten Web security vulnerabilities listed by OWASP, misconfiguration of the Web server, and cross-site scripting attack vulnerabilities. , local file inclusion and remote file inclusion, SQL injection vulnerability, file upload vulnerability, remote code execution vulnerability or remote command execution and other vulnerabilities.



(Web application testing)

4.3 Intelligent vulnerability verification

The "automated penetration testing platform" has powerful vulnerability verification and matching functions, is fully compatible with third-party security scanning tools, and And relevant tools can be directly called through the platform for vulnerability scanning and verification, and the system can convert the results of vulnerability scanning and verification Import to provide more vulnerability exploitation data for the platform and more vulnerability combinations for related penetration work to achieve Rapid penetration of targets.

The "automated penetration testing platform" supports the import of scanning results and vulnerability verification from a variety of third-party security scanning tools. Such as Green Alliance Aurora, Venus Sky Mirror, Acunetix, Amap, AppScan, Burp, Core Impact, Foundstone, Microsft MBSA, Nexpose, Nessus, NetSparker, Nmap, etc.

4.4 Mobile terminal penetration

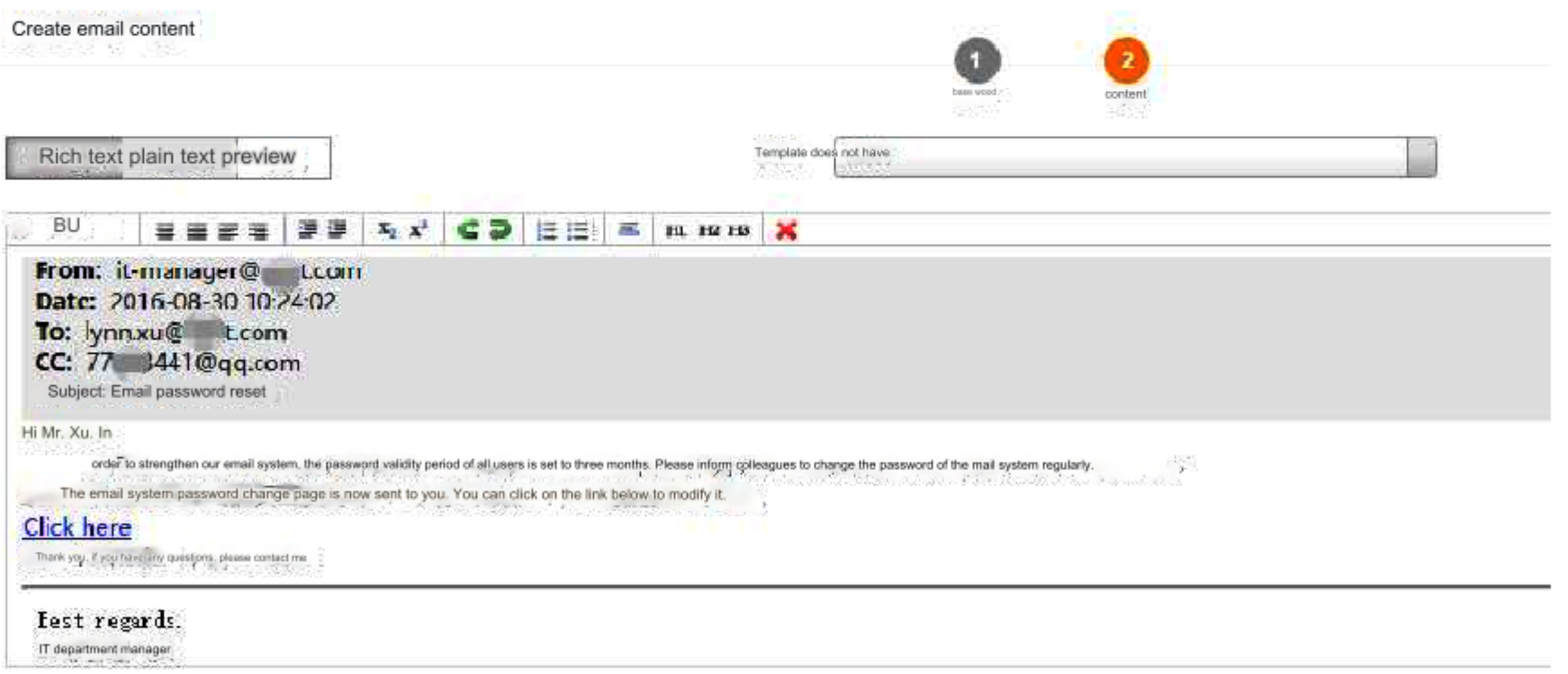
Currently, mobile terminals are becoming more and more popular. In order to meet more user penetration scenarios and penetration needs, the system has collected and organized vulnerability exploitation modules for Android and iOS systems. Users can integrate Android and iOS through the "automated penetration testing platform" The system's vulnerability exploitation module can carry out penetration work on mobile terminals in real time, and the platform supports online generation of remote control programs for Android systems.

4.5 Social engineering attacks

The "automated penetration testing platform" integrates a social engineering module to conduct security awareness tests on corporate employees. For example, various combination tests of simulated phishing, browser vulnerabilities, Office vulnerabilities, etc.

The social engineering module is mainly used to assist users in quickly establishing social engineering projects. By inducing the target to share sensitive information or execute certain dangerous codes, it ultimately achieves the purpose of invading the target system and obtaining target information. Penetration personnel perform social engineering tests to assess whether members of an organization adhere to safe operating practices. Social engineering attack projects can enable the target to check emails, open links and other operations, analyze the progress of the attack, and collect statistical attack data.

Social engineering capabilities assist in completing operations in social engineering attacks. The system divides social engineering functions into three components: email, web pages, and portable files. The combination of the three components assists in completing the following types of attacks:

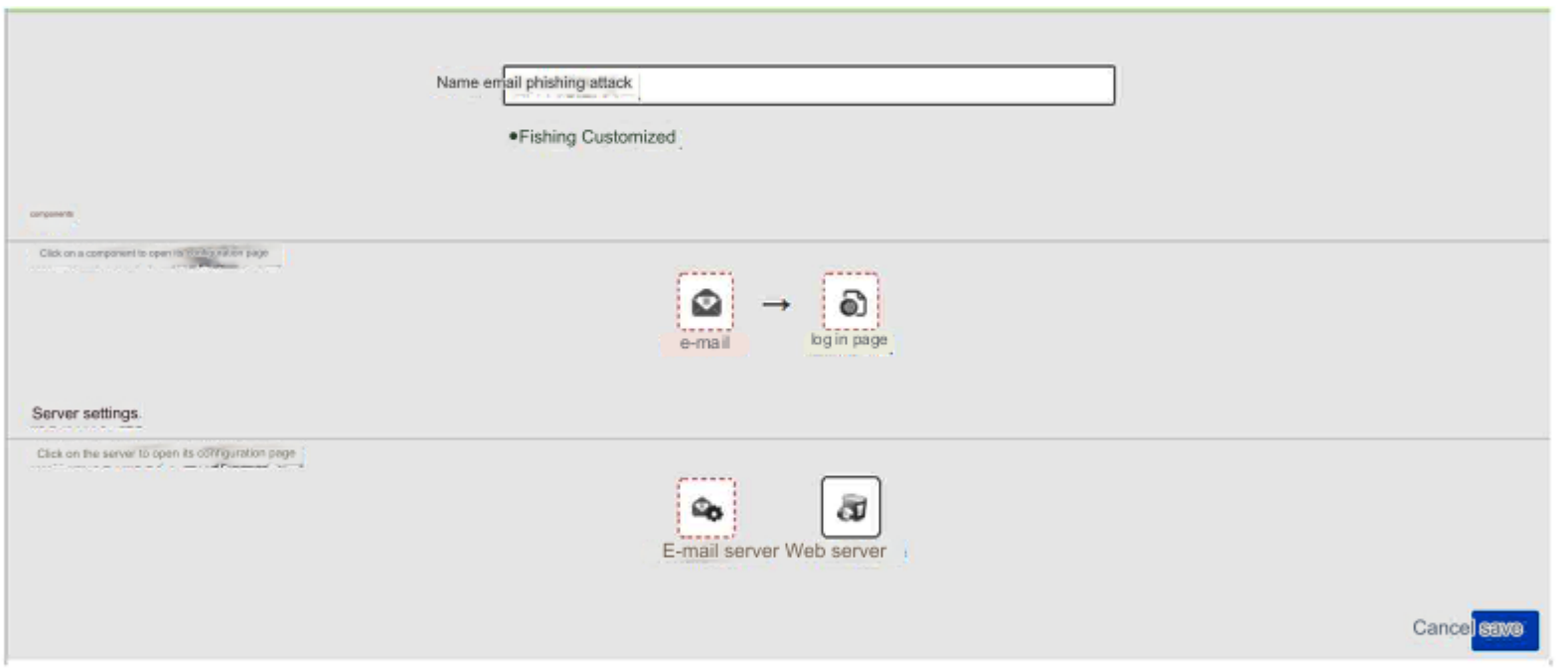


(phishing email)

(fishing successful)

➢ email phishing

The platform supports specifying email sending servers, using Web page components to clone and forge Web sites, establishing email content templates for the forged sites, inducing targets to submit sensitive information on the forged Web sites, and ultimately achieving the purpose of collecting target sensitive information for further attacks. .



(Phishing email configuration interface)

> Browser/file vulnerability attacks

The platform supports the establishment of a site that automatically detects browsers and exploits vulnerabilities through Web page components. The target is induced to browse

Browse the specified site, and after the browser vulnerability is successfully exploited, a connection session is automatically established.

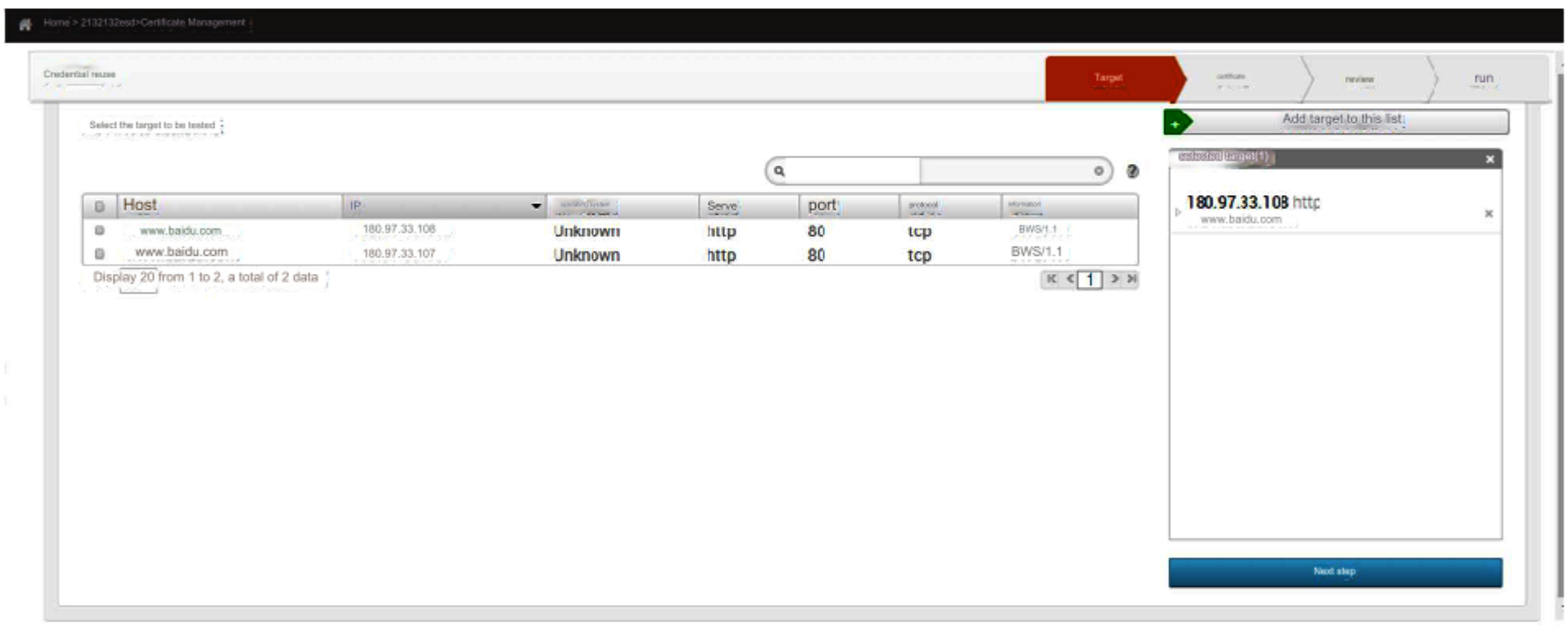
The platform supports file vulnerabilities such as Office, PDF, pictures, etc., and generates files with attack payloads. Trick the target into opening or browsing the text

The software automatically establishes a connection session after the vulnerability is successfully exploited.

(Browser/file attack configuration interface)

4.6 Credential verification

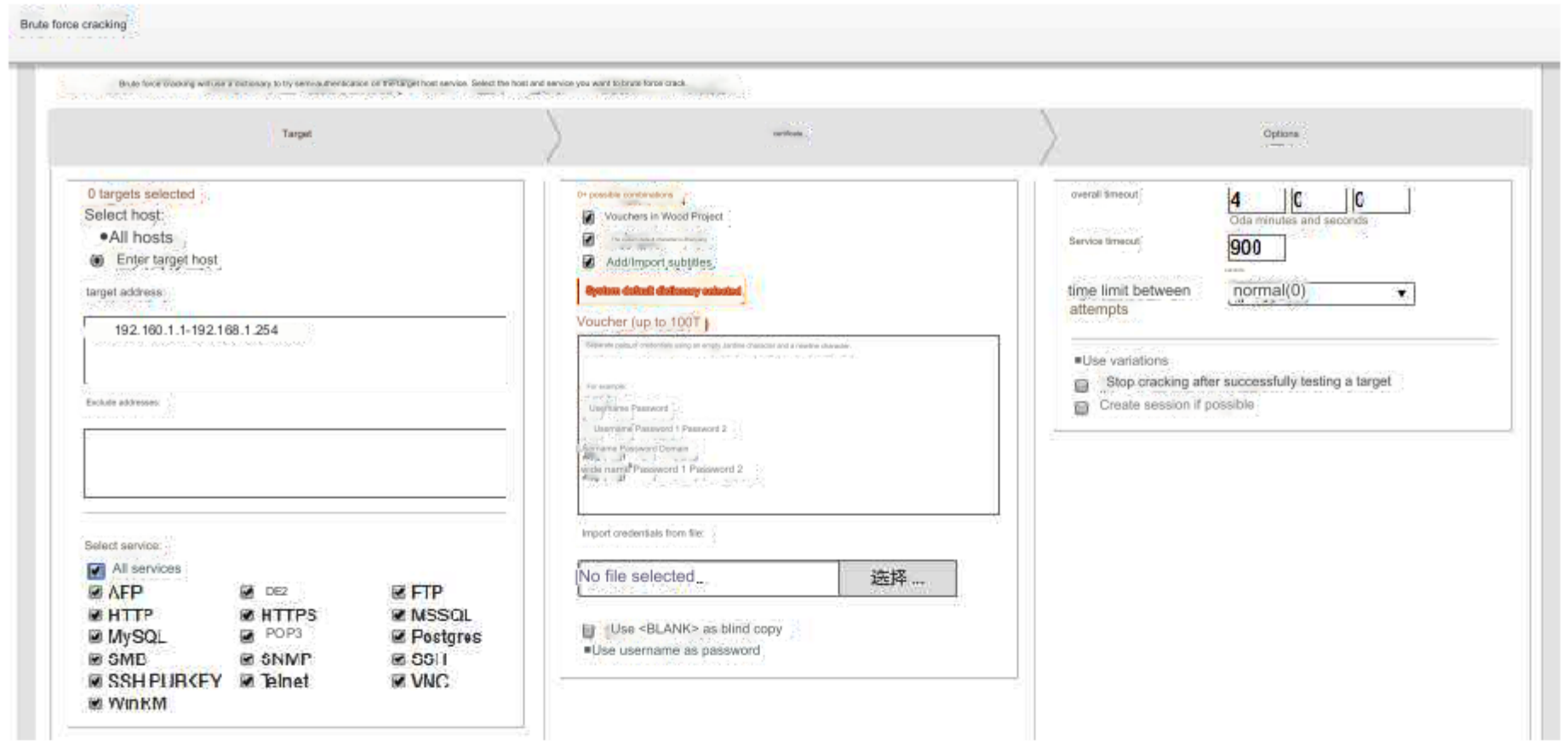
"Automated penetration testing platform" supports credential verification function. Users can use the account password, Key, Hash, etc. that have been collected from evidence to verify other hosts through the platform, which can assess the impact of leaked security information.



(Credential verification)

4.7 Weak password scanning

The "automated penetration testing platform" integrates the violent PJ module and supports AFP, DB2, FTP, HTTP, HTTPS, MSSQL, MySQL, POP3, PostgreSQL, SMB, SNMP, SSH, SSH PUBKEY, Telnet, VNC, WinRM and other protocols; it can be based on The scan results of the host automatically select the protocol and support user-defined dictionaries.

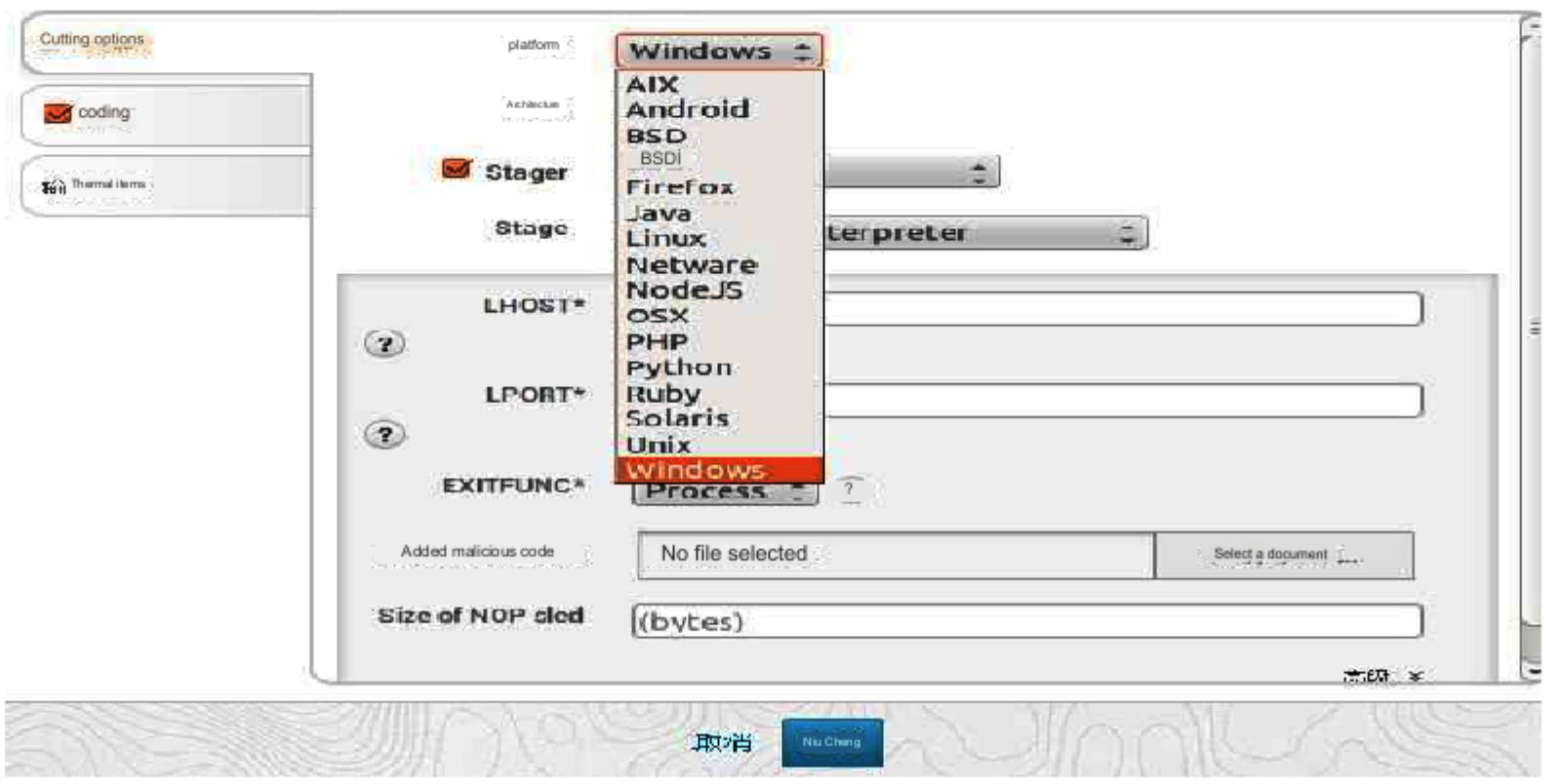


(violent PJ)

4.8 Load Generator

Classic payload: The platform supports generating a variety of attack payloads for penetration testing. The generated payload supports various operating systems and commonly used web server-side languages, including: Linux, Unix, AIX, BSD, R, Windows, OSX, Netware, iOS, Android, Firefox, Java, Python, Ruby, NodeJS, etc.

Dynamic payload: The system supports the generation of a variety of dynamically encoded attack payloads targeting the Windows platform to evade detection by anti-virus software.



(Load generation)

4.9 Replay attack

For successful penetration attacks, there is no need to re-carry out complex attack operations after the session established with the target is terminated or disconnected.

You can choose to replay the attack directly, and reinfiltrate and establish a session based on the previous attack parameters.

4.10 Springboard attack

Springboard attacks are mainly for advanced usage scenarios. After successfully penetrating a host, the penetrated host can be used as a springboard to further attack other networks connected to the host. For example, infiltrate a host through the Internet, and then scan and attack the intranet through the host, such as sniffing on the intranet.

4.11 Investigation and evidence collection

After the "automated penetration testing platform" successfully penetrates the target host, it can realize the evidence collection function of the controlled host, such as screenshots of the vulnerable host, configuration files, keylogging, file operations and other comprehensive functions.

Screenshot: intercept the target host system interface and obtain target host desktop information and other data information;

Configuration file: Obtain the target host configuration file and master the target host system and application-related configuration data information, which is beneficial to

Take full control of the target host;

Keyboard logging: It can record the keylogging data performed by the target host operator in real time, and covertly obtain the relevant data information of the target host, such as account password and other data;

File operations: Comprehensive management operations can be performed on the files of the target host through the "automated penetration testing platform", such as deleting files, uploading files, downloading files, and viewing files.

4.12 Advanced scheduled tasks

The "automated penetration testing platform" provides periodic task functions to satisfy users' penetration assessment and detection of their own platforms. Users can develop task plans according to their needs and achieve regular automated penetration and inspection of the target system; and the system supports task chains. A combination of different tasks can be executed in a customized configuration sequence to conduct comprehensive penetration detection and analysis of the target system.

4.13 Teamwork

The "automated penetration testing platform" provides multi-user roles, divided into administrators, auditors, and ordinary users; permissions can be assigned by project (projects can limit network scope, etc.). Through multi-user and multi-role system management, it is ensured that the platform can operate scientifically, stably and effectively.

4.14 Log audit

The "automated penetration testing platform" facilitates users to manage the system in real time and master the system usage, provides operation audits, event audits, user behavior audits, and supports system status JK.

4.15 Report generation

The "automated penetration testing platform" supports the generation of corresponding penetration reports for each penetration work. Report generation supports HTML/PDF/Word formats and supports customized LOGOs, etc.; report generation supports a variety of templates (audit reports, information collection reports, Web applications Test reports, social engineering reports), and support automatic sending to designated mailboxes.

5 product parameters

project	parameter	Standard Edition	Professional version
Quick scan takes time	Average time spent on 1-5 hosts	30 minutes	30 minutes
Default concurrent scan	Default number of hosts scanned simultaneously	5	5
Number of vulnerability libraries	100,000+	support	support
Number of vulnerability check items	300,000+	support	support
Maximum concurrent scans	Maximum number of hosts scanned simultaneously	10	10
Total number of modules	Including utilization, assistance, post-infiltration and other modules	4000+	4000+
Number of modules utilized	Only use the number of modules	1700+	1700+
IP number authorization	Whether to limit the total number of target IPs	unlimited	unlimited
Web interface	Operate via browser interface	support	support
Command line operation	Operation via terminal command line	support	support
Support IPv6	Support IPv6 network scanning	support	support
independent property rights	Code is completely autonomous	support	support
Exploit coverage	Including operating systems, network equipment, databases, middleware, and systems Software, etc.	support	support
Password Brushing Support Protocol	Protocol: AFP, DB2, FTP, HTTP, HTTPS, MSSQL, MySQL, POP3, Po penetration greSQL, SMB、SNMP、SSH、SSH PUBKEY、Telnet、 VNC、WinRM	support	support
Sub-project management	Support project management of penetration testing targets	support	support
quick guide	Quick guide to common penetration testing operations	support	support

Web audit	Scan and audit web applications	support	support
External report import	Import report results scanned by third-party applications	support	support
Vulnerability verification	Conduct penetration testing and verification of scanned vulnerabilities (reports of mainstream missed scans) (such as Green Alliance, Qiming)	support	support
Credential reuse	Test other hosts with the found credentials	support	support
evidence collection	Collect evidence of successfully exploited target vulnerabilities	support	support
Post penetration module	Modules available for post-penetration operations	support	support
Automatic post penetration	After successful exploitation, the customized post-penetration module can be automatically executed.	support	support
Session persistence	The session after successful utilization can be persisted	support	support
social engineering attack	Assist social engineering testing to test personnel's security awareness	support	support
IDS/IPS bypass	Support configuration parameters to attempt to bypass IDS/IPS	support	support
Avoid anti-virus software	Supports a certain degree of anti-kill function when infiltrating	support	support
load generation	Supports generating specifically configured attack payloads	support	support
Agency Springboard	Supports the use of proxy springboards for intranet penetration	support	support
VPN Springboard	Supports the use of VPN springboard for intranet penetration	support	support
replay attack	Supports replay of previously successful attacks	support	support
Generate report	Supports report generation for security testing assessments	support	support
report format	HTML\PDF\WORD	support	support
Number of report templates	Number of different report templates	support	support
Custom reports	Supports customizing report content	support	support
Maximum number of supported users	Number of users supported by the web interface	1	3
Scheduled Tasks	Support advanced automated scheduled tasks	support	support
Vulnerability assessment support scope	Operating system (Windows, Linux, UNIX, OS, etc.), data	support	support

	Database (SQL Server, DB2, Oracle, MySQL, etc.), Web applications, middleware, network equipment (routing, switching, firewall, etc.)		
Black box vulnerability assessment	Assess vulnerabilities through network remote fingerprinting	support	support
White box vulnerability assessment	Login scan using login credentials	support	support
Scan policy template	Built-in more than 8 scanning policy templates for different vulnerability assessment requirements	support	support
Custom scan strategy	Scan policy templates can be customized and configured	support	support
Exploitable vulnerability information	Prompts vulnerabilities that have publicly exploited methods and provides relevant vulnerability exploits source information, etc.	support	support
Vulnerability judgment basis	Scanned vulnerabilities can be viewed and judged based on	support	support
Accurate risk scoring	In addition to the CVSS standard vulnerability score, based on asset importance, vulnerability Exposure and threat levels provide a more accurate risk score	support	support
Virtualization platform scan	Supports scanning of mainstream virtualization platforms such as VMware/KVM, etc.	support	support
Weak password scanning	Supports weak password scanning for common protocols	support	support
baseline scan	CIS, customized baseline scan strategy	support	support
Enhanced web scanning capabilities	Able to detect Web applications and Web Services applications based on Javascript, Ajax and Flash (including SOAP 1.2, Json, WSDL, XML), and detection use cases can cover all OWASP Top 10 threats	not support	support
API interface	Provide API interface for external applications to call	not support	support

6 Product Deployment

6.1 Applicable environment

"Automated Penetration Testing Platform" is a platform that integrates hundreds of vulnerability templates and penetration testing methods to support automated penetration testing of various network devices and hosts. The platform adopts a variety of deployment methods and can be adapted to users' special tasks of conducting penetration testing against specific network targets. The system integrates a variety of vulnerability templates and testing methods to fully meet the user's needs for penetration testing, WEB application testing, vulnerability verification, weak password scanning, mobile terminal penetration, credential verification and other penetration testing attacks on the target network.

6.2 Deployment method

The platform supports multiple ways of deploying applications. Supports installation on portable hardware such as laptops, and also supports deployment to virtualization platforms. Only basic network connectivity is required for security detection and assessment. The system is generally used as an active test, but also provides a passive test deployment method for special scenarios. Specific deployment requirements are as follows:

Configuration Environment	Environmental parameters
Deployment method	Active test deployment: The system is able to connect to the target network, either through a proxy or VPN.
	Passive test deployment: Apply a dedicated passive test module in the system to connect the system to a Network port for traffic mirroring, analyze and test the mirrored network traffic.
Hardware environment	Recommended dual-core CPU, 4GB running memory, 120G storage or above configuration
	Operating system type: Ubuntu 16.04 LTS 64-bit
virtualized environment	Recommended VMWare ESXi6.5
	Recommended VMWare Workstation 11
	VMWare Player 11 or above is recommended
	VMWare Fusion (for Mac)
Web environment	Internet access

7 product advantages

> Automation

The entire penetration platform consists of six parts: QB collection, threat modeling, vulnerability analysis, penetration attack utilization, post-penetration testing, and reporting. It provides automated support for the entire penetration testing process according to different penetration environments.

>Professional vulnerability library

The system has built-in Metasploit commercial-grade professional version vulnerability exploitation platform, which integrates thousands of operating system and application software vulnerabilities, as well as hundreds of ShellCode, and is constantly updated to fully meet the needs of in-depth vulnerability scanning.

> Flexible custom scanning

It supports customizing the start time of website scanning to avoid website business peaks, or setting periodic scanning tasks according to the needs of the business online process.

> Rich application scenarios

The platform includes automated penetration testing, web application testing, mobile terminal penetration, social engineering attacks, credential verification, weak password scanning, payload generation, replay attacks, springboard attacks and other types of attack methods and templates, which can effectively expand user application scenarios.

> Strong professionalism

The platform supports the generation of professional penetration testing reports. Users can select the best penetration attack methods based on the test reports to implement professional penetration testing attacks.