
Text-based Summary of Penetration Testing

1. Preliminary Understanding of Penetration Testing

Penetration testing is a mechanism provided to prove that network defense is working as planned. Actually, penetration testing does not have a standard definition. The common perspective reached by some international security organizations is that penetration testing is an evaluation method to assess the security of computer network systems by simulating the attack methods of malicious hackers. This process includes a proactive analysis of any weaknesses, technical defects, or vulnerabilities in the system, which is carried out from a place where an attacker may exist, and this location has the conditions to actively exploit security vulnerabilities.

1.1 The origin of penetration testing

As early as 1965, computer security experts reminded governments and enterprises that the more powerful interaction ability of computers, the more data would be stolen. At the Joint Computer Conference in 1967, more than 15000 computer security experts, government and corporate analysts discussed the issues about possible eavesdropping of computer communications and propose the term of "penetration testing". And they even identify the main challenges that computer communications currently face. RAND Company initially proposed the assumption of ensuring network security through system testing. RAND in cooperation with the Advanced Research Projects Agency (ARPA) of the United States to present a groundbreaking report called The Willis Report. The report discusses network security issues and puts forward corresponding strategic and technical countermeasures. Even now, this report is the basis of network security solutions. Since the report, some governments and enterprises have built specialized teams to unearth vulnerabilities in computer systems and networks to protect computer and communication systems from malicious penetrations and attacks. In the late 1960s, the well-known Tiger Team was established to evaluate the ability of computer networks to resist attacks. Penetration tests conducted by RAND and the government reveal two issues: first, computer systems can be penetrated. Second, it is a meaningful practice to exploit penetration testing techniques to uncover vulnerabilities in systems, networks, hardware, and software, which need further research and development.

James P. Anderson was one of the early pioneers in the development of penetration testing. In 1972, he proposed a series of concrete steps that possibly penetrate and attack the system tested by the Tiger Team. The methods of Anderson can be summarized as follows: first finding vulnerabilities and designing attack strategy, then finding the weaknesses and dealing with threats in the attack process. This basic method is still in use up to now. In the 1970s and 1980s, it was innovative to research how to build a secure-safe system. In an article published in 1980, Anderson showed how to design a program that can monitor the running circumstance of computer systems, which detects hacker activities by identifying the anomalistic circumstance of the system. Because this principle is uncomplicated and easy to understand, current computer users can easily understand how it works. Many concrete methods can be implemented around this the monitoring mode proposed by Anderson. Nevertheless, the work was groundbreaking at

the time and many methods in this work formed part of the current system defense standards.

1.2 Interpretation of penetration testing

The effective way to reduce the attack by hackers is to conduct a security assessment of web sites and systems in advance and comprehensively prepare for the potential network penetration attacks. Finding the biggest culprits of cyber threats through security assessment is of great significance to network security. Penetration testing is a subbranch of security assessment, which originated from the military network attack and defense technology.

Penetration testing is a kind of beneficial supplement to the network security evaluation, it acts as a simulated attacker to inspect and ensure the computer network system. Specifically, penetration testing is to require test personnel to conduct controllable hacking methods within the allowed range, to simulate as much as possible the attacker using various methods and technologies, so as to verify the security of the system in the real application environment. In other words, penetration testing means that security personnel in different locations (such as Local Area Network, Internet, etc.) utilize various means to test a specific network and disclose vulnerabilities in the system, finally output the penetration testing report and submit it to the network owner. According to the penetration testing report, the network administrator can be clearly aware of the security risks and vulnerabilities in the computer system.

Penetration testing has two prominent characteristics:

- Penetration testing is a gradually deepen process;
- Penetration testing is a security assessment using attack methods that do not affect the normal operation of computer systems.

1.3 The significance of penetration testing

Use an analogy to explain the necessity of penetration testing. Suppose we want to build a vault, and we have built it according to the construction specifications. Can the vault be put into use immediately? Certainly not! Because it is unclear how safe the entire vault system is and whether it can ensure that the valuables stored in the vault are foolproof. So, what should be done at this time? We can ask some security experts in the industry to conduct a comprehensive inspection and evaluation of this vault, such as checking whether the vault's door is easily damaged; checking whether the vault's alarm system warns in time when an abnormality occurs; checking whether all doors, windows, passageways and other key and easy-to-break parts are unbreakable; checking the vault management security system, video security monitoring system, etc. It will even ask special personnel to simulate the invasion of the vault to verify the actual security of the vault, and expects thus can find and reveal existing problems. The process is like a penetration testing of a vault. The vault is like our information system, and various tests, inspections, and simulated intrusions are equivalent to penetration testing.

Perhaps we still have such questions: If we update my security policies and procedures regularly, upgrade the system in time, and use security software to ensure all the system patches have been applied. Do I still need penetration testing? Need! These measures are equivalent to the specifications for the construction of the vault, it does not mean that we can rest easy when we have constructed the vault according to the specifications. Penetration testing can aid us to understand the current network situation by identifying security issues. Penetration testing can prove the effectiveness of the defense measures, or detect problems and help resolve potential

risks. Discovering vulnerabilities in the network in advance and making necessary enhancement is like trying to look ahead at what might happen; while being discovered by others and using the vulnerabilities to attack the system, the remedy after a security incident is like restoring the valuable things after the damage has been already done. Obviously, planning ahead is better than fixing late.

2. The Conception and Workflow of Penetration Testing

In this section, this article conducts conventional penetration testing on web sites to explain the conception and processes of penetration testing.

2.1 Information collection

Collecting accurate information can greatly improve the effectiveness of penetration testing more. When conducting a penetration test on a target website, we can first sufficiently query the domain name, Whois information, the script type of the website, and determine whether the target website is a whole-site system, the system version of the website server, and service middleware. And a simple test of the target website to determine whether there is a firewall and whether there is a side station.

2.2 Vulnerability detection and utilization

1. Vulnerability of the integrated station system: When we find that the website is an integrated system, we can search the website to discover whether there is a known vulnerability in the system. If there is a vulnerability, we can utilize it to penetration. If no vulnerabilities are found, we can consider the penetrate it from its neighborhood.

2. SQL injection: When the script file of the website is found to be written as PHP, ASP, ASPX, JSP, JSPX, etc., we can consider whether there is a SQL injection vulnerability.

3. XSS attack: Check if there is a message board on the target website or other modules that can input data. If this module exists, consider whether we can carry out XSS attacks and test XSS attacks. However, because XSS attacks are easily discovered by experienced administrators, it is recommended to use XSS attacks when other penetration testing methods cannot be used.

4. File inclusion: If a URL like `/include.php?file=/web/file.php` exists in this website, we can consider and test whether there is a file inclusion vulnerability.

5. Backup files/ Download of source code: Scan the directories of target website through the scanning tool, we may find the backup file or source code of the website. Extract all files and use them to reconstruct the operating environment of the website, and sensitive information such as administrator accounts and passwords might be found.

6. Port utilization: Scan the target website through the port scanning tool, analyze the results, and check whether the website has opened a high-risk port. If we find a high-risk port, we can consider using a tool to attack the port or unauthorized access to the port.

7. Middleware: Collect the middleware service data of the target website and check whether there are known vulnerabilities.

How to get the access and control permission of the target:

1. When we get the permission of server console, look for the available upload point and

upload one-command Trojan.

2. If we cannot upload one-command Trojan directly, consider using the vulnerability analyzed by IIS6, Nginx and other services to upload.

3. Utilize the database backup function to back up files containing one-command Trojan;

4. If it is found that there is an inclusion vulnerability in the early stage, and if we can parse any file according to the script file, we can directly include the web shell that contains a file that saves one-command Trojan;

5. If the SQL statement can be executed, the access and control permission can be accessed by exporting the SQL statement;

6. The permission of an integrated station system can be access by directly searching on the Internet.

2.3 Privilege elevation and intranet penetration

When we get control permission, usually the permissions are relatively low. Thus we need to escalate the current permissions.

1. In the early stage, if we get the system information about version, we can find the corresponding privilege escalation tool for the system. When the corresponding vulnerability of the system is patched, we can consider using some other services, such as MYSQL to perform privilege escalation.

2. When the authority is sufficient, we can use the tool to grab the password of the system administrator, or directly create a user and increase the authority. Finally, we can log into the server remotely.

3. After entering the server, we should first check whether there is monitoring software.

4. Collect various passwords in the system (administrator password, database password, etc.), which may be useful in later penetration testing.

5. Check whether there are available ports and services on this machine because the servers in the intranet are often highly similar. By checking the situation of this machine, we can get a general understanding of the situation of other servers, and then utilize this information for further penetration.

2.4 Cleaning of penetration traces

A successful penetration test should not be discovered and traced by the administrator. After the penetration test, remember to clean up the traces, such as system logs, software usage records, created accounts, and various tools used.

3. The usage and practice of penetration testing tools

3.1 Information Collection

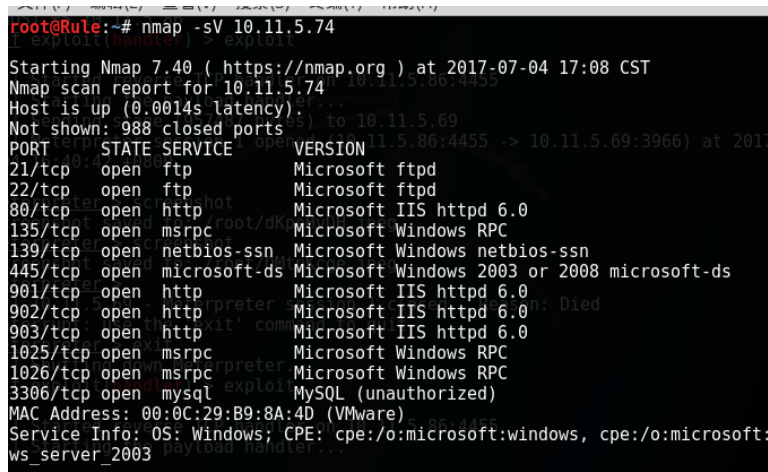
In the web penetration test of general targets, when we get the website IP, we should first check what services are available on the port 80 and 8080 of the website (browser access). If some simple and well-used vulnerabilities are found, the next operating can be conducted. If not, we can try to scan the target IP port to see if there are opening sensitive ports and services, and then take corresponding measures.

- 1) Target IP: 10.11.5.74;
- 2) Direct access to the 80 and 8080 port, as shown in the figure below, the PHPcmsV9 information can be found through the robots.txt file. When it is viewed on the search engine, we find that some vulnerabilities about file reading and scripts that can be utilized, and record it.



The 8080 port of the IP is not open. Generally, the port is open for server middleware or other websites (Using server middleware vulnerabilities is often more efficient than exploiting website vulnerabilities).

- 3) Information detection (port scanning)
- The result is obtained by using Nmap as shown in the figure below. We can find that 21, 80, 3306 and other ports have open services, we can try ftp weak password, 3306 weak passwords, GET SHELL and other operations. At the same time, we can also find 901, 902, 903 and other unspecified ports (man-made settings). The detected service is the same as 80, indicating that it is also related to the website service.



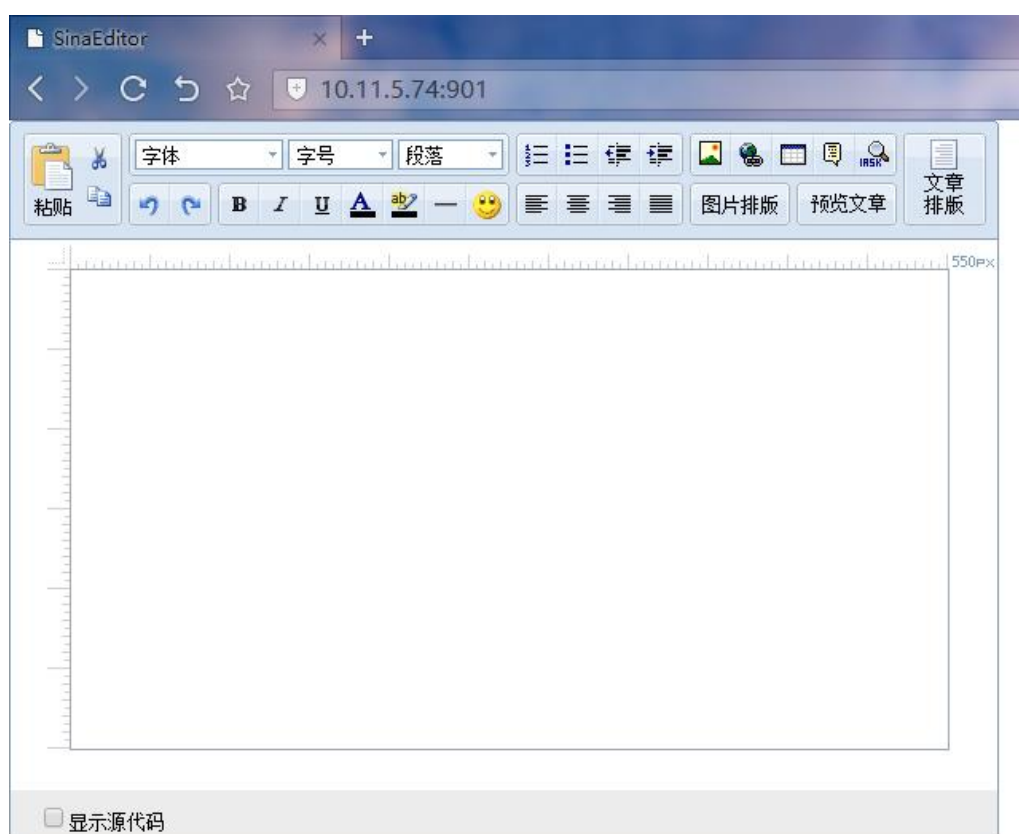
3.2 The detection and utilization of vulnerability

- 1) Known information: port 80, 901, 902, 903 open services; operating system Windows2003; Internet Information Services IIS6.0; database MySQL.
- 2) Searching the vulnerabilities (901,902,903)

As shown in the figure below, an editor is found on port 901. Practically, the editor information often exists in the related files of the website directory. First of all, we should check the version of the editor and use the search engine to obtain the operation method.



```
1 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
2 <html>
3 <head>
4     <meta http-equiv="Content-Type" content="text/html; charset=gb2312">
5     <title>SinaEditor</title>
6     <link rel="StyleSheet" href="editor/base.css">
7     <script type="text/javascript" src="editor/editor.js"></script>
8     <script type="text/javascript">
9     var guid = "132448.743" ;
10    var sState = "iframe";
11    var checkEdit;
12
13    function save_article() {
14        et.save();
```

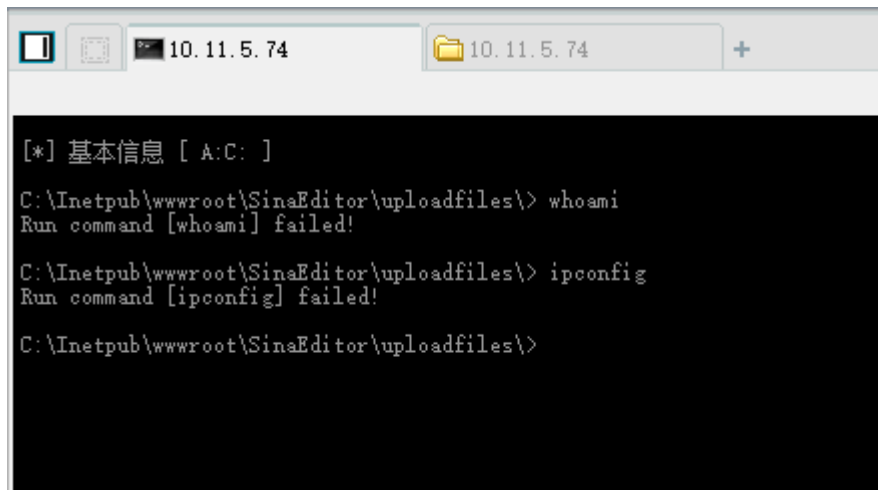


3) The exploitation of vulnerability

There is upload function in the editor, we can upload a picture to verify if the editor is available, and try to upload scripts such as ASP, PHP, etc. directly. Because Internet Information Services is IIS6.0, we can try to utilize the parsing vulnerability such as the interpretation of '1.asp' '1.jpg'. If it is the 'js' verification of front-end, we can try to disable 'js' or upload the files under allowed format, and then use burpsuite to modify it.

3.3 The utilization of web shell

After penetrating the web shell, we should first check our permissions. As shown in the following figure, here we can find that the command execution failed. The reason is that the permissions are low or the administrator has set up defensive measures.

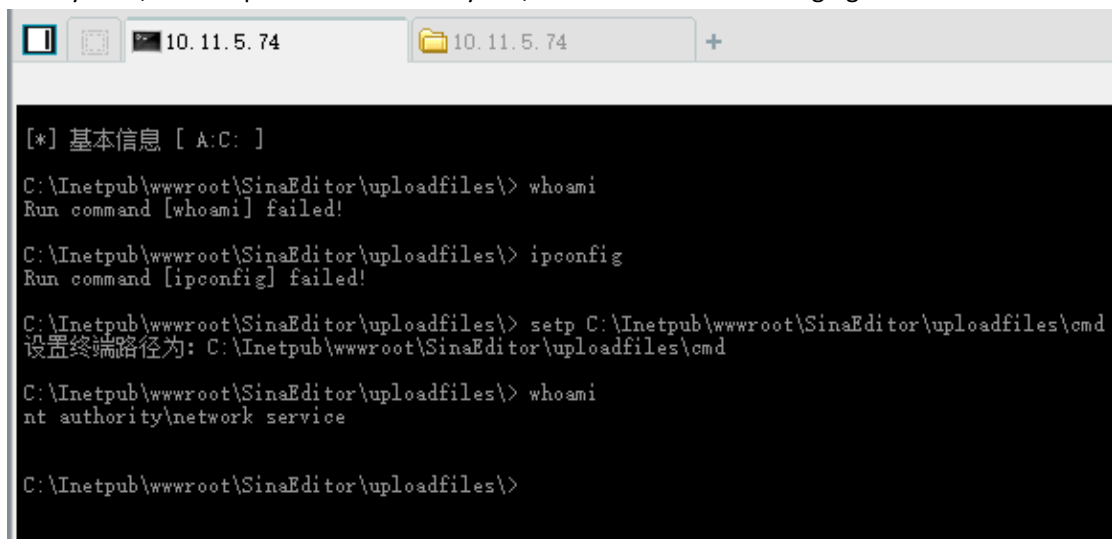


```
10.11.5.74 10.11.5.74 +
[*] 基本信息 [ A:C: ]
C:\Inetpub\wwwroot\SinaEditor\uploadfiles> whoami
Run command [whoami] failed!

C:\Inetpub\wwwroot\SinaEditor\uploadfiles> ipconfig
Run command [ipconfig] failed!

C:\Inetpub\wwwroot\SinaEditor\uploadfiles>
```

We can try to upload a cmd and use SETP to set the terminal path. The command is executed successfully here, but the permissions are very low, as shown in the following figure.



```
10.11.5.74 10.11.5.74 +
[*] 基本信息 [ A:C: ]
C:\Inetpub\wwwroot\SinaEditor\uploadfiles> whoami
Run command [whoami] failed!

C:\Inetpub\wwwroot\SinaEditor\uploadfiles> ipconfig
Run command [ipconfig] failed!

C:\Inetpub\wwwroot\SinaEditor\uploadfiles> setp C:\Inetpub\wwwroot\SinaEditor\uploadfiles\cmd
设置终端路径为: C:\Inetpub\wwwroot\SinaEditor\uploadfiles\cmd

C:\Inetpub\wwwroot\SinaEditor\uploadfiles> whoami
nt authority\network service

C:\Inetpub\wwwroot\SinaEditor\uploadfiles>
```

And thus, we can continue to escalate the system, as shown below.



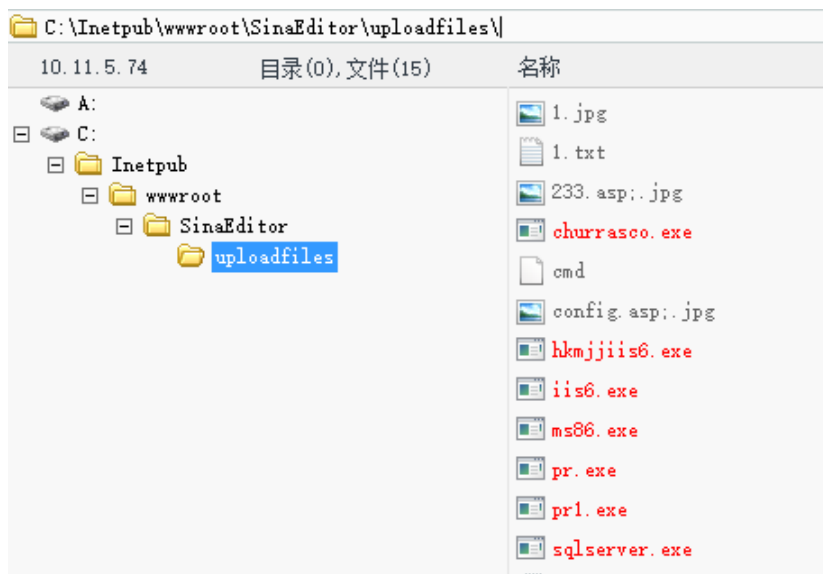
```
C:\Inetpub\wwwroot\SinaEditor\uploadfiles> C:\Inetpub\wwwroot\SinaEditor\uploadfiles\iis6.exe "net user admin123 admin1233 /add"
[IIS6Up] -> IIS Token PipeAdmin golds7n Version
[IIS6Up] -> This exploit gives you a Local System shell
[IIS6Up] -> Set registry OK
[process walking]: 3176 w3wp.exe
[process walking]: 13056 cmd
[process walking]: 13068 iis6.exe
[IIS6Up] -> Can not find wmiprvse.exe

C:\Inetpub\wwwroot\SinaEditor\uploadfiles> net user
\\SECSEVER 的用户帐户

Administrator      ASPNET              ftp
Guest              IUSR_SECSEVER      IWAM_SECSEVER
SUPPORT_388945a0
命令成功完成。

C:\Inetpub\wwwroot\SinaEditor\uploadfiles> C:\Inetpub\wwwroot\SinaEditor\uploadfiles\pr.exe "net user admin123 admin1233 /add"
Run command [C:\Inetpub\wwwroot\SinaEditor\uploadfiles\pr.exe "net user admin123 admin1233 /add"] failed!

C:\Inetpub\wwwroot\SinaEditor\uploadfiles> |
```



We can continue the penetration test, search for the database password, view the files of other websites, and upgrade the permissions of the database MySQL, as shown in the following figure.



3.4 Postscript

After getting the web shell, in addition to viewing permissions, the most important thing is to check whether there is any security software in the running programs. We can search it by browsing the files or probing through the files in the system.

4. Processing of penetration test results

During the design of penetration testing, a large account of boundaries needs to be set to prevent scope creep, (i.e., which devices, services, and networks that need to be tested, and which are not tested). The range depends on the goal of the penetration test. Be sure to record and save the scheme, because it will be the test framework after the penetration test, which can help we determine which test results should be analyzed and which are not.

Once we have identified the test results of those vulnerabilities within the scope of the test, then use various resources to verify the effectiveness. This is a crucial task because there is nothing that can always provide accurate information based on our test range. These resources generally

include network test results provided by tools like Nmap. In addition, the data can be compared with the results provided by vulnerability assessment tools such as Nessus.

Penetration testing is still an important method for discovering weak locations in network security, which though requires a lot of time and effort. If we do not specify a strategy for how to exploit the test results, the testing is meaningless. Only by confirming the test scope, verifying the results, using indicators to classify their severity, and reporting the findings concisely, the current network security risk status can be factually reflected.